Международный союз электросвязи

Безопасность в электросвязи и информационных технологиях

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

Декабрь 2003 года

МСЭ-Т Сектор Стандартизации Электросвязи МСЭ

Международный союз электросвязи

Безопасность в электросвязи и информационных технологиях

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

Выражение благодарности

В подготовку настоящего Руководства внесли вклад многие авторы, которые участвовали либо в разработке соответствующих Рекомендаций МСЭ-Т, либо в работе собраний исследовательских комиссий, практикумов и семинаров МСЭ-Т. Особой благодарности заслуживают следующие участники и авторы. Г-жа Лакшми Раман за подготовку пункта 6.4 и части текста раздела 2. Над редакцией последнего также работали г-да Херб Бертайн и Рао Васиреди. Данные для раздела 3, посвященного угрозам и рискам, получены по результатам работы МСЭ-Т, а также на основании доклада [Shannon]. Содержание раздела 5 и пункта 6.5 составлено по материалам [Wisekey], а также по материалам, любезно предоставленным проф. Дэйвидом Чадуиком, в частности для описания системы электронных рецептов в Солфорде в пункте 6.5.2 (также использованы материалы [Policy]). Описание VoIP и систем H.323 МСЭ-Т в пункте 6.1 подготовлено по данным [Packetizer] и [Euchner], а также по данным, любезно предоставленным г-ном Мартином Ойхнером. Основу пункта 6.2 составляет J.169 МСЭ-Т и подготовленный г-ном Эриком Розенфельдом обзор, содержащийся в пункте 6.1.2. Пункт 6.3 построен на материалах T.30 и T.36 МСЭ-Т. Признательность хочется также выразить многочисленным рецензентам, пожелавшим остаться неизвестными. В основе Приложения C лежит вклад многих экспертов из различных исследовательских комиссий МСЭ-Т, которые ответили на Вопросник по безопасности, разработанный ИК 17 МСЭ-Т, а Приложение B составлено по материалам Каталога Рекомендаций, связанных с безопасностью, который ведется экспертами МСЭ-Т в рамках Вопроса 10/17, в частности г-ном Шандором Мазгоном.

Содержание

Предисловие

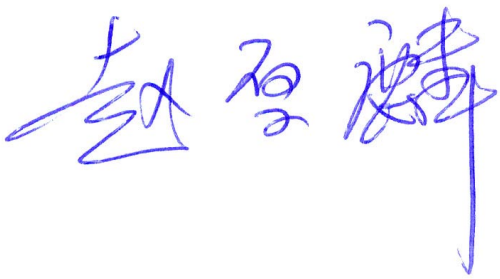
Цифровая безопасность, ограниченная в прошлом узкими областями применения, такими как банковские, авиакосмические и военные приложения, медленно, но неотвратимо становится необходимой для всех.

Возросшее значение цифровой безопасности может быть объяснено содержанием широко освещаемых новостей, как например сообщения о вирусах, распространяемых электронной почтой, или о хакерах, похищающих данные кредитных карт. Однако это только одна сторона явления. По мере того, как вычислительная техника и сети во все большей степени становятся частью нашей повседневной жизни, наравне с водой и электричеством, все чаще о цифровой безопасности говорят не только эксперты, но и в органах государственной власти, компаниях и потребители. А если так много аспектов нашей деловой и частной жизни зависят от компьютеров и сетей, абсолютно необходимо обеспечить защиту при эксплуатации этих систем.

Необходимо также, чтобы обеспечение безопасности осуществлялось как хорошо продуманный процесс: от планирования и проектирования системы, ее реализации до стратегии и методов развертывания, эксплуатации и применения этой системы. При разработке стандартов вопрос безопасности всегда должен решаться с самого начала, а не по окончании работ, – поскольку именно на этом этапе возникает уязвимость. Роль комитетов по стандартам заключается в анализе рынка и документов для выявления проблем, с тем чтобы по возможности найти обходные пути, а также в выпуске спецификаций или руководящих принципов, которые помогают конструкторам и пользователям создавать в достаточной степени устойчивые системы связи.

МСЭ-Т работает над проблемой безопасности в электросвязи и информационных технологиях в течение многих лет. Однако все еще не всегда бывает легко определить, какие именно вопросы охвачены, и где их можно найти. Настоящее Руководство – это первая попытка собрать воедино всю имеющуюся информацию. Я хотел бы выразить благодарность инженерам Бюро стандартизации электросвязи МСЭ, которые вместе с различными экспертами от членов МСЭ проделали бóльшую часть этой тяжелой работы. Руководство задумано как справочник в помощь технологам, руководителям среднего звена, а также регламентарным органам при практической реализации функций безопасности. На примере нескольких приложений в Руководстве поясняются вопросы безопасности и уделяется особое внимание тому, как они решаются в Рекомендациях МСЭ-Т.

Надеюсь, что данное Руководство окажется полезным для тех, кто занимается вопросами безопасности, и авторы будут благодарны читателям за предложения в отношении следующих изданий.



Хоулинь Чжао

Директор Бюро стандартизации электросвязи

МСЭ

Женева, декабрь 2003 года

Резюме

Отрасль связи, удовлетворяя потребности приобретающей глобальный характер среды торговли, способствует росту производительности и позволяет сообществам практически во всех промышленных секторах объединяться во всемирном масштабе. Столь высокая эффективность инфраструктуры электросвязи в немалой степени обусловлена наличием стандартов, которые разрабатывают такие организации, как МСЭ-Т. Стандарты, поддерживающие эффективность действующих сетей, также закладывают и основы для сетей следующего поколения. Однако хотя стандарты по-прежнему отвечают потребностям конечного пользователя и отрасли, растущие масштабы применения открытых интерфейсов и протоколов, многочисленность новых участников, огромное разнообразие приложений и платформ, а также продуктов, не всегда прошедших надлежащие испытания, увеличивают вероятность злонамеренного использования сетей. В последние годы резкий скачок случаев нарушения безопасности (таких как вирусы и нарушение конфиденциальности хранимых данных) наблюдается во всех глобальных сетях и зачастую приводит к существенным расходам. Следовательно, вопрос заключается в том, как организовать поддержку открытой инфраструктуры связи, не подвергая риску передаваемую информацию. Ответ дает деятельность групп по стандартам, направленная на борьбу с угрозами безопасности во всех элементах инфраструктуры связи – от детализации спецификаций протоколов и приложений до процесса управления сетями. Цель настоящего Руководства по безопасности заключается в том, чтобы выделить и дать общий обзор многочисленных разработанных МСЭ-Т, иногда в сотрудничестве с другими организациями по разработке стандартов, Рекомендаций по обеспечению защиты инфраструктуры связи и связанных с ней услуг и приложений.

Для рассмотрения многочисленных аспектов безопасности необходимо установить какую-то структуру и архитектуру, с тем чтобы иметь общий язык для обсуждения понятий.

В разделе 2 дается обзор архитектурных элементов, определенных в Рекомендации МСЭ-Т X.805, и восьми параметров безопасности, разработанных для решения проблемы межконцевой безопасности в сетевых приложениях – секретность, конфиденциальность данных, аутентификация, целостность, фиксация авторства, управление доступом, безопасность связи и готовность. Эти общие принципы используются для представления и толкования элементов, обсуждаемых в последующих разделах. Основными элементами являются слои безопасности, плоскости безопасности и параметры, применяемые к комбинации любого слоя с любой плоскостью.

В разделе 3 при обсуждении проблемы безопасности вводятся три ключевых термина: уязвимость, угроза и риск. Описаны отличительные особенности каждого из них и приведен ряд примеров. Основная задача данного раздела – показать, как возникает риск нарушения безопасности в результате одновременного существования уязвимости и угрозы.

Раздел 4 построен на информации предыдущих разделов в целях определения метатребований в отношении организации структуры безопасности. Ключевым условием обеспечения безопасности для борьбы с угрозами является определение механизмов и алгоритмов, связанных с мерами безопасности, такими как аутентификация, управление доступом и шифрование данных. В разделе 5 эти механизмы определяются с применением концепций инфраструктур открытого ключа и управления полномочиями. Эти механизмы и инфраструктуры могут применяться для большого числа различных приложений конечного пользователя.

Наряду с указанными структурой, архитектурой и механизмами МСЭ-Т разрабатываются положения по безопасности для ряда систем и услуг, которые определяются в его Рекомендациях. Вследствие этого большое внимание в настоящем Руководстве уделено приложениям, как это видно в разделе 6. В данном первом издании представлен выборочный набор приложений – голосовые и мультимедийные приложения на основе IP (H.323 и IPCablecom), приложения в области здравоохранения и для факсимильной передачи. Эти приложения описаны с точки зрения архитектуры развертывания и определения протоколов, удовлетворяющих потребности в безопасности. Наряду с обеспечением безопасности информации, используемой в приложениях, необходимо также защищать инфраструктуру сети и процесс управления сетевыми услугами. В раздел 6 включены также примеры стандартов, в которых определены положения безопасности, учитывающие аспекты управления сетью.

Кроме этого, в настоящее издание Руководства включен перечень акронимов и определений, связанных с безопасностью и другими вопросами, которые рассматриваются в данном документе. Этот перечень составлен на основе соответствующих Рекомендаций МСЭ-Т и иных источников (таких как терминологическая база данных МСЭ-Т SANCHO и справочники по безопасности систем связи, подготовленные 17-й Исследовательской комиссией МСЭ-Т). Перечень составляет Приложение A.

В данном Руководстве также содержится действующая версия каталога Рекомендаций МСЭ-Т, касающихся проблематики безопасности, – представленный в Приложении B перечень является полным и иллюстрирует масштабность проводимой МСЭ-Т работы в области безопасности. В Приложении C мы представили резюме связанной с безопасностью деятельности всех исследовательских комиссий МСЭ-Т. Содержание указанных приложений постоянно обновляется и размещается на Web-сайте по адресу www.itu.int/ITU-T.

И в заключение, проактивная деятельность МСЭ-Т ведется не только в области технологий, базирующихся на IP, но и направлена на удовлетворение потребностей многочисленных различных отраслевых сегментов, где требования в отношении обеспечения безопасности отличаются большим разнообразием. В настоящем Руководстве показано, каким образом можно применять содержащиеся в Рекомендациях МСЭ-Т решения – как в отношении общей структуры и архитектуры, так и для конкретных систем и приложений, которые благодаря поставщикам сетей и услуг уже получили всемирное распространение.

1 Область применения Руководства

В настоящем Руководстве дается обзор проблемы безопасности в области электросвязи и информационных технологий, в нем освещены практические вопросы и показано, как МСЭ-Т решает различные задачи безопасности. Руководство носит учебный характер: в нем сведены воедино соответствующие материалы из Рекомендаций МСЭ-Т и объяснена взаимосвязь между ними. В данном первом издании Руководства охвачены не все аспекты безопасности, в частности не включены вопросы, связанные с готовностью, по которым МСЭ-Т может предложить обширную информацию, а также вопросы экологического ущерба, решением которых также активно занимается МСЭ-Т. Представленные здесь аспекты определены по результатам проведенной работы, а аспекты, по которым ведутся работы, войдут в последующие издания настоящего Руководства.

Руководство адресовано инженерам и управляющим по продуктам, студентам и научному сообществу, а также сотрудникам регламентарных органов, стремящимся более глубоко разобраться в вопросах безопасности применяемых на практике приложений.

2 Базовая архитектура и основные параметры безопасности

В Рекомендации X.805 определена общая структура архитектуры и параметров при обеспечении межконцевой безопасности распределенных приложений. Общие принципы и определения применимы ко всем приложениям, хотя такие более частные вопросы как угрозы и уязвимость, а также меры противодействия им или меры по их предупреждению в значительной степени зависят от области действия конкретного приложения.

Архитектура безопасности определяется двумя основными понятиями: слой и плоскость. Слои безопасности связаны с выполнением требований, которые применимы к сетевым элементам и системам, образующим сквозную сеть. При распределении требований по слоям применяется иерархический подход в целях достижения межконцевой безопасности за счет обеспечения безопасности каждого слоя. Тремя слоями являются: слой инфраструктуры, слой услуг и слой приложений. Одним из преимуществ основанного на определении слоев подхода является возможность его многократного применения для обеспечения межконцевой безопасности различных приложений. Степень уязвимости каждого слоя различна, и, следовательно, меры противодействия должны определяться исходя из задач, выполняемых каждым слоем. Слой инфраструктуры образуют сетевые средства передачи, а также отдельные сетевые элементы. Примерами относящихся к слою инфраструктуры элементов могут служить маршрутизаторы, коммутаторы и серверы, а также каналы связи между ними. Слой услуг определяет безопасность предлагаемых потребителям сетевых услуг. Они составляют широкий диапазон – от услуг базового подключения, таких как услуги выделенных линий, до дополнительного сервиса, такого как мгновенный обмен сообщениями. Слой приложений обеспечивает выполнение требований к сетевым приложениям, используемым потребителями. Приложения могут быть простыми, как электронная почта, или сложными, как групповая визуализация, где используются сверхвысокопроизводительные передатчики видеоинформации для ведения нефтепоисковых работ или проектирования автомобилей и т. д.

Вторая составляющая структуры связана с безопасностью деятельности, осуществляемой в сетевой среде. В рамках концепции безопасности определяются три плоскости безопасности, которые отражают три типа защищаемой деятельности, возможной в сетевой среде. Плоскостями безопасности являются: 1) плоскость административного управления, 2) плоскость оперативного управления и 3) плоскость конечного пользователя. Плоскости безопасности обеспечивают конкретные потребности, связанные с административным управлением сетью, оперативным управлением сети или управлением сигнализацией и деятельностью конечного пользователя, соответственно. Плоскость административного управления, подробно описываемая в пункте 6.4, связана с функциями Эксплуатации, Администрирования, Технического обслуживания и Обеспечения (OAM&P), такими как обеспечение пользователя или сети и т. д. Плоскость оперативного управления связана с вопросами сигнализации для настройки (и модификации) межконцевой связи по сети независимо от среды передачи и технологии, используемых в сети. Плоскость конечного пользователя обеспечивает безопасность доступа и использования сети потребителями. Эта плоскость также служит для защиты потоков данных конечного пользователя.

Наряду с двумя составляющими – слоями безопасности и плоскостями безопасности (три плоскости безопасности и три слоя безопасности) – в рамках структуры определены также восемь параметров, разработанных для решения проблемы сетевой безопасности. Эти параметры определяются в нижеследующих разделах. В архитектурном аспекте указанные параметры применяются к каждой ячейке 3×3 матрицы, образуемой между слоями и плоскостями, с тем чтобы могли быть определены меры противодействия. На рисунке 1 показаны плоскости, слои и параметры архитектуры безопасности. В разделе 6.4, посвященном плоскости административного управления, показано, какой в Рекомендациях МСЭ-Т принят подход к трем ячейкам 3×3 матрицы для плоскости административного управления.

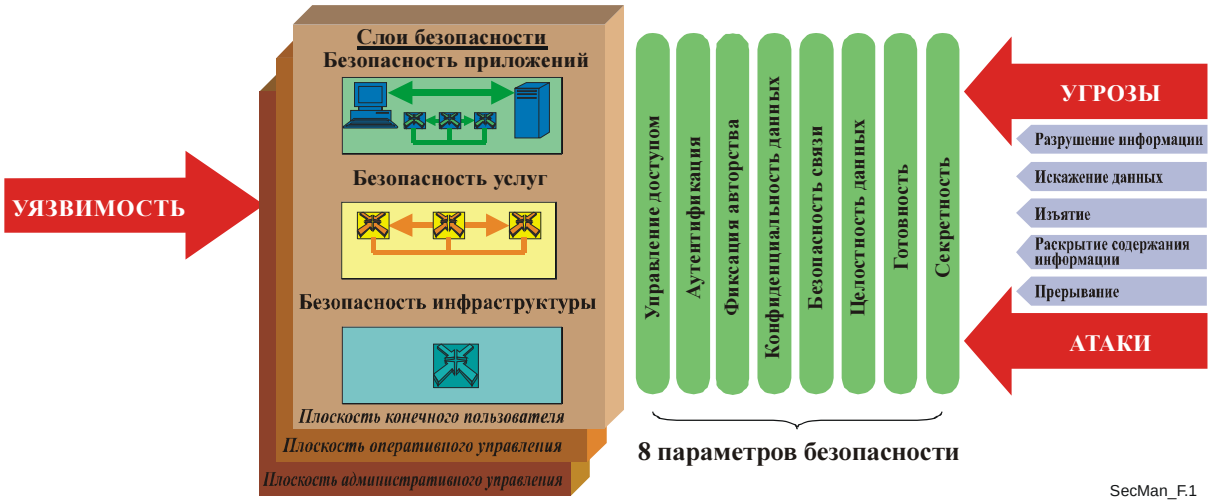


Рисунок 1
Элементы архитектуры безопасности согласно Рекомендации МСЭ-Т X.805

2.1 Секретность и конфиденциальность данных

Понятие секретности является основным мотивационным фактором обеспечения безопасности. Под секретностью обычно понимается право частного лица контролировать или воздействовать на то, какая касающаяся его информация может быть собрана и сохранена, а также кем и кому содержание этой информации может быть открыто. В расширенном значении секретность также связывается с определенными техническими средствами (как например криптография), которые обеспечивают невозможность раскрытия содержания этой информации лицами, для сведения которых она не предназначена, то есть содержание информации, которой обмениваются стороны, доступно только тем, кто имеет на это конкретное разрешение.

В основном секретность и конфиденциальность используются как равнозначные термины, однако следует отметить, что в Рекомендации МСЭ-Т X.805 проводится различие между понятиями секретность и конфиденциальность данных – первое относится к защите ассоциации идентификационной информации пользователей и действий, выполняемых ими (таких как принятый порядок осуществления покупок в онлайновом режиме, посещаемые сайты Интернет и т. д.), в то время как второе относится к защите от несанкционированного доступа к содержанию данных. Для обеспечения конфиденциальности данных, как правило, используются такие методы, как шифрование, списки управления доступом и права доступа к файлу.

Термин “секретность” встречается в нескольких Рекомендациях МСЭ-Т, в том числе в Рекомендациях F.115, H.235, J.160, Q.1531, X.800 и X.805.

2.2 Аутентификация

Аутентификацией называется обеспечение доказательства того, что предъявленная идентификационная информация данного объекта является верной. В настоящем Руководстве термин “объект” включает не только пользователей – физических лиц, но и устройства, услуги и приложения. Аутентификация служит также для гарантирования того, что объект не предпринимает попытки нелегального проникновения или не генерирует неразрешенную повторную передачу перехваченного сообщения предыдущей передачи. Существуют два типа аутентификации: аутентификация источника данных (то есть аутентификация, запрошенная в ассоциации с установлением связи) и аутентификация равноправного объекта (то есть аутентификация в ассоциации без установления связи). Сеть должна гарантировать установление обмена данными с равноправным объектом – адресатом (но не с объектом, предпринимающим попытку нелегального проникновения или генерирующим повторную передачу перехваченного сообщения по предыдущему соединению) и идентичность заявленного источника данных. Аутентификация обычно следует после идентификации. Защиту информации, используемой для идентификации, аутентификации и авторизации, должна осуществлять сеть.

Термин "аутентификация" встречается в нескольких Рекомендациях МСЭ-Т, в том числе в Рекомендациях F.500, F.851, F.852, H.235, J.160, J.93, M.60, X.217, X.217-bis, X.509, X.800, X.805 и X.811.

2.3 Целостность

Целостность данных – это показатель того, что данные не были изменены несанкционированным образом. В более широком смысле целостность данных гарантирует также, что информация защищена от неразрешенного изменения, удаления, создания и дублирования, а также обеспечивает индикацию попыток осуществления таких несанкционированных действий.

Термин "целостность" встречается в нескольких Рекомендациях МСЭ-Т, в том числе в Рекомендациях H.235, J.160, J.93, J.95, Q.1290, Q.1531, X.800 и X.815.

2.4 Фиксация авторства

Фиксация авторства – это способность предотвратить отказ пользователя от признания выполненных им действий. Таковыми действиями являются: создание, передача, прием и доставка контента, например отправка или прием сообщений, установление или прием вызовов, участие в аудио- и видеоконференциях и т. д.

Требования к обеспечению фиксации авторства предусматривают предоставление неопровержимых доказательств факта отправки и/или приема данных, с тем чтобы не допустить отказа отправителя от законного сообщения или отрицания адресатом получения сообщения. Сеть может обеспечивать один или оба следующих режима: либо прием данных осуществляется с проверкой источника данных, что защищает от любой попытки отправителя неправомерно отказаться от передачи данных или от их контента, либо отправитель располагает средствами подтверждения доставки данных, так что получатель не может впоследствии отрицать факт получения данных или их контента.

Термин "фиксация авторства" встречается в нескольких Рекомендациях МСЭ-Т, в том числе в Рекомендациях F.400, F.435, F.440, J.160, J.93, J.95, M.60, T.411, X.400, X.805, X.813 и X.843.

2.5 Другие параметры, определенные в Рекомендации X.805

Наряду с понятиями Секретность и Конфиденциальность данных, Аутентификация, Целостность и Фиксация авторства, в Рекомендации МСЭ-Т X.805 определяются еще три параметра безопасности: Управление доступом, Связь и Готовность.

Параметр безопасности *Управление доступом* служит для защиты от несанкционированного использования сетевых ресурсов. Управление доступом обеспечивает предоставление разрешения на доступ к сетевым элементам, хранимой информации, медиапотокам, услугам и приложениям только уполномоченным персоналу или устройствам. Управление доступом определяется в пункте 6.3 Рекомендации МСЭ-Т X.810 и в Рекомендации МСЭ-Т X.812. Оно связано с аутентификацией, но не выходит в сферу ее охвата.

Параметр безопасности *Связь* является новым параметром, определенным в X.805, который служит для обеспечения передачи медиапотоков только между имеющими соответствующие полномочия конечными точками. Этот параметр относится к мерам по управлению потоками трафика в сети, направленным на защиту трафика от переадресации и перехвата.

Параметр безопасности *Готовность* используется для обеспечения отсутствия отказа в санкционированном доступе к сетевым элементам, хранимой информации, медиапотокам, услугам и приложениям вследствие сетевого прерывания. К этой категории относятся меры по возвращению сети в исходное состояние и восстановлению после аварии.

3 Уязвимость, угрозы и риски

При том огромном внимании, которое уделяется реализации наиболее выгодных решений на базе ИТ или определению того, какие из самых современных и масштабных Web-приложений, серверов и баз данных в наибольшей степени отвечают целям организации, проблема защиты информации, которую обрабатывают эти средства, зачастую приобретает второстепенное значение. На многих предприятиях бытует ошибочное мнение, что отсутствие попыток нападения означает отсутствие угрозы.

Органы стандартизации имеют уникальную возможность и исключительные полномочия решить проблему уязвимости безопасности на уровне протоколов. Органы стандартизации могут предпринять немедленные и относительно несложные действия по повышению уровня безопасности всех протоколов, находящихся в настоящее время в процессе стандартизации.

Уязвимость безопасности это недоработки или недостатки проекта, реализации или эксплуатации системы, которые могут привести к нарушению безопасности системы (RFC 2828). Уязвимость безопасности не является риском, угрозой или атакой.

Уязвимость бывает четырех типов. Уязвимость *модели угроз*, обусловленная сложностью предсказания будущих угроз (например, система сигнализации №7). Уязвимость *проекта и спецификации*, являющаяся следствием ошибок и упущений при разработке протокола, которые делают такой протокол уязвимым по сути (например, WEP в IEEE 802.11b a.k.a. WiFi). Уязвимость *реализации*, которая представляет собой уязвимость, вносимую ошибками реализации протокола. Наконец, уязвимость *эксплуатации и конфигурации*, возникающая в результате ненадлежащего использования опций или неэффективной политики внедрения (например, непридание законной силы применению шифрования в сети WiFi или выбор администратором сети неустойчивого поточного шифра).

Согласно X.800 *угроза безопасности* – это потенциальное нарушение безопасности, которое может быть активным (когда возможно изменение состояния системы) и пассивным (несанкционированное раскрытие содержания информации без изменения состояния системы). Примерами активных угроз являются нелегальное проникновение под видом полномочного объекта или отказ в обслуживании, а в качестве примера пассивной угрозы можно привести подслушивание в целях захвата нешифрованного пароля. Угрозы могут исходить от хакеров, террористов, вандалов, группировок организованной преступности или от государства, но в подавляющем большинстве случаев источники угроз находятся в самом учреждении.

Риск нарушения безопасности возникает при сочетании уязвимости безопасности и угрозы безопасности. Например, дефект переполнения в приложении операционной системы (то есть уязвимость) в сочетании с осведомленностью об этом хакера, наличием соответствующих инструментов и доступа (то есть угроза) может привести к возникновению риска атаки на Web-сервер. Последствиями рисков нарушения безопасности являются потеря данных, искажение данных, потеря секретности, подлог, простой и утрата доверия сообщества пользователей.

В то время как угрозы могут меняться, уязвимость безопасности существует на протяжении всего срока эксплуатации протокола. Риски нарушения безопасности, обусловленные свойствами протокола, в случае стандартизованных протоколов могут быть весьма существенными и глобальными по масштабу. Следовательно, важно понять и выявить уязвимость протоколов.

4 Требования к структуре системы безопасности

Требования к общей структуре сетевой безопасности обусловлены совокупностью различных факторов:

- Потребителям/абонентам необходимо испытывать доверие к предлагаемым сетям и услугам, включая готовность услуг (особенно экстренного обслуживания) в условиях крупных катастроф (включая террористические акты).
- Органы государственной власти предъявляют требования к безопасности, издавая директивы и применяя законодательство, с тем чтобы обеспечить готовность услуг, добросовестную конкуренцию и защиту частной жизни.
- Операторы сетей и поставщики услуг сами нуждаются в обеспечении безопасности для защиты своих эксплуатационных и коммерческих интересов и выполнения своих обязательств перед потребителями и населением.

Требования к безопасности сетей и услуг электросвязи должны базироваться преимущественно на согласованных на международном уровне стандартах безопасности, поскольку это повышает степень функциональной совместимости, а также позволяет избегать дублирования усилий и не заниматься изобретением колеса. Предоставление и использование услуг и механизмов, обеспечивающих безопасность, может быть довольно дорогим относительно стоимости защищаемых транзакций. Следует проанализировать соотношение между стоимостью мер по обеспечению безопасности и возможными финансовыми последствиями нарушения безопасности. Таким образом, важным фактором является возможность определить параметры безопасности в соответствии с услугами, подлежащими защите. Используемые услуги и механизмы обеспечения безопасности должны предоставляться таким образом, который допускает указанную параметризацию. Учитывая большое количество возможных сочетаний функций обеспечения безопасности, желательно иметь профили безопасности, охватывающие широкий диапазон сетевых услуг электросвязи.

Содействовать повторному применению решений и продуктов будет стандартизация, ускоряющая обеспечение безопасности и делающая ее менее дорогой.

Существенными преимуществами применения стандартизованных продуктов и для продавцов, и для пользователей систем являются экономия масштаба при разработке продуктов и функциональная совместимость компонентов в среде сети электросвязи в отношении безопасности.

Услуги и механизмы обеспечения безопасности, которые могут быть использованы в сетях электросвязи или поставщиками услуг, относятся к средствам защиты от преднамеренных атак, таких как отказ в обслуживании, подслушивание, имитация соединения, искажение сообщений (изменение, задержка, удаление, вставка, повторная передача перехваченного сообщения, перемаршрутизация, неправильная маршрутизация или изменение порядка следования сообщений), отказ от авторства или фальсификация. Защита включает предупреждение, локализацию и восстановление после атаки, меры по предотвращению прерываний в обслуживании вследствие естественных событий (погодные условия и т. д.), а также управление связанной с безопасностью информацией. Должны быть определены условия, разрешающие санкционированный перехват по запросу должным образом уполномоченных правоприменительных органов.

5 PKI и управление полномочиями в соответствии с X.509

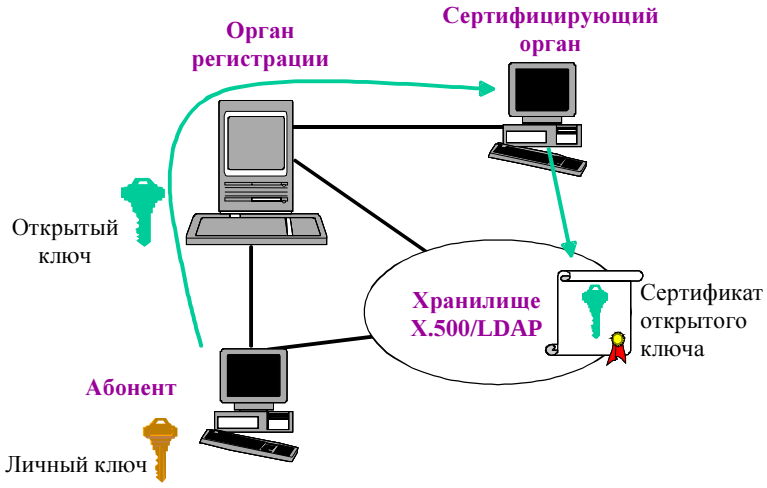
Инфраструктура открытого ключа (PKI) в соответствии с X.509 обеспечивает стандарт для жесткой аутентификации, базирующейся на сертификатах открытого ключа и полномочиях на сертификацию. PKI обеспечивает расширяемый метод аутентификации сообщения сторон, участвующих в сеансе связи. Базовой технологией PKI является шифрование с открытым ключом, в силу чего эта технология будет описана первой. Наряду с PKI, X.509 обеспечивает также инфраструктуру управления полномочиями (PMI), которая описывает стандарт жесткой авторизации, базирующейся на сертификатах атрибута и полномочиях в отношении атрибута. PMI используется для установления прав и привилегий пользователей. Компоненты PKI и PMI представлены на рисунке 2.

5.1 Шифрование с секретным и открытым ключом

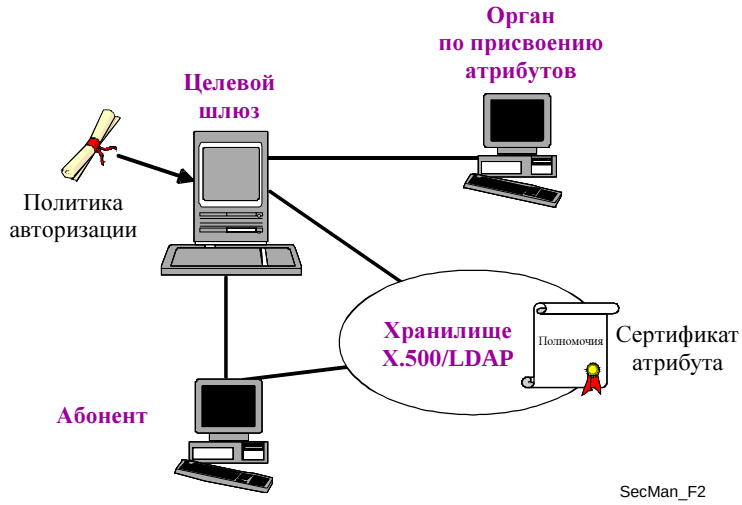
Симметричное (или *с секретным ключом*) шифрование относится к криптографическим системам, в которых используются одинаковые ключи шифрования и дешифрования, как показано на рисунке 3a). Симметричные криптосистемы требуют начальных соглашений для лиц, совместно использующих уникальный секретный ключ. Ключ должен быть распространен среди соответствующих лиц с помощью надежных средств, поскольку знание ключа шифрования означает знание ключа дешифрования и наоборот.

Асимметричное (или *с открытым ключом*) шифрование включает пару ключей, как показано на рисунке 3b): открытый ключ и личный ключ. Один ключ является открытым, а другой – секретным. Открытый ключ отличается от личного ключа и несмотря на математическую связь между ними, реального способа вывода личного ключа из открытого ключа не существует. Открытые ключи распространяются широко, в то время как личный ключ всегда хранится в секрете (например, на кредитной карточке с микропроцессором или на жетоне, а в будущем также в PDA или в мобильном телефоне). В общем смысле для того, чтобы отправить кому-либо зашифрованные конфиденциальные данные, отправитель шифрует данные с помощью открытого ключа получателя, а получатели зашифрованных данных дешифруют их с помощью своих соответствующих личных ключей. Для отправки кому-либо аутентифицированных данных отправитель шифрует данные с помощью своего личного ключа, а получатель проводит аутентификацию данных с помощью соответствующего открытого ключа отправителя. Однако используемое таким образом асимметричное шифрование имеет два недостатка. Во-первых, шифрование с открытым ключом является дорогостоящим за счет времени вычисления, поэтому неэффективно шифровать целые сообщения, используя асимметричное шифрование. Во-вторых, невозможно направлять сообщения к адресатам, если зашифровано все сообщение целиком, поскольку промежуточные узлы не смогут определить получателя такого сообщения. Вследствие этого асимметричное шифрование используется на практике только для шифрования небольших частей сообщений. Если необходима конфиденциальность, сообщение шифруется с помощью традиционного симметричного шифрования, а симметричный ключ шифруется асимметрично с помощью открытого ключа получателя. Если необходима аутентификация, сообщение рандомизируется с помощью безопасной односторонней функции рандомизации, как например SHA1 или MD5, а результирующая 160-ти или 128-ми битовая хеш-функция асимметрично шифруется с помощью личного ключа отправителя и добавляется в сообщение (которое посылается открытым текстом) до его отправки. Такая добавленная криптографическая контрольная последовательность называется цифровой подписью и является важным параметром электронной торговли.

Шифрование с открытым ключом находится в зависимости от людей, которые владеют верными открытыми ключами их соответствующих держателей частных ключей. Если Боб ошибочно полагает, что владеет открытым ключом Элис, в то время как этот открытый ключ на самом деле принадлежит личному ключу, которым владеет Джейн, Боб будет думать, что сообщения, имеющие цифровую подпись Джейн, на самом деле поступают от Элис (что позволит Джейн осуществлять нелегальное проникновение под именем Элис). Кроме этого, если Боб хочет послать конфиденциальное сообщение Элис, Джейн сможет перехватить и расшифровать это сообщение, в то время как Элис не сможет его прочитать. Таким образом, ключевым фактором является наличие способа проверки подлинности законного владельца открытого ключа.

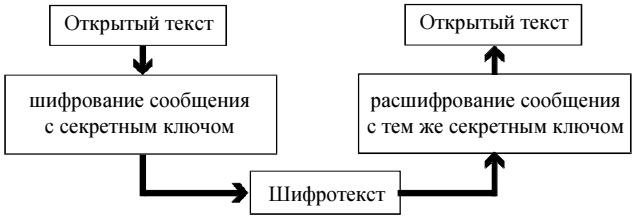


a) Компоненты инфраструктуры с открытым ключом



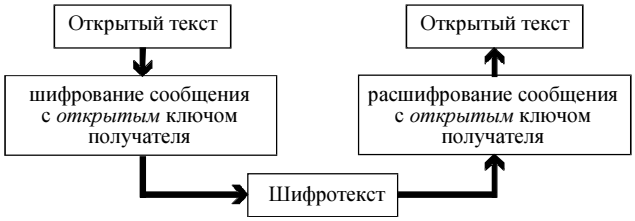
b) Компоненты инфраструктуры управления полномочиями

Рисунок 2
Компоненты PKI и PMI



– Обе стороны пользуются единым секретным ключом
– Проблема: сложно обеспечить обмен ключами при полной секретности
– Наилучший пример: DES (стандарт шифрования данных)

a) Шифрование с (симметричным) секретным ключом



Каждый участник имеет
– Личный ключ, которым более никто не владеет, и
– Открытый ключ, известный всем

Проблема: медленнее, чем шифрование с секретным ключом
Наилучший пример: RSA

b) Шифрование с (ассиметричным) открытым ключом

SecMan_F3

Рисунок 3
Схема процессов шифрования с симметричным (или с личным) и асимметричным (или с открытым) ключами и их особенности

5.2 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 стандарте X.509. Говоря кратко, сертификат открытого ключа 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 времени действия сертификата, номера версии X.509, которой соответствует данный сертификат, и не имеющего обязательного характера набора полей расширения, в которых хранится информация о стратегии сертификации указанного CA. Затем сертификат целиком сопровождается цифровой подписью, для которой используется личный ключ CA. Теперь сертификат X.509 может быть опубликован без ограничений, например на Web-сайте, в директории LDAP или в V-карте, присоединяемой к сообщениям электронной почты, а подпись CA гарантирует, что его содержание не может быть случайным образом подделано.

Очевидно, что для обеспечения возможности проверки подлинности сертификата отрытого ключа пользователя необходимо иметь доступ к действительному открытому ключу того CA, который выдало сертификат пользователя, с тем чтобы проверить подпись на сертификате пользователя. Открытый ключ CA может быть сертифицирован другим (вышестоящим) CA, в результате чего по мере продвижения по цепочке сертификатов проверка подлинности открытых ключей приобретает рекурсивный характер. В итоге эта цепочка должна иметь некую конечную точку, где, как правило, находится сертификат CA, являющегося “корнем доверия”, который подписан им самим. 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, что ключ и наименование CA не подделывались с момента создания сертификата. Однако мы не можем

безоговорочно принять наименование CA, заключенное в им самим подписанном сертификате, поскольку CA сам вставил наименование в сертификат. Таким образом, имеющим критическое значение компонентом инфраструктуры открытого ключа является метод безопасного распространения открытых ключей корневых CA (как ими самими подписанных сертификатов), 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.

5.3 Инфраструктуры открытых ключей

Основным назначением PKI является выдача сертификатов открытых ключей и управление ими, включая сертификаты корневого CA, подписанные им самим. Управление ключами включает создание конкретной пары ключей, создание сертификатов открытых ключей, аннулирование сертификатов открытых ключей (например, если открытый 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, а стандарт X.509 предоставляет механизмы для распространения информации (ее части) об этой стратегии в полях расширения сертификатов X.509, выданных данным CA. Стратегические правила и процедуры, которым следует CA, как правило определяются в стратегии применения сертификатов (CP) и в заявлении о практике применения сертификатов (CPS), публикуемых данным CA. Указанные документы способствуют обеспечению общей основы качества для оценки того, насколько можно доверять сертификатам открытых ключей, выданных данным CA, как на международном уровне, так и на уровне секторов. Эти документы также обеспечивают нам правовые рамки (частично), необходимые для создания межучрежденческого доверия, а также для определения ограничений на использование выданных сертификатов.

Следует отметить, что в целях аутентификации с использованием сертификатов открытых ключей необходимы конечные точки для обеспечения цифровых подписей с использованием значения связанного личного ключа. Только лишь обмен сертификатами открытых ключей не защищает от опасных атак при вмешательстве извне (типа “человек-посредник”).

5.4 Инфраструктура управления полномочиями

В первых версиях Рекомендации МСЭ-Т X.509 содержалось описание базовых элементов инфраструктур открытых ключей (PKI). В них же давалось определение сертификатов открытых ключей. Утвержденное в 2000 году пересмотренное издание содержит существенно расширенные характеристики сертификатов атрибутов и основу для инфраструктуры управления полномочиями. Описанные механизмы позволяют осуществлять установку полномочий доступа пользователя в среде, объединяющей оборудование различных производителей и многочисленные приложения.

Концепции PMI и PKI весьма сходны, но первое относится к авторизации, а область действия второго – аутентификация. На рисунке 2 и в таблице 1 показано сходство двух инфраструктур.

Таблица 1
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 гарантировании того, что они выполняют предписанную стратегию безопасности, установленную источником полномочий. Информация, касающаяся стратегии, увязывается с именем пользователя в сертификате атрибута и состоит из ряда элементов, показанных на рисунке 4.

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

Рисунок 4
Структура сертификата атрибута согласно X.509

Для управления PMI в Рекомендации X.509 описаны пять компонентов: контролер полномочий, верификатор полномочий, объектный метод[1], стратегия присвоения полномочий и переменные среды (см. рисунок 5). Эти компоненты позволяют верификатору полномочий управлять доступом к объектному методу с помощью контролера полномочий в соответствии со стратегией предоставления полномочий.

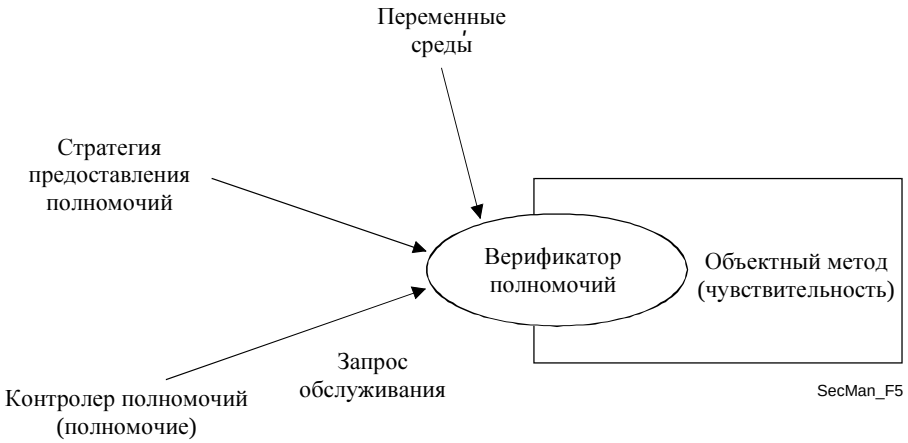


Рисунок 5
Модель управления PMI согласно Рекомендации МСЭ-Т X.509

Если для какой-либо реализации необходимо делегирование полномочий, в Рекомендации X.509 рассмотрены четыре компонента модели делегирования для PMI: верификатор полномочий, SoA, другие AA и контролер полномочий (см. рисунок 6).

[1] Объектный метод определяется как действие, которое может быть осуществлено в отношении ресурса (например, файловая система может иметь объектные методы для чтения, записи и выполнения).

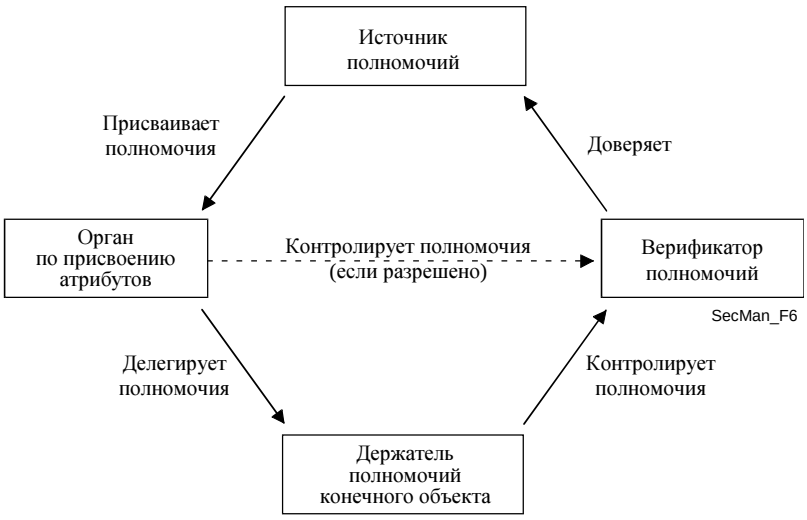


Рисунок 6
Модель делегирования для PMI согласно Рекомендации МСЭ-Т X.509

В последних реализациях схем авторизации, соответствующих модели управления доступом по ролевому признаку (RBAC), предполагается, что конкретному пользователю присваивается некая роль. Стратегия авторизации связывает набор разрешений и роль. При доступе к ресурсу роль, которая присвоена пользователю, проверяется согласно правилам стратегии для получения разрешения на выполнение каких-либо последующих действий. Система электронных рецептов, описанная в пункте 6.5.2, является иллюстрацией применения системы RBAC.

6 Приложения

Рассматриваемые в настоящем разделе приложения относятся к двум разным классам. Первый класс составляют приложения, ориентированные на конечного пользователя. Одним из примеров таких приложений является VoIP, для которого описаны архитектура и компоненты сети, используемые для обеспечения функционирования этого ориентированного на конечного пользователя приложения. Вопросы безопасности и примененные решения по обеспечению безопасности представлены для трех плоскостей, которые поддерживают мультимедийные приложения с VoIP как отдельный случай. В данной работе рассмотрены другие ориентированные на пользователя приложения – система IPCablecom, которая предоставляет в режиме реального времени базирующиеся на IP услуги по кабельным сетям и услуги по передаче факсимильных сообщений. Рассмотрены также приложения, не относящиеся исключительно к отрасли электросвязи, а именно приложения в области электронного здравоохранения, в частности система электронных рецептов. Ко второму классу относятся приложения, предназначенные для управления сетью. Важным аспектом здесь является безопасность, необходимая для обеспечения качества и целостности услуг, предоставляемых поставщиками. Таким образом, обязательным является предоставление функциям управления соответствующих полномочий и авторизации.

6.1 VoIP с использованием систем H.323

Передача голоса по IP (VoIP), известная также как IP-телефония, это предоставление по сети с использованием протокола IP (на котором также базируется Интернет) услуг, традиционно предоставляемых по ТСОП с коммутацией каналов. К таким услугам относятся основные услуги по передаче речи и соответствующие дополнительные услуги, как например голосовые 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 Интернет представляет собой частный случай VoIP, когда трафик речевых сообщений переносится по магистралям общедоступного Интернет.

H.323 является “зонтичной” Рекомендацией МСЭ-Т, формирующей основу для передачи звуковых сигналов, видеоряда и данных по локальным вычислительным сетям (ЛВС) или по сетям, базирующимся на протоколе IP, включая Интернет, 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. При условии

соответствия положениям H.323 мультимедийные продукты и приложения различных производителей могут быть функционально совместимыми, обеспечивая таким образом для пользователей возможность связи без проблем совместимости. H.323 был первым получившим определение протоколом VoIP и считается основой для функционирующих в среде ЛВС продуктов, применяемых в сферах торговли, коммерческой деятельности, индустрии развлечений и профессиональных приложений. Важными Рекомендациями, составляющими части системы H.323, являются:

- H.323 – "зонтичный" документ, в котором описывается использование H.225.0, H.245 и других соответствующих документов для предоставления услуг мультимедийных конференций в пакетном режиме.
- H.225.0 – описывает три протокола сигнализации (RAS, сигнализации о соединении и "Приложение G").
- H.245 – Протокол управления для мультимедийной связи (общая с H.310, H.323 и H.324)
- H.235 – Безопасность для систем на базе H.245
- H.246 – Межсетевое взаимодействие с ТСОП
- H.450.x – Дополнительные услуги
- H.460.x – Различные расширения протокола H.323
- H.501 – Протокол для управления мобильностью и внутри-/междоменной связи
- H.510 – Пользователь, терминал и мобильность услуг
- H.530 – Спецификация безопасности для H.510

МСЭ-Т утвердил первую версию спецификации H.323 в 1996 году. Версия 2 была утверждена в январе 1998 года, а действующая версия 5 утверждена в июле 2003 года. Стандарт имеет широкую область применения и охватывает как автономные устройства, так и системы на базе персональных компьютеров, а также двухточечные и многоточечные конференции. В H.323 также рассматриваются вопросы управления соединением, управления мультимедийной связью, управления широкополосной связью и интерфейсы между ЛВС и другими сетями.

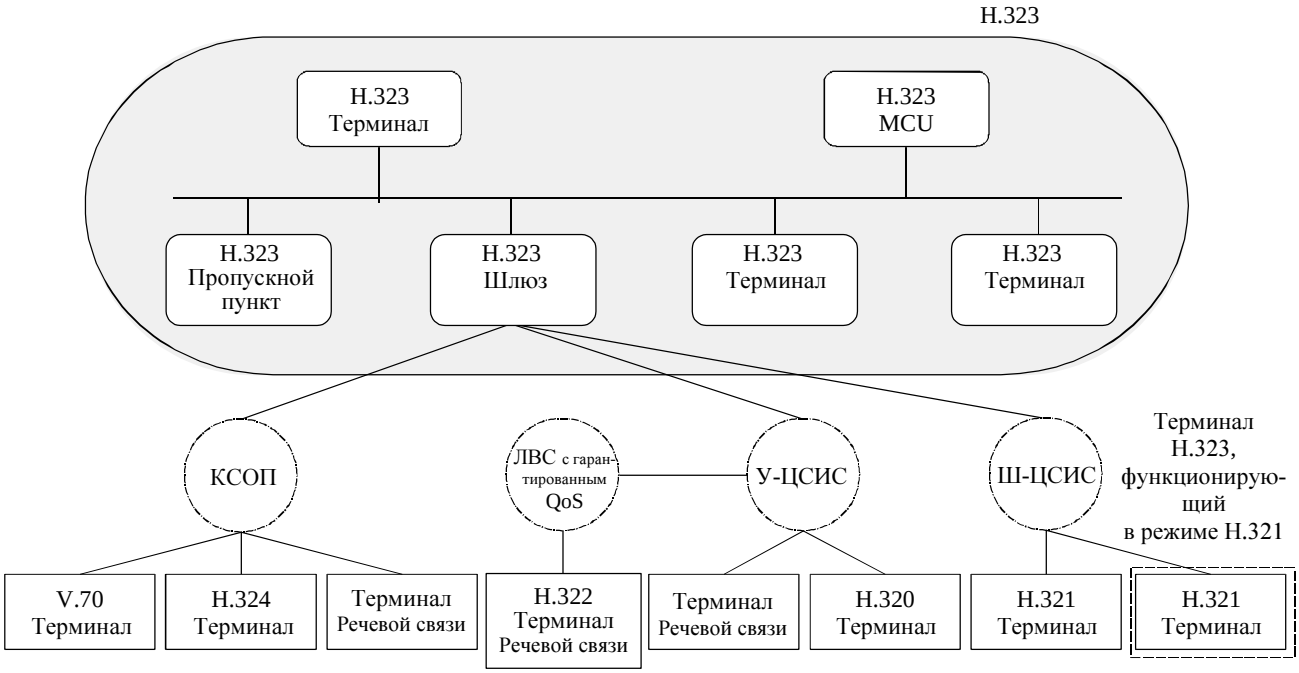
H.323 является частью крупной серии стандартов связи, обеспечивающих возможность организации видеоконференций в рамках широкого диапазона сетей. Известная как H.32X, эта серия включает Рекомендации H.320 и H.324, в которых рассматриваются, соответственно, связь по ЦСИС и ТСОП. В настоящем Руководстве дается обзор стандарта H.323, его достоинств, архитектуры и приложений.

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 7.

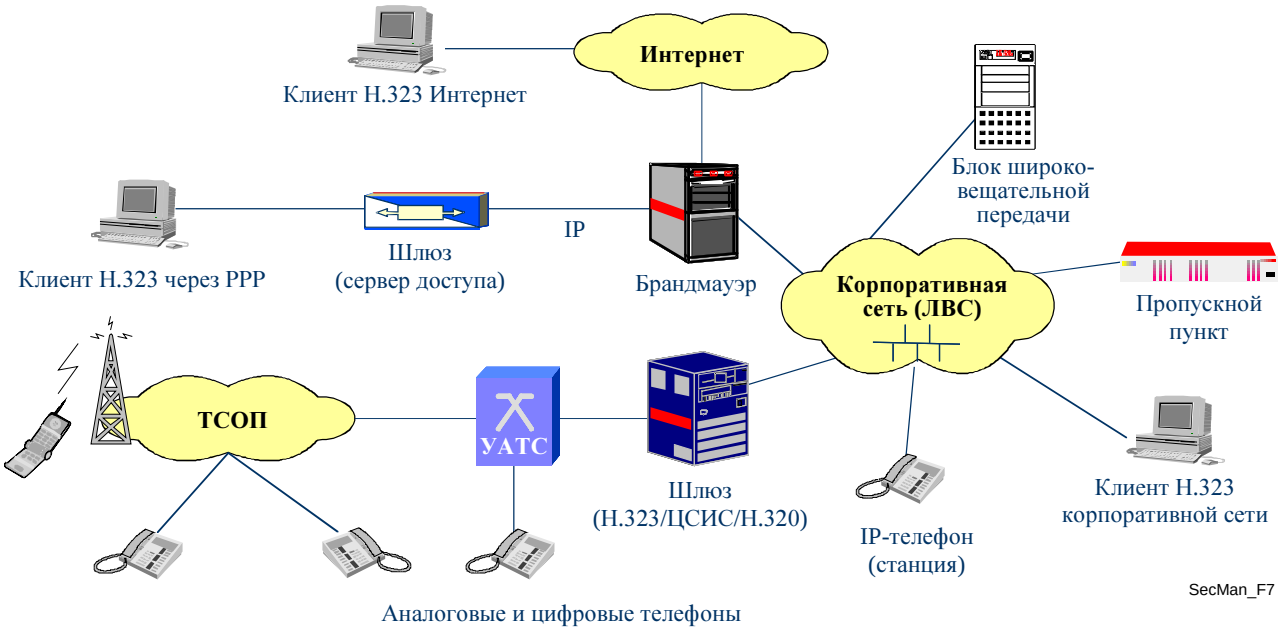
Терминалы (T) – это клиентские конечные точки на IP магистрали, которые обеспечивают двустороннюю связь. Терминалы H.323 должны поддерживать передачу речи и могут поддерживать видеокодеки, протоколы многоадресной передачи данных T.120 и возможности MCU. Примеры: IP телефоны, видеофоны, инфракрасные устройства, системы голосовой почты, IP-телефоны (например, NetMeeting™).

Шлюз (GW) – необязательный элемент в многосторонней связи H.323. Шлюзы выполняют множество функций, наиболее распространенной являются функция трансляции между конечными точками конференции H.323 и другими типами терминалов. Эта функция включает преобразование форматов передачи (то есть H.225.0 в H.221) и трансляцию процедур связи (то есть H.245 в H.242). Наряду с этим шлюз также осуществляет преобразования между аудио- и видеокодеками, осуществляет установку и разъединение соединения как на стороне ЛВС, так и на стороне сети с коммутацией каналов.

Пропускной пункт (GK) – является одним из важнейших компонентов функционирующей в соответствии с H.323 сети. Он действует как центральная точка для всех соединений в своей зоне и предоставляет услуги по управлению установлением соединения для зарегистрированных конечных точек. Во многих случаях пропускной пункт H.323 работает как виртуальный коммутатор, поскольку он управляет выдачей разрешений, выполняет трансляцию адресов и может либо разрешить установление соединения напрямую между конечными точками, либо может направить сигнализацию о соединении через собственно вызов для выполнения таких функций как следящая переадресация/поиск, переадресация по сигналу "занято" и т. д. Связанными с пропускными пунктами являются *пограничные* (или равноправные) элементы *(BE)*, которые отвечают за обмен адресной информацией и участвуют в авторизации вызова между административными доменами. Их функции также обеспечивают взаимосвязь между различными "группами" или сетями H.323. Это осуществляется путем обмена серией сообщений, как показано на рисунке 8.



a) Система H.323 и ее компоненты [Packetizer]

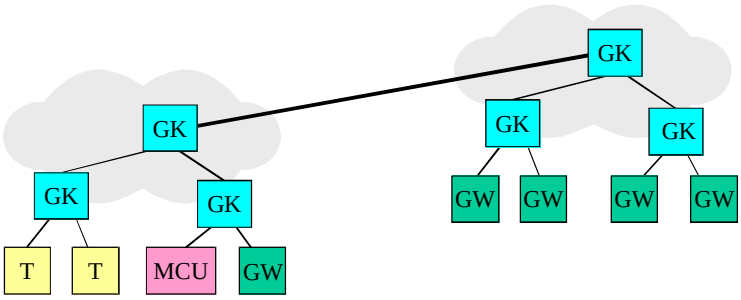


b) Сценарии развертывания на основе H.323 [Euchner]

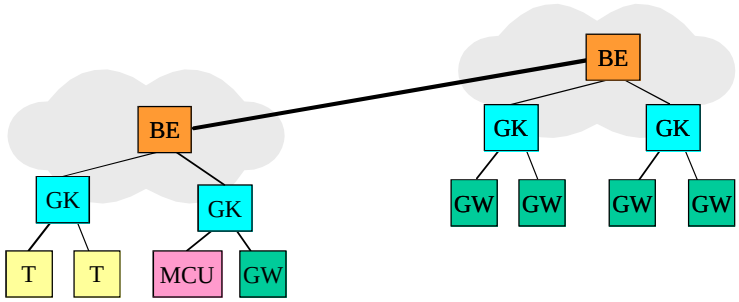
Рисунок 7
Система H.323: компоненты и сценарии развертывания

Многоточечный блок управления (MCU) поддерживает конференции между тремя и более конечными точками. Согласно H.323 в состав MCU входит обязательный многоточечный контроллер, а также ни одного или несколько многоточечных процессоров. Многоточечный контроллер управляет сигнализацией о соединении, но не взаимодействует напрямую ни с одним из медиапотоков. Это взаимодействие осуществляют многоточечные процессоры, которые смешивают, коммутируют и обрабатывают биты аудио-, видеосигналов и/или данных. Возможности многоточечного контроллера и многоточечного процессора могут быть реализованы в специальном компоненте или могут составлять часть функций других компонентов H.323.

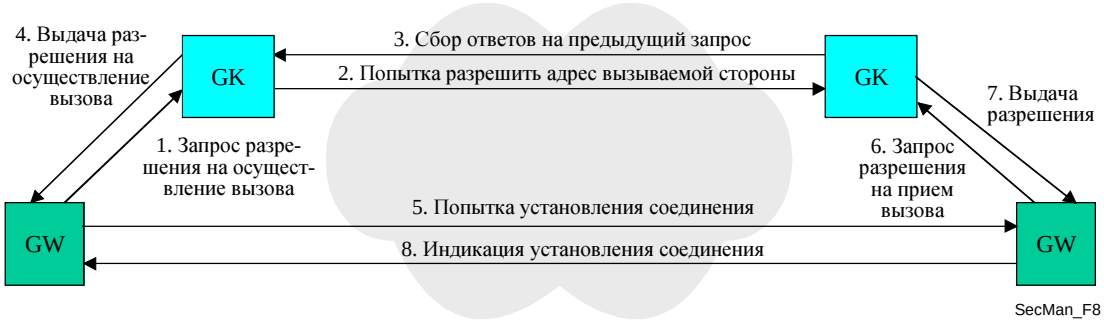
Несмотря на то что стандарт H.323 с самого начала разрабатывался как протокол мультимедийной связи, основной сферой его применения в настоящее время является рынок услуг речевой связи по IP. Находящиеся в эксплуатации сети H.323 переносят миллиарды минут речевого и видеотрафика в месяц (учитывая только сети общего пользования); большая часть трафика VoIP обрабатывается в соответствии с H.323. В настоящее время по оценкам на долю VoIP приходится более 10 процентов всех минут международной дальней связи. Объем видеотрафика H.323 также постоянно возрастает. Основная причина этого заключается в полноте и законченности протокола и его реализаций, а также в том, что H.323 доказал свою исключительную расширяемость и соответствие потребностям как поставщиков услуг, так и промышленных предприятий, обеспечив широчайший диапазон продуктов от стеков и чипов до радиотелефонов и оборудования видеоконференцсвязи.



a) Топология с применением протокола RAS[1]



b) Топология с применением протоколов H.225.0/Приложение G



c) Поток сообщений высокого уровня при установлении соединения

Легенда: BE – пограничный элемент; GK – пропускной пункт; GW – шлюз; MCU – многоточечный блок управления; T – терминал

Рисунок 8
Связи между административными доменами

Ниже перечислены функциональные характеристики систем H.323:

- Возможности многоадресной передачи речи, видеоряда и данных
- Связь между терминалами различных типов, включая ПК–телефон, факс–факс, телефон–телефон и Web-вызовы
- Поддержка факсимильной связи и модемной связи по IP T.38
- Множество дополнительных услуг (переадресация вызова, подключение к установленному соединению и т. д.)
- Полная функциональная совместимость с другими системами H.32x, включая H.320 (ЦСИС) и H.323M (подвижная радиосвязь 3GPP)
- Спецификация разложения медиашлюза (через протокол управления шлюзом H.248)
- Поддержка безопасности сигнализации и среды передачи
- Мобильность пользователя, терминала и служебного терминала
- Поддержка сигнализации при экстренном обслуживании

Примерами применения H.323 являются оптовый транзит, выполняемый операторами, особенно для магистралей VoIP (коммутаторы класса 4 для речевого трафика) и услуги по телефонным карточкам. При организации корпоративной связи стандарт H.323 используется для УАТС на базе IP, услуг центрекс на базе IP, речевых виртуальных частных сетей, 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 аудио-визуальный доступ, соединение ПК–телефон, доставка клиентам новостей и иной информации.

6.1.1 Вопросы безопасности в 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 9.

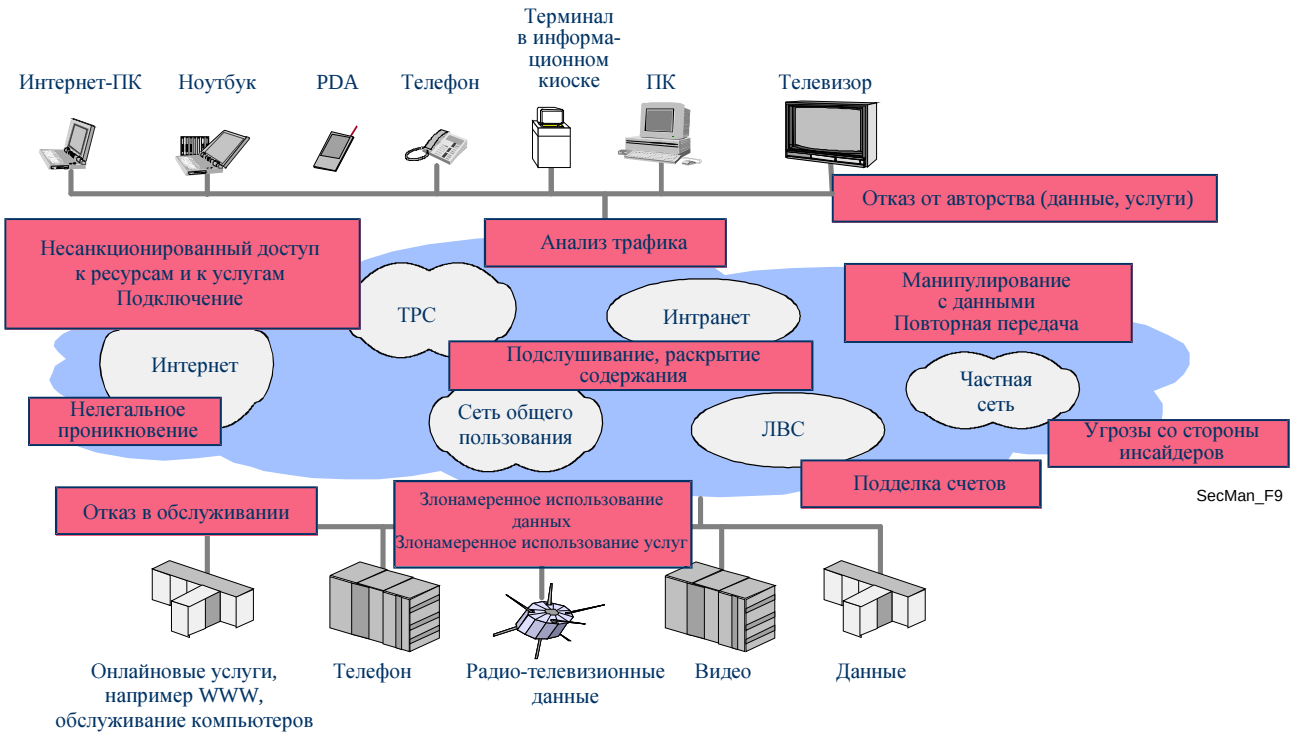


Рисунок 9
Угрозы безопасности в среде мультимедийной связи

Основными вопросами обеспечения безопасности в среде мультимедийной связи и IP-телефонии являются [Euchner]:

- 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). Аналогичным образом пользователи могут захотеть узнать, с кем установлена телефонная связь.
- 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.
- Угрозы нарушения безопасности аутентификации пользователя/терминала и сервера, такие как нелегальное проникновение, атаки типа “человек-посредник”, подмена IP-адреса и захват 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 ТСОП), 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 направлена на защиту 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, используя для этого малый объем квитирования и короткий двойной пробег, с тем чтобы избежать длительного времени установки соединения или внесения ухудшения качества речи за счет задержек прохождения пакетов или дрожания, вызванного процедурами обеспечения безопасности.
- Конфиденциальность речевой связи достигается за счет шифрования пакетов речевых сообщений, то есть RTP обеспечивает полезную нагрузку и противодействует подслушиванию прослушиваемых речевых сигналов. 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 H.323. На практике, однако, могут возникнуть и другие проблемы безопасности, выходящие за рамки H.323 (например, стратегия безопасности, безопасность управления сетью, параметризация безопасности, безопасность реализации, эксплуатационная безопасность или разрешение случаев нарушения безопасности).

6.1.2 Как обеспечивается безопасность для VoIP

Для мультимедийной системы H.323 в Рекомендации МСЭ-Т H.235 определяется структура безопасности, включая спецификацию механизмов безопасности и протоколов безопасности для H.323. Стандарт H.235 первоначально был введен для систем H.323 версии 2 в 1998 году. После этого с течением времени H.235 получил дальнейшее развитие за счет объединения предложенных механизмов безопасности, включения более сложных алгоритмов безопасности (например, высокоскоростное шифрование по стандарту AES с повышенной защитой) и разработки полезных и эффективных профилей безопасности для конкретных случаев и условий эксплуатации. Версия 3 H.235 является действующей Рекомендацией МСЭ-Т в области безопасности для систем на базе H.323, которая обеспечивает расширяемую защиту как для небольших групп, предприятий, так и для крупных операторов.

Говоря кратко, H.235 обеспечивает криптографическую защиту протоколов управления (протокола RAS и сигнализации о соединении H.225.0 и H.245), а также криптографическую защиту потоков аудио/видео медиаданных. Используя различные режимы сигнализации H.323, H.235 предоставляет средства для 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. Управление ключами H.235 поддерживает “классическую” двухточечную связь, но возможны также многоточечные конфигурации при использовании многоточечных блоков (то есть MCU), когда в рамках одной группы осуществляется связь между несколькими мультимедийными терминалами.

H.235 охватывает широкий набор мер безопасности, предназначенных для использования в различных средах, таких как связь между предприятиями и внутри предприятий, а также между операторами. В зависимости от исходных условий, таких как имеющаяся инфраструктура безопасности, функциональные возможности и платформы терминалов (простые конечные точки или интеллектуальные конечные точки), H.235 предоставляет набор соответствующим образом параметризованных и совмещающихся профилей безопасности. Имеющиеся профили безопасности определяют методы безопасности, диапазон которых простирается от простых профилей с общим секретным ключом и защищенным паролем (H.235, Приложение D для аутентификации и целостности сообщений) до более сложных профилей с цифровыми подписями и сертификатами PKI X.509 (H.235, Приложение E и Приложение F). Это позволяет реализовывать как межсегментную защиту с использованием более простых, но менее гибких методов, так и сквозную защиту с использованием расширяемых возможностей на базе PKI. Приложение I H.235 ослабляет жесткую зависимость от архитектуры, центром которой является сервер, с пропускными пунктами-маршрутизаторами и предоставляет меры защиты, направленные на обеспечение безопасности модели одноранговой сети.

Для соблюдения жестких эксплуатационных ограничений в H.235 используются специальные оптимизированные методы обеспечения безопасности, такие как шифрование методом эллиптических кривых и современный стандарт шифрования AES. Шифрование речи, если таковое реализовано, осуществляется на прикладном уровне путем шифрования полезной нагрузки RTP. Это позволяет получить выгоду благодаря незначительному воздействию на конечные точки за счет плотного взаимодействия с процессором цифровой обработки сигналов (DSP) и использования кодеков со сжатием речевого сигнала, а также за счет отсутствия зависимости от типа платформы операционной системы. При условии наличия и пригодности в рамках H.235 могут использоваться (или повторно использоваться) такие существующие инструменты безопасности, как доступные Интернет-программы и стандарты безопасности (IPSec, SSL/TLS).

На рисунке 10 показана область действия H.235, а также условия для установления соединений (блоки H.225.0 и H.245) и двунаправленная связь (шифрование полезной нагрузки RTP, содержащей сжатые аудио- и/или видеосигналы). Функциональные возможности включают механизмы аутентификации, целостности, секретности и фиксации авторства. Пропускные пункты осуществляют аутентификацию путем управления разрешениями в конечных точках и обеспечивают механизмы поддержания фиксации авторства. Безопасность транспортного и более низких уровней, базирующихся на IP, выходит за область применения H.323 и H.235, но обычно реализуется с использованием протоколов обеспечения безопасности IP IETF (IPSec) и обеспечения безопасности транспортного уровня (TLS). В общем случае TPSec и TLS могут применяться для аутентификации и необязательно конфиденциальности (то есть шифрования) на уровне IP, прозрачном для любого протокола (приложения), функционирующего на более высоких уровнях. Для этого модификация протокола приложения не требуется, а необходимо лишь изменение стратегии безопасности на каждом конце.

Рисунок 10
Безопасность в H.323 в соответствии с H.235 [Euchner]

Наряду с тем, что H.235 в основном предназначена для использования в “статических” условиях H.323 с ограниченной мобильностью, была признана необходимость обеспечения безопасной мобильности пользователя и терминала в среде распределенных систем H.323, выходящей за рамки внутридоменной связи и мобильности, ограниченной зоной действия пропускного пункта. Эти потребности в безопасности удовлетворяет Рекомендация МСЭ-Т H.530, в которой рассматриваются следующие аспекты безопасности:

- Аутентификация мобильного терминала/пользователя и авторизация во внешних посещаемых доменах
- Аутентификация посещаемого домена
- Управление ключами безопасности
- Защита данных сигнализации между мобильным терминалом и посещаемым доменом

Кроме H.235 расширяемое управление ключами с применением LDAP и SSL3 обеспечивают H.350 и H.350.2. Рекомендация МСЭ-Т H.350.x обеспечивает несколько важных функций, которые позволяют предприятиям и операторам осуществлять безопасное управление работой большого числа пользователей услуг передачи видеоданных и речевых сообщений по IP. H.350 предоставляет способ подключения услуг H.323, SIP, H.320 и базовых услуг обмена сообщениями к службе справочников, с тем чтобы к мультимедийной связи возможно было бы применять современные методы управления опознаванием. Кроме этого, в архитектуре определено стандартизированное место хранения полномочий в отношении безопасности для этих протоколов.

H.350 не меняет архитектуру безопасности какого-либо протокола, но вместе с тем предлагается стандартизированное место хранения, в случае необходимости, полномочий в отношении аутентификации. Следует заметить, что и H.323, и SIP поддерживают аутентификацию с общим секретным ключом (H.235, Приложение D и протокол HTTP Digest, соответственно). Для реализации таких подходов необходимо, чтобы сервер вызовов имел доступ к паролю. Таким образом, если нарушается безопасность сервера вызовов или справочников H.350, также вероятно нарушение безопасности паролей. Этот недостаток скорее может быть следствием недостатков систем (справочник H.350 или серверы вызовов) или порядка их эксплуатации, а не самого стандарта H.350.

Настоятельно рекомендуется, чтобы серверы вызовов и справочник H.350 до начала обмена информацией проводили взаимную аутентификацию. Также настоятельно рекомендуется, чтобы связь между справочниками H.350 и серверами вызовов или конечными точками устанавливалась по безопасным каналам, таким как SSl и TLS.

Следует отметить, что списки управления доступом на серверах LDAP относятся к вопросам стратегии и не являются частью стандарта. Системным администраторам рекомендуется руководствоваться общепринятыми правилами при установке параметров управления доступом в атрибутах H.350. Например, атрибуты пароля должны быть доступны только пользователям, прошедшим процедуру аутентификации, а атрибуты адресов могут быть открытыми.

6.2 Система IPCablecom

Система IPCablecom позволяет операторам систем кабельного телевидения предоставлять услуги, базирующиеся на протоколе IP, в реальном масштабе времени (например, услуги речевой связи) по своим сетям, модернизированным в части поддержки кабельных модемов. Архитектура системы IPCablecom определена в Рекомендации МСЭ-Т J.160. На самом верхнем уровне архитектура IPCablecom взаимодействует с тремя сетями: "HFC сеть доступа J.112", "управляемая IP-сеть" и ТСОП. Узел доступа (AN) обеспечивает связь между "HFC сетью доступа J.112" и "управляемой IP-сетью". Шлюз сигнализации (SG) и медиашлюз (MG) обеспечивают связь между "управляемой IP-сетью" и ТСОП. На рисунке 11 представлена базовая архитектура IPCablecom.

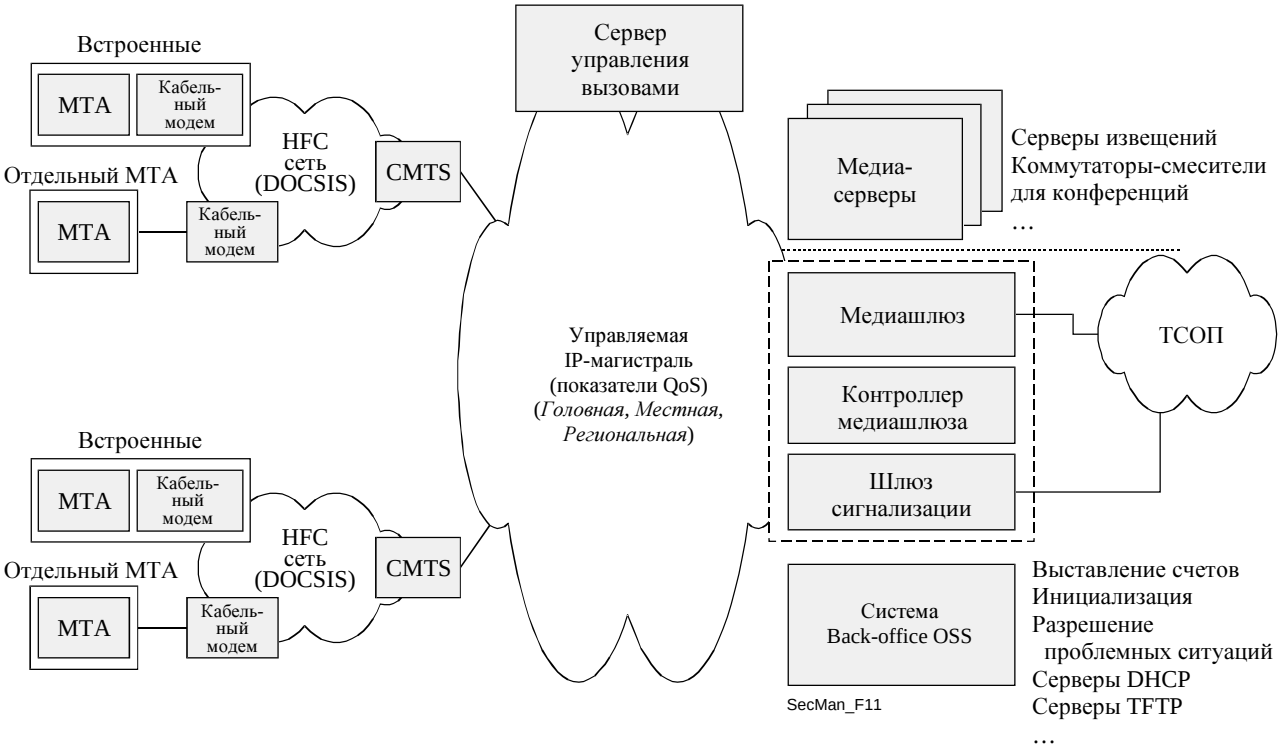


Рисунок 11
Базовая архитектура IPCablecom [J.165]

Комбинированная оптокоаксиальная кабельная (HFC) сеть доступа J.112 обеспечивает высокоскоростной, надежный и безопасный транспорт между точкой расположения клиента и головным узлом сети. Эта сеть доступа может поддерживать все возможности J.112, включая качество обслуживания, и осуществляет взаимодействие с физическим уровнем через оконечную систему кабельных модемов (CMTS).

Управляемая IP-сеть выполняет несколько функций. Во-первых, она обеспечивает взаимодействие между базовыми функциональными компонентами IPCablecom, которые отвечают за сигнализацию, среду передачи данных, инициализацию, качество обслуживания. Наряду с этим управляемая IP-сеть осуществляет IP-связь по линиям большой протяженности между другими управляемыми IP-сетями и HFC сетями J.112. В состав управляемой IP-сети входят следующие функциональные компоненты: сервер управления вызовами, сервер извещений, шлюз сигнализации, медиашлюз, контроллер медиашлюза и несколько серверов Back-office системы эксплуатационной поддержки (OSS).

Сервер управления вызовами (CMS) выполняет управление вызовами и связанными с сигнализацией услугами для адаптера медиатерминала (MTA), узла доступа и шлюзов ТСОП в сети IPCablecom. CMS является защищенным сетевым элементом, который располагается в управляемой IP-части сети IPCablecom. *Серверы извещений* являются логическими сетевыми компонентами, которые управляют информационными тонами и сообщениями и осуществляют их воспроизведение в соответствии с происходящими в сети событиями. *Шлюз сигнализации* отправляет и принимает сигнализацию сети с коммутацией каналов на стороне сети IPCablecom. Для IPCablecom функция шлюза сигнализации заключается только в поддержке не связанной со средствами передачи сигнализации в формате SS7 (связанная со средствами передачи сигнализация в форме многочастотных тонов поддерживается непосредственно функцией медиашлюза). *Контроллер медиашлюза* (MGC) принимает и согласовывает информацию сигнализации о соединении между сетью IPCablecom и ТСОП. Он поддерживает и контролирует общее состояние вызова для требующих взаимодействия с ТСОП вызовов. *Медиашлюз* (MG) обеспечивает сетевое взаимодействие носителей между ТСОП и IP-сетью IPCablecom. Каждый носитель представлен как конечная точка, а MGS дает MG команду на установку и контроль медиасоединений с другими конечными точками сети IPCablecom. MGC также дает MG команду на обнаружение и генерацию событий и сигналов, относящихся к известному MGC состоянию вызова. В состав *Back-office OSS* входят компоненты управления производственной деятельностью, услугами и сетью, обеспечивающие основные процессы ведения коммерческой деятельности. Основными сферами действия OSS являются: устранение неисправностей, управление качеством функционирования, управление безопасностью, управление расчетами и управление конфигурацией. IPCablecom определяет ограниченный набор функциональных компонентов и интерфейсов OSS, необходимый для поддержки инициализации устройств MTA и передачи сообщений о событиях в целях доставки информации для выставления счетов.

6.2.1 Вопросы безопасности в IPCablecom

Любой интерфейс протокола IPCablecom представляет собой объект угроз, создающих риски безопасности как для абонента, так и для поставщика услуг. Например, медиапоток может проходить через огромное число потенциально неизвестных линий поставщиков услуг Интернет и услуг магистралей Интернет. В результате медиапоток может подвергаться преднамеренному подслушиванию, приводящему к потере секретности связи.

6.2.2 Механизмы обеспечения 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 службами безопасности. В контексте архитектуры X.805 средства защиты для IPCablecom охватывают все девять ячеек, образуемых тремя плоскостями и тремя слоями, показанными на рисунке 1. Например, IPSec поддерживает службы безопасности протоколов сигнализации для плоскости административного управления. Безопасность инфраструктуры административного управления достигается за счет использования протокола SNMP v3.

Услуги безопасности, предоставляемые через основной слой услуг IPCablecom, включают аутентификацию, управление доступом, целостность, конфиденциальность и фиксацию авторства. Для удовлетворения собственных конкретных требований к безопасности любой интерфейс протокола IPCablecom может не использовать или использовать одну и более таких услуг.

Система безопасности IPCablecom выполняет требования к безопасности входящих в нее интерфейсов протоколов путем:

- выявления конкретной для каждого интерфейса протокола модели угроз;
- определения услуг безопасности (аутентификация, авторизация, конфиденциальность, целостность и фиксация авторства), необходимых для защиты от выявленных угроз;
- определения конкретного механизма безопасности, обеспечивающего необходимые услуги безопасности.

Механизмы безопасности включают как протокол безопасности (например, IPSec, безопасность RTP-уровня 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. На рисунке 12 показана совокупность всех интерфейсов безопасности IPCablecom. Отсутствие протокола управления ключами означает отсутствие потребности в нем для данного интерфейса. Интерфейсы IPCablecom, для которых не требуется защита, на рисунке 12 не показаны.

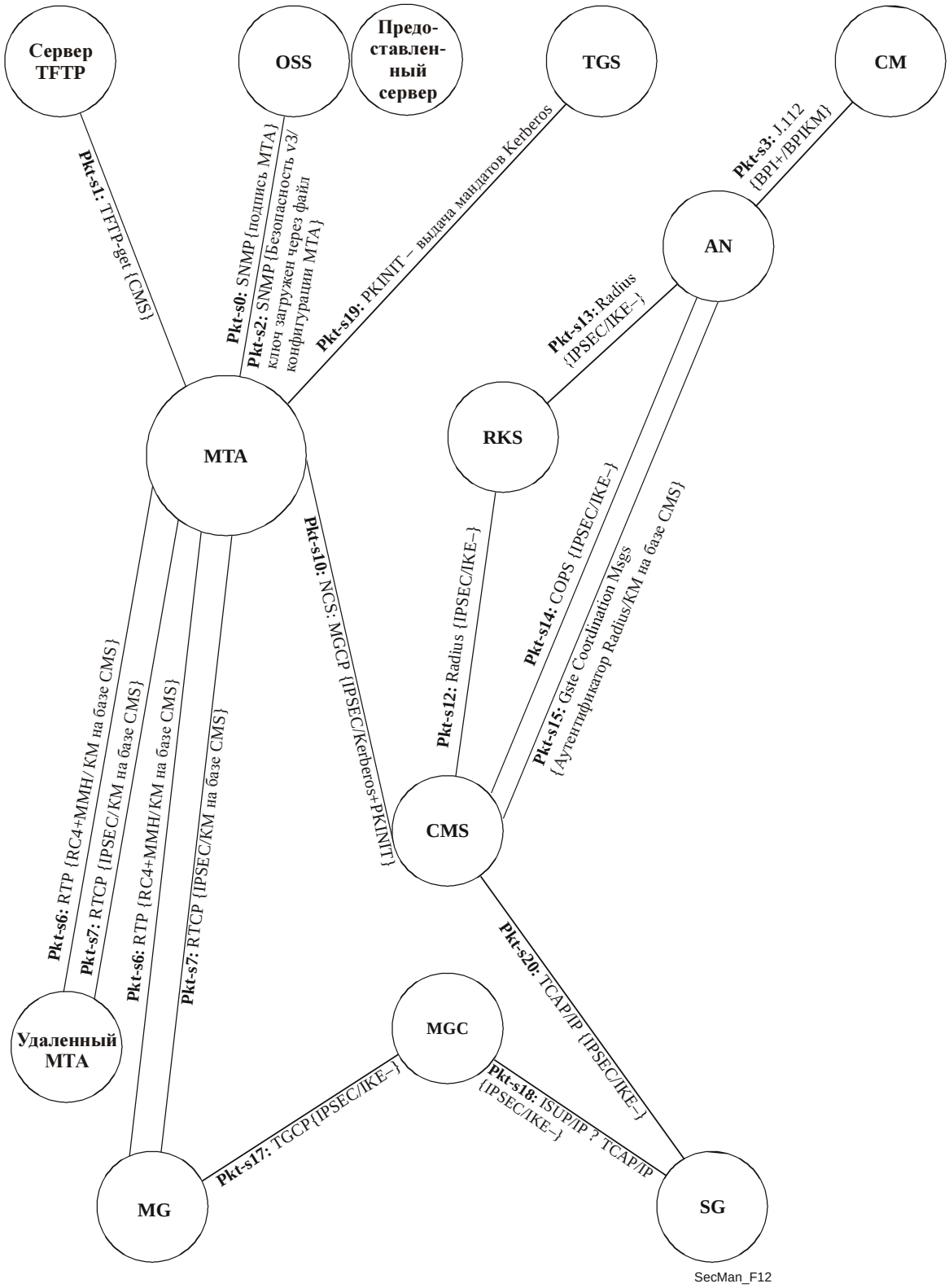
Архитектура безопасности IPCablecom подразделяет инициализацию устройств на три отдельные операции: регистрация абонента, инициализация устройства и авторизация устройства. Процесс *регистрации абонента* включает создание постоянного расчетного счета абонента, который однозначно определяет MTA к CMS по серийному номеру MTA или адресу MAC. Расчетный счет также используется для идентификации услуг, на которые подписан данный абонент в отношении MTA. Регистрация абонента может происходить по основному или вспомогательному каналу. Конкретная спецификация процесса регистрации абонента выходит за рамки IPCablecom и может различаться у разных поставщиков услуг. Для *инициализации устройства* устройство MTA проверяет аутентичность файла конфигурации, который он загружает, установив сначала безопасность SNMPv3 (используя аутентификацию на основе Kerberos и управление ключами) между собой и сервером инициализации. Сервер инициализации затем сообщает MTA местонахождение файла конфигурации и хеш-функцию файла конфигурации. MTA находит файл конфигурации, вычисляет хеш-функцию файла конфигурации и сравнивает результат с хеш-функцией, полученной от сервера инициализации. Если хеш-функции совпадают, файл конфигурации считается прошедшим аутентификацию. Файл конфигурации может быть, но необязательно, зашифрованным для обеспечения секретности (также должна быть включена секретность SNMPv3 для безопасной передачи ключа шифрования файла конфигурации к MTA). *Авторизация устройства* выполняется, когда прошедшее инициализацию устройство MTA проводит собственную аутентификацию в отношении сервера управления вызовами и устанавливает защищенное соединение с этим сервером до начала функционирования в полном объеме. Авторизация устройства обеспечивает защиту сигнализации последующих вызовов по установленному защищенному соединению.

Защищенными могут быть и трафик сигнализации, и медиапоток. Безопасность полного трафика сигнализации, который включает сигнализацию QoS, сигнализацию о соединении и сигнализацию с интерфейсом шлюза ТСОП, обеспечивается через IPSec. Управление защищенным соединением IPSec выполняется с помощью двух протоколов управления ключами: Kerberos/PKINIT и IKE. Kerberos/PKINIT используется для обмена ключами между клиентами MTA и их сервером CMS, IKE – для управления всей прочей сигнализацией SA IPSec. Что касается медиапотоков, то каждый медиапакет RTP шифруется в целях обеспечения секретности и проходит процедуру аутентификации в целях обеспечения целостности и проверки источника пакета. MTA могут согласовывать конкретный алгоритм шифрования, хотя единственным требуемым алгоритмом шифрования является AES. Каждый пакет RTP может включать необязательный код аутентификации сообщения (MAC). Алгоритм MAC также может согласовываться, хотя единственным специфицированным на данный момент является алгоритм MMH. В вычислении MAC участвуют незашифрованный заголовок и зашифрованная полезная нагрузка пакета.

Ключи для шифрования и вычисления MAC, которыми обмениваются отправляющие и принимающие сигналы MTA в виде части сигнализации о соединении, извлекаются из сквозного секретного и необязательного дополнения. Таким образом, и обмен ключами для обеспечения безопасности медиапотоков также является защищенным системой безопасности сигнализации о соединении.

Безопасность обеспечивается также для OSS и системы выставления счетов. Агенты SNMP в устройствах IPCablecom реализуют протокол SNMPv3. Модель безопасности пользователя SNMPv3 [RFC 2274] выполняет аутентификацию и предоставляет средства обеспечения секретности для трафика SNMP. Для управления доступом к объектам MIB может использоваться управление доступом типа View-based Access Control SNMPv3 [RFC 2275].

Протокол управления ключами IKE используется для установления ключей шифрования и аутентификации между сервером ведения записей (RKS) и каждым сетевым элементом IPCablecom, который генерирует сообщения о событии. После установления сетевой ассоциации безопасности IPSec эти ключи должны быть созданы между каждым RKS (первичным, вторичным и т. д.) и каждыми CMS и AN. Также может выполняться обмен ключами между MGC и RKS, порядок которого определяется оборудованием поставщика на этапе 1 IPCablecom. Сообщения о событиях передаются от CMS и AN к RKS с использованием транспортного протокола RADIUS, который, в свою очередь, защищен IPSec.



IKE –	IKE с заданными коллективными ключами
IKE+	IKE требует сертификаты открытых ключей
KM на базе CMS	Ключи, произвольно генерируемые и распространяемые CMS

Рисунок 12
Интерфейсы безопасности IPCablecom
(обозначение: <метка>: <протокол> {<протокол безопасности>/<протокол управления ключами>})

6.3 Защищенная факсимильная передача

Факсимильная связь является весьма популярным приложением. Первоначально разработанное для передачи по ТСОП (Т.4 МСЭ-Т) и затем по ЦСИС (Т.6 МСЭ-Т) это приложение позднее получило развитие для использования в IP-сетях (включая Интернет) не в реальном масштабе времени (e-mail relay) согласно Т.37 МСЭ-Т и в реальном масштабе времени (используя RTP) согласно Т.38 МСЭ-Т. Факсимильной связи присущи две типичные проблемы безопасности, независимо от среды – ТСОП, ЦСИС или IP, – аутентификация (и иногда фиксация авторства) соединения и конфиденциальность передаваемых данных. При этом Т.37 и Т.38 делают эти проблемы еще более важными вследствие распределенного характера IP-сетей.

В Рекомендации МСЭ-Т Т.36 описаны два независимых технических решения, которые могут использоваться для шифрования передаваемых документов, с тем чтобы обеспечить защищенную факсимильную передачу. Эти два решения базируются на алгоритме HKM/HFX40 (Т.36, Приложение A) и алгоритме RSA (Т.26, Приложение B). Несмотря на то что оба алгоритма ограничивают сеансовые ключи 40 битами (в силу национальных правил, действовавших на момент утверждения данной Рекомендации в 1997 году), для алгоритмов, которым необходимы более длинные ключи, разработан механизм генерирования избыточного сеансового ключа (из 40-битового сеансового ключа). В Приложении C к Т.36 описано использование системы HKM в целях обеспечения возможностей управления защищенными ключами для факсимильных терминалов путем односторонней регистрации между объектами X и Y или защищенной передачи секретного ключа между объектами X и Y. В Приложении D к Т.36 представлены процедуры использования системы шифров несущей HFX40 в целях обеспечения конфиденциальности сообщения для факсимильных терминалов. Наконец, в Приложении E к Т.36 описан, в аспекте его применения, алгоритм вычисления хеш-функции HFX40-I, необходимые расчеты и информация, которой должны обмениваться факсимильные терминалы для обеспечения целостности передаваемого факсимильного сообщения в качестве либо выбранной, либо запрограммированной заранее альтернативы шифрованию сообщения.

Наряду с этим Т.36 определяет следующие услуги безопасности:

- Взаимная аутентификация (обязательная)
- Услуга безопасности (необязательная), которая включает взаимную аутентификацию, целостность сообщений и подтверждение приема сообщения
- Услуга безопасности (необязательная), которая включает взаимную аутентификацию, конфиденциальность сообщений (шифрование) и установку сеансовых ключей
- Услуга безопасности (необязательная), которая включает взаимную аутентификацию, целостность сообщений, подтверждение приема сообщения, конфиденциальность сообщений (шифрование) и установку сеансовых ключей

Исходя из перечисленных выше услуг безопасности, определены четыре профиля безопасности, что показано в таблице 2, см. ниже.

Таблица 2
Профили безопасности в Приложении H к Т.30

Услуги безопасности	**Профили безопасности**			
	1	2	3	4
Взаимная аутентификация	X	X	X	X
• Целостность сообщения • Подтверждение приема сообщения		X		X
• Конфиденциальность сообщения (шифрование) • Установка сеансовых ключей			X	X

6.3.1 Безопасность факсимильной связи при использовании HKM и HFX

Сочетание систем *управления ключами Hawthorne* (HKM) и *факсимильного шифра Hawthorne* (HFC) обеспечивает следующие возможности в отношении защищенной передачи документов между объектами (терминалами или операторами терминалов):

- взаимная аутентификация объектов;
- установка секретных сеансовых ключей;
- конфиденциальность документов;
- подтверждение приема;
- подтверждение или отрицание целостности документа.

Управление ключами обеспечивается при использовании системы HKM, определенной в Приложении B к T.36. В документе представлены две процедуры: первая – регистрация и вторая – защищенная передача секретного ключа. Во время регистрации устанавливаются взаимные секретные ключи и эта процедура обеспечивает безопасность всех последующих передач. В последующих передачах система HKM осуществляет взаимную аутентификацию, установку секретных сеансовых ключей для обеспечения конфиденциальности и целостности документов, подтверждения приема и подтверждения или отрицания целостности документов.

Конфиденциальность документов обеспечивается за счет использования шифра несущей, определенного в Приложении D к T.36. В шифре несущей используется 12-разрядный десятичный ключ, который примерно эквивалентен 40-битовому сеансовому ключу.

Целостность документов обеспечивается за счет использования системы, определенной в Приложении E к T.36, а в Рекомендации T.36 описан алгоритм применения хеш-функции, включая соответствующие вычисления и обмен информацией.

В режиме регистрации два терминала обмениваются информацией, которая позволяет объектам однозначно идентифицировать друг друга. В основе этого лежит соглашение между пользователями о секретном одноразовом ключе. Каждый объект хранит 16-разрядное число, однозначно связанное с объектом, с которым проведена регистрация.

Когда требуется осуществить защищенную передачу документа, передающий терминал передает в качестве вызова принимающему объекту 16-разрядное секретное число, связанное с принимающим объектом, а также произвольное число и зашифрованный сеансовый ключ. Принимающий терминал отвечает посылкой 16-разрядного ключа, связанного с передающим объектом, а также произвольного числа и повторно зашифрованной версии вызова, полученного от передающего устройства. В то же время он передает в качестве вызова передающему объекту произвольное число и зашифрованный сеансовый ключ. Передающий терминал отвечает произвольным числом и повторно зашифрованной версией вызова, полученного от принимающего объекта. Эта процедура позволяет двум данным объектам провести взаимную аутентификацию. В это же время передающий терминал посылает произвольное число и зашифрованный сеансовый ключ, который должен использоваться для шифрования и вычисления хеш-функции.

После передачи документа передающий терминал посылает произвольное число и зашифрованный сеансовый ключ в качестве вызова принимающему объекту. В это же время он посылает произвольное число и зашифрованное значение хеш-функции, которая позволяет принимающему объекту удостовериться в целостности принятого документа. Принимающий терминал передает произвольное число и повторно зашифрованную версию полученного от передающего объекта вызова. В это же время он посылает произвольное число и зашифрованный документ контроля целостности, который служит подтверждением или отрицанием целостности принятого документа. Алгоритм вычисления хеш-функции, используемый для контроля целостности документа, применяется ко всему документу.

Предусмотрен режим переопределения, при котором два терминала не осуществляют обмен какими-либо сигналами безопасности. Пользователи договариваются о том, что одноразовый секретный сеансовый ключ вводится вручную. Он используется передающим терминалом для шифрования документа и принимающим терминалом для дешифрования документа.

6.3.2 Безопасность факсимильной связи при использовании RSA

В Приложении H к T.30 определены механизмы обеспечения параметров безопасности на базе криптографического механизма шифрования с открытыми ключами Ривеста, Шамира и Адлмана (RSA). Подробное описание алгоритма RSA см. [ApplCryp, pp. 466–474]. Схема кодирования документа, передаваемого при обеспечении параметров безопасности, может быть любого типа из определенных в Рекомендациях T.4 и T.30 (модифицированная схема Хаффмана, MR, MMR, символьный режим, как определено в Приложении D к T.4, BFT, иной режим передачи, определенный в Приложении C к T.4).

Базовым алгоритмом работы с цифровыми подписями (услуги аутентификации и обеспечения целостности) является алгоритм RSA, с использованием пары ключей “открытый ключ"/"секретный ключ”.

При предоставлении необязательной услуги обеспечения конфиденциальности маркер, содержащий сеансовый ключ “Ks”, который используется для кодирования документа, тоже шифруется с помощью алгоритма RSA. Пара применяемых для этой цели ключей ("открытый ключ шифрования"/"секретный ключ шифрования”) не идентична паре, применяемой для услуг аутентификации и обеспечения целостности. Это делается для изолирования указанных двух видов функций.

Реализация используемого в Приложении H механизма RSA описана в документе ISO/IEC 9796 (Схема цифровых подписей для восстановления сообщений).

Для кодирования маркера, содержащего сеансовый ключ, при обработке алгоритма RSA применяются те же правила избыточности, которые установлены в ISO/IEC 9796. Следует отметить, что для некоторых администраций в дополнение к RSA может потребоваться реализация механизма *алгоритма цифровой подписи* (DSA) [ApplCryp, pp. 483–502].

По умолчанию в схеме Приложения H к T.30 *сертифицирующие органы* не участвуют, однако они могут привлекаться факультативно для удостоверения открытого ключа отправителя факсимильного сообщения. В этом случае открытый ключ может быть сертифицирован согласно Рекомендации X.509. Средства передачи сертификата открытого ключа отправителя описаны в Приложении H, но вместе с тем точный формат сертификата подлежит дальнейшему изучению и фактическая передача сертификата согласовывается в протоколе.

Режим регистрации предусматривается в качестве обязательной функции. Этот режим позволяет передающей и принимающей сторонам регистрировать и хранить в безопасности открытые ключи другой стороны до установления защищенной факсимильной связи между ними. В режиме регистрации может быть исключена необходимость введения пользователем вручную с терминала открытых ключей своих абонентов (открытые ключи имеют достаточно большую длину, 64 октета и более).

Поскольку в режиме регистрации разрешен обмен открытыми ключами и их хранение в терминалах, не требуется передавать ключи во время сеанса факсимильной связи.

Как описано в приложении, некоторые подписи применяются по результатам работы “хеш-функций”.

Могут использоваться следующие хеш-функции: либо SHA-1 (*алгоритм аутентификации и проверки целостности информации*) – алгоритм, разработанный НИСТ США, либо MD-5 (RFC 1321). Для SHA-1 длина получаемого в процессе хеширования результата составляет 160 битов, а для MD-5 длина полученного в процессе хеширования результата составляет 128 битов. Терминал, соответствующий Приложению H к T.30, может реализовать либо SHA-1, либо MD-5, либо оба алгоритма. Применение конкретного алгоритма согласовывается в протоколе (см. далее).

Кодирование данных для обеспечения услуги конфиденциальности является необязательным. В рамках применения Приложения H к T.30 зарегистрированы пять необязательных схем кодирования: FEAL-32, SAFER K-64, RC5, IDEA и HFX40 (как описано в Рекомендации T.36). В некоторых странах применение этих схем может регулироваться национальными правилами.

Могут также использоваться и другие необязательные алгоритмы. Они выбираются в соответствии с ISO/IEC 9979 (процедура регистрации криптографических алгоритмов).

Возможность терминала работать с одним из этих алгоритмов и фактическое использование конкретного алгоритма во время сеанса связи согласовывается в протоколе. Для кодирования используется сеансовый ключ. Базовая длина сеансового ключа составляет 40 битов. Для алгоритмов, которые используют сеансовые ключи длиной 40 битов (например, HFX40), фактически используемым в алгоритме кодирования ключом является сеансовый ключ "Ks", а для алгоритмов, которым необходимы ключи, превышающие 40 битов (например, FEAL-32, IDEA, SAFER K-64, для которых необходимы соответственно ключи длиной 64 бита, 128 битов и 64 бита), для получения требуемой длины применяется механизм избыточности. Полученный в результате ключ называется "избыточный сеансовый ключ". "Избыточный сеансовый ключ" – это ключ, который фактически используется в алгоритме кодирования.

6.4 Приложения для управления сетью

Как отмечается в разделе, посвященном требованиям к структуре безопасности, обязательным условием является защита трафика управления, который используется для мониторинга сети электросвязи и управления ею. Обычно категории трафика управления определяются в переводе на информацию, необходимую для выполнения функций управления обработкой отказов, конфигурацией, качеством функционирования, расчетами и безопасностью. Область действия управления безопасностью охватывает как настройку сети управления безопасностью, так и управление безопасностью информации, которая связана с тремя плоскостями и тремя слоями безопасности, образующими архитектуру безопасности. Последнее составляет предмет настоящего раздела.

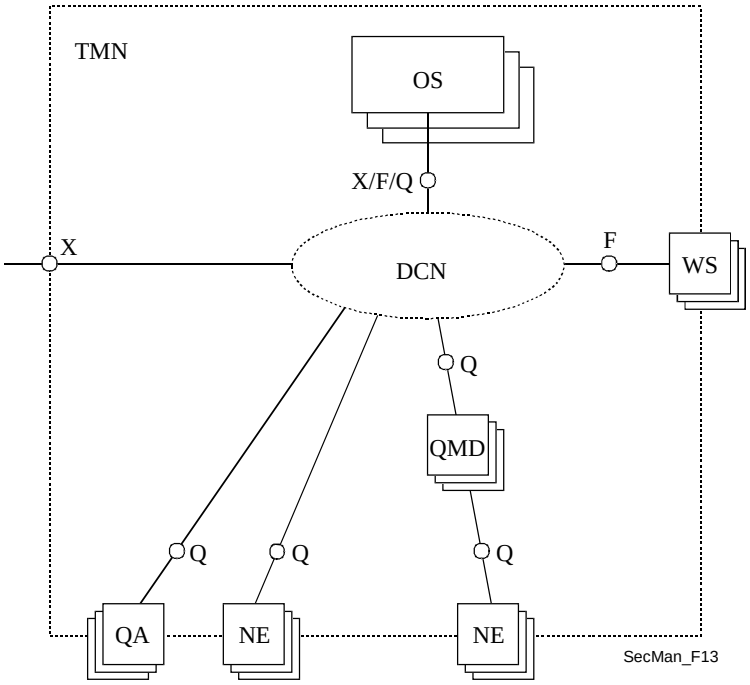
Традиционно в сети электросвязи трафик управления зачастую передается по отдельной сети, которая предназначена только для переноса трафика управления сетью и по которой пользовательский трафик не передается. Такая сеть обычно называется сетью управления электросвязью (TMN), которая описана в Рекомендации МСЭ-Т М.3010. TMN является отдельной и изолированной от инфраструктуры сети общего пользования, поэтому какие-либо прерывания связи, возникающие вследствие угрозы безопасности в плоскости конечного пользователя в сети общего пользования, на TMN не распространяются. Благодаря такому разделению относительно просто обеспечить защиту трафика сети управления, поскольку доступ к этой плоскости ограничен полномочными администраторами сети, а трафик ограничен разрешенными процессами управления. С введением сетей следующего поколения трафик приложений конечных пользователей может иногда совмещаться с трафиком управления. Несмотря на то что такой подход минимизирует затраты за счет необходимости 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 административного и оперативного управления. Плоскость административного управления становится доступной для огромного числа конечных пользователей, и возникает возможность осуществления множества самых разнообразных злонамеренных действий.

Для обеспечения полной сквозной структуры все меры безопасности (например, управление доступом, аутентификация) должны применяться к каждому типу осуществляемых в сети процессов (то есть процессы в плоскости административного управления, в плоскости оперативного управления, в плоскости конечного пользователя) в отношении инфраструктуры сети, сетевых услуг и сетевых приложений. Существует ряд Рекомендаций МСЭ-Т, специально посвященных аспекту безопасности плоскости административного управления для сетевых элементов (NE) и систем административного управления (MS), которые являются частями сетевой инфраструктуры.

Наряду с тем, что, как будет отмечено ниже, существует много стандартов, посвященных обеспечению безопасности управляющей информации для поддержания в работоспособном состоянии инфраструктуры электросвязи, к аспекту управления относится также еще одна проблема, связанная со средой, в которой должны взаимодействовать различные поставщики услуг, с тем чтобы предоставлять услуги межабонентского типа, такие как выделенные линии для абонентов, пересекающие географические границы, или для регламентарных или государственных учреждений в условиях ликвидации последствий чрезвычайных ситуаций.

6.4.1 Архитектура административного управления сетью

Архитектура для обеспечения сетевого административного управления сетью электросвязи описана в Рекомендации М.3010, а физическая архитектура представлена на рисунке 13. Сеть управления устанавливает интерфейсы, которые определяют процессы обмена, необходимые для выполнения функций OAM&P на различных уровнях.



Интерфейс

DCN сеть передачи данных
NE сетевой элемент
OS операционная система
WS рабочая станция

Рисунок 13
Пример физической архитектуры из M.3010

В аспекте обеспечения безопасности требования для различных интерфейсов варьируются. Интерфейс Q находится в пределах одного административного домена, а интерфейс X расположен между различными административными доменами, которыми могут владеть разные поставщики услуг. При том, что услуги безопасности необходимы для обоих интерфейсов – Q и X, для интерфейса X в большей степени обязательны меры противодействия, и они должны быть более жесткими. В Рекомендации МСЭ-Т M.3016 дан обзор угроз безопасности, уязвимости и мер обеспечения безопасности для таких интерфейсов, а конкретные меры, необходимые для интерфейса X, подробно представлены в Рекомендации МСЭ-Т M.3320. Характеристики протоколов для различных слоев связи определены в Рекомендациях МСЭ-Т Q.811 и Q.812.

Анализируя проблему безопасности в контексте административного управления, следует рассматривать два ее аспекта. Первый относится к плоскости административного управления для межконцевых процессов (например, услуги VoIP). Управляющие процессы, предполагающие административное управление работой пользователей, должны быть защищены. Это называется *безопасностью управляющей информации*, которая передается по сети для обеспечения функционирования межабонентских приложений. Вторым аспектом является управление информацией безопасности. Независимо от типа приложения, например VoIP или составление донесения о неисправностях между двумя поставщиками услуг, меры безопасности, такие, как использование ключей шифрования, тоже должны находиться под управлением. Это обычно называется *управлением информацией безопасности*. Примером может служить PKI, рассмотренная в предыдущем разделе. В Рекомендации МСЭ-Т M.3400 описан ряд функций, относящихся к обоим указанным аспектам.

Для определенной в X.805 структуры можно использовать несколько Рекомендаций, посвященных функциям управления для трех ячеек плоскости административного управления. В следующих ниже подразделах приводятся в качестве примеров некоторые из этих Рекомендаций и показано, как в них решаются проблемы безопасности. Наряду с Рекомендациями для трех уровней плоскости административного управления существуют другие Рекомендации, в которых описаны родовые или общие услуги, такие, как отчеты об аварийных ситуациях при физическом нарушении безопасности, функции ревизии, а также информационные модели, определяющие уровни защиты для различных целей (то есть объекты управления).

6.4.2 Пересечение плоскость административного управления – слой инфраструктуры

Функциями данной ячейки является определение методов обеспечения безопасности процессов административного управления, осуществляемых элементами инфраструктуры сети, а именно передающими и коммутационными элементами и линиями связи между ними, а также конечными системами, такими, как серверы. Например, такие действия, как инициализация сетевого элемента, должны выполняться имеющим полномочия пользователем. Межконцевая связь может рассматриваться через сеть(и) доступа и базовую(ые) сеть(и). Эти сети могут быть построены с применением различных технологий. Для сетей доступа и базовых сетей разработаны специальные Рекомендации. В анализируемом здесь примере для доступа используется пассивная оптическая сеть для широкополосного доступа (BPON). Административное управление полномочиями пользователей для такой сети доступа определяется с применением унифицированной методологии моделирования согласно Рекомендации Q.834.3, а обмен управляющей информацией – с применением CORBA (обобщенная архитектура посредника объектных запросов) согласно Q.834.4. Описываемый в указанных Рекомендациях интерфейс является интерфейсом типа Q, который показан на рисунке 13. Он 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 функционирует на межконцевом сетевом уровне и охватывает системы административного управления разных поставщиков. На рисунке 14 показаны различные объекты, используемые для создания, удаления, распределения и применения информации управления доступом для пользователей системы управления элементами. В списке полномочий пользователя каждого авторизованного пользователя содержится перечень разрешенных функций управления. Диспетчер управления доступом проверяет идентификатор и пароль пользователя управляющих функций и предоставляет доступ к функциональным возможностям, разрешенным в списке полномочий.

6.4.3 Пересечение плоскость административного управления – слой услуг

Пересечение плоскости административного управления и слоя услуг относится к защите процессов, выполняемых для контроля и оперативного управления ресурсами сети, которые необходимы для предоставления услуг поставщиком. Рекомендации МСЭ-Т охватывают два аспекта такого пересечения. Один аспект составляет гарантирование надлежащих мер безопасности для предоставляемых по данной сети услуг. Примером может служить обеспечение того, что только получившие допуск пользователи имеют разрешение на выполнение операций, связанных с инициализацией услуги. Вторым аспектом является определение того, какой обмен административной информацией и управляющей информацией является достоверным. Такое определение поможет обнаруживать случаи нарушения безопасности. Случаи нарушения безопасности зачастую разрешаются с помощью специальных систем административного управления.

Примером Рекомендации, посвященной первому аспекту – функциям управления услуги, является Рекомендация МСЭ-Т M.3208.2 по управлению соединениями. Потребитель услуги, владеющий заранее предоставленными линиями связи, использует эту услугу для создания сквозного соединения по выделенной линии. Данная услуга управления соединениями позволяет абоненту создавать/активизировать, изменять и удалять выделенные линии связи в пределах заранее предоставленных ресурсов. Учитывая, что пользователь задает параметры сквозного соединения, необходимо обеспечить, что выполнять такие операции разрешено только имеющим полномочия пользователям. Параметры безопасности, определенные для процессов административного управления, которые связаны с данной услугой, являются набором тех восьми параметров, которые обсуждались в разделе 2.5. Это аутентификация одноранговых объектов, контроль целостности данных (для предотвращения неразрешенного изменения данных в процессе их транзита) и управление доступом (для обеспечения того, что какой-либо абонент не получит, злонамеренно или случайно, доступа к данным другого абонента).

Рекомендация МСЭ-Т M.3210.1 является примером Рекомендации, в которой определяются административные функции, связанные с плоскостью административного управления для услуг беспроводной связи. Это соответствует второму аспекту, рассмотренному выше.

В беспроводной сети пользователи при роуминге из своей сети приписки в визитную сеть могут пересекать различные административные домены. В определенных в МСЭ-Т M.3210.1 услугах описывается, как домен обнаружения мошенничества в сети приписки собирает информацию об абоненте, зарегистрировавшемся в визитной сети. В сценариях a) и b) на рисунке 15 показано инициирование контроля процесса управления сетью приписки или визитной сетью.

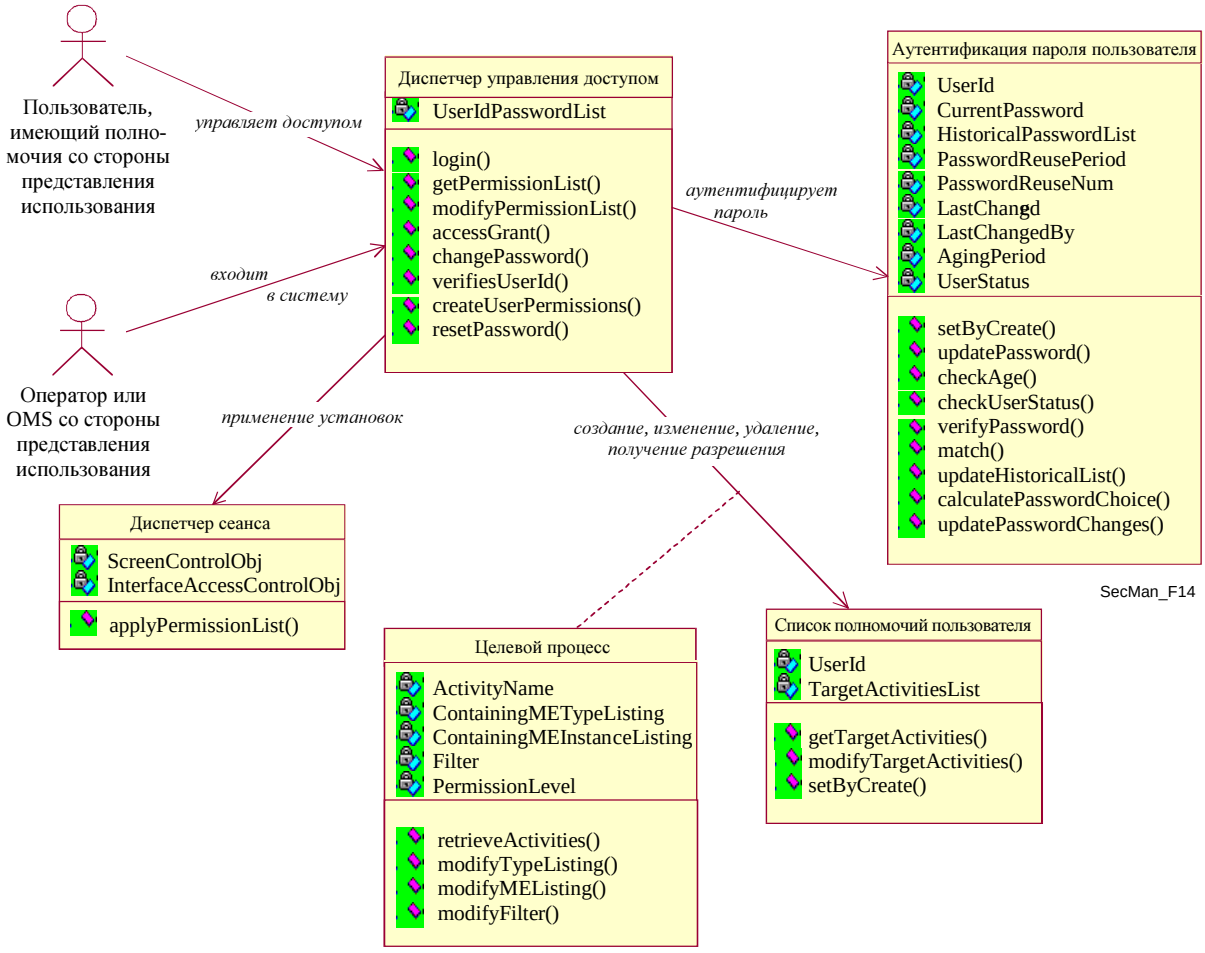


Рисунок 14
Администрирование полномочий пользователя по Q.834.3

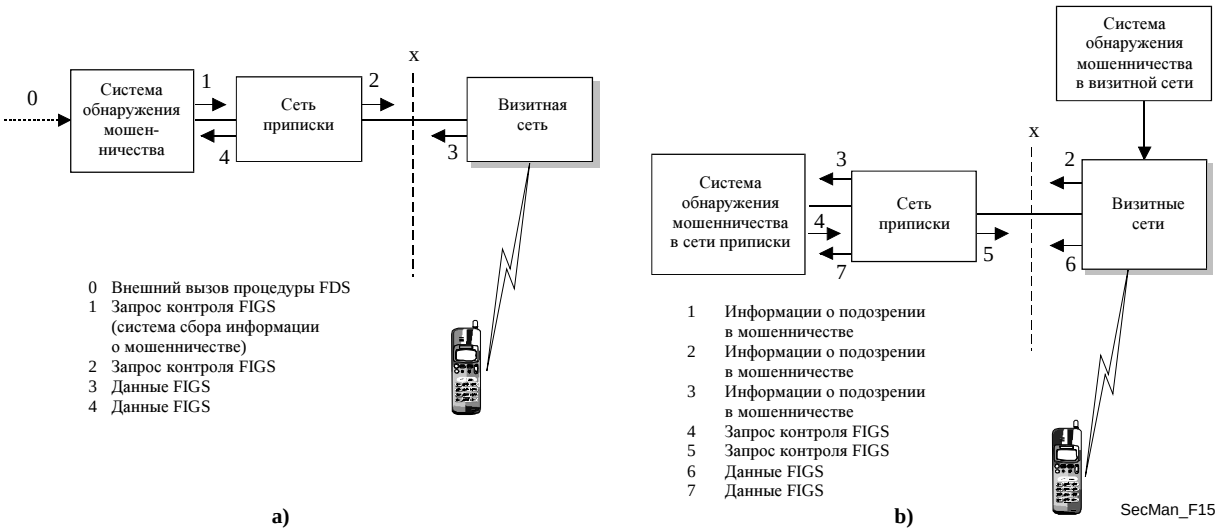


Рисунок 15
Схема обнаружения мошенничества при пользовании услугами беспроводной связи согласно Рекомендации M.3210.1

6.4.4 Пересечение плоскость административного управления – слой приложений

Третья ячейка, образующаяся на пересечении плоскости административного управления и слоя приложений, связана с обеспечением безопасности сетевых приложений конечного пользователя. Такие приложения, как передача сообщений и работа со справочниками, описаны в Рекомендациях серии X.400 и X.500.

Другой класс приложений, в которых необходимо обеспечивать защиту управляющих процессов, образуют сами приложения административного управления. Возможно, это определение представляется несколько нечетким, поэтому предпочтительнее пояснить его на конкретных примерах. Конечным пользователем таких приложений является осуществляющий административное управление (эксплуатацию) персонал администрации поставщика услуг. Рассмотрим случай, когда один поставщик услуг для предоставления своих услуг по обеспечению межабонентского соединения пользуется услугами предоставления соединения другого поставщика услуг. В зависимости от регламентарной или рыночной среды некоторые поставщики услуг могут предлагать услуги доступа, а другие, называемые *компаниями, предоставляющими услуги связи*, могут предлагать установление соединения для дальней связи. Для установления межабонентского соединения между географически разнесенными токами предоставляющие услуги связи компании арендуют услуги доступа у местных поставщиков услуг. В случае прерывания обслуживания включается приложение административного управления, называемое административной службой составления отчета о неисправности, для подготовки отчета о неисправностях, которые были обнаружены между системами административного управления. 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 поиск статуса неисправностей, вошедших в донесение. На рисунке 16 показаны виды взаимодействия, которые должны быть защищены. Аналогично администрированию почтовых ящиков приложений электронной почты осуществляется администрирование полномочий 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.

В Рекомендации X.790 содержится описание такого приложения административного управления и приводятся механизмы, такие, как список управления доступом и двусторонняя аутентификация, для защиты процессов. Указанное приложение вместе с механизмами безопасности для аутентификации реализовано в соответствии с этими Рекомендациями и внедряется.

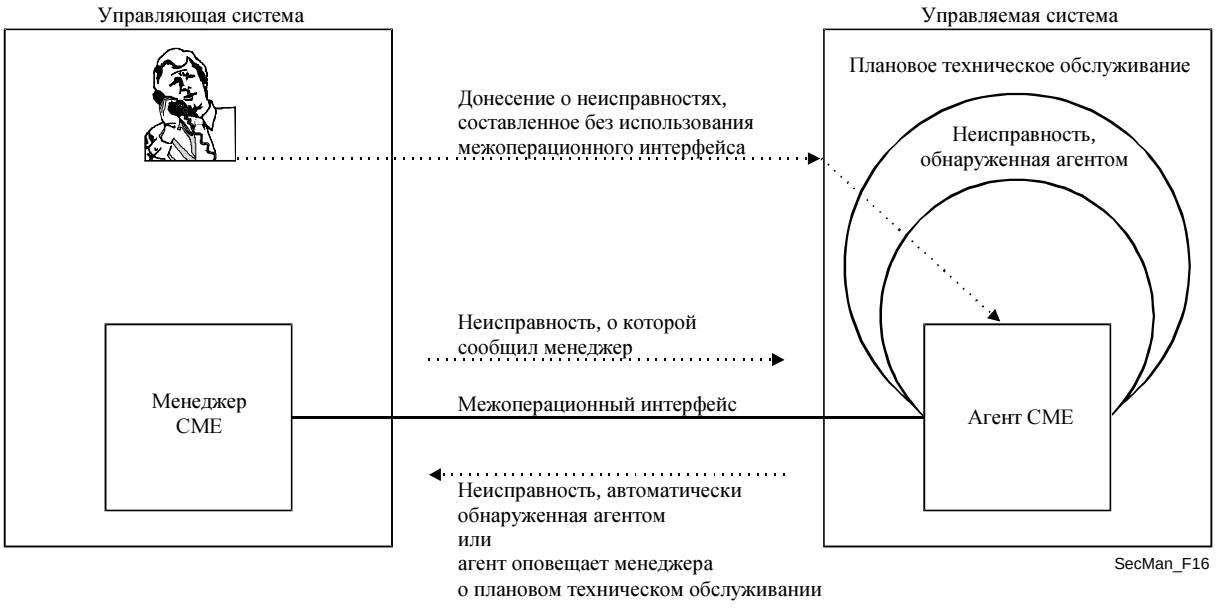


Рисунок 16
Составление отчета о неисправности согласно МСЭ-Т X.790

6.4.5 Общие услуги управления безопасностью

Рекомендации X.736, X.740 и X.741 содержат описания общих услуг, применимых для всех трех ячеек плоскости административного управления при использовании в интерфейсе протокола передачи общей управляющей информации (CMIP). В Рекомендации X.736 определены даже такие типы, как физическое нарушение безопасности, аварийные сигналы, поступающие в результате событий такого типа, донесение о которых передается управляющим системам. Это процесс плоскости административного управления, который может использоваться для донесения о нарушении безопасности, в случае если не имеющий полномочий пользователь получает доступ к функциям инициализации в сетевых элементах или регистрирует пользователей для доступа к услугам или почтовым ящикам. Функция ревизии, определенная в X.740, описывает регистрацию случаев нарушения безопасности и может применяться на всех трех уровнях. В X.741 описана весьма обобщенная и полная модель распределения полномочий управления доступом к управляющим процессам, независимым от целевого объекта. Модель обладает множеством функций за счет возможности распределения полномочий на уровне мелких структурных единиц атрибутов целевых объектов.

В Рекомендации МСЭ-Т Q.816 также приняты общие услуги безопасности, определенные на форуме Рабочей группы по управлению объектами (OMG) для управляющих процессов, выполняемых с использованием системы CORBA.

6.5 Электронные рецепты

Для работы системы здравоохранения требуется и ею производится широкий спектр данных и информации, которые необходимо собирать, обрабатывать, распределять, иметь к ним доступ и использовать их, обеспечивая при этом безопасность и соблюдая жесткие этические и правовые нормы. Это абсолютно необходимо в отношении клинической и административной информации, но также важно и в отношении информации иного типа, такой, как содержащаяся в эпидемиологических базах данных, базах данных по специальной литературе и базах знаний.

Источники данных и информации этих типов расположены в рамках и за пределами инфраструктуры здравоохранения и находятся на различном расстоянии от пользователей. На практике пользователи на разных стадиях своей деятельности нуждаются в комбинировании информации такого типа и осуществляют такое комбинирование, например: врач может обращаться к базе знаний, осматривая пациента, и делать соответствующую запись в его истории болезни, которая может использоваться для выписывания счетов.

Контакты и деловые операции в системе здравоохранения имеют множество аспектов. Они происходят, например, между пациентом и врачом, между двумя врачами, между врачом и экспертом-консультантом, между пациентом и медицинским учреждением, таким, как лаборатория по проведению анализов, аптека или реабилитационный центр. Контакты могут осуществляться в рамках собственного населенного пункта, в другой части страны или за рубежом. Для всех видов таких контактов предварительно необходимы данные и информация, а также их необходимо получать во время контакта или непосредственно после него. Такие данные и информация могут иметь разный объем, требоваться в разное время и принимать разную форму, такую, как речь, числа, текст, графические, статические или динамические изображения, и зачастую представляют рациональное сочетание этих форм.

Источники и хранилища таких данных и информации могут находиться в различных точках и отличаться по форме, например полные истории болезни, написанные от руки рецепты, а также заключения врача, консультанта или лаборатории.

Традиционно все такие контакты носили личный характер, и основными формами общения и ведения историй болезни являлась устная и письменная речь, а перевозки в основном осуществлялись государственными и частными службами с использованием автомобильного, железнодорожного или воздушного транспорта. По мере своего развития сеть телефонных услуг стала сетью общения специалистов и учреждений здравоохранения, на национальном и международном уровнях, до появления и распространения современных телематических средств в области здравоохранения.

Применение техники в клиническом/медицинском аспектах служб здравоохранения неуклонно расширялось и охватывало контрольно-измерительное оборудование и аппаратуру, особенно датчики и измерительные приборы, лабораторные службы, получение статических и динамических изображений. По мере роста масштабов использования таких технологий, а также по мере их развития и усложнения неизбежным стало отделение многих таких специальных технических служб от основных учреждений здравоохранения – отделение в географическом плане и, что более важно, в плане управления. Таким образом, проблема связи между этими использующими технику службами и основными службами здравоохранения стала важным аспектом обеспечения эффективности и экономичности этих служб.

Распространение применения информационных и коммуникационных технологий (ИКТ) в секторе здравоохранения началось более 25 лет назад с использования простой электронной системы передачи сообщений (электронной почты), по которой передавались лишь буквенно-цифровые записи и заключения. Точно так же как речевая связь служила основным побудительным мотивом для установки телефонов в кабинетах врачей и медицинских учреждениях, электронная почта стала основным доводом в пользу создания современных каналов электросвязи. И по мере развития электронной почты возрастал спрос на ее быстродействие и географический охват: большее количество пунктов доступны с большей скоростью и при большей полосе пропускания для передачи возрастающих по объему приложений к сообщениям электронной почты. За последнее десятилетие был зафиксирован экспоненциальный рост масштабов использования электронной почты в секторе здравоохранения – как в пределах одной страны, так и между странами и даже в беднейших странах, в основном через Интернет. Например, электронные деловые операции захватывают те функции, для которых не требуется личных контактов, такие, например, как составление и отправка рецептов и заключений, назначение времени приема и составление графика работы служб, направление пациентов к специалистам и, там, где возможны подобные услуги электросвязи, передача медицинских изображений и их расшифровка соответствующим специалистом, как устно, так и письменно.

Другим уровнем усложнения использования ИКТ является телемедицина – "предоставление медицинского обслуживания с использованием передачи аудио- и визуальной информации и данных", включая реальную постановку диагноза, осмотр и даже лечение географически удаленного пациента. Телемедицина представляет собой важную и развивающуюся область и, как ожидается, изменит многие традиционные подходы, существующие в здравоохранении; несомненно, это зарождение новой парадигмы в медицинском обслуживании.

Еще одной областью, которая, собственно говоря, не является новой, но которая будет расширяться с телематической поддержки, является доступ к системам, базирующимся на знаниях, и использование этих систем. Эти системы, называемые также экспертными системами и системами поддержки принятия решения, представляют собой системы, которые обеспечивают экспертный совет или указание по научно-медицинским вопросам и процедурам. Например, введя в систему координаты и симптомы пациента, можно получить диагностическую поддержку, рекомендации относительно дополнительных исследований или предложение по назначению лечения.

Все вышеперечисленные разработки оказывают также значительное воздействие на соответствующие управляющие информационные системы (MIS), необходимые для сектора здравоохранения и используемые в нем, например Hospital MIS. Это уже более не системы для административного управления больничным лечением пациентов от приема до выписки/перевода, они включают теперь большое число интеллектуальных, дружественных в отношении медицинского персонала интерфейсов для связи, например, с клиническими системами поддержки принятия решения, линиями связи телемедицины, Web-порталами и т. д.

Следует упомянуть еще два реальных аспекта, которые касаются персонала системы здравоохранения и пациентов: их мобильность и необходимость иметь свободу рук, и которые, следовательно, относятся к собственно медицинскому обслуживанию. Мобильность означает возможность для медицинских работников получения необходимой медицинской информации, например электронной истории болезни пациента, или доступа к инструменту или аппаратуре из любой удаленной точки и в любой момент, и в случае необходимости при условии проверки их полномочий, в пределах здания или города, а также в пределах всей страны и между странами. А свобода рук означает, что должны быть найдены такие методы идентификации и авторизации, которые не требовали бы выполнения медицинским работником ручных операций, например открытие двери или набор на клавиатуре компьютера.

Таким образом, здравоохранение представляет собой весьма информационноемкий сектор, в котором сбор, передача, обработка, представление и распределение данных и информации о здоровье и связанных со здоровьем, как в пределах всей страны, так и между странами, являются ключевыми факторами эффективности, продуктивности и экономичности эксплуатации и развития служб здравоохранения.

Решающим условием является безопасность и конфиденциальность всех информационных потоков, а также строгое соблюдение этических и правовых норм и положений.

6.5.1 Значение PKI и PMI для приложений электронного здравоохранения

Создавая свою цепочку сертифицирующих органов, PKI воспроизводит иерархическую структуру реального мира, как геополитическую иерархию (регионы–страны–государства–населенные пункты), так и тематическую (здравоохранение–терапия–хирургия–специализированная хирургия–поставщики, и т. д.). Кроме того, учитывая тот факт, что сектору здравоохранения присущи повсеместный характер, проникновение во все элементы иерархической структуры и возрастающее трансграничное взаимодействие, определение стандартизованных PKI/PMI для здравоохранения становится очевидной необходимостью.

Техническая совместимость систем здравоохранения должна обеспечиваться за счет широкого использования технических стандартов. Большинство поставщиков продуктов в области безопасности уже приняли такие стандарты, как, например МСЭ-Т X.509. Поскольку аутентификация пользователя является имеющим решающее значение приложением, которое зависит от местной информации, свобода выбора той или иной PKI и PMI не должна ухудшать возможности пользователя по взаимодействию с лицами, сертифицированными другой PKI/PMI в секторе здравоохранения (что, безусловно, включает по крайней мере минимальную стандартизацию в отношении управления доступом и другой связанной с этим политикой, действующей в секторе здравоохранения). Для достижения этого возможно применение разнообразных стратегий, которые могут включать взаимное признание разных инфраструктур или использование общего корня. Принятие технических стандартов, техническое взаимодействие различных инфраструктур и стандартизация конкретной стратегии гарантируют создание эффективной и интегрированной среды для осуществления операций в области здравоохранения во всемирном масштабе.

6.5.2 Система электронных рецептов в Солфорде

Система электронных рецептов, описанная в [Policy], является хорошим примером применения PKI и PMI в электронном здравоохранении. Учитывая большое число специалистов, участвующих в программе электронной передачи рецептов (ETP) в Соединенном Королевстве (34,5 тыс. врачей общей практики, 10 тыс. выписывающих лекарства сестер, число которых увеличится до 120 тыс. в течение ближайших нескольких лет, 44 тыс. зарегистрированных фармацевтов и 22 тыс. стоматологов), и весьма малый объем реально требуемых авторизаций (то есть различные уровни разрешений для выписки, отпуска лекарств и получения права на бесплатные рецепты), управление доступом по ролевому признаку (RBAC) представляется идеальным механизмом авторизации для ETP. Увязывая это с количеством возможных пациентов в Соединенном Королевстве (60 млн) и учитывая тот факт, что бесплатные рецепты составляют 85 процентов от общего числа выписанных рецептов [FrecPresc], схема RBAC должна также использоваться, если это возможно, для управления доступом к бесплатным рецептам. Учитывая весьма значительное число людей, которым необходимы разрешение/получение прав, важно не стремиться централизовать управление ролями, а распределить его между компетентными органами, в противном случае система станет неуправляемой.

Для каждого специалиста существует официальный орган, который наделяет его правом работать по специальности. В Соединенном Королевстве регистрацию врачей и исключение их из списка в случае профессионального преступления осуществляет Генеральный медицинский совет. Те же функции в отношении стоматологов выполняет Генеральный совет стоматологов, в отношении сестер – Совет по медсестринству и акушерству, и Королевский фармацевтический колледж – в отношении фармацевтов. В описанной выше системе ETP распределение ролей предоставлено этим органам, поскольку это функция, которую они уже успешно выполняют.

Созданное в июне 2001 года Министерство труда и пенсий (DWP) взяло на себя функции бывших министерств социального обеспечения, а также образования и занятости. Это министерство выплачивает пособия по безработице и пенсии и вместе с Управлением по установлению цен на отпускаемые по рецептам лекарства (PPA) определяет право на бесплатные рецепты. Многие люди имеют право на получение бесплатного рецепта, включая лиц в возрасте от 60 лет и выше, детей в возрасте до16 лет, молодежь в возрасте 16, 17 и 18 лет, занятая в системе очного образования, лица или их супруги, получающие помощь для поддержания дохода или пособие для ищущих работу, лица, указанные в сертификате Государственной службы здравоохранения (по форме HC2) об освобождении от оплаты медицинских расходов для малоимущих, беременные женщины, женщины, родившие в течение последних 12 месяцев, и военные пенсионеры по инвалидности. Соответственно, управление этими правами распределено между различными подразделениями DWP и PPA.

Для каждого специалиста его профессиональным органом определяется сертификат атрибута роли, и он хранится в каталоге LDAP, принадлежащем этому профессиональному органу. Система ETP сможет принять решение по полномочиям в отношении выписки и отпуска лекарств, если имеет доступ к таким каталогам LDAP. Аналогично, если DWP распределяет сертификаты атрибута роли лицам, по различным причинам имеющим право на бесплатные рецепты, и хранит их в каталоге (или каталогах) LDAP, то система ETP сможет принять решение о праве на бесплатный рецепт, обратившись к этому каталогу LDAP, и при этом фармацевту не нужно опрашивать пациентов, имеют ли они соответствующее право. Последнее может понадобиться только лишь в случае, когда пациент получил это право впервые, например, у женщины впервые определяется беременность ее врачом, а DWP не имел достаточного времени для составления официального сертификата атрибута.

Эти роли затем используются механизмом принятия решения о полномочиях (таким как PERMIS, см. www.permis.org) для определения, разрешено ли врачам выписывать рецепты, фармацевтам отпускать препараты и пациентам получать бесплатные рецепты в соответствии со стратегией ETP. Все приложения ETP (система выписки рецептов, система отпуска лекарств, система PPA) считывают стратегию ETP в момент инициализации, затем, когда конкретный специалист запрашивает какое-либо действие, например, прописывание или отпуск лекарств, механизм принятия решения о полномочиях извлекает роль этого лица из соответствующего каталога LDAP и принимает решение в соответствии со стратегией. Таким образом, пользователи могут получить доступ к многочисленным приложениям, и для этого им нужно владеть только парой ключей PKI. Выпуск сертификатов атрибута роли может осуществляться без участия пользователей, и они не должны беспокоиться о том, как и где хранятся и используются системой эти сертификаты.

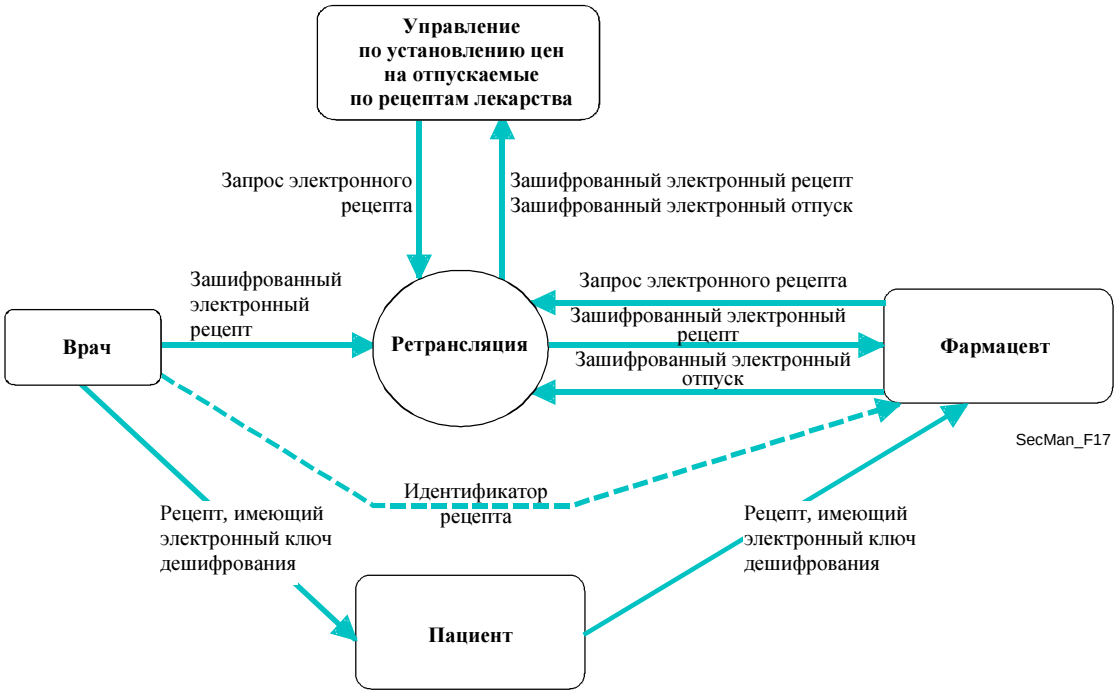


Рисунок 17
Система электронных рецептов Солфорд

На рисунке 17 представлен пример реализации системы электронных рецептов в Соединенном Королевстве, который иллюстрирует ряд вопросов обеспечения безопасности этой реализации с помощью ключей. Ядром системы является инфраструктура безопасности, которая обеспечивает не только жесткую аутентификацию (то есть PKI с сертификатами открытых ключей), но и жесткую авторизацию (то есть PMI), в которой конкретные права, которыми обладают медицинские специалисты, выдаются в соответствии с их ролью, которая хранится в сертификатах атрибутов. В традиционных моделях используются списки для управления доступом, скрытые в каждом конкретном приложении (например, медицинские карты, базы данных выписки рецептов, информация о страховании и т. д.), которые предписывают пользователям (врачам, фармацевтам, пациентам и т. д.) получить и управлять возможно несколькими различными опознавательными знаками (например, имя пользователя/пароль, карточки и т. д.). В новых моделях, где реализованы PKI и PMI, пользователям необходим только один опознавательный знак – сертификат открытого ключа пользователя, для того чтобы пользоваться различными услугами и ресурсами, которые в географическом и/или топологическом планах разнесены. Сертификаты атрибутов пользователей хранятся в системе, но не пользователями, и перемещаются между компонентами, как это необходимо для получения доступа. Поскольку сертификаты атрибутов имеют цифровую подпись выдавшего органа, они не могут быть подделаны в процессе таких перемещений.

В приведенном на рисунке 17 примере электронные рецепты создаются врачом, снабжаются цифровой подписью (в целях аутентификации), симметрично шифруются с применением произвольного сеансового ключа (для конфиденциальности), затем отправляются в центральный пункт хранения. Пациент получает выписанный на бумаге рецепт, содержащий штрих-код, несущий ключ симметричного шифрования. Затем пациент обращается в аптеку по своему выбору, предъявляет рецепт, фармацевт сканирует штрих-код, затем извлекает рецепт и дешифрует его. В конечном счете пациент контролирует, кто уполномочен отпускать лекарственные средства по его рецепту, аналогично тому, как это делается в рамках существующей бумажной системы. Но этого недостаточно. Необходимо также контролировать, кто уполномочен проживать и отпускать лекарственные средства и кто имеет право на бесплатный рецепт.

Хотя выше представлена в значительной степени интегрированная система, на практике она может быть распределенной, когда каталог атрибутов врачей не является частью системы, осуществляющей аутентификацию фармацевтов или хранящей права и стратегии отпуска лекарств, и т. д., которые полагаются на доверенные третьи стороны для проведения аутентификации и авторизации различных участников. Несмотря на то что для PKI и PMI могут применяться патентованные продукты, использование стандартизованных решений, таких, как МСЭ-Т X.509, позволяет в настоящее время обеспечить более общий и глобальный доступ к электронным рецептам.

7. Выводы

МСЭ-Т на протяжении длительного времени разрабатывает комплект основополагающих Рекомендаций в области безопасности: X.800 является базовым документом по архитектуре безопасности для взаимодействия открытых систем, а серия X.810–X.816 определяет структуру безопасности для открытых систем и включает общий обзор, аутентификацию, управление доступом, фиксацию авторства, конфиденциальность, целостность, а также аудит безопасности и аварийные извещения безопасности, соответственно. Недавно была разработана Рекомендация МСЭ-Т X.805, посвященная архитектуре безопасности для систем, обеспечивающих межабонентскую связь. Представленное в X.805 изменение архитектуры учитывает возрастающие угрозы и уязвимость, являющиеся следствием возникновения среды, которую образуют множество сетей и множество поставщиков услуг. Рекомендация X.509 по структуре открытых ключей и атрибутов, несомненно, является документом МСЭ-Т по приложениям безопасности, на который наиболее часто делаются ссылки, прямо или косвенно, в других стандартах, разработанных на основе принципов X.809.

В дополнение к этим основополагающим Рекомендациям МСЭ-Т разрабатывает положения по безопасности для некоторых систем и услуг, определенных его Рекомендациями. В настоящем Руководстве некоторые из них представлены в разделе 6: речь по протоколу IP с использованием H.323 или IPCablecom, защищенная факсимильная передача и административное управление сетью. Также приведен пример использования открытых ключей и инфраструктуры управления полномочиями в электронном здравоохранении. Следует проявить бдительность, существует множество областей, потребностям в безопасности электросвязи и информационных технологий которых посвящены Рекомендации МСЭ-Т. Эти вопросы и такие аспекты, как предотвращение мошенничества, восстановление и ликвидация последствий чрезвычайных ситуаций, которые изучаются исследовательскими комиссиями МСЭ-Т, будут рассмотрены в следующих изданиях. Работа МСЭ-Т в области безопасности подкрепляется организацией международных семинаров и практикумов по вопросам безопасности или участием в них, разработкой проектов по безопасности и назначением в МСЭ-Т ведущей исследовательской комиссии по деятельности в области безопасности.

Справочная литература

В дополнение к Рекомендациям МСЭ-Т (которые можно найти по адресу: www.itu.int/ITU-T/publications/recs.html) были также использованы следующие материалы:

[ApplCryp] B. Schneier, "Applied Cryptography – Protocols, Algorithms and Source Code in C" 2nd edition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] D. W. Chadwick; "The Use of X.509 in E-Healthcare", Workshop on Standardization in E-health; Geneva, 23-25 May 2003; PowerPoint at www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html and audio presentation at www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram

[Euchner] M. Euchner, P-A. Probst; "Multimedia Security within Study Group 16: Past, Presence and Future", ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html

[FreePresc] Free prescriptions statistics in the UK; www.doh.gov.uk/public/sb0119.htm

[Packetizer] "A Primer on the H.323 Series Standard" www.packetizer.com/iptel/h323/papers/primer/

[Policy] D. W. Chadwick, D. Mundy; "Policy Based Electronic Transmission of Prescriptions"; IEEE POLICY 2003, 4-6 June, Lake Como, Italy. sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf

[SG17] ITU-T Study Group 17; "Lead Study Group on Communication System Security" www.itu.int/ITU-T/studygroups/com17/cssecurity.html (*Section 2* on the Catalogue of ITU-T Recommendations related to Communications System Security; *Section 3* on Compendium of Security Definitions in ITU-T Recommendations)

[Shannon] G. Shannon; "Security Vulnerabilities in Protocols"; ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s1p2.html

[Wisekey] S. Mandil, J. Darbellay; "Public Key Infrastructures in e-health"; written contribution to Workshop on Standardization in E-health; Geneva, 23-25 May 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc

Приложение A: Терминология в области безопасности

Следующие акронимы и термины выбраны из соответствующих рекомендаций МСЭ-Т и других внешних источников, как указано ниже. В Приложении A.3 приведены дополнительные источники.

A.1 Наиболее часто употребляемые акронимы в области безопасности

Акроним	Определение
3DES	[H.235] Тройной DES
A	[M.3010] Агент
A/M	[M.3010] Агент/менеджер
AA	[X.509] Орган по присвоению атрибутов
AAA	[X.805] Аутентификация, авторизация и учет
AARL	[X.509] Список аннулирования органа по присвоению атрибутов
ACI	[X.810] Информация управления доступом
ACRL	[X.509] Список аннулирования сертификатов атрибутов
AE	[M.3010] Прикладной объект
AES	[H.235] [J.170] Усовершенствованный стандарт шифрования
AH	[J.170] Аутентификационный заголовок является протоколом безопасности IPSec, который обеспечивает целостность сообщения для полных IP-пакетов, включая IP-заголовки.
ASCII	[T.36] Американский стандартный код для обмена информацией
ASD	[J.170] Данные конкретного приложения. Поле, относящееся к конкретному приложению в заголовке IPSec, которое вместе с IP-адресом назначения обеспечивает уникальный номер для каждой SA.
ASN.1	[H.680] Абстрактно-синтаксическая нотация версии один
ASP	[X.805] Поставщик прикладных услуг
ATM	[X.805] Асинхронный режим передачи
ATM	[M.3010] Асинхронный режим передачи
AuF	[H.530] Функция аутентификации, см. Рек. МСЭ-Т H.510 [6]
B(n)	[T.36] Базовое значение (n)
BE	[H.530] Пограничный элемент, см. Рек. МСЭ-Т H.225.0, Приложение G [2]
BES	[H.235] Сервер нижнего уровня
BML	[M.3010] Уровень менеджмента
B-OSF	[M.3010] Уровень менеджмента – Функция операционной системы
BPI+	[J.170] Базовый интерфейс обеспечения секретности плюс является частью безопасности стандарта J.112, которая работает на уровне MAC.
CA	[H.234] [H.235] [J.170] [X.509] Сертифицирующий орган. Доверенная организация, которая принимает приложения сертификатов от объектов, аутентифицирует приложения, выдает сертификат и осуществляет сопровождение информации о статусе сертификатов. [J.170] Агент вызова. Часть CMS, которая поддерживает состояние установившейся связи и управляет связью со стороны линии связи.
CARL	[X.509] Список аннулирования сертифицирующего органа
CBC	[H.235] [J.170] Сцепление блоков шифротекста
CCA	[H.234] Национальный сертифицирующий орган
CFB	[H.235] Режим обратной связи по шифрованному тексту
CH_n	[H.530] Номер вызова n
CM	[J.170] Кабельный модем
CME	[X.790] Согласованный объект управления
CMIP	[M.3010] Протокол передачи общей управляющей информации
CMIS	[X.790] Общая служба передачи управляющей информации

Акроним	Определение
CMISE	[X.790] Элемент общей службы передачи управляющей информации
CMS	[J.170] Криптографический стандарт на синтаксис сообщений. [J.170] Сервер управления вызовами, который управляет аудиосоединениями. Также в терминологии MGCP/SGCP имеет название “агент вызова” (это один из примеров сервера приложений).
CMTS	[J.112] Оконечная система кабельных модемов
CNM	[X.790] Управление сетью клиента
CORBA	[SANCHO] Обобщенная архитектура посредника объектных запросов
CRL	[H.235] [X.509] Список аннулирования сертификатов
DCF	[M.3010] Функция передачи данных
DCN	[M.3010] Сеть передачи данных
dCRL	[X.509] дельта-Список аннулирования сертификатов
DES	[H.235] [J.170] Стандарт шифрования данных
DH	[H.235] [H.350] Диффи-Хеллман
DHCP	[J.170] [X.805] Протокол динамической конфигурации узлового компьютера
DIB	[X.509] Информационная база справочника
DIT	[X.509] Справочное информационное дерево
DN	[X.790] Отличительное имя
DNS	[H.235] [J.170] [X.805] Сервер имен доменов
DOCSIS	[J.170] Спецификация интерфейса службы передачи данных по кабелю
DoS	[X.805] Отказ в обслуживании
DQoS	[J.170] Динамическое качество обслуживания
DS-3	[X.805] Цифровой сигнал уровня 3
DSA	[X.509] Агент системы каталогов
DSCP	[J.170] Кодовое значение DiffServ. Поле в каждом IP-пакете, которое идентифицирует правило пошаговой обработки. В версии 4 IP происходит переопределение байта октета класса трафика в DSCP. В версии 6 IP октет класса трафика используется как DSCP. См. Приложение C.
DSS	[H.235] Стандарт цифровой подписи
DTMF	[H.235] [J.170] Двухтональные многочастотные (тональные сигналы)
DUA	[X.509] Агент пользователя справочника
EARL	[X.509] Список аннулирования сертификатов атрибутов конечного объекта
ECB	[H.235] Режим электронной кодовой книги
ECC, EC	[H.235] Система шифрования методом эллиптических кривых (см. Спецификацию безопасности консорциума ATM Forum – ATM Forum Security Specification Version 1.1, пункт 8.7). Система шифрования с открытым ключом.
EC-GDSA	[H.235] Алгоритм цифровой подписи на эллиптических кривых с аналоговым добавлением алгоритма цифровой подписи НИСТ (DSA) (см. также [ISO/IEC 15946-2, chapter 5])
ECKAS-DH	[H.235] Схема соглашения о ключе на эллиптических кривых Диффи-Хелмана. Схема соглашения о ключе Диффи-Хелмана с использованием криптографии на основе эллиптических кривых.
EML	[M.3010] Уровень управления сетевыми элементами
EOFB	[H.235] Расширенный режим OFB
E-OSF	[M.3010] Уровень управления сетевыми элементами – функция операционной системы
EP	[H.235] Конечная точка
EP_{ID}	[H.530] Идентификатор конечной точки MT, см. Рек. МСЭ-Т H.225.0 [1]
EPRL	[X.509] Список аннулирования сертификатов открытых ключей конечного объекта
ESH	[T.36] Зашифрованная и скремблированная открытая хэш-функция (24 десятичных разряда)
ESIM	[T.36] Зашифрованное скремблированное сообщение о целостности. Число, состоящее из 12 десятичных разрядов.
ESP	[J.170] Безопасное сокрытие содержания IPSec
ESSK	[T.36] Зашифрованный скремблированный секретный ключ. Число, состоящее из 12 десятичных разрядов.

Акроним	Определение
FDS	[M.3210.1] Система обнаружения мошенничества
FEAL	[T.36] Алгоритм высокоскоростного шифрования данных – семейство алгоритмов, преобразующих 64-битовый открытый текст в 64-битовые блоки шифротекста с 64-битовым секретным ключом. Аналогичен DES, но имеет более простую f-функцию. Разработан для обеспечения скорости и простоты, что делает его подходящим для относительно несложных микропроцессоров (например, для смарт-карт) (см. A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
FIGS	[M.3210.1] Система сбора информации о мошенничестве
FQDN	[J.170] Полностью уточненное наименование домена. Более подробно см. в IETF RFC 821.
FTP	[X.805] Протокол передачи файлов
FU	[X.790] Функциональный блок
GCA	[H.234] Общий сертифицирующий орган
GDMI	[M.3210.1] Указания для определения интерфейса административного управления TMN
GDMO	[M.3010] Руководящие принципы для определения управляемых объектов
GK	[H.235] [H.510] [H.530] Пропускной пункт
GK_{ID}	[H.530] Идентификатор визитного пропускного пункта, См. Рек. МСЭ-Т H.225.0 [1]
GNM	[X.790] Общая модель сети
GRJ	[H.530] Неприем пропускного пункта
GRQ	[H.530] Запрос пропускного пункта
GW	[H.235] Пропускной пункт
h[*]	[H.234] Результат функции h, примененной к *
H-BE	[H.530] BE приписки
HFC	[J.165] Комбинированная оптокоаксиальная (кабельная сеть)
HFX	[T.30] [T.36] Факсимильный шифр Hawthorne
H-GK	[H.530] GK приписки
HKM	[T.30] [T.36] Алгоритм управления ключами Hawthorne
HKMD1	[T.36] Двойное шифрование с использованием алгоритма HKM
HLF	[H.530] Опорная функция местонахождения
HMAC	[J.170] Код аутентификации сообщения с хэш-функцией. Алгоритм аутентификации сообщения, базирующийся на хэш-функциях SHA-1 или MD5 и определенный в RFC 2104.
HMAC-SHA1-96	[H.530] Код аутентификации хешированного сообщения с защищенным алгоритмом хеширования 1
$HMAC_Z$	[H.530] Код аутентификации хешированного сообщения/отклик с совместно используемым секретным значением Z, если Z не показан, применяется секретное значение следующего участка.
iCRL	[X.509] Косвенный список аннулирования сертификатов
ICV	[H.235] Значение проверки целостности
ID	[H.235] Идентификатор
IDEA	[T.36] Международный алгоритм шифрования данных – это алгоритм шифрования, который разработали Сюэцзя Лай (Xuejia Lai) и Джейм Масси (James Massey) в 1992 году и в котором используется блочный шифр со 128-битовым ключом (64-битовые блоки со 128-битовым ключом); в целом считается весьма криптостойким. Относится к числу наиболее популярных алгоритмов. В течение нескольких лет его использования не появилось ни одного официального сообщения о предпринятых в отношении него атак, несмотря на ряд попыток их обнаружения (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html).
Idx	[T.36] Последние шесть цифр факсимильной идентификации (номер телефона факсимильной связи) X
Idy	[T.36] Последние шесть цифр факсимильной идентификации (номер телефона факсимильной связи) Y
IKE	[J.170] Межсетевой обмен ключами – это механизм управления ключами, используемый для согласования и выведения ключей для SA в IPSec.
IKE–	[J.170] Нотация, определенная для указания на использование IKE с заданными коллективными ключами для аутентификации.

Акроним	Определение
IM	[T.36] Сообщение о контроле целостности, которое используется для подтверждения или отрицания целостности принятого сообщения (12 десятичных разрядов).
IMT-2000	[M.3210.1] Система международной подвижной электросвязи
Imy	[T.36] Сообщение о контроле целостности, генерируемое Y для подтверждения или отрицания целостности полученного сообщения (12 десятичных разрядов).
IN	[M.3010] Интеллектуальная сеть
IP	[X.805] Протокол Интернет
IPSec	[H.235] [H.530] [J.170] [X.805] Безопасность протокола Интернет
ISAKMP	[H.235] Протокол управления ключами и установления межсетевой ассоциации безопасности
ISDN	[M.3010] Цифровая сеть с интеграцией служб
ISTP	[J.170] Протокол для передачи сигнальной информации по IP-сетям
IV	[H.235] Вектор инициализации
IVR	[J.170] Интерактивная система речевой связи
K	[H.530] Динамический ключ сеанса/канала
KDC	[J.170] Центр распределения ключей
LAN	[M.3010] Локальная вычислительная сеть
LDAP	[H.235] Облегченный протокол доступа к каталогу
LLA	[M.3010] Логическая многоуровневая архитектура
MAC	[H.235] [J.170] Код идентификации сообщений. Элемент данных фиксированной длины, который отправляется вместе с сообщением для обеспечения целостности, также называется MIC. [J.170] Управление доступом к среде. Подуровень канального уровня. Обычно работает над физическим уровнем.
MAF	[M.3010] Прикладная функция управления
ГВС	[M.3010] Городская вычислительная сеть
MAPDU	[X.790] Блок данных прикладного протокола управления
MCU	[H.235] Многоточечный блок. [H.323] Многоточечный блок управления
MD5	[H.235] [J.170] Протокол Message Digest No. 5
MG	[J.170] Медиашлюз
MGC	[J.170] Контроллер медиашлюза
MGCP	[J.170] Протокол управления медиашлюзом
MIB	[J.170] [M.3010] Административная база данных
MIS	[M.3010] Служба передачи управляющей информации
MO	[M.3010] Управляемые объекты
mod n	[T.36] арифметика по модулю с основанием n
MPS	[H.235] Поток с множественными полезными нагрузками
MPx	[T.36] Взаимный примитив X.Число, состоящее из 16 десятичных разрядов, которое может генерировать только X. MPx создаются X с использованием алгоритма HKM с примитивами, сформированными из UINx, UCNx, Idx и Idy.
Mpy	[T.36] Взаимный примитив Y
MRP	[H.530] Маршрутизация через посредника в условиях мобильности
MS	[M.3210.1] Услуги административного управления
MSB	[J.170] Старший значащий бит
MT	[H.530] Мобильный терминал, См. Рек. МСЭ-Т H.510 [6]
MTA	[J.170] Адаптер медиатерминала
NAT	[H.235] Трансляция сетевых адресов
NCS	[J.170] Сигнализация вызовов в сети
NE	[M.3010] [X.790] Сетевой элемент
NEF	[M.3010] Функция элемента сети

Акроним	Определение
NEF-MAF	[M.3010] Функция элемента сети – Прикладная функция управления
NML	[M.3010] [M.3210.1] Уровень административного управления сетью
NOC	[X.790] Центр эксплуатации сети
N-OSF	[M.3010] Уровень управления сетью – Функция операционной системы
NTP	[H.530] Сетевой протокол времени
O	[M.3010] Необязательный
OA&M	[M.3010] Эксплуатация, администрирование и техническое обслуживание
OAM&P	[SANCHO] Эксплуатация, администрирование, техническое обслуживание и обеспечение
OCSP	[H.235] Протокол оперативного состояния сертификата
ODP	[X.810] Открытая распределенная обработка данных
OFB	[H.235] Режим обратной связи с выхода
OID	[H.235] [H.530] [J.170] [M.3010] Идентификатор объекта
OS	[M.3010] [X.790] Операционная система
OSF	[M.3010] Функция операционной системы
OSF-MAF	[M.3010] Функция операционной системы – Прикладная функция управления
OSI	[M.3010] [X.790] [X.805] [X.810] Взаимосвязь открытых систем
OSS	[J.170] Поддержка операционной системы. Программное обеспечение back-office, которое используется для конфигурирования, управления качеством, устранения отказов, учета и управления безопасностью.
OT	[T.36] Одноразовый ключ. Число, состоящее из от 6 до 64 десятичных разрядов, согласованное обоими пользователями.
Otx	[T.36] Одноразовый ключ, который первым использовал X при регистрации X с Y.
Oty	[T.36] Одноразовый ключ, который первым использовал Y при инициировании Y регистрации с X для выполнения взаимной регистрации, независимо от того, аналогичен он Otx или отличается от него.
P(n)	[T.36] Фазовое значение (n)
PBX	[M.3010] Учрежденческая АТС
PDU	[H.235] Протокольный блок данных
PH	[T.36] Открытая хэш-функция сообщения (24 десятичных разряда)
PKCROSS	[J.170] Использует PKINIT для установления ключей межобластного действия и связанных с ними стратегий межобластного действия, которые должны применяться при выдаче билетов сервиса для пересечения областей между областями и доменами в целях поддержки внутридоменной и междоменной сигнализации CMS–CMS (CMSS).
PKCS	[H.235] [J.170] [X.509] Криптографический стандарт с открытым ключом
PKI	[H.235] [H.530] [X.509] [J.170] Инфраструктура открытого ключа. Процесс выдачи сертификатов открытого ключа, в котором участвуют стандарты, сертифицирующие органы, а также осуществляется связь между органами и протоколами для административного управления процессами выдачи сертификатов.
PMI	[X.509] Инфраструктура управления полномочиями
PRF	[H.235] Псевдослучайная функция
Primitive	[T.36] 64-разрядное составное число, формируемое из UIN и UCN
procREGxy	[T.36] Процедура выполнения регистрации между X и Y
procSTKxy	[T.36] Процедура защищенной передачи секретного ключа от X к Y
PRS	[T.36] Псевдослучайная последовательность
ТСОП	[SANCHO] Телефонная сеть общего пользования
PTO	[M.3010] Государственный оператор электросвязи
PTR	[X.790] Отчет о неисправностях, составленный поставщиком
PVC	[X.805] Постоянный виртуальный канал
PW	[H.530] Пароль мобильного пользователя
QA	[M.3010] Q-адаптер
QoS	[SANCHO] Качество обслуживания

Акроним	Определение
R	[M.3010] Ресурс
R_1	[H.530] Произвольное число
RADIUS	[J.170] Служба удаленной аутентификации пользователей по телефонным линиям
RBAC	[X.509] Управление доступом по ролевому признаку
RC4	[J.170] Поточный шифр с переменной длиной ключа, предоставляемый в шифрокомплекте, который используется для шифрования медиатрафика в IPCablecom.
RCN	[T.36] Зарегистрированное криптографическое число. Число, состоящее из 16 десятичных разрядов.
RDN	[X.790] Относительное отличительное имя
RIP	[H.530] Запрос в процессе действия
RKS	[J.170] Сервер ведения записей. Устройство, которое собирает сообщения о событиях и выполняет их корреляцию.
RNCn	[T.36] Несекретное произвольное число, связанное с SCn. Число, состоящее из 4 десятичных разрядов.
RNIM	[T.36] Несекретное произвольное число, связанное с IM. Число, состоящее из 4 десятичных разрядов.
RNK	[T.36] Несекретное произвольное число, которое используется для обеспечения вариаций примитивов, генерируемых из MPx в процессе шифрования SK. Число, состоящее из 4 десятичных разрядов.
RNSRn	[T.36] Несекретное произвольное число, связанное с SRn. Число, состоящее из 4 десятичных разрядов.
RNSSn	[T.36] Несекретное произвольное число, связанное с SSn. Число, состоящее из 4 десятичных разрядов.
RRJ	[H.530] Отклонение регистрации
RRQ	[H.530] Запрос регистрации
RSA	[H.235] [T.30] [T.36] Алгоритм Ривеста, Шамира и Адлмана (алгоритм шифрования с открытыми ключами)
RSVP	[J.170] Протокол резервирования ресурсов
RTCP	[H.235] [J.170] Транспортный протокол управления реального времени
RTO	[J.170] Интервал для повторной передачи
RTP	[H.225.0] [H.235] [J.170] Протокол реального времени
SA	[J.170] Ассоциация безопасности
SAFER K-64	[T.36] Алгоритм на базе метода криптостойкого и скоростного шифрования с 64-битовым ключом был введен Дж. Л. Масси (J. L. Massey) в 1993 году и является итерированным блочным шифром с 64-битовыми открытым текстом и блоками шифротекста (см. A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
SCn	[T.36] Секретный ключ вызова, число n. Число, состоящее из 12 десятичных разрядов.
SDH	[M.3010] Синхронная цифровая иерархия
SDP	[J.170] Протокол описания сеанса
SDU	[H.235] Сервисный блок данных
SG	[J.170] Шлюз сигнализации является агентом сигнализации, который принимает/отправляет исходную сигнализацию SCN на границе IP-сети. В частности функция SS7 SG преобразует варианты ISUP и TCAP в SS7-Интернет шлюзе в общую версию ISUP и TCAP.
SH	[T.36] Скремблированная нешифрованная хеш-функция (24 десятичных разряда)
SHA1	[H.235] Защищенный алгоритм хеширования №1
SI	[X.810] Информация безопасности
SIP	[J.170] [X.805] Протокол инициирования сеанса связи. Управляющий протокол (сигнализация) прикладного уровня для создания, модификации и завершения сеансов с одним или более участниками.
SIP+	[J.170] Протокол инициирования сеанса связи плюс. Расширение SIP.
SK	[T.36] Секретный ключ, который может быть SCn, SRn, SSn и т. д. Число, состоящее из 12 десятичных разрядов.
SMAPM	[X.790] Протокольная машина прикладного уровня управления системой
SMK	[M.3010] Совместно используемые знания об управлении
SML	[M.3010] [M.3210.1] Уровень административного управления услугами
SMO	[X.790] Обзор управления системой
SMTP	[X.805] Простой протокол передачи почтовых сообщений

Акроним	Определение
SNMP	[J.170] [X.805] Простой протокол управления сетью
SNTP	[H.530] Простой протокол сетевого времени
SOA	[X.509] Источник полномочий
SONET	[X.805] Сеть синхронной оптической связи
S-OSF	[M.3010] Уровень управления услугами – Функция операционной системы
SRn	[T.36] Ключ кодирования ответа, число n. Число, состоящее из 12 десятичных разрядов.
SRTP	[H.225.0] [H.235] Защищенный протокол реального времени
SS	[T.36] Секретный сеансовый ключ, используемый с алгоритмом обеспечения целостности HFX40-I (12 десятичных разрядов)
SS7	[J.170] [X.805] Система сигнализации номер 7 – это архитектура и набор протоколов для выполнения внеполосной сигнализации соединений с телефонной сетью.
SSK	[T.36] Скремблированный секретный ключ. Число, состоящее из 12 десятичных разрядов.
SSL	[H.235] [X.805] Уровень защищенных разъемов
SSn	[T.36] Секретный сеансовый ключ, число n, который должен использоваться вместе с шифром несущей и/или хеш-функцией. Число, состоящее из 12 десятичных разрядов.
SSx	[T.36] Секретный сеансовый ключ, генерируемый X, который должен использоваться вместе с алгоритмом шифрования HFX40 (12 десятичных разрядов).
TCAP	[J.170] Прикладной протокол возможностей обработки транзакций. Протокол стека SS7, который используется для выполнения транзакций удаленных баз данных с пунктом управления сигнализацией.
TD	[J.170] Интервал для разъединения
TF	[M.3010] Функция преобразования
TF-MAF	[M.3010] Функция преобразования – Прикладная функция управления
TFTP	[J.170] Тривиальный протокол передачи файлов
TGS	[J.170] Сервер выдачи разрешения является подсистемой KDC, которая используется для выдачи разрешений Kerberos.
TKx	[T.36] Передаточный ключ, шифрование MPx, которое осуществляет X. Число, состоящее из 16 десятичных разрядов.
TLS	[H.235] Обеспечение безопасности транспортного уровня
TMN	[M.3010] [M.3210.1] [X.790] Сеть управления электросвязью
T_n	[H.530] Метка времени номер n
TSAP	[H.235] Пункт доступа к службе транспортного уровня
TSP	[X.790] Приоритет службы электросвязи
TTP	[X.810] Доверенная третья сторона
TTR	[X.790] Отчет о неисправностях электросвязи
UCN	[T.36] Уникальное зашифрованное число, например, UCNx, UCNy. Число, состоящее из 16 десятичных разрядов, известное только системе
UDP	[J.170] Протокол пользовательских дейтаграмм
UIN	[T.36] Уникальное идентификационное число, например, UINx, UINy, значащее число, состоящее из 48 десятичных разрядов, известное только системе
V-BE	[H.530] Визитный BE
V-GK	[H.530] Визитный GK
VLF	[H.530] Функция местонахождения посетителя
VoIP	[X.805] Голос по протоколу IP
VPN	[X.805] Виртуальная частная сеть
W	[H.530] Составное значение с арифметической комбинацией половинных ключей Диффи-Хелмана
WSF	[M.3010] Функция рабочей станции
WSSF	[M.3010] Функция поддержки рабочей станции
WT	[H.530] Нешифрованный маркер мобильности
X	[T.36] Имя одного объекта

Акроним	Определение
x	[T.36] Суффикс, определяющий, что X является владельцем или осуществил генерирование.
X<<Y>>	[H.234] Сертификат Y, генерацию которого осуществил X
XOR'd	[T.36] [H.235] Выполнение операции "Исключающее ИЛИ"
Xp	[H.234] Открытый ключ RSA объекта X
Xp[*]	[H.234] Шифрование/дешифрование [*] с Xp. В случае RSA это выполняется путем возведения в степень.
Xs	[H.234] Секретный ключ RSA объекта X
Xs[*]	[H.234] Шифрование/дешифрование [*] с Xs. В случае RSA это выполняется путем возведения в степень.
XT	[H.530] Криптомаркер для аутентификации MT
Y	[T.36] Имя второго объекта
y	[T.36] Суффикс, определяющий, что Y является владельцем или осуществил генерирование.
ZZ	[H.530] Совместно используемое секретное значение/пароль мобильного пользователя, которое используется на коллективной основе с соответствующей функцией AuF.
ZZMT	[H.530] Совместно используемое секретное значение мобильного терминала, которое используется на коллективной основе с соответствующей функцией AuF.
ZZ_n	[H.530] Совместно используемое секретное число n

A.2 Наиболее часто употребляемые определения в области безопасности

Термин	Термин	Определение
Access control	**Управление доступом**	[H.235] [X.800] Предотвращение несанкционированного использования ресурса, в том числе предотвращение использования ресурса неразрешенным образом (X.800). [J.170] Ограничение потока информации от ресурсов системы только потоками уполномоченных лиц, программ, процессов и других системных ресурсов сети. [X.805] Параметр безопасности “управление доступом” служит для защиты от несанкционированного использования сетевых ресурсов. Управление доступом обеспечивает предоставление разрешения на доступ к сетевым элементам, хранимой информации, информационным потокам, услугам и приложениям только уполномоченному персоналу или устройствам. Кроме этого, управление доступом по ролевому признаку (RBAC) организует различные уровни доступа в целях обеспечения того, что только имеющие полномочия лица и устройства могут получить доступ к сетевым элементам и работать с ними.
Access control list	**Список управления доступом**	[X.800] Список объектов и их прав доступа, имеющих полномочия на получение доступа к ресурсу.
Access Node	**Узел доступа**	[J.170] В контексте данного документа узлом доступа является устройство окончания каналов на втором уровне, который выполняет операции завершения соединения CM на сетевом конце. Определяется применяемой технологией. В Приложении A к J.112 называется INA, а в Приложении B – CMTS
Accountability	**Отчетность**	[X.800] Свойство, гарантирующее, что действия объекта могут отслеживаться с однозначной привязкой к конкретному объекту.
Active threat	**Активная угроза**	[X.800] Угроза преднамеренного несанкционированного изменения состояния системы. (Примечание – Примерами активных угроз безопасности могут служить: изменение сообщений, повторная передача перехваченных сообщений, включение подложного сообщения, нелегальное проникновение под видом полномочного объекта и отказ в обслуживании.)
Agent	**Агент**	[X.790] Согласно определению, данному в Рекомендации X.701, Обзор управления системами (SMO), но со следующими ограничениями. В отношении конкретной службы (или ресурса) электросвязи должна быть обеспечена возможность управления службой таким образом, что одна система играет роль диспетчера, а другая – роль агента.
Alias	**Псевдоним**	[X.790] Иное имя, кроме идентификатора объекта, по которому может быть опознан, обозначен или идентифицирован (обычно клиентом) отчет о неисправностях.

Термин	Термин	Определение
Application association	**Прикладная ассоциация**	[X.790] Взаимоотношения между двумя объектами прикладного уровня, которые складываются в результате осуществляемого этими объектами обмена управляющей информацией протокола прикладной системы при использовании ими услуг представительного уровня.
Application context	**Контекст приложения**	[X.790] Однозначно определенный набор сервисных элементов прикладного уровня, соответствующих опций и любой иной необходимой информации для обеспечения сетевого взаимодействия объектов прикладного уровня в ассоциации приложений.
Application entity	**Объект прикладного уровня**	[X.790] Аспекты прикладного процесса, относящегося к OSI.
Associated Alarms	**Связанные аварийные сигналы**	[X.790] Аварийные сигналы, непосредственно связанные с данной определенной неисправностью.
Asymmetric cryptographic algorithm	**Асимметричный криптографический алгоритм**	[X.810] Алгоритм выполнения шифрования или соответствующего дешифрования, при котором для шифрования и дешифрования используются разные ключи. (ПРИМЕЧАНИЕ – В некоторых асимметричных криптографических алгоритмах для дешифрования шифротекста или генерирования цифровой подписи требуется использование более одного личного ключа.)
Attack	**Атака**	[H.235] Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности системы или в целях использования их недостатков. При непосредственной атаке на систему используются недостатки базовых алгоритмов, принципов или свойств механизма обеспечения безопасности. Косвенные атаки предпринимаются путем обхода механизма безопасности или принуждения системы использовать этот механизм неправильно.
Attribute	**Атрибут**	[X.790] Информация, касающаяся управляемого объекта, которая используется для описания (частично либо полностью) этого управляемого объекта. Эта информация содержит тип атрибута и его соответствующее значение (однозначное) или значения (многозначное) атрибута.
Attribute Authority	**Орган по присвоению атрибутов**	[X.509] AA – это орган, который назначает полномочия путем выдачи сертификатов атрибутов.
Attribute Authority Revocation List	**Список аннулирования органа по присвоению атрибутов**	[X.509] AARL – это список аннулирования, в котором содержится перечень ссылок на сертификаты атрибутов, выданные органами по присвоению атрибутов, которые выдавший их орган не считает более действительными.
Attribute certificate	**Сертификат атрибута**	[X.509] Структура данных, имеющая цифровую подпись органа по присвоению атрибутов, которая связывает некоторые значения атрибутов с идентификационной информацией о держателе этого атрибута.
Attribute Certificate Revocation List	**Список аннулирования сертификатов атрибутов**	[X.509] ACRL – это список аннулирования, содержится перечень ссылок на сертификаты атрибутов, которые выдавший их орган не считает более действительными.
Attribute type	**Тип атрибута**	[X.790] Компонент атрибута, который определяет класс информации, которую несет данный атрибут.
Attribute value	**Значение атрибута**	[X.790] Конкретный экземпляр класса информации, который определен типом атрибута.
Audio Server	**Аудиосервер**	[J.170] Аудиосервер воспроизводит информационные сообщения сети IPCablecom. Информационные сообщения необходимы для незавершенных взаимодействий и для предоставления расширенных информационных услуг пользователю. Комплектующими элементами услуг аудиосервера являются медиа-устройства воспроизведения и контроллеры медиа-устройств воспроизведения.
Audit	**Аудит**	[X.800] См. Аудит безопасности.
Audit trail	**Данные проверки**	[X.800] См. Данные проверки безопасности.

Термин	Термин	Определение
Authentication	**Аутентификация**	[H.235] [X.800] [X.811] Обеспечение гарантий верности предъявленной идентификационной информации. См. Аутентификация источника данных и Аутентификация равноправного объекта (Примечание – Термин "аутентификация" не используется для обозначения целостности данных; вместо этого используется термин "целостность данных"). [J.170] Процесс проверки идентификационной информации, предъявленной одним объектом другому объекту. [X.805] Параметр безопасности "аутентификация" служит для подтверждения идентификации объектов, между которыми установлена связь. Аутентификация гарантирует верность предъявленной идентификационной информации объектов, установивших связь (например, лицо, устройство, услуга или приложение), и гарантирует, что объект не предпринимает попытки нелегального проникновения и не генерирует повторную передачу перехваченного сообщения по предыдущему соединению.
Authentication exchange	**Обменная аутентификация**	[X.800] Механизм, предназначенный для удостоверения идентификационной информации объекта путем обмена информацией.
Authentication function	**Функция аутентификации**	[H.530] AuF является функциональным объектом безопасности в домене приписки, который поддерживает связь по обеспечению безопасности с абонентами – мобильными пользователями и абонентами – мобильными терминалами.
Authentication information	**Информация аутентификации**	[X.800] Информация, которая используется для установления верности предъявленной идентификационной информации.
Authentication token; (token)	**Аутентификационный маркер (маркер)**	[X.509] Информация, передаваемая в процессе жесткой обменной аутентификации, которая может использоваться для аутентификации отправителя этой информации.
Authenticity	**Аутентичность**	[J.170] Способность удостоверения того, что данная информация не была изменена или фальсифицирована, а действительно представлена объектом, который заявлен держателем этой информации.
Authority	**Орган**	[X.509] Объект, ответственный за выдачу сертификатов. В указанной спецификации определены два типа органов: сертифицирующий орган, который выдает сертификаты открытых ключей, и орган по присвоению атрибутов, который выдает сертификаты атрибутов.
Authority certificate	**Сертификат органа**	[X.509] Сертификат, выданный органу (например, сертифицирующему органу или органу по присвоению атрибутов).
Authorization	**Авторизация**	[H.235] Предоставление разрешения на основании прошедшей аутентификацию идентификации. [J.170] Действие по предоставлению доступа к услуге или устройству при наличии разрешения на такой доступ. [X.800] Предоставление прав, которое включает предоставление доступа на основании прав доступа.
Availability	**Готовность**	[X.800] Свойство быть доступным и годным к эксплуатации по запросу имеющего полномочия объекта.
Availability	**Готовность**	[X.805] Параметр безопасности "готовность" используется для обеспечения отсутствия отказа в санкционированном доступе к сетевым элементам, хранимой информации, медиапотокам, услугам и приложениям вследствие событий, воздействующих на сеть. К этой категории относятся меры по восстановлению после аварии.
Base CRL	**Базовый CRL**	[X.509] CRL, который используется в качестве основания при генерации dCRL.
Business management layer	**Слой менеджмента**	[M.3010] Слой управления, который отвечает за все предприятие и не является предметом стандартизации.
CA-certificate	**Сертификат CA**	[X.509] Сертификат одного CA, выданный другому CA.
Cancelled	**Аннулированный**	[X/790] Диспетчер может потребовать от агента "аннулировать" отчет о неисправностях. Диспетчер хочет прервать данный отчет о неисправностях (либо вследствие возникшей ошибки, либо вследствие отсутствия состояния неисправности). При определенных условиях (например, неисправность не прошла диспетчеризацию или не была протестирована) агент "аннулирует" отчет о неисправностях путем приведения его в состояние "закрыт по запросу клиента". "Аннулирование" отчета о неисправностях может быть затребовано по причинам коммерческого характера, не входящим в область действия данной Рекомендации (например, если клиент должен оплачивать составление отчета о неисправностях).

Термин	Термин	Определение
Capability	**Возможность**	[X.800] Маркер, который используется в качестве идентификатора для ресурса, обозначающего, что владение им дает права доступа к данному ресурсу.
Certificate	**Сертификат**	[H.235] Набор относящихся к безопасности данных, который выдан органом безопасности или доверенной третьей стороной, в совокупности с информацией безопасности, которая используется для предоставления услуг обеспечения целостности и аутентификации источника в отношении данных. (X.810). В данной Рекомендации этот термин означает сертификаты "открытого ключа", которые являются значениями, представляющими открытый ключ (или иную необязательную информацию) владельца как проверенный и подписанный доверенным органом в не допускающем фальсификацию формате.
Certificate policy	**Стратегия применения сертификата**	[X.509] Поименованный набор правил, которые определяют применимость сертификата к конкретному семейству и/или классу приложений с общими требованиями к безопасности. Например, стратегия применимости данного сертификата может определять применимость типа сертификата к аутентификации транзакций электронного обмена данными для торговли товарами в пределах данного ценового диапазона.
Certificate Revocation List	**Список аннулирования сертификатов**	[X.509] CRL – это подписанный перечень, определяющий набор сертификатов, которые более не считаются действительными распределителем сертификатов. В дополнение к общему термину CRL определены несколько специфических CRL для CRL, охватывающих конкретные области.
Certificate serial number	**Серийный номер сертификата**	[X.509] Целое число, уникальное для выдавшего органа, которое однозначно связано с сертификатом, выданным данным CA.
Certificate user	**Пользователь сертификата**	[X.509] Объект, которому необходимо с уверенностью знать открытый ключ другого объекта.
Certificate validation	**Проверка достоверности сертификата**	[X.509] Процесс удостоверения того, что сертификат является действительным на данный момент времени, включая возможность построения и отслеживания пути сертификата, и удостоверения того, что все сертификаты этой линии являются действительными (то есть их срок не истек и они не аннулированы) на данный момент времени.
Certificate-using system	**Система с использованием сертификата**	[X.509] Реализация определенных в данной спецификации справочника функций, которые используются пользователем сертификата.
Certification Authority	**Сертифицирующий орган**	[X.509] CA – это орган, которому одним или более пользователями доверено создавать и распределять сертификаты открытых ключей. Сертифицирующий орган может выполнять необязательную функцию по созданию ключей пользователей. [X.810] Орган, которому доверено (в контексте стратегии обеспечения безопасности) создавать сертификаты безопасности, содержащие один или более классов данных, относящихся к безопасности.
Certification Authority Revocation List	**Список аннулирования сертифицирующего органа**	[X.509] CARL представляет собой список аннулирования, содержащий перечень выданных сертифицирующим органам сертификатов открытых ключей, которые выдавший орган не считает более действительными.
Certification path	**Путь сертификата**	[X.509] Упорядоченная последовательность сертификатов объектов в DIT вместе с открытым ключом первого объекта данного пути, по которой может быть определен открытый ключ конечного объекта данного пути.
Channel	**Канал**	[X.800] Тракт передачи информации
Cipher	**Шифр**	[H.235] Криптографический алгоритм, математическое преобразование [J.170] Алгоритм, осуществляющий преобразование данных между нешифрованным текстом и шифротекстом.
Ciphersuite	**Шифрокомплект**	[J.170] Набор, который может содержать алгоритм шифрования и алгоритм аутентификации сообщения (например, MAC или HMAC). В общем случае он может также содержать алгоритм управления ключами, который не применяется в контексте IPCablecom.
Ciphertext	**Шифротекст**	[X.800] 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.)

Термин	Термин	Определение
Clearing trouble reports	**Создание отчетов о неисправностях**	[X.790] Утверждение агента, означающее, что определенные в отчете о неисправностях действия или затребованные объектом восстановительные мероприятия успешно выполнены в целях устранения неисправности, или что такие действия более не требуются, и в обоих случаях данный отчет о неисправностях потенциально может быть закрыт.
Cleartext	**Незашифрованный текст**	[X.800] Открытые данные, семантическое содержание которых доступно.
Client	**Клиент**	[X.790] Пользователь услуги, предоставляемой системой или сетью.
Closed-out	**Закрыт**	[X.790] Отчет о неисправностях считается “закрытым”, когда агент определяет, что указанная в отчете неисправность либо устранена, либо более не существует, и агент обновляет статус отчета, с тем чтобы указать, что отчет о неисправностях “закрыт”. Изменить статус отчета о неисправностях на “закрыт” (“closedOut”) может только агент. Статус отчета о неисправностях может быть изменен на “закрыт по запросу клиента” (“closedOutByCustReq”), если от диспетчера поступил запрос аннулировать отчет.
Closing trouble reports	**Закрытие отчетов о неисправностях**	[X.790] Утверждение агента, означающее, что неисправность устранена, и что подтверждающий это отчет о неисправностях может подвергаться дальнейшей обработке только в целях создания ретроспективной записи о неисправности и/или для удаления отчета.
Communication	**Связь**	[X.805] Параметр безопасности “связь” служит для обеспечения передачи информационных потоков только между имеющими соответствующие полномочия конечными точками (в процессе передачи между этими конечными точками информация не переадресована и не перехвачена).
Conditionally trusted entity	**Условно доверенный объект**	[X.810] Объект, являющийся доверенным в контексте стратегии обеспечения безопасности, но который не может нарушить безопасность, оставаясь при этом необнаруженным.
Confidentiality	**Конфиденциальность**	[H.235] Свойство, которое служит для предотвращения раскрытия информации неуполномоченными лицами, объектами или процессами. [J.170] Способ защиты информации от раскрытия кому бы то ни было кроме санкционированных сторон. Для обеспечения конфиденциальности информация шифруется. Способ также известен как секретность. [X.800] Способ защиты информации от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами.
Conformant management entity	**Согласованный объект управления**	[X.790] Реальная открытая система, которая поддерживает интерфейс взаимодействия, определенный в данной Рекомендации.
Contact	**Контакт**	[X.790] Лицо, которое может предоставить дополнительную информацию о неисправности от имени диспетчера или агента.
Credential	**Полномочие**	[H.530] В данной Рекомендации под полномочием [такое как HMACZZ(GKID) или HMACZZ(W)] понимается некая часть данных, к которым функция AuF криптографически применила свое коллективное число ZZ, которое используется на совместной основе с мобильным пользователем. Полномочие передается для подтверждения авторизации и временного охвата в процессе проверки авторизации.
Credentials	**Полномочия**	[X.800] Данные, которые передаются для установления предъявляемой идентификационной информации объекта.
CRL distribution point	**Точка распространения CRL**	[X.509] Запись в справочнике или иной источник распространения CRL; распространяемый через точку распространения CRL может содержать записи аннулирования для единственного поднабора полного набора сертификатов, выданных CA, или может содержать записи аннулирования для многих CA.
Cryptanalysis	**Криптоанализ**	[J.170] Процесс восстановления незашифрованного текста сообщения или ключа шифрования без доступа к ключу. [X.800] Анализ криптографической системы и/или входных и выходных данных для извлечения секретных переменных и/или уязвимых данных, включая открытый текст.
Cryptographic algorithm	**Криптографический алгоритм**	[H.235] Математическая функция, которая вычисляет результат по одному или нескольким входным значениям.

Термин	Термин	Определение
Cryptographic chaining	**Криптографическое сцепление**	[X.810] Режим использования криптографического алгоритма, при котором преобразование осуществляется алгоритмом, который зависит от значений предыдущих входных или выходных данных.
Cryptographic checkvalue	**Криптографическое контрольное значение**	[X.800] Информация, получаемая в результате выполнения криптографического преобразования (см. Криптография) в блоке данных. (Примечание – Вывод контрольного значения может быть выполнен за один или за несколько шагов, и это значение является результатом математической функции ключа и блока данных. Обычно используется для проверки целостности блока данных.)
Cryptographic system, cryptosystem	**Криптографическая система, криптосистема**	[X.509] Криптографическая система или криптосистема – это библиотека преобразований из незашифрованного текста в шифротекст и наоборот. Конкретное преобразование (или конкретные преобразования), которое должно использоваться, выбирается ключами. Преобразования обычно описывается математическим алгоритмом.
Cryptography	**Криптография**	[X.800] Дисциплина, включающая принципы, средства и методы для преобразования данных, необходимого 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. Атака на принцип, средство или метод называется криптоанализом.)
Customer	**Потребитель**	[X.790] Потребителем является пользователь услуг электросвязи, предоставляемых поставщиком услуг. Конкретно в контексте данной Рекомендации потребителем является пользователь, который выбирает интерфейс OS (операционная система)–OS OSI для целей управления сетью между юрисдикциями, с тем чтобы осуществлять управление используемыми услугами (или ресурсами) электросвязи. Потребитель (или представитель потребителя) действует в роли диспетчера. Не требуется, чтобы интерфейс ограничивался случаями взаимодействия двух сторон – потребителя услуг традиционной электросвязи и поставщика услуг. Два поставщика (оператора) услуг электросвязи могут использовать этот интерфейс для обмена отчетами о неисправностях в тех ситуациях, когда их сети взаимодействуют между собой в целях предоставления услуги конечному пользователю. В этом случае роль потребителя может меняться в зависимости от ситуации. Однако в любой ситуации один оператор является потребителем и выступает в роли диспетчера, а другой – поставщиком и выступает в роли агента.
Data communication network	**Сеть передачи данных**	[M.3010] Сеть связи в пределах TMN или между несколькими TMN, которая поддерживает функцию передачи данных (DCF).
Data confidentiality	**Конфиденциальность данных**	[X.509] 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.805] Параметр безопасности "конфиденциальность данных" используется для защиты данных от несанкционированного раскрытия их содержания. Конфиденциальность данных обеспечивает невозможность прочтения содержания данных не имеющими полномочия объектами. Шифрование, списки управления доступом и права доступа к файлам являются методами, часто применяемыми для обеспечения конфиденциальности данных.
Data integrity	**Целостность данных**	[X.800] Целостность данных – это показатель того, что данные не были изменены или разрушены несанкционированным образом. [X.805] Параметр безопасности "целостность данных" удостоверяет правильность и верность данных. Данные защищены от неразрешенного изменения, удаления, создания и дублирования, а также обеспечивается индикация попыток осуществления таких несанкционированных действий.
Data origin authentication	**Аутентификация источника данных**	[X.800] Подтверждение того, что источник полученных данных соответствует объявленному.
Decipherment	**Дешифрование**	[X.800] Инверсия соответствующего обратимого шифрования.
Decryption	**Декодирование**	[X.800] См. Дешифрование.

Термин	Термин	Определение
Defer	**Задержать**	[X.790] Отложить или приостановить работу над отчетом о неисправностях до наступления соответствующих условий, когда работа может быть продолжена.
Delegation	**Делегирование**	[X.509] Передача полномочия от одного объекта, который владеет данным полномочием, другому объекту.
Delegation path	**Путь делегирования**	[X.509] Упорядоченная последовательность сертификатов, которая может быть обработана наряду с аутентификацией идентификационной информации контролера полномочий для проверки аутентичности полномочия котроллера полномочий.
Delta-CRL	**дельта-CRL**	[X.509] dCRL является частичным списком аннулирования, который содержит только записи для тех сертификатов, статус аннулирования которых изменялся с момента составления справочной базы CRL.
Denial of service	**Отказ в обслуживании**	[X.800] Недопущение санкционированного доступа к ресурсам или задержка выполнения операций, критических во времени.
Digital fingerprint	**Цифровой “отпечаток”**	[X.810] Характеристика элемента данных, например, криптографическое контрольное значение или результат выполнения односторонней хеш-функции в отношении данных, которая достаточно индивидуальна для этого элемента данных, и вследствие этого невозможно путем вычислений найти другой элемент данных, обладающий теми же характеристиками.
Digital signature	**Цифровая подпись**	[X.800] Данные, добавленные к блоку данных, или криптографическое преобразование (см. Криптография) блока данных, которые позволяют получателю данных удостоверить источник и целостность данных и обеспечить защиту от мошенничества, например, получателем.
Distinguishing identifier	**Уникальный идентификатор**	[X.810] Данные, которые однозначно определяют объект.
Downstream	**Прямое направление**	[J.170] Направление от головного узла сети к местоположению абонента.
Element management layer	**Уровень управления сетевыми элементами**	[M.3010] Уровень управления, который отвечает за управление сетевыми элементами на индивидуальной или коллективной основе.
Encipherment	**Шифрование**	[H.235] Шифрование (кодирование) – это процесс превращения данных в нечитаемые для несанкционированных объектов путем применения криптографического алгоритма (алгоритма кодирования). Дешифрование (декодирование) является обратной операцией, в результате которой криптотекст преобразуется в открытый текст. [X.800] Криптографическое преобразование данных (см. Криптография) для создания шифротекста. (Примечание – Шифрование может быть необратимым, и в этом случае выполнение соответствующего процесса дешифрования невозможно.)
Encryption	**Кодирование**	[J.170] Метод, используемый для преобразования информации в форме открытого текста в шифротекст. [X.800] См. Шифрование.
End entity	**Конечный объект**	[X.509] Имеющий сертификат объект, который использует свой открытый ключ не для целей подписи сертификатов, или объект, который является доверенной стороной.
End-entity Attribute Certificate Revocation List	**Список аннулирования сертификатов атрибутов конечного объекта**	[X.509] EARL является списком аннулирования, содержащим перечень сертификатов атрибутов, выданных не являющимся AA держателям, которые распределитель сертификатов не считает более действительными.
End-entity Public-key Certificate Revocation List	**Список аннулирования сертификатов открытых ключей конечного объекта**	[X.509] EPRL является списком аннулирования, содержащим перечень сертификатов открытых ключей, которые выданы не являющимся CA объектам и которые распределитель сертификатов не считает более действительными.
Endpoint	**Конечная точка**	[J.170] Терминал, шлюз или MCU.
End-to-end encipherment	**Сквозное шифрование**	[X.800] Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения. (См. также шифрование по участкам.)

Термин	Термин	Определение
Environmental variables	**Переменные среды**	[X.509] Это те аспекты стратегии, необходимые для принятия решения по аутентификации, которые не содержатся в статических структурах, но доступны с помощью некоторых местных средств верификатору полномочий (например, время суток или текущий статус отчета).
Escalating a trouble report	**Ужесточение отчета о неисправностях**	[X.790] Идентификация отчета о неисправности, который требует принятия срочных и безотлагательных мер для устранения этой неисправности.
Event	**Событие**	[X.790] Мгновенное явление, которое изменяет глобальный статус объекта. Изменение статуса может носить постоянный или временный характер, допускающий следовательно наблюдение, контроль и определение качества работы и т. д. События могут создавать или не создавать отчеты; они могут быть спонтанными или плановыми; могут вызывать другие события или могут быть вызваны одним или несколькими другими событиями.
Event Message	**Сообщение о событии**	[J.170] Сообщение, захватывающее единичную часть соединения.
F interface	**Интерфейс f**	[M.3010] Интерфейс, применяемый в опорных точках f.
F reference points	**Опорные точки f**	[M.3010] Опорная точка, которая находится между функциональным блоком рабочей станции (WSF) и функциональным блоком операционной системы (OSF).
Fault management	**Устранение неисправностей**	[X.790] Устранение неисправностей представляет собой набор функций, которые обеспечивают обнаружение, локализацию и корректирование анормального функционирования сети электросвязи и ее среды.
Full CRL	**Полный CRL**	[X.509] Полный список аннулирования, содержащий записи по всем сертификатам, которые были аннулированы в данной области.
Function block	**Функциональ-ный блок**	[M.3010] Наименьший (используемый) блок функциональных возможностей TMN, подлежащий стандартизации.
G reference points	**Опорные точки g**	[M.3010] Опорная точка, которая находится за пределами TMN между людьми-пользователями и функциональным блоком рабочей станции (WSF). Не считается частью TMN, несмотря на то что передает информацию TMN.
Gateway	**Шлюз**	[J.170] Устройства, осуществляющие связь между областью речевой связи IPCablecom и ТСОП. Примерами служат медиашлюзы, которые обеспечивают интерфейсы между каналами-носителями и ТСОП и транскодируют медиапотоки, а также шлюзы сигнализации, которые отправляют и принимают сигнализацию сети с коммутацией каналов на границе сети IPCablecom.
Hash function	**Хеш-функция**	[X.509] Функция (математическая), которая отображает значения из крупного (возможно очень крупного) домена в меньшем диапазоне. “Хорошей” считается такая хеш-функция, результаты применения которой к (крупной) совокупности значений в домене распределяются равномерно (и вероятно произвольно) по диапазону. [X.810] Функция (математическая), которая отображает значения из крупной (возможно очень крупной) совокупности значений в меньшем диапазоне значений.
Header	**Заголовок**	[J.170] Протокольная управляющая информация, которая находится в начале протокольного блока данных.
Holder	**Держатель**	[X.509] Объект, которому делегированы некоторые полномочия либо напрямую источником полномочий, либо косвенным образом через другой орган по присвоению атрибутов.
Home border element	**Пограничный элемент приписки**	[H.530] H-BE является пограничным элементом (BE), который расположен в границах домена приписки.
Identity-based security policy	**Стратегия обеспечения безопасности на основе идентификации**	[X.800] Стратегия обеспечения безопасности, в основу которой положена идентификационная информация и/или атрибуты пользователей, групп пользователей или объектов, действующих от имени пользователей, а также ресурсов/объектов, к которым обеспечивается доступ.
Indirect CRL	**Косвенный CRL**	[X.509] iCRL является списком аннулирования, который по крайней мере содержит информацию аннулирования по сертификатам, выданным органами, отличными от органа, выпустившего данный CRL.

Термин	Термин	Определение
Integrity	**Целостность**	[H.235] Показатель того, что данные не были изменены несанкционированным образом. [J.170] Способ удостоверения того, что информация не подвергается изменению, за исключением изменений, выполняемых имеющими на это полномочия объектами. [X.800] См. Целостность данных
Interface	**Интерфейс**	[M.3010] Архитектурная структура, которая обеспечивает взаимосвязь между физическими блоками в опорных точках.
Jurisdiction	**Юрисдикция**	[X.790] Это понятие относится к функциональному разделению сетей электросвязи. Юрисдикция бывает одного из четырех следующих видов: a) местная телефонная сеть, b) сеть обмена информацией между телефонными сетями, c) сеть конечного пользователя и d) комбинации вышеперечисленного.
Kerberos	**Kerberos**	[J.170] Протокол сетевой аутентификации с секретным ключом, который использует на выбор криптографические алгоритмы для шифрования и централизованную базу данных ключей для аутентификации.
Key	**Ключ**	[J.170] Математическая величина, введенная в выбранный криптографический алгоритм. [X.800] Последовательность символов, которые управляют операциями шифрования и дешифрования.
Key agreement	**Соглашение о ключах**	[X.509] Метод онлайнового согласования значения ключа без передачи ключа, даже в зашифрованном виде, например метод Диффи-Хелмана (более подробно о механизмах соглашения о ключах см. ISO/IEC 11770-1).
Key Exchange	**Обмен ключами**	[J.170] Обмен между объектами открытыми ключами, которые должны использоваться для кодирования связи между этими объектами.
Key management	**Управление ключами**	[H.235] [X.800] Генерирование, хранение, распределение, удаление, архивирование и применение ключей в соответствии со стратегией обеспечения безопасности.
Key-Management	**Управление ключами**	[J.170] Процесс распределения коллективных симметричных ключей, необходимых для работы протокола безопасности.
Link-by-link encipherment	**Шифрование по участкам**	[X.800] Индивидуальное применение шифрования к данным на каждом участке системы связи. См. также Сквозное шифрование. (Примечание – В результате шифрования по участкам данные на объектах ретрансляции будут находиться в форме открытого текста.)
Logical layered architecture	**Логическая многоуровневая архитектура**	[M.3010] Архитектурная концепция, согласно которой функции управления организуются в группировки уровней управления и которая описывает взаимосвязь между уровнями.
M reference points	**Опорные точки m**	[M.3010] Опорная точка, которая находится за пределами TMN между функциональным блоком адаптера Q (QAF) и управляемыми объектами, которые не соответствуют Рекомендациям по TMN.
Managed resource	**Управляемый ресурс**	[M.3010] Обобщение тех аспектов ресурсов электросвязи (логических и физических), которые требуются для управления электросвязью.
Management application function	**Прикладная функция управления**	[M.3010] Функция, которая представляет функциональные возможности (часть) одной или более услуг административного управления.
Management domain	**Домен управления**	[M.3010] Совокупность управляемых ресурсов, которые подчиняются общей стратегии управления.
Management function	**Функция управления**	[M.3010] Наименьшая часть услуги административного управления, воспринимаемая пользователем услуги.
Management function set	**Набор функций управления**	[M.3010] Набор функций управления TMN – это группировка функций управления TMN, которые сочетаются контекстуально, то есть они относятся к конкретной возможности управления (например, функции тревожных сообщений, контроль управления трафиком). Набор функций управления TMN является наименьшим повторно используемым элементом функциональной спецификации. Набор функций управления TMN должен рассматриваться как единое целое. Аналогичен части требований SMF (функции управления системой) OSI.

Термин	Термин	Определение
Management service	**Услуга административного управления**	[M.3010] Услуга административного управления – это предложение удовлетворения конкретных потребностей в отношении управления электросвязью.
Management layer	**Уровень управления**	[M.3010] Архитектурное понятие, отражающее конкретные аспекты управления и подразумевающее кластеризацию информации управления, поддерживающей данный аспект.
Manager	**Диспетчер**	[X.790] Согласно определению, данному в Рекомендации X.701, Обзор управления системами (SMO), но со следующими ограничениями. В отношении конкретной службы (или ресурса) электросвязи должна быть обеспечена возможность управления службой таким образом, что одна система играет роль диспетчера, а другая – роль агента.
Manipulation detection	**Контроль работы с данными**	[X.800] Механизм, используемый для определения случаев изменения данных (непредумышленно или намеренно).
Masquerade	**Нелегальное проникновение**	[X.800] Предпринимаемая объектом попытка представить себя другим объектом.
Media stream	**Медиапоток**	[H.235] Медиапоток может быть аудио-, видеопотоком, потоком данных или комбинацией этих типов. Медиапотоки переносят данные пользователей или приложений (полезная нагрузка), но не управляющую информацию.
Mobility routing proxy	**Маршрутизация через посредника в условиях мобильности**	[H.530] MRP является необязательным функциональным элементом, который действует как промежуточный функциональный объект, завершающий действие ассоциации безопасности последовательного канала.
Network element	**Сетевой элемент**	[M.3010] Архитектурное понятие, которое представляет оборудование электросвязи (или группы/части оборудования электросвязи) и поддерживает оборудование или любой элемент или группы элементов, которые считаются относящимися к оборудованию электросвязи, выполняющему функции элемента сети (NEF).
Network element function	**Функция элемента сети**	[M.3010] Функциональный блок, который представляет функции электросвязи и осуществляет связь с функциональным блоком TMN OSF, с тем чтобы быть охваченным контролем и/или управлением.
Network management layer	**Уровень административного управления сетью**	[M.3010] Уровень административного управления, который отвечает за управление, включая координацию действий, в ракурсе сети.
Non-repudiation	**Фиксация авторства**	[H.235] Защита от отказа признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи. [J.170] Способность предотвратить последующее непризнание отправителем факта отправки сообщения или выполнения действия. [X.805] Параметр безопасности “фиксация авторства” служит средством защиты от непризнания каким-либо лицом или объектом факта выполнения конкретного действия, связанного с данными, путем предоставления доказательств различных действий в сети (таких как доказательство обязательства, намерения или совершения; доказательство источника данных, доказательство владения, доказательство использования ресурса). Параметр обеспечивает наличие свидетельства, которое может быть представлено третьей стороне и использовано в качестве доказательства того, что имело место некоторое событие или действие.
Notarization	**Заверение**	[X.800] Регистрация данных с участием доверенной третьей стороны, которая позволяет впоследствии удостоверить соответствие характеристик этих данных, таких как содержание, источник, время и доставка.
Object method	**Объектный метод**	[X.509 Действие, которое может быть осуществлено в отношении ресурса (например, файловая система может иметь объектные методы для чтения, записи и выполнения).
One-way function	**Односторонняя функция**	[X.509] Функция (математическая) f, характеризующаяся простотой вычисления, но для общего значения y в диапазоне представляется сложным в вычислительном плане найти значение x в домене из условия, что f(x) = y. Может существовать небольшое количество значений y, для которых несложно с помощью расчетов определить значение x. [X.810] Функция (математическая), характеризующаяся простотой вычисления, но имея результат невозможно с помощью расчетов найти какое-либо значение, которое могло быть использовано для получения этого результата.

Термин	Термин	Определение
One-way hash function	**Односторонняя хеш-функция**	[X.810] Функция (математическая), которая одновременно является односторонней функцией и хеш-функцией.
Operations system	**Операционная система**	[M.3010] Физический блок, который выполняет функции операционной системы (OSF).
Operations systems function	**Функция операционной системы**	[M.3010] Функциональный блок, который обрабатывает информацию, относящуюся к управлению электросвязью для целей контроля/координации функций электросвязи и/или управления ими, включая функции административного управления (то есть саму TMN).
Outage	**Простой**	[X.790] Недоступность услуги или ресурса.
Passive threat	**Пассивная угроза**	[X.800] Угроза несанкционированного раскрытия содержания информации без изменения состояния системы.
Password	**Пароль**	[H.530] [X.800] Конфиденциальная аутентификационная информация, состоящая как правило из строки символов.
Peer-entity authentication	**Аутентификация равноправного объекта**	[X.800] Подтверждение того, что равноправный объект в ассоциации является заявленным объектом.
Perceived severity	**Воспринимаемая серьезность**	[X.790] Сложность проблемы с точки зрения составляющего отчет о неисправностях.
Physical block	**Физический блок**	[M.3010] Архитектурная структура, представляющая реализацию одного или более функциональных блоков.
Physical security	**Физическая безопасность**	[X.800] Меры, предпринимаемые для обеспечения физической защиты ресурсов от умышленных и непреднамеренных угроз.
Policy	**Стратегия**	[X.800] См. Стратегия обеспечения безопасности.
Policy mapping	**Отображение политики**	[X.509] Признание того, что когда CA, находящийся в одном домене, сертифицирует CA, находящийся в другом домене, конкретная стратегия применения сертификатов, действующая во втором домене, может рассматриваться находящимся в первом домене органом как эквивалентная (но необязательно идентичная во всех аспектах) конкретной стратегии применения сертификатов, действующей в первом домене.
Priority	**Приоритет**	[X.790] Степень срочности, которую запрашивает диспетчер для разрешения проблемной ситуации.
Privacy	**Секретность**	[H.235] Режим связи, при котором расшифровывать связь могут только имеющие на это разрешение стороны. Как правило, это достигается с помощью шифрования и коллективного ключа (коллективных ключей) для шифра. [J.170] Способ обеспечения того, что содержание информации не раскрывается сторонам, не имеющим на это разрешения. Для обеспечения конфиденциальности информация как правило кодируется. Также называется конфиденциальностью. [X.800] 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.) [X.805] Параметр безопасности "секретность" применяется в целях защиты информации, которая может быть извлечена в результате наблюдения действий в сети. Примерами такой информации могут служить посещаемые пользователем Web-сайты, географическое местоположение пользователя, а также IP-адреса и наименования DNS устройств в сети поставщика услуг.
Private channel	**Частный канал**	[H.235] В контексте данной Рекомендации частный канал – это канал, явившейся результатом предварительного соглашения о защищенном канале. В данном контексте может использоваться для обслуживания медиапотоков.
Private Key	**Личный ключ**	[J.170] Ключ, который используется в криптографии с открытым ключом, принадлежит конкретному объекту и должен оставаться секретным. [X.810] Ключ, который используется с асимметричным криптографическим алгоритмом и количество владельцев которого ограничено (обычно единственным объектом).

Термин	Термин	Определение
Private key; Secret key (deprecated)	**Личный ключ; Секретный ключ (реже)**	[X.509] Это ключ (в криптосистеме с открытым ключом) из пары ключей пользователя, который известен только пользователю.
Privilege	**Полномочие**	[X.509] Атрибут или свойство, назначенное объекту соответствующим органом.
Privilege asserter	**Контролер полномочий**	[X.509] Держатель полномочий, который использует свой сертификат атрибута или сертификат открытого ключа для контроля полномочий.
Privilege Management Infrastructure (PMI)	**Инфраструктура управления полномочиями (PMI)**	[X.509] Инфраструктура, способная поддерживать управление полномочиями при поддержке комплексной службы авторизации и при взаимодействии с инфраструктурой открытого ключа.
Privilege policy	**Стратегия распределения полномочий**	[X.509] Стратегия, определяющая для верификаторов полномочий условия предоставления/выполнения критичных услуг для обозначенных контролеров полномочий. Стратегия распределения полномочий соотносится с атрибутами, связанными с данной услугой, а также с атрибутами, связанными с контролерами полномочий.
Privilege verifier	**Верификатор полномочий**	[X.509] Объект, который удостоверяет подлинность сертификатов в соответствии со стратегией распределения полномочий.
Proxy	**Посредник**	[J.170] Средство, которое косвенно предоставляет какие-либо услуги или действует в качестве представителя при доставке информации, устраняя тем самым необходимость в центральном компьютере для поддержки этой услуги.
Public Key	**Открытый ключ**	[J.170] 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.810] Ключ, который используется с асимметричным криптографическим алгоритмом и доступ к которому может быть открытым.
Public Key Certificate	**Сертификат открытого ключа**	[J.170] Увязывание открытого ключа объекта с одним или более атрибутами, связанными с его идентификационной информацией, также называется цифровой подписью.
Public key cryptography	**Криптография с открытым ключом**	[H.235] Система шифрования, использующая асимметричные ключи (для шифрования/дешифрования), между которыми существует математическая взаимосвязь, не поддающаяся вычислению. [J.170] Процедура, в которой для шифрования и дешифрования используется пара ключей – открытый ключ и личный ключ, также называемая асимметричным алгоритмом. Доступ к открытому ключу пользователя открыт всем для использования этого ключа при отправке сообщения его владельцу. Личный ключ пользователя является секретным и единственным ключом, с помощью которого можно расшифровать сообщения, отправленные этим пользователем зашифрованными с помощью его открытого ключа.
Public Key Infrastructure (PKI)	**Инфраструктура открытого ключа (PKI)**	[X.509] Инфраструктура, способная поддерживать управление открытыми ключами, обеспечивающее поддержку услуг аутентификации, кодирования, целостности и фиксации авторства.
Public Telecommuni-cation Operator (PTO)	**Государственный оператор электросвязи (PTO)**	[M.3010] Используется для краткого обозначения администраций электросвязи, признанных эксплуатационных организаций, частных (потребитель и третья сторона) администраций и/или иных организаций, осуществляющих эксплуатацию или использующих сеть управления электросвязи (TMN).
Public-key	**Открытый ключ**	[X.509] Это ключ (в криптосистеме с открытым ключом) из пары ключей пользователя, содержание которого открыто.
Public-key certificate	**Сертификат открытого ключа**	[X.509] Открытый ключ пользователя в сочетании с некоторой иной информацией, подделка которого исключена за счет шифрования с личным ключом сертифицирующего органа, который его выдал.
Q adapter	**Адаптер q**	[M.3010] Физический блок, характеризуемый содержащимся функциональным блоком адаптера q и соединяющий физические объекты типов NE и OS, интерфейсы которых не совместимы с TMN (в опорных точках m), с интерфейсами q.
Q interface	**Интерфейс q**	[M.3010] Интерфейс, применяемый в опорных точках q.

Термин	Термин	Определение
Q reference points	**Опорные точки q**	[M.3010] Опорная точка, которая находится между NEF и OSF, между QAF и OSF и между OSF и OSF.
Reference point	**Опорная точка**	[M.3010] Архитектурная структура, используемая для определения границ функциональных блоков управления, и которая определяет границы зон обслуживания между двумя функциональными блоками управления.
Relying party	**Доверяющая сторона**	[X.509] Пользователь или агент, которые при принятии решения основываются на данных сертификата.
Repudiation	**Непризнание авторства**	[X.800] Отказ признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи.
Revocation certificate	**Сертификат аннулирования**	[X.810] Сертификат безопасности, выданный органом безопасности для указания, что конкретный сертификат безопасности был аннулирован.
Revocation list certificate	**Сертификат списка аннулирования**	[X.810] Сертификат безопасности, который определяет список сертификатов безопасности, которые были аннулированы.
Role assignment certificate	**Сертификат назначения роли**	[X.509] Сертификат, содержащий атрибут роли, которым предмету/держателю сертификата назначается одна или более ролей.
Role specification certificate	**Сертификат определения роли**	[X.509] Сертификат, содержащий назначение полномочий какой-либо роли.
Root Private Key	**Корневой личный ключ**	[J.170] Личный ключ подписи сертифицирующего органа наивысшего уровня. Обычно используется для подписания сертификатов открытых ключей для сертифицирующих органов более низких уровней или для иных объектов.
Routing control	**Управление маршрутизацией**	[X.800] Применение правил в процессе маршрутизации для выбора или обхода конкретных сетей, каналов и ретрансляторов.
Rule-based security policy	**Стратегия безопасности на основе правил**	[X.800] Стратегия безопасности на основе глобальных правил, которые распространяются на всех пользователей. Эти правила обычно связаны со сравнением критичности ресурсов, к которым имеется доступ, и владением соответствующими атрибутами пользователей, групп пользователей или объектов, действующих от имени пользователей.
Seal	**Печать**	[X.810] Криптографическое контрольное значение, которое обеспечивает поддержку целостности, но не защищает от подлога, осуществляемого получателем (то есть не обеспечивает фиксацию авторства). Если печать связана с элементом данных, этот элемент данных называется имеющим печать. (Примечание – Несмотря на то что печать не обеспечивает фиксацию авторства, некоторые механизмы фиксации авторства используют услугу целостности, обеспечиваемую печатями, например, для защиты связи с доверенными третьими сторонами).
Secret key	**Секретный ключ**	[X.810] Ключ, который используется с симметричным алгоритмом шифрования. Владение секретным ключом ограничивается (обычно двумя объектами).
Secure interaction rules	**Правила защищенного взаимодействия**	[X.810] Правила стратегии обеспечения безопасности, которые регулируют взаимодействие между доменами безопасности.
Security administrator	**Администратор безопасности**	[X.810] Лицо, ответственное за определение или выполнение требований одной или более частей стратегии обеспечения безопасности.
Security audit	**Аудит безопасности**	[X.800] Независимый анализ или ревизия системных записей и действий для проверки на адекватность управляющих функций системы, для обеспечения соответствия установленным стратегическим и эксплуатационным процедурам, для выявления нарушения безопасности и для предложения каких-либо изменений в управлении, стратегии или процедурах.
Security audit trail	**Данные проверки безопасности**	[X.800] Данные, которые собраны и могут быть использованы для содействия проведению аудита безопасности.
Security authority	**Орган безопасности**	[X.810] Объект, ответственный за определение, реализацию и выполнение стратегии обеспечения безопасности.

Термин	Термин	Определение
Security certificate	**Сертификат безопасности**	[X.810] Набор связанных с безопасностью данных, выданных органом безопасности или доверенной третьей стороной, вместе с информацией безопасности, которая используется для обеспечения услуг целостности и аутентификации источника данных. (Примечание – Все сертификаты считаются сертификатами безопасности (соответствующие определения см. в ISO 7498-2). Термин "сертификат безопасности" принят во избежание терминологического несоответствия с Рекомендацией МСЭ-Т X.509 | ISO/IEC 9594-8; то есть стандартом аутентификации справочника).
Security certificate chain	**Цепочка сертификатов безопасности**	[X.810] Упорядоченная последовательность сертификатов безопасности, в которой первый сертификат безопасности содержит связанную с безопасностью информацию, а все последующие сертификаты безопасности содержат информацию безопасности, которая может использоваться для проверки достоверности предыдущих сертификатов безопасности.
Security domain	**Домен безопасности**	[X.810] Совокупность элементов, стратегий обеспечения безопасности, органа безопасности и набора связанных с обеспечением безопасности действий, в котором набор элементов является объектом стратегии безопасности для определенных действий, а управление стратегией обеспечения безопасности выполняется органом безопасности для домена безопасности.
Security domain authority	**Орган безопасности домена**	[X.810] Орган безопасности, ответственный за осуществление стратегии обеспечения безопасности для домена безопасности.
Security information	**Информация безопасности**	[X.810] Информация, необходимая для реализации услуг обеспечения безопасности.
Security label	**Метка безопасности**	[X.800] Маркировка, связанная с ресурсом (которым может быть блок данных), определяющая имя или обозначение атрибутов безопасности данного ресурса. (Примечание – Маркировка и/или связывание может быть явным или неявным.)
Security policy	**Стратегия обеспечения безопасности**	[X.509] Набор правил, установленных органом безопасности, который управляет использованием и предоставлением услуг и средств безопасности. [X.800] Набор критериев для предоставления услуг безопасности (см. также Стратегия обеспечения безопасности на основе идентификационной информации и на основе правил). (Примечание – Полная стратегия обеспечения безопасности неизбежно затрагивает многие вопросы, выходящие за рамки OSI.)
Security policy rules	**Правила стратегии обеспечения безопасности**	[X.810] Представление стратегии обеспечения безопасности для домена безопасности в пределах реальной системы.
Security profile	**Профиль безопасности**	[H.235] Набор (поднабор) согласованных, взаимодействующих процедур и характеристик, которые выходят за рамки H.235 МСЭ-Т и используются для защиты мультимедийной связи H.323 между участвующими в определенном сценарии объектами.
Security recovery	**Восстановление безопасности**	[X.810] Принимаемые решения и выполняемые процедуры при обнаружении нарушения безопасности или при возникновении подозрения о таком нарушении.
Security service	**Услуга безопасности**	[X.800] Услуга, предоставляемая каким-либо уровнем открытых систем связи, которая гарантирует достаточную защиту систем или процессов передачи данных.
Security token	**Маркер безопасности**	[X.810] Совокупность данных, которая защищена одной или более услугами безопасности, вместе с информацией безопасности, используемой при предоставлении этих услуг безопасности, которая передается между установившими связь объектами.
Selective field protection	**Селективная защита полей**	[X.800] Защита конкретных полей в сообщении, которое подлежит передаче.
Sensitivity	**Критичность**	[X.509] Характеристика ресурса, которая воздействует на его значение или важность. [X.800] Характеристика ресурса, которая воздействует на его значение или важность и может также включать его уязвимость.
Service	**Услуга**	[X.790] Данный термин означает возможности электросвязи, которые потребитель покупает или арендует у поставщика услуг. Услуга является абстракцией ракурса, ориентированного на сетевой элемент или ориентированного на оборудование. Различные сетевые элементы могут предоставлять одинаковые услуги, и различные услуги могут предоставляться одинаковыми сетевыми элементами.

Термин	Термин	Определение
Service management layer	**Служебный уровень управления**	[M.3010] Уровень административного управления, который связан с контрактными аспектами услуг, предоставляемых потребителям или доступных для потенциальных потребителей, и является ответственным за них, включая обработку заказов на предоставление услуг, работу с жалобами и выставление счетов.
Service provider	**Поставщик услуг**	[X.790] Система или сеть, которые предоставляют потребителю услуги электросвязи. В контексте данного документа поставщик услуг – это поставщик услуг электросвязи, который предоставляет интерфейс OS-OS OSI, с тем чтобы обеспечить для потребителей возможности сетевого управления между юрисдикциями с целью управления предоставляемыми услугами (ресурсами) (см. Потребитель). Поставщик услуг выступает в роли агента. Не требуется, чтобы интерфейс ограничивался случаями взаимодействия двух сторон – потребителя услуг традиционной электросвязи и поставщика услуг. Вполне возможно, что два оператора услуг, чьи сети взаимодействуют между собой в целях предоставления услуги конечному пользователю, могут использовать этот интерфейс. В этом случае роль потребителя и поставщика услуг может меняться в зависимости от ситуации. Однако в любой ситуации один оператор является потребителем и выступает в роли диспетчера, а другой – поставщиком и выступает в роли агента.
Service relationship	**Служебная взаимосвязь**	[H.530] Дает ссылку на установленную ассоциацию безопасности между двумя функциональными объектами, предполагая что представлен, по крайней мере, какой-либо коллективный ключ.
Shared secret	**Коллективное секретное значение**	[H.530] Означает ключ системы защиты для криптографических алгоритмов; может быть выведен по значению пароля.
Signature	**Подпись**	[X.800] См. Цифровая подпись.
Simple authentication	**Простая аутентификация**	[X.509] Аутентификация посредством соглашений о простых паролях.
Source of Authority	**Источник полномочий**	[X.509] SOA является органом по присвоению атрибутов, которому верификатор полномочий для конкретного ресурса доверяет как высшему органу по назначению набора полномочий.
Spamming	**Рассылка спама**	[H.235] Атака типа “отказ в обслуживании”, возникающая при пересылке незапрашиваемых данных, которые перегружают систему. Особым случаем является рассылка медиаспама при передаче пакетов RTP на порты UDP. Обычно система переполняется пакетами, и обработка поглощает весьма значительные ресурсы системы.
Status of a trouble report	**Статус отчета о неисправностях**	[X.790] Стадия, в которую переходит отчет о неисправностях после его конкретизации/создания, в процессе устранения неисправности.
Strong authentication	**Жесткая аутентификация**	[X.509] Аутентификация с помощью криптографически выведенных полномочий.
Symmetric (secret-key based) cryptographic algorithm	**Симметричный криптографический алгоритм (на основе секретного ключа)**	[H.235] Алгоритм выполнения шифрования или соответствующий алгоритм выполнения дешифрования, в котором для шифрования и дешифрования требуется один и тот же ключ. (X.810).
Symmetric cryptographic algorithm	**Симметричный криптографический алгоритм**	[X.810] Алгоритм выполнения шифрования или соответствующий алгоритм выполнения дешифрования, в котором для шифрования и дешифрования требуется один и тот же ключ.
Telecommunications management network	**Сеть управления электросвязью**	[M.3010] Архитектура для осуществления управления, включая планирование, обеспечение, утановку, техническое обслуживание, эксплуатацию и администрирование оборудования, сетей и услуг электросвязи.
Threat	**Угроза**	[H.235] Потенциальное нарушение безопасности (X.800). [X.800] Потенциальное нарушение безопасности.

Термин	Термин	Определение
Time-stamp	**Метка времени**	[X.790] Значение времени, которое используется для указания того, когда было выполнено конкретное действие или наступило конкретное событие.
Traffic analysis	**Анализ трафика**	[X.800] Анализ информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота).
Traffic flow confidentiality	**Конфиденциальность потоков трафика**	[X.800] Услуга обеспечения конфиденциальности для защиты от анализа трафика.
Traffic padding	**Подстановка трафика**	[X.800] Генерирование фальшивых экземпляров связи, фальшивых блоков данных и/или фальшивых данных в пределах блоков данных.
Transformation function	**Функция преобразования**	[M.3010] Функциональный блок, который осуществляет преобразование между опорной точкой TMN и опорной точкой не-TMN (являющейся интеллектуальной собственностью или иным образом стандартизованной). Часть не-TMN данного функционального блока находится за границей TMN.
Trouble	**Неисправность**	[X.790] Любая причина, которая может привести к восприятию или способствовать восприятию диспетчером ухудшения качества обслуживания одной или более сетевых услуг или одного или более сетевых ресурсов, находящихся под управлением.
Trouble administration	**Администрирование неисправностей**	[X.790] Администрирование неисправностей состоит из набора функций, которые позволяют подготовить отчет о неисправностях и проследить их статус. Услуги администрирования неисправностей включают запрос формата отчета о неисправностях, ввод отчета о неисправностях, добавление информации о неисправностях, аннулирование отчета о неисправностях, запрос статуса отчета о неисправностях, анализ предыстории неисправности, извещение об изменении значения атрибута (например, статус отчета/время фиксации), создание/удаление объекта (отчет о неисправностях), проверку завершения устранения неисправности и изменение информации администрирования неисправностей.
Trouble history record	**Ретроспективная запись о неисправности**	[X.790] Запись выборочной информации из отчета о неисправностях, которая сохраняется для создания предыстории после закрытия отчета о неисправностях.
Trouble management	**Устранение неисправностей**	[X.790] Отчет о неисправностях и отслеживание неисправностей между взаимодействующими на коллективной основе СМЕ до устранения неисправностей. (Различие между интерфейсами в пределах юрисдикции и между юрисдикциями не проводится.)
Trouble reporting	**Сообщение о неисправности**	[X.790] Процесс сообщения об обнаружении неисправности, для устранения которой может использоваться процесс устранения неисправностей.
Trouble resolution	**Ликвидация неисправностей**	[X.790] Процесс диагностирования и выполнения ремонтных действий, необходимых для устранения проблемной ситуации. Включает процесс назначения конкретных рабочих заданий или общей ответственности за очистку и закрытие отчета о неисправностях.
Trouble tracking	**Отслеживание неисправностей**	[X.790] Способность прослеживать отчет о неисправностях с момента его создания до его закрытия.
Trouble type	**Тип неисправности**	[X.790] Описание или категория неисправности, которая была обнаружена.
Trust	**Доверие**	[[X.509] В общем случае объекту может быть указано "доверять" другому объекту, когда этот (первый) объект делает предположение о том, что поведение второго объекта будет в точности соответствовать ожидаемому первым объектом. Такое доверие можно применять только к некоторым определенным функциям. Ключевая роль доверия в этой структуре заключается в описании взаимосвязи между выполняющим аутентификацию объектом и органом. Объект должен быть уверен, что может доверять органу в отношении создания только достоверных и надежных сертификатов. [X.810] Объекту X указано доверять объекту Y в отношении набора действий, только лишь если объект X полагается на определенность поведения объекта Y в отношении этих действий.
Trusted entity	**Доверенный объект**	[X.810] Объект, который может нарушить стратегию обеспечения безопасности либо путем выполнения действий, которые не предполагаются, либо путем невыполнения действий, которые предполагаются.
Trusted functionality	**Доверенная функциональность**	[X.800] Функциональность, воспринимаемая как корректная по определенным критериям, например как установленная стратегией обеспечения безопасности.

Термин	Термин	Определение
Trusted third party	**Доверенная третья сторона**	[X.810] Орган безопасности или его агент, который является доверенным в отношении некоторых связанных с безопасностью действий (в контексте стратегии обеспечения безопасности).
Unconditionally trusted entity	**Безусловно доверенный объект**	[X.810] Доверенный объект, который может нарушить стратегию обеспечения безопасности, оставаясь необнаруженным.
User	**Пользователь**	[M.3010] Лицо или процесс, который применяет услуги управления для осуществления операций управления.
Visited border element	**Визитный пограничный элемент**	[H.530] V-BE является пограничным элементом (BE), расположенный в пределах визитного домена.
Workstation	**Рабочая станция**	[M.3010] Физический блок, который выполняет функции рабочей станции (WSF).
Workstation function	**Функция рабочей станции**	[M.3010] Функциональный блок, который интерпретирует информацию TMN для человека-пользователя и наоборот.
X interface	**Интерфейс x**	[M.3010] Интерфейс, применяемый в опорных точка x.
X reference points	**Опорные точки x**	[M.3010] Опорная точка, которая находится между функциональными блоками OSF в разных TMN. (Примечание – Объекты, расположенные за пределами опорной точки x, могут быть частью среды TMN (OSF) или частью среды не-TMN (подобной OSF). Такая классификация в опорных точках x невидима.)
X.509 certificate	**Сертификат X.509**	[J.170] Спецификация сертификата открытого ключа, разработанная как часть каталога стандартов X.500 МСЭ-Т.

A.3 Другие источники терминов и определений МСЭ-Т

Онлайновая база данных МСЭ-Т SANCHO (*Аббревиатуры и определения, используемые в Секторе для тезаурусов в области электросвязи – Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented*), обеспечивающая доступ к принятым в публикациях МСЭ-Т терминам и определениям, а также аббревиатурам и акронимам на английском, испанском и французском языках. Это онлайновый источник, свободный доступ к которому осуществляется по адресу www.itu.int/sancho. Также регулярно публикуется версия на CD-ROM. Все перечисленные выше термины и определения содержатся в SANCHO и сопровождаются перечнем Рекомендаций, в которых они встречаются.

ИК 17 МСЭ-Т разрабатывает каталог определений в области безопасности, используемых в Рекомендациях МСЭ-Т, который размещен по адресу www.itu.int/ITU-T/studygroups/com17/cssecurity.html.

Приложение B: Каталог Рекомендаций МСЭ-Т, связанных с безопасностью

B.1 Аспекты безопасности, рассмотренные в данном Руководстве

F.400 *Обзор систем и служб обработки сообщений*

В данной Рекомендации содержится обзор всей системы и службы обработки сообщений (MHS), и он является общим обзором MHS. Этот обзор представляет собой одну из Рекомендаций группы Рекомендаций, описывающих модель системы, элементы службы "система обработки сообщений" (MHS) и услуги. В данной Рекомендации дан обзор возможностей MHS, используемых поставщиками услуг для обеспечения служб обработки сообщений (МН) общего пользования, дающих пользователям возможность обмениваться сообщениями по методу с промежуточным накоплением. Система обработки сообщений разработана в соответствии с принципами эталонной модели взаимосвязи открытых систем (OSI) для приложений МСЭ-Т (X.200) и использует услуги представительного уровня и услуги, предоставляемые другими, более общими прикладными служебными элементами. MHS может быть построена с использованием любой сети, соответствующей принципам взаимосвязи открытых систем (OSI). Услуга переноса сообщений, предоставляемая MTS, не зависит от приложения. Примерами стандартизованных приложений являются служба IPM (F.420 + X.420), служба передачи сообщений EDI (F.435 + X.435) и служба обмена речевыми сообщениями (F.440 + X.440). Оконечные системы могут использовать службу переноса сообщений (MT) для конкретных приложений, которые двусторонне определены. Службы обработки сообщений, предоставляемые поставщиками услуг, относятся к группе телематических служб. Службы общего пользования, построенные на MHS, а также доступ в MHS и от MHS для служб общего пользования определены в Рекомендациях серии F.400. Технические аспекты MHS освещены в Рекомендациях серии X.400. Общая архитектура системы MHS определена в Рекомендации МСЭ-Т X.402. Элементами службы являются функции службы, обеспечиваемые посредством прикладных процессов. Считается, что элементами службы должны быть предоставляемые пользователям компоненты служб, и они являются или элементами базовой службы, или необязательными пользовательскими возможностями, классифицируемыми как существенные необязательные пользовательские возможности или как дополнительные необязательные пользовательские возможности. Возможности обеспечения **безопасности** MHS описаны в пункте 15 F.400, включая **угрозы безопасности** MHS, модель безопасности, элементы службы, описывающие характеристики безопасности (определены в Приложении B), **управление безопасностью**, зависимость защиты MHS, безопасность IPM. Вопрос 11/17

F.440 *Служба обработки сообщений: Служба обмена речевыми сообщениями **(VM)***

В этой Рекомендации заданы общие и рабочие аспекты, аспекты качества обслуживания международной службы обмена речевыми сообщениями (**VM**) общего пользования – специфического типа службы обработки сообщений (МН) общего пользования. Эта служба является международной службой электросвязи, предоставляемой Администрациями, которая дает возможность абонентам отправлять сообщение одному или более получателям и принимать сообщения по сетям электросвязи, используя комбинацию методов "накопление и передача" и "накопление и поиск". Служба VM дает абонентам возможность запрашивать выполнение различных функций во время обработки речевых и кодированных сообщений и обмена этими сообщениями. Некоторые функции входят в базовую службу VM. Другие, не базовые, функции могут быть выбраны абонентом или для конкретного сообщения, или на согласованный в контракте период времени, если они обеспечиваются Администрациями. Взаимосвязь со службой межабонентского обмена сообщениями (IPM) может обеспечиваться как опция службы VM. Готовность базовых функций должна обеспечиваться Администрациями на международном уровне. Небазовые функции, доступные пользователю, классифицируются как существенные или дополнительные. Существенные необязательные функции должны обеспечиваться Администрациями на международном уровне. Дополнительные необязательные функции могут быть на основании двустороннего соглашения сделаны доступными некоторыми Администрациями для использования внутри страны и на международном уровне. Небазовые функции называются необязательными пользовательскими возможностями. Служба VM может быть организована с использованием любой сети электросвязи. Служба VM может организовываться отдельно или в сочетании с различными телематическими службами или службами передачи данных. Технические спецификации и протоколы, которые должны использоваться в службе VM, определены в Рекомендациях серии X.400.

Приложение G: **Защищенные** элементы службы обмена речевыми сообщениями

Приложение H: Общий обзор **безопасности** обмена речевыми сообщениями Вопрос 11/17

F.851 *Универсальная персональная электросвязь **(UPT)** – Описание службы (набор служб 1)*

Данная Рекомендация содержит описание службы и эксплуатационного обеспечения универсальной персональной электросвязи (**UPT**). Рекомендация содержит общее описание службы с точки зрения индивидуального абонента UPT или пользователя UPT. UPT также дает возможность пользователю UPT работать с определенным им самим набором абонированных услуг, с помощью которых пользователь задает персональные требования для формирования профиля службы UPT. Пользователь UPT может использовать службу UPT с минимальным риском нарушения секретности или ошибочной тарификации, вызванной злонамеренным использованием. В принципе со службой UPT может использоваться любая базовая служба электросвязи. Службы, обеспечиваемые для пользователя UPT, ограничиваются только используемыми сетями и терминалами. Первой среди существенных функций для пользователя является "аутентификация идентичности пользователя UPT", а необязательной пользовательской функцией – аутентификация поставщика службы UPT. В разделе 4.4 подробно описаны требования к безопасности. Вопрос 3/2

H.233 *Система обеспечения конфиденциальности для аудиовизуальных служб*

Система засекречивания состоит из двух частей – механизма обеспечения конфиденциальности, или процесса шифрования данных, и подсистемы управления ключами. В данной Рекомендации описывается обеспечивающая конфиденциальность часть системы засекречивания, пригодная для использования в узкополосных аудиовизуальных службах. Хотя для такой системы засекречивания требуется алгоритм шифрования, в Рекомендацию не включена спецификация такого алгоритма: система подходит для более чем одного определенного алгоритма. Система обеспечения конфиденциальности может применяться для каналов точка-точка между терминалами или между терминалом и многоточечным блоком управления (MCU); она может быть расширена для многоточечной работы, при которой нет шифрования в MCU. Вопрос G/16

H.234 *Система управления ключами шифрования и аутентификации для аудиовизуальных служб*

Система засекречивания состоит из двух частей – механизма обеспечения конфиденциальности, или процесса шифрования данных, и подсистемы управления ключами. В данной Рекомендации описываются методы аутентификации и управления ключами для системы засекречивания, пригодной для использования в узкополосных аудиовизуальных службах. Секретность достигается использованием *секретных ключей*. Ключи загружаются в часть системы, обеспечивающую конфиденциальность, и управляют процессом шифрования и дешифрования передаваемых данных. При доступе третьих лиц к используемым ключам система засекречивания перестает быть безопасной. Поэтому обеспечение хранения ключей пользователями является важной частью любой системы засекречивания. В данной Рекомендации определены три альтернативных практических метода управления ключами. Вопрос G/16

H.235 *Защита и шифрование для мультимедийных терминалов серии H (H.323 и других терминалов на базе H.245)*

Защищенная связь в реальном масштабе времени по незащищенным сетям обычно включает *аутентификацию* и *засекречивание* (шифрование данных). В данной Рекомендации описываются усовершенствования структуры интерактивной конференцсвязи посредством включения таких услуг безопасности, как аутентификация оконечного пункта и засекречивание информации, описываются рекомендуемые для использования инфраструктура безопасности и конкретные методы засекречивания. Предлагаемая схема может применяться как в простых конференциях точка-точка, так и в многоточечных конференциях для любых терминалов, в которых используется протокол управления H.245. Эта версия (11/00) включает криптографию эллиптической кривой, профили защиты (простая на базе пароля и усовершенствованная цифровая подпись), защитные меры противодействия (защита носителей информации от спама), усовершенствованный алгоритм шифрования (AES), служба узла базы данных, идентификаторы объектов (см. Руководство разработчика H.323). Вопрос G/16

Приложение F H.235 *Профиль гибридной защиты*

В данном Приложении описывается эффективный и масштабируемый, реализованный на базе PKI профиль гибридной защиты, использующий цифровые подписи из Приложения E к H.235 и базовый профиль защиты из Приложения D к H.235. Это приложение предлагается в качестве опции. В объектах защиты H.323 (терминалы, пропускные пункты, шлюзы, MCU и т. д.) может быть реализован профиль гибридной защиты для усиленной безопасности или в случае необходимости. Термин "гибридный" означает в данном тексте, что процедуры обеспечения безопасности из профиля подписи в Приложении E к H.235 применяются в облегченной форме; здесь цифровые подписи соответствуют процедурам RSA. Однако цифровые подписи применяются только там, где это абсолютно необходимо, иначе применяются высокоэффективные симметричные методы защиты из базового профиля безопасности Приложения D к H.235. Профиль гибридной защиты может применяться в масштабируемой "глобальной" IP-телефонии. В этом профиле защиты устранены ограничения простого

базового профиля защиты Приложения D к H.235, возникающие в случае его строго применения. Кроме того, в этом профиле защиты устранены некоторые недостатки Приложения E к H.235, такие как потребность в более широкой полосе и улучшенных характеристиках, необходимых для обработки в случае строгого его применения. Например, профиль гибридной защиты не зависит от (статического) администрирования совместно используемых секретных ключей на этапах передачи в различных доменах. Таким образом, пользователи могут значительно проще выбирать своего поставщика VoIP. Следовательно, этот профиль защиты поддерживает также некоторый вид мобильности пользователя. В нем несимметричное шифрование с подписями и сертификатами используется только там, где это необходимо, а в других случаях используются более простые и эффективные симметричные методы. Он обеспечивает туннелирование сообщений H.245 для обеспечения их целостности, а также некоторые меры для фиксации авторства сообщений. Профиль гибридной защиты предусматривает модель с GK-маршрутизацией и базируется на методах туннелирования H.245; поддержка моделей без GK-маршрутизации подлежит дальнейшему изучению. Вопрос G/16

H.323 *Мультимедийные системы связи на основе пакетов (Приложение J: Защита для простых типов оконечных пунктов)*

В данной Рекомендации описываются терминалы и другие объекты, обеспечивающие службы передачи аудио-, видеосигналов, данных и/или мультимедийной связи в реальном масштабе времени по пакетным сетям (PBN), которые могут не обеспечивать гарантированное качество обслуживания. Обеспечение передачи аудиосигналов является обязательным, видеосигналов и данных – необязательным; однако в случае обеспечения этих услуг обязательной является возможность использовать общий режим работы, так чтобы терминалы, поддерживающие этот тип информации, могли бы взаимодействовать между собой. Пакетная сеть может включать локальные сети, сети предприятий, городские сети, внешние и внутренние сети (включая Интернет), соединения точка-точка, одиночный сегмент сети или структуру взаимодействующих сетей, содержащую много сегментов со сложной топологией; отдельные элементы могут использовать конфигурации точка-точка, многопунктовые или широковещательные конфигурации. Такие объекты могут взаимодействовать с терминалами в Ш-ЦСИС, У-ЦСИС, в локальных сетях с гарантированным качеством обслуживания, в коммутируемой телефонной сети общего пользования (GSTN) и/или в беспроводных сетях, а объекты могут быть встроены в персональные компьютеры или реализованы в виде автономных устройств, таких как видеотелефоны.
Вопрос G/16

H.530 *Защита для H.510 в мультимедийных мобильных связных средах H.323*

Целью данной Рекомендация является определение процедур обеспечения безопасности в мобильных связных средах H.323, таких как рассмотренные в H.510, где описывается мобильность для мультимедийных систем и служб H.323. Данная Рекомендация содержит подробные сведения о процедурах защиты для H.510. На настоящий момент возможности сигнализации H.235 в версиях 1 и 2 разработаны для обеспечения безопасности в связных средах H.323, являющихся в большинстве случаев статическими. Эти связные среды и мультимедийные системы могут обладать некоторой ограниченной мобильностью внутри зон пропускных пунктов; H.323 в общем и H.235 в частности обеспечивают лишь весьма незначительную поддержку защиты роуминга мобильных пользователей и терминалов в различных доменах с большим числом объектов, характеризующихся мобильностью, например в распределенной связной среде. Сценарии мобильности H.323, описанные в H.510, в части мобильности терминала представляют также новую ситуацию с гибким и динамическим характером в отношении защиты. Роуминг пользователей и мобильных терминалов H.323 должен аутентифицироваться чужим визитным доменом. Аналогично, мобильный пользователь желал бы получать подтверждение правильности идентификации визитного домена. В дополнение к этому было бы также полезно получать подтверждение об идентификации терминалов, дополняющее аутентификацию пользователя. Таким образом, эти требования включают взаимную аутентификацию пользователя и визитного домена и также, при желании, идентификацию терминала. Так как обычно мобильный пользователь известен только в домене приписки, абонентом которого он является и в котором ему назначен пароль, визитный домен первоначально “не знает” мобильного пользователя. Поэтому визитный домен не имеет с мобильным пользователем и мобильным терминалом никакой установленной взаимосвязи для обеспечения безопасности. С тем чтобы дать визитному домену возможность гарантирования аутентификации и авторизации мобильного пользователя и мобильного терминала, визитный домен должен осуществить с доменом приписки через промежуточную сеть и служебные объекты определенные меры безопасности, такие как проверки авторизации или управление ключами. Это также требует безопасности связи и управления ключами между визитным доменом и доменом приписки. Несмотря на то что в принципе мобильные связные среды H.323 более открыты, чем закрытые сети H.323, естественно, также существует необходимость соответствующей безопасности при выполнении задач управления ключами. Также верно и то, что связь внутри доменов мобильности и через домены мобильности требует защиты от попыток злонамеренного использования. Вопрос G/16

J.93 *Требования к условному доступу при вторичном предоставлении цифрового телевидения или кабельных телевизионных систем*

В данной Рекомендации определены требования к засекречиванию данных и доступу для защиты сигналов цифрового телевидения MPEG, проходящих по сетям кабельного телевидения между кабельным головным узлом и самым удаленным абонентом. Используемые в этом процессе конкретные криптографические алгоритмы отсутствуют в J.93, так как они определяются в регионе и/или промышленностью. SG 9

J.96 Amd 1 *Технический метод обеспечения секретности при дальней международной передаче телевидения MPEG-2 в соответствии с Рекомендацией J.89*

Данная Рекомендация содержит общий стандарт на систему условного доступа при дальней международной передаче цифрового телевидения в соответствии с профессиональным профилем MPEG-2 (4:2:2). Описывается базовая совместимая система скремблирования (BISS), в основу которой положена спецификация DVB-CSA, использующая постоянные открытые ключи, называемые “словами сеанса связи”. Другой обратносовместимый режим вводит дополнительный механизм для вставки “шифрованных слов сеанса связи” при одновременном сохранении совместимости. Вопрос 6/9

J.170 *Спецификация безопасности IPCablecom (J.sec)*

В данной Рекомендации определены архитектура безопасности, протоколы, алгоритмы, соответствующие функциональные требования и некоторые технологические требования, которые могут обеспечить безопасность системы для сети IPCablecom. Для каждого интерфейса элемента сети, как определено в Рекомендации, должны предоставляться услуги аутентификации, управления доступом, обеспечения целостности сообщения и переносимого содержимого, обеспечения конфиденциальности и фиксации авторства. ИК 9

M.3010 *Принципы построения сети управления электросвязью*

Данная Рекомендация содержит концепции архитектур сети управления электросвязью (TMN) (функциональная архитектура TMN, информационная архитектура TMN и физическая архитектура TMN) и ее основных элементов. В данной Рекомендации описывается взаимосвязь трех архитектур и сформулированы основы для определения требований к спецификации физических архитектур из функциональных и информационных архитектур TMN. Проблеме безопасности посвящены только некоторые части данной Рекомендации. Приведена логическая эталонная модель для деления функций управления на части – логическая многоуровневая архитектура (LLA). В данной Рекомендации определен также порядок демонстрации соответствия и согласованности TMN для целей достижения взаимодействия сетей. Требования к TMN включают способность обеспечения защищенного доступа к управляющей информации авторизованным пользователям управляющей информации. TMN содержит функциональные блоки, для которых с использованием методов обеспечения безопасности реализованы функциональные возможности защиты связной среды с целью обеспечения безопасности информации, проходящей через интерфейсы и хранящейся в управляющих приложениях. Принципы и механизмы обеспечения безопасности связаны также с управлением правами доступа пользователей TMN к информации, относящейся к приложениям TMN. Вопрос 7/4

M.3016 *Обзор безопасности TMN (M.3sec)*

Данная Рекомендация содержит обзор и основные положения, определяющие угрозы безопасности TMN, и в ней показаны возможности использования доступных услуг безопасности в рамках функциональной архитектуры TMN, описанной в Рекомендации M.3010. Данная Рекомендация является общей по характеру и не определяет и не указывает требования к конкретному интерфейсу TMN. Вопрос 7/4

M.3210.1 *Управление безопасностью для категории IMT2000 – Требования*

Данная Рекомендация является одной из серии Рекомендаций, посвященных службе управления TMN, которые содержат описание услуг управления, целей и сущности для аспектов управления сетями IMT2000. Данная Рекомендация базируется на группах функций, определенных в Рекомендации МСЭ-Т M.3400, путем определения новых групп функций, функций и параметров и добавления дополнительных семантических определений и ограничений. В данной Рекомендации описываются подгруппа служб по управлению безопасностью для выработки требований и проведения анализа управления безопасностью и профиль для обнаружения мошенничества в сети мобильной связи IMT2000. Основное внимание уделено интерфейсу X между двумя поставщиками услуг и службам управления, требующимся между

ними для обнаружения и предотвращения мошенничества с помощью системы сбора информации о мошенничестве (FIGS), как средства контроля определенной группы действий абонентов, с тем чтобы ограничить их финансовую уязвимость, следствием которой является создание неоплаченных счетов на крупные суммы, начисляемые во время их перемещений. Вопрос 14/4

M.3320 *Требования к интерфейсу X*

Данная Рекомендация является частью серии Рекомендаций, посвященных передаче информации для управления сетями и службами электросвязи, и только некоторые ее части посвящены аспектам безопасности. Целью данной Рекомендации является определение структуры всех функциональных требований, требований к услугам и требований сетевого уровня к обмену информацией TMN между Администрациями. Данная Рекомендация содержит также общие принципы использования интерфейса X TMN для обмена информацией между Администрациями, признанными эксплуатационными организациями, другими операторами сетей, поставщиками услуг, клиентами и другими объектами. Вопрос 9/4

M.3400 *Функции управления TMN*

Данная Рекомендация входит в серию Рекомендаций, которые посвящены сети управления электросвязью (TMN) и содержит спецификации функций управления TMN и групп функций управления TMN. Содержание Рекомендации разработано в поддержку “информационной базы задач B” (Роли, ресурсы и функции), связанной с задачей 2 (Описать контекст управления TMN) в методологии спецификации интерфейса TMN, изложенной в Рекомендации МСЭ-Т M.3020. При проведении анализа контекста управления TMN желательно учитывать максимальное использование групп функций управления TMN, имеющихся в этой Рекомендации. Вопрос 7/4

Q.293 *Периоды времени, через которые следует активизировать меры безопасности*

Это извлечение из Синей книги, содержащее только разделы с 8.5 (Периоды времени, через которые следует активизировать меры безопасности) по 8.9 (Метод разделения нагрузки) Q.293. ИК 4

Q.813 *Прикладной служебный элемент преобразования мер безопасности для сервисного элемента удаленной обработки (STASE-ROSE)*

Данная Рекомендация содержит спецификации для поддержки преобразований мер безопасности, таких как шифрование, хэш-функция, простановка печати и подписи, предназначенные для всех протокольных блоков данных (PDU) сервисного элемента удаленной обработки (ROSE). Преобразования мер безопасности используются для организации различных услуг безопасности, таких как аутентификация, обеспечение конфиденциальности, обеспечение целостности и фиксация авторства. В данной Рекомендации описывается подход к обеспечению преобразований мер безопасности, который реализован на прикладном уровне и не требует реализации специальных функциональных возможностей для защиты ни на одном из нижних уровней стека взаимосвязи открытых систем (OSI). Вопрос 18/4

Q.815 *Спецификация модуля безопасности для защиты целого сообщения*

В данной Рекомендации определен необязательный модуль безопасности для использования с Рекомендацией Q.814 – “агент интерактивного обмена электронными данными”, который обеспечивает услуги безопасности для всех данных (PDU). В частности, модуль безопасности обеспечивает фиксацию авторства в точках передачи и приема, а также целостность всего сообщения. Вопрос 18/4

Q.817 *TMN PKI − Цифровые сертификаты и профили списков аннулирования сертификатов*

В данной Рекомендации дано разъяснение порядка использования в TMN цифровых сертификатов и списков аннулирования сертификатов и сформулированы требования к использованию расширений сертификатов и списков аннулирования сертификатов. Данная Рекомендация предназначена для обеспечения взаимодействия между элементами TMN, которые используют инфраструктуру с открытым ключом (PKI) для поддержки функций, относящихся к безопасности. Целью данной Рекомендации является создание обеспечивающего взаимодействие, масштабируемого механизма для распространения ключа и управления им в TMN, на всех интерфейсах, а также при поддержке на интерфейсе X услуги

фиксации авторства. Он применяется на всех интерфейсах и приложениях TMN и не зависит от того, какой стек протоколов связи или какой протокол управления сетью используется. Устройства PKI могут применяться для широкого спектра функций безопасности, таких как аутентификация, обеспечение целостности, фиксация авторства и обмен ключами (M.3016). Однако в данной Рекомендации не определено, как такие функции должны быть реализованы – с PKI или без PKI. Вопрос 18/4

Q.1531 *Требования к защите UPT для сервисного набора 1*

В данной Рекомендации определены требования к безопасности UPT как для связи пользователь-сеть, так и для межсетевой связи, применимые для сервисного набора 1 UPT, как это определено в Рекомендации F.851. Данная Рекомендация охватывает все аспекты безопасности для UPT с использованием доступов DTMF и доступов пользователей, реализованных на базе внеполосной сигнализации DSS 1. ИК 15

Q.1741.1 *Ссылки IMT-2000 на базовую сеть UMTS с сетью доступа UTRAN на основе версии GSM 1999 года*

Данная Рекомендация содержит ссылки на следующие спецификации безопасности 3GPP:

TS 21.133: Угрозы безопасности и требования к защите

TS 22.100: Фаза 1 UMTS

TS 22.101: Принципы службы UMTS

TS 33.102: Архитектура безопасности

TS 33.103: Руководящие принципы по интеграции безопасности

TS 33.105: Требования к криптографическому алгоритму

TS 33.106: Требования к санкционированному перехвату

TS 33.107: Архитектура и функции санкционированного перехвата

TS 33.120: Цели и принципы безопасности СИК

Q.1741.2 *Ссылки IMT-2000 на базовую сеть UMTS с сетью доступа UTRAN на базе версии 4 GSM*

Данная Рекомендация содержит ссылки на следующие спецификации безопасности 3GPP:

TS 21.133: Безопасность 3G; угрозы безопасности и требования к защите

TS 22.048: Механизмы обеспечения безопасности для прикладных инструментальных средств (U)SIM; этап 1

TS 22.101: Аспекты службы; принципы службы

TS 33.102: Безопасность 3G; архитектура безопасности

TS 33.103: Безопасность 3G; руководства по интеграции

TS 33.105: Требования к криптографическому алгоритму

TS 33.106: Требования к санкционированному перехвату

TS 33.107: Безопасность 3G; архитектура и функции санкционированного перехвата

TS 33.120: Цели и принципы безопасности

TS 33.200: Безопасность сетевого домена – MAP

TS 35.205, .206, .207 и .208: Безопасность 3G; спецификация комплекта алгоритмов MILENAGE: Пример комплекта алгоритмов для функций аутентификации и генерации ключа 3GPP f1, f1*, f2, f3, f4, f5 и f5*; (.205: Общий; .206: Спецификация алгоритма; .207: Тестовые данные разработчика; .208: Тестовые данные соответствия проекту) СИК

Q.1741.3 *Ссылки IMT-2000 на базовую сеть UMTS с сетью доступа UTRAN на базе версии 5 GSM*

Данная Рекомендация содержит ссылки на следующие спецификации безопасности 3GPP:

TS 22.101: Аспекты службы; принципы службы

TS 33.102: Безопасность 3G; архитектура безопасности

TS 33.106: Требования к санкционированному перехвату

TS 33.107: Безопасность 3G; архитектура и функции санкционированного перехвата

TS 33.108: Безопасность 3G; интерфейс передачи разговора для санкционированного перехвата (LI)

TS 33.200: Безопасность сетевого домена – MAP

TS 33.203: Безопасность 3G; безопасность доступа для служб, базирующихся на протоколе IP

TS 33.210: Безопасность; безопасность сетевого домена (NDS); безопасность уровня IP-сети

TS 35.205, .206, .207, .208 и .909: Безопасность 3G; спецификация комплекта алгоритмов MILENAGE: пример комплекта алгоритмов для функций аутентификации и генерации ключа 3GPP f1, f1*, f2, f3, f4, f5 и f5*; (.205: Общий; .206: Спецификация алгоритма; .207: Тестовые данные разработчика; .208: Тестовые данные проверки соответствия проекту; .909: Резюме и результаты проектирования и оценки) СИК

Q.1742.1 *Ссылки IMT-2000 на базовую сеть с сетью доступа cdma2000 на основе ANSI-41*

В данной Рекомендации произведено присоединение опубликованных стандартов базовой сети организаций по разработке стандартов (ОРС) к стандартам спецификации 3GPP2, которая была утверждена 17 июля 2001 года для члена семейства IMT-2000 "Базовая сеть с сетью доступа cdma2000 на основе ANSI-41". Спецификация 3GPP2, которая была утверждена в июле 2002 года, будет присоединена к опубликованным стандартам базовой сети в будущей Рекомендации МСЭ-Т Q.1742.2. Присоединение радиоинтерфейса и сети радиодоступа, а также стандартов от ОРС для этого члена семейства IMT-2000 выполнено в Рекомендации МСЭ-R M.1457. Присоединения для других членов семейства IMT-2000 выполнены в Рекомендациях МСЭ-Т серии Q.174x. В данной Рекомендации для этого члена семейства IMT-2000 произведено объединение и присоединение соответствующих стандартов на базовую сеть ряда организаций по разработке стандартов в общую Рекомендацию. СИК

Q.1742.2 *Ссылки IMT-2000 (утверждены 11 июля 2002 года) на базовую сеть с сетью доступа cdma2000 на основе ANSI-41*

В данной Рекомендации произведено присоединение опубликованных стандартов базовой сети региональных организаций по разработке стандартов (ОРС) к стандартам спецификации 3GPP2, которая была утверждена 11 июля 2002 года для члена семейства IMT-2000 "Базовая сеть с сетью доступа cdma2000 на основе ANSI-41". Спецификация 3GPP2, которая была утверждена 17 июля 2001 года, была присоединена в Рекомендации МСЭ-Т Q.1742.1 к опубликованным стандартам базовой сети региональных организаций по разработке стандартов. Спецификация 3GPP2, которая была утверждена в июле 2003 года, будет присоединена к опубликованным стандартам базовой сети в будущей Рекомендации МСЭ-Т Q.1742.3. Присоединение радиоинтерфейса и сети радиодоступа, а также стандартов от ОРС для этого члена семейства IMT-2000 выполнено в Рекомендации МСЭ-R M.1457. Присоединения для других членов семейства IMT-2000 выполнены в Рекомендациях МСЭ-Т серии Q.174x. В данной Рекомендации произведено объединение и присоединение региональных стандартов на базовую сеть этого члена семейства IMT-2000 в общую Рекомендацию. СИК

Q.1742.3 *Технические спецификации, на которые сделаны ссылки в Q.1742.3, с межсистемными спецификациями аспектов безопасности:*

N.S0003-0 Модуль идентификации пользователя (версия 1.0; апрель 2001 года)

N.S0005-0 Межсистемные операции сотовой радиосвязи (версия 1.0; даты нет)

N.S0009-0 IMSI (версия 1.0; даты нет)

N.S0010-0 Расширенные функции в широкополосных системах с шумоподобными сигналами (версия 1.0; даты нет)

N.S0011-0 OTASP и OTAPA (версия 1.0; даты нет)

N.S0014-0 Усовершенствования аутентификации (версия 1.0; даты нет)

N.S0018 Предварительная оплата TIA/EIA-41-D (версия 1.0.0; 14 июля 2000 года)

N.S0028 Межсетевое взаимодействие GSM MAP и ANSI-41 MAP Rev. B Версия: 0 (версия 1.0.0; апрель 2002 года)

Спецификации пакетных данных:

P.S0001-A Стандарт беспроводной IPсети (версия 3.0.0; 16 июля 2001 года)

P.S0001-B Стандарт беспроводной IP-сети (версия 1.0.0; 25 октября 2002 года)

Спецификации сервисных и системных аспектов:

S.R0005-B Эталонная модель сети для систем с шумоподобными сигналами cdma2000, Пересмотр: B (версия 1.0; 16 апреля 2001 года)

S.R0006 Описание функций беспроводной связи, Пересмотр: 0 (версия 1.0.0; 13 декабря 1999 года)

S.R0009-0 Модуль идентификации пользователя (версия 1.0; этап 1), Пересмотр: 0 (13 декабря 1999 года)

S.R0018 Предварительная оплата (версия 1.0.0; этап 1), Пересмотр: 0 (13 декабря 1999 года)

S.R0019 Система услуг, привязанных к местонахождению (версия 1.0.0; LBSS), Описание этапа 1 (22 сентября 2000 года)

S.R0032 Усовершенствованная аутентификация абонента (версия 1.0; ESA) и усовершенствованная конфиденциальность абонента (ESP) (6 декабря 2000 года)

S.R0037-0 Модель архитектуры IP-сети для систем с шумоподобными сигналами cdma2000 (версия 2.0; 14 мая 2002 года)

S.R0048 Идентификатор оборудования мобильной связи 3G (версия 1.0; MEID) (10 мая 2001 года)

S.S0053 Общие криптографические алгоритмы (версия 1.0; 21 января 2002 года)

S.S0054 Спецификация интерфейса для общих криптографических алгоритмов (версия 1.0; 21 января 2002 года)

S.S0055 Усовершенствованные криптографические алгоритмы (версия 1.0; 21 января 2002 года)

S.R0058 Требования к системе домена IP-мультимедиа (версия 1.0; 17 апреля 2003 года)

S.R0059 Унаследованный домен MS – Требования к системе этапа 1 (версия 1.0; 16 мая 2002 года)

S.R0066-0 Требования этапа 1 к службам определения местоположения на базе IP (версия 1.0; 17 апрель 2003 года)

S.R0071 Требования к инспектированию пакетов данных унаследованной системы, требования этапа 1 (версия 1.0; 18 апреля 2002 года)

S.R0072 Все требования к инспектированию IP-пакетов данных, требования этапа 1 (версия 1.0; 18 апрель 2002 года)

S.R0073 Управление конфигурацией телефонного аппарата с эфирным доступом в Интернет (версия 1.0; IOTA) этап 1 (11 июля 2002 года)

S.S0078-0 Общие алгоритмы защиты (версия 1.0; 12 декабря 2002 года) СИК

T.30 *Процедуры для факсимильной передачи документов по телефонным сетям общего пользования*

Приложение G содержит процедуры защищенной факсимильной передачи документа G3 с использованием систем HKM и HFX. Приложение H содержит меры безопасности при факсимильной передаче G3 на базе алгоритма RSA. ИК 16

T.36 *Средства защиты для использования с факсимильными терминалами группы 3*

В данной Рекомендации приведены два независимых технических решения, которые могут использоваться для защиты факсимильной передачи. Эти технические решения основываются на алгоритмах HKM/HFX40 и алгоритме RSA. ИК 16

T.123 изм., Приложение B *Расширенные транспортные соединения*

В данном Приложении к измененной Рекомендации T.123 описывается протокол согласования соединения (CNP), обеспечивающий согласование средств защиты. Используемый механизм защиты включает различные средства обеспечения безопасности сети и транспортировки типа узел-узел и содержит такие средства, как TLS/SSL, IPSEC с/без IKE или с/без ручного управления ключами, X.274/ISO TLSP и GSS-API. Вопрос 1/16

T.503 *Модель применения документа для обмена факсимильными документами Группы 4*

В данной Рекомендации определена модель применения документа, которая может использоваться любой телематической службой. Ее целью является задание формата обмена, пригодного для обмена факсимильными документами Группы 4, которые содержат только растровую графику. Обмен документами производится в форматированном виде, который позволяет получателю вывести документ на экран или на печать, как это предусмотрено отправителем. ИК 16

T.563 *Характеристики оконечного оборудования аппаратуры факсимильной связи Группы 4*

В данной Рекомендации определены общие виды аппаратуры факсимильной связи Группы 4 и интерфейс с физической сетью. ИК 16

T.611 *Программируемый связной интерфейс (**PCI**) **APPLI/COM** для служб факсимильной связи Группы 3, факсимильной связи Группы 4, телетекса, телекса, электронной почты (E-mail) и передачи файлов*

В данной Рекомендации определен программируемый связной интерфейс, называемый "**APPLI/COM**", который обеспечивает универсальный доступ к различным службам электросвязи, таким как телефакс группы 3 или другим телематическим службам. В данной Рекомендации описывается структура, содержимое сообщений и способ обмена сообщениями между двумя устройствами (то есть LA, местное приложение и CA, приложение связи). *Любому соединению предшествует процесс вхождения в связь (login process), и оно завершается процессом прекращения связи (logout process), оба процесса способствуют реализации схем безопасности, что особенно важно в многопользовательских системах. Они также предоставляют средства реализации механизмов защиты между местным приложением (LA) и приложением связи (CA).* В данной Рекомендации сформирован интерфейс прикладного программирования (**API**) высокого уровня, который защищает характерные свойства связи, но обеспечивает эффективное управление и контроль всех операций связи для разработчиков приложений. ИК 8

X.217 *Информационная технология – Взаимосвязь открытых систем – Определение службы для сервисного элемента управления ассоциацией*

В данной Рекомендации определены службы сервисного элемента управления ассоциацией (**ACSE**) для управления связью приложений в среде взаимосвязи открытых систем. ACSE поддерживает модели связи с установлением и без установления соединения. В ACSE определены три функциональных узла. Обязательный функциональный узел "ядро" используется для создания и отмены ассоциаций приложений. ACSE содержит два необязательных функциональных узла, один из которых является необязательным функциональным узлом "аутентификация", без добавления новых служб обеспечивающим дополнительные средства для обмена информацией в целях поддержки аутентификации во время создания ассоциации. Средства аутентификации ACSE могут использоваться для поддержки ограниченного класса методов аутентификации.

Дополнение 1: Поддержка механизмов аутентификации для режима без установления соединения
Вопрос 11/17

X.227 *Информационная технология – Взаимосвязь открытых систем – Протокол с установлением соединения для сервисного элемента управления ассоциацией: Спецификация протокола*

Данная спецификация протокола определяет процедуры, которые могут использоваться в случаях связи между системами, которые намерены взаимодействовать в среде взаимосвязи открытых систем в режиме с установлением соединения, то есть протокол режима с установлением соединения для сервисного элемента приложения для управления ассоциацией приложений (**ACSE**). Спецификация протокола содержит функциональный узел "ядро", который используется для создания и аннулирования ассоциаций приложений. Функциональный узел "аутентификация" без добавления новых служб обеспечивает дополнительные средства для обмена информацией в целях поддержки аутентификации во время создания ассоциации. Средства аутентификации ACSE могут использоваться для поддержки ограниченного класса методов аутентификации. Функциональный узел "согласование контекста приложения" обеспечивает дополнительные средства для выбора контекста приложения во время создания ассоциации. Данная спецификация протокола включает приложение, в котором описывается протокольная машина, называемая "механизм протокола управления ассоциацией" (ACPM), представленный в виде таблицы состояний. Данный протокол включает приложение, в котором

описывается простой механизм аутентификации, использующий пароль с заголовком AE и предназначенный для общего пользования, а также включает пример спецификации механизма аутентификации. Этому механизму аутентификации присвоено следующее имя (из типа данных OBJECT IDENTIFIER ASN.1):

{joint-iso-itu-t(2) association-control(2) authentication-mechanism(3) password-1(1)}.

Паролем для этого механизма аутентификации является значение аутентификации. Типом данных значения аутентификации должен быть "GraphicString" (ГрафическаяСтрока). Вопрос 11/17

X.237 *Информационная технология – Взаимосвязь открытых систем – Протокол без установления соединения для сервисного элемента управления ассоциацией: Спецификация протокола*

Дополнение 1 к данной Рекомендации содержит маркер расширяемости ASN.1 в модуле, описывающем протокол. Он также расширяет спецификацию протокола без установления соединения ACSE для обеспечения поддержки транспортировки параметров аутентификации в A-UNIT-DATA APDU.
Вопрос 11/17

X.257 *Информационная технология – Взаимосвязь открытых систем – Протокол без установления соединения для сервисного элемента управления ассоциацией: Форма "свидетельства о соответствии реализации протоколу" (PICS)*

Данная Рекомендация содержит форму "свидетельства о соответствии реализации протоколу" (PICS) для протокола без установления соединения OSI для сервисного элемента управления ассоциацией (ACSE), который определен в Рекомендации X.237. Форма PICS представляет в табличной форме обязательные и необязательные элементы протокола без установления соединения ACSE. Форма PICS используется для указания возможностей и вариантов выбора конкретной реализации протокола без установления соединения ACSE. Вопрос 11/17

X.272 *Сжатие данных и засекречивание в сетях с ретрансляцией кадров*

В данной Рекомендации определены услуги сжатия данных и засекречивания для сетей с ретрансляцией кадров (Frame Relay), включая согласование и инкапсуляцию сжатия данных, сжатие защищенных данных и шифрование "поверх" ретрансляции кадров. Наличие в сети услуги сжатия данных увеличивает эффективную пропускную способность сети. Спрос на передачу уязвимых данных в сетях общего пользования требует средств для обеспечения засекречивания данных. Для достижения оптимальных коэффициентов сжатия данных целесообразно производить сжатие данных до их шифрования. Поэтому желательно в службе сжатия данных также иметь средства для согласования протоколов шифрования данных. Так как задача сжатия и последующего шифрования данных требует больших объемов вычислений, эффективность обработки достигается посредством одновременного выполнения сжатия и шифрования данных (сжатие защищенных данных). Протоколы сжатия данных базируются на протоколе управления каналом PPP (IETF RFC 1661) и на протоколе управления шифрованием PPP (IETF RFC 1968 и 1969). Данная Рекомендация применяется для кадров "ненумерованной информации" (UI), инкапсулированных с использованием Приложения E к Q.933. Это Приложение определяет сжатие данных и засекречивание как в постоянных (PVC), так и в коммутируемых (SVC) виртуальных соединениях. Вопрос 10/17

X.273 *Информационная технология – Взаимосвязь открытых систем – Протокол безопасности сетевого уровня*

В данной Рекомендации задан протокол, предназначенный для поддержки услуг обеспечения целостности, конфиденциальности, аутентификации и управления доступом, определенных в модели безопасности взаимосвязи открытых систем (OSI) как применимые в протоколах сетевого уровня с установлением и без установления соединения. Протокол поддерживает эти услуги посредством использования криптографических механизмов, меток грифа секретности и назначаемых атрибутов безопасности, таких как криптографические ключи. Вопрос 11/17

X.274 *Информационная технология – Электросвязь и передача информации между системами – Протокол безопасности транспортного уровня*

В данной Рекомендации задан протокол, который может поддерживать услуги обеспечения целостности, обеспечения конфиденциальности, аутентификации и управления доступом, определенные в модели безопасности взаимосвязи открытых систем (OSI) как относящиеся к транспортному уровню. Протокол поддерживает эти услуги посредством использования криптографических механизмов, меток грифа секретности и назначаемых атрибутов безопасности, таких как криптографические ключи.

Вопрос 11/17

X.400/F.400 *Обзор системы и службы обработки сообщений*

В данной Рекомендации определены сервисные элементы системы обработки сообщений (MHS) для определенных как относящиеся к прикладному уровню услуг **безопасности:** обеспечение конфиденциальности, обеспечение целостности, аутентификация, фиксация авторства и управление доступом для направлений "агент пользователя – агент пользователя" (UA)-to-UA), "агент передачи сообщений – агент передачи сообщений (MTA)-to-MTA), "агент пользователя – агент передачи сообщений" (UA-to-MTA) и "агент пользователя – хранилище сообщений" (UA-to-Message Store (MS)). (См. F.400) Вопрос 11/17

X.402 *Информационная технология – Системы обработки сообщений (MHS): Общая архитектура*

В данной Рекомендации содержатся спецификации процедур обеспечения безопасности и идентификаторов объектов, предназначенных для использования в протоколах системы обработки сообщений (MHS) при реализации услуг обеспечения конфиденциальности, обеспечения целостности, аутентификации, фиксации авторства и управления доступом, которые определены как относящиеся к прикладному уровню. Вопрос 11/17

X.411 *Информационная технология – Системы обработки сообщений (MHS): Система пересылки сообщений: Определение и процедуры абстрактной услуги*

В данной Рекомендации содержатся спецификации механизмов и процедур, поддерживающих услуги обеспечения конфиденциальности, обеспечения целостности, аутентификации и фиксации авторства, которые определены как относящиеся к прикладному уровню. Протокол поддерживает эти услуги посредством использования криптографических механизмов, меток грифа секретности и цифровых подписей, как это определено в Рекомендации X.509. Хотя в данной Рекомендации определен протокол, использующий несимметричные криптографические методы, поддерживаются также симметричные криптографические методы. Вопрос 11/17

X.413 *Информационная технология – Системы обработки сообщений (MHS): Хранилище сообщений: Определение абстрактной услуги*

В данной Рекомендации содержатся спецификации механизмов, протокола и процедур, поддерживающих услуги обеспечения конфиденциальности, обеспечения целостности, управления доступом, аутентификации и фиксации авторства, которые определены как относящиеся к прикладному уровню. Протокол поддерживает эти услуги как непосредственный пользователь хранилища сообщений.

Вопрос 11/17

X.419 *Информационная технология – Системы обработки сообщений (MHS): Спецификации протокола*

В данной Рекомендации содержатся спецификации процедур и контекста приложений для определения защищенного доступа для объектов системы обработки сообщений (MHS) и удаленных пользователей путем обеспечения услуг аутентификации и управления доступом, которые определены как относящиеся к прикладному уровню. Вопрос 11/17

X.420 *Информационная технология – Системы обработки сообщений (MHS) – Система межабонентского обмена сообщениями*

В данной Рекомендации содержатся спецификации механизмов, протокола и процедур для обмена объектами между пользователями межабонентского обмена сообщениями или агентами пользователя от имени их непосредственного пользователя, который определен как относящийся к прикладному уровню. Поддерживаемые услуги безопасности: обеспечение целостности, обеспечение конфиденциальности, аутентификация и управление доступом, определенные как относящиеся к прикладному уровню.

Вопрос 11/17

X.435 *Информационная технология – Системы обработки сообщений (MHS): Система передачи сообщений для электронного обмена данными*

В данной Рекомендации содержатся спецификации механизмов, протокола и процедур для обмена объектами между агентами пользователя электронного обмена данными (EDI) от имени его непосредственного пользователя. Поддерживаемые услуги безопасности: обеспечение целостности, обеспечение конфиденциальности, аутентификация и управление доступом, определенные как относящиеся к прикладному уровню. Вопрос 11/17

X.440 *Информационная технология – Системы обработки сообщений: Система голосовых сообщений*

В данной Рекомендации определены механизмы, протокол и процедуры для обмена объектами между агентами пользователя голосовыми сообщениями от имени его непосредственного пользователя. Поддерживаемые услуги безопасности: обеспечение целостности, обеспечение конфиденциальности, аутентификация и управление доступом, определенные как относящиеся к прикладному уровню.
Вопрос 11/17

X.500 *Информационная технология – Взаимосвязь открытых систем – Справочник: Обзор концепций, моделей и служб*

В данной Рекомендации определен Справочник и возможности его защиты. Вопрос 9/17

X.501 *Информационная технология – Взаимосвязь открытых систем – Справочник: Модели*

В данной Рекомендации определено использование Справочником своих структур открытого ключа и сертификата атрибутов согласно X.509. Вопрос 9/17

X.509 *Информационная технология – Взаимосвязь открытых систем – Справочник:*

---- *Структура аутентификации (издание 1993 года – второе издание/версия)*
---- *Структура аутентификации (издание 1997 года – третье издание/версия)*
---- *Структуры открытого ключа и сертификата атрибутов (издание 2000 года – четвертое издание/версия)*

В данной Рекомендации определена структура для сертификатов открытого ключа и для сертификатов атрибутов и определена структура для организации Справочником услуг аутентификации для своих пользователей. В ней описаны два уровня аутентификации: простая аутентификация, использующая пароль для подтверждения предъявленной идентификационной информации, и усиленная аутентификация, включающая мандаты, которые формируются с использованием криптографических методов. Хотя простая аутентификация обеспечивает некоторую ограниченную защиту от несанкционированного доступа, в качестве основы для предоставления защищенных услуг следует использовать только усиленную аутентификацию. Определенные здесь структуры могут использоваться для применения профиля к инфраструктурам открытого ключа (**PKI**), к инфраструктурам управления полномочиями (**PMI**). Структура сертификатов открытого ключа включает спецификацию объектов данных, используемых как для представления самих сертификатов данных, так и в качестве извещений об аннулировании выданных сертификатов, которые не должны больше действовать. Хотя структура определяет некоторые критические компоненты **PKI**, она не определяет **PKI** во всей полноте. Однако она создает основу, на которой формируются полные **PKI** и их спецификации. Структура для сертификатов атрибутов включает спецификацию объектов данных, используемых как для представления самих сертификатов, так и в качестве извещений об аннулировании выданных сертификатов, которые не должны больше действовать. Хотя структура определяет некоторые критические компоненты **PMI**, она не определяет **PMI** во всей полноте. Однако она создает основу, на которой формируются полные **PMI** и их спецификации. Также определены *информационные объекты* для фиксации объектов PKI и PMI в Справочнике и для сравнения представленных объектов с хранящимися объектами. Вопрос 9/17

X.519 *Информационная технология – Взаимосвязь открытых систем – Справочник: Спецификация протокола*

В данной Рекомендации определены процедуры и содержание приложений для определения защищенного доступа при связывании объектов Справочника. Вопрос 9/17

X.733 *Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция тревожного оповещения*

В данной Рекомендации определена функция управления системой, которая может использоваться прикладным процессом в централизованной или децентрализованной среде управления для взаимодействия в целях управления системами. В Рекомендации определена функция, состоящая из общих определений, услуги и функциональных узлов, которая находится на прикладном уровне эталонной модели взаимосвязи открытых систем. Тревожные оповещения, определенные этой функцией, содержат информацию, которая может потребоваться диспетчеру для выполнения действий по поддержанию рабочего состояния системы и обеспечения качества обслуживания. Вопрос 17/4

X.735 *Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция управления регистрацией*

В данной Рекомендации определена функция управления системой, которая может использоваться прикладным процессом в централизованной или децентрализованной среде управления для взаимодействия в целях управления системами. В данной Рекомендации определена функция управления регистрацией, состоящая из услуг и двух функциональных узлов. Эта функция находится на прикладном уровне. Вопрос 17/4

X.736 *Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция отчетов о неисправности системы защиты информации*

В данной Рекомендации | Международном стандарте определена функция отчетов о неисправности системы защиты информации. Функция отчетов о неисправности системы защиты информации является функцией управления системами, которая может использоваться прикладным процессом в централизованной или децентрализованной среде управления для обмена информацией в целях управления системами, как это определено Рекомендацией МККТТ X.700 | ISO/IEC 7498-4. Данная Рекомендация | Международный стандарт находится на прикладном уровне по Рекомендации МККТТ X.200 | ISO 7498 и определена согласно модели, приведенной в ISO/IEC 9545. Роль функций управления системами описана в Рекомендации МККТТ X.701 | ISO/IEC 10040. Отчеты о неисправности системы защиты информации, определенные этой функцией управления системами, содержат относящуюся к рабочему состоянию и качеству обслуживания информацию, которая связана с защитой. Вопрос 14/4

X.740 *Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция контрольного журнала защиты*

В данной Рекомендации | Международном стандарте определена функция контрольного журнала защиты. Функция контрольного журнала защиты является функцией управления системами, которая может использоваться прикладным процессом в централизованной или децентрализованной среде управления для обмена информацией и командами в целях управления системами, как это определено Рекомендацией МККТТ X.700 | ISO 7498-4. Данная Рекомендация | Международный стандарт находится на прикладном уровне по Рекомендации МККТТ X.200 | ISO 7498 и определена согласно модели, приведенной в ISO/IEC 9545. Роль функций управления системами описана в Рекомендации МККТТ X.701 | ISO/IEC 10040. Вопрос 14/4

X.741 *Информационная технология – Взаимосвязь открытых систем – Управление системой: Объекты и атрибуты для управления доступом*

В данной Рекомендации | Международном стандарте определена модель управления доступом и управляющая информация, необходимая для организации и администрирования управления доступом в соответствии с управлением системами OSI. Стратегии обеспечения безопасности, принятые для каких-либо конкретных случаев, не определены и оставлены для выбора при реализации. Эта спецификация является общим приложением и может использоваться для управления безопасностью приложений многих типов. Вопрос 14/4.

X.800 *Архитектура защиты при взаимосвязи открытых систем для применений МККТТ*

В данной Рекомендации определены общие, относящиеся к безопасности архитектурные элементы, которые могут быть применены надлежащим образом в случаях, когда требуется безопасность связи между открытыми системами. В рамках эталонной модели они задают руководящие принципы и ограничения в отношении усовершенствования существующих Рекомендаций или разработки новых Рекомендаций в контексте взаимосвязи открытых систем для обеспечения защищенной связи и реализуют тем самым согласованный подход к обеспечению безопасности при взаимосвязи открытых систем. Данная Рекомендация расширяет эталонную модель для охвата аспектов безопасности, которые являются общими архитектурными элементами протоколов связи, но не рассмотрены в эталонной модели. Данная Рекомендация содержит общее описание услуг безопасности и относящихся к ним механизмов, которые могут быть предоставлены эталонной моделью, и определяет позиции внутри эталонной модели, где могут предоставляться эти услуги и механизмы. Вопрос 10/17

X.802 *Информационная технология – Модель безопасности нижних уровней*

В данной Рекомендации описываются межуровневые аспекты пересмотра услуг безопасности на нижних уровнях эталонной модели взаимосвязи открытых систем (транспортный, сетевой, канальный, физический). Описаны архитектурные концепции, общие для этих уровней, база для взаимодействий, относящихся к межуровневой безопасности, и размещение протоколов безопасности на нижних уровнях.
Вопрос 10/17

X.803 *Информационная технология – Взаимосвязь открытых систем – Модель безопасности верхних уровней*

В данной Рекомендации описываются выбор, размещение и использование услуг и механизмов обеспечения безопасности на верхних уровнях (прикладной, представительный и сеансовый уровни) эталонной модели взаимосвязи открытых систем. Вопрос 10/17

X.805 *Архитектура безопасности для систем, обеспечивающих межконцевую связь*

В данной Рекомендации определены общие, относящиеся к безопасности архитектурные элементы, которые при надлежащем применении, в частности, в средах, образуемых оборудованием многих изготовителей, могут обеспечить надлежащую защиту сети от злонамеренных и неумышленных атак и функционирование этой сети при обеспечении таких технических характеристик, как высокая степень готовности, надлежащее время реакции, целостность, масштабируемость и функция точного выставления счетов. Вопрос 10/17

X.810 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Обзор*

В данной Рекомендации определена структура, внутри которой заданы услуги безопасности для открытых систем. Эта часть структур безопасности описывает организацию структуры безопасности, определяет концепции безопасности, требующиеся более чем в одной части структуры безопасности, и описывает взаимосвязь услуг и механизмов, определенных в других частях структуры. Указанная структура характеризует все аспекты аутентификации так, как они применяются в открытых системах, взаимосвязь аутентификации с другими функциями безопасности, такими как управление доступом, и требования к управлению для аутентификации. Вопрос 10/17

X.811 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура аутентификации*

В данной Рекомендации определена общая структура для организации аутентификации. Главной целью аутентификации является противодействие таким угрозам, как нелегальное проникновение и повторная передача перехваченного сообщения. Вопрос 10/17

X.812 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура управления доступом*

В данной Рекомендации определена общая структура для организации управления доступом. Главной целью управления доступом является противодействие таким угрозам, как несанкционированные операции с применением компьютера или системы связи; эти угрозы часто делят на классы, известные как несанкционированное использование, раскрытие содержания, модификация, разрушение и отказ в обслуживании. Вопрос 10/17

X.813 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура фиксации авторства*

В данной Рекомендации определена общая структура организации услуг фиксации авторства. Целью услуг фиксации авторства является сбор, обработка, обеспечение доступности и предоставление неопровержимых доказательств в отношении идентификации отправителей и получателей, участвующих в передаче данных. Вопрос 10/17

X.814 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура конфиденциальности*

В данной Рекомендации определена общая структура для организации услуг обеспечения конфиденциальности. Обеспечение конфиденциальности – это способ защиты информации от доступа к ней или ее раскрытия неуполномоченными лицами, устройствами или процессами. Вопрос 10/17

X.815 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура целостности*

В данной Рекомендации определена общая структура для организации услуг обеспечения целостности информации. Обеспечение целостности – это способ недопущения изменения или разрушения данных несанкционированным способом. Вопрос 10/17

X.816 *Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура аудита и аварийных извещений безопасности*

В данной Рекомендации описывается базовая модель для обработки аварийных извещений безопасности и проведения аудита безопасности для открытых систем. Аудит безопасности – это независимый обзор и проверка записей и функционирования системы. Услуга аудита безопасности дает возможность органу, проводящему аудит, задавать, выбирать и управлять событиями, которые должны быть зарегистрированы в процессе текущего аудита безопасности. Вопрос 10/17

X.830 *Информационная технология – Взаимосвязь открытых систем – Родовая безопасность верхних уровней: Обзор, модели и нотация*

Данная Рекомендация относится к серии Рекомендаций, обеспечивающих комплект средств, которые предназначены в помощь при создании протоколов верхнего уровня взаимосвязи открытых систем, поддерживающих организацию услуг безопасности. В данной Рекомендации определено следующее: a) общие модели функций протокола обмена информацией безопасности и преобразований безопасности; b) комплект инструментов нотации для поддержки спецификации требований к защите селективного поля в спецификации абстрактного синтаксиса и для поддержки спецификации обменов информацией безопасности и преобразований безопасности; c) комплект информационных руководящих принципов в отношении применения средств родовой безопасности верхнего уровня, охватываемых этой серией Рекомендаций. Вопрос 10/17

X.831 *Информационная технология – Взаимосвязь открытых систем – Общая безопасность верхних уровней: Определение услуги – Служебный элемент обмена информацией безопасности (SESE)*

Данная Рекомендация относится к серии Рекомендаций, обеспечивающих комплект средств, которые предназначены в помощь при создании протоколов верхнего уровня взаимосвязи открытых систем, поддерживающих организацию услуг безопасности. В данной Рекомендации определена услуга, предоставляемая служебным элементом обмена информацией безопасности (SESE). SESE – прикладной сервисный элемент (ASE), который способствует передаче информации безопасности для поддержки предоставления услуг безопасности в рамках прикладного уровня взаимосвязи открытых систем.
Вопрос 10/17

X.832 *Информационная технология – Взаимосвязь открытых систем – Родовая безопасность верхних уровней: Спецификация протокола служебного элемента обмена информацией безопасности (SESE)*

Данная Рекомендация относится к серии Рекомендаций, обеспечивающих комплект средств, которые предназначены в помощь при создании протоколов верхнего уровня взаимосвязи открытых систем, поддерживающих организацию услуг безопасности. В данной Рекомендации задан протокол, предоставляемый служебным элементом обмена информацией безопасности (SESE). SESE – прикладной сервисный элемент (ASE), который способствует передаче информации безопасности для поддержки предоставления услуг безопасности в рамках прикладного уровня взаимосвязи открытых систем.
Вопрос 10/17

X.833 *Информационная технология – Взаимосвязь открытых систем – Родовая безопасность верхних уровней: Спецификация защищающего синтаксиса передачи*

Данная Рекомендация относится к серии Рекомендаций, обеспечивающих комплект средств, которые предназначены в помощь при создании протоколов верхнего уровня взаимосвязи открытых систем, поддерживающих организацию услуг безопасности. В данной Рекомендации | Международном стандарте определен защищающий синтаксис передачи, связанный с поддержкой представительного уровня для услуг безопасности на прикладном уровне. Вопрос 10/17

X.834 *Информационная технология – Взаимосвязь открытых систем – Родовая безопасность верхних уровней: Форма свидетельства о соответствии реализации протоколу (PICS) служебного элемента обмена информацией безопасности (SESE)*

Данная Рекомендация относится к серии Рекомендаций о родовой безопасности верхних уровней (GULS). Это – форма свидетельства о соответствии реализации протоколу (PICS) для протокола служебного элемента обмена информацией безопасности, определенного в Рекомендации МСЭ-Т X.832, и обмена информацией безопасности, описанного в Рекомендации МСЭ-Т X.830.

Приложение C. Данная Рекомендация содержит описание стандартизованных возможностей и опций в форме, которая поддерживает оценку соответствия конкретной реализации. Вопрос 10/17

X.835 *Информационная технология – Взаимосвязь открытых систем – Родовая безопасность верхних уровней: Форма свидетельства о соответствии реализации протоколу (PICS) защищающего синтаксиса передачи*

Данная Рекомендация относится к серии Рекомендаций о родовой безопасности верхних уровней (GULS). Это – форма свидетельства о соответствии реализации протоколу (PICS) для протокола защищающего синтаксиса передачи, определенного в Рекомендации МСЭ-Т X.833. Данная Рекомендация содержит описание стандартизованных возможностей и опций в форме, которая поддерживает оценку соответствия конкретной реализации. Вопрос 10/17

X.841 *Информационная технология – Методы обеспечения безопасности – Информационные объекты безопасности для управления доступом*

Данная Рекомендация по информационным объектам безопасности (SIOs) для управления доступом содержит определения объектов, которые обычно требуются в стандартах по безопасности для исключения многочисленных и различных определений одной и той же функциональной возможности. Точность таких определений достигается путем использования абстрактно-синтаксической нотации версии один (ASN.1). Данная Рекомендации посвящена только статическим аспектам информационных объектов безопасности (SIOs). Вопрос 10/17

X.842 *Информационная технология – Методы защиты – Руководящие принципы по использованию услуг доверенной третьей стороны и управлению этими услугами*

Данная Рекомендация является руководством по использованию услуг доверенной третьей стороны (TTP) и управлению этими услугами; дано четкое определение выполняемых базовых функций и предоставляемых услуг, их описание и назначение, роли и ответственность TTP и объектов, использующих их услуги. В данной Рекомендации определены различные основные категории услуг TTP, включая создание метки времени, фиксацию авторства, управление ключами, управление сертификатами и службу электронного государственного нотариуса. Вопрос 10/17

X.843 *Информационная технология – Методы защиты – Спецификация услуг TTP для поддержки применения цифровых подписей*

В данной Рекомендации определены услуги, требующиеся для поддержки применения цифровых подписей для фиксации авторства документа. Так как это включает в себя обеспечение целостности и аутентификацию автора, то описанные здесь услуги могут также комбинироваться для реализации услуг обеспечения целостности и аутентификации. Вопрос 10/17

X.901 *Информационная технология – Открытая распределенная обработка – Эталонная модель: Обзор*

Быстрое распространение распределенной обработки данных вызвало необходимость создания координирующей структуры для стандартизации открытой распределенной обработки данных (**ODP**). Представленная эталонная модель обеспечивает такую структуру. Она образует архитектуру, в рамках которой может быть интегрирована поддержка распределения, взаимодействия и переносимости. В данной Рекомендации содержится мотивационный обзор ODP, включающий анализ требований, обоснование и пояснение ключевых концепций, и представлена схема архитектуры ODP. В Рекомендацию включен поясняющий материал по интерпретации и применению эталонной модели пользователями, которыми могут быть разработчики стандартов и проектировщики систем ODP. Рекомендация содержит также классификацию требуемой области стандартизации, приведенную в терминах эталонных точек соответствия, определенных в Рекомендации X.903. Системы ODP должны быть защищенными, то есть должны строиться и эксплуатироваться с использованием таких методов, которые обеспечивают защиту оборудования и данных системы от несанкционированного доступа, незаконного использования и от любых других угроз или атак. Выполнение требований к обеспечению безопасности значительно осложняется при удаленном взаимодействии, мобильности частей и пользователей системы. Правила безопасности для систем ODP могут определять: правила обнаружения угроз безопасности; правила защиты от угроз безопасности; правила ограничения размеров любого ущерба, который является следствием любого нарушения безопасности. Вопрос 26/17

X.902 *Информационная технология – Открытая распределенная обработка – Эталонная модель: Основы*

Данная Рекомендация содержит определение концепций и аналитической структуры для нормализованного описания (произвольных) систем распределенной обработки данных. В ней вводятся принципы соответствия стандартам ODP и порядок их применения. Определение дано только на уровне детализации, достаточном для поддержки Рекомендации X.903 и для задания требований к новым методам составления спецификаций. Вопрос 26/17

X.903 *Информационная технология – Открытая распределенная обработка – Эталонная модель: Архитектура*

Данная Рекомендация содержит спецификацию характеристик, требующихся для квалификации распределенной обработки данных как открытой. Эти характеристики представляют собой ограничения, которым должны соответствовать стандарты ODP. Используются методы описания из Рекомендации X.902 Вопрос 26/17

X.904 *Информационная технология – Открытая распределенная обработка – Эталонная модель: Архитектурная семантика*

Данная Рекомендация содержит нормализацию концепций моделирования ODP, определенных в Рекомендации X.902, пункты 8 и 9. Нормализация выполнена путем интерпретации каждой концепции в терминах построения различных стандартизованных методов формального описания. Вопрос 26/17

B.2 Аспекты безопасности, не охваченные данным Руководством (надежность и физическая защита линейно-кабельных сооружений)

Защита линейно-кабельных сооружений от коррозии, влияний окружающей среды, пожаров, последствий деятельности людей и других форм повреждений всех типов кабелей, применяемых для электросвязи общего пользования и относящихся к ним структур, является одним из элементов, повышающих уровень безопасности транспортировки информации в аспектах надежности и готовности сети. Конструкция оборудования и кабеля, монтаж и контроль являются существенными факторами обеспечения хорошего качества канала связи. Чем больше объем транспортируемой информации, тем более важной является физическая защита линейно-кабельных сооружений. Рекомендации серии L содержат методы, позволяющие повысить уровень безопасности линейно-кабельных сооружений и, соответственно, информации, которая передается от одного оконченного узла к другому.

L.3 *Бронирование кабелей*

Для кабелей, укладываемых непосредственно в землю, бронирование способствует безопасной прокладке и надежной работе за счет обеспечения защиты кабелей от механических повреждений от камней и землеройных машин и орудий, грызунов и насекомых, химической или электролитической коррозии, воздействия атмосферных разрядов и воздействий, вызванных близостью линии электропередачи. Вопрос 8/6

L.4 *Алюминиевые оболочки кабеля*

Универсальное использование алюминия для оболочек кабелей желательно в тех случаях, когда требуется, чтобы стоимость кабеля не возрастала по сравнению с использованием свинца, а также если алюминиевые оболочки в большей степени удовлетворяют техническим требованиям. В частности, использование кабелей с алюминиевой оболочкой представляется особенно интересным в случае магистральных кабелей. Вопрос 8/6

L.5 *Оболочки кабеля, выполненные из металлов, но не из свинца или алюминия*

В зависимости от конкретных применений, могут использоваться другие типы бронирования, такие как гофрированный алюминий, медная фольга и т. д. Вопрос 8/6

L.7 *Применение совместной катодной защиты*

Под совместной катодной защитой нескольких подземных металлический структур понимается защита от коррозии этих структур с использованием общих защитных устройств. Система совместной защиты для нескольких подземных металлических структур состоит из электрических соединений между структурами и общих защитных устройств, выполняющих катодную защиту и требования по току утечки. Методы совместной защиты увеличивают надежность находящихся в земле структур, повышают эффективность устройств катодной защиты, а также снижают общие затраты на создание и эксплуатацию системы защиты. Вопрос 7/6

L.16 *Проводящие пластмассовые материалы (CPM) как защитные покрытия для металлических оболочек кабелей*

Самыми важными преимуществами кабелей CPM являются: согласованная защита против коррозии, разрядов молнии, влияния линий электропередачи и линий привода электротранспорта; сокращение эксплуатационных расходов, особенно на заземление; упрощение проектов защиты. Вопрос 8/6

L.20 *Разработка правил пожарной безопасности для оборудования связи*

Для существующих зданий и при проектировании и строительстве новых зданий предприятий связи администрации должны разрабатывать внутренние правила пожарной безопасности в соответствии с предусмотренным конкретным использованием каждого здания, содержащие минимальные руководящие указания по пожарной безопасности и защите от пожара. Вопрос 2/6

L.21 *Системы сигнализации и обнаружения огня, детекторы и звуковые приборы*

Для защиты недвижимого имущества, а там, где это необходимо, и жизни людей, должны быть установлены защитные системы обнаружения огня и сигнализации для инициирования ряда различных действий, таких как обнаружение и локализация пожара, обеспечение помощи при блокировании и/или тушении пожара, процедуры аварийной эвакуации, вызов пожарной команды. Вопрос 2/6

L.22 *Защита от пожара*

Учитывая возможность серьезных повреждений, которые могут возникнуть при пожаре, и важность предотвращения пожара для безопасности, предоставления услуг и сохранения экономических показателей систем связи, существует ряд аспектов, которые следует принимать во внимание, такие как снижение коэффициента пожарной нагрузки, деление здания на отсеки (пожарные секторы) для уменьшения и задержки распространения огня, сбор статистики пожаров. Вопрос 2/6

L.23 *Тушение пожара – Классификация, расположение и монтаж оборудования для тушения пожара в помещениях*

Противопожарные средства, применяемые в зданиях предприятий связи, могут варьироваться в зависимости от режима работы и места нахождения помещения, а также от степени его заполненности. Они являются теми факторами, которые определяют объем действий противопожарной службы, распределенных первоначально в случае угрозы возникновения пожара. Вопрос 2/6

L.25 *Обслуживание волоконно-оптической кабельной сети*

Системы и процедуры обслуживания обладают способностью контролировать качество волоконно-оптической кабельной сети независимо от оборудования передачи. Вопрос 5/6

L.28 *Внешняя дополнительная защита для кабелей, прокладываемых по дну моря*

Для кабелей, прокладываемых на мелководье, вероятность повреждений выше, чем для глубоководных сооружений, вследствие воздействия окружающей среды (например, движение волн, подводные землетрясения и оползни и т. д.), а также вследствие деятельности людей, затрагивающей дно моря (например, лов рыбы, организация и обслуживание других служб и кабелей).

В дополнение к различным видам брони, используемым обычно в конструкции кабелей – например, твердая броня (RA), бронирование из стальных проводов, такое как одиночная броня (SA), двойная броня (DA), при необходимости может использоваться дополнительная внешняя защита. Такая защита может применяться как вблизи от берега на мелководье, так и на берегу, на участке между кромкой воды и местом соединения на берегу, или вдоль трассы кабеля там, где внешние воздействия или особенности рельефа морского дна могут повредить кабели. Вопрос 10/6

L.32 *Устройства защиты для кабелей, проложенных через границы пожарных секторов*

При наличии большого числа пересечений кабелями границ пожарных секторов здания предприятия связи, что снижает эффективность противопожарной системы, подходящей стратегией является применение пассивных средств защиты от дыма и огня, таких как покрытие мест пересечения кабелями секторов несгораемыми материалами или использование систем защиты кабелей. Вопрос 2/6

L.45 *Минимизация воздействия линейно-кабельных сооружений в сетях электросвязи на окружающую среду*

Приведена подробная методология, разработанная для минимизации воздействий (например, волны и CO_2), вызываемых использованием линейно-кабельных сооружений в окружающей среде. Эта методология базируется на анализе жизненного цикла, который является периодом *от начала до окончания* владения изделием. Вопрос 1/6

L.46 *Защита кабелей и линейных сооружений электросвязи от биологической атаки*

Описываются биологические атаки и меры противодействия для защиты кабелей электросвязи. Рассмотрены виды биологических атак, уязвимость кабелей, особенности повреждений; обсуждаются альтернативные способы защиты линейных сооружений, включая зависимость от местоположения кабеля. Вопрос 1/6

Следующие Рекомендации посвящены обеспечению готовности сетей SDH и OTN:

G.841 *Типы и характеристики защитных архитектур сети SDH*

В данной Рекомендации описываются различные механизмы защиты для сетей синхронной цифровой иерархии (SDH), их задачи и применение.

Схемы защиты классифицированы как защита трассы SDH (на уровне секции или тракта) и как защита соединения подсети SDH (с встроенным контролем, с контролем без вмешательства и с контролем подуровня). Вопросы Q.15, 16, 17, 18/15

G.842 *Взаимодействие защитных архитектур сети SDH*

В данной Рекомендации описываются механизмы взаимодействия защитных архитектур сети. Взаимодействие описывается для одиночных и двойных взаимных соединений между узлами при обмене трафиком между кольцами. Каждое кольцо может быть сконфигурировано для защиты с общим MS или для защиты SNCP. Вопросы Q.15, 16, 17, 18/15

G.808.1 *Коммутация с общей защитой – Защита линейной трассы и подсети*

Данная Рекомендация содержит обзор коммутации с линейной защитой. Он охватывает схемы защиты на базе оптических транспортных сетей (OTN), сетей синхронной цифровой иерархии (SDH) и сетей с асинхронным режимом передачи (ATM). Обзоры защиты кольца и схем взаимных соединений подсети с двойными узлами (то есть кольцо) будут приведены в других Рекомендациях.

Вопросы Q.15, 16, 17, 18/15

G.873.1 *Оптическая транспортная сеть (OTN) – Линейная защита*

В данной Рекомендации определен протокол APS и операция коммутации защиты для схем линейной защиты для оптической транспортной сети на уровне единицы данных оптического канала (ODUk). В данной Рекомендации рассмотрены следующие схемы защиты: защита трассы ODUk; защита соединения подсети ODUk с встроенным контролем; защита соединения подсети ODUk с контролем без вмешательства; защита соединения подсети ODUk с контролем подуровня. Вопросы Q.15, 16, 17, 18/15

G.781 *Функции уровней синхронизации*

Надежность источников тактовой синхронизации SDH и PDH. В данной Рекомендации приведена библиотека базовых образующих блоков распределения синхронизации, называемых “атомными функциями” и набор правил, в соответствии с которыми они объединяются для описания функциональных возможностей синхронизации цифрового оборудования передачи.

Вопросы Q.15, 16, 17, 18/15

G.911 *Параметры и методы расчета надежности и готовности волоконно-оптических систем*

Надежность и готовность волоконно-оптических систем: В данной Рекомендации задан минимальный набор параметров, необходимых для определения параметров надежности и готовности волоконно-оптических систем. Приведены различные параметры для характеристик надежности системы и технического обслуживания, для надежности активных оптических устройств, надежности пассивных оптических устройств и для надежности оптического волокна и кабеля. В Рекомендации приведены также руководящие принципы и методы расчета прогнозируемой надежности устройств, узлов и систем. Приведены примеры. Вопросы Q.15, 16, 17, 18/15

G.784 *Административное управление синхронной цифровой иерархии SDH*

Административное управление SDH. Рекомендация G.784 рассматривает функции “устранение неисправностей”, “конфигурирование”, “учет”, “управление качеством” и “управление безопасностью” (FCAPS) элементов сети SDH. Аспекты управления безопасностью в этих Рекомендациях оставлены “для дальнейшего изучения”. Вопрос Q.14/15

G.874 *Аспекты административного управления элементом оптической транспортной сети*

Административное управление оптической транспортной сетью (OTN). Рекомендация G.874 рассматривает функции “устранение неисправностей”, “конфигурирование”, “учет”, “управление качеством” и “управление безопасностью” (FCAPS) элементов сети OTN. Аспекты административного управления безопасностью в этих Рекомендациях оставлены “для дальнейшего изучения”.Вопрос Q.14/15

G.7712/Y.1703 *Архитектура и спецификация сети передачи данных*

Данная Рекомендация содержит аспекты безопасности сетей передачи информации управления (MCN) и сетей передачи сигнализации (SCN). Приведенные в этой Рекомендации функции передачи данных поддерживают сетевые службы без установления соединения. В будущих версиях могут быть добавлены дополнительные функции для поддержки сетевых служб с установлением соединения. Вопрос Q.14/15

Примечание: Рекомендации в сериях G.650, 660–690, 950–970 могут содержать некоторые элементы, относящиеся к надежности.

Приложение C: Перечень исследовательских комиссий и Вопросов, связанных с проблемой безопасности

Деятельность МСЭ –Т в области стандартизации осуществляется техническими исследовательскими комиссиями (ИК), в которых представители членов МСЭ-Т разрабатывают Рекомендации (стандарты) для различных областей международной электросвязи. ИК ведут свою работу в основном в форме изучения Вопросов. Каждый из них предполагает проведение технических исследований в конкретной области стандартизации электросвязи. Во всех ИК есть Председатель ИК и несколько заместителей председателя, назначенные Всемирной ассамблеей по стандартизации электросвязи (ВАСЭ). Ниже следует перечень исследовательских комиссий МСЭ-Т на исследовательский период 2001–2004 годов, их наименования и мандаты, а также перечень Вопросов для изучения, связанных с деятельностью в области безопасности.

ИК 2	Эксплуатационные аспекты предоставления услуг, сети и характеристики работы *Ведущая исследовательская комиссия по вопросам определения услуг, нумерации, маршрутизации и глобальной мобильности*
Мандат: отвечает за проведение исследований, относящихся к следующим вопросам: принципы предоставления услуг, определение и эксплуатационные требования к эмуляции услуг; требования к нумерации, присвоению наименований и адресации и распределение ресурсов, включая критерии и процедуры резервирования и распределения; требования к маршрутизации и взаимодействию; человеческие факторы; эксплуатационные аспекты сетей и связанные с ними требования к эксплуатационным характеристикам, включая управление трафиком сети, качество обслуживания (технические вопросы трафика, эксплуатационные характеристики и служебные измерения); эксплуатационные аспекты взаимодействия традиционных сетей электросвязи и вновь создаваемых сетей; оценка обратной связи со стороны операторов, производственных компаний и пользователей по различным аспектам работы сети.	
Основные Вопросы, связанные с безопасностью: - Q.5/2 – Качество обслуживания в сетях	

ИК 3	Принципы тарификации и расчетов, включая соответствующие экономические и стратегические вопросы электросвязи
Мандат: отвечает за проведение исследований, относящихся к принципам тарификации и расчетов для международных услуг электросвязи, а также за изучение соответствующих экономических и стратегических вопросов электросвязи. С этой целью 3-я Исследовательская комиссия, в частности, способствует активизации сотрудничества входящих в нее Членов в целях установления расчетных такс на как можно более низких уровнях без ущерба для эффективности услуг с учетом необходимости поддержания независимого финансового управления электросвязью на прочной основе.	
Основные Вопросы, связанные с безопасностью: *Нет*	

ИК 4	Управление электросвязью, включая TMN *Ведущая исследовательская комиссия по вопросам TMN*
Работа ИК 4 в области безопасности как ведущей исследовательской комиссии по вопросам управления охватывает следующие направления: a) вопросы архитектуры и требования к архитектуре для интерфейсов управления; b) конкретные требования к защите сети управления (также называемой плоскостью управления), особенно в условии конвергенции сетей; c) протокол и модели для обеспечения защиты управляющей информации и управление параметрами безопасности.	

Управление сетью электросвязи определяется при различных уровнях абстракции – от управления информацией на уровне сетевого элемента до услуг управления, предлагаемых потребителю. Требования к безопасности для информации, которой обмениваются системы управления и системы управления и сетевые элементы, зависят от того, находятся ли сети управления в пределах одной или нескольких административных областей. Исходя из принципов архитектуры, в действующих Рекомендациях определены конкретные требования, механизмы и поддерживающие протоколы, а также разрабатывается еще ряд Рекомендаций.

Основные Вопросы, связанные с безопасностью:
- Q.16/4 – Обеспечение управления TMN для IMT-2000 и интеллектуальных сетей

ИК 5	Защита от электромагнитных воздействий окружающей среды

ИК 5 отвечает за проведение исследований, относящихся к защите сетей и оборудования электросвязи от помех и ударов молнии, а также за проведение исследований по электромагнитной совместимости (ЭМС). Выполняя свою задачу, ИК 5 ведет исследования в рамках нескольких Вопросов и разрабатывает ряд Рекомендаций и пособий, посвященных защите сети от электромагнитных угроз. Электромагнитные угрозы включают злонамеренно создаваемые нестационарные процессы большой мощности, такие как возникновение электромагнитного импульса в результате высотного ядерного взрыва (HEMP) и мощное сверхвысокочастотное излучение (HPM). Наряду с этим электромагнитная защита может охватывать проблему утечки информации в сетях электросвязи вследствие непредвиденного радиоизлучения оборудования.

Природа умышленных угроз и соответствующие средства их смягчения аналогичны тем, которые применяются к естественным или непреднамеренным электромагнитным возмущениям. Следовательно, традиционная деятельность 5-й Исследовательской комиссии, касающаяся защиты от ударов молнии и контроля электромагнитных помех (EMI), укрепляет защиту сети от умышленно создаваемых человеком угроз. В настоящее время ИК 5 назначены для изучения шесть Вопросов, касающихся защиты сети электросвязи от электромагнитных воздействий.

Наряду со значительным сходством между злонамеренными создаваемыми человеком электромагнитными угрозами и случайными или естественными электромагнитными условиями, между ними существуют и значительные различия. Выполняя свою задачу, ИК 5 ведет исследования в рамках нескольких Вопросов и разрабатывает ряд Рекомендаций и пособий, посвященных защите сети от электромагнитных угроз.

Двумя основными областями обеспечения электромагнитной безопасности являются:

- Устойчивость и защищенность сетей и оборудования электросвязи в отношении воздействия умышленно создаваемых человеком нестационарных процессов большой мощности. К таким угрозам относятся:
  - электромагнитные поля, создаваемые ядерными взрывами на большой высоте – электромагнитный импульс в результате высотного ядерного взрыва (HEMP);
  - генераторы мощных электромагнитных (HPE) сигналов, включая источники мощного сверхвысокочастотного излучения (HPM) и ультраширокополосных (UWB) сигналов.
- Возможность утечки информации в сетях электросвязи вследствие непредвиденного радиоизлучения оборудования.

В последнее время уровень осведомленности о существовании угроз безопасности, связанных с этими процессами, возрастает благодаря появлению в средствах массовой информации статей, репортажей и телепрограмм, посвященных данных вопросам.

Природа умышленных электромагнитных угроз и соответствующие средства их смягчения аналогичны тем, которые применяются к естественным или непреднамеренным электромагнитным возмущениям. Например, существует сходство между HEMP и электромагнитными импульсами, создаваемыми молнией. Методы экранирования и фильтрации, которые снижают уровень излучения оборудованием нежелательной радиоэнергии, также уменьшают вероятность непреднамеренной утечки энергии. Следовательно, традиционная деятельность 5-й Исследовательской комиссии, касающаяся защиты от ударов молнии и контроля электромагнитных помех (EMI), укрепляет защиту сети от умышленно создаваемых человеком угроз. В нижеследующей таблице перечислены Вопросы, назначенные для изучения 5-й Исследовательской комиссии на исследовательский период 2001–2004 годов, касающиеся обеспечения безопасности сети.

Основные Вопросы, связанные с безопасностью:

- Q.2/5 – ЭМС, связанная с широкополосными системами доступа (*Контроль нежелательного излучения широкополосных систем доступа способствует уменьшению вероятности утечки информации).*
- Q.4/5 – Устойчивость новых типов оборудования связи и сетей доступа (*Устойчивость оборудования к ударам молнии повышает устойчивость оборудования к волнам, наводимым HEMP*).
- Q.5/5 – Защита фиксированных, подвижных и беспроводных систем от ударов молнии (*Методы, используемые для защиты от ударов молнии, также повышают устойчивость оборудования к воздействиям HEMP и HPE*).
- Q.6/5 – Конфигурация соединений и заземление систем электросвязи в глобальной окружающей среде (*Надлежащее соединение и меры по обеспечению заземления также помогают повысить устойчивость оборудования к воздействиям HEMP и HPE*).
- Q.12/5 – Ведение и совершенствование действующих Рекомендаций по ЭМС (*ЭМС оборудования электросвязи повышает устойчивость функционирования оборудования в среде излучаемых HEMP, а также в среде излучаемых HPE. Также ЭМС оборудования электросвязи снижает вероятность утечки информации*).
- Q.13/5 – Ведение и совершенствование Рекомендаций по вопросам устойчивости (*Устойчивость оборудования к ударам молнии повышает устойчивость оборудования к волнам, наводимым HEMP*).

ИК 6	Линейно-кабельные сооружения

Мандат: отвечает за проведение исследований, касающихся линейно-кабельных сооружений, в таких областях как сооружение, прокладка, соединение, оконечная нагрузка, защита всех типов кабелей для систем электросвязи общего пользования и относящихся к ним структур от коррозии и других видов повреждений под воздействием внешних условий, за исключением электромагнитных процессов.

Основные Вопросы, связанные с безопасностью:

- Q.1/6 – Вопросы влияния сооружений электросвязи на окружающую среду
- Q. 2/6 – Пожаробезопасность
- Q. 5/6 – Техническое обслуживание волоконно-оптической кабельной сети

ИК 9	Интегрированные широкополосные кабельные сети и передача телевизионных сигналов и звуковых программ *Ведущая исследовательская комиссия по вопросам интегрированных широкополосных кабельных и телевизионных сетей*

Исследовательская комиссия МСЭ по “Интегрированным широкополосным кабельным сетям и передаче телевизионных сигналов и звуковых программ” (ИК 9) является ведущей исследовательской комиссией по вопросам интегрированных широкополосных кабельных и телевизионных сетей. Исследовательская комиссия готовит и ведет рекомендации по:

- использованию кабельных и гибридных сетей, предназначенных в первую очередь для доставки телевизионных и звуковых программ на домашние приемники, в качестве интегрированных широкополосных сетей, применяемых также для передачи речи и других нормируемых по времени услуг, видеопрограмм по заказу, интерактивных услуг и т. д;
- использованию систем электросвязи для трансляции, первичного распределения и вторичного распределения телевизионных и звуковых программ, а также предоставления других аналогичных услуг передачи данных.

В этой роли ИК 9 проводит оценку угроз и уязвимости широкополосных сетей и услуг, ведет документирование объектов защиты, оценивает меры противодействия и определяет архитектуру безопасности. Основными исследуемыми вопросами безопасности являются защищенные широкополосные услуги, защищенные услуги VoIP, защищенные услуги домашней сети и защищенная среда приложений для интерактивных телевизионных служб.

Деятельность, связанная с безопасностью, строится по следующим направлениям:

- *Защищенные широкополосные услуги:* обеспечение защищенных услуг для сетей широкополосного доступа, а именно, аутентификация кабельного модема, управление криптографическими ключами, секретность и целостность передаваемых данных и защищенная загрузка программного обеспечения кабельного модема.
- *Защищенные услуги VoIP:* IPCablecom является специальным проектом по нормируемым по времени интерактивным услугам, предоставляемым по кабельным телевизионным сетям с использованием протокола IP, в частности звук и видео по IP. Предоставляемые в рамках IPCablecom услуги по обеспечению безопасности включают аутентификацию адаптера мультимедийного терминала (MTA) для поставщика услуг, аутентификацию поставщика услуг для MTA, защищенные инициализацию и конфигурацию устройства, защищенное управление устройствами, защищенную сигнализацию и защищенную среду передачи.
- *Защищенные услуги домашней сети:* усовершенствованные кабельные модемы могут обеспечить услуги домашней сети, такие как брандмауэры и трансляция сетевых адресов. Защищенные услуги, предоставляемые для усовершенствованных кабельных модемов, включают аутентификацию адаптера мультимедийного терминала (MTA) для поставщика услуг, аутентификацию поставщика услуг для MTA, защищенные инициализацию и конфигурацию устройства, защищенное управление устройствами, фильтрацию \пакетов/функциональные возможности брандмауэра, защищенное управление брандмауэрами и защищенную загрузку программного обеспечения усовершенствованного кабельного модема.
- *Защищенная среда приложений для интерактивных телевизионных служб:* Интерактивные телевизионные службы базируются на защищенных услугах, определенных в спецификации Java и мультимедийной домашней платформы (MHP).

Основные Вопросы, связанные с безопасностью:

- Q.6/9 – Методы и практика ограниченного доступа и защиты от копирования в цифровых кабельных сетях непосредственного телевизионного вещания
- Q13/9 – IP-приложения передачи звуковых и видеосигналов по сетям кабельного телевидения

ИК 11	Требования к сигнализации и протоколы *Ведущая исследовательская комиссия по вопросам интеллектуальных сетей*

Мандат: отвечает за проведение исследований, касающихся требований к сигнализации и протоколов, связанных с функциями протокола Интернет (IP), некоторых функций, связанных с мобильностью, мультимедийных функций, а также внесение изменений в действующие рекомендации по протоколам доступа и межсетевой сигнализации АРП, У-ЦСИС и ТСОП.

Основные Вопросы, связанные с безопасностью:

- Q.1/11 – Требования к сигнализации для поддержки сигнализации для услуг: новых, дополнительных, базирующихся на IP и базирующихся на IN.
- Q.6/11 – Требования к сигнализации для поддержки сигнализации для служебного взаимодействия при коммутируемом доступе в Интернет и при передаче речи, данных и информации мультимедиа по сетям, базирующимся на IP.
- Q.12/11 – Сигнализация доступа и сети для усовершенствованных узкополосных и широкополосных услуг.

ИК 12	Характеристики сети и оконечного оборудования при сквозной передаче *Ведущая исследовательская комиссия по вопросам качества обслуживания и характеристик*

Мандат: отвечает за выработку руководящих принципов по характеристикам сквозной передачи сетей, оконечного оборудования и их взаимодействия в зависимости от воспринимаемого пользователем качества и восприятия пользователем текста, речи и изображения. Данная работа включает также связанные с этим вопросы передачи для всех сетей (например, базирующихся на ПЦИ, СЦИ, АРП и IP) и всех оконечных устройств электросвязи (например, микротелефонная трубка, громкоговорящий телефон, наушники, мобильный телефон, видеотелефонное устройство и устройство интерактивного речевого ответа).

Основные Вопросы, связанные с безопасностью:

Q.12/12 – Соображения по характеристикам передачи для телефонных услуг, предоставляемых по сетям, в которых используется протокол Интернет (IP)/

Q.13/12 – Требования к QoS/характеристикам мультимедиа.

ИК 13	Сети, работающие на базе множественных протоколов и протокола Интернет, и обеспечение их взаимодействия *Ведущая исследовательская комиссия по вопросам, относящимся к протоколу Интернет (IP), Ш-ЦСИС, глобальной информационной инфраструктуре и спутниковой связи*

Исходя из содержания своих обязанностей, 13-я Исследовательская комиссия проводит исследования, относящиеся к:

- обеспечению взаимодействия неоднородных сетей, охватывающих множество доменов;
- множеству протоколов и современным технологиям с целью обеспечения высококачественной и надежной работы сетей.
- Конкретными аспектами являются архитектура, сетевое взаимодействие и адаптация, вопросы сквозной связи, маршрутизация и требования к транспортным сетям.

Учитывая, что эта комиссия является ведущей исследовательской комиссией по вопросам, относящимся к IP, Ш-ЦСИС, глобальной информационной структуре и спутниковой связи, а также к новому проекту NGN, в ходе ее деятельности будет затронуто множество связанных с безопасностью вопросов в самом широком смысле слова.

Традиционно 13-я Исследовательская комиссия МСЭ-Т неявным образом рассматривала аспекты безопасности, занимаясь вопросами архитектуры и сетевой структуры, понимая абсолютную необходимость охвата таких аспектов (как в отношении архитектуры, так и в аспекте реализации) для обеспечения функциональной и надежной сети.

Сложность вопросов безопасности возрастает по мере реализации новых, в большей или меньшей степени открытых, технологий цифровой связи с коммутацией пакетов и либерализованной средой, которые описаны, например в концепции ГИИ. Это особенно верно, когда участвуют третьи стороны, согласно понятию “цепи добавленной стоимости” в концепции ГИИ (или поднабор соответствующих NGN). В этих условиях вопросы безопасности во всех ее аспектах приобретают еще большую важность и должны решаться явным образом.

Исходя из этого, 13-я Исследовательская комиссия приняла решение включать во все новые или пересматриваемые Рекомендации раздел по безопасности, содержащий ссылки на те разделы данной Рекомендации, в которых рассматриваются вопросы безопасности. Даже если в данной Рекомендации не затрагиваются аспекты безопасности, этот факт, тем не менее, должен быть отражен в указанном специальном разделе по безопасности. Данное решение уже признано ИК 17, и намечено предложить его для принятия всем исследовательским комиссиям МСЭ-Т.

Также в ИК 13 было решено, что о Рекомендациях, содержащих связанные с безопасностью параметры, следует сообщать в 17-ю Исследовательскую комиссию МСЭ-Т, с тем чтобы обеспечить своевременное обновление “Каталога утвержденных Рекомендаций по безопасности” и “Сборника утвержденных МСЭ-Т определений в области безопасности”.

Кроме того, в нескольких разделах нового проекта по NGN рассматриваются аспекты безопасности, и особое внимание им уделяется в разделе 6.6.

Основные Вопросы, связанные с безопасностью:

Q.1/13 – Принципы, требования, структуры и архитектуры для общей среды неоднородных сетей

Q.3/13 – OAM и управление сетью в сетях, базирующихся на протоколе IP, и в других сетях

Q.4/13 – Управление ресурсами, связанными с широкополосными службами и IP-службами

Q.6/13 – Характеристики IP-сетей и создаваемая глобальная информационная инфраструктура

Q.7/13 – Передача ячеек АТМ/Ш-ЦСИС и характеристики готовности

Q.8/13 – Ошибки при передаче и характеристики готовности

Q.10/13 – Архитектура базовой сети и принципы взаимодействия

Q.11/13 – Механизмы, позволяющие IP-службам работать в сетях общего пользования

ИК 15	Оптические и другие транспортные сети *Ведущая исследовательская комиссия по транспортным аспектам сети доступа и оптическим технологиям*

В соответствии с Вопросом 14 ИК 15 (Q.14/15) Комиссия отвечает за определение требований в отношении административного и оперативного управления, а также поддержку информационных моделей для оборудования, осуществляющего транспортные функции. Q.14/15 следует установленным МСЭ-Т понятию и структуре TMN для определения указанных требований и моделей. Управление безопасностью является одной из пяти ключевых функциональных категорий управления TMN. Управление безопасностью входит в сферу охвата и изучается в рамках Q.14/15.

- Требования к управлению оборудованием, осуществляющему транспортные функции: в G.7710/Y.1701, G.784, и G.874 рассматриваются функции управления оборудованием (EMF) элементов транспортных сетей, которые являются общими для множества технологий, специфическими для сетевых элементов СЦИ и специфическими для сетевых элементов оптических транспортных систем, соответственно. Дается описание приложений для управления датой и временем, управления устранением неисправностей, управления конфигурацией, управления расчетами, управление качеством функционирования и управления безопасностью. В результате этих приложений устанавливаются спецификации функций EMF и требования к ним. Требования к управлению безопасностью, входящие в эти Рекомендации, в настоящее время исследуются.

- Архитектура и требования к сети передачи данных: в G.7712/Y.1703 определяются требования к архитектуре для сети передачи данных (DCN), которая может поддерживать распределенную передачу управляющей информации, относящуюся к сети управления электросвязью (TMN), распределенную передачу сигнализации, относящуюся к транспортной сети с автоматической коммутацией (ASTN), и иную распределенную передачу (например, служебный канал или передача речи, удаленная загрузка программного обеспечения). Для разных приложений (например, TMN, ASTN и т. д.) требуется сеть передачи в пакетном режиме для транспортировки информации между различными компонентами. Например, для TMN необходима сеть связи, которая является сетью передачи управления (MCN), для транспортировки управляющих сообщений между компонентами TMN (например, компоненты NEF и OSF). Для ASTN требуется сеть связи, которая является сетью передачи сигнализации (SCN), для транспортировки сообщений сигнализации между компонентами ASTN (например, компонентами CC). В отношении требований к безопасности MCN в G.7712/Y.1703 делается ссылка на M.3016. Требования к безопасности SCN описаны в G.7712/Y.1703.

- Распределенное управление вызовами и соединениями: в G.7713/Y.1704 содержатся требования к распределенному управлению вызовами и соединениями для интерфейса пользователь-сеть (UNI) и интерфейса сеть-узел (NNI). Содержащиеся в данной Рекомендации требования определяют порядок связи через интерфейсы для осуществления автоматических операций с вызовами и соединениями. Наряду с прочими определены атрибуты безопасности, позволяющие проводить аутентификацию операций с вызовами и соединениями (например, это может быть информация, разрешающая аутентификацию запроса вызова и, возможно, проверку целостности запроса вызова).

- Архитектура и требования для маршрутизации в оптических сетях с автоматической коммутацией: в G.7715/Y.1706 определяются требования и архитектура для функций маршрутизации, используемых для установления коммутируемых соединений (SC) и программируемых постоянных соединений (SPC) в рамках структуры оптической сети с автоматической коммутацией (ASON). Данная Рекомендация охватывает следующие основные области: архитектура маршрутизации ASON, функциональные компоненты, включая выбор маршрута, атрибуты маршрутизации, абстрактные сообщения и диаграммы состояния. В отношении соображений безопасности в данной Рекомендации делаются ссылки на Рекомендации МСЭ-Т M.3016 и X.800. В частности, в Рекомендации говорится, что в зависимости от условий применения протокола маршрутизации степень важности общих целей безопасности, определенных в Рекомендации МСЭ-Т M.3016 – конфиденциальность, целостность данных, отчетность и готовность, – может меняться. Анализ угроз предлагаемого протокола маршрутизации исходя из Рекомендации МСЭ-Т X.900, должен учитывать следующие события: нелегальное проникновение, подслушивание, несанкционированный доступ, потеря или искажение информации (включая атаки типа повторной передачи перехваченных сообщений), фиксация авторства, фальсификация и отказ в обслуживании.

- Структура управления ASON: в серии G рассматриваются аспекты управления плоскости оперативного управления ASON и взаимодействие между плоскостью административного управления и плоскостью оперативного управления ASON. Будут включены требования к управлению устранением неисправностей, управлению конфигурацией, управлению расчетами, управлению качеством функционирования и управлению безопасностью для компонентов плоскости оперативного управления.

Основные Вопросы, связанные с безопасностью:
- Q.14/15 – Управление сетью для транспортных систем и оборудования

ИК 16	Мультимедийные службы, системы и оконечные устройства *Ведущая исследовательская комиссия по вопросам мультимедийных услуг, систем и оконечного оборудования, а также электронного бизнеса и электронной торговли*

16-я Исследовательская комиссия является ведущей исследовательской комиссией по вопросам мультимедийных услуг, систем и оконечного оборудования, а также ведущей комиссией по вопросам электронного бизнеса и электронной торговли. Вопрос G (из WP2/16) охватывает "Безопасность мультимедийных систем и услуг" и в его рамках рассматриваются следующие вопросы безопасности.

Развитые мультимедийные (ММ) приложения, такие как телефония по сетям с коммутацией пакетов, голос по IP, интерактивные конференции и групповая работа; передача сообщений ММ, потоковая транспортировка аудио/видеоданных и другие подвержены разнообразным серьезным угрозам в неоднородной среде. Атаки, заключающиеся в злоупотреблении, злонамеренном искажении, подслушивании и отказе в обслуживании, представляют лишь небольшую часть возможных рисков, особенно в сетях, базирующихся на IP.

Общепризнано, что указанные приложения имеют общие потребности в защите, которые могут быть удовлетворены с помощью общих мер защиты, например обеспечение безопасности сети. Вместе с тем, ММ приложения, как правило, имеют потребности в обеспечении безопасности, обусловливаемые конкретным приложением, которые наилучшим образом удовлетворяются на прикладном уровне. Вопрос G посвящен проблемам безопасности ММ приложений и при необходимости в нем принимаются в расчет дополнительные меры сетевой защиты.

Основные Вопросы, связанные с безопасностью:
- Q.G/16 – Защита информации в мультимедийных системах и службах

ИК 17	Сети передачи данных и программное обеспечение электросвязи *Ведущая исследовательская комиссия по вопросам ретрансляции кадров, безопасности системы связи, языкам и средствам описания*

Мандат: отвечает за проведение исследований, относящихся к сетям передачи данных, к применению открытых систем связи, включая передачу данных по сети, каталоги и безопасность, к языкам технических описаний и методам их использования, а также к прочим вопросам, связанным с аспектами программного обеспечения систем электросвязи.

Основные Вопросы, связанные с безопасностью:

Q.9/17 – Службы и системы каталогов

Q.10/17 – Требования к безопасности, модели безопасности и руководящие принципы обеспечения безопасности для систем и служб связи (Примечание: 17-я Исследовательская комиссия согласовала разделение Вопроса 10/17 на шесть отдельных Вопросов: G/17 – Проект безопасности, H/17 – Архитектура и структура безопасности, I/17 – Безопасность киберсреды, J/17 – Управление безопасностью; K/17 – Телебиометрия и L/17 – Защищенные услуги связи)

СИК	Специальная исследовательская комиссия "IMT-2000 и последующие системы" *Ведущая исследовательская комиссия по IMT 2000 и последующим системам, а также по вопросам мобильности*
Специальная исследовательская комиссия МСЭ-Т "IMT-2000 и последующие системы" включила безопасность в качестве ключевого аспекта своих содержащих ссылки Рекомендаций для членов семейства IMT-2000 (3G), определенных в сериях Рекомендаций Q.1741.x (3GPP) и Q.1742.x (3GPP2). Сюда относятся оценка воспринимаемых угроз и перечень требований к безопасности, способной противостоять этим угрозам, целей и принципов безопасности, определенная архитектура безопасности (то есть функции и механизмы безопасности), требования к криптографическим алгоритмам, требования в отношении санкционированного перехвата, а также архитектура и функции санкционированного перехвата. Эти исследования проводятся в рамках Вопросов 3, 6 и 7 СИК. Основными целями исследований по вопросам санкционированного перехвата являются выработка определения полезного перехвата и контроль соответствующей информации, которая должна быть предоставлена поставщиками услуг национальным правоприменительным органам. Перехват, касающийся информации и содержания связи, может быть либо технически независимым, либо зависимым от сетей 3G или развернутых сетей подвижной связи 3G.	
Основные Вопросы, связанные с безопасностью: - 3/SSG – Определение существующих и развивающихся систем IMT-2000 - 6/SSG – Гармонизация развития систем IMT-2000 - 7/SSG – Конвергенция фиксированных и существующих систем IMT-2000	

Блоки обеспечения безопасности – МСЭ-Т

Структура архитектуры безопасности

X.800 – Архитектура защиты при взаимосвязи открытых систем для применений МККТТ
X.802 – Информационная технология – Модель безопасности нижних уровней
X.803 – Информационная технология – Взаимосвязь открытых систем – Модель безопасности верхних уровней
X.805 – Архитектура безопасности для систем, обеспечивающих межконцевую связь
X.810 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Обзор
X.811 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура аутентификации
X.812 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура управления доступом
X.813 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура фиксации авторства
X.814 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура конфиденциальности
X.815 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура целостности
X.816 – Информационная технология – Взаимосвязь открытых систем – Структуры безопасности для открытых систем: Структура аудита и аварийных извещений безопасности

Протоколы

X.273 – Информационная технология – Взаимосвязь открытых систем – Протокол безопасности сетевого уровня
X.274 – Информационная технология – Электросвязь и передача информации между системами –Протокол безопасности транспортного уровня

Безопасность при ретрансляции кадров

X.272 – Сжатие данных и засекречивание в сетях с ретрансляцией кадров

Методы обеспечения безопасности

X.841 – Информационная технология – Методы обеспечения безопасности – Информационные объекты безопасности для управления доступом
X.842 – Информационная технология – Методы защиты – Руководящие принципы по использованию услуг доверенной третьей стороны и управлению этими услугами
X.843 – Информационная технология – Методы защиты – Спецификация услуг TTP для поддержки применения цифровых подписей

Службы Справочника и аутентификация

X.500 – Информационная технология – Взаимосвязь открытых систем – Справочник: Обзор концепций, моделей и служб
X.501 – Информационная технология – Взаимосвязь открытых систем – Справочник: Модели
X.509 – Информационная технология – Взаимосвязь открытых систем – Справочник
X.519 – Информационная технология – Взаимосвязь открытых систем – Справочник: Спецификация протокола

Безопасность управления сетью

M.3010 – Принципы построения сети управления электросвязью
M.3016 – Обзор безопасности TMN
M.3210.1 – Управление безопасностью для категории IMT2000 – Требования
M.3320 – Требования к интерфейсу X
M.3400 – Функции управления TMN

Управление системами

X.733 – Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция тревожного оповещения
X.735 – Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция управления регистрацией
X.736 – Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция отчетов о неисправности системы защиты информации
X.740 – Информационная технология – Взаимосвязь открытых систем – Управление системами: Функция контрольного журнала защиты
X.741 – Информационная технология – Взаимосвязь открытых систем – Управление системой: Объекты и атрибуты для управления доступом

Факсимильная связь

T.30 Приложение G – Процедуры для факсимильной передачи документов по телефонным сетям общего пользования
T.30 Приложение H – Средства защиты для использования с факсимильными терминалами группы 3
T.36 – Средства защиты для использования с факсимильными терминалами группы 3
T.503 – Модель применения документа для обмена факсимильными документами Группы 4
T.563 – Характеристики оконечного оборудования аппаратуры факсимильной связи Группы 4

Телевизионные и кабельные системы

J.91 – Технические методы обеспечения секретности при дальней международной передаче телевидения
J.93 – Требования к условному доступу при вторичном предоставлении цифрового телевидения или кабельных телевизионных систем
J.170 – Спецификация безопасности IPCablecom

Мультимедийная связь

H.233 – Система обеспечения конфиденциальности для аудиовизуальных служб
H.234 – Система управления ключами шифрования и аутентификации для аудиовизуальных служб
H.235 – Защита и шифрование для мультимедийных терминалов серии H (H.323 и других терминалов на базе H.245)
H.323 Приложение J – Мультимедийные системы связи на основе пакетов (Защита для простых типов оконечных пунктов)
H.350.2 – Архитектура служб Справочника для H.235
Защита для в мультимедийных мобильных связных средах

Рекомендации МСЭ-Т доступны через Web-сайт МСЭ http://www.itu.int/publications/bookshop/how-to-buy.html (на данном сайте содержится информация об ограниченном бесплатном доступе к Рекомендациям МСЭ-Т)

Важные направления текущей работы МСЭ-Т в области безопасности:

Телебиометрия, Управление безопасностью, Безопасность мобильности, Электросвязь в чрезвычайных ситуациях

Более подробная информация об МСЭ-Т и его исследовательских комиссиях размещена по адресу http://www.itu.int/ITU-T