Международный союз электросвязи

Безопасность в электросвязи и информационных технологиях

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

МСЭ-Т

Сектор стандартизации электросвязи МСЭ

2006 г.

Международный союз электросвязи

МСЭ-Т

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

Международный союз электросвязи

Безопасность в электросвязи и информационных технологиях

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

Июнь 2006 г.

Международный союз 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: Герберт Бертайн, Дэвид Чадуик, Мартин Ойхнер, Майкл Хэрроп, Шандор Мазгон, Стивен Меттлер, Крис Раделе, Лакшми Раман, Эрик Розенфельд, Нил Сейтс, Рао Васиреди, Тим Уокер, Хьюнг-Юл Юм, Джо Зебарт, а также консультанты МСЭ/БРЭ.

Содержание

Стр.

Стр.

Предисловие

Еще сравнительно недавно проблема безопасности в электросвязи и информационных технологиях относилась к таким специальным областям, как банковская деятельность, авиакосмические и военные приложения. Однако по мере стремительного роста и широкого распространения средств передачи данных, особенно интернета, безопасность стала касаться практически каждого человека.

Возросшее внимание к проблеме безопасности ИКТ можно объяснить, в частности, часто сообщаемыми случаями распространения вирусов и "червей", проникновения хакеров и возникновения угрозы для неприкосновенности личной жизни. Однако поскольку в настоящее время вычислительная техника и сети стали важной частью повседневной жизни, возникает настоятельная необходимость в принятии эффективных мер безопасности для защиты компьютерных и телекоммуникационных систем органов государственной власти, промышленности, торговли, ключевых инфраструктур и потребителей. Кроме того, все большее число стран принимают законодательство о защите данных, которое требует соблюдения установленных стандартов в отношении конфиденциальности и целостности данных.

Крайне важно также хорошо продумать процесс: обеспечения безопасности на всех стадиях – от планирования и проектирования до реализации и развертывания. При разработке стандартов вопрос безопасности всегда должен решаться с самого начала, а не задним числом. Если аспект безопасности не рассмотреть должным образом на стадии разработки стандартов и систем, при реализации вполне могут обнаружиться уязвимые элементы. Комитеты по стандартам играют очень значимую роль в защите систем связи и информационных технологий, обеспечивая осведомленность в вопросах безопасности, заботясь о том, чтобы аспекты безопасности стали одним из главных элементов технических характеристик, и снабжая конструкторов и пользователей руководящими указаниями в отношении того, как сделать системы и услуги связи достаточно надежными.

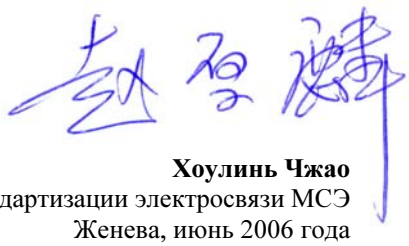
В течение многих лет МСЭ-Т активно занимается проблемой безопасности в электросвязи и информационных технологиях. Однако не всегда легко определить, какие именно вопросы рассмотрены и где с ними можно ознакомиться. Настоящее Руководство представляет собой попытку собрать воедино всю имеющуюся информацию о работе МСЭ-Т.

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.

Первый вариант настоящего Руководства (2003 г.) был опубликован в декабре 2003 года перед первым этапом Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО). Воодушевленные тем, что сообщество ИКТ во всем мире горячо откликнулось на выпуск этого издания, а также, приняв во внимание ценные предложения и отклики от читателей, мы подготовили второе издание. В издании, опубликованном в октябре 2004 года, изменена структура, включены дополнительно новые материалы и расширены некоторые аспекты. Настоящее третье издание 2006 года учитывает новую структуру исследовательских комиссий и Вопросы, определенные в результате Всемирной ассамблеи стандартизации электросвязи, которая проводилась 5–14 октября 2004 года во Флорианополисе (ВАСЭ-04).

Я хотел бы выразить свою признательность инженерам Бюро стандартизации электросвязи МСЭ, которые совместно с экспертами, представляющими членов МСЭ, подготовили основную часть первого издания. Я также хотел бы поблагодарить всех, кто представил нам ценные предложения и кто принял участие в подготовке нового издания. Я особо признателен г-ну Герберту Бертайну, председателю 17-й Исследовательской комиссии МСЭ-Т, которая является ведущей исследовательской комиссией по вопросам безопасности, а также группе сотрудничающих сторон из 17-й исследовательской комиссии и других исследовательских комиссий 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, июнь 2006 года

Резюме

Отрасль связи внесла заметный вклад в повышение производительности и эффективности во всем мире на основе развития инфраструктур связи, которые соединяют сообщества практически во всех промышленных секторах и уголках земли. Это стало возможным во многом благодаря применению стандартов, разработанных такими организациями, как МСЭ-Т. Эти стандарты обеспечивают функциональную совместимость и эффективность работы сетей, а также закладывают основы для сетей последующих поколений. 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, которые не всегда проходят надлежащие испытания, увеличивают вероятность злонамеренного использования сетей. В последние годы во всех глобальных сетях наблюдается резкое увеличение случаев нарушения безопасности (таких как внедрение вирусов и атаки, приводящие к нарушению конфиденциальности хранимых данных), что влечет за собой крупные расходы. Следовательно, вопрос заключается в том, как содержать инфраструктуру открытой связи, не подвергая риску передаваемую через нее информацию. В значительной степени ответом на этот вопрос является разработка достаточно надежных технических характеристик, обеспечивающих противодействие угрозам безопасности во всех элементах инфраструктуры связи. Для достижения этой цели группы по стандартам занимаются, в частности, разработкой стандартных архитектур и структур, стандартов по управлению безопасностью, протоколов и методов, относящихся конкретно к безопасности и обеспечивающих защиту протоколов связи, а также мер, позволяющих свести к минимуму уязвимые элементы стандартов связи в целом.

Цель настоящего Руководства по безопасности заключается в том, чтобы представить обзор многочисленных Рекомендаций по обеспечению защиты инфраструктуры связи и связанных с ней услуг и приложений, которые разработаны МСЭ-Т, иногда в сотрудничестве с другими организациями по разработке стандартов.

Для рассмотрения многосторонних аспектов безопасности необходимо установить структуру и архитектуру, которые будут предусматривать общую лексику для обсуждения понятий.

В разделе 2 представлены основные архитектуры и элементы безопасности, которые определены в Рекомендациях МСЭ-Т, и восемь параметров безопасности, разработанных для решения проблемы сквозной безопасности в сетевых приложениях – секретность, конфиденциальность данных, аутентификация, целостность данных, сохранность информации, управление доступом, безопасность связи и готовность. Эти общие принципы используются как основа для многих других стандартов в отношении других услуг и механизмов безопасности.

В разделе 3 вводятся ключевые понятия, связанные с безопасностью, а именно, угрозы, уязвимые элементы и риски, а также объясняется взаимосвязь между этими понятиями и их значимость для органов, устанавливающих стандарты.

В разделе 4 на основе информации, содержащейся в предыдущих разделах, определяются требования в отношении безопасности сетей электросвязи. В частности, в этом разделе рассматриваются цели, для которых обеспечивается безопасность сетей электросвязи, и услуги, которыми можно воспользоваться для достижения этих целей.

В разделе 5 вводятся важные понятия инфраструктур открытого ключа и управления полномочиями. Эти инфраструктуры и лежащие в их основе механизмы особенно важны в обеспечении услуг по аутентификации и авторизации.

МСЭ-Т разрабатывает положения по безопасности для ряда систем и услуг, которые определяются в его Рекомендациях, и, как следует из раздела 6, большое внимание в настоящем Руководстве уделяется приложениям. К ним относятся голосовые и мультимедийные приложения на основе IP (H.323 и IPCablecom), приложения в области здравоохранения и для факсимильной передачи. Эти приложения описаны в аспекте 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 по безопасности, учитывающие аспекты управления сетью.

В разделе 7 рассматриваются аспекты готовности и безопасности инфраструктуры. Эти два аспекта относятся к ключевым сферам компетенции МСЭ-Т, хотя не всегда они расцениваются как факторы обеспечения безопасности. В этом разделе приводится информация о расчетах готовности и способах ее укрепления в транспортной сети. В заключительной части раздела содержатся руководящие указания относительно защиты линейных сооружений.

В разделе 8 изложены руководящие принципы, недавно утвержденные МСЭ-Т, относительно организации мер по устранению аварии и управления ситуацией в случае нарушения безопасности. По общему признанию этот вопрос имеет первостепенное значение, если учесть рост угроз безопасности в инфраструктуре электросвязи и информационных систем.

Кроме этого, в настоящее Руководство включен действующий вариант каталога Рекомендаций МСЭ-Т, касающихся аспектов безопасности; в Приложении A приводится длинный перечень, который еще раз иллюстрирует масштабность проводимой МСЭ-Т работы в области безопасности. В настоящем Руководстве содержится также перечень акронимов и определений, связанных с безопасностью и другими вопросами, которые рассматриваются в настоящем документе. Этот перечень составлен на основе соответствующих Рекомендаций МСЭ-Т и иных источников (таких как терминологическая база данных МСЭ-Т SANCHO и Справочник по утвержденным МСЭ-Т определениям терминов в области безопасности, который был подготовлен 17-й Исследовательской комиссией МСЭ-Т). Перечень приводится в Приложении B. В Приложении C мы представили резюме связанной с безопасностью деятельности, осуществляемой каждой из исследовательских комиссий МСЭ-Т. Содержание указанных приложений постоянно обновляется и размещается на веб-сайте по адресу: www.itu.int/ITU-T.

В заключение отметим, что проактивная деятельность МСЭ-Т ведется не только в области технологий, базирующихся на IP, но и направлена на удовлетворение потребностей многочисленных 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 приводится обзор проблемы безопасности в области электросвязи и информационных технологий, освещаются практические вопросы и показано, как МСЭ-Т решает различные задачи обеспечения безопасности в современных приложениях. Руководство носит учебный характер: в нем собраны воедино соответствующие материалы по безопасности из Рекомендаций МСЭ-Т и объясняется взаимосвязь между ними. В Руководстве рассматриваются дополнительные аспекты безопасности и, в частности, касающиеся готовности, по которым МСЭ-Т может предложить обширную информацию, а также проблемы, связанные с экологическим ущербом, решением которых также активно занимается МСЭ-Т. Кроме того, в нем отражены результаты стандартизации в области безопасности, которые были получены со времени выпуска второго издания. Представленные здесь аспекты отражают уже проведенную работу, а те аспекты, по которым работа еще не закончена, будут рассмотрены в последующих изданиях настоящего Руководства.

Руководство адресовано, в частности, инженерам и менеджерам по продукту, студентам и научному сообществу, а также сотрудникам регуляторных органов, стремящимся более глубоко разобраться в вопросах безопасности для применяемых на практике приложений.

2 Базовые архитектуры и услуги обеспечения безопасности

В ходе работы по стандартизации связи, проводившейся в начале 1980-х годов, была признана необходимость в разработке элементов архитектуры безопасности. Это привело к созданию архитектуры безопасности для взаимосвязи открытых систем (Рек. МСЭ-Т X.800). Однако было признано также, что это всего лишь первый этап в разработке набора стандартов для услуг и механизмов обеспечения безопасности. В результате этой работы, основная часть которой была проведена совместно с МОС, были разработаны последующие рекомендации, в том числе относительно моделей и структур безопасности, в которых указано, какие конкретные виды защиты можно применять в конкретных ситуациях. Кроме того, была выявлена необходимость в других архитектурах безопасности, таких как архитектуры безопасности для открытой распределенной обработки и для систем, обеспечивающих сквозную связь. Эта проблема рассматривается в недавно опубликованной Рекомендации X.805 МСЭ-Т, которая дополняет другие Рекомендации серии X.800, предлагая решения в области защиты, нацеленные на обеспечение сквозной защиты сети.

2.1 Архитектура безопасности для взаимосвязи открытых систем (Рек. X.800)

Первая из архитектур безопасности связи была стандартизирована в Рек. МСЭ-Т X.800 "Архитектура защиты для взаимосвязи открытых систем". В этой Рекомендации определяются общие архитектурные элементы, связанные с безопасностью, которые могут применяться в соответствии с обстоятельствами, требующими защиты. В частности, в Рек. X.800 содержится общее описание услуг обеспечения безопасности и соответствующих механизмов, которые могут использоваться для оказания этих услуг. В ней определяется также, в отношении базовой эталонной модели взаимосвязи открытых систем (OSI) с семью уровнями, наиболее пригодное расположение для оказания услуг обеспечения безопасности.

Рек. МСЭ-Т X.800 касается только тех видимых аспектов канала связи, которые позволяют оконечным системам добиться безопасной передачи информации между ними. Она не является какой-либо спецификацией по реализации систем и не служит основой для оценки соответствия реализации тому или иному другому стандарту безопасности. В ней также не указаны сколько-нибудь подробно дополнительные меры защиты, которые могут потребоваться в оконечных системах для обеспечения характеристик защиты OSI.

Хотя Рек. X.800 была разработана специально для архитектуры безопасности OSI, как показала практика, базовые понятия, содержащиеся в Рек. X.800, имеют намного более широкое применение и признание. Предусмотренный стандарт имеет особое значение, поскольку он представляет впервые достигнутое на международном уровне согласие в отношении определения базовых услуг по обеспечению безопасности (*аутентификация*, *управление доступом*, *конфиденциальность данных*, *целостность данных* и *сохранность информации*), наряду с более общими (всеобъемлющими) услугами, такими как *проверенные функциональные возможности*, *обнаружение событий*, а также *проверка безопасности* и *восстановление защиты*. До принятия Рек. X.800 существовал широкий круг представлений о том, какие базовые услуги защиты необходимы и в чем именно должна заключаться каждая услуга. В Рек. X.800 отражено четко согласованная международная позиция в отношении этих услуг. (Более подробно базовые услуги обеспечения безопасности рассматриваются в разделе 2.3.)

Ценность и общая применимость Рек. X.800 основана именно на том, что она отражает единодушие в отношении значений терминов, употребляемых для описания характеристик защиты, набора услуг обеспечения безопасности, которые необходимы для защиты передачи данных, а также характера этих услуг.

В процессе разработки Рек. X.800 была выявлена необходимость в дополнительных стандартах, связанных с безопасностью связи. В результате, после выпуска Рек. X.800 началась работа по разработке ряда вспомогательных стандартов и дополнительных Рекомендаций в области архитектуры. Ниже рассматриваются некоторые из этих Рекомендаций.

2.2 Нижние и верхние уровни моделей безопасности (Рек. X.802 и Рек. X.803)

Цель разработки моделей безопасности на нижних и верхних уровнях (соответственно Рек. X.802 и Рек. X.803) состоит в том, чтобы показать, как концепции безопасности, разработанные в Структурах безопасности, могут быть применены к конкретным областям архитектур для взаимосвязи открытых систем.

Цель модели безопасности на верхних уровнях (Рек. X.803) состоит в том, чтобы обеспечить разработчиков стандартов моделью архитектуры для разработки независящих от приложений услуг и протоколов для безопасности на верхних уровнях модели OSI с семью уровнями. В разделе "Взаимодействие между прикладным уровнем и уровнем представления" содержатся указания относительно расположения услуг безопасности и взаимосвязи между ними. В частности, в этом же разделе Рекомендации описано, как функции преобразования безопасности (такие как шифрация) используются на прикладном уровне и на уровне представления. Кроме того, вводится понятие *обмена безопасности*, а также описаны понятия *стратегии безопасности* и *состояния безопасности*.

Модель безопасности на нижних уровнях (Рек. X.802) содержит указания относительно разработки протоколов для безопасности и элементов протоколов, пригодных для нижних уровней модели OSI. В ней представлена основа для взаимодействия в целях безопасности между нижними уровнями, а также размещения протоколов для безопасности.

2.3 Структуры безопасности (Рек. X.810–X.816)

Структуры безопасности были разработаны с целью обеспечить всеобъемлющее и согласованное описание услуг обеспечения безопасности, указанных в Рек. X.800. Они предназначены для решения всех аспектов вопроса о том, как могут быть применены услуги обеспечения безопасности в контексте конкретной архитектуры защиты, включая возможные будущие архитектуры защиты. Структуры нацелены на обеспечение защиты системных объектов внутри систем и на взаимодействие между системами. Они не предусматривают методику построения систем или механизмов.

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

2.3.1 Обзор структуры безопасности (Рек. X.810)

В обзоре структуры безопасности представлены различные структуры и описаны общие понятия, включая домены безопасности, ответственный объект и политику защиты, которые используются во всех структурах. В нем также описан формат общих данных, который может быть использован для безопасной передачи информации как в аспекте аутентификации, так и в аспекте управления доступом.

2.3.2 Структура аутентификации (Рек. X.811)

Аутентификация – это обеспечение гарантии заявленной подлинности объекта. Объектами могут быть не только физические лица, но и устройства, услуги и приложения. Аутентификация может также гарантировать, что объект не пытается выдать себя за другой объект или несанкционированным образом воспроизвести предыдущее сообщение. В Рек. X.800 определены два вида аутентификации: *аутентификация отправителя данных* (т. е. удостоверение того, что источником полученных данных является заявленный источник) и *аутентификация равноправного объекта* (т. е. удостоверение того, что равноправным объектом в ассоциации защиты является заявленный объект).

Структура аутентификации занимает одно из первых мест в иерархии стандартов аутентификации, которые предусматривают понятия, номенклатуру и классификацию методов аутентификации. Эта структура: определяет основные понятия аутентификации; устанавливает возможные классы механизма аутентификации; определяет услуги для этих классов механизма аутентификации; устанавливает функциональные требования для протоколов поддержки этих классов аутентификации; и устанавливает требования по общему управлению аутентификацией.

Аутентификация, как правило, следует за идентификацией. Информация, используемая для идентификации, аутентификации и авторизации, должна быть защищена.

2.3.3 Структура управления доступом (Рек. X.812)

Управление доступом – это предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным образом. Управление доступом гарантирует, что доступ к элементам сети, хранимой информации, информационным потокам, услугам и приложениям имеет только уполномоченный персонал или допущенные устройства.

Структура управления доступом описывает модель, которая включает все аспекты управления доступом в открытых системах, взаимосвязи с другими функциями обеспечения безопасности (такими как аутентификация и проверка), а также эксплуатационные требования в отношении управления доступом.

2.3.4 Структура сохранности информации (Рек. X.813)

Сохранность информации – это способность не допустить, чтобы объекты впоследствии отказались от того, что они выполнили действия. Сохранность информации связана с установлением доказательств, которые впоследствии могут быть использованы для опровержения ложных утверждений. В Рек. X.800 предусмотрены две формы услуги по сохранности информации – *сохранность информации с доказательством доставки*, которое используется для опровержения ложного отказа получателя признать, что данные были получены, и *сохранность информации с доказательством происхождения*, которое используется для опровержения ложного отказа отправителя признать, что данные были отправлены. Однако в более широком смысле понятие сохранности информации может применяться во многих других контекстах, включая сохранность в контенте создания, представления, хранения, передачи и получения данных.

Структура сохранности информации расширяет понятия услуг по обеспечению сохранности информации, как они описаны в Рек. X.800, и предусматривает основу для развития этих услуг. Она также устанавливает возможные механизмы поддержки этих услуг и общие эксплуатационные требования в отношении сохранности информации.

2.3.5 Структура обеспечения конфиденциальности (Рек. X.814)

Конфиденциальность – это характеристика, которая делает информацию недоступной или не раскрываемой для неуполномоченных лиц, объектов или процессов.

Цель услуги обеспечения конфиденциальности состоит в том, чтобы защитить информацию от несанкционированного раскрытия. Структура обеспечения конфиденциальности относится к конфиденциальности информации при поиске, передаче и управлении; она определяет основные понятия конфиденциальности, устанавливает возможные классы механизмов обеспечения конфиденциальности и средства, необходимые для каждого класса этих механизмов, устанавливает процесс управления и необходимые вспомогательные услуги, а также направляет взаимодействие с другими услугами и механизмами обеспечения безопасности.

2.3.6 Структура обеспечения целостности (Рек. X.815)

Целостность данных – это характеристика, которая свидетельствует о том, что данные не были изменены несанкционированным образом. В общем смысле услуга по обеспечению целостности состоит в необходимости гарантировать, что данные не были искажены, или что, в случае искажения, пользователь узнает об этом. Хотя существуют различные аспекты целостности (такие как целостность данных и целостность системы), в Рек. X.800 рассматривается практически только целостность данных.

Структура целостности относится к целостности данных при поиске и передаче информации, а также управлении ею. Она определяет основные понятия целостности, устанавливает возможные классы механизма обеспечения целостности и средства для каждого класса такого механизма, устанавливает

процесс управления, необходимый для поддержки класса механизма, и направляет взаимодействие механизма обеспечения целостности и вспомогательных услуг с другими услугами и механизмами обеспечения безопасности.

2.3.7 Структура проверки безопасности и аварийных извещений (Рек. X.816)

Проверка безопасности – это независимый просмотр и изучение системных записей и действий с целью определения адекватности средств управления системой, обеспечения соответствия с установленной политикой и оперативными процедурами, обнаружения нарушений защиты и представления рекомендаций относительно каких-либо обозначенных изменений в управлении, политике и процедурах *Аварийное извещение* – это сообщение, которое направляется, если обнаружено связанное с безопасностью событие, которое согласно политике в области безопасности определено как тревожная ситуация.

Структура проверки и аварийного извещения определяет основные понятия и предусматривает общую модель проверки безопасности и аварийных извещений, устанавливает критерии для проверки безопасности и направления аварийного извещения, определяет возможные классы проверки и механизмов направления аварийных извещений, определяет услуги для этих классов механизмов, устанавливает функциональные требования для поддержки этих механизмов, а также общие эксплуатационные требования в отношении проверки безопасности и аварийных извещений.

2.4 Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами (Рек. X.805)

Недавно появился новый подход к архитектуре безопасности сетей. В результате была разработана Рек. МСЭ-Т X.805, в которой определена архитектура сквозной сетевой защиты. Эта архитектура может применяться к различным видам сетей, если сквозная защита представляет собой проблему независимо от технологии сети. 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.

Эта архитектура безопасности определяется двумя основными понятиями: слой и плоскость. Первая составляющая – слои безопасности – касается требований, которые применимы к сетевым элементам и системам, образующим сквозную сеть. При распределении требований по слоям применяется иерархический подход в целях достижения сквозной защиты 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 по различным приложениям для обеспечения сквозной защиты. Уязвимые элементы на каждом слое различны, и, следовательно, меры противодействия должны определяться исходя из потребностей каждого слоя. Слой инфраструктуры состоит из сетевых средств передачи данных, а также из отдельных сетевых элементов. Примерами элементов, относящихся к слою инфраструктуры, являются маршрутизаторы, коммутаторы и серверы, а также каналы связи между ними. Слой услуг относится к безопасности предлагаемых потребителям сетевых услуг. Они составляют широкий диапазон – от услуг базового подключения, таких как услуги выделенных каналов, до дополнительных услуг, таких как немедленная передача текстовых сообщений. Слой приложений касается требований к сетевым приложениям, используемым потребителями. Приложения могут быть простыми, как электронная почта, или сложными, как групповая визуализация, когда сверхвысокопроизводительные передатчики видеоинформации используются для ведения нефтепоисковых работ или проектирования автомобилей и т. д.

Вторая составляющая касается защиты сетевых операций. Эта архитектура безопасности определяет три плоскости безопасности, которые отражают три вида операций, осуществляемых в сети. Плоскостями безопасности являются: 1) плоскость административного управления, 2) плоскость оперативного управления и 3) плоскость конечного пользователя. Эти плоскости безопасности обеспечивают конкретные потребности в защите, которые связаны, соответственно, с управлением сетью, контролем за сетью или сигнальными операциями, а также операциями конечного пользователя. Плоскость административного управления, подробно рассмотренная ниже в пункте 6.4, связана с функциями эксплуатации, администрирования, технического обслуживания и обеспечения (OAM&P), такого как обеспечение пользователя или сети и т. д. Плоскость оперативного управления связана с сигнальными операциями для настройки (и модификации) сквозной связи по сети независимо от среды передачи и технологии, используемой 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 безопасности, разработанных для обеспечения безопасности сети. Эти параметры определяются в нижеследующих разделах. В архитектурном аспекте указанные параметры применяются к каждой ячейке трехрядной квадратной матрицы, образуемой между слоями и плоскостями, с тем чтобы определить надлежащие меры противодействия. На рисунке 2-1 показаны плоскости, слои и параметры архитектуры безопасности. В разделе 6.4, посвященном плоскости административного управления, показано, какой принят подход в других Рекомендациях МСЭ-Т в отношении трех ячеек трехрядной квадратной матрицы для плоскости административного управления.

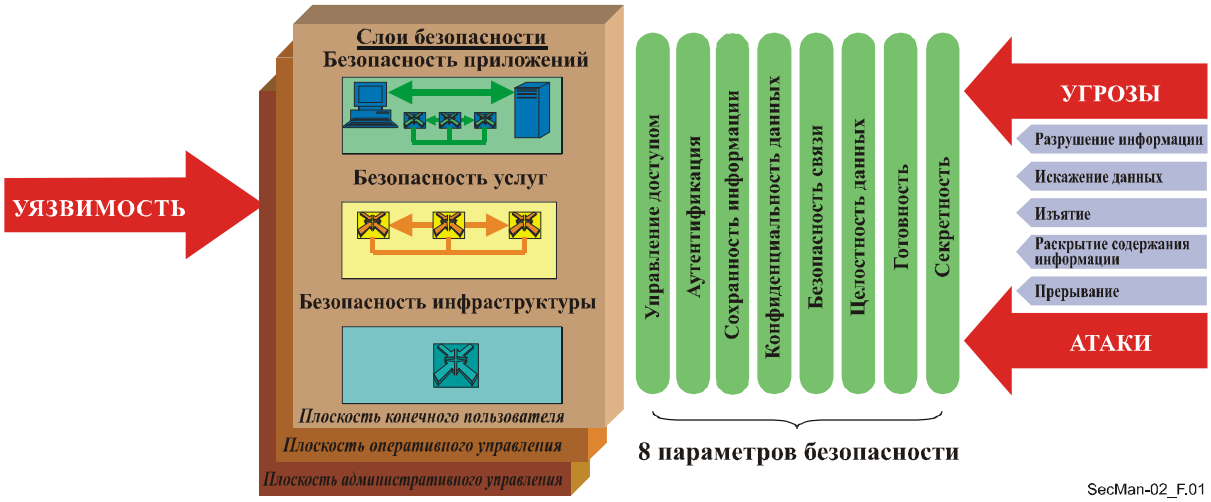


Рисунок 2-1 – Элементы архитектуры безопасности согласно Рек. МСЭ-Т X.805

Рек. X.805 основана на некоторых понятиях, которые установлены в Рек. X.800 и Структурах безопасности (Рек. X.810–X.816), рассмотренных выше. В частности, функциональные характеристики базовых услуг обеспечения безопасности, предусмотренных в Рек. X.800 (*управление доступом*, *аутентификация*, *конфиденциальность данных*, *целостность данных* и *сохранность информации*) согласуются с функциональными характеристиками соответствующих параметров защиты, предусмотренных в Рек. X.805 (как показано на рисунке 2-1). Кроме того, такие параметры безопасности, как *безопасность связи*, *готовность* и *секретность*, предусмотренные в Рек. X.805, обеспечивают новые виды защиты сети. Эти восемь параметров безопасности рассматриваются ниже.

– *Управление доступом* как параметр безопасности обеспечивает защиту от несанкционированного использования ресурсов сети. Управление доступом гарантирует, что только уполномоченный персонал или уполномоченные устройства будут допущены к сетевым элементам, хранимой информации, информационным потокам, услугам и приложениям.

– *Аутентификация* как параметр безопасности служит для подтверждения идентичности объектов связи. Аутентификация гарантирует достоверность заявленной идентичности объектов, участвующих в связи (например, физического лица, устройства, услуги или применения), а также гарантирует, что объект не пытается выдать себя за другой объект или воспроизвести несанкционированным образом предыдущее сообщение.

– *Сохранность информации* как параметр безопасности обеспечивает средства для предотвращения отрицания физическим лицом или объектом факта совершения им конкретного действия в отношении данных посредством предъявления имеющегося доказательства различных действий, связанных с сетью (таких как доказательство обязательства, намерения или совершения; доказательство происхождения данных, доказательство права собственности, доказательство использования источника). Этот параметр обеспечивает наличие доказательств, которые могут быть предъявлены третьему лицу и использоваться в подтверждение того, что произошло какое-либо событие или совершено какое-либо действие.

– Конфиденциальность данных как параметр безопасности обеспечивает защиту данных от несанкционированного раскрытия. Этот параметр гарантирует, что содержание данных не будет понято неуполномоченными объектами. Для обеспечения конфиденциальности данных используются, как правило, такие методы, как шифрование, списки управления доступом и право на доступ к файлу.

– Безопасность связи как параметр безопасности гарантирует, что информация передается только между уполномоченными конечными точками (информация не изменяет направления и не перехватывается при передаче между этими конечными точками).

– Целостность данных как параметр безопасности обеспечивает правильность и точность данных. Данные защищены от несанкционированного изменения, удаления, создания и дублирования, а также обеспечивается указание на такие несанкционированные операции.

– Готовность как параметр безопасности обеспечивает, что вследствие влияющих на сеть событий не возникнет отказа в санкционированном доступе к элементам сети, хранимой информации, потокам данных, услугам и приложениям. В эту категорию включены варианты восстановления после аварий.

– Секретность как параметр безопасности предусматривает защиту информации, которая могла бы быть получена на основе наблюдения за сетевыми операциями. Примерами такой информации являются веб-сайты, которые посетил пользователь, географическое расположение пользователя, IP-адреса и имена DNS в сети поставщика услуг.

Архитектура безопасности, предусмотренная в Рек. X.805, может служить указанием для разработки всеобъемлющей политики в области безопасности, планов реагирования на инциденты и восстановления, а также технологических архитектур с учетом каждого параметра безопасности на каждом слое и в каждой плоскости безопасности на стадии определения и планирования. Архитектура безопасности, предусмотренная в Рек. X.805, может также быть использована как основа для анализа безопасности, в рамках которого следует изучить вопрос о том, как осуществление программы защиты отражает параметры, плоскости и слои безопасности при внедрении методик и процедур и размещении технологий. После введения программы безопасности ее следует обновлять, с тем чтобы она соответствовала постоянно меняющимся средствам защиты. Эта архитектура безопасности может помочь в управлении методами и процедурами обеспечения безопасности, планами реагирования на инциденты и восстановления, а также технологическими архитектурами, обеспечивая учет каждого параметра безопасности на каждом слое и в каждой плоскости безопасности при внесении изменений в программу безопасности.

3 Основные понятия безопасности: угрозы, уязвимые элементы и риски

При разработке структуры безопасности любого вида очень важно иметь четкое представление о том, какие ресурсы нуждаются в защите, от каких угроз необходимо защитить эти ресурсы, каковы уязвимые элементы, связанные с этими ресурсами, и общие риски, которым эти угрозы и уязвимые элементы подвергают ресурсы.

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

– услуги в области связи и компьютерных операций;

– информация и данные, включая программное обеспечение и данные, относящиеся к услугам обеспечения безопасности; и

– оборудование и средства.

Согласно Рек. X.800 *угроза безопасности* – это потенциальное нарушение безопасности. Примерами угроз являются:

– несанкционированное раскрытие информации;

– несанкционированное разрушение или изменение данных, оборудования или других ресурсов;

– кража, удаление или потеря информации или других ресурсов;

– прерывание обслуживания или отказ в обслуживании; и

– выдача себя за допущенный объект.

Угрозы бывают *случайными* или *умышленными* и могут быть *активными* или *пассивными*. Случайная угроза – это угроза без какого-либо преднамеренного умысла, как, например, ошибка в системе или программе или физический сбой оборудования. Умышленная угроза – это угроза, которая реализуется неким объектом, совершающим преднамеренное действие. (Если реализуется умышленная угроза, она называется *атакой*). Активная угроза – это угроза, которая приводит к некоторому изменению состояния, такому как изменение данных или разрушение оборудования. Пассивная угроза не приводит к изменению состояния. Примером пассивной угрозы является перехват информации.

Уязвимость защиты представляет собой результат ошибки или дефекта, которыми можно воспользоваться с целью нарушения системы или содержащейся в ней информации (Рек. X.800). Уязвимость позволяет реализовать угрозу.

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

Риск нарушения безопасности представляет собой показатель негативных последствий, которые могут наступить, если воспользоваться уязвимостью защиты, т. е. если будет реализована угроза. Хотя риск невозможно полностью устранить, одной из целей защиты является уменьшение риска до приемлемого уровня. Для этого необходимо понять угрозы и уязвимые элементы и принять надлежащие меры противодействия (т. е. применить услуги и механизмы защиты).

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

Организации по стандартизации несут ответственность и имеют уникальную возможность для решения проблемы уязвимости защиты, которая может быть заложена в технических характеристиках, таких как архитектуры, структуры и протоколы. Даже при надлежащей осведомленности относительно рисков уязвимые элементы и угрозы, связанные с обработкой информации и сетями связи, невозможно обеспечить адекватную защиту без систематического применения защиты в соответствии с установленной политикой, которую необходимо периодически пересматривать и обновлять. Кроме того, следует надлежащим образом обеспечить управление мерами безопасности и обработку инцидентов. Это включает установление ответственности и конкретных действий в отношении предотвращения или устранения последствий любого инцидента в области безопасности (необходимые положения, механизмы контроля, меры противодействия, гарантии или действия). В настоящее время МСЭ-Т работает над новыми рекомендациями, которые будут охватывать эти аспекты управления безопасностью.

4 Требования к безопасности сетей электросвязи

В данном разделе приводятся основные соображения в отношении необходимости определения элементов безопасности и их характеристик с точки зрения пользователей, в том числе операторов сетей электросвязи. Эти соображения вытекают из требований, выраженных различными участниками рынка электросвязи. Основное внимание в данном разделе уделяется работе, проделанной после принятия Рек. МСЭ-Т Е.408 "*Требования к безопасности сетей электросвязи*". В этой Рекомендации содержится обзор требований к безопасности и структура, которая опознает угрозы безопасности сетей электросвязи в общем виде (как для фиксированной, так и для подвижной связи; как для голосовой связи, так и для передачи данных), а также приводится руководство по планированию мер противодействия, которые могут быть приняты для уменьшения рисков, создаваемых угрозами.

Рекомендация носит общий характер и не устанавливает и не рассматривает конкретных требований для конкретных сетей.

В ней рассматриваются не какие-либо новые услуги обеспечения безопасности, а использование существующих услуг, которые определены в других Рекомендациях МСЭ-Т и соответствующих стандартах, установленных другими организациями.

Выполнение данных требований будет способствовать международному сотрудничеству в следующих областях, связанных с безопасностью сетей электросвязи:

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

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

4.1 Обоснование

Требования к общей структуре сетевой безопасности для международной электросвязи обусловлены совокупностью различных факторов:

- *Потребителям*/*абонентам* необходимо испытывать доверие к сети и предлагаемым услугам, включая готовность услуг (особенно экстренного обслуживания) в условиях крупных катастроф (включая гражданские акции с применением насилия).
- *Общественность* и *органы власти* требуют закрепления мер защиты в директивах и законодательстве, 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 клиентами и населением на национальном и международном уровнях

Требования к безопасности сетей электросвязи должны базироваться преимущественно на согласованных на международном уровне стандартах безопасности, поскольку выгоднее использовать уже существующие, чем разрабатывать новые. Расходы на обеспечение и использование услуг и механизмов безопасности могут быть довольно значительными в сравнении со стоимостью защищаемых транзакций. Поэтому важно иметь возможность определить параметры безопасности в соответствии с услугами, подлежащими защите. Используемые услуги и механизмы 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.

Стандартизация будет способствовать *повторному применению решений и продуктов*, а это значит, что меры безопасности могут внедряться более оперативно и с меньшими затратами.

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

Необходимо предоставлять услуги и механизмы обеспечения безопасности, которые защищают 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 поступления сообщений), отрицание факта получения или отправления или фальсификация. Защита включает предупреждение, обнаружение и восстановление после атаки, а также управление информацией, касающейся безопасности. Защита должна также включать меры по предотвращению прерываний в обслуживании вследствие природных явлений (погодные условия и т. д.) или злонамеренных атак (насильственных действий). Следует предусмотреть возможность подслушивания или наблюдения по просьбе надлежащим образом уполномоченных правоохранительных органов.

4.2 Общие задачи безопасности для сетей электросвязи

В данном разделе описана конечная цель мер безопасности, используемых в сетях электросвязи, и главное внимание уделяется тому, на что направлены требования в отношении безопасности, а не тому, как этого добиться.

Задачи безопасности для сетей электросвязи состоят в следующем:

a) Только уполномоченные пользователи должны иметь доступ к сетям электросвязи и возможность их использования.

b) Уполномоченные пользователи должны обладать доступом к ресурсам, в отношении которых им предоставлен доступ, и возможностью работать с ними.

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

d) Все пользователи должны нести ответственность за свои и только свои действия в сетях электросвязи.

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

f) Следует обеспечить возможность извлечения информации, связанной с безопасностью, из сетей электросвязи (но только уполномоченные пользователи должны иметь возможность извлечения такой информации).

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

h) По обнаружении преодоления защиты необходимо иметь возможность восстановления нормальных уровней защиты.

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

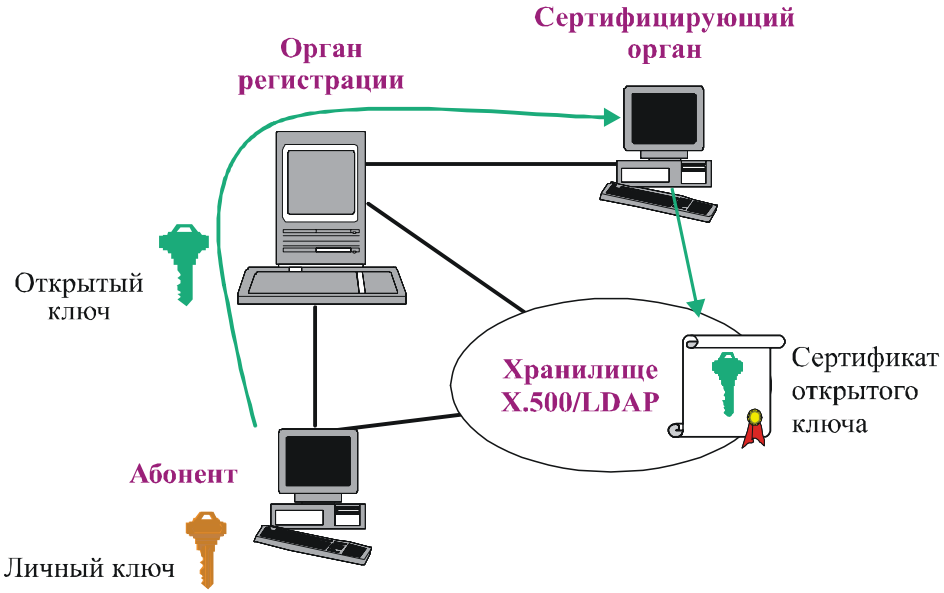
Термин "доступ к ресурсам" следует понимать как возможность не только выполнения функций, но и чтения информации.

Можно продемонстрировать, что при осуществлении следующих мер безопасности возможно выполнение первых пяти из вышеуказанных задач безопасности сетей электросвязи:

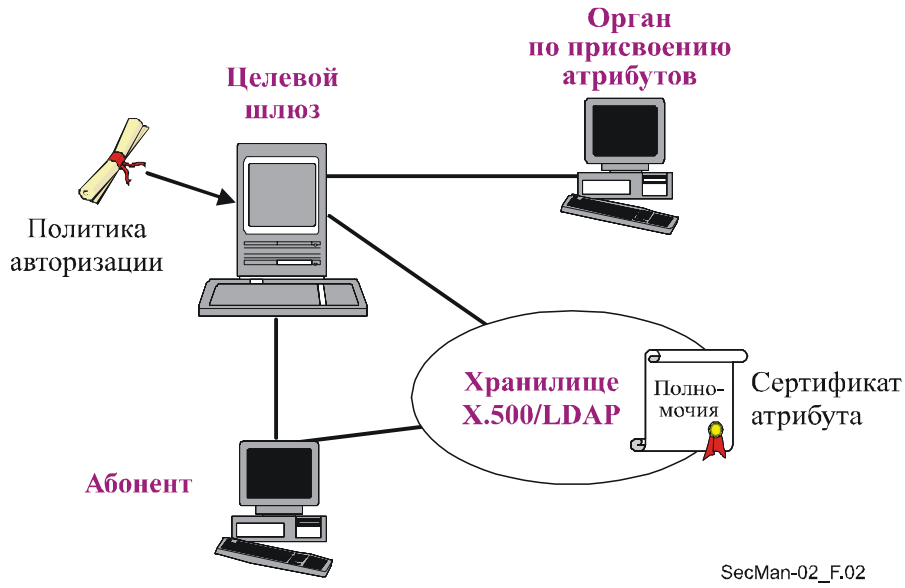
- конфиденциальность;
- целостность данных (безусловно, требуется также обеспечение целостности системных программ);
- отчетность, включая аутентификацию, сохранность информации и управление доступом; и
- готовность.

5 Инфраструктуры открытого ключа и управления полномочиями

В Рек. МСЭ-Т X.509 "*Справочник: Структуры сертификатов открытых ключей и атрибутов*" представлен стандарт инфраструктуры открытого ключа для точной аутентификации, основанной на сертификатах открытого ключа и полномочиях на сертификацию. PKI обеспечивает управление открытыми ключами в целях услуг по обеспечению аутентификации, шифрования, целостности данных и сохранности информации. Базовой технологией PKI является шифрование с открытым ключом, которое описано ниже. Помимо определения структуры аутентификации для PKI в Рек. X.509 предусмотрена также инфраструктура управления полномочиями (PMI), которая используется для определения прав и полномочий пользователей в контексте точной аутентификации на основе сертификатов атрибута и полномочий в отношении атрибута. Компоненты PKI и PMI представлены на рисунке 5-1.



(a) Компоненты инфраструктуры с открытым ключом



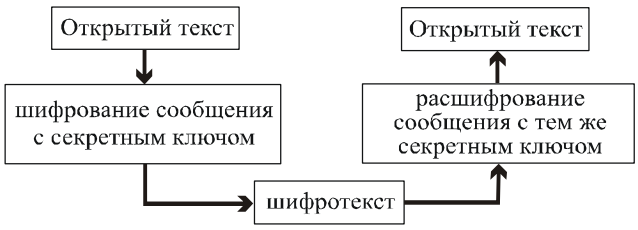
(b) Компоненты инфраструктуры управления полномочиями

Рисунок 5-1 – Компоненты PKI и PMI

5.1 Шифрование с секретным и с открытым ключом

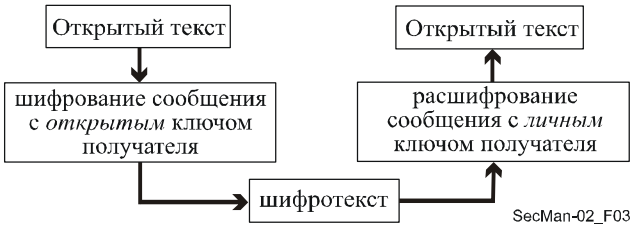
Симметричное (или *с секретным ключом*) шифрование относится к криптографической системе, в которой для шифрования и дешифрования используются один и тот же ключ, как показано на рисунке 5-2a). Симметричные криптосистемы требуют начальных договоренностей, с тем чтобы лица совместно пользовались уникальным секретным ключом. Ключ должен быть распространен среди соответствующих лиц с помощью надежных средств, поскольку знание ключа шифрования подразумевает знание ключа дешифрования, и наоборот.

При асимметричном (или *с открытым ключом*) шифровании используется пара ключей, как показано на рисунке 5-2b): открытый ключ и личный ключ. Открытые ключи могут распространяться широко, а личный ключ всегда хранится в секрете. Обычно личный ключ хранится на карточке со встроенной микросхемой или на аутентификационном маркере). Открытый ключ формируется из личного ключа, и, хотя эти ключи математически связаны, не существует какого-либо реального способа повернуть процесс в обратную сторону и вывести личный ключ из открытого ключа. Для того чтобы отправить кому-либо конфиденциальные данные с надежным использованием шифра ключа, отправитель шифрует данные с помощью открытого ключа получателя. Получатель дешифруют их с помощью своего соответствующего личного ключа. Шифрование с открытым ключом может также использоваться для применения цифровой подписи к данным с целью подтверждения, что документ или сообщение исходит от лица, которое выдает себя за отправителя (или автора). На самом деле цифровая подпись представляет собой дайджест данных, которые порождаются с помощью личного ключа подписавшегося лица, и добавляется к документу или сообщению. Получатель использует открытый ключ подписавшегося лица с целью подтверждения подлинности цифровой подписи. (ПРИМЕЧАНИЕ. – Некоторые системы открытого ключа используют две пары открытого и личного ключа – одну для шифрования/дешифрования, а другую для цифровой подписи/проверки).



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

(a) Шифрование с симметричным (или секретным) ключом



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

(b) Шифрование с асимметричным (или открытым) ключом

Рисунок 5-2 – Схема процессов шифрования с симметричным (или секретным) и асимметричным (или открытым) ключами и их особенности

При симметричном шифровании каждая пара пользователей должна иметь свою собственную пару ключей, отличных от других, и эти ключи следует распределить и держать в секрете. С другой стороны, при асимметричном шифровании открытые ключи шифрования могут быть опубликованы в каталоге, и каждый сможет пользоваться одним и тем же (открытым) ключом шифрования для отправления данных конкретному пользователю. Это делает асимметричное шифрование более масштабируемым по сравнению с симметричным шифрованием. Однако асимметричное шифрование является дорогостоящим за счет времени вычисления, и поэтому неэффективно шифровать целые сообщения, используя асимметричное шифрование. Вследствие этого асимметричное шифрование обычно применяется для обмена симметричными ключами, которые затем используются для шифрования текстовой части сообщения с помощью симметричного алгоритма, являющегося более экономным в аспекте вычисления. Если необходима цифровая подпись, 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.

Следует отметить, что, независимо от применения симметричного или асимметричного шифрования, невозможно маршрутизировать сообщения их получателям, если сообщение зашифровано целиком, поскольку промежуточные узлы будут не в состоянии установить адрес получателя. Поэтому заголовки сообщений должны быть, как правило, незашифрованными.

Безопасная работа системы открытого ключа во многом зависит от действительности открытых ключей. Обычно открытые ключи публикуются в форме цифровых сертификатов, которые содержатся в каталоге X.500. В сертификате указывается не только открытый ключ шифрования и, в соответствующих случаях, ключ проверки подписи для лица, но и дополнительная информация, в том числе о подлинности сертификата. Сертификаты, аннулированные по какой-либо причине, обычно перечисляются в каталоге в списке аннулирования сертификатов (CRL). Прежде чем воспользоваться открытыми ключами, обычно проверяется их действительность в CRL.

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 Рек. МСЭ-Т 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 срока 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. После этого сертификат X.509 может быть опубликован без ограничений, например на веб-сайте, в директории LDAP или в V-карте, присоединяемой к сообщениям электронной почты. Подпись CA гарантирует, что его содержание не может быть изменено без обнаружения.

Для того чтобы обеспечить возможность подтверждения подлинности сертификата отрытого ключа пользователя, необходимо иметь доступ к действительному открытому ключу того CA, который выдал сертификат, с целью проверки подписи CA на сертификате. Открытый ключ CA может быть сертифицирован другим (вышестоящим) CA, в результате чего подлинность открытых ключей может подтверждаться цепочкой сертификатов. В итоге эта цепочка должна иметь некую конечную точку, где, как правило, находится сертификат CA, являющегося "корнем доверия". Открытые ключи корневого CA распространяются как подписанные им самим сертификаты (в которых корневой CA удостоверяет, что данный ключ является его собственным открытым ключом). Эта подпись позволяет убедиться в том, что ключ и наименование CA не подделывались с момента создания сертификата. Однако мы не можем безоговорочно принять наименование CA, заключенное в подписанном им самим сертификате, поскольку CA сам вставил наименование в сертификат. Таким образом, одним из важнейших компонентов инфраструктуры открытого ключа является метод безопасного распространения открытых ключей корневых CA (как подписанных ими самими 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 пар ключей, создание сертификатов открытых ключей, аннулирование сертификатов открытых ключей (например, если личный ключ пользователя подвергся опасности), хранение и архивирование ключей и сертификатов, а также их уничтожение по истечении срока службы. Каждый CA функционирует в соответствии с набором стратегических процедур, а в Рек. МСЭ-Т X.509 предусмотрены механизмы для распространения некоторой части информации об этой стратегии в полях расширения сертификатов X.509, выданных данным CA. Стратегические правила и процедуры, которым следует CA, обычно определяются в стратегии применения сертификатов (CP) и в заявлении о практике применения сертификатов (CPS), публикуемых этим CA. Указанные документы способствуют обеспечению общей основы для оценки того, насколько можно доверять сертификатам открытых ключей, выданным этим CA, как на международном уровне, так и на уровне секторов. Эти документы также обеспечивают правовую основу (частично), необходимую для укрепления доверия между учреждениями, 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. Обмен сертификатами открытых ключей сам по себе не защищает от опасных атак при вмешательстве извне (типа "человек-посредник").

5.4 Инфраструктура управления полномочиями

В первых версиях Рек. МСЭ-Т X.509 (1988 г., 1993 г. и 1997 г.) "*Справочник: структура аутентификации*" содержалось описание базовых элементов, необходимых для инфраструктур открытых ключей (PKI). К ним относилось определение сертификатов открытых ключей. Пересмотренное издание Рек. МСЭ-Т X.509, которое было утверждено в 2000 году, содержит существенно расширенные характеристики сертификатов атрибута и основу для инфраструктуры управления полномочиями (PMI). (PMI управляет полномочиями в целях содействия всеобъемлющей службе авторизации в связи с PKI). Описанные механизмы позволяют осуществлять установку полномочий пользователя в отношении доступа в среде, объединяющей оборудование различных производителей и многочисленные приложения.

Концепции PMI и PKI весьма сходны, но PMI относится к авторизации, а область действия PKI – аутентификация. На рисунке 5-1 и в таблице 5-1 показано сходство двух инфраструктур.

ТАБЛИЦА 5-1

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 том, чтобы обеспечить выполнение ими предписанной стратегии безопасности, которую установил источник полномочий. Информация, касающаяся стратегии, увязывается с именем пользователя в сертификате атрибута и состоит из ряда элементов, показанных на рисунке 5-3.

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

Рисунок 5-3 – Структура сертификата атрибута согласно Рек. X.509

Для управления PMI в Рек. МСЭ-Т X.509 описаны пять компонентов: контролер полномочий, верификатор полномочий, объектный метод[1], стратегия присвоения полномочий и переменные среды (см. рисунок 5-4). Эти компоненты позволяют верификатору полномочий управлять доступом к объектному методу с помощью контролера полномочий в соответствии со стратегией предоставления полномочий.

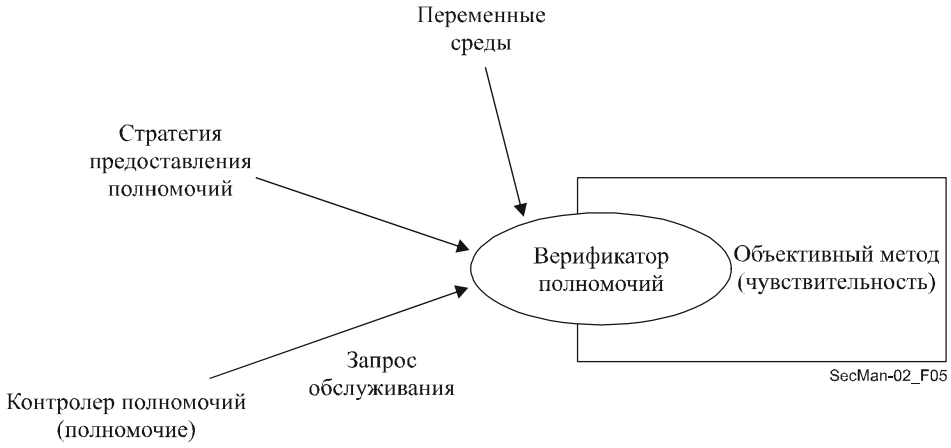


Рисунок 5-4 – Модель управления PMI согласно Рек. МСЭ-Т X.509

Если для какой-либо реализации необходимо делегирование полномочий, в Рек. МСЭ-Т X.509 рассмотрены четыре компонента модели делегирования для PMI: верификатор полномочий, источник полномочий, другие органы по присвоению атрибутов и контролер полномочий (см. рисунок 5-5).

[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 5-5 – Модель делегирования для PMI согласно Рек. МСЭ-Т X.509

В последних реализациях схем авторизации, которые соответствуют модели управления доступом по ролевому признаку (RBAC), предполагается, что конкретному пользователю присваивается некая роль. Стратегия авторизации связывает набор разрешений и роль. При доступе к ресурсу роль, которая присвоена пользователю, сверяется с правилами стратегии для получения разрешения на выполнение каких-либо последующих действий. 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 голос по протоколу IP (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 конечного пользователя приложения – система IPCablecom, которая предоставляет в реальном масштабе времени базирующиеся на IP услуги по кабельным сетям, и передача факсимильных сообщений. Рассмотрены также приложения, не относящиеся исключительно к отрасли электросвязи, а именно, приложения в области электронного здравоохранения и, в частности, система электронных рецептов. Ко второму классу относятся приложения, предназначенные для управления сетью. Важным аспектом 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

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

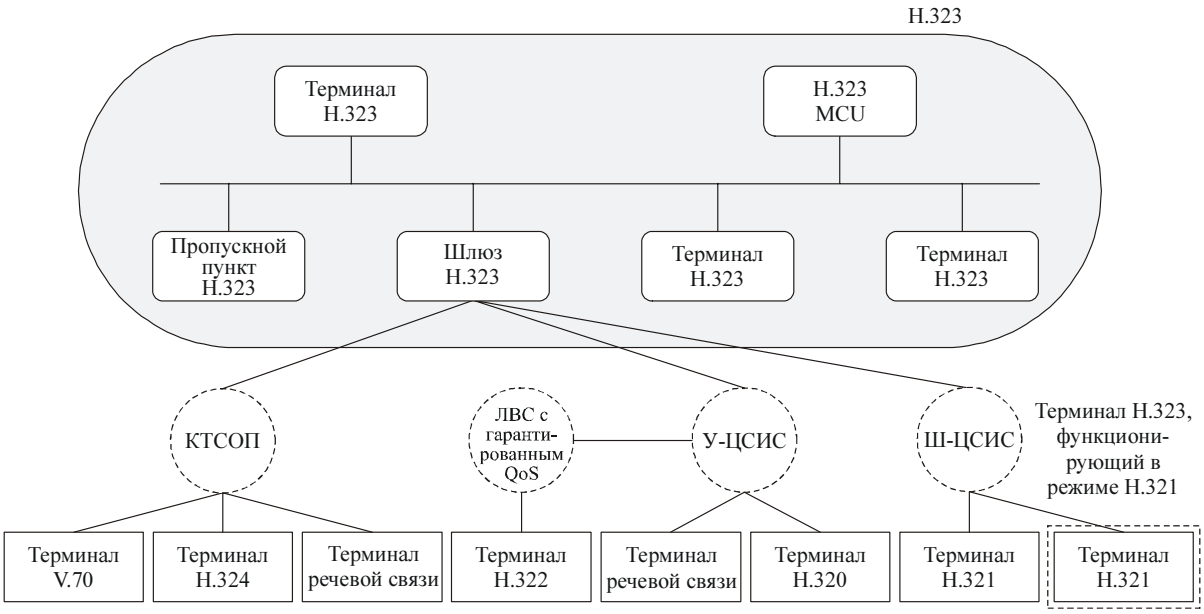
H.323 является "зонтичной" Рекомендацией МСЭ-Т, формирующей основу для передачи звуковых сигналов, видеоряда и данных по сетям с коммутацией пакетов данных, включая интернет, локальные вычислительные сети (ЛВС) и региональные распределенные сети (WAN), которые не обеспечивают гарантированного качества обслуживания (QoS). Эти сети доминируют в современных корпоративных настольных системах и включают сетевые технологии с коммутацией пакетов TCP/IP и IPX по Ethernet, Fast Ethernet и Token Ring. При условии соответствия положениям H.323 мультимедийные продукты и приложения различных производителей могут быть функционально совместимыми и таким образом обеспечивать пользователям возможность связи без проблем совместимости. H.323 был первым получившим определение протоколом VoIP и считается основой для функционирующих в среде VoIP продуктов, применяемых в сферах торговли, коммерческой деятельности, обслуживания, индустрии развлечений и профессиональных приложений. Ниже указаны важные Рекомендации, составляющие части системы H.323.

- 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.x – Безопасность для систем на базе H.323.
- H.246 – Межсетевое взаимодействие с КТСОП.
- 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 Рекомендации H.323 в 1996 году. Версия 2 была утверждена в январе 1998 года, а действующая версия 6 утверждена в 2006 году. 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 различными сетями.

H.323 является частью крупной серии стандартов связи, обеспечивающих возможность организации видеоконференций в рамках широкого диапазона сетей. Известная как H.32x, эта серия Рекомендаций включает H.320 и H.324, в которых рассматриваются, соответственно, связь по ЦСИС и КТСОП. 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 6-1.



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

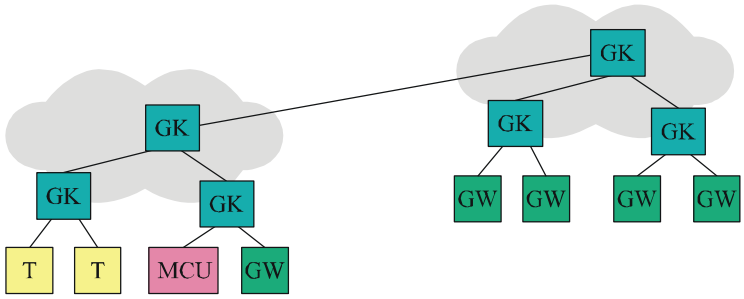
(b) Система H.323: компоненты и сценарии развертывания [Euchner]

Рисунок 6-1 – Система H.323: компоненты и сценарии развертывания

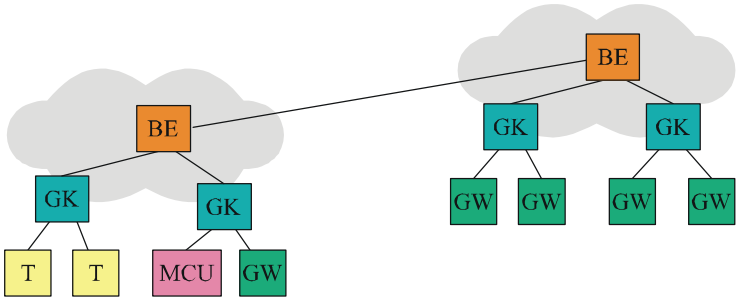
Терминалы (T) – это клиентские конечные точки на IP магистрали, которые обеспечивают двунаправленную связь. Терминалы H.323 должны поддерживать передачу речи и могут поддерживать видеокодеки, протоколы многоадресной передачи данных T.120 и возможности MCU. Примеры: IP телефоны, видеофоны, инфракрасные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

Шлюз (GW) выполняет множество функций, наиболее распространенной из которых является функция трансляции между конечными точками конференции H.323 и другими типами терминалов. Эта функция включает преобразование форматов передачи (например, H.225.0 в H.221) и трансляцию процедур связи (например, H.245 в H.242). Наряду с этим шлюз также осуществляет преобразования между аудио- и видеокодеками, осуществляет установку и разъединение соединения как на стороне сети с коммутацией пакетов, так и на стороне сети с коммутацией каналов.

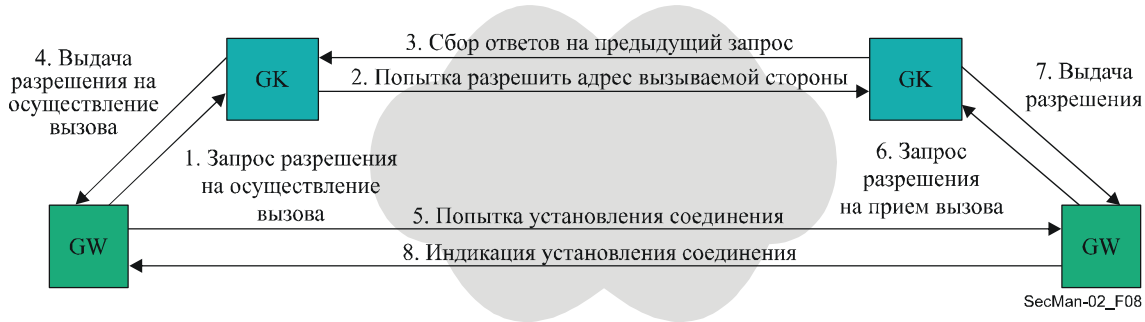
Пропускной пункт (GK) является одним из важнейших компонентов сети, функционирующей в соответствии с H.323. Он действует как центральная точка для всех соединений в своей зоне и предоставляет услуги по управлению установлением соединения для зарегистрированных конечных точек. Во многих случаях пропускной 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 направить сигнализацию о соединении через себя для выполнения таких функций, как следящая переадресация/поиск, переадресация по сигналу "занято" и т. д. С пропускными пунктами связаны *пограничные* (или равноправные) *элементы (BE)*, которые отвечают за обмен адресной информацией и участвуют в авторизации вызова между административными доменами или внутри них. Их функции также обеспечивают взаимосвязь между различными "группами" или сетями H.323. Это осуществляется путем обмена серией сообщений, как показано на рисунке 6-2.



(a) Топология с применением протокола RAS



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



(c) Поток сообщений высокого уровня при установлении соединения

Пояснения к рисунку: BE – пограничный элемент; GK – пропускной пункт; GW – шлюз; MCU – многоточечный блок управления; T – терминал; RAS – протокол регистрации, вхождения и состояния

Рисунок 6-2 – Связь между административными доменами

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.

Находящиеся в эксплуатации сети H.323 переносят каждый месяц миллиарды минут речевого и видеотрафика; 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 масштабируемость и соответствие потребностям как поставщиков услуг, так и промышленных предприятий, обеспечив широчайший диапазон продуктов от стеков и чипов до радиотелефонов и оборудования видеоконференц-связи.

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 веб-вызовы;
- поддержка факсимильной связи, передачи текста по IP 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; и
- поддержка сигнализации при экстренном обслуживании.

Примерами применения H.323 являются оптовый транзит, выполняемый операторами, особенно для магистралей VoIP (сравнимыми с коммутаторами 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, телефон–ПК и ПК–ПК; оно может также использоваться для доставки 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 6-3.

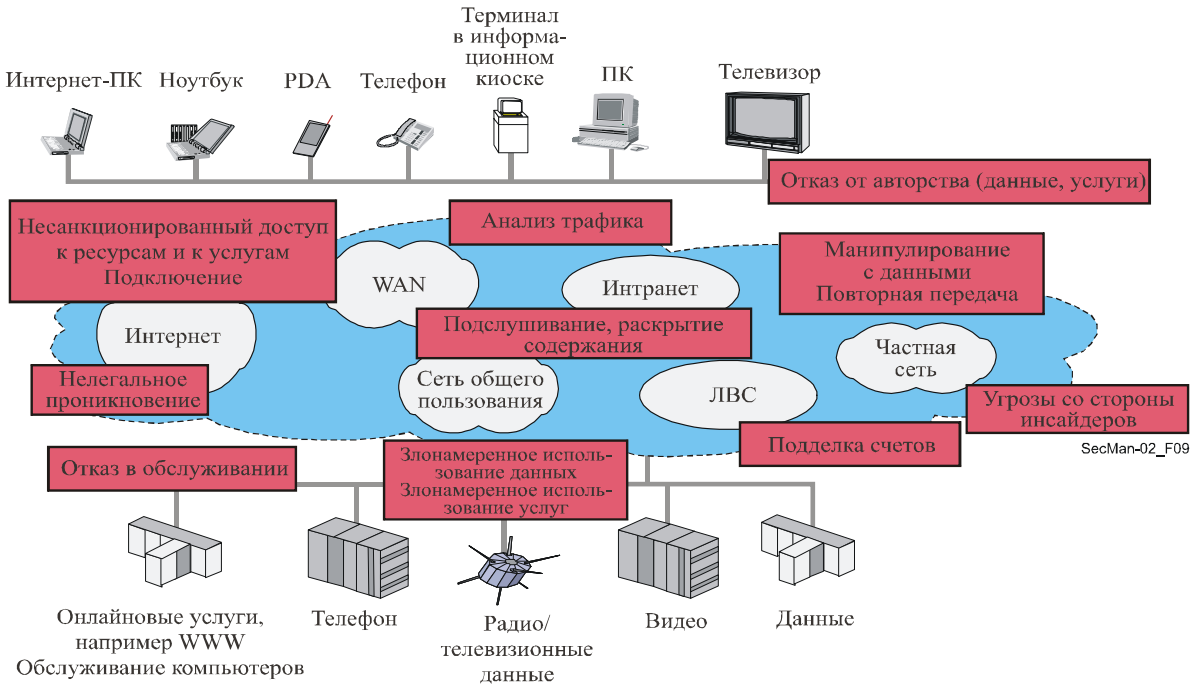


Рисунок 6-3 – Угрозы безопасности в среде мультимедийной связи

Основные вопросы обеспечения безопасности в среде мультимедийной связи и IP-телефонии дополнительно описаны ниже [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 КТСОП), или ресурсов сети (QoS, полоса пропускания, кодеки и т. д.). Как правило, функции аутентификации и авторизации выполняются вместе, с тем чтобы выполнить решение о предоставлении доступа. Аутентификация и авторизация помогают срывать такие атаки, как нелегальное проникновение, злонамеренное использование и подлог, манипулирование и отказ в обслуживании.
- Защита безопасности сигнализации 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, т. е. 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 Обзор Рекомендаций подсерии H.235x

Для мультимедийной системы H.323 в Рек. МСЭ-Т H.235.0 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. С тех пор 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. H.235.0–H.235.9 в версии 4 представляют собой действующую серию Рекомендацией МСЭ-Т в области безопасности для систем на базе H.323, которые обеспечивают масштабируемую защиту как для небольших групп, предприятий, так и для крупных операторов.

В бывшей версии 3 Рек. МСЭ-Т H.235 была в значительной мере изменена структура всех ее частей и приложений, которые стали составлять полный набор отдельных Рекомендаций подсерии H.235.x, в которой Рек. H.235.0 называется "Структура безопасности для мультимедийных систем, основанных на стандартах серии H (H.323 и других, основанных на H.245)". Эта Рекомендация содержит обзор стандартов подсерии H.235.x и предусматривает общие процедуры с базовым текстом.

Говоря кратко, Рекомендации МСЭ-Т подсерии H.235.x предусматривают 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 (т. е. MCU), когда в рамках одной группы осуществляется связь между несколькими мультимедийными терминалами.

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 6-4 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 сохранности информации. Пропускные пункты осуществляют аутентификацию путем управления разрешениями в конечных точках и обеспечивают механизмы поддержания сохранности информации. Безопасность транспортного и более низких уровней, базирующихся на IP, выходит за 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 при желании для конфиденциальности (т. е. 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.

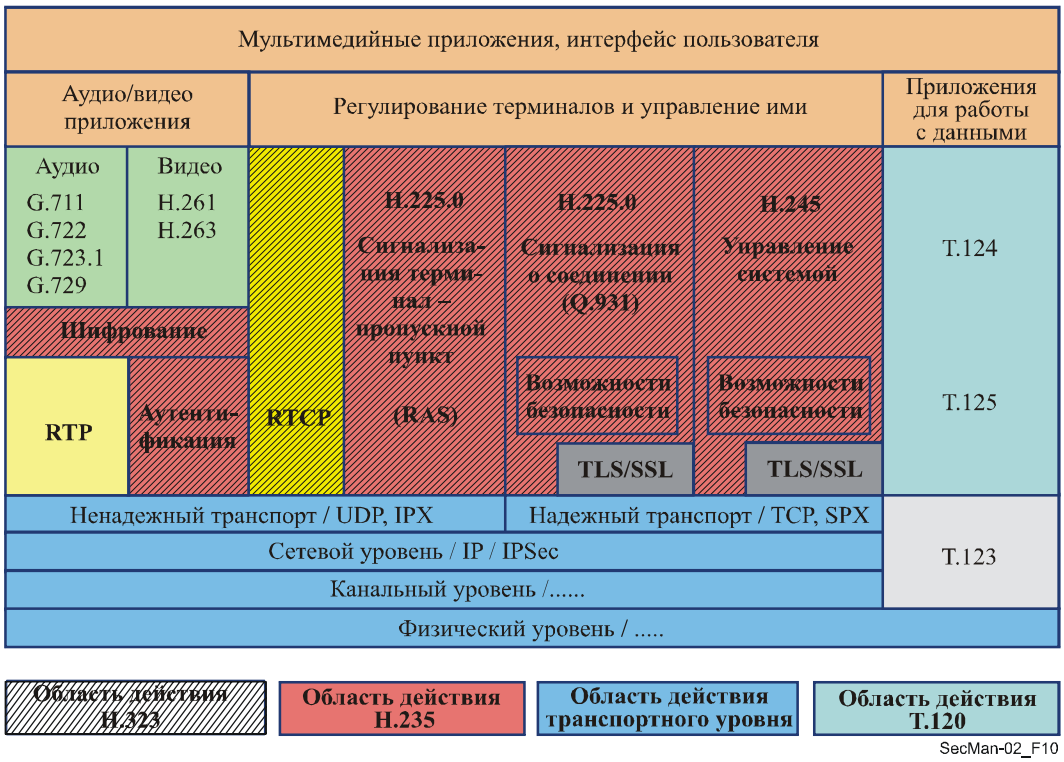


Рисунок 6-4 – Безопасность в H.323 в соответствии с H.235 [Euchner]

Рекомендации МСЭ-Т серии H.235.x охватывают 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, такие как простые конечные точки или интеллектуальные конечные точки, H.235.x предоставляет набор соответствующим образом параметризованных и совмещающихся профилей безопасности для конкретных сценариев. Имеющиеся профили безопасности определяют методы безопасности, диапазон которых простирается от простых профилей с общим секретным ключом и защищенным паролем (H.235.1 для аутентификации и целостности сообщений в отношении сигнализации о соединении согласно P.225.0) до более сложных профилей с цифровыми подписями и сертификатами PKI в соответствии с X.509 (H.235.2). Это позволяет реализовывать как межсегментную защиту с использованием более простых, но менее масштабируемых методов, так и сквозную защиту с использованием масштабируемых возможностей на базе PKI. H.235.3 называют гибридным профилем защиты, поскольку в этой Рекомендации сочетается симметричные процедуры безопасности, предусмотренные в H.235.1, с использованием сертификатов на базе PKI и подписи согласно H.235.2, и тем самым достигаются оптимальные результаты и более короткое время соединения. Кроме того, H.235.3 открывает возможность для оптимального осуществления насыщенных вычислениями операций в функциональном процессоре системы безопасности, основанном на сетевом посреднике.

Рекомендация H.235.4 под названием "Защита соединения с прямой и селективной маршрутизацией" ослабляет жесткую зависимость от архитектуры, центром которой является сервер, с пропускными пунктами-маршрутизаторами и предоставляет меры защиты, направленные на обеспечение безопасности модели одноранговой сети. В этой Рекомендации определяются процедуры управления ключами в корпоративной и междоменной связи. В частности, H.235.4 охватывает указанные сценарии, когда пропускной пункт выполняет прямую маршрутизацию или когда пропускной пункт может даже селективно выполнять некоторую маршрутизацию трафика сигнализации о соединении согласно H.225.0.

Если многие профили безопасности в соответствии с H.235 предполагают модель пропускного пункта-маршрутизатора согласно H.323, то H.235.4 больше посвящена защищенной одноранговой связи с целью освобождения соответствующих пропускных пунктов от задач маршрутизации сигнализации согласно H.323 и обеспечения большей масштабируемости и лучших результатов в целом. В H.235.4, предусматривающей поддержку соединений с прямой маршрутизацией, пропускные пункты функционируют преимущественно на местном уровне в пределах своих доменов, с тем чтобы выполнить аутентификацию пользователя/терминала, а также регистрацию, разрешение соединения, определение адресов и регулирование полосы пропускания. С другой стороны, терминалы осуществляют установление соединения напрямую между конечными точками сквозным образом, как показано в сценарии на рисунке 6-5.

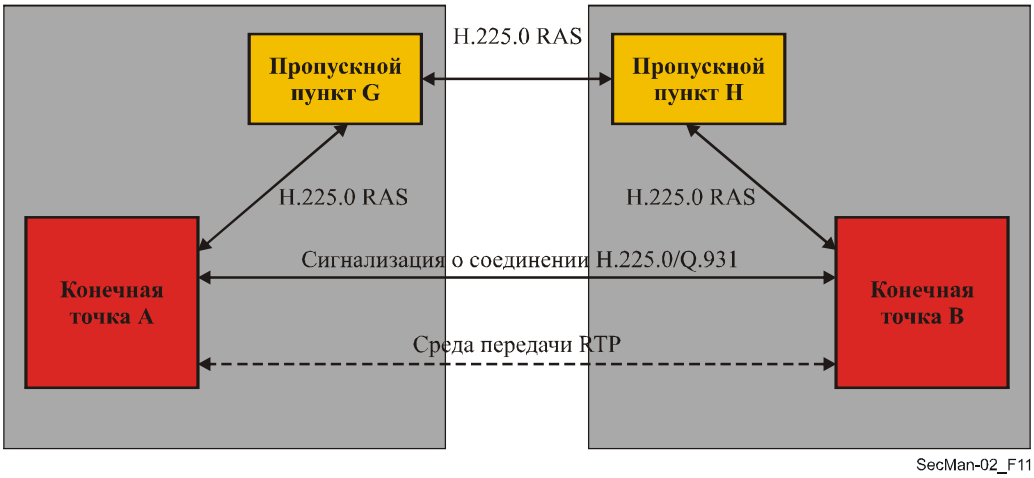


Рисунок 6-5 – Сценарий прямой маршрутизации согласно H.235.4

После того как конечная точка (КТ) "A" просит пропускной пункт "G" разрешить соединение с КТ "B", один пропускной пункт (либо "G" в условиях корпоративной связи, либо "H" в условиях междоменной связи) формирует ключ сигнализации о сквозном соединении для обеих конечных точек – "A" и "B". Практически таким же образом, как и сервер Kerberos (см. приложение в Рек. МСЭ-Т J.191), конечная точка "A" надежно получает сформированный ключ в рамках одного маркера защиты, при этом получая другой маркер защиты с тем же ключом для конечной точки "B". Во время соединения КТ "A", с одной стороны, напрямую применяет ключ для защиты сигнализации о соединении в направлении КТ "B", но, с другой стороны, также воспроизводит другой маркер защиты с ключом в направлении КТ "B". H.235.4 способна использовать профили безопасности H.235.1 или H.235.3.

Дополнительное процедурное обеспечение междоменных сценариев в H.235.4 позволяет различать случаи, когда конечные точки или пропускные пункты не содействуют возможности для соглашения о ключах Diffie-Hellman; и все-таки в итоге конечным точкам "A" и "B" обеспечивается секретность совместного сеанса, которая предоставляет сквозную защиту сигнализации H.323 в аспекте аутентификации, целостности или конфиденциальности.

В целях обеспечения более сильной защиты систем, использующих персональные идентификационные номера (PIN) или пароли для аутентификации пользователей H.235.5 предусматривает другую *структуру для надежной аутентификации в RAS с использованием слабо зашифрованных совместных секретных ключей* с помощью применения методов открытых ключей для надежного использования PIN/паролей. В настоящее время определен один конкретный профиль, в котором применяется метод обмена зашифрованными ключами для согласования хорошо зашифрованного общего секретного ключа, который защищен от пассивных или активных (типа "человек-посредник") атак. Структура позволяет определить новые профили с использованием других методов согласования на основе открытых ключей.

В Рек. МСЭ-Т H.235.6 под названием "*Профиль шифрования речи с управлением внутренним ключом H.235/H.245*" собраны все процедуры, необходимые для шифрования потока данных RTP, включая сопровождающее управление ключами, которое полностью выражено в полях сигнализации H.245.

В интересах более полной конвергенции с SIP и SRTP Рек. МСЭ-Т H.235.7 под названием "*Использование протокола управления ключами MIKEY для защищенного протокола реального масштаба времени (SRTP) в рамках H.235*" применяет защищенный протокол реального масштаба времени (SRTP, RFC 3711) в рамках H.235. В этой Рекомендации указано, как использовать управление ключами IETF MIKEY в рамках H.235.7 для распределения ключей в сквозной среде SRTP.

Другой, дополнительный подход предусмотрен в Рек. H.235.8 "*Обмен ключами для SRTP с использованием защищенных каналов сигнализации*", задача которого состоит в том, чтобы сигнализировать параметры ввода ключа для SRTP в нешифрованной сквозной связи при условии наличия некоторого защищенного средства передачи данных.

Вопрос о том, как позволить сигнализации H.323 пересечь NAT (трансляцию сетевых адресов) и FW (межсетевое устройство защиты), давно является крупной проблемой размещения на практике. В Рек. МСЭ-Т H.235.9 "*Поддержка H.323 с помощью шлюза безопасности*" рассмотрены процедуры безопасности, которые позволяют конечной точке/терминалу H.323 обнаружить шлюзы безопасности H.323, при этом предполагается, что такой объект охватывает функциональность шлюза прикладного уровня (ALG) NAT/FW H.323. Предполагаемый защищенный шлюз сигнализации H.323 обнаруживает осуществляемые транзакции по сигнализации и вовлекается в процесс управления ключами для сигнализации H.225.0.

Наряду с тем, что H.235.0 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 Рек. МСЭ-Т H.530, в которой рассматриваются следующие аспекты безопасности:

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

На рисунке 6-6 показан базовый сценарий, который рассматривается в H.530, когда мобильный терминал (MT) H.323 может подключиться либо напрямую к своему базовому домену через базовый пропускной пункт (H-GK), либо к любому внешнему пропускному пункте (V-GK) в посещаемом домене. Поскольку мобильный терминал и пользователь неизвестны посещаемому домену, посещаемый пропускной пункт прежде всего должен запросить функцию аутентификации (AuF) в базовом домене, где приписан и известен MT. Таким образом, посещаемый домен делегирует задачу аутентификации функции аутентификации в базовом домене и позволяет этой функции выполнить аутентификацию и принять на основании нее решение. Кроме того, функция аутентификации обеспечивает V-GK криптографическую привязку MT и динамический ключ для V-GK с использованием встроенного криптографического протокола безопасности в рамках H.530. Функция аутентификации надежно сообщает свое решение посещаемому контрольному пункту, которое выполняется на стадии регистрации терминала.

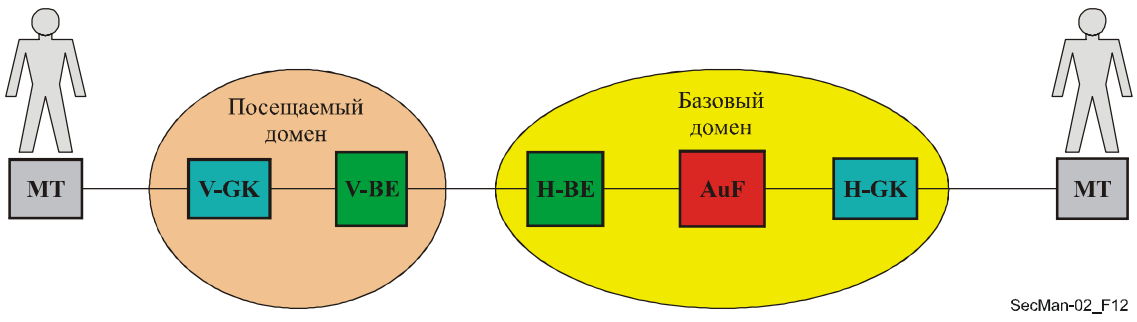


Рисунок 6-6 – Сценарий H.530

Связь между посещаемым доменом и базовым доменом использует общий протокол H.501 для управления мобильной связью на базе H.323 и связи внутри домена и между доменами. По получении от AuF решения об аутентификации и авторизации посещаемый пропускной пункт и MT согласовывают новый ключ для динамического связывания, которым они совместно пользуются в течение действия их ассоциации безопасности. Этот ключ связывания используются для защиты любой дополнительной сигнальной связи H.323 между MT и V-GK; мультимедийная сигнальная связь осуществляется на местном уровне в адрес посещаемого домена и не требует взаимодействия с базовым доменом.

В H.530 учитывается весьма упрощенная архитектура безопасности, когда MT совместно использует только предопределенный общий секретный ключ (например, пароль по абонементу) со своей AuF в базовом домене, но не требуется, чтобы MT совместно использовал какие-либо заранее заданные ассоциации безопасности с любыми посещаемыми доменами. Защиты безопасности между объектами внутри доменов, а также между доменами требует только симметричных совместно используемых секретных ключей; такие ключи могут быть установлены, в частности, посредством согласования на уровне междоменного обслуживания. В H.530 вновь используются существующие профили безопасности H.235, такие как H.235.1 для защиты сигнальных сообщений H.501/H.530 между доменами.

Кроме H.235.0 масштабируемое управление ключами с применением о
(LDAP) и уровня защищенных разъемов (SSL/TLS) обеспечивают H.350 и H.350.2. Рек. 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 предусматривает способ подключения услуг H.323, SIP, H.320 и базовых услуг обмена сообщениями к службе справочников, с тем чтобы к мультимедийной связи можно 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 (соответственно, H.235.1 и протокол HTTP Digest). 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.

6.1.3 H.323 и устройства NAT/FW

Интернет разрабатывался на основе принципа "сквозной" связи. Это означает, что любое устройство в сети может напрямую связываться с любым другим устройством в сети. Однако из-за проблем, связанных с безопасностью и нехваткой сетевых адресов IPv4, межсетевые устройства защиты и устройства для трансляции сетевых адресов (NAT) часто используются на границе сети. Эти границы включают резидентный домен, домен поставщика услуг, домен предприятия и иногда домен страны. В рамках одного домена иногда используется несколько межсетевых устройств защиты или устройств для трансляции сетевых адресов.

Межсетевые устройства защиты предназначены для жесткого контроля за тем, как перемещается информация по границам сети, и обычно они настроены для блокирования большинства сообщений IP. Если межсетевое устройство защиты явно не сконфигурировано таким образом, чтобы позволить пройти трафику H.323 из внешних устройств во внутренние устройства H.323, связь становится просто невозможной. Это вызывает проблему для любого пользователя оборудования H.323.

Устройства NAT транслируют адрес, используемый во внутреннем домене, в адреса, используемые во внешнем домне, и наоборот. Адреса, используемые в резидентном домене или домене предприятия, обычно, но не всегда, выделяются из адресных пространств частной сети, которые определены в RFC 1597. Ими являются:

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

Эти устройства NAT вызывают для большинства протоколов IP еще более серьезную проблему рассогласования. H.323, SIP и другие протоколы связи в реальном масштабе времени, которые функционируют в сетях с коммутацией пакетов, должны предоставлять адрес IP и переносить информацию таким образом, чтобы другие стороны в связи знали, куда направить медиапотоки (например, аудио- и видеопотоки).

МСЭ-Т изучал вопросы, связанные с прохождением через NAT/FW, и разработал серию из трех Рекомендаций для систем H.323, с тем чтобы позволить этим системам "бесшовно" проходить через одно или несколько устройств NAT/FW. Это Рекомендации H.460.17 ("*Использования подключения сигнализации о соединении как транспорта для сообщений RAS H.323*"), H.460.18 ("*Прохождение сигнализации H.323 через трансляторы сетевых адресов и межсетевые устройства защиты*") и H.460.19 ("*Прохождение данных H.323 через трансляторы сетевых адресов и межсетевые устройства защиты*").

Во всех этих Рекомендациях используется структура базовой расширяемости, введенная в версии 4 H.323, и это значит, что любая версия 4 H.323 или устройство более высокого уровня может быть адаптировано с целью поддержки этих процедур прохождения NAT/FW. Кроме того, в H.460.18 предусмотрены способы, позволяющие более старым устройствам, для которых не предназначены эти Рекомендации, надлежащим образом проходить границы NAT/FW с помощью "посредника".

На рисунке 6-7 показано, как специальный "посредник" может быть использован, с тем чтобы помочь устройствам, "не знающим" NAT/FW, надлежащим образом пройти границы этих устройств:

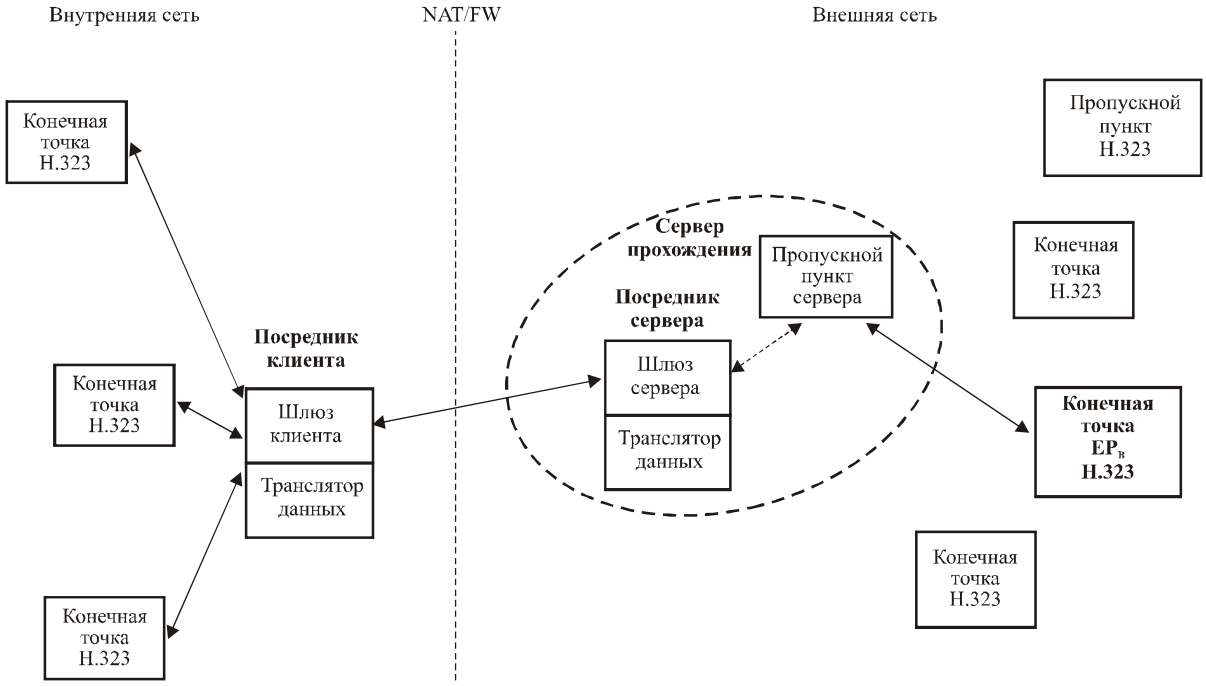


Рисунок 6-7 – Архитектура H.460.18, полностью разобранная реализация

Вышеприведенная топология может также быть целесообразной в случае, когда, например, предприятие желает контролировать маршрут, по которому сигнализация о соединении и данные проходят через сеть. Однако H.460.17 и H.460.18 (в которых рассматриваются сигнальные аспекты прохождения через NAT/FW) позволяют конечным точкам проходить границы NAT/FW без помощи каких-либо специальных внутренних "посредников". На рисунке 6-8 показана одна такая топология:

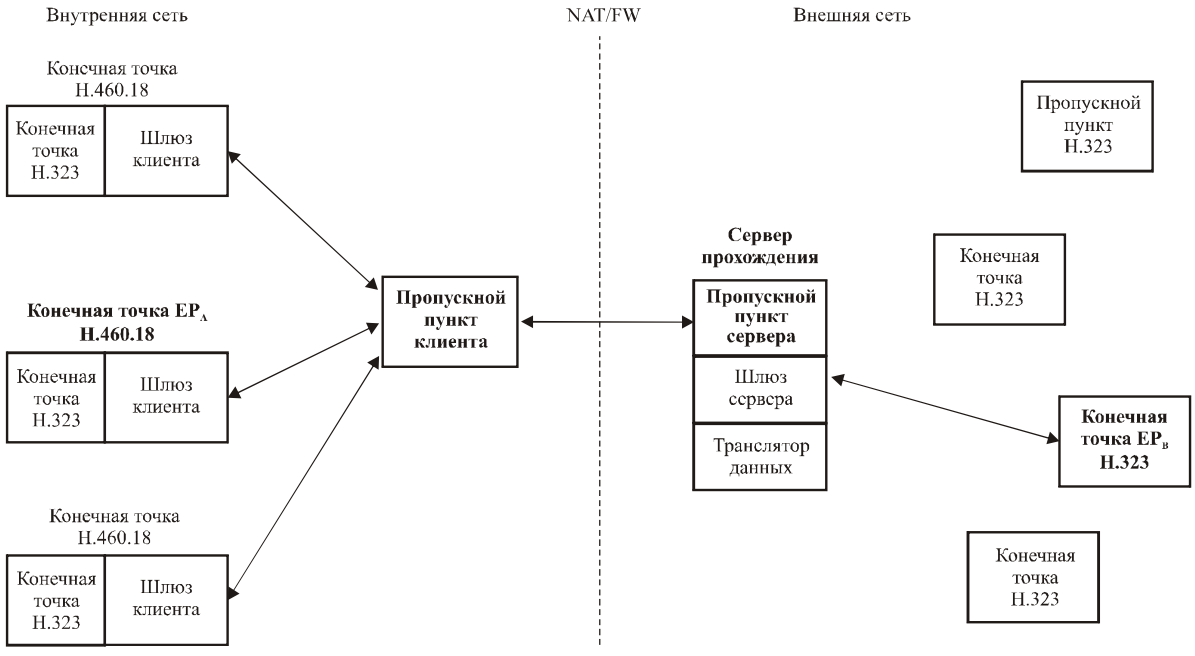


Рисунок 6-8 – Архитектура связи через пропускные пункты

В вышеприведенной топологии на базе H.460.18 конечные точки во внутренней сети связываются с пропускным пунктом, который тоже приписан к внутренней сети для разрешения адреса внешних объектов (например, номера телефона или URL H.323 к адресу IP). Пропускной пункт во внутренней сети связывается с пропускным пунктом во внешней сети для обмена этой информацией об адресах и передает эту информацию обратно вызывающей конечной точке. Когда устройство во внутренней сети помещает вызов на устройство во внешней сети, оно использует процедуры, предусмотренные в H.460.18, для открытия необходимых микроканалов через устройства NAT/FW для получения сигнала от внутренней сети к внешней сети. Кроме того, оно использует процедуры, предусмотренные в H.460.19 для открытия необходимых микроканалов, с тем чтобы позволить потокам надлежащим образом проходить через внутреннюю сеть на внешнюю сеть, и наоборот.

Когда вызывающее и вызываемое устройства приписаны к разным частным сетям, разделенным устройствами NAT/FW и интернетом общего пользования, необходимы по крайней мере один "пропускной пункт сервера" и один "ретранслятор данных" (предусмотренные в H.460.18), с тем чтобы надлежащим образом маршрутизировать сигнализацию и данные между двумя частными сетями. Это сочетание устройств часто называется как "пограничный контроллер сессий". Причина заключается всего лишь в том, что по конструкции не существует способа для вхождения IP пакета внутри одной частной сети в другую частную сеть без помощи какого-то объекта в сети общего пользования, который выполнил бы функцию посредника для этого пакета.

Разумеется, отправление вызова и соединение в пределах одной и той же частной сети, которые в настоящее осуществляются без каких-либо специальных процедур обработки вызовов (H.460.17, H.460.18 и H.460.19, не мешают надлежащей работе устройств H.323 в пределах одной и той же внутренней сети.

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 Рек. МСЭ-Т J.160. На очень высоком уровне архитектура IPCablecom взаимодействует с тремя сетями: "HFC сеть доступа J.112", "управляемая IP-сеть" и КТСОП. 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 КТСОП. На рисунке 6-9 представлена базовая архитектура IPCablecom.

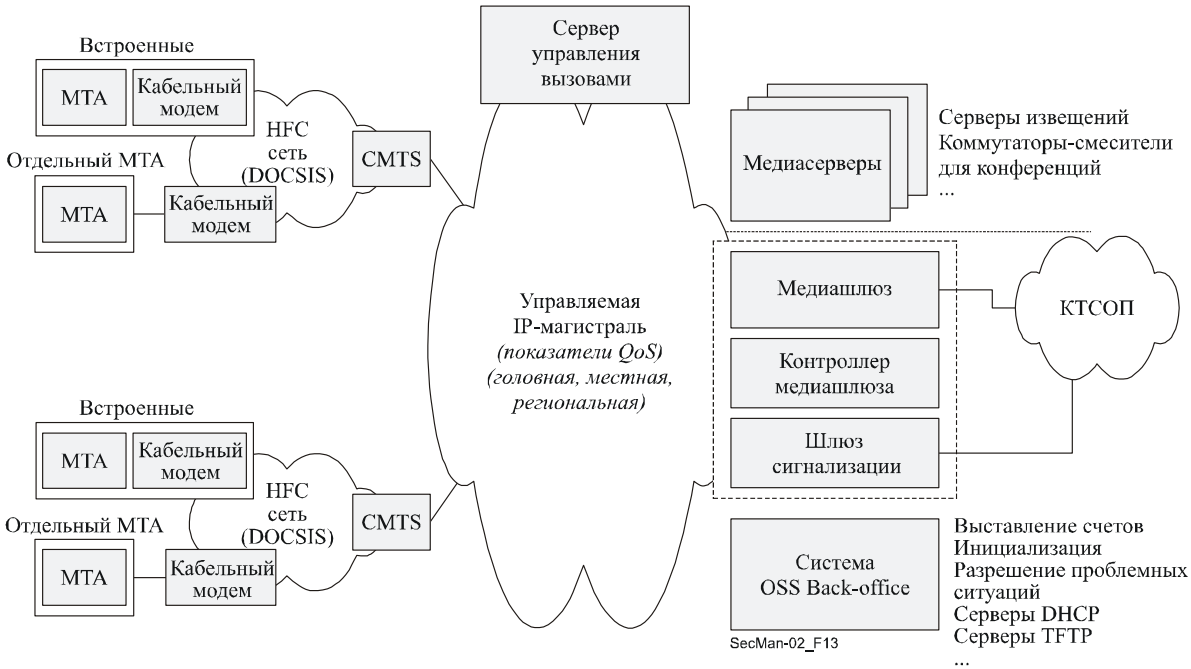


Рисунок 6-9 – Базовая архитектура IPCablecom [J.165]

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 и 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 КТСОП 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 КТСОП. Он поддерживает и контролирует общее состояние вызова для требующих взаимодействия с КТСОП вызовов. *Медиашлюз* (MG) обеспечивает сетевое взаимодействие носителей между КТСОП 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 для угроз, создающих риски безопасности как для абонента, так и для поставщика услуг. Например, медиапоток может проходить через огромное число потенциально неизвестных линий поставщиков услуг интернета и услуг магистралей интернета. 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 2-1. 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 сохранность информации. 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 сохранность информации), 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 6-10 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 6-10 не показаны.

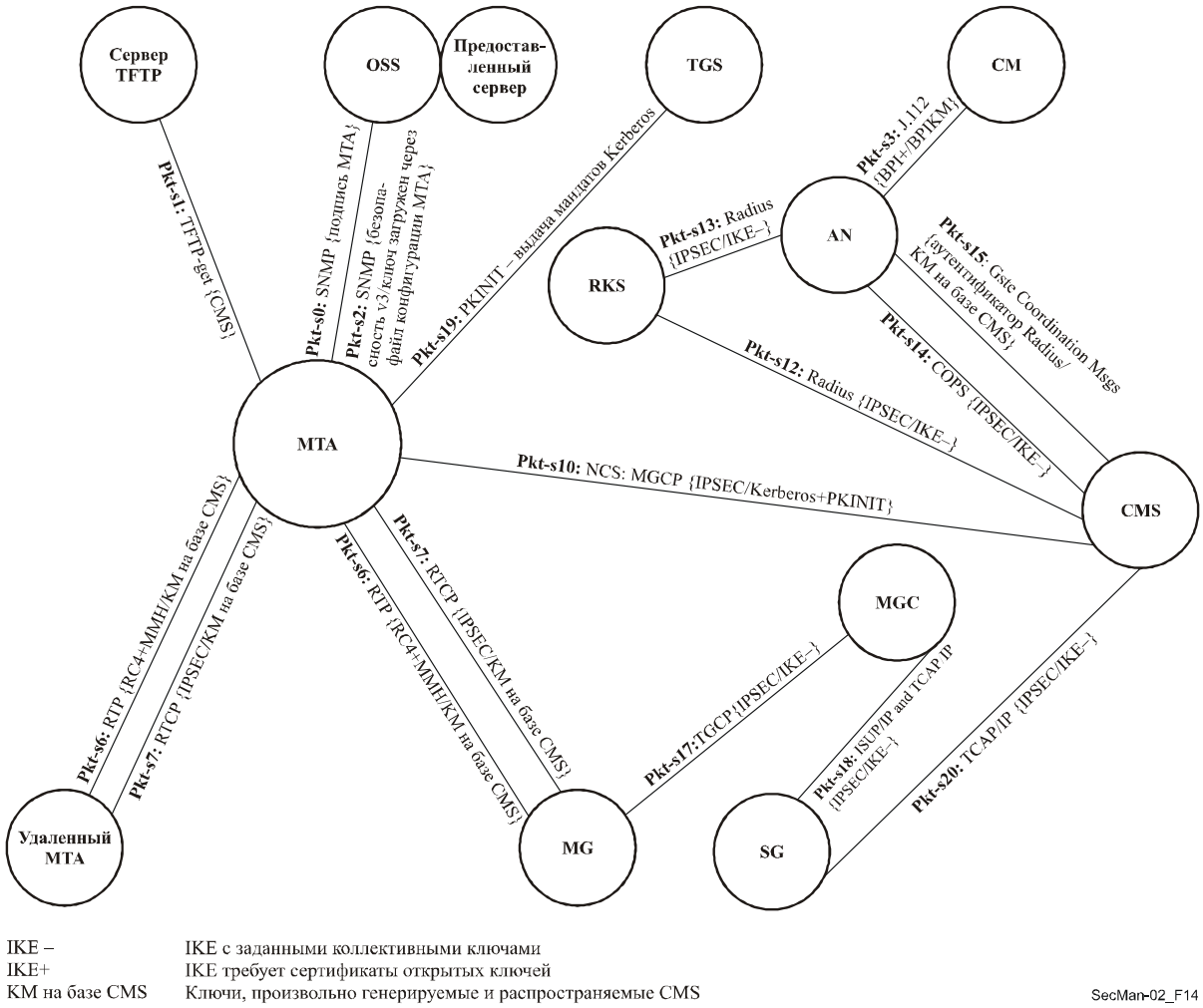


Рисунок 6-10 – Интерфейсы безопасности IPCablecom (обозначение: <метка>: <протокол> { <протокол безопасности> / <протокол управления ключами> })

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 при желании 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 КТСОП, 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.

6.3 Защищенная факсимильная передача

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

В Рек. 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 А) и алгоритме RSA

(T.36, 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 T.36 описано использование системы НКМ 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 T.36 представлены процедуры использования системы шифров несущей HFX40 в целях обеспечения конфиденциальности сообщения для факсимильных терминалов. Наконец, в Приложении E к T.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 T.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 6-1, ниже.

ТАБЛИЦА 6-1

Профили безопасности в Приложении H к T.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 НКМ и HFX

Сочетание систем *управления ключами Hawthorne* (НКМ) 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 НКМ, 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 НКМ 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, определенного в Приложении D к Т.36. В шифре используется 12-разрядный десятичный ключ, который примерно эквивалентен 40-битовому сеансовому ключу.

Целостность документов обеспечивается за счет использования системы, определенной в Приложении E к Т.36, а в Рек. МСЭ-Т Т.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 Т.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, p. 466–474*]. Схема кодирования документа, передаваемого при обеспечении параметров безопасности, может быть любого типа из определенных в Рек. МСЭ-Т Т.4 и Т.30 (модифицированная схема Хаффмана, MR, MMR, символьный режим, как определено в Приложении D к Т.4, BFT, иной режим передачи, определенный в Приложении C к Т.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 к Т.30 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, p. 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 Рек. МСЭ-Т X.509. Средства передачи сертификата открытого ключа отправителя описаны в Приложении H к T.30, 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 допускается 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 Национальным институтом стандартов и технологии (NIST) 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 Рек. МСЭ-Т T.36). В некоторых странах применение этих схем может регулироваться национальными правилами.

Могут также использоваться и другие необязательные алгоритмы. Они выбираются в соответствии с серией ISO/IEC 18033.

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

В соответствии с архитектурой безопасности, рассмотренной в разделе 2.4, обязательным условием является защита трафика в плоскости административного управления. Этот трафик 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 (СУЭ), которая описана в Рек. МСЭ-Т M.3010. СУЭ 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 СУЭ 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

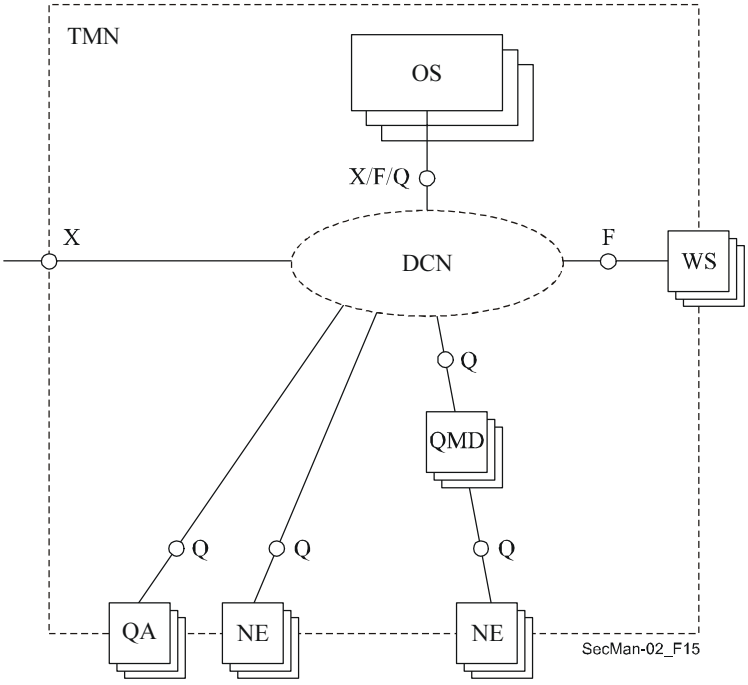
минимизирует затраты за счет необходимости создания только инфраструктуры единой интегрированной сети, он создает множество новых проблем, связанных с обеспечением безопасности. Угрозы в плоскости конечного пользователя становятся при таком подходе угрозами для плоскостей административного и оперативного 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 (т. е. 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 сквозные услуги, такие как выделенные линии для абонентов, пересекающие географические границы, или для регуляторных органов 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 Рек. МСЭ-Т M.3010, а физическая архитектура представлена на рисунке 6-11. Сеть управления устанавливает интерфейсы, которые определяют процессы обмена, необходимые для выполнения функций OAM&P на различных уровнях.



Интерфейс

DCN	Сеть передачи данных	QA	Q Адаптер
NE	Сетевой элемент	QMD	Q Посредническое устройство
OS	Операционная система	F	F интерфейс
WS	Рабочая сила	Q	Q интерфейс
		X	X интерфейс

Рисунок 6-11 – 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 Рек. МСЭ-Т M.3016.0 приводиться обзор и структура, которая определяет угрозы безопасности для СУЭ. В рамках Рекомендаций серии M.3016 Рек. M.3016.1 устанавливает конкретные требования, M.3016.2 описывает услуги обеспечения безопасности, а M.3016.3 определяет механизмы, которые могут противодействовать угрозе. Поскольку не все требования нуждаются в поддержке со стороны различных организаций по разработке стандартов, M.3016.4 предусматривает образец для создания профилей, основанных на требованиях, услугах и механизмах обеспечения безопасности, которые могут быть использованы в соответствии со специфической политикой организации в области безопасности. Конкретные меры, необходимые для интерфейса X, подробно представлены в Рек. МСЭ-Т M.3320. Характеристики протоколов для различных слоев связи определены в Рек. 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 сквозных 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 сквозных 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 Рек. 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 (см. рисунок 2-1). 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 (т. е. объекты управления).

6.4.2 Пересечение плоскости административного управления и слоя 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. Возможность сквозного взаимодействия 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 Рек. МСЭ-Т 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 6-11. 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 сквозном сетевом уровне и охватывает системы административного управления разных поставщиков. На рисунке 6-12 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.

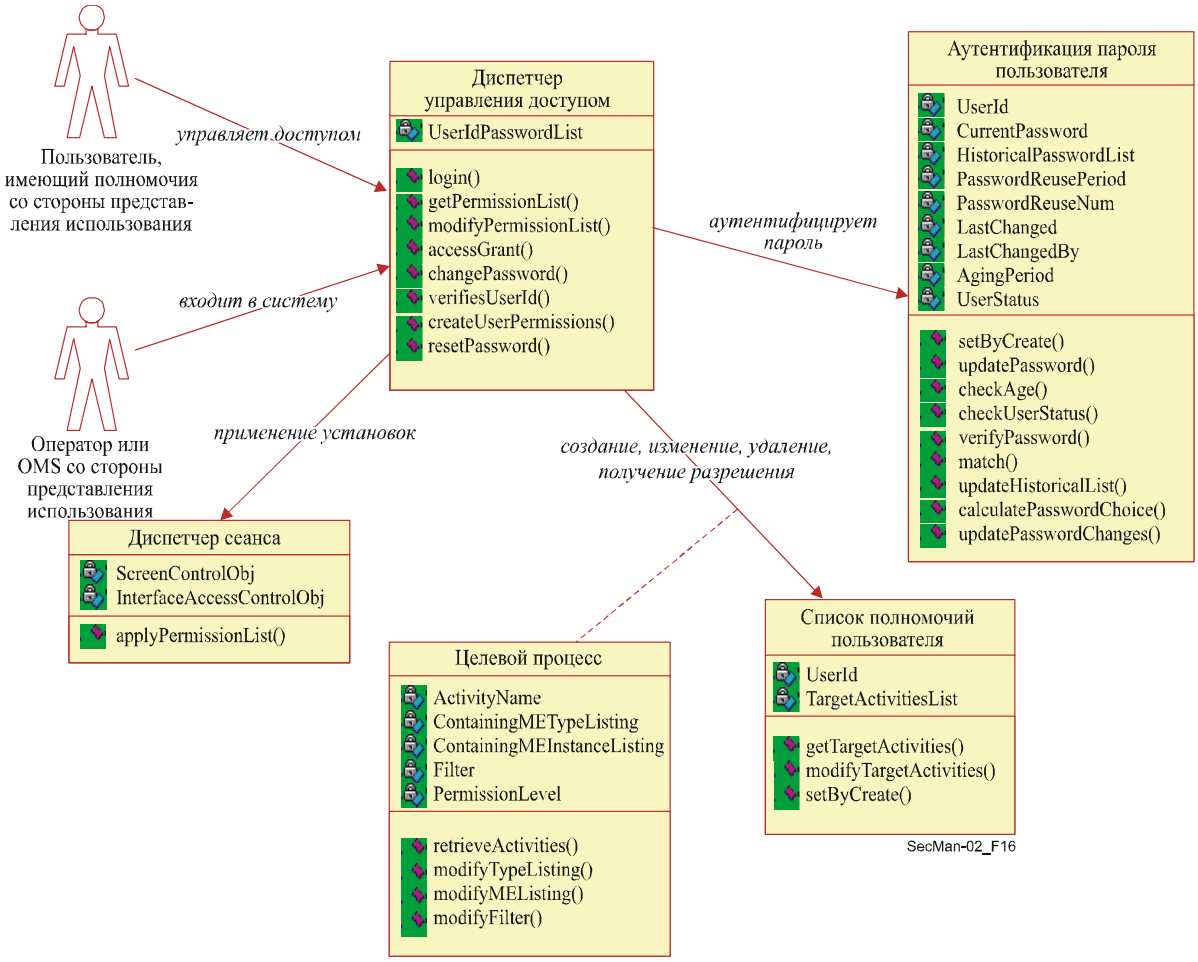


Рисунок 6-12 – Администрирование полномочий пользователя по Q.834.3

6.4.3 Пересечение плоскости административного управления и слоя 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 Рек. МСЭ-Т М.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 2.4. 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).

Рек. МСЭ-Т М.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 Рек. МСЭ-Т М.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 6-13 показано инициирование контроля процесса управления сетью приписки или визитной сетью. Система обнаружения мошенничества в сети приписки требует информацию о функциях, когда абонент регистрируется в визитной сети до ухода из сети после снятия с регистрации в сети. Затем можно разработать профили, относящиеся к использованию на основе записей данных вызова и слежения (анализа) на уровне услуги или для абонента. Затем система обнаружения мошенничества может проанализировать мошенническое поведение и инициировать соответствующие аварийные сигналы.

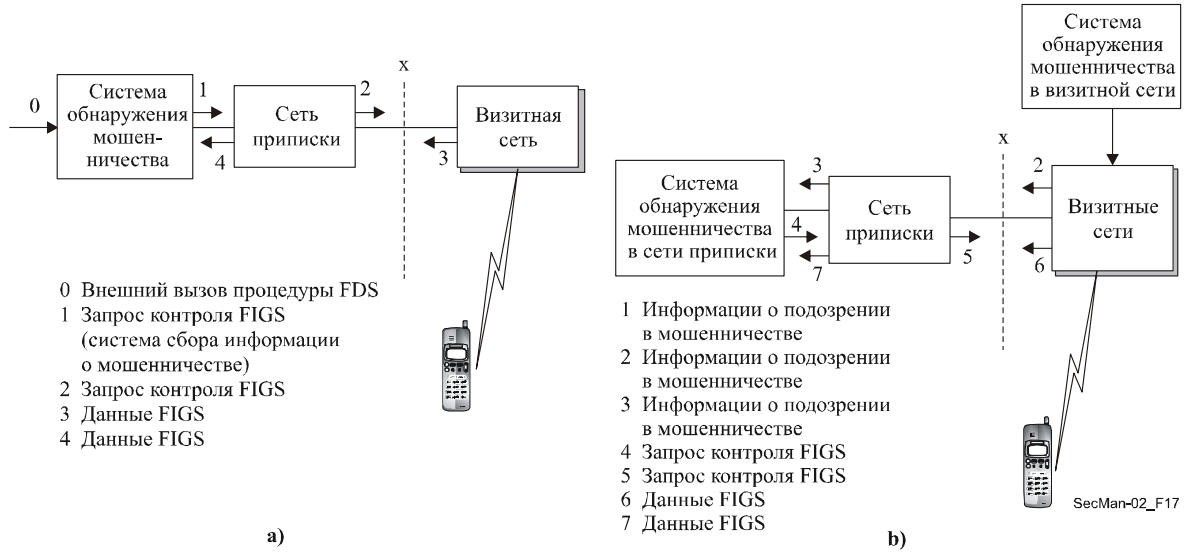


Рисунок 6-13 – Схема обнаружения мошенничества при пользовании услугами беспроводной связи согласно Рек. МСЭ-Т М.3210.1

6.4.4 Пересечение плоскости административного управления и слоя 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 установлению сквозного соединения пользуется услугами предоставления соединения другого поставщика услуг. В зависимости от регуляторной или рыночной среды некоторые поставщики услуг могут предлагать услуги доступа, а другие, называемые *компаниями, предоставляющими услуги связи*, могут предлагать установление соединения для дальней связи. Для установления сквозного 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 необходимые действия для поиска статуса неисправностей, вошедших в донесение. На рисунке 6-14 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.

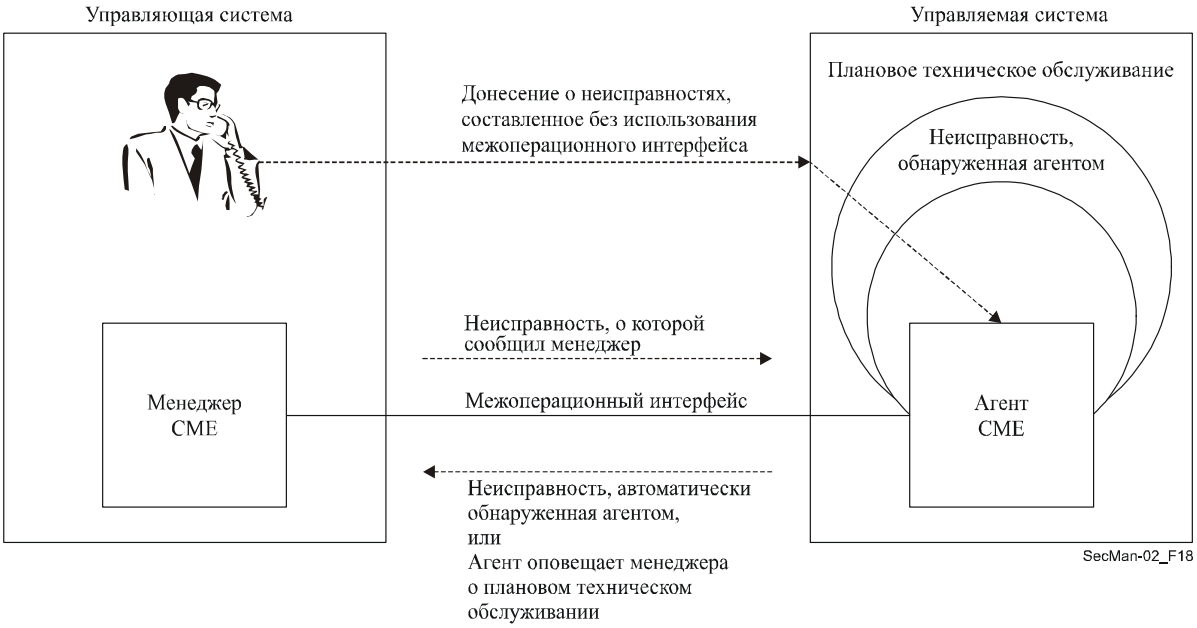


Рисунок 6-14 – Составление отчета о неисправности согласно Рек. МСЭ-Т X.790

В Рек. МСЭ-Т 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.

6.4.5 Общие услуги управления безопасностью

Рек. МСЭ-Т 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). Краткое описание услуг, включенных в эти Рекомендации, приводится ниже. Отметим, что все эти функции считаются, соответственно, функциями слоя административного управления.

6.4.5.1 Функция передачи аварийных сигналов: Передача аварийных сигналов в целом является одной из ключевых функций в интерфейсе управления. Если обнаруживается сбой в результате неисправности (сбой в работе оборудования) или нарушения режима безопасности, в систему управления поступает аварийный сигнал. В аварийном сообщении содержится ряд параметров, с тем чтобы система управления могла установить причину сбоя и осуществить правильные действия. Параметры по любому событию включают поле обязательного ввода, называемое типом события, и набор других полей, называемых информацией о событии. Последняя состоит из такой информации, как серьезность аварийного сигнала, возможные причины аварийного сигнала, детектор нарушения безопасности и пр. Причины аварийного сигнала связаны с типами событий, как показано в таблице 6-2.

ТАБЛИЦА 6-2

Причины аварийного сигнала

Тип события	Причины аварийного сигнала
нарушение целостности	дублированная информация пропавшая информация обнаруженное изменение информации нарушение последовательности информации неожиданная информация
функциональное нарушение	отказ в обслуживании перерыв по техническим причинам процедурная ошибка неустановленная причина
физическое нарушение	повреждение кабеля обнаружение вторжения неустановленная причина
нарушение службы или механизма безопасности	отказ в обеспечении аутентификации нарушение конфиденциальности отказ в обеспечении сохранности информации попытка несанкционированного доступа неустановленная причина
нарушение во временной области	задержанная информация ключ с истекшим сроком действия действия в нерабочее время

Эти причины аварийного сигнала более подробно объясняются в X.736. Некоторые из причин аварийного сигнала связаны с угрозами, рассмотренными в предыдущих разделах.

6.4.5.2 Функция регистрации данных проверки безопасности: Для того чтобы пользователь системы управления безопасностью мог зарегистрировать и иметь данные проверки в отношении нарушений безопасности, в Рек. МСЭ-Т X.740 установлен ряд событий, фиксируемых в данных проверки. К ним относятся соединение, разъединение, использование механизма защиты, операции по управлению и учет загрузки. Модель использует механизм регистрации, который определен в Рек. МСЭ-Т X.735, т. е. общий журнал для регистрации любого события, генерированного системой управления. В результате функции регистрации определяются два события, которые относятся к нарушению безопасности – отчет об обслуживании и отчет об использовании. Отчет об обслуживании касается предоставления обслуживания, отказа в обслуживании или восстановления обслуживания. Отчет об использовании применяется для указания того, что создана регистрационная запись, которая содержит статистические данные, относящиеся к безопасности. Как и в отношении любого события, определен ряд значений причин в отношении отчета об обслуживании. К ним относятся, в частности, запрос на обслуживание, отказ в обслуживании, сбой в обслуживании, восстановление обслуживания и т. д. Можно определить, если потребуется, новые типы событий, поскольку два типа, которые указаны в Рекомендации, в будущем могут оказаться недостаточными.

6.4.5.3 В Рек. МСЭ-Т X.741 очень подробно описана модель, связанная с назначением функции управления доступом различным управляемым объектам. Требования, которые соответствуют приведенным в этой Рекомендации определениям управления доступом, включают защиту информации управления доступом от несанкционированного введения, удаления, изменения; разрешенные операции на объектах соответствуют правам доступа для инициаторов операций и предотвращают передачу информации управления не имеющим доступа получателям. С целью удовлетворения этих требований описаны различные уровни управления доступом. В отношении административных операций положения, предусмотренные в Рекомендации, обеспечивают ограничение доступа на множественных уровнях: управляемый объект в целом, атрибуты объекта, величины атрибутов, контекст доступа и действия на объекте. Установлен ряд схем, таких как список управления доступом, на основе функциональных возможностей, метки и контекста и политика по управлению доступом может применять одну или несколько таких схем. В этой модели, основанной на политике и информации управления доступом (ACI), принимается решение о том, разрешить или не разрешить запрашиваемую операцию. Например, ACI включает правила, идентификацию инициатора, идентификацию целей и т. д. Эта модель является многофункциональной, и в каком-либо приложении могут не потребоваться все функциональные возможности.

6.4.5.4 Услуги безопасности на основе CORBA: Хотя Рекомендации серии X.700 предполагают использование CMIP как протокола интерфейса управления, в отрасли существуют и другие тенденции, в соответствии с которыми вводится применение протокола, услуг и других моделей интерфейсов управления, которые основаны на о . . МСЭ-Т Q.816 определяется структура использования этих услуг в контексте интерфейсов управления. В целях поддержки требований для этих интерфейсов эта Рекомендация ссылается на спецификацию OMG для общих услуг безопасности.

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 информационно-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, веб-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 информационно емкий 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 Рек. 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 (34 500 врачей общей практики, 10 000 выписывающих лекарства сестер, число которых увеличится до 120 000 в течение ближайших нескольких лет, 44 000 зарегистрированных фармацевтов и 22 000 стоматологов), и весьма малый объем реально требуемых авторизаций (т. е. 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 до 16 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 о полномочиях 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.

На рисунке 6-15 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 (т. е. PKI с сертификатами открытых ключей), но и жесткую авторизацию (т. е. 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.

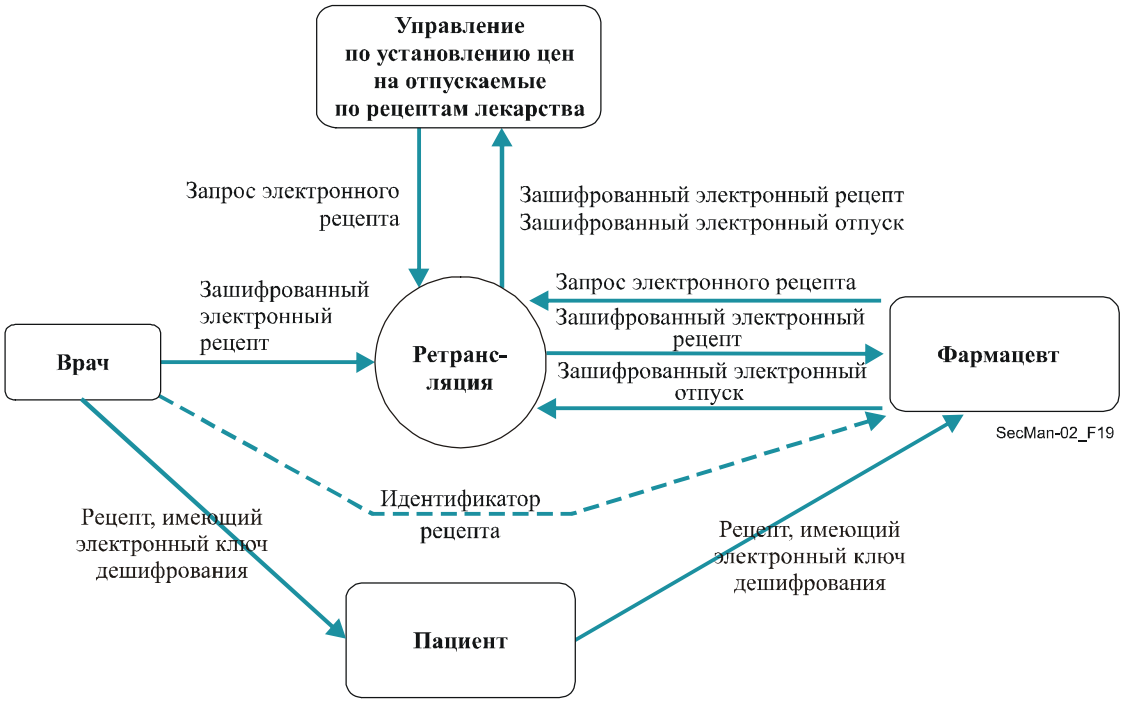


Рисунок 6-15 – Система электронных рецептов Солфорд

В приведенном на рисунке 6-15 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 Рек. МСЭ-Т X.509, позволяет в настоящее время обеспечить более общий и глобальный доступ к электронным рецептам.

6.6 Защищенная сквозная передача данных по подвижной связи

Широкое распространение получили терминалы подвижной связи с функциональными возможностями по передаче данных (такие как мобильный телефон IMT-2000, портативный компьютер или КПК с радиокарточкой), и появляются услуги по разнообразным приложениям (например, мобильная электронная коммерция) для терминалов подвижной связи, соединенных с сетью подвижной связи. В среде электронной коммерции обеспечение безопасности не только необходимо, но и крайне важно.

В интересах оператора подвижной связи проводятся исследования во многих областях безопасности (например, архитектура безопасности для сети подвижной телефонной связи IMT-2000). Однако важно также проводить исследования в интересах пользователя подвижной связи и поставщика прикладных услуг (ASP).

Одним из наиболее важных аспектов исследований в области безопасности в интересах пользователя подвижной связи и ASP является обеспечение безопасности сквозной передачи данных по подвижной связи между мобильным терминалом и сервером приложений.

Кроме того, для системы подвижной связи, которая соединяет сеть подвижной связи с открытой сетью, необходимо провести исследование в области обеспечения безопасности на верхних уровнях (приложение, представление и сеанс связи) эталонной модели OSI, поскольку существуют разнообразные возможные реализации сетей подвижной связи (например, мобильная телефонная сеть IMT-2000, беспроводная ЛВС, Bluetooth) или открытых сетей.

6.6.1 Структура технологий защиты сквозной передачи данных по подвижной связи

В Рек. МСЭ-Т X.1121 описаны модели защищенной сквозной передачи данных по подвижной связи между терминалами подвижной связи и серверами приложений на верхних уровнях. В этой Рекомендации определены две модели безопасности для структуры безопасности сквозной передачи данных по подвижной связи между пользователем подвижной связи и ASP – обобщенная модель и модель со шлюзом. Пользователь подвижной связи использует терминал подвижной связи для получения доступа к различным услугам подвижной связи, которые предоставляют ASP. ASP предоставляет услугу подвижной связи пользователям подвижной связи через сервер приложений. Шлюз безопасности подвижной связи ретранслирует пакеты с терминалов подвижной связи на сервер приложений и преобразует протокол связи на основе подвижной сети в протокол связи на основе открытой сети, и наоборот.

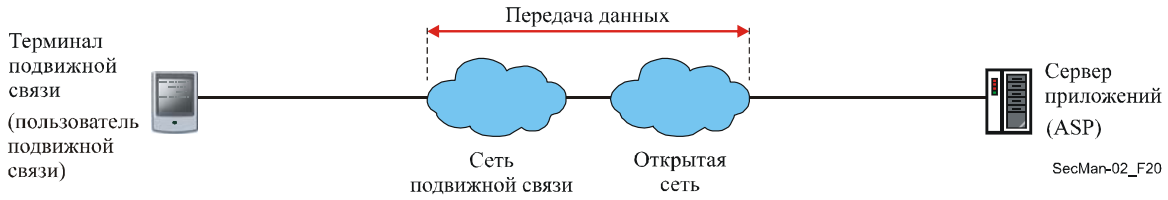


Рисунок 6-16 – Общая модель сквозной передачи данных между пользователем и ASP

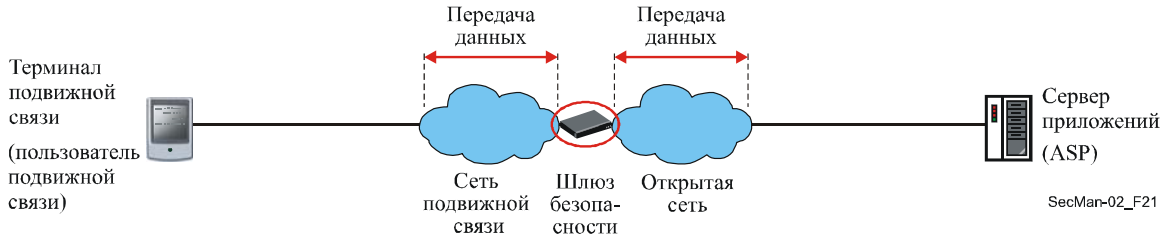


Рисунок 6-17 – Модель сквозной передачи данных по подвижной связи между пользователем подвижной связи и ASP с использованием шлюза

В Рек. МСЭ-Т X.1121 описаны также угрозы безопасности для сквозной передачи данных по подвижной связи и требования к безопасности в интересах пользователя подвижной связи и ASP в обеих моделях. Существуют два вида угроз: вид общих угроз, присутствующих в любой открытой сети, и вид угроз, характерных для подвижной связи. На рисунке 6-18 показаны угрозы для сквозной передачи данных по подвижной связи.

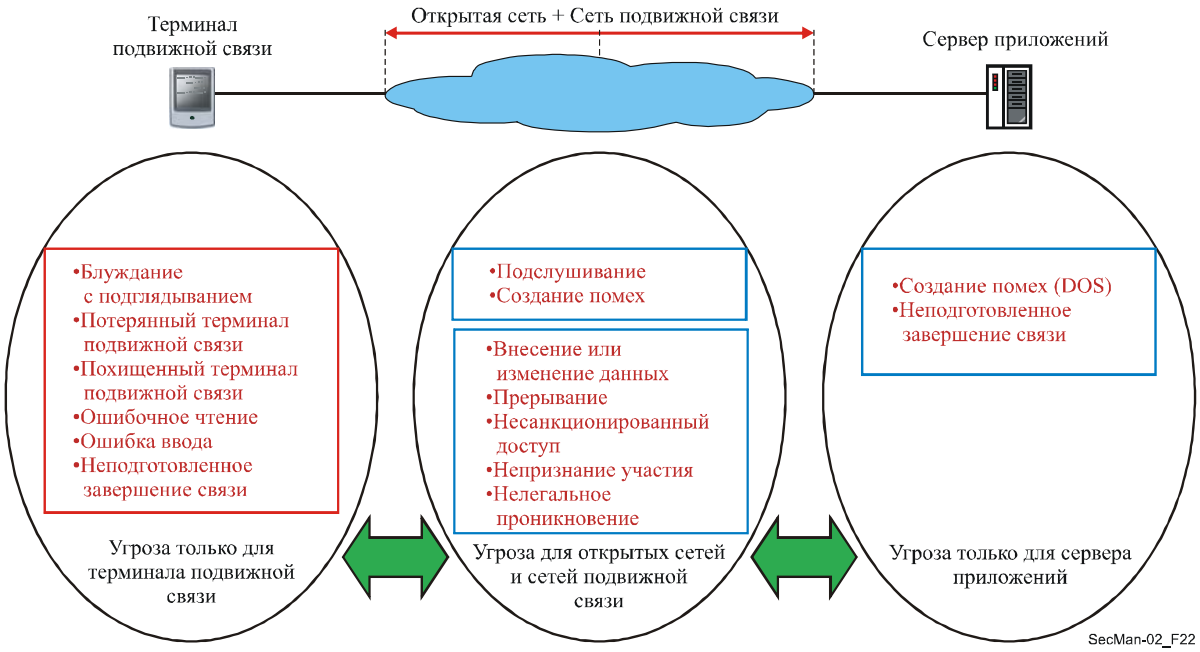


Рисунок 6-18 – Угрозы в сквозной передаче данных по подвижной связи

Кроме того, в Рек. МСЭ-Т X.1121 место реализации технологий безопасности, если требуется для каждого объекта и отношений между объектами в сквозной передаче данных по подвижной связи (см. рисунок 6-19).

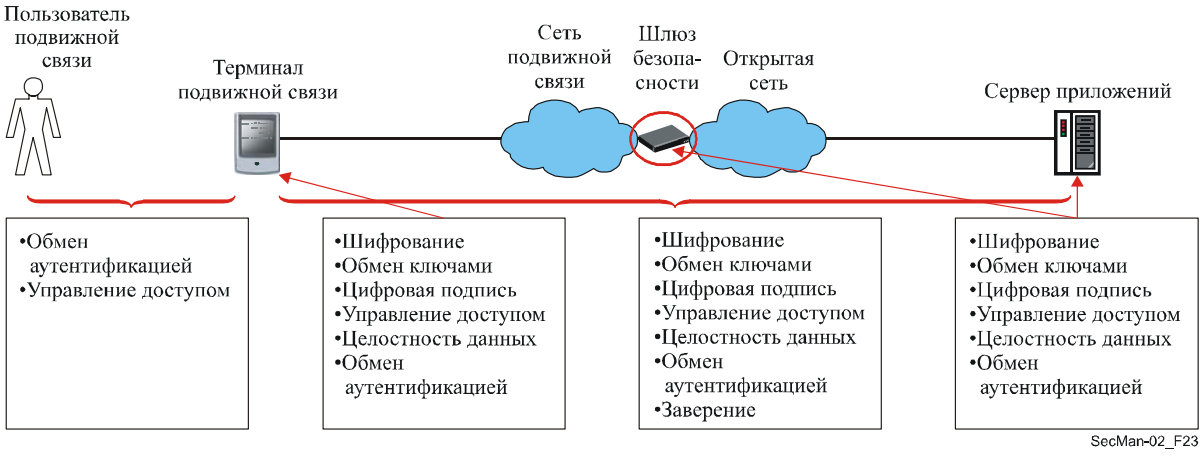


Рисунок 6-19 – Функция безопасности, необходимая для каждого объекта и отношений между ними

6.6.2 Применение технологии PKI для защиты сквозной передачи данных по подвижной связи

Этот раздел касается Рек. МСЭ-Т X.1122. Хотя технология PKI весьма пригодна для защиты сквозной передаче данных по подвижной связи, некоторые характеристики, присущие передаче данных по подвижной связи, могут потребовать адаптации технологии PKI при построении систем безопасности подвижной связи. В целях обеспечения услуг безопасности в сквозной передаче данных по подвижной связи были определены два вида моделей PKI. Один относится к общей модели PKI, в которой отсутствует функция шлюза безопасности, используемого в сквозной передаче данных по подвижной связи, а второй вид относится к модели PKI с использованием шлюза, в которой существует шлюз безопасности для соединения с сетью подвижной связи и открытой сетью. На рисунке 6-20 показана общая модель PKI для подвижной сквозной связи. Она включает четыре объекта. CA пользователя подвижной связи выдает сертификат пользователя подвижной связи пользователю подвижной связи и управляет хранилищем для хранения списка аннулированных сертификатов (CRL), которые уже выдал CA пользователя. Удостоверяющий орган (VA) пользователя предоставляет пользователю подвижной связи услугу в реальном масштабе времени по удостоверению сертификата. CA со стороны ASP выдает сертификат ASP поставщику прикладных услуг и управляет хранилищем для хранения списка аннулированных сертификатов, которые уже выдал CA со стороны ASP. Удостоверяющий орган со стороны ASP предоставляет услугу в реальном масштабе времени по удостоверению сертификата для сертификатов ASP.

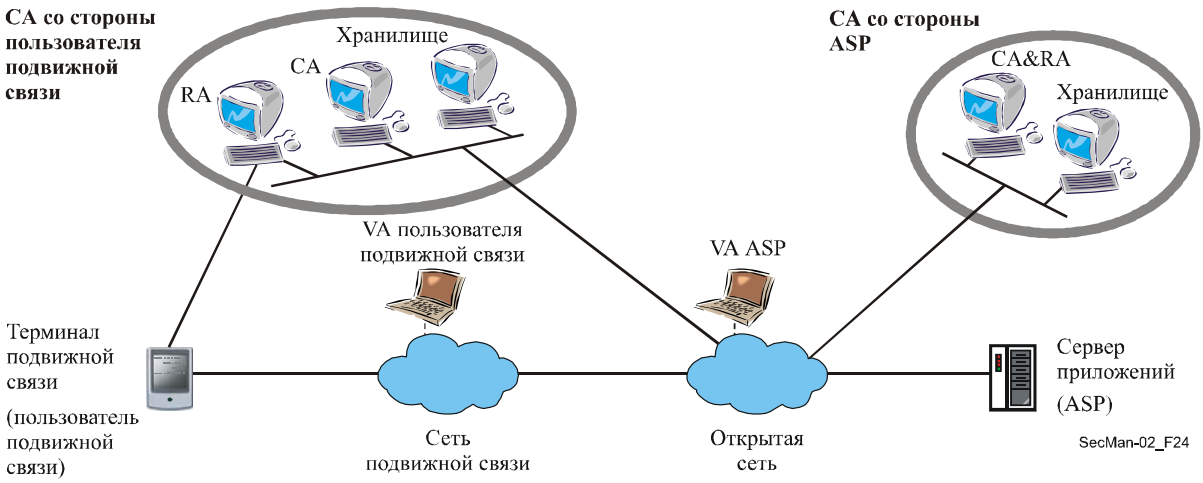


Рисунок 6-20 – Общая модель PKI для сквозной передачи данных по подвижной связи

Существуют два метода выдачи сертификатов, в зависимости от места генерирования открытых/личных ключей. Один метод предусматривает генерирование и изготовление пары криптографических ключей на месте производства терминала подвижной связи, а при другом методе пара криптографических ключей генерируется в терминале подвижной связи или к терминалу подвижной связи прикрепляется смарт-карта наподобие защищенного маркера. На рисунке 6-21 показана процедура получения терминалом подвижной связи сертификата с использованием процедуры управления сертификатом, когда пара криптографических ключей генерируется в терминале подвижной связи.

Рисунок 6-21 – Процедура выдачи сертификата для терминала подвижной связи

Терминал подвижной связи обладает ограниченными вычислительными возможностями и объемом памяти. Поэтому схема удостоверения сертификата в реальном масштабе времени имеет преимущество по сравнению с основанной на CRL схемой удостоверения сертификата в автономном режиме. Когда терминал подвижной связи получает пару сообщение-подпись с цепочкой сертификатов и хочет проверить подлинность подписи, сертификат следует использовать после проверки подлинности сертификата с использованием схемы удостоверения сертификата. На рисунке 6-22 показана процедура удостоверения сертификата в реальном масштабе времени для терминала подвижной связи.

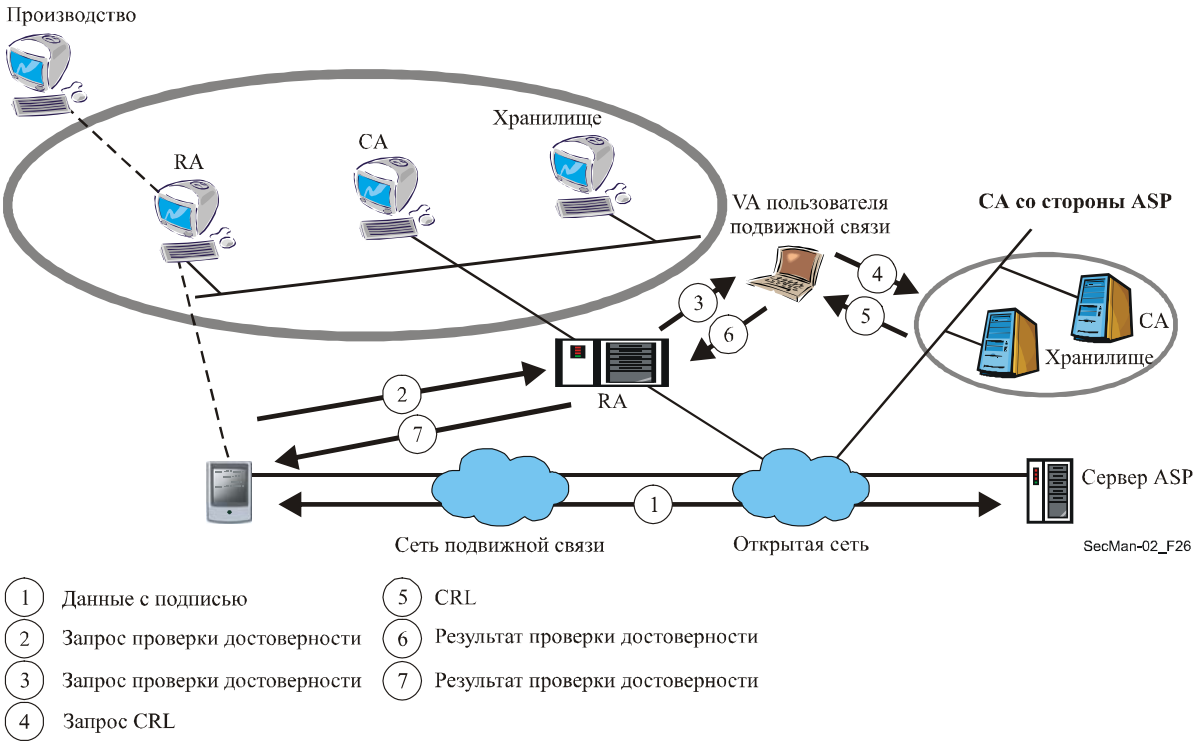


Рисунок 6-22 – Процедура удостоверения сертификата для сквозной передачи данных по подвижной связи

Система PKI для сквозной подвижной связи может быть использована для двух моделей: одна применяется для уровня сеанса связи, а другая – для прикладного уровня. Модель для уровня сеанса связи предусматривает такие услуги безопасности, как аутентификация клиента, аутентификация сервера, а также обеспечение конфиденциальности и целостности данных. Модель для прикладного уровня предусматривает услугу по обеспечению сохранности информации и конфиденциальности для сквозной передачи данных по подвижной связи.

В заключение отметим, что Рек. МСЭ-Т X.1122 описывает способы построения защищенных систем подвижной связи на основе PKI в следующих аспектах: функциональная совместимость с существующими системами на основе PKI в открытой сети; использование PKI в среде подвижной связи (включая генерирование ключей, заявку на сертификат и выдачу сертификата, использование сертификата и вопросы, касающиеся CA) и PKI в целом (включая управление сертификатом на протяжении срока действия). Эта Рекомендация может использоваться как основополагающий документ при построении систем надежной подвижной связи на основе технологии PKI.

7 Параметр готовности и слой инфраструктуры

Рек. МСЭ-Т X.805, представленная в разделе 2, касается:

- параметров безопасности как набора мер защиты, предназначенных для конкретного аспекта сетевой безопасности; и
- слоев безопасности. Параметры безопасности применяются к иерархии сетевого оборудования и групп устройств, которые определяются как слои защиты.

Готовность как параметр безопасности обеспечивает, что в результате событий, влияющих на сеть, не будет отказа в санкционированном доступе к сетевым элементам, хранимой информации, информационным потокам, услугам и приложениям. К этой категории относятся решения по восстановлению после бедствий.

Инфраструктура как слой безопасности состоит из сетевых средств передачи, а также отдельных сетевых элементов, защищаемых параметрами безопасности. Слой инфраструктуры представляет собой блоки основания сетей, их услуг и приложений. Примерами компонентов, которые относятся к слою инфраструктуры, являются отдельные маршрутизаторы, коммутаторы и серверы, а также линии связи между отдельными маршрутизаторами, коммутаторами и серверами.

Функциональные, эксплуатационные и оперативные требования, указанные МСЭ-Т, как часть вышеизложенных концепций, многочисленны и разнообразны. Они могут касаться защищенности от помех, борьбы с перегрузками, сообщений об отказах и мер по исправлению, а также многого другого. В остальной части данного раздела представлены некоторые различные точки зрения в отношении требований, предъявляемых к сетям электросвязи, с целью ограничения рисков и последствий неготовности для ресурсов передачи данных.

С тем чтобы оператор сети электросвязи мог выбрать необходимую топологию сети в связи с обеспечением готовности, предлагается ссылка на Приложение A к Рек. G.827 "Примеры топологий маршрутов и расчеты сквозной готовности маршрута".

7.1 Топология маршрутов и расчеты сквозной готовности маршрута

На рисунках 7-1 и 7-2 показаны основные топологии маршрутов, которые можно построить с использованием заранее заданных элементов маршрута.

На рисунке 7-1 показан простой основной маршрут без защиты, а на рисунке 7-2 добавлен маршрут сквозной защиты, который в целях обеспечения максимальной защиты должен быть отдельным.

Эта форма защиты называется 1+1. Каждый маршрут имеет двустороннее соединение с сигналом передачи с каждого конца, постоянно соединенного с обоими маршрутами, и с коммутирующим устройством на каждом приемнике для выбора наилучшего сигнала.

Более экономично использовать один маршрут защиты для защиты нескольких других маршрутов. Этот вариант известен как механизм 1:n, и он требует селективных коммутаторов как на передатчиках, так и на приемниках.

В целях расчетов сквозной готовности более удобно использовать коэффициент неготовности. В Приложении A к Рек. МСЭ-Т G.827 предусмотрены некоторые основные принципы оценки готовности

для простого базового маршрута (рисунок 7-1), сквозная защита 1+1 (рисунок 7-2) или топология коэффициента защиты 1:n.

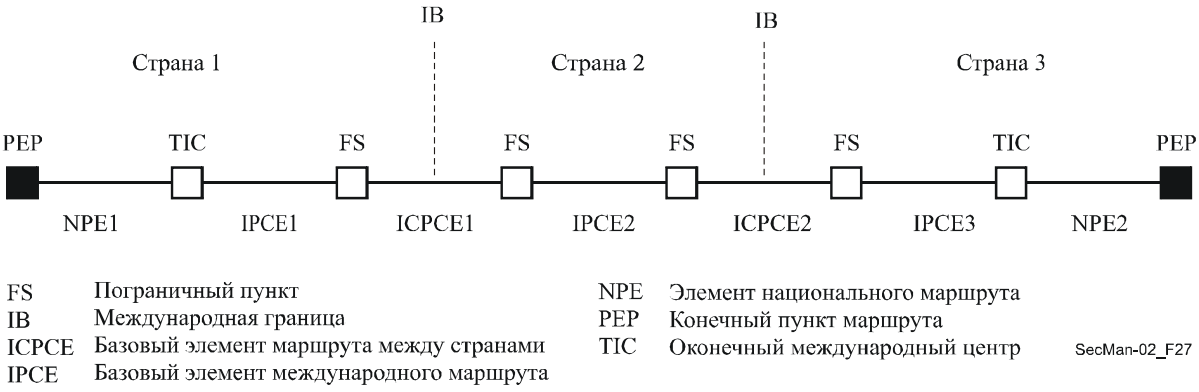


Рисунок 7-1 – Пример простого базового маршрута без защиты

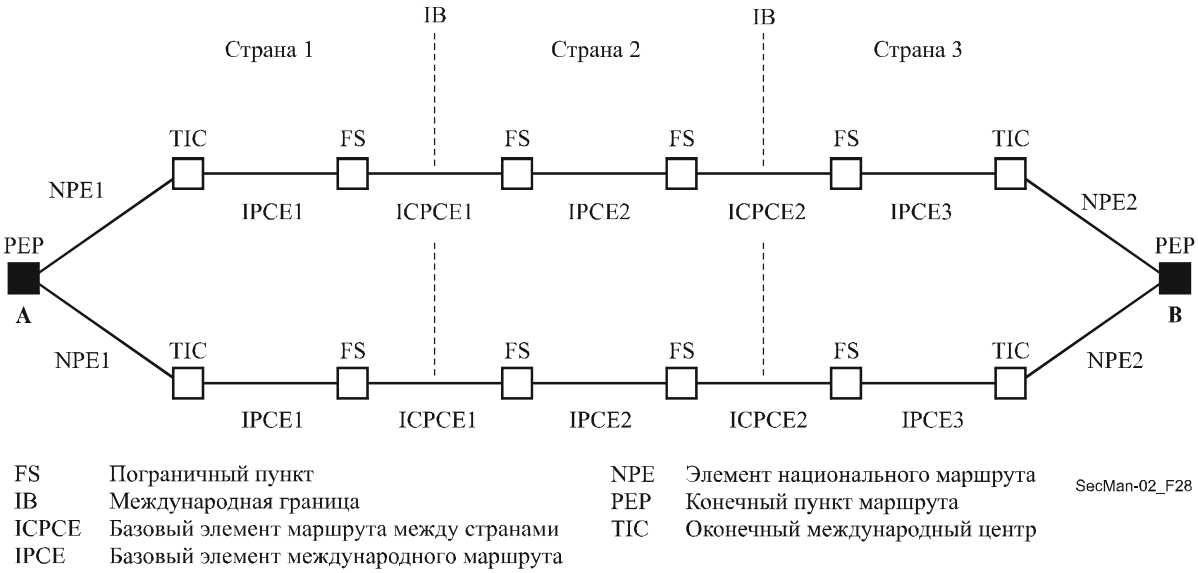


Рисунок 7-2 – Пример маршрута со сквозной защитой

В разделе 7.3 рассматриваются более сложные топологии, например, кольцевая топология синхронной цифровой иерархии (SDH), где показано, что трафик может быть перенаправлен вокруг отказавшей линии, но маршрут защиты зависит от коммутационных возможностей различных узловых точек на кольце и может оказаться не самым коротким расстоянием между двумя узловыми точками. В более сложных топологиях довольно трудно оценить готовность. Этот вопрос рассматривается в нескольких материалах, указанных в Дополнении I к Рек. G.827.

7.2 Усиление готовности транспортной сети – обзор

В разделах 7.2–7.4 описаны архитектурные особенности для более распространенных подходов к усилению готовности транспортной сети. Усиление достигается с помощью замены отказавших или изношенных транспортных объектов на другие, более специализированные объекты или объекты, совместно использующие ресурс. Замена обычно инициируется в результате обнаружения дефекта, ухудшения качества работы или внешнего запроса (например, со стороны органа, управляющего сетью).

Защита – Она использует заранее заданные возможности между узловыми точками. Самая простая архитектура имеет один выделенный защитный объект для каждого рабочего объекта (1+1). Наиболее сложная архитектура имеет m-количество защитных объектов для n-количества рабочих объектов (m:n). Переключение защиты может быть или однонаправленным, или двунаправленным. При переключении двунаправленной защиты выполняются коммутационные действия для обоих направлений трафика, даже если отказ однонаправленный. При переключении однонаправленной защиты выполняются коммутационные действия только для затронутого направления трафика в случае однонаправленного отказа.

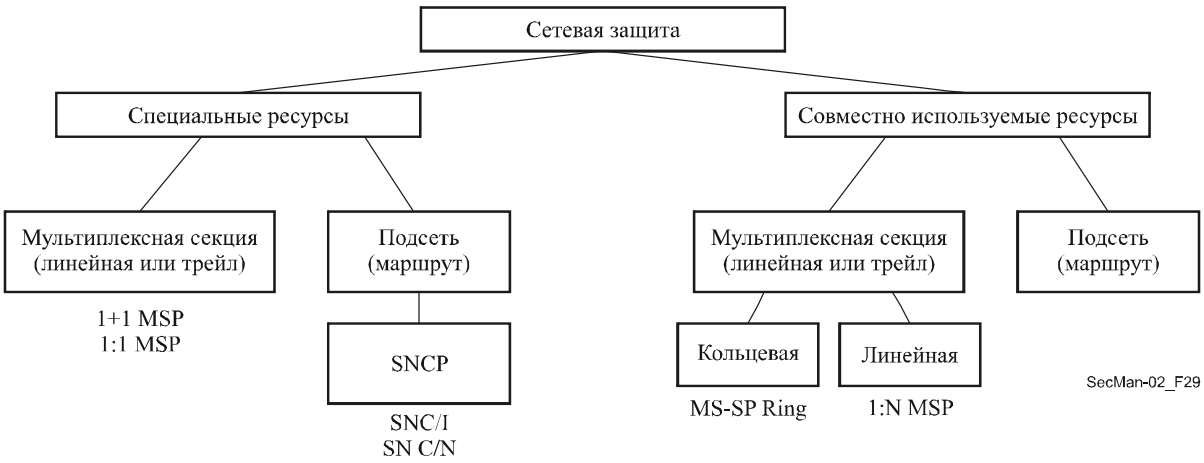
Восстановление – Оно пользуется любой возможностью, имеющейся между узловыми точками. В целом алгоритмы, используемые для восстановления, связаны с выбором нового маршрута. При выполнении функции восстановления какая-то доля возможностей транспортной сети резервируется для изменения маршрута рабочего трафика.

В Рек. МСЭ-Т G.805 содержится ключевая информация по этим аспектам.

7.3 Защита

Высокий уровень служебной готовности может быть достигнут только посредством использования очень надежной и живучей инфраструктуры. Так, если отказало высоконадежное оборудование, должна существовать возможность переключения на альтернативный источник сигнала (защитный канал).

Существуют два вида защиты. Один из них – это защита оборудования, предполагающая наличие резервных блоков. Тогда в случае отказа на блоке автоматически включается другой блок. Существует также защита сети, т. е. защита от пореза оптического волокна при наличии альтернативного маршрута для прохождения сигнала. Эти альтернативные маршруты могут быть или выделенными, или совместно используемыми. Соответствующие механизмы показаны на рисунке 7-3.



SNC/I	Защита соединения подсети/Встроенный мониторинг
SNC/N	Защита соединения подсети/Мониторинг без вмешательства
SNCP	Защита соединения подсети
1+1 MSP	Защитная коммутация мультиплексной секции 1+1
1:N MSP	Защитная коммутация мультиплексной секции 1:N
MS-SPRing	Кольцо совместно используемой защиты мультиплексной секции

Рисунок 7-3 – Варианты защитной коммутации

Механизмы защиты могут быть однонаправленными или двунаправленными. Они также могут быть двусторонними и односторонними. Эти термины определены в Рек. МСЭ-Т G.780/Y.1351.

Однонаправленная защита определяется следующим образом: "В отношении однонаправленного отказа (т. е. отказа, затрагивающего только одно направление передачи данных) коммутируется только затронутое направление (трасса, соединение подсети (SNC) и пр.)". Это означает, что при осуществлении защитной коммутации принимается только локальное решение на стороне приемника (локальный узел), без учета статуса удаленного узла. В случае однонаправленного отказа (т. е. отказа, затрагивающего только одно направление передачи данных) на защиту переключается только затронутое направление.

Двунаправленная защита определяется следующим образом: "В отношении однонаправленного отказа коммутируются оба направления (трасса, соединение подсети (SNC) и пр.), включая затронутое и незатронутое". Это означает, что при осуществлении защитной коммутации учитывается и локальный, и удаленный статус. В случае однонаправленного отказа (т. е. отказа, затрагивающего только одно направление передачи данных) на защиту переключаются оба направления, включая затронутое и незатронутое.

Двусторонняя операция (защиты) определяется следующим образом: "При двусторонней операции сигнал трафика (услуга) всегда возвращается на рабочее SNC/трасса, если запрос на коммутацию прекращается, т. е. когда рабочее SNC/трасса восстановились от повреждения или отменен внешний запрос". Это означает, что при двустороннем режиме после восстановления рабочего канала сигнал на защитном канале переключается обратно на рабочий канал.

Односторонняя операция (защиты) определяется следующим образом: "При односторонней операции сигнал трафика (услуга) не возвращается на рабочее SNC/трасса, если запрос на коммутацию прекращается". Это означает, что при одностороннем режиме (применимом только к архитектурам 1+1) после восстановления рабочего канала сохраняется выбор нормального или защищенного сигнала трафика с защитного канала.

Наиболее распространенными формами защиты являются:

- 1:1 MSP (Защитная коммутация мультиплексной секции 1:1, см. подраздел 7.3.1);
- 1+1 MSP (Защитная коммутация мультиплексной секции 1+1, см. подраздел 7.3.2);
- MS-SPRing (Совместно используемое защитное кольцо мультиплексной секции, см. подраздел 7.3.3);
- SNCP (Защита соединения подсети, см. подраздел 7.3.4).

Эти механизмы защиты будут рассмотрены более подробно. Однако следует применять общий набор базовых Рекомендаций: G.841 (характеристики), G.842 (взаимодействие), G.783 (функциональные модели), G.806 (дефекты) и G.808.1 (общая защитная коммутация).

7.3.1 Защитная коммутация мультиплексной секции по схеме 1:1

Диаграмма сети показана на рисунке 7-4.

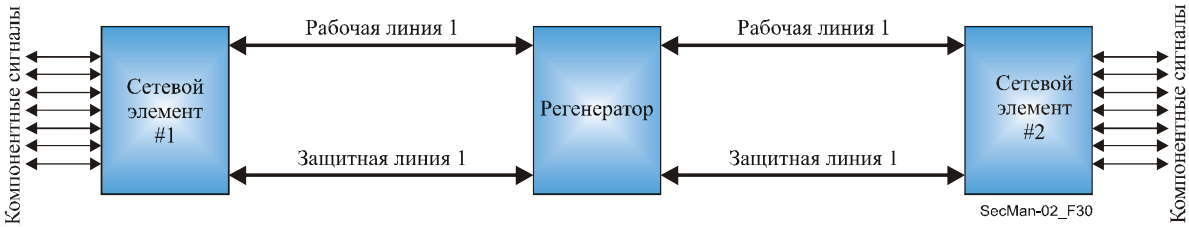


Рисунок 7-4 – Диаграмма сети для защитной коммутации по схеме 1:1

При защитной коммутации 1:1 существует один защитный канал для каждой рабочей линии. Возможно, что по защитному каналу переносится другой трафик, который может быть вытеснен.

Диаграмма внутренней структуры сетевого элемента показана на рисунке 7-5.

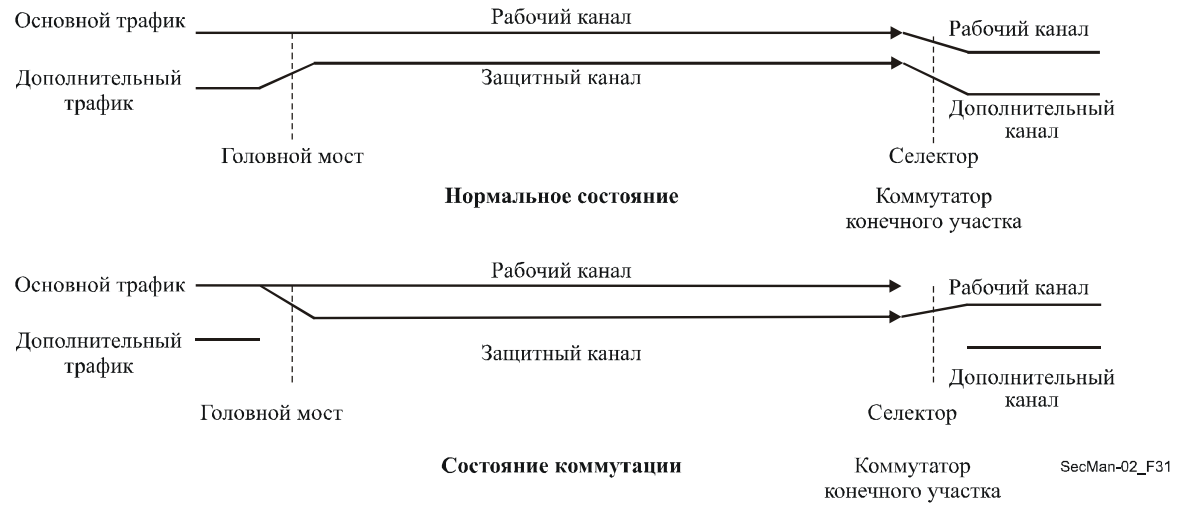


Рисунок 7-5 – Линейная защита мультиплексной секции по схеме 1:1

При нормальных условиях "дополнительный трафик" может переноситься по защитному каналу. Однако если получены К1/К2 байты, не имеющие без ошибок (с активацией функции защиты), то "основной трафик" переносится по мосту на защитный канал в головной точке и коммутируется в "конечной точке". Контроль осуществляется через байты К1 и К2 на защитном канале.

Это соответствует линейной защите на синхронном транспортном модуле на уровне N (уровень STM-N ($N \geq 1$)).

Условия, которые могут инициировать коммутацию, – это принудительная коммутация и ряд условий, возникающих в результате дефекта или отказа (например, отсутствие сигнала, потеря блока данных, избыточное количество ошибок, ослабление сигнала). Подробности приводятся в Рек. МСЭ-Т G.806.

7.3.2 Защитная коммутация мультиплексной секции по схеме 1+1

На рисунке 7-6 показана диаграмма сети.

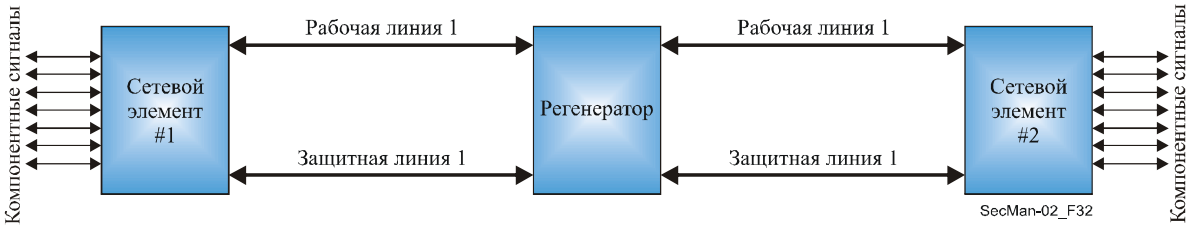


Рисунок 7-6 – Диаграмма сети для защитной коммутации по схеме 1+1

В защитной коммутации по схеме 1+1 существует один защитный канал для каждого рабочего канала. Защитный канал переносит копию сигнала рабочих каналов.

Диаграмма внутреннего сетевого элемента оказана на рисунке 7-7.

Рисунок 7-7 – Линейная защита мультиплексной секции по схеме 1+1

Сигнал передачи постоянно переносится по мосту на защитную линию. Приемник выбирает лучший сигнал.

В схеме защиты 1+1 отсутствует возможность для "дополнительного трафика". Эта схема предусматривает функцию защиты линии. Таким образом, она работает только на STM-n, независимо от пропускной способности линии. Ее можно рассматривать как поднабор защитной коммутации 1:1. Она не требует использования контрольного механизма (байты К1 и К2 автоматической защитной коммутации (APS) заголовка мультиплексной секции (MSOH). Она осуществляет коммутацию на основе того же состояния отказа, как указано в подразделе 7.3.1.

В этом механизме защиты существует вариант, называемый двунаправленным 1+1, когда переключаются селекторы на обеих конечных точках. Это требует контроля с помощью передаваемых байтов К1/К2.

7.3.3 Защитная коммутация MS-SPRing

Диаграмма сети показана на рисунке 7-8.

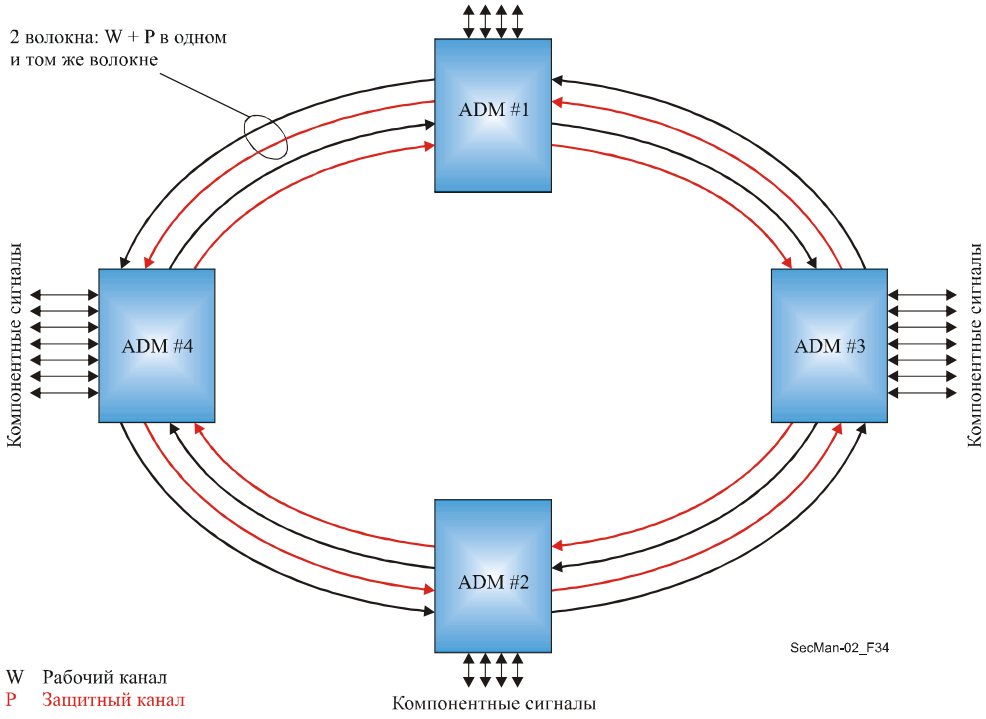


Рисунок 7-8 – Диаграмма сети для защитной коммутации MS-SPRing

Двухволоконная конфигурация MS-SPRing преобладает в сетях SDH. Существуют два волокна для каждого отрезка кольца, при этом каждое из этих волокон переносит половину полосы пропускания для рабочего и защитного каналов (например, линия STM-64 с административными единицами (AU) AU-4 с 1 по 32 для рабочего канала и AU-4 с 33 по 64 для защиты). Нормальный трафик, переносимый по рабочим каналам в одном волокне, защищается защитными каналами в обратном направлении.

Двухволоконная функция MS-SPRing показана на рисунке 7-9.

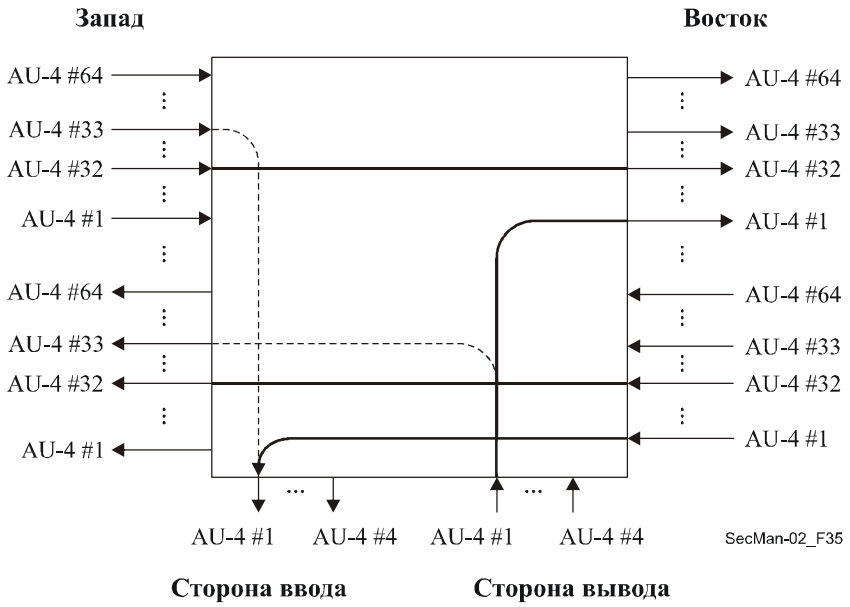


Рисунок 7-9 – Кольцо STM-64 с вводом-выводом STM-4

На рисунке 7-9 фазовый сигнал "Add AU-4 #1" переводится в сигнал "передача восток AU-4 #1". Он вводится с "получение восток AU-4 #1" на "ввод AU-4 #1". Существует также сквозное соединение на AU-4 #32, как показано на рисунке 7-9.

Если происходит обрыв на восточном волокне, то необходимо передать "вывод AU-4 #1" на защиту западной стороны ("передача запад AU-4 #33") и сигнал получения ввести с защиты западной стороны ("получение запад AU-4 #33") на "ввод AU-4 #1"). "AU-4 #32" с западной стороны необходимо закольцевать на AU-4 #64. AU-4 #32 с восточной стороны будет закольцован на защитный канал (AU-4 #64) с другой стороны обрыва, и, таким образом, на этом узле защита ("получение запад AU-4 #64") необходимо закольцевать на рабочий канал ("AU-4 #32").

Защитная коммутация осуществляется на уровне модульности AU-4 или AU-3 по всем сигналам в волокне. Запросы и подтверждения передаются с помощью байтов K1 и K2 автоматической защитной коммутации (APS) заголовка мультиплексной секции (MSOH). K1 и K2 передают на линии, которая несет защитные каналы. Они передаются в обоих направлениях (восток и запад), при этом одно из них представляет собой короткий тракт, а другое – длинный.

Бесшумная настройка выполняется для того, чтобы избежать доставки трафика не тому клиенту в случае локализации или отказа узла с трафик вход/выход (услуги, оказанные с одного временного канала, но на разных отрезках). Описания бесшумной настройки приводится в Дополнении II к Рек. G.841.

Отказы при отсутствии сигнала и ослаблении сигнала такие же, как и в случае коммутации линейной защиты (см. подраздел 7.3.1).

Существуют три конфигурации коммутации:

- нормальная (без ошибок);
- ошибка на восточной стороне (необходимо закольцевать запад и ввод/вывод только с запада);
- ошибка на западной стороне (необходимо закольцевать восток и ввод/вывод только с запада);
- коммутация отрезка для 4-волоконной функции MS-SPRing (коммутация на защиту без кольцевания).

7.3.4 Защитная коммутация SNCP

Диаграмма сети показано на рисунке 7-10.

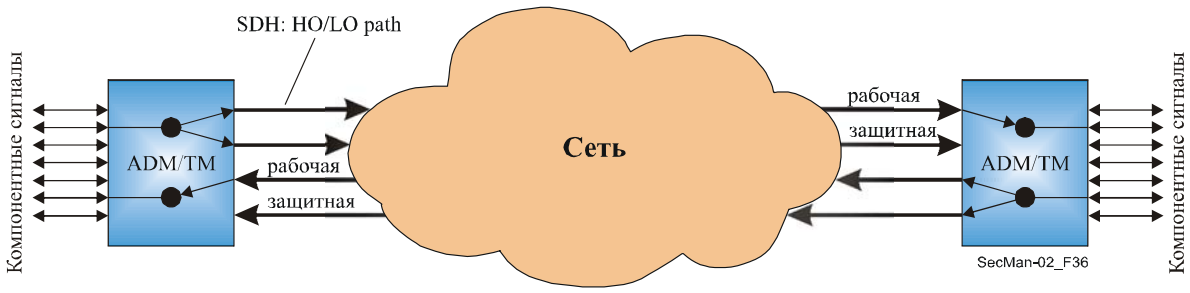


Рисунок 7-10 – Защитная коммутация SNCP

SNCP основана на тракте. Так, в один момент коммутируется только один сигнал (AU-3, AU-4 и т. д.). ЕЕ можно также рассматривать как однонаправленную 1+1 для отдельных трактов. Защитная коммутация осуществляется на уровне тракта:

- SDH: виртуальный контейнер высокого порядка HO – VC-4/3
  компонентный блок более низкого порядка LO – TU-3/2/11/12

Никакой протокол не используется (кроме принудительной коммутации). Решение о коммутации между рабочей копией и защитной копией определяется местными условиями, в которых производится мониторинг обеих копий.

- Время для защитной коммутации должно быть менее 50 миллисекунд. Таким образом, в случае пореза волокна с высокой пропускной способностью, например, 10 Гбит/с или 40 Гбит/с при защите SNCP для всех трактов обычно невозможно соблюсти это ограничение во времени, если защитная коммутация осуществляется в программе, которая предусматривает обработку дефекта в конечном автомате и обмен сообщениями между коммутатором и центральным контроллером.

7.4 Восстановление

В Рек. МСЭ-Т G.805 описаны методы усиления готовности транспортной сети. Для разъяснения этих методов употребляются термины "защита" (замена отказавшего ресурса на заранее установленный резервный ресурс) и "восстановление" (замена отказавшего ресурса посредством перемаршрутизации с использованием запасных возможностей). В целом действия по защите выполняются в пределах десятков миллисекунд, тогда как действия по восстановлению выполняются в диапазоне от сотен миллисекунд до нескольких секунд.

Слой управления волоконно-оптической сетью с автоматической коммутацией (ASON) обеспечивает оператору сети возможность предлагать вызовы потребителя с выбираемым классом услуги (CoS) (например, готовность, продолжительность прерываний, секунды с ошибками и пр.). Защита и восстановление – это механизмы (используемые сетью), которые поддерживают CoS, запрошенный пользователем. Выбор механизма, обеспечивающего живучесть системы (защита, восстановление или отсутствие такого механизма) для конкретного соединения, которое поддерживает вызов, основан на следующем: политика оператора сети, топология сети и возможности размещенного оборудования. Различные механизмы обеспечения живучести могут использоваться для соединений, которые составляются для обеспечения вызова. Если вызов проходит сеть, обслуживаемую несколькими

операторами, то каждая сеть должна отвечать за живучесть транзитных соединений. Запросы соединения на UNI и E-NNI будут содержать только запрашиваемый CoS без выраженного указания вида защиты или восстановления.

Защита или восстановления соединения может быть инициирована или временно выключена командой, поступившей с плоскости административного управления. Эти команды могут использоваться для выполнения планового технического обслуживания. Они могут также применяться для отмены автоматических операций при некоторых исключительных обстоятельствах отказа.

См. Рек. МСЭ-Т G.8080/Y1304.

7.5 Линейно-кабельные сооружения

Существует множество аспектов, относящихся к вопросу обеспечения безопасности систем электросвязи. МСЭ-Т рассматривает также аспекты, связанные с физической безопасностью линейно-кабельных сооружений. Изучаются проблемы, касающиеся устойчивой работы оборудования в случае пожара, стихийного бедствия и намеренного или случайного вторжения людей. Два наиболее важных вопроса, связанных с безопасностью, – это вопрос о том, как сделать компоненты систем, кабельные линии, соединительные муфты, шкафы и пр. физически устойчивыми к повреждениям, и вопрос о мониторинге систем в целях предотвращения какого-либо повреждения, если это возможно, или реагирования на проблемы, а также функционального восстановления систем самым оперативным образом.

В целом наиболее важными факторами, которые следует рассмотреть в связи с этими аспектами безопасности, являются:

- причина повреждения/потери данных:
  - техническое обслуживание сети;
  - аварии и катастрофы (ненамеренные);
  - вандализм (намеренный; бессистемный);
  - доступ со стороны неуполномоченных сотрудников (например, гражданских лиц, технических специалистов других операторов);
  - преступность (например, повреждение терминала или кросскоммутатора с целью взлома; кража кабелей; незаконный отвод кабеля и т. д.); и
  - намеренное сосредоточенное усилие или насилие;
- варианты размещения линейно-кабельных сооружений:
  - внутренние помещения (центральный офис, помещения для клиентов);
  - наружные подвесные (подверженность воздействию человека и природным явлениям);
  - наружные наземные (возможность повреждений в результате работ); и
  - наружные подземные (в траншеях или углубленные в почву).

В целом в отношении в качестве мер защиты физических объектов можно порекомендовать следующее: Большинство этих мер регулируются на уровне местной практики и правилами отдельных операторов:

- избегать применения узлов на уровне поверхности (шкафы, опоры, стенной короб): подверженность риску аварий, вандализма, насильственных действий, пожара и проявления обычного любопытства; более надежно использовать подземные узлы и кабели;
- шкафы на улице (или другие короба на уровне поверхности) должны быть иметь конструкцию, обеспечивающую защищенность от несанкционированного вскрытия;
- все корпуса должны запираться или запечатываться во избежание нежелательного доступа;
- кабели, находящиеся в канале, являются более защищенными, чем кабели, уложенные непосредственно в землю; так, последние могут случайно повредиться во время земляных работ;
- концевые или демаркационные точки могут иметь (запираемое) разделение между сетью и стороной клиента или между каналами, используемыми разными операторами;
- терминалы клиента, расположенные внутри помещения, более защищены, чем наружные (настенные) оконечные устройства клиента (например, на случай взлома);
- целесообразно хранить запасной кабель в местах прохождения сети, чтобы в случае повреждения (как в воздушной среде, так и под землей, его можно было легко устранить;

- в отношении волоконно-оптических кабелей рекомендуется поддерживать надлежащий уровень разделения и динамическую оптическую стабильность, с тем чтобы избежать потери данных/нарушения трафика при техническом обслуживании сети; и
- для очень важных линий можно порекомендовать дублирование (резервные линии) посредством физического разделения кабелей и сетей (например, кольцевых структур для банков и больниц).

Можно принять и другие меры, в частности:

- ввести процедуры защиты наружных установок;
- установить системы пожарообнаружения, а также системы наблюдения и контроля за наружными сооружениями;
- установить критерии оценки надежного сосуществования в одной и той же части сети нескольких операторов, предоставляющих многофункциональное обслуживание, например, POTS, ISDN, xDSL, без какого-либо наносящего ущерб взаимодействия;
- использовать технические решения, которые обеспечивают быструю реализацию развязывания при сохранении целостности, надежности и функциональной совместимости внутри сетевых топологий, используемых обычно во всем мире;
- установить сигнальные устройства вдоль подземных кабелей;
- обеспечить мониторинг, техническое обслуживание и системные испытания для наружных сооружений;
- изучить схему кабелей, которая выполняет главную функцию защиты физической целостности среды передачи данных – оптическое волокно; и
- рассмотреть аспекты, связанные с конструкцией кабелей, соединением волокна, организатором волокон и герметичными муфтами, блоками разветвления, изысканиями трассы кабеля и планированием маршрута, характеристиками кабелеукладочного судна, действиями по погружению и закладке, методами проведения ремонта, методами и защиты и испытаний в отношении наземных волоконно-оптических кабелей, приспособленных к морской среде.

8 Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи

Управление безопасностью и осведомленность предполагают ряд процессов. К ним относятся определение структур и процедур для обработки и распространения информации об инцидентах безопасности. В этой области эксперты МСЭ-Т также откликнулись на выраженные пожелания и разработали Рек. МСЭ-Т E.409. Целью Рек. МСЭ-Т E.409 "*Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*" являются анализ, структурирование и предложение метода для создания организации по управлению инцидентами внутри организации электросвязи, участвующей в обеспечении международной электросвязи, в центре внимания которой находятся течение и структура инцидента. Понятия "течение" и "обработка" используются при определении необходимости классифицировать какое-либо событие как "событие", "инцидент" "инцидент безопасности" или "кризис". Течение охватывает также первые критические решения, которые предстоит принять.

Эта Рекомендация содержит обзор и рамочные положения, которые служат руководством для планирования организации по реагированию на инциденты и обработки инцидентов безопасности.

Рекомендация носит общий характер, и в ней не определяются и не рассматриваются требования для конкретных сетей.

При том что эта Рекомендация предназначена для содействия международным разработкам в области безопасности сети электросвязи, таким разработкам было бы способствовать применение требований и к национальным инфокоммуникационным сетям (ICN).

Компьютерная преступность такими же быстрыми темпами, как и расширение использования компьютеров в международной электросвязи. За последние годы число компьютерных преступлений резко увеличилось, что подтверждено несколькими международными и национальными обследованиями. В большинстве стран отсутствуют точные цифры относительно числа компьютерных "взломов" или инцидентов безопасности, особенно тех, которые связаны с международной электросвязью.

Большинство организаций или компаний электросвязи не имеют специализированной организации для обработки инцидентов безопасности в инфокоммуникационных сетях (ICN) (хотя они могут иметь общую кризисную группу для обработки кризисов любого типа). Когда возникает инцидент безопасности ICN, он обрабатывается в режиме, применимом к данному случаю, т. е. человек, который обнаружил инцидент безопасности ICN, берет на себя ответственность за его обработку наилучшим для него образом. Возможно, в некоторых организациях пытаются забыть об инцидентах безопасности ICN и скрывать их, поскольку они могут повлиять на производительность, готовность и доходы.

Часто при обнаружении инцидента безопасности ICN, человек, который его обнаружил, не знает, кому сообщить об этом. Это может привести к использованию администратором системы или сети обходного действия или скороспелого решения лишь для того, чтобы избавиться от проблемы. Они не имеют делегированных полномочий, времени или опыта для исправления системы таким образом, чтобы инцидент безопасности ICN не повторился. Это является главными доводами в пользу создания обученного подразделения или группы, которые смогут обрабатывать инциденты безопасности быстро и правильно. Кроме того, многие из этих вопросов могут относиться к различным областям, таким как связи со средствами массовой информации, право, обеспечение соблюдения законов, доля на рынке или финансовые вопросы.

Использование разной систематики при сообщении об инциденте или при его обработке ведет к неправильному пониманию. Это, в свою очередь, может привести к тому, что инцидент безопасности ICN не получит ни должного внимания, ни быстрой обработки, которая необходима для остановки, ограничения и предотвращения повторения инцидента. Это может вызвать серьезные последствия для затронутой организации ("жертвы").

Чтобы иметь возможность добиться успеха в обработке инцидента и в сообщении о нем, необходимо понимать, каким образом обнаруживаются, обрабатываются и разрешаются инциденты. С помощью установления общей структуры инцидентов (т. е. физических, административных или организационных и логических инцидентов) можно получить общую картину структуры и течения какого-либо инцидента. Единообразная терминология служит основой для общего понимания слов и терминов.

8.1 Определения

Термин "инцидент безопасности" может быть определен определить как "взлом, угроза, слабое место и неисправность системы безопасности, которые могут повлиять на безопасность организационных ресурсов". В этой Рекомендации предполагается, что инцидент носит менее серьезный характер, чем инцидент безопасности, а инцидент информационной безопасности является определенным типом инцидента безопасности.

На рисунке 8-1 показана пирамида событий. Внизу находится событие, за которым следуют инцидент и инцидент безопасности, а на самом верху расположены кризис и катастрофа. Чем ближе к верхней части находится событие, тем оно серьезнее. Для того чтобы использовать общую и обоснованную терминологию в отношении обработки инцидентов в области ICN, рекомендуется употреблять нижеуказанные термины.

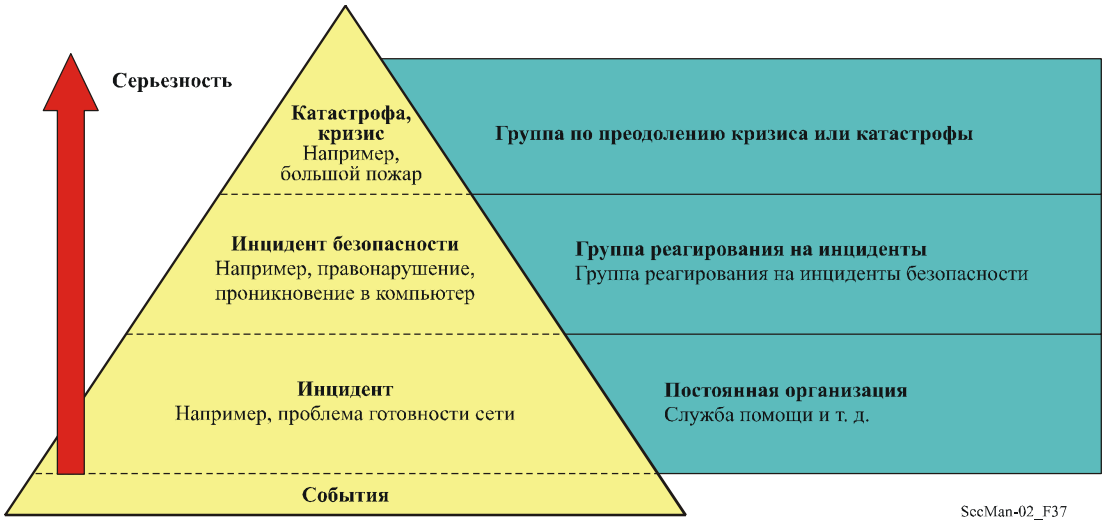


Рисунок 8-1 – Пирамида событий в Рек. МСЭ-Т E.409

8.1.1 **Событие**: Событие – это наблюдаемое явление, которое невозможно предсказать (целиком) или которым невозможно управлять.

8.1.2 **Инцидент**: Событие, которое может привести к явлению или эпизоду, не имеющему серьезного характера.

8.1.3 **Инцидент безопасности**: Инцидент безопасности – это любое неблагоприятное событие, в результате которого некий аспект безопасности может подвергнуться угрозе.

8.1.4 **Инцидент безопасности инфокоммуникационных сетей (ICN)**: Любое фактическое или предполагаемое неблагоприятное событие в отношении безопасности ICN. Это включает:

- проникновение в компьютерные системы ICN через сеть;
- появление компьютерных вирусов;
- зондирование через сеть уязвимостей ряда компьютерных систем;
- утечку вызовов учрежденческой АТС; и
- любые другие нежелательные события, являющиеся результатом несанкционированных внутренних или внешних действий, включая атаки в виде отказа в обслуживании, бедствия и другие чрезвычайные ситуации, и т. д.

8.1.5 **Кризис**: Кризис – это состояние, вызванное некоторым событием, или знание о приближающемся событии, которое может привести к серьезным негативным последствиям. Во время кризиса можно, в лучшем случае, иметь возможность принять меры для предотвращения перехода кризиса в катастрофу. На случай возникновения *катастрофы* обычно имеется План возобновления работы (BCP), а также группа кризисного управления для преодоления этой ситуации.

8.2 Обоснование

Рекомендуется, чтобы организации электросвязи, создающие группы реагирования на инциденты (компьютерной безопасности) (CSIRT), в качестве первого шага объявляли используемую ими систематику во избежание ошибочного понимания. Осуществлять сотрудничество значительно легче, когда используется один и тот же "язык".

Рекомендуется, чтобы организации использовали термины "инцидент" и "инцидент безопасности ICN", а также определили собственные производные термины с учетом серьезности инцидента безопасности ISN. По существу инцидент безопасности ICN является любым нежелательным, несанкционированным событием. Это значит, что инцидент безопасности ICN охватывает проникновение в компьютер, атаку "отказ в обслуживании" или вирус в зависимости от мотивировки, опыта и доступных хорошо осведомленных ресурсов в организации. В организациях, имеющих эффективную группу по борьбе с вирусами, вирусы могут рассматриваться не как инциденты безопасности ICN, а скорее как инциденты.

Примером, или шаблоном, такого образования производных терминов может быть следующее:

- Инциденты
  - Нарушение сетевого этикета Интернета (рассылка спама, вредоносный контент и т. д.)
  - Нарушение стратегии обеспечения безопасности
  - Отдельные вирусы
- Инциденты безопасности ICN
  - Сканирование и зондирование
  - Проникновение в компьютер
  - Компьютерные диверсия и повреждение (атаки на готовность, такие как "бомбардировка", атаки DoS)
  - Злонамеренное программное обеспечение (вирусы, программы "троянский конь", черви и т. д.)
  - Кража информации и шпионаж
  - Маскировка под законного пользователя

Использование одной и той же степени детализации и точности в терминологии дает возможность приобретать опыт в отношении:

- руководящих указаний относительно строгости и области применения;
- указания о необходимости действовать оперативно (например, для восстановления требуемого уровня безопасности);
- возможных встречных мер; и
- возможных соответствующих затрат.

9 Заключение

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 в серии X.810–X.816 определяется структура безопасности для открытых систем, которая включает общий обзор, аутентификацию, управление доступом, сохранность информации, конфиденциальность, целостность, а также проверку безопасности и аварийные извещения безопасности, соответственно. Недавно была разработана Рек. МСЭ-Т X.805, посвященная архитектуре безопасности для систем, обеспечивающих сквозную связь. Представленное в X.805 изменение архитектуры учитывает возрастающие угрозы и уязвимость, появившиеся вследствие возникновения среды, которую образуют множество сетей и множество поставщиков услуг. Рек. МСЭ-Т X.509, посвященная структуре открытых ключей и сертификату атрибутов, несомненно, является документом МСЭ-Т по приложениям безопасности, на который чаще всего ссылаются, прямо или косвенно, в других стандартах, разработанных на основе принципов X.509.

В дополнение к этим основополагающим Рекомендациям МСЭ-Т разрабатывает положения по безопасности для некоторых систем и услуг, определенных в его Рекомендациях. 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 обратить внимание на то, что, существует множество областей, в которых необходимо обеспечить безопасность электросвязи и информационных технологий и которые освещены в Рекомендациях МСЭ-Т. Эти вопросы и такие аспекты, как предотвращение мошенничества и ликвидация последствий бедствий, которые изучаются исследовательскими комиссиями МСЭ-Т, будут дополнительно 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 обеспечению безопасности, назначением в МСЭ-Т ведущей исследовательской комиссии по деятельности в области безопасности и сотрудничеством с другими организациями, занимающимися разработкой стандартов (например, ISO/IEC JTC 1/SC 27).

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] SCHNEIER (B.), "*Applied Cryptography – Protocols, Algorithms and Source Code in C*" 2nd edition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] CHADWICK (D. W.), "*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] UECHNER (M.), PROBST (P.-A.), "*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] CHADWICK (D. W.), MUNDY (D.), "*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 Telecommunication Security*" www.itu.int/ITU-T/studygroups/com17/tel-security.html (Catalogue of Approved Recommendations related to Telecommunication Security; Approved ITU-T Security Definitions)

[Shannon] SHANNON (G.), "*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] MANDIL (S.), DARBELLAY (J.), "*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

ISO/IEC 18033-1:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: General*

ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*

ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: Block ciphers*

ISO/IEC 18033-4:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: Stream ciphers*

Приложение А

Каталог Рекомендаций МСЭ-Т, связанных с безопасностью

Составлено 17-й Исследовательской комиссии МСЭ-Т, которая является ведущей комиссией по безопасности электросвязи

№	НАЗВАНИЕ	ГЛАВНАЯ ЦЕЛЬ И АСПЕКТЫ БЕЗОПАСНОСТИ	Исследовательская комиссия
E.408	Требования к безопасности сетей электросвязи	В этой Рекомендации представлен обзор требований к безопасности и структуру, которая выявляет угрозы безопасности сетей электросвязи в целом (как фиксированной, так и подвижной связи; как речевой, так и для передачи данных), и обеспечивает руководство для планирования встречных мер, которые могут быть приняты для уменьшения рисков, возникающих в результате угроз.	ИК2
E.409	Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи	Эта Рекомендация содержит анализ, структурирование и предложение метода для создания организации по управлению инцидентами внутри организации электросвязи, участвующей в обеспечении международной электросвязи, в центре внимания которой находятся течение и структура инцидента. Понятия "течение" и "обработка" используются при определении необходимости классифицировать какое-либо событие как "событие", "инцидент" "инцидент безопасности" или "кризис". Течение охватывает также первые критические решения, которые предстоит принять. Чтобы иметь возможность добиться успеха в обработке инцидента и в сообщении о нем, необходимо понимать, каким образом обнаруживаются, обрабатываются и разрешаются инциденты. С помощью установления общей структуры инцидентов (т. е. физических, административных или организационных и логических инцидентов) можно получить общую картину структуры и течения какого-либо инцидента. Единообразная терминология служит основой для общего понимания слов и терминов.	ИК17
F.400	Обзор систем и служб обработки сообщений	В этой Рекомендации содержится обзор всей системы и службы обработки сообщений (MHS), и он является общим обзором MHS. Этот обзор входит в группу Рекомендаций, описывающих модель системы, элементы службы "система обработки сообщений" (MHS) и услуги. В этой Рекомендации дан обзор возможностей MHS, используемых поставщиками услуг для обеспечения служб обработки сообщений (MH) 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 передачи 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 передачи 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 Рек. 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.	ИК17

F.440	Служба обработки сообщений: Служба обмена речевыми сообщениями (VM)	В этой Рекомендации заданы общие и рабочие аспекты, а также аспекты качества обслуживания международной службы обмена речевыми сообщениями (VM) общего пользования – специфического типа службы обработки сообщений (MH) общего пользования. Эта служба является международной службой электросвязи, предоставляемой Администрациями, которая дает абонентам возможность 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	ИК17
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.	ИК2
G.808.1	Обобщенная защитная коммутация – линейная защита канала и подсети	Представляет обзор линейной защитной коммутации. Она охватывает схемы защиты на базе оптических транспортных сетей (OTN), сетей с синхронной цифровой иерархией (SDH) и сетей с асинхронным режимом передачи (ATM). Обзоры схем межсоединений кольцевой защиты и подсети с двойным узлом (например, кольцевой) будут даны в других Рекомендациях.	ИК15
G.827	Параметры и цели функции готовности для сквозных международных цифровых трактов с постоянной скоростью передачи	Определяет параметры и цели работы сети для элементов тракта и сквозной готовности международных цифровых трактов с постоянной скоростью передачи. Эти параметры не зависят от типа физической сети, поддерживающей сквозной тракт, например, волоконно-оптической, радиорелейной или спутниковой. Содержит также руководство в отношении методов повышения готовности и вычисления сквозной готовности сочетания сетевых элементов.	ИК12
G.841	Типы и характеристики защитных архитектур SDH сетей	Описывает различные механизмы защиты сетей с синхронной цифровой иерархией (SDH), их задачи и приложения. Схемы защиты классифицируются как защита трассы SDH (на уровне раздела или на уровне тракта) и как защита соединения подсети SDH (с встроенным мониторингом, мониторингом без вмешательства и мониторингом подуровня).	ИК15

G.842	Взаимодействие архитектур защиты SDH сетей	В этой Рекомендации описаны механизмы взаимодействия между архитектурами защиты. Взаимодействие представлено в отношении присоединения в одном узле или в двух узлах с целью обмена трафиком между кольцами. Каждое кольцо может иметь конфигурацию для защиты с совместным использованием MS или для защиты SNCP.	ИК15
G.873.1	Волоконно-оптическая транспортная сеть (OTN) – Линейная защита	В этой Рекомендации определяется протокол APS и функция защитной коммутации для схем линейной защиты волоконно-оптической транспортной сети на уровне единицы данных оптического канала (ODUk). Схемы защиты, рассмотренные в этой Рекомендации, – это ODUk защита трассы; ODUk защита соединения подсети со встроенным мониторингом; ODUk защита соединения подсети с мониторингом без вмешательства; и ODUk защита соединения подсети с подуровневым мониторингом.	ИК15
G.911	Параметры и методы расчета в отношении надежности и готовности волоконно-оптических систем	В этой Рекомендации устанавливается минимальный набор параметров, необходимых для описания надежности и готовности волоконно-оптических систем. В ней приводятся различные параметры для надежности и технического обслуживания систем, для надежности активного оптического устройства, для надежности пассивного оптического устройства и для надежности оптического волокна и кабеля. В ней также содержатся руководящие указания и методы расчета прогнозируемой надежности устройств, блоков и систем, а также приводятся примеры.	ИК15
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 этой Рекомендации описывается 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 конкретного 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 отсутствует дешифрование в MCU.	ИК16
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 этой Рекомендации определены три альтернативных практических метода *управления ключами*.	ИК16
H.235	Защита и шифрование для мультимедийных терминалов серии H (H.323 и других терминалов на базе H.245)	В этой Рекомендации описаны усовершенствования в рамках Рекомендаций серии H.3xx с целью включения таких услуг безопасности, как *аутентификация* и *обеспечение секретности* (*шифрование данных*). Предложенная схема применима как к простому двухточечному соединению, так и к многоточечной конференции для терминалов, использующих протокол управления, предусмотренный в Рек. МСЭ-Т H.245. Например, системы H.323 функционируют через пакетные сети, не обеспечивая гарантированного качества обслуживания. По тем же техническим причинам, по которым базовая сеть не обеспечивает QoS, сеть не предоставляет *безопасную услугу*. Безопасная связь в реальном масштабе времени через незащищенные сети в целом связана с двумя важными аспектами – *аутентификация и секретность*. В этой Рекомендации описана инфраструктура безопасности и конкретные методы *обеспечения секретности*, которыми пользуются мультимедийные терминалы серии H.3xx. Рекомендация охватывает проблемы, касающиеся интерактивной конференц-связи. Эти проблемные аспекты включают *аутентификацию и секретность* всех потоков в реальном масштабе времени, которыми обмениваются в рамках конференц-связи, но не ограничиваются только ими. Предусматриваются протокол и алгоритмы, необходимые для связи между объектами H.323. В этой Рекомендации используются общие возможности, обеспеченные в Рек. МСЭ-Т H.245, и, собственно, любой стандарт, функционирующий в связи с эти протоколом управления, может применять эту структуру безопасности. Предполагается, что при любой возможности другие терминалы серии H могут взаимодействовать и напрямую использовать методы, описанные в этой Рекомендации. Первоначально она не предусматривает полной реализации во всех областях и конкретно посвящена *аутентификации конечной точки и секретности данных*.	ИК16

		Она предусматривает возможность согласовывать услуги и функциональные характеристики в общей форме и селективно выбирать применяемые методы криптографии и возможности. Конкретный способ их использования связан с системными возможностями, требованиями к приложениям и конкретными ограничениями стратегии безопасности. В Рекомендации, в зависимости от цели, например длины ключа, предлагаются различные варианты для разных криптографических алгоритмов предлагаются разные варианты. Для конкретных услуг по обеспечению безопасности могут быть предназначены определенные *криптографические алгоритмы* (например, один для шифрования потока данных, а другой для шифрования сигнализации). Следует также отметить, что некоторые из имеющихся криптографических алгоритмов или механизмов (например, с ограниченной длиной ключа) могут быть зарезервированы в целях экспорта или для других национальных потребностей. В этой Рекомендации предусматриваются хорошо известные алгоритмы сигнализации, наряду с нестандартизованными или собственными криптографическими алгоритмами сигнализации. Не существует каких-либо специально предписанных алгоритмов; однако настоятельно рекомендуется, чтобы для обеспечения функциональной совместимости конечные точки поддерживали максимальное возможное число применимых алгоритмов. Это совпадает с концепцией, согласно которой Рек. МСЭ-Т H.245 не гарантирует функциональной совместимости между кодеками двух объектов. Версия 2 Рек. МСЭ-Т H.235 отменяет версию 1 H.235, внося несколько усовершенствований, таких как шифрование методом эллиптических кривых, профили безопасности (простой на основе пароля и сложный на основе цифровой подписи), новые меры противодействия в области безопасности (защита носителей информации от спама), внедрение усовершенствованного алгоритма шифрования (AES), поддержка службы угла базы данных, определение идентификаторов объектов и изменения, внесенные из Руководства разработчика H.323. Версия 3 H.235 отменяет версию 2 H.235, предусматривая процедуру для шифрованных DTMF сигналов, идентификаторы объектов для алгоритмов шифрования при шифровании информационного сигнала среды, более совершенные способ поточного шифрования OFB (EOFB) для шифрования потока данных, содержащийся в Приложении D и предназначенный только в отношении аутентификации вариант для беспрепятственного прохождения NAT/системы защиты доступа, процедура распределения ключей на канале RAS, процедуры для более безопасной доставки сеансового ключа и более надежного распределения сеансовых ключей. В ней также содержатся обновленные процедуры защиты многократных потоков информационных сигналов, более надежное обеспечение безопасности для вызовов с прямой маршрутизацией, как предусмотрено в новом Приложении I, средства сигнализации для более гибкой отчетности об ошибках, разъяснения и более продуктивные методы быстрого запуска системы безопасности и для сигнализации Diffie-Hellman, наряду с более длинными параметрами Diffie-Hellman и изменениями, внесенными из руководства разработчиков H.323. Приложение F/H.235: *Гибридный профиль безопасности*. В этом приложении описан экономичный и масштабируемый *гибридный профиль безопасности на основе PKI* с внедрением *цифровых подписей* из Приложения E/H.235 и *базового профиля безопасности* из Приложения D/H.235. Это приложение рассматривается в качестве одного из вариантов. Объекты безопасности в H.235 (терминалы, пропускные пункты, шлюзы, многоточечные блоки и пр.) могут реализовать этот *гибридный профиль безопасности* для усиления безопасности или если потребуется. Понятие "гибридный" в этом документе означает, что процедуры безопасности в профиле подписи, предусмотренном в Приложении E/H.235, фактически применяются в облегченной форме; цифровые подписи все еще соответствуют процедурам RSA. Однако *цифровые подписи* используются только в случае, когда это абсолютно необходимо, тогда как в иных случаях применяются высокоэффективные *симметричные методы обеспечения безопасности* в базовом профиле безопасности, предусмотренном в Приложении D/H.235. Гибридный профиль безопасности применим для масштабируемой "глобальной" телефонии на основе IP. Этот профиль безопасности при строгом применении преодолевает ограничения, свойственные простому, базовому профилю безопасности, который предлагается в Приложении D/H.235. Кроме того, этот профиль безопасности при строгом применении лишен некоторых недостатков профиля, предусмотренного в E/H.235, таких как необходимость в более высокой пропускной способности и повышенные функциональные потребности в обработке. Например, гибридный профиль безопасности не зависит от (статического) управления совместными секретными ключами сетевых элементов в разных доменах. Так, пользователи могут гораздо проще выбрать поставщика услуг VoIP. Следовательно, этот профиль безопасности обеспечивает также определенную подвижность пользователя.	

		Он применяет асимметричное шифрование с использованием подписей и сертификатов только в случае необходимости, а в иных случаях использует более простые и более экономичные симметричные методы. Это обеспечивает туннелирование сообщений H.245 для обеспечения целостности сообщений H.245, а также в некоторой степени сохранность информации в сообщениях. Гибридный профиль безопасности предусматривает модель с GK-маршрутизацией и базируется на методах туннелирования H.245; поддержка моделей без GK-маршрутизации подлежит дальнейшему изучению Приложение G/H.235: *Использование протокола управления ключами MIKEY для SRTP в H.235*. Это приложение позволяет применять для безопасности данных разработанный IETF Защищенный протокол реального времени (SRTP), если протокол управления ключами MIKEY обеспечивает необходимые ключи и параметры безопасности среди участвующих конечных точек сквозной связи. Приложение G может применяться в области H.323 в отношении систем H.323, функционирующих на основе Приложения G к H.235. В приложении определяются расширения протокола безопасности относительно RAS и сигнализации о соединении, предусмотренных в H.225.0, а также относительно H.245 и рассматриваются соответствующие процедуры. Кроме того, в этом приложении предусмотрены возможности для поддержки взаимодействия с объектами IETF SIP, которые реализуют протокол управления ключами MIKEY и SRTP. Следует отметить, что это приложение разработано как профиль безопасности H.235, которые предлагается как вариант и может дополнять другие характеристики безопасности H.235 (см. его Приложения B и D.7). ПРИМЕЧАНИЕ. – H.235 была преобразована следующим образом: • H.235.0. Безопасность: Структура безопасности для мультимедийных систем серии H (H.323 и другие основанные на H.245) • H.235.1. Безопасность: Базовый профиль безопасности • H.235.2. Безопасность: Профиль безопасности с подписью • H.235.3. Безопасность: Гибридный профиль безопасности • H.235.4. Безопасность: Защита соединения с прямой и селективной маршрутизацией • H.235.5. Безопасность: Структура для надежной аутентификации в RAS с использованием слабо зашифрованных совместных секретных ключей • H.235.6. Безопасность: Профиль шифрования речи с управлением внутренним ключом H.235/H.245 • H.235.7. Безопасность: Использование протокола управления ключами MIKEY для SRTP в H.235 • H.235.8. Безопасность: Обмен ключами для SRTP с использованием надежных каналов сигнализации • H.235.9. Безопасность: Поддержка шлюза безопасности для H.323.	
H.323	Мультимедийные системы связи на основе пакетов	В этой 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 вычислительные сети, сети предприятий, городские сети, внутренние сети и внешние сети (включая интернет), соединения точка-точка, одиночный сегмент сети или объединенную сеть, содержащую много сегментов со сложной топологией; поэтому объекты 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. Приложение I: Безопасность для простых типов конечных точек.	ИК16

H.350.2	Архитектура служб каталогов для H.235	В этой Рекомендации описана схема LDAP для представления элементов H.235. Она представляет собой вспомогательную категорию, относящуюся к H.350, и многие ее функциональные характеристики обусловлены этой архитектурой. Прежде чем изучать эту Рекомендацию, разработчики должны подробно ознакомиться с H.350. К ее атрибутам относятся такие элементы, как идентичность, пароль и сертификат. Эти элементы могут быть загружены в конечную точку для автоматической конфигурации, или к ним можно получить доступ с пропускного пункта для сигнализации соединения и аутентификации. Область применения этой Рекомендации не включает нормативные методы использования самих каталогов LDAP или содержащихся в них данных. Цель данной схемы состоит не в том, чтобы представить все возможные элементы данных в протоколе H.235, а в том, чтобы представить минимальный набор, необходимый для достижения целей проектирования, перечисленных в H.350.	ИК16
H.530	Симметричные процедуры обеспечения безопасности для подвижной связи H.323 в H.510	В этой Рекомендации предусмотрены процедуры обеспечения безопасности в средах подвижной связи H.323, к которым применяется H.510, где описана подвижность для мультимедийных систем и служб. В ней приводится подробная информация о процедурах обеспечения безопасности для H.510. На настоящий момент возможности сигнализации H.235 в версиях 1 и 2 разработаны для обеспечения безопасности в средах H.323, являющихся преимущественно статическими. Эти среды и мультимедийные системы могут обладать некоторой ограниченной подвижностью в пределах зон пропускных пунктов; H.323 в целом и H.235 в частности обеспечивают весьма незначительную поддержку для надежного роуминга пользователей и терминалов подвижной связи в различных доменах с большим числом объектов, характеризующихся подвижностью, например в распределенной среде. Сценарии подвижности H.323, описанные в H.510, применительно к подвижности терминала создают новую ситуацию своим гибким и динамическим характером, в том числе в аспекте безопасности. Пользователи и терминалы подвижной связи, которые пользуются роумингом H.323, должны аутентифицироваться чужим, визитным доменом. Аналогичным образом, пользователь подвижной связи захочет получить доказательство подлинной идентичности визитного домена. Помимо этого, может также понадобиться доказательство идентичности терминалов в дополнение к аутентификации пользователя. Таким образом, эти требования предполагают взаимную аутентификацию пользователя и визитного домена, и, при желании, идентичности терминала. Обычно на первоначальной стадии только базовый домен знает пользователя подвижной связи, где он или она зарегистрирован(а) и где ему или ей выделен пароль; визитный домен не знает пользователя подвижной связи. Собственно визитный домен не имеет с пользователем и терминалом подвижной связи никакой установленных отношений в аспекте безопасности. С тем чтобы визитный домен мог получить гарантию аутентификации и авторизации в отношении пользователя и терминала подвижной связи, визитный домен должен через промежуточную сеть и служебные объекты передать базовому домену определенные задания по безопасности, такие как проверка авторизации или управление ключами. Это также требует обеспечения безопасности связи и управления ключами между визитным доменом и базовым доменом. Несмотря на то, что в принципе среды подвижной связи H.323 более открыты, чем закрытые сети H.323, естественно, необходимо также надлежащим образом защитить выполнение заданий по управлению ключами. Также верно и то, что связь внутри доменов подвижной связи и между доменами подвижной связи требует защиты от попыток злонамеренного искажения информации.	ИК16
J.93	Требования в отношении условного доступа во вторичном распределении цифрового телевидения по кабельным телевизионным системам	В этой Рекомендации определены требования в отношении секретности данных и доступа с целью защиты сигналов цифрового телевидения MPEG, проходящих по кабельным телевизионным сетям между входным концом кабеля и конечным абонентом. Используемые в этом процессе точные криптографические алгоритмы отсутствуют в J.93, так как они определяются в регионе и/или в отрасли.	ИК9

J.96	Технический метод обеспечения секретности в дальней международной телевизионной передаче телевидения MPEG-2 в соответствии с Рекомендацией J.89	В этой Рекомендации предусмотрен общий стандарт для системы условного доступа в дальней международной передаче цифрового телевещания в соответствии с профессиональным профилем MPEG-2 (4:2:2). В ней описывается базовая совместимая система скремблирования (BISS), основанная на спецификации DVB-CSA, с использованием постоянных незашифрованных ключей, называемых "символами сеанса связи". Другой совместимый с предыдущими версиями режим вводит дополнительный механизм для вставки "шифрованных символов сеанса связи" при одновременном сохранении функциональной совместимости.	ИК9
J.112	Системы передачи для служб интерактивного кабельного телевидения	Службы цифрового телевидения введены во многих странах, и широко признанны преимущества их расширения с целью предоставления интерактивных услуг. Системы распределения кабельного телевидения особенно подходят для реализации двунаправленных услуг по передаче данных, и эта Рекомендация дополняет и расширяет область применения J.83 "Цифровые многопрограммные системы для телевизионных, звуковых служб и служб передачи данных для распределения по кабелю", с тем чтобы предусмотреть двунаправленную передачу данных по коаксиальному и гибридному волоконно-коаксиальному кабелю для интерактивных служб. В ней содержатся также несколько приложений, посвященных различным существующим средам передачи данных. Рекомендуется, чтобы для введения быстрого доступа в Интернет и/или интерактивных служб кабельного телевидения использовать эти системы с целью получения преимуществ экономии за счет масштаба и содействия функционал ной совместимости. В Рекомендации предусмотрены требования в отношении безопасности, рекомендуется использовать спецификацию SP-DOCSS для передачи данных по кабельной системе безопасности (DOCSS); спецификация для сменного модуля безопасности (SP-RSM) и спецификацию базовой безопасности кабельной передачи данных (SP-BDS).	ИК9
J.160	Структура архитектуры для предоставления критичных по времени услуг по сетям кабельного телевидения с использованием кабельных модемов	Предоставляется структура архитектуры, которая позволит операторам кабельного телевидения предоставлять критичные по времени услуги по своим сетям, усовершенствованным для поддержки кабельных модемов. Услугами по обеспечению безопасности, предоставляемыми посредством основного уровня услуг системы IPCablecom, являются аутентификация, управление доступом, целостность, конфиденциальность и фиксация авторства. Интерфейс протокола IPCablecom может не использовать, использовать одну или несколько таких услуг для выполнения свойственных ему конкретных требований по обеспечению безопасности. Безопасность в IPCablecom отвечает требованиям к обеспечению безопасности каждого составляющего интерфейса протокола путем: • определения конкретной модели угроз для каждого составляющего интерфейса протокола; • определения услуг по обеспечению безопасности (аутентификация, санкционирование, конфиденциальность, целостность и фиксация авторства), требуемых для рассмотрения выявленных угроз; • указания конкретного механизма обеспечения безопасности, предоставляющего требуемые услуги по обеспечению безопасности. Механизмы обеспечения безопасности включают как протокол обеспечения безопасности (например, IPsec, безопасность уровня RTP и безопасность SNMPv3), так поддерживающий протокол управления ключами защиты (например, IKE, PKINIT/Kerberos).	ИК9
J.170	Спецификация обеспечения безопасности в IPCablecom	Определяется архитектура обеспечения безопасности, протоколы, алгоритмы, связанные с ними функциональные требования и любые технологические требования, которые могут обеспечить безопасность системы в сети IPCablecom. Должны быть предоставлены *услуги по обеспечению безопасности - аутентификация, управление доступом, целостность сообщения и содержания носителя, конфиденциальность и фиксация авторства*, как определено в этом документе для каждого интерфейса сетевого элемента.	ИК9

J.191	Пакет функций на основе IP для усовершенствования кабельных модемов	Предоставляется набор функций на основе IP, которые могут быть добавлены в кабельный модем, что позволит кабельным операторам предоставлять своим клиентам дополнительный набор усовершенствованных услуг, включая поддержку качества обслуживания (КО) в IPCablecom, повышенную безопасность, дополнительные функции управления и снабжения и улучшенную адресацию и обработку пакетов. Эти функции на основе IP присущи логическому элементу услуги портала (УП или просто портал). Кабельный модем, обладающий этими улучшенными функциями, - это усовершенствованный кабельный IP-модем (IPCM), который является реализацией класса устройств для домашнего доступа (ДД) J.190. Как описано в Рекомендации МСЭ-Т J.190, класс устройств ДД включает функциональные возможности кабельного модема и услуг портала. Вопросы обеспечения безопасности в Главе 11: определяются интерфейсы для обеспечения безопасности, протоколы и функциональные требования, необходимые для надежной доставки в портал по кабелю IP-услуг в безопасных условиях. Целью любой технологии безопасности является защита ценности, будь то поступления или коммерческий информационный актив какого-либо типа. Угрозы таким поступлениям существуют, если пользователь сети осознает их ценность, тратит усилия или деньги и изобретает технику, для того чтобы обойти осуществление необходимых платежей. Приложение С: угрозы безопасности и предупредительные меры.	ИК9
M.3010	Принципы сети управления электросвязью	Определяется концепция архитектур сети управления электросвязью (СУЭ) (функциональной архитектуры СУЭ, информационной архитектуры СУЭ и физических архитектур СУЭ) и их фундаментальных элементов, описывается взаимосвязь между этими тремя архитектурами и предоставляется основа для получения требований к спецификации физических архитектур СУЭ на основе функциональных и информационных архитектур СУЭ. Предоставляется логическая эталонная модель для разделения функциональных возможностей управления, называемая логической многослойной архитектурой (LLA). В настоящей Рекомендации определяется так же, как показать совместимость и соответствие для достижения взаимодействия. Эти требования к СУЭ включают возможность обеспечения безопасного доступа правомочных пользователей информации управления к этой информации. СУЭ включает функциональные блоки, для которых функция обеспечения безопасности осуществляется с помощью методов обеспечения безопасности для защиты среды СУЭ в целях обеспечения защищенности информации, которой обмениваются через интерфейсы и которая относится к приложению, относящемуся к управлению. Принципы и механизмы обеспечения безопасности имеют также отношение к управлению правами доступа пользователей СУЭ к информации, связанной с приложениями СУЭ.	ИК4
M.3016	Безопасность для плоскости административного управления	Предоставляется обзор и основа для идентификации угроз безопасности в отношении СУЭ и показывается, как доступные услуги обеспечения безопасности могут быть использованы в рамках функциональной архитектуры СУЭ, описанной в Рекомендации МСЭ-Т M.3010. Данная Рекомендация является обобщенной по своему характеру и не имеет целью определение или рассмотрение требований для конкретного интерфейса СУЭ. ПРИМЕЧАНИЕ. – Структура Рек. МСЭ-Т M.3016 была изменена следующим образом: • M.3016.0 – Безопасность для плоскости административного управления: обзор. • M.3016.1 – Безопасность для плоскости административного управления: требования по безопасности. • M.3016.2 – Безопасность для плоскости управления: услуги по обеспечению безопасности. • M.3016.3 – Безопасность для плоскости управления: механизм обеспечения безопасности. • M.3016.4 – Безопасность для уровня управления: проформа структуры.	ИК4
M.3210.1	Услуги управления СУЭ для управления обеспечением безопасности сетей IMT-2000	Одна из серии рекомендаций об услугах управления СУЭ, в которой предоставляется описание услуг управления, цели и контекст аспектов управления сетями IMT-2000. В настоящей Рекомендации описывается подгруппа услуг управления обеспечением безопасности для предоставления требований и анализа управления обеспечением безопасности и параметры *контроля за мошенничеством* в подвижной сети IMT-2000. Обращается внимание на интерфейс X между двумя поставщиками услуг и услугами управления, необходимыми обоим поставщикам для обнаружения и предотвращения мошенничества путем применения системы сбора информации о мошенничестве (FIGS) как средства наблюдения за определенным набором действий абонентов, с тем чтобы ограничить их финансовые риски перед большим количеством неоплаченных счетов, выставляемых на счета абонента, в то время как он перемещается. Рекомендация основана на наборах функций, указанных в Рек. МСЭ-Т M.3400, определяет новые наборы функций, функции и параметры и добавляет дополнительную семантику и ограничения.	ИК4

M.3320	Структура требований к управлению для интерфейса X СУЭ	Является частью серии, в которой рассматривается передача информации для управления услугами и сетями электросвязи, и только в некоторых частях рассматриваются аспекты обеспечения безопасности. Настоящая Рекомендация предназначена для определения основы для всех функциональных требований, требований к услугам и требований к сетевому уровню для обмена информацией СУЭ между администрациями. В ней предоставляется также общая основа использования интерфейса X СУЭ, предназначенного для обмена информацией между администрациями, признанными эксплуатационными организациями, другими операторами сетей, поставщиками услуг, клиентами и другими субъектами. Рекомендация включает спецификации требований обеспечения безопасности, предъявляемые к интерфейсу X СУЭ.	ИК4
M.3400	Функции управления СУЭ	Одна из серии рекомендаций о сети управления электросвязью (СУЭ), в которой предоставляются спецификации функций управления СУЭ и наборов функций управления СУЭ. Содержание разработано для поддержки целевой информационной базы B (Роли, ресурсы и функции), связанной с Целью 2 (Описание контекста управления СУЭ) в методике спецификации интерфейса СУЭ, указанной в Рек. МСЭ-Т M.3020. При выполнении анализа контекста управления СУЭ желательно учитывать максимальное использование наборов функций управления СУЭ, имеющихся в настоящей Рекомендации, В нее входят описания функции управления обеспечением безопасности, поддерживаемой СУЭ.	ИК4
Q.293	Интервалы, на которых должны быть приняты меры по обеспечению безопасности	В этой выдержке из Синей Книги содержатся только пункты 8.5 (Интервалы, на которых должны быть приняты меры по обеспечению безопасности) – 8.9 (Метод совместного использования нагрузки) Рек. МСЭ-Т Q.293.	ИК4
Q.813	Элемент прикладной услуги преобразований в целях обеспечения безопасности для элемента услуги дистанционных операций (ЭПУПБ-ЭУДО)	Предоставляются спецификации для поддержки преобразований в целях обеспечения безопасности, например *шифрование, хеширование, закрытие информации и подписи*, большое внимание уделено блокам данных протокола (БДП) элемента услуги дистанционных операций (ЭУДО). Преобразования в целях обеспечения безопасности используются для предоставления различных услуг обеспечения безопасности, например *аутентификации, конфиденциальности, целостности и неотрекаемости*. В настоящей Рекомендации описывается подход к обеспечению преобразований в целях безопасности, который реализуется на прикладном уровне и не требует наличия конкретных функциональных возможностей обеспечения безопасности в любом из базовых уровней стека ВОС. Настоящая Рекомендация направлена на повышение безопасности СУЭ путем поддержки преобразований в целях обеспечения безопасности блоков БДП ЭУДО и обмена соответствующей информацией об обеспечении безопасности.	ИК4
Q.815	Спецификация модуля обеспечения безопасности для защиты всего сообщения	Определяется факультативный модуль обеспечения безопасности для использования с Рек. МСЭ-Т Q.814, *Спецификация интерактивного агента взаимного обмена электронными данными*, который предоставляет услуги обеспечения безопасности для блоков данных протокола (БДП) в целом. В частности, модуль обеспечения безопасности поддерживает *фиксацию авторства в отношении отправителя и получателя*, а также *целостность сообщения* в целом.	ИК4
Q.817	Инфраструктура ключей общего пользования (PKI) СУЭ − Профили цифровых сертификатов и списков аннулирования сертификатов	Объясняется, как могут быть использованы в СУЭ цифровые сертификаты и списки аннулирования сертификатов, и предоставляются требования к использованию расширений сертификатов и списков аннулирования сертификатов. Рекомендация предназначена для содействия взаимодействию элементов СУЭ, которые используют инфраструктуру ключей общего пользования (PKI) для поддержки функций, относящихся к обеспечению безопасности. Цель состоит в предоставлении обеспечивающего взаимодействие и расширяемого механизма *управления и распространения ключей* в СУЭ, распространяемого на все интерфейсы, а также для поддержки *услуги неотрекаемости* через интерфейс X. Он применяется ко всем приложениям и интерфейсам СУЭ. Он не зависит от того, какой стек протоколов связи или какой протокол управления сетью используется. Средства PKI могут использоваться для широкого диапазона функций обеспечения безопасности, например, *аутентификации, целостности, неотрекаемости и обмена ключами защиты* (M.3016). Однако не указывается, каким образом такие функции должны быть реализованы – с PKI или без PKI.	ИК4
Q.1531	Требования обеспечения безопасности системы UPT (универсальная персональная электросвязь) для 1-го набора услуг	Указываются требования обеспечения безопасности системы UPT для связи между пользователем и сетью и между сетями, применимые к 1-му набору услуг UPT, определенному в Рек. МСЭ-Т F.851. Настоящая Рекомендация охватывает все аспекты обеспечения безопасности УПЭ с использованием доступов DTMF и доступов пользователей на основе внеполосной системы сигнализации DSS1.	ИК11

Q.1741.1	Ссылки на IMT-2000 для версии 1999 года, эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN	Включает ссылки на спецификации обеспечения безопасности 3GPP, т. е. на *TS 21.133: Угрозы безопасности и требования ее обеспечения, TS 33.102: Архитектура обеспечения безопасности, TS 33.103: Руководство по интеграции безопасности, TS 33.105: Требования к криптографическим алгоритмам, TS 33.106: Требования к законному перехвату, TS 33.107: Архитектура и функции законного перехвата, TS 33.120: Цели и принципы обеспечения безопасности*.	ИК19
Q.1741.2	Ссылки на IMT-2000 для версии 4, эволюционировавшей из GSM базовой сети UMTS с использованием сети доступа UTRAN	Включает ссылки на спецификации обеспечения безопасности 3GPP, такие как *TS 21.133: Угрозы безопасности и требования ее обеспечения, TS 22.048: Механизмы обеспечения безопасности для прикладного инструментария (U) SIM, TS 22.101: Аспекты обслуживания; принципы обслуживания, TS 33.102: Архитектура обеспечения безопасности, TS 33.103: Руководство по интеграции безопасности, TS 33.105: Требования к криптографическим алгоритмам, TS 33.106: Требования к законному перехвату, TS 33.107: Архитектура и функции законного перехвата, TS 33.120: Цели и принципы обеспечения безопасности,TS 33.200: Безопасность сетевого домена – MAP, TS 35.205, .206, .207, и .208: Спецификация набора алгоритмов MILENAGE*.	ИК19
Q.1741.3	Ссылки IMT-2000 на версию 5 центральной сети UMTS развитой GSM	Включает ссылки на спецификации обеспечения безопасности 3GPP, такие как *TS 22.101: Аспекты обслуживания; принципы обслуживания, TS 33.102: Архитектура обеспечения безопасности, TS 33.106: Требования к законному перехвату, TS 33.107: Архитектура и функции законного перехвата, TS 33.108: Интерфейс эстафетной передачи для законного перехвата (ЗП), TS 33.200: Безопасность сетевого домена – MAP, TS 33.203: Безопасность доступа для услуг на основе IP, TS 33.210: Безопасность; Безопасность сетевого домена (БСД); Безопасность уровня IP-сети, TS 35.205, .206, .207, .208 и .909: Спецификация набора алгоритмов MILENAGE*.	ИК19
Q.1742.1	Связь стандартов IMT-2000 со стандартом развитой основной сети ANSI-41 с сетью доступа cdma2000	Данная Рекомендация связывает стандарты для основной сети, опубликованные организациями по разработке стандартов (ОРС), со спецификациями 3GPP2, утвержденными 17 июля 2001 г. для стандарта семейства IMT-2000 "Развивающаяся основная сеть ANSI-41 с сетью доступа cdma2000". Спецификации 3GPP2, утвержденные в июле 2002 г., будут связаны с опубликованными стандартами для основной сети в будущей Рекомендации МСЭ-Т Q.1742.2. Стандарты радиоинтерфейса и радиосети доступа связаны со стандартами ОРС для этого стандарта из семейства IMT-2000 в Рекомендации МСЭ-R M.1457. Связь с другими стандартами семейства IMT-2000 определена в Рекомендациях МСЭ-Т серии Q.174x. Данная Рекомендация объединяет и связывает в общую рекомендацию соответствующие стандарты для основной сети, созданные рядом организаций по разработке стандартов, с этим стандартом семейства IMT-2000.	ИК19
Q.1742.2	Ссылки IMT-2000 (утвержденные на 11 июля 2002 года) на развитую опорную сеть ANSI-41 с сетью доступа cdma2000	Эта Рекомендация связывает стандарты для основной сети, опубликованные региональными организациями по разработке стандартов (ОРС), с теми спецификациями 3GPP2, которые были утверждены 11 июля 2002 года для стандарта семейства IMT-2000 "Развитая опорная сеть ANSI-41 с сетью доступа cdma2000". Спецификации 3GPP2, которые были утверждены 17 июля 2001 года, были связаны со стандартами для основной сети, опубликованными региональными организациями по разработке стандартов, в Рекомендации МСЭ-Т Q.1742.1. Спецификации 3GPP2, которые были утверждены в июле 2003 года, будут связаны с опубликованными стандартами для основной сети в будущей Рекомендации МСЭ-Т Q.1742.3. Радиоинтерфейс и сеть радиодоступа, а также стандарты ОРС для этого стандарта семейства IMT-2000 связаны в Рекомендации МСЭ-R M.1457-1. Связи для других стандартов семейства IMT-2000 определены в Рекомендациях МСЭ-Т серии Q.174x. Настоящая Рекомендация совмещает в себе и связывает в глобальную рекомендацию региональные стандарты для основной сети этого стандарта семейства IMT-2000.	ИК19
Q.1742.3	Эталонные спецификации IMT-2000 (утверждены по состоянию на 30 июня 2003 года) для развитой базовой сети ANSI-41 с сетью доступа cdma2000	Технические спецификации, упомянутые в Q.1742.3 в отношении аспектов обеспечения безопасности. *Межсистемные спецификации*: N.S0003-0 Модуль идентификации пользователя (версия 1.0; апрель 2001 г.) N.S0005-0 Межсистемные операции в сотовой радиосвязи (версия 1.0; дата отсутствует) N.S0009-0 IMSI (версия 1.0; дата отсутствует)	ИК19

		N.S0010-0 Усовершенствованные функции в широкополосных системах с распределенным спектром (версия 1.0; дата отсутствует) N.S0011-0 OTASP и OTAPA (версия 1.0; дата отсутствует) N.S0014-0 Усовершенствования аутентификации (версия 1.0; дата отсутствует) N.S0018 Начисление по предоплате TIA/EIA-41-D (версия 1.0.0; 14 июля 2000 г.) N.S0028 Сетевое взаимодействие между MAP GSM и MAP ANSI-41 (Rev. B, пересмотр: 0) (версия 1.0.0; апрель 2002 г.) *Спецификации пакетных данных*: P.S0001-A Стандарт беспроводной IP-сети (версия 3.0.0; 16 июля 2001 г.) P.S0001-B Стандарт беспроводной IP-сети (версия 1.0.0; 25 октября 2002 г.) *Спецификации услуг и системных аспектов*: S.R0005-B Эталонная сетевая модель для систем с распределенным спектром cdma2000 (пересмотр: B) (версия 1.0; 16 апреля 2001 года) S.R0006 Описание беспроводных функций (пересмотр: 0) (версия 1.0.0; 13 декабря 1999 г.) S.R0009-0 Модуль идентификации пользователя (версия 1.0; этап 1), пересмотр: 0 (13 декабря 1999 г.) S.R0018 Начисление по предоплате (версия 1.0.0; этап 1), пересмотр: 0 (13 декабря 1999 г.) S.R0019 Описание этапа 1 системы предоставления услуг на основе местоположения (LBSS) (версия 1.0.0) (22 сентября 2000 г.) S.R0032 Улучшенная аутентификация абонента (ESA) (версия 1.0) и улучшенная конфиденциальность абонента (ESP) (6 декабря 2000 г.) S.R0037-0 Модель архитектуры IP-сети для систем с распределенным спектром cdma2000 (версия 2.0; 14 мая 2002 г.) S.R0048 Идентификатор оборудования подвижной связи 3G (MEID) (версия 1.0) (10 мая 2001 г.) S.S0053 Общие криптографические алгоритмы (версия 1.0; 21 января 2002 г.) S.S0054 Спецификация интерфейса для общих криптографических алгоритмов (версия 1.0; 21 января 2002 г.) S.S0055 Улучшенные криптографические алгоритмы (версия 1.0; 21 января 2002 г.) S.R0058 Требования к системе мультимедийного IP-домена (версия 1.0; 17 апреля 2003 г.) S.R0059 Унаследованный домен ПС – требования к системе на этапе 1 (версия 1.0; 16 мая 2002 г.) S.R0066-0 Требования предоставления IP-услуг на основе местоположения на этапе 1 (версия 1.0; 17 апреля 2003 г.) S.R0071 Требования к требованиям контроля за пакетными данными унаследованной системы на этапе 1 (версия 1.0; 18 апреля 2002 г.) S.R0072 Требования к требованиям контроля только за пакетными IP-данными на этапе 1 (версия 1.0; 18 апреля 2002 г.) S.R0073 Управление конфигурацией доступа в интернет через карманный радиотелефон (IOTA) (версия 1.0), этап 1 (11 июля 2002 г.) S.S0078-0 Общие алгоритмы обеспечения безопасности (версия 1.0; 12 декабря 2002 г.)	

T.30	Процедуры для факсимильной передачи документов в коммутируемой телефонной сети общего пользования	В Приложении G предоставляются процедуры факсимильной передачи документов Группы 3 с использованием систем HKM и HFX. В Приложении H описываются возможности обеспечения безопасности факсимильной передачи документов Группы 3 на основе *алгоритма RSA*.	ИК16
T.36	Возможности обеспечения безопасности при использовании факсимильных терминалов Группы 3	Описываются два независимых технических решения, которые могут использоваться в контексте безопасной факсимильной передачи. Два технических решения основаны на алгоритмах HKM/HFX40 и *алгоритме RSA*.	ИК16
Прило-жение B к T.123	Соединения для расширенного транспортирования	В этом приложении к пересмотренной Рек. T.123 описывается *протокол переговоров о соединении (CNP)*, который позволяет согласовать возможность обеспечения безопасности. Применяемый механизм обеспечения безопасности включает различные средства для обеспечения сетевой и транспортной безопасности на межузловой основе, включающие TLS/SSL, IPSEC без IKE или ручное *управление ключами защиты*, X.274/TLSP ИСО и GSS-API.	ИК16
T.503	Прикладной профиль документа для обмена факсимильными документами Группы 4	Определяется прикладной профиль документа, который может использоваться любой телематической услугой. Цель Рекомендации состоит в определении формата обмена, подходящего для обмена факсимильными документами Группы 4, которые содержат только растровую графику. Обмен документами происходит только в форматированной форме, которая позволяет получателю отображать или распечатывать документ в том виде, который был предусмотрен отправителем.	ИК16
T.563	Характеристики терминалов для факсимильной аппаратуры Группы 4	Определяются общие аспекты факсимильной аппаратуры Группы 4 и интерфейса с физической сетью.	ИК16
T.611	Программный интерфейс связи (PCI) APPLI/COM для факсимильной Группы 3, факсимильной Группы 4, телетекса, телекса, электронной почты и услуг передачи файлов	Описывается программный интерфейс связи, называемый APPLI/COM, который обеспечивает унифицированный доступ к различным услугам связи, например к телефаксу группы 3 или другим телематическим услугам. В этой Рекомендации описывается структура и содержание сообщений и способ обмена сообщениями между местным приложением (МП) и приложением связи (ПС). Любому установлению связи предшествует процесс входа в систему, а завершается связь с помощью процесса выхода из системы, причем оба процесса содействуют реализации схем обеспечения безопасности, особенно важных в системах со многими пользователями, и предоставляют средства внедрения механизма обеспечения безопасности между МП и ПС. Настоящая Рекомендация устанавливает ППИ (прикладной программный интерфейс) высокого уровня, который предоставляет разработчикам приложений мощное средство для контроля и слежения за деятельностью в области электросвязи.	ИК16
X.217	Информационные технологии – Взаимодействие открытых систем – Определение услуги элемента услуги управления ассоциациями	Определяется услуги, предоставляемые элементом услуги управления ассоциациями (ACSE), для управления приложениями-ассоциациями в среде взаимодействия открытых систем. Элемент ACSE поддерживает режимы связи, ориентированные и не ориентированные на соединение. В ACSE определяется три функциональных блока. Обязательный *функциональный блок ядра* используется для установления и разблокировки приложения-ассоциаций. Элемент ACSE включает два функциональных блока, один из которых является факультативным функциональным блоком *аутентификации*, предоставляющим дополнительные средства для обмена информацией с целью поддержки аутентификации в ходе установления ассоциации без добавления новых услуг. *Средства аутентификации* элемента ACSE могут использоваться для поддержки ограниченного класса *методов аутентификации*. Поправка 1 обеспечивает поддержку механизмов аутентификации для режима без установления соединения.	ИК17

X.227	Информационные технологии – Взаимодействие открытых систем – Ориентированный на соединение протокол для элемента услуги управления ассоциациями: спецификация протокола.	Спецификация протокола определяет процедуры, применимые к моментам установления связи между системами, которые желают взаимодействовать в среде взаимодействия открытых систем в режиме, ориентированном на соединение, т. е. протокол режима, ориентированного на соединение, для приложения-услуги-элемента с целью управления приложением-ассоциациями (элемент услуги управления ассоциациями (ACSE)). Спецификация протокола включает блок *функционального ядра*, используемый для установления и разблокировки приложения-ассоциаций. *Функциональный блок аутентификации* предоставляет дополнительные средства для обмена информацией с целью поддержки *аутентификации* в ходе установления ассоциации без добавления новых услуг. *Средства аутентификации* ACSE могут использоваться для поддержки ограниченного класса *методов аутентификации*. Функциональный блок согласования прикладного контекста предоставляет дополнительное средство для выбора прикладного контекста в ходе установления ассоциации. Данная спецификация протокола включает приложение, в котором в виде таблицы состояний описывается протокольная машина, называемая протокольной машиной установления ассоциациями (ACPM). Данная спецификация протокола включает приложение, в котором описывается простой механизм аутентификации, использующий в качестве пароля название объекта приложения, предназначена для общего использования, и включает также пример *спецификации механизма аутентификации*. Данному механизму аутентификации присвоено следующее имя (ИДЕНТИФИКАТОР ОБЪЕКТА типа данных ASN.1): {joint-iso-itu-t(2) association-control(2) authentication-mechanism(3) password-1(1)} ({совместно-исо-мсэ-т(2) управление-ассоциаццией(2) механизм-аутентификации(3) пароль-1(1)}). Для данного механизма аутентификации паролем является значение аутентификации. Типом данных значения аутентификации должна быть "GraphicString" (графическая строка).	ИК17
X.237	Информационные технологии – Взаимодействие открытых систем – Протокол режима без установления соединения для элемента услуги управления ассоциациями: спецификация протокола	Поправка 1 к настоящей Рекомендации включает маркер расширяемости ASN.1 в модуле, описывающем этот протокол. Она усовершенствует также спецификацию протокола режима без установления соединения для ACSE с целью обеспечения поддержки транспортировки параметров аутентификации в APDU A-UNIT-DATA.	ИК17
X.257	Информационные технологии – Взаимодействие открытых систем – Протокол режима без установления соединения для элемента услуги управления ассоциациями: проформа свидетельства о соответствии протокольной реализации (PICS)	Предоставляется проформа свидетельства о соответствии протокольной реализации (PICS) для протокола режима без установления соединения в среде ВОС для элемента услуги управления ассоциациями (ACSE), указанного в Рек. МСЭ-Т X.237. Проформа PICS представляет в табличном виде обязательные и факультативные элементы протокола режима без установления соединения для ACSE. Проформа PICS используется для указания свойств и вариантов конкретной реализации протокола режима без установления соединения для ACSE.	ИК17

X.272	Сжатие данных и обеспечение конфиденциальности для сетей с ретрансляцией кадров	Описывается услуга сжатия данных и услуга обеспечения конфиденциальности для сетей с ретрансляцией кадров, включая согласование и инкапсуляцию сжатия данных, *безопасное сжатие данных, аутентификацию и шифрование данных* поверх ретрансляции кадров. Наличие *услуги сжатия* данных в сети увеличит ее пропускную способность. Потребность в передаче критичных данных по сетям общего пользования требует средств обеспечения *конфиденциальности* данных. В целях достижения оптимальных отношений сжатия важно осуществлять сжатие данных перед их *шифрованием*. Следовательно, в *услуге сжатия данных* желательно также предоставлять средства согласования *протоколов шифрования данных*. Поскольку задача сжатия и последующего шифрования данных связана с интенсивными вычислениями, эффективность достигается путем обеспечения одновременного *сжатия и шифрования данных (безопасного сжатия данных)*. Протоколы сжатия данных основаны на протоколе управления линией PPP (IETF RFC 1661) и протоколе управления шифрованием PPP (IETF RFC 1968 и 1969). Настоящая Рекомендация применяется к ненумерованным информационным кадрам (UI), инкапсулированным с использованием Приложения E Рек. Q.933. В ней рассматривается сжатие и конфиденциальность данных как при постоянных виртуальных соединениях (PVC), так и при коммутируемых виртуальных соединениях (SVC).	ИК17
X.273	Информационные технологии – Взаимодействие открытых систем – протокол обеспечения безопасности на сетевом уровне	Определяется протокол для поддержки *услуг обеспечения целостности, конфиденциальности, аутентификации и управления доступом*, указанный в модели обеспечения безопасности ВОС как применяемый к протоколам сетевого уровня для режима с установлением соединений и режима без установления соединений. Протокол поддерживает эти услуги путем использования *механизмов шифрования*, *маркировки защищаемой информации* и *присвоенных атрибутов,* таких как *криптографические ключи*.	ИК17
X.274	Информационные технологии – Электросвязь и обмен информацией между системами – Протокол обеспечения безопасности транспортного уровня	Определяется протокол, который может поддерживать *услуги обеспечения целостности, конфиденциальности, аутентификации и управления доступом*, указанные в модели обеспечения безопасности ВОС как относящихся к транспортному уровню. Протокол поддерживает эти услуги путем использования *механизмов шифрования*, *маркировки защищаемой информации* и присвоенных *атрибутов обеспечения безопасности,* таких как *криптографические ключи*.	ИК17
X.400/ F.400	Обзор систем и услуг обработки сообщений	Определяются элементы услуги, применяемые к системе обработки сообщений (MHS), для услуг обеспечения безопасности (*конфиденциальности, целостности, аутентификации, неотрекаемости* и *управления доступом*) между двумя агентами пользователя, двумя агентами передачи сообщений (MTA), UA и MTA, и UA и хранилищем сообщений (MS), которые определены как относящиеся к прикладному уровню. (см. F.400)	ИК17
X.402	Информационные технологии – Системы обработки сообщений (MHS): общая архитектура	В настоящей Рекомендации указываются процедуры обеспечения безопасности и идентификаторы объектов для использования в протоколах MHS с целью реализации услуг обеспечения *конфиденциальности, целостности, аутентификации, неотрекаемости* и *управления доступом*, которые определены как относящиеся к прикладному уровню.	ИК17
X.411	Информационные технологии – Системы обработки сообщений (MHS): определение и процедуры абстрактной услуги	Указываются механизмы и процедуры, поддерживающие *услуги конфиденциальности, целостности, аутентификации, неотрекаемости*, которые определены как относящиеся к прикладному уровню. Протокол поддерживает три услуги путем использования *криптографических механизмов, маркировки защищаемой информации, и цифровых подписей*, как указано в Рек. МСЭ-Т X.509. Несмотря на то, что настоящая Рекомендация определяет протокол, в котором используются *асимметричные методы шифрования,* поддерживаются также *симметричные методы шифрования*.	ИК17

X.413	Информационные технологии – Системы обработки сообщений (MHS): хранилище сообщений: определение абстрактной услуги	Определяются механизмы, протокол и процедуры, поддерживающие *услуги обеспечения целостности, управления доступом, аутентификации и неотрекаемости*, указанные как относящиеся к прикладному уровню. Протокол поддерживает эти услуги от имени непосредственного пользователя хранилища сообщений.	ИК17
X.419	Информационные технологии – Системы обработки сообщений (MHS): спецификации протоколов	Определяются процедуры и прикладные контексты с целью установления безопасного доступа к объектам MHS и удаленным пользователям путем предоставления услуг *аутентификации и управления доступом*, указанные как относящиеся к прикладному уровню.	ИК17
X.420	Информационные технологии – Системы обработки сообщений (MHS) – Система межперсональных сообщений	Определяются механизмы, протокол и процедуры для обмена объектами между пользователями системы межперсональных сообщений или агентами пользователя от имени его непосредственного пользователя, установленные как относящиеся к прикладному уровню. Поддерживаются услуги обеспечения безопасности - *целостности, конфиденциальности, аутентификации и управления доступом*, указанные как относящиеся к прикладному уровню.	ИК17
X.435	Информационные технологии – Системы обработки сообщений: система передачи для обмена электронными данными	Определяются механизмы, протокол и процедуры для обмена объектами между агентами пользователя системы обмена электронными данными (EDI) от имени их непосредственного пользователя. Поддерживаются услуги обеспечения безопасности – *целостности, конфиденциальности, аутентификации и управления доступом*, указанные как относящиеся к прикладному уровню.	ИК17
X.440	Системы обработки сообщений: система передачи голосовых сообщений	Определяются механизмы, протокол и процедуры для обмена объектами между агентами пользователя голосовой системы от имени их непосредственного пользователя. Поддерживаются услуги обеспечения безопасности - *целостности, конфиденциальности, аутентификации и управления доступом*, указанные как относящиеся к прикладному уровню.	ИК17
X.500	Информационные технологии – Взаимосвязь открытых систем – Справочник: Обзор понятий, моделей и услуг	Наряду с другими Рекомендациями настоящая Рекомендация создана для облегчения взаимодействия систем обработки информации с целью предоставления справочных услуг. Комплекс таких систем, вместе со справочной информацией, которая в них содержится, может рассматриваться как единое целое, называемое *Справочником*. Информация, содержащаяся в Справочнике, которая известна под общим названием информационной базы данных Справочника (DIB), как правило, используется для содействия установлению связи между, с или относительно таких объектов, как прикладные объекты, люди, терминалы и листы рассылки. Справочник играет важную роль в процессе взаимосвязи открытых систем, целью которой является обеспечение (с минимальными техническими соглашениями за пределами самих стандартов взаимодействия) взаимодействия систем обработки информации. В настоящей Рекомендации вводятся и моделируются понятия Справочника и DIB, рассматриваются услуги и возможности, которые они предоставляют. В других Рекомендациях эти модели используются для определения абстрактной услуги, предоставляемой Справочником, и для определения протоколов, при помощи которых эта услуга может быть получена или предоставлена. В настоящей Рекомендации определяются Справочник и его функции обеспечения безопасности.	ИК17
X.501	Информационные технологии – Взаимосвязь открытых систем – Справочник: модели	В Рекомендации предоставляется ряд различных моделей Справочника в качестве основы для других Рекомендаций МСЭ-Т серии X.500. Этими моделями являются общая (функциональная) модель, модель административных полномочий, обобщенные информационные модели Справочника, отражающие взгляды пользователя Справочника и административного пользователя об информации Справочника, обобщенные модели системного агента справочника (DSA) и информационные модели DSA, а также эксплуатационная структура и модель обеспечения безопасности. В Рекомендации определяется использование в справочнике структур сертификатов открытых ключей и атрибутов X.509.	ИК17

X.509	Информационные технологии – Взаимосвязь открытых систем – Справочник: Основа аутентификации (издание 1993 г. – *второе издание/версия*) Основа аутентификации (издание 1997 г. – *третье издание/версия*) Структуры сертификатов открытых ключей и атрибутов (издание 2000 г. – *четвертое издание/версия*) Структуры сертификатов открытых ключей и атрибутов (издание 2005 г. – *пятое издание/версия*)	Определяется структура сертификатов открытых ключей и атрибутов и определяется основа предоставления справочником услуг аутентификации для его пользователей. Описываются два уровня аутентификации: *простая аутентификация*, при которой пароль используется в качестве проверки заявленной идентификационной информации; и *строгая аутентификация*, при которой имя пользователя и пароль формируются с использованием методов шифрования. Тогда как простая аутентификация предоставляет некоторую ограниченную защиту против несанкционированного доступа, только строгая аутентификация должна использоваться в качестве основы для предоставления защищенных услуг. Определенные структуры могут использоваться для применения профиля к *инфраструктурам открытых ключей* (PKI) и *инфраструктурам управления полномочиями* (PMI). Структура сертификатов открытых ключей включает спецификацию объектов данных, используемую для представления самих сертификатов, а также уведомления об аннулировании в отношении выпущенных сертификатов, которым больше не следует доверять. Тогда как в Рекомендации определяются некоторые критичные компоненты PKI, в ней не определяется PKI в целом. Однако предоставляется основа для создания полных инфраструктур PKI и их спецификаций. Структура для сертификатов атрибутов включает спецификацию *объектов данных*, используемую для представления самих сертификатов, а также *уведомлений об аннулировании* в отношении выпущенных сертификатов, которым больше не следует доверять. Тогда как в Рекомендации определяются некоторые критичные компоненты PMI, в ней не определяется PMI в целом. Однако предоставляется основа для создания полных инфраструктур PMI и их спецификаций. Определяются также *информационные объекты* для размещения в справочнике объектов PKI и PMI и для сравнения представленных и сохраненных значений.	ИК17
X.519	Информационные технологии – Взаимосвязь открытых систем – Справочник: спецификация протокола	Определяются процедуры и прикладные контексты для установления защищенного доступа в ходе привязки объектов Справочника.	ИК17
X.680	Информационные технологии – Системные и сетевые аспекты ВОС – Абстрактная синтаксическая нотация версии 1 (ASN.1): спецификация основной нотации	Предоставляется стандартная нотация, называемая абстрактной синтаксической нотацией версии 1 (ASN.1), для определения синтаксиса информационных данных. Определяется ряд типов простых данных и указывается нотация для ссылки на эти типы и определения значений этих типов. Нотации ASN.1 могут быть применены всегда, когда необходимо определить абстрактный синтаксис информации без какого-либо ограничения в отношении того, каким образом информация кодируется на передаче. Нотация ASN.1 используется для определения типов данных, значений и ограничений, налагаемых на типы данных, т. е. она определяет число простых типов и их признаков и определяет нотацию для ссылок на эти типы и для указания значений этих типов; определяет механизмы для создания новых типов на основе большего числа базовых типов и определяет нотацию для определения таких типов; определяет наборы символов (путем ссылки на другие рекомендации) для использования в ASN.1. Тип данных (или сокращенно - тип) – это категория информации (например, цифровой, текстовой, в виде неподвижных изображений или видеоинформации). Значение данных (или сокращенно – значение) – это пример такого типа. Настоящая Рекомендация определяет несколько базовых типов и соответствующих им значений и правила для их объединения в более сложные типы и значения. В некоторых архитектурах протоколов каждое сообщение определяется как двоичное значение последовательности октетов. Однако разработчикам стандартов необходимо определять довольно сложные типы данных для переноса сообщений, не задумываясь об их представлении в двоичной форме. В целях определения этих типов данных для них необходима нотация, которая необязательно определяет представление каждого значения. Такой нотаций является ASN.1. Данная нотация дополняется спецификацией одного или нескольких алгоритмов, называемых правилами кодирования, которые определяют значение октетов, переносящих прикладную семантику (называемой синтаксисом перехода). ПРИМЕЧАНИЕ. – Серия рекомендаций об ASN.1 (и в частности отличительные и канонические правила кодирования ASN.1) были широко использованы во многих Рекомендациях и стандартах, относящихся к вопросам обеспечения безопасности. В частности, Рекомендация H.323 и рекомендации серий X.400 и X.500 существенно зависят от ASN.1. Эти рекомендации создали и продолжают создавать важные структурные элементы для работы в области обеспечения безопасности.	ИК17

X.681	Информационные технологии – Системные и сетевые аспекты ВОС – Абстрактная синтаксическая нотация версии 1 (ASN.1): спецификация информационного объекта	Предоставляется нотация ASN.1, которая позволяет определять классы информационных объектов, а также отдельные информационные объекты и их наборы и присваивать имена для обращения к ним, т. е. предоставляется нотация для определения классов информационных объектов, информационных объектов и наборов информационных объектов. Класс информационного объекта определяет формат концептуальной таблицы (набор информационных объектов), в которой одна колонка предусмотрена для каждого поля в классе информационного объекта, а полная строка определяет информационный объект. Разработчику приложения часто необходимо создавать протокол, который будет работать с любым представителем некоторого класса информационных объектов, где представитель класса может определяться различными другими органами, и может быть добавлен со временем. Примерами таких классов информационных объектов являются "операции" услуги дистанционной работы (ROS) и "атрибуты" справочника в среде ВОС. В настоящей Рекомендации дается нотация, которая позволяет определять классы информационных объектов, а также отдельные информационные объекты и их наборы и присваивать имена для обращения к ним. См. ПРИМЕЧАНИЕ, выше (X.680).	ИК17
X.682	Информационные технологии – Системные и сетевые аспекты ВОС – Абстрактная синтаксическая нотация версии 1 (ASN.1): спецификация ограничений	Является частью рекомендаций, относящихся к абстрактной синтаксической нотации версии 1 (ASN.1), и предоставляет нотацию для установления ограничений, определяемых пользователем, табличных ограничений и ограничений по содержанию. Предоставляется нотация ASN.1 для общего случая ограничения и спецификации исключения, с помощью которых могут быть ограничены значения данных типа структурированных данных. Нотация обеспечивает также передачу сигнализации, если и когда-то или иное ограничение нарушается. Разработчикам приложений требуется нотация для определения типа структурированных данных с целью транспортирования их семантики. Нотация необходима также для дополнительного ограничения значений, которые могут появиться. Примеры таких ограничений держат в определенных пределах диапазон некоторого(ых) компонента(ов) или используют определенный информационный объект для ограничения компонента "ObjectClassFieldType" или используют "AtNotation" для определения соотношения между компонентами. См. ПРИМЕЧАНИЕ, выше (X.680).	ИК17
X.683	Информационные технологии – Системные и сетевые аспекты ВОС – Абстрактная синтаксическая нотация версии 1 (ASN.1): Задание параметров спецификаций ASN.1	Рекомендация является частью рекомендаций, относящихся к абстрактной синтаксической нотации версии 1 (ASN.1), и определяет нотацию для задания параметров спецификации ASN.1, т. е. определяет положения в отношении параметризированных имен для обращения и параметризированных присвоений для типов данных, которые являются полезными для разработчиков при составлении спецификаций в тех случаях, когда на некоторых этапах разработки какие-либо аспекты остаются неопределенными до более позднего этапа, на котором создается полное определение абстрактного синтаксиса. Разработчикам приложений приходится составлять спецификации, в которых некоторые аспекты остаются неопределенными. Эти аспекты определяются на более позднем этапе в одной или нескольких других группах (каждый по-своему) для создания полностью определенной спецификации с целью использования в определении абстрактного синтаксиса (одного для каждой группы). В некоторых случаях аспекты спецификации (например, предельные значения) могут оставаться неопределенными даже в момент определения абстрактного синтаксиса, их определение завершается с помощью спецификации международных стандартизированных профилей или функциональных профилей некоторого другого органа. См. ПРИМЕЧАНИЕ, выше (X.680).	ИК17
X.690	Информационные технологии – Правила кодирования ASN.1: Спецификация правил базового кодирования (BER), канонических правил кодирования (CER) и отличительных правил кодирования (DER)	Устанавливает набор правил базового кодирования (BER), которые могут применяться к значениям типов, определенных с использованием нотации ASN.1, т. е. использоваться для получения спецификации синтаксиса перехода для значений типов, определенных с использованием нотации, которая указана в серии Рекомендаций МСЭ-Т X.680 и называется абстрактной синтаксической нотации версии 1 или ASN.1. Применение этих правил кодирования создает синтаксис перехода для таких значений. В спецификации этих правил кодирования подразумевается, что они также используются для декодирования, т. е. эти правила базового кодирования должны применять также для декодирования такого синтаксиса перехода в целях идентификации значений переданных данных. В Рекомендации определяется также набор канонических и отличительных правил кодирования, ограничивающих кодирование значений только одним вариантом, предоставляемым правилами базового кодирования, т. е. определяется также набор отличительных правил кодирования (DER) и набор канонических правил кодирования (CER), которые налагают ограничения на правила базового кодирования (BER). Ключевым различием между ними является то, что DER используют форматы кодирования определенной длины, тогда как CER используют форматы неопределенной длины. DER больше подходят для малых кодируемых значений, тогда как CER годятся для больших значений. В спецификации этих правил кодирования подразумевается, что они также используются для декодирования. См. ПРИМЕЧАНИЕ, выше (X.680).	ИК17

X.691	Информационные технологии – Правила кодирования ASN.1: Спецификация правил пакетного кодирования (PER)	В серии Рекомендаций X.680 описывается абстрактная синтаксическая нотация версии 1 (ASN.1) – нотация для определения сообщений, которыми должны обмениваться приложения. В настоящей Рекомендации описывается набор правил кодирования, которые могут быть применены к значениям всех типов ASN.1 с целью достижения гораздо более компактного представления, по сравнению с достижимым с помощью правил базового кодирования и их производных (описанных в Рек. X.690), т. е. она описывает набор правил пакетного кодирования, которые могут быть использованы для получения синтаксиса перехода для значений типов, определенных в Рек. МСЭ-Т X.680. Правила пакетного кодирования должны также применяться для декодирования такого синтаксиса перехода в целях определения значений переданных данных. Существует более одного набора правил кодирования, которые могут применяться к значениям типов ASN.1. Эти правила пакетного кодирования (PER) называются так, потому что с их помощью достигается гораздо более компактное представление, чем может быть достигнуто посредством правил базового кодирования (BER), а их производные описаны в Рек. МСЭ-Т X.690. См. ПРИМЕЧАНИЕ, выше (X.680).	ИК17
X.692	Информационные технологии – Правила кодирования ASN.1: Спецификация нотации управления кодированием (ECN) + Приложение E: Поддержка кодирования Хоффмана	Определяется нотация управления кодированием (ECN), используемая для определения способов кодирования типов ASN.1 или частей типов, которые отличаются от способов кодирования, обеспечиваемых стандартизованными правилами кодирования, таких как правила базового кодирования (BER) и правила пакетного кодирования (PER). В рекомендации предоставляется несколько механизмов для такой спецификации, а также методы соединения спецификаций способов кодирования с определениями типов, к которым они должны применяться. Нотация ECN может использоваться для кодирования спецификации всех типов ASN.1, но может также использоваться совместно со стандартизованными правилами кодирования, такими как BER или PER для определения только кодирования типов, имеющих специальные требования. Любой тип ASN.1 определяет некоторый набор абстрактных значений. Правила кодирования определяют представление этих абстрактных значений в виде последовательности битов. См. ПРИМЕЧАНИЕ, выше (X.680).	ИК17
X.693	Информационные технологии – Правила кодирования ASN.1: Правила кодирования с использованием XML	Опубликование абстрактной синтаксической нотации версии 1 (ASN.1) привело к тому, что она стала обычно используемой нотацией для определения сообщений, которыми должны обмениваться равноправные приложения. В настоящей Рекомендации определяются правила кодирования, которые могут применяться для кодирования значений типов ASN.1 с использованием расширяемого языка разметки (XML), т. е. определяется набор правил базового кодирования с XML (XER), которые могут применяться для получения синтаксиса перехода для типов значений, определенных в серии Рекомендаций X.680. В данной Рекомендации определяется также набор правил канонического кодирования с XML, которые налагают ограничения на правила базового кодирования с XML и создают уникальный способ кодирования для любого данного значения ASN.1. В спецификации этих правил кодирования подразумевается, что они также используются для декодирования. Применение этих правил кодирования образует синтаксис перехода для таких значений. В спецификации этих правил кодирования подразумевается, что они также используются для декодирования. Существует более одного набора правил кодирования, которые могут применяться к значениям типов ASN.1. В настоящей Рекомендации определяется два набора правил кодирования, использующих расширяемый язык разметки (XML). Она называются правилами кодирования с XML (XER) для ASN.1 и создают документ XML, соответствующий XML 1.0 W3C. Первый набор называется правилами базового кодирования с XML. Второй набор называется правилами канонического кодирования с XML, поскольку существует только один способ кодирования той или иной величины ASN.1 с использованием этих правил кодирования. (Правила канонического кодирования обычно используются для приложений, использующих функции, относящиеся к обеспечению безопасности, такие как цифровые подписи.)	ИК17
X.733	Информационные технологии – Взаимодействие открытых систем – Управление системами: функция аварийного оповещения	Определяется функция управления системами, которая может использоваться каким-либо прикладным процессом в централизованной или децентрализованной среде управления для взаимодействия с целью осуществления управления системами. В настоящей Рекомендации определяется функция, которая состоит из типичных определений, служебных и функциональных блоков, и располагается на прикладном уровне. Оповещения об аварийной ситуации, определяемые этой функцией, предоставляют информацию, которая может быть необходима администратору для осуществления действий, в соответствии с условиями эксплуатации системы и качеством предоставляемого ею обслуживания.	ИК4

X.735	Информационная технология – Взаимодействие открытых систем – Управление системами: функция управления журналом регистрации	Определяется функция управления системами, которая может использоваться каким-либо прикладным процессом в централизованной или децентрализованной среде управления для взаимодействия с целью осуществления управления системами. В настоящей Рекомендации определяется функция управления журналом регистрации, которая состоит из служебных и двух функциональных блоков. Данная функция располагается на прикладном уровне.	ИК4
X.736	Информационные технологии – Взаимодействие открытых систем – Управление системами: функция оповещения о нарушении безопасности	Определяется функция оповещения о нарушении безопасности, являющаяся функцией управления системами, которая может использоваться каким-либо прикладным процессом в централизованной или децентрализованной среде управления для обмена информацией с целью осуществления управления системами. Данная Рекомендация относится к прикладному уровню. Оповещения о нарушении безопасности, определяемые этой функцией управления системами, предоставляют информацию, которая касается условий эксплуатации и качества обслуживания, относящихся к обеспечению безопасности.	ИК4
X.740	Информационные технологии – Взаимо-действие открытых систем – Управление системами: Функция предоставления данных проверки безопасности	Определяется функция предоставления данных проверки безопасности. Функция предоставления данных проверки безопасности – это функция управления системами, которая может использоваться каким-либо прикладным процессом в централизованной или децентрализованной среде управления для обмена информацией и командами с целью осуществления управления системами. Данная функция располагается на прикладном уровне.	ИК4
X.741	Информационные технологии – Взаимодействие открытых систем – Управление системами: объекты и атрибуты для управления доступом	Определяются спецификации, применимые к обеспечению управления доступом для приложений, в которых используются протоколы и услуги управления в среде ВОС. Информация об управлении доступом, определенная настоящей Рекомендацией, может быть использована для поддержки схем управления доступом, основанных на списках управления, возможностях, уровнях защиты и контекстных ограничениях.	ИК4
X.790	Функция управления неисправностями для приложений МСЭ-Т	Рассматриваются вопросы управления нарушениями работы систем и сетей связи с позиции поставщика услуги и пользователя этой услуги. Нарушение работы, называемое "неисправностью", является проблемой, которая неблагоприятно влияет на качество обслуживания, воспринимаемого пользователями сети. При обнаружении неисправности, возможно в результате аварийного оповещения, уведомление о неисправности может поступить от пользователя, или же уведомление может быть автоматически выдано системой. Управление этим уведомлением о неисправности необходимо, с тем чтобы обеспечить его принятие во внимание и устранение неисправности для восстановления услуги к прежнему уровню ее возможностей. Формат уведомления определяется так, чтобы позволить пользователю сообщить о неисправности, которая затем должна быть устранена поставщиком услуг. В ходе устранения неисправности поставщиком услуги ее пользователь может определять текущее состояние решения проблемы путем выдачи запроса на информацию об этом. После устранения неисправности поставщик может уведомить об этом пользователя. В Рекомендацию включена информация о конкретных типах неисправностей; однако следует учесть, что применение настоящей Рекомендации для конкретного приложения может потребовать использования типов неисправностей, характерных для данного приложения, что предусмотрено в данной Рекомендации. Во время появления неисправности сеть могла взаимодействовать с другой сетью с целью предоставления услуги, и проблема или нарушение работы могли быть вызваны другой сетью. Поэтому может быть необходимо осуществлять обмен информацией об управлении неисправностями между системами управления через интерфейсы, которые могут быть интерфейсами между клиентом и поставщиком услуг или между поставщиками услуг и могут представлять собой границы между сферами различных полномочий, а также границы внутри одной и той же сферы полномочий. В дополнение к обмену информацией о неисправности, которая уже была обнаружена, может быть также необходимо обмениваться предварительной информацией о недоступности услуги. Таким образом, поставщику услуг может быть необходимо информировать клиента о будущей недоступности услуги (например, из-за запланированного технического обслуживания). Сфера применения Рекомендации включает все перечисленные выше процессы обмена информацией управления.	ИК4

X.800	Архитектура обеспечения безопасности в среде взаимодействия открытых систем для приложений МККТТ	Определяются общие элементы архитектуры, имеющие отношение к обеспечению безопасности, которые могут применяться соответствующим образом в условиях, при которых требуется защита связи между открытыми системами. В рамках эталонной модели в Рекомендации устанавливаются руководящие принципы и ограничения для улучшения существующих рекомендаций или для разработки новых рекомендаций в контексте ВОС, с тем чтобы сделать возможной защищенную связь и, таким образом, обеспечить последовательный подход к безопасности при ВОС. Настоящая Рекомендация расширяет эталонную модель для охвата аспектов обеспечения безопасности, которые являются общими элементами архитектуры протоколов связи, но не обсуждаются в эталонной модели. В данной Рекомендации содержится общее описание услуг обеспечения безопасности и относящихся к ним механизмов, которые могут быть обеспечены эталонной моделью, и определяются положения этих услуг и механизмов в рамках эталонной модели, где они могут быть предоставлены.	ИК17
X.802	Информационная технология – Модель обеспечения безопасности низших уровней	Описываются аспекты перекрестного уровня, относящиеся к пересмотру услуг обеспечения безопасности на низших уровнях эталонной модели ВОС (транспортном, сетевом, линии передачи данных, физическом). В Рекомендации описываются общие для этих уровней архитектурные решения, основа взаимодействия, относящаяся к обеспечению безопасности между уровнями, и размещение протоколов обеспечения безопасности на низших уровнях.	ИК17
X.803	Информационные технологии – Взаимодействие открытых систем – модель обеспечения безопасности высших уровней	Описываются выбор, размещение и использование услуг и механизмов обеспечения безопасности на высших уровнях (прикладной уровень, уровень представления и сеансовый уровень) эталонной модели ВОС.	ИК17
X.805	Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами	Рекомендация определяет общие элементы архитектуры, относящиеся к обеспечению безопасности, которые при надлежащем применении, в частности, в условиях наличия многих поставщиков, могут обеспечить должную защиту сети от предумышленных и неумышленных попыток нарушения защиты, и направлена на обеспечение таких рабочих параметров, как высокая готовность, соответствующие время реакции, целостность, расширяемость и функция правильного выставления счетов.	ИК17
X.810	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: обзор	Определяется инфраструктура, в рамках которой определяются услуги обеспечения безопасности открытых систем. В этой части инфраструктуры обеспечения безопасности описывается организация *инфраструктуры обеспечения безопасности*, определяются *концепции обеспечения безопасности*, требуемые для нескольких частей инфраструктуры обеспечения безопасности и описывается взаимосвязь услуг и механизмов, определенных в других частях. Данная инфраструктура описывает все аспекты *аутентификации*, применяемые к открытым системам, взаимосвязь аутентификации с другими функциями обеспечения безопасности, такими как *управление доступом* и требования к управлению аутентификацией.	ИК17
X.811	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: основа аутентификации	Определяется общая основа для обеспечения аутентификации. Главная цель аутентификации состоит в *противодействии угрозам маскировки и повторной передачи*.	ИК17

X.812	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: основа управления доступом	Определяется общая основа для обеспечения управления доступом. Главная цель управления доступом состоит в *противодействии угрозам несанкционированных операций*, в которых задействована компьютерная система или система связи; эти угрозы часто подразделяют на классы, известные как *несанкционированное использование, разглашение, изменение, разрушение и отказ в услуге*.	ИК17
X.813	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: основа обеспечения неотрекаемости	Определяется общая основа для предоставления услуг обеспечения неотрекаемости. Главная цель услуги неотрекаемости состоит в *сборе, поддержании, предоставлении в распоряжение и подтверждении неопровержимых доказательств в отношении идентификации отправителей и получателей, задействованных в передаче данных*.	ИК17
X.814	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: основа обеспечения конфиденциальности	Определяется общая основа для предоставления услуг обеспечения конфиденциальности. Конфиденциальность является свойством, обеспечивающим, чтобы *информация не поступала в распоряжение* посторонних лиц, объектов или процессов и *не разглашалась им*.	ИК17
X.815	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: основа обеспечения целостности	Определяется общая основа для предоставления услуг обеспечения целостности. Целостностью называется свойство, благодаря которому *данные не изменяются и не разрушаются* несанкционированным образом.	ИК17
X.816	Информационные технологии – Взаимодействие открытых систем – инфраструктура обеспечения безопасности открытых систем: основа проверки безопасности и сигналов нарушения безопасности	Описывается базовая модель для обработки сигналов нарушения безопасности и проведения проверки безопасности в отношении открытых систем. Проверка безопасности является *независимым рассмотрением и анализом записей и действий системы*. Услуга проверки безопасности предоставляет проверяющему органу возможность определять, выбирать и управлять событиями, которые должны быть записаны в данных проверки безопасности.	ИК17

X.830	Информационные технологии – Взаимодействие открытых систем – Типичные высшие уровни обеспечения безопасности: обзор, модели и нотация	Относится к серии Рекомендаций, в которых предоставляется набор средств для оказания помощи в создании протоколов высшего уровня ВОС, которые поддерживают предоставление услуг обеспечения безопасности. В Рекомендации определяется следующее: a) общие *модели функций протокола обмена данными о безопасности и преобразований данных о безопасности*; b) набор *инструментов нотации* для поддержки спецификации требований выборочной защиты полей в спецификации абстрактного синтаксиса и для поддержки спецификации обменов данными о безопасности и преобразований данных о безопасности; c) набор *информативных руководящих принципов* в отношении применения типичных средств обеспечения безопасности высшего уровня, охватываемых данной серией рекомендаций.	ИК17
X.831	Информационные технологии – Взаимодействие открытых систем – Типичные высшие уровни обеспечения безопасности: определение услуги, обеспечиваемой элементом услуги обмена данными о безопасности (SESE)	Относится к серии Рекомендаций, в которых предоставляется набор средств для оказания помощи в создании протоколов высшего уровня ВОС, которые поддерживают предоставление услуг обеспечения безопасности. В настоящей Рекомендации определяется услуга, предоставляемая элементом услуги обмена данными о безопасности (SESE). Элемент SESE является элементом прикладной услуги (ASE), который содействует передаче *информации о безопасности* для поддержки предоставления *услуг обеспечения безопасности* на прикладном уровне ВОС.	ИК17
X.832	Информационные технологии – Взаимодействие открытых систем – Типичные высшие уровни обеспечения безопасности: определение протокола элемента услуги обмена данными о безопасности (SESE)	Относится к серии Рекомендаций, в которых предоставляется набор средств для оказания помощи в создании протоколов высшего уровня ВОС, которые поддерживают предоставление услуг обеспечения безопасности. В настоящей Рекомендации *определяется протокол*, предоставляемый элементом услуги обмена данными о безопасности (SESE). Элемент SESE является элементом прикладной услуги (ASE), который содействует передаче *информации о безопасности* для поддержки предоставления *услуг обеспечения безопасности* на прикладном уровне ВОС.	ИК17
X.833	Информационные технологии – Взаимодействие открытых систем – Типичные высшие уровни обеспечения безопасности: спецификация синтаксиса защиты перехода	Относится к серии Рекомендаций, в которых предоставляется набор средств для оказания помощи в создании протоколов высшего уровня ВОС, которые поддерживают предоставление услуг обеспечения безопасности. В настоящей Рекомендации определяется синтаксис для защиты перехода, связанный с поддержкой уровня представления для *услуг обеспечения безопасности* на прикладном уровне ВОС.	ИК17

X.834	Информационные технологии – Взаимодействие открытых систем – Типичные высшие уровни обеспечения безопасности: проформа свидетельства о соответствии протокольной реализации (PICS) элемента услуги обмена данными о безопасности (SESE)	Относится к серии Рекомендаций по обеспечению безопасности типичных высших уровне (GULS). В Рекомендации содержится проформа свидетельства о соответствии протокольной реализации (PICS) для протокола элемента услуги обмена данными о безопасности, определенного в Рекомендации МСЭ-Т X.832, и обмена данными о безопасности, определенного в Рекомендации МСЭ-Т X.830. В Приложении C дается описание стандартных возможностей и вариантов в форме, которая обеспечивает оценку соответствия конкретной реализации.	ИК17
X.835	Информационные технологии – Взаимодействие открытых систем – Типичные высшие уровни обеспечения безопасности: проформа PICS защиты синтаксиса перехода	Относится к серии Рекомендаций по обеспечению безопасности типичных высших уровне (GULS). В Рекомендации содержится проформа свидетельства о соответствии протокольной реализации (PICS) для протокола защиты синтаксиса перехода, определенного в Рек. МСЭ-Т X.833. В настоящей Рекомендации дается описание стандартных возможностей и вариантов в форме, которая обеспечивает оценку соответствия конкретной реализации.	ИК17
X.841	Информационные технологии – Методы обеспечения безопасности – Информационные объекты, относящиеся к обеспечению безопасности, для управления доступом	Содержатся определения объектов, которые обычно необходимы в *стандартах обеспечения безопасности* с целью недопущения многих и разных определений одной и той же функциональной возможности. Точность этих определений достигается путем использования абстрактной синтаксической нотации версии 1 (ASN.1). Настоящая Рекомендация охватывает только статические аспекты информационных объектов, имеющих отношение к безопасности (SIO).	ИК17
X.842	Информационные технологии – Методы обеспечения безопасности – Руководящие принципы для использования услуг пользующейся доверием третьей стороны и управления ими	Содержатся руководящие принципы для использования услуг пользующейся доверием третьей стороны (TTP) и управления ими, четкое определение выполняемых базовых функций и предоставляемых услуг, их описание и назначение, а также роли и обязательства пользующихся доверием третьих сторон (TTP) и объектов, использующих их услуги. В настоящей Рекомендации определяются различные главные категории услуг TTP, включая *отметку времени, фиксацию авторства, управление ключами защиты, управление сертификатами и электронного нотариуса*.	ИК17
X.843	Информационные технологии – Методы обеспечения безопасности – Спецификации услуг TTP для поддержки применения цифровых подписей	Определяются услуги, необходимые с целью поддержки применения цифровых подписей для обеспечения *неотрекаемости* в отношении создания документа. Поскольку это подразумевает *целостность* документа и *аутентификацию* создателя, описанные услуги могут быть также объединены для реализации услуг *обеспечения целостности и аутентификации*.	ИК17

X.901	Информационные технологии – Открытая распределенная обработка – Эталонная модель: обзор	Быстрое развитие способов распределенной обработки привело к необходимости в основе для координации работы по стандартизации открытой распределенной обработки (ODP). Такую основу предоставляет данная эталонная модель, которая позволяет создать архитектуру для поддержки распределения, взаимодействия и возможности встроенной переносимости. В настоящей Рекомендации содержится мотивационный обзор ODP, в котором предоставляется сфера применения, обоснованность и разъяснение ключевых концепций, а также конфигурация архитектуры ODP. В Рекомендации содержится пояснительный материал о том, каким образом пользователи, разработчики стандартов и архитекторы ODP должны понимать и использовать эталонную модель. В ней также содержится деление на категории требуемых областей стандартизации в виде эталонных точек соответствия, указанных в Рекомендации МСЭ-Т X.903. Системы ODP должны быть защищенными, т. е. они должны создаваться и обслуживаться так, чтобы в отношении средств систем и данных обеспечивалась *защита от несанкционированного доступа, незаконного использования и любых других угроз и попыток нарушения защиты*. Требования к обеспечению безопасности трудно удовлетворить при взаимодействиях на расстоянии и подвижном характере системы и ее пользователей. Правила обеспечения безопасности для систем ODP могут определять: *обнаружение угроз для безопасности; защиту от угроз для безопасности; ограничение любого ущерба, причиняемого любыми брешами в защите*.	ИК17
X.902	Информационные технологии – Открытая распределенная обработка – Эталонная модель: основы	В Рекомендации содержится определение концепций и аналитической основы для стандартизованного описания систем (произвольной) распределенной обработки. Вводятся принципы соответствия стандартам ODP способ их применения. Рекомендация относится только к уровню детализации, достаточной для *установления требований к новым методам спецификации*.	ИК17
X.903	Информационные технологии – Открытая распределенная обработка – Эталонная модель: архитектура	В Рекомендации содержится спецификация характеристик, требуемых для того, чтобы квалифицировать систему распределенной обработки как открытую. Речь идет об ограничениях, которым должны соответствовать стандарты ODP. Используются описательные методы из Рекомендации МСЭ-Т X.902.	ИК17
X.904	Информационные технологии – Открытая распределенная обработка – Эталонная модель: семантика архитектуры.	Предоставляется стандартизация концепций моделирования ODP, определенных в пунктах 8 и 9 Рекомендации МСЭ-Т X.902. Стандартизация достигается путем интерпретации каждой концепции в виде конструкций различных стандартизованных формальных методов описания.	ИК17
X.1051	Система управления информационной безопасностью – Требования к электросвязи (ISMS-T)	Для организаций электросвязи информация и вспомогательные процессы, устройства, сети и линии электросвязи являются важными активами коммерческой деятельности. Для должного управления этими активами и для правильного и успешного продолжения коммерческой деятельности организаций электросвязи крайне важно осуществлять управление информационной безопасностью. В настоящей Рекомендации представлены требования к организациям электросвязи в части управления информационной безопасностью. В настоящей Рекомендации определяются требования к созданию, внедрению, эксплуатации, контролю, анализу, техническому обслуживанию и усовершенствованию документированной системы управления информационной безопасностью (ISMS) в контексте всех рисков, связанных с коммерческой деятельностью в электросвязи. В ней определяются требования к реализации средств контроля безопасности применительно к потребностям отдельных предприятий электросвязи или их частей.	ИК17

X.1081	Телебиометрическая мультимодальная модель – Основа для спецификации аспектов безопасности и защищенности в телебиометрике	Определяется телебиометрическая мультимодальная модель, предоставляющая общую основу для спецификации четырех взаимосвязанных вопросов обеспечения безопасности - конфиденциальности, аутентификации, защищенности и безопасности. Эта телебиометрическая мультимодальная модель охватывает все возможности защищенных и безопасных мультимодальных взаимодействий "человек–машина" и частично получена на основе стандартов ISO 31 и IEC 60027-1. Относящиеся к человеку познавательные, перцепционные и поведенческие модальности также важны в области электросвязи и, вероятно, будут использоваться в будущем каким-либо биометрическим датчиком или исполнительным элементом в целях аутентификации. На них также распространяется эта телебиометрическая мультимодальная модель. Представлена систематика взаимодействий, которые могут иметь место на мультимодальном уровне, когда человеческое тело взаимодействует с электронными, фотонными, химическими или материальными устройствами, которые улавливают биометрические параметры либо воздействуют на это тело. Аутентификация человека при сохранении его конфиденциальности и защищенности может быть определена в виде взаимодействий между устройствами и сферой его персональной конфиденциальности, которая моделирует и охватывает взаимодействия человека с его внешней средой, делая обсуждение таких взаимодействий ясным и технически понятным. Настоящая Рекомендация включает спецификацию сферы персональной конфиденциальности, классификацию модальностей взаимодействия через такую сферу, базовые и производные единицы для измерения и определения (в количественном аспекте) таких взаимодействий, а также иерархию масштабов для относительной близости.	ИК17
X.1121	Структура технологий безопасности для сквозной подвижной передачи данных	Описываются угрозы безопасности подвижной сквозной передаче данных и требования к безопасности подвижных пользователей и поставщиков прикладных услуг (ASP) на высшем уровне эталонной модели ВОС для подвижной сквозной передачи данных между подвижным терминалом в сети подвижной связи и прикладным сервером в открытой сети. Кроме того, в Рекомендации показано, где в моделях подвижной сквозной передачи данных появляются технологии обеспечения безопасности, которые реализуют некоторую функцию обеспечения безопасности. Предоставляется структура технологий обеспечения безопасности для подвижной сквозной передачи данных.	ИК17
X.1122	Руководящие указания по созданию защищенных систем подвижной связи на основе инфраструктуры открытого ключа (PKI)	Технология PKI – это технология обеспечения безопасности, которая применяется к отношению между подвижным терминалом и сервером приложений в общей модели подвижной сквозной передачи данных между подвижным пользователем и ASP (поставщик прикладных услуг), или к отношению между подвижным терминалом и шлюзом обеспечения безопасности подвижной связи или между шлюзом обеспечения безопасности подвижной связи и сервером в модели шлюза подвижной сквозной передачи данных между подвижным пользователем и ASP. Хотя технология использования инфраструктуры открытого ключа (PKI) является весьма полезной технологией для обеспечения защиты подвижной сквозной передачи данных, существуют характеристики, свойственные подвижной сквозной передаче, которые требуют адаптации технологии PKI при создании защищенных систем подвижной связи (шифрование, цифровая подпись, обеспечение целостности данных и так далее). В настоящей Рекомендации содержатся руководящие указания по созданию защищенных систем подвижной связи на основе технологии PKI.	ИК17

Приложение B

Терминология в области безопасности

Следующие сокращения и определения МСЭ-Т, относящиеся к вопросам обеспечения безопасности, были взяты из соответствующих Рекомендаций 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*), обеспечивает доступ к принятым в публикациях МСЭ-Т "терминам и определениям", а также "аббревиатурам и акронимам" на английском, испанском и французском языках. Свободный доступ к этому онлайновому ресурсу 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.

ИК17 МСЭ-Т разработала каталог определений в области безопасности, используемых в Рекомендациях МСЭ-Т, который размещен по адресу http://www.itu.int/ITU-T/studygroups/com17/tel-security.html.

B.1 Термины и определения, относящиеся к вопросам обеспечения безопасности

Приведенный ниже список содержит большее количество обычно используемых терминов по вопросам обеспечения безопасности, по сравнению с определенными в существующих Рекомендациях МСЭ-Т. Более полный список определений по вопросам обеспечения безопасности содержится в каталоге, который ведется 17-й Исследовательской комиссией (см. ссылку выше).

Термин	Термин	Определение	Ссылка
Управление доступом	**access control**	1. Предотвращение несанкционированного использования ресурса, в том числе предотвращение использования ресурса неразрешенным образом. 2. Ограничение потока информации от ресурсов системы только информацией от уполномоченных лиц, программ, процессов и других системных ресурсов сети.	X.800 J.170
Список управления доступом	**access control list**	Список объектов, имеющих полномочия на получение доступа к ресурсу, и их прав доступа.	X.800
Стратегия управления доступом	**access control policy**	Набор правил, которые определяют условия, при которых доступ может иметь место.	X.812
Услуга управления доступом	**access control service**	Услуга управления доступом предоставляет способы, обеспечивающие доступ субъектов к ресурсам только разрешенным образом. Рассматриваемыми ресурсами могут быть физическая система, программное обеспечение системы, приложения и данные. Услуга управления доступом может быть определена и реализована на различных уровнях модульности СУЭ: уровне агента, уровне объекта или уровне атрибута. Данные об ограничении доступа содержатся в информации об управлении доступом - способах определения объектов, которым разрешен доступ; виде разрешенного доступа (чтение, запись, изменение, создание, удаление).	M.3016.2
Случайные угрозы	**accidental threats**	Угрозы, не связанные с умышленным намерением. Примеры известных случайных угроз включают нарушения работы системы, грубые эксплуатационные ошибки и ошибки в программном обеспечении.	X.800
Отчетность	**accountability**	Свойство, гарантирующее, что действия объекта могут отслеживаться с однозначной привязкой к конкретному объекту.	X.800
Активная угроза	**active threat**	Угроза преднамеренного несанкционированного изменения состояния системы. *Примечание.* – Примерами активных угроз безопасности могут служить: изменение сообщений, повторное использование перехваченных сообщений, включение случайных сообщений, подмена под видом разрешенного объекта и отказ в обслуживании, злонамеренное изменение таблиц маршрутизации посторонним пользователем.	X.800
Арбитр	**adjudicator**	Объект, рассматривающий споры, которые могут возникать в результате событий или действий, связанных с непризнанием авторства, т. е. объект, который оценивает фактические данные и определяет, возникло или нет оспариваемое событие или действие. Эффективность *рассмотрения спора* может обеспечиваться, если только стороны, участвующие в споре, признают *полномочия* арбитра.	X.813
Алгоритм	**algorithm**	Математический процесс, который может использоваться для скремблирования и дескремблирования потока данных.	J.93
Асимметричный метод аутентификации	**asymmetric authentication method**	Метод аутентификации, при котором не вся информация об аутентификации совместно используется обеими сторонами.	X.811
Асимметричный криптографический алгоритм	**asymmetric cryptographic algorithm**	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.	X.810

Термин	Термин	Определение	Ссылка
Злонамеренное воздействие	**attack**	Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности системы или в целях использования их недостатков. При непосредственном злонамеренном воздействии на систему используются недостатки базовых алгоритмов, принципов или свойств механизма обеспечения безопасности. Косвенные злонамеренные воздействия предпринимаются путем обхода механизма безопасности или принуждения системы к неправильному использованию этого механизма.	H.235
Атрибут	**attribute**	В контексте обработки сообщений – единица информации, компонент списка атрибутов, который описывает пользователя или список рассылки и который может также обнаружить его в зависимости от физической или организационной структуры системы обработки сообщений (или лежащей в ее основе сети).	X.400
Орган по присвоению атрибутов	**Attribute Authority**	1. Орган, который назначает полномочия путем выдачи сертификатов атрибутов. 2. Объект, которому один или несколько объектов доверяют создание и подпись сертификатов атрибутов. *Примечание.* – Орган сертификации (ОС) может быть также органом по присвоению атрибутов.	X.509 X.842
Сертификат атрибута	**attribute certificate**	Структура данных, имеющая цифровую подпись органа по присвоению атрибутов, которая связывает некоторые значения атрибутов с идентификационной информацией о держателе этого атрибута.	X.509
Тип атрибута	**attribute type**	Идентификатор, который обозначает класс информации (например, персональные имена). Является частью атрибута.	X.400
Значение атрибута	**attribute value**	Тип атрибута, который обозначает конкретный экземпляр класса информации (например, персональные имена). Является частью атрибута.	X.400
Проверка	**audit**	См. Проверка обеспечения безопасности.	X.800
Данные проверки	**audit trail**	См. Проверка данных обеспечения безопасности.	X.800
Аутентифицированная идентификация	**authenticated identity**	Отличительный идентификатор администратора доступа, удостоверяемый путем аутентификации.	X.811
Аутентификация	**authentication**	1. Процесс подтверждения идентификации. *Примечание.* – См. *Администратор доступа* и *Верификатор* и две отличительные формы аутентификации (аутентификация источника данных. + аутентификация объекта). Аутентификация может быть односторонней или взаимной. *Односторонняя* аутентификация обеспечивает уверенность в идентификации только одного администратора доступа. *Взаимная* аутентификация обеспечивает уверенность в идентификации обоих администраторов доступа. 2. Обеспечение уверенности в заявленной идентификации объекта. 3. См. *Аутентификация происхождения данных* и *Аутентификация одноранговых объектов*. Термин "аутентификация" не используется применительно к целостности данных; вместо него используется термин "целостность данных". 4. Подтверждение идентификации объектов, относящихся к установлению ассоциаций. Например, они могут быть прикладными объектами, прикладными процессами и людьми-пользователями приложений. *Примечание.* – Данный термин был определен для разъяснения того, что рассматривается более широкая сфера аутентификации, по сравнению с аутентификацией одноранговых объектов из Рекомендации МККТТ X.800. 5. Процесс проверки идентификационной информации, предъявленной одним объектом другому объекту. 6. Процесс, предназначенный для предоставления возможности системе проводить достоверную проверку идентификации стороны.	X.811 X.811 X.800 X.217 J.170 J.93

Термин	Термин	Определение	Ссылка
Сертификат аутентификации	**authentication certificate**	Сертификат безопасности, который гарантирован органом сертификации и который может быть использован для обеспечения идентификации объекта	X.811
Обмен данными аутентификации	**authentication exchange**	1. Механизм, предназначенный для идентификации объекта посредством обмена информацией. 2. Последовательность одной или нескольких передач информации обмена данными аутентификации в целях осуществления аутентификации.	X.800 X.811
Услуга аутентификации	**authentication service**	Услуга аутентификации предоставляет доказательство того, что идентификация объекта или субъекта на самом деле является идентификацией, которая заявлена им. В зависимости от действующего субъекта и целей идентификации могут потребоваться следующие виды аутентификации: аутентификация пользователя, аутентификация одноранговых объектов, аутентификация происхождения данных. Примерами механизмов, используемых для реализации услуги аутентификации являются пароли и персональные идентификационные номера (PIN) (простая аутентификация), а также методы, основанные на шифровании (строгая аутентификация).	M.3016.2
Аутентификационный маркер (маркер)	**authentication token (token)**	Информация, передаваемая в процессе обмена данными строгой аутентификации, которая может использоваться для аутентификации отправителя этой информации.	X.509
Аутентичность	**authenticity**	1. Способность обеспечивать, чтобы данная информация не была изменена или фальсифицирована, а была действительно представлена объектом, который заявлен держателем этой информации. 2. Свойство, обеспечивающее возможность проверки заявленного источника данных для удовлетворения получателя.	J.170 T.411
Орган	**authority**	Объект, ответственный за выдачу сертификатов. Определены два типа органов: орган сертификации, который выдает сертификаты открытых ключей, и орган по присвоению атрибутов, который выдает сертификаты атрибутов.	X.509
Сертификат органа	**authority certificate**	Сертификат, выданный органу (например, органу сертификации или органу по присвоению атрибутов).	X.509
Авторизация	**authorization**	1. Предоставление прав, которое включает предоставление доступа на основании прав доступа. *Примечание.* – Данное определение подразумевает права на осуществление некоторой деятельности (такой как доступ к данным) и что они были предоставлены некоторому процессу, объекту или агенту-человеку. 2. Предоставление разрешения на основании идентификации, прошедшей аутентификацию. 3. Действие по предоставлению доступа к услуге или устройству при наличии разрешения на такой доступ.	X.800 H.235 J.170
Готовность	**availability**	Свойство быть доступным и годным к эксплуатации по запросу имеющего полномочия объекта.	X.800
Кабельный портал обеспечения безопасности	**cable security portal (CSP)**	Функциональный элемент, управляющий обеспечением безопасности и функциями преобразования между HFC (коаксиальный гибридный волоконный кабель) и домом.	J.191
Сервер управления вызовами	**call management server (CMS)**	Система IPCablecom. Управляет звуковыми соединениями. Также называется агентом вызова в терминологии протокола MGCP/SGCP.	J.191
Возможность	**capability**	Маркер, который используется в качестве идентификатора для ресурса, обозначающего, что владение им дает права доступа к данному ресурсу.	X.800

Термин	Термин	Определение	Ссылка
Сертификат	**certificate**	Набор относящихся к обеспечению безопасности данных, который выдан органом обеспечения безопасности или пользующейся доверием третьей стороной, в совокупности с информацией о безопасности, которая используется для предоставления услуг обеспечения целостности и аутентификации источника данных в отношении данных. (сертификат безопасности – X.810). Термин имеет отношение к сертификатам "открытого ключа", которые являются значениями, представляющими открытый ключ владельца (или иную факультативную информацию) как проверенный и подписанный пользующимся доверием органом в формате, не допускающем фальсификацию.	H.235
Стратегия применения сертификата	**certificate policy**	Поименованный набор правил, которые определяют применимость сертификата к конкретному семейству и/или классу приложений с общими требованиями к обеспечению безопасности. Например, стратегия применения данного сертификата может указывать применимость типа сертификата к аутентификации транзакций электронного обмена данными для торговли товарами в пределах данного ценового диапазона.	X.509
Список аннулирования сертификатов	**Certificate Revocation List (CRL)**	1. Подписанный список, определяющий набор сертификатов, которые распределитель сертификатов более не считает действительными. В дополнение к общему термину CRL определены несколько конкретных типов CRL для списков CRL, охватывающих конкретные сферы применения. 2. Список CRL включает порядковые номера аннулированных сертификатов (например, вииду того, что ключ был раскрыт, или поскольку субъект больше не работает в компании), срок действия которых еще не истек.	X.509 Q.817
Орган сертификации	**Certification Authority (CA)**	1. Орган, которому одним или более пользователями доверено создавать и распределять сертификаты открытых ключей. Орган сертификации может выполнять факультативную функцию по созданию ключей пользователей. 2. Объект, которому доверено (в контексте стратегии обеспечения безопасности) создавать сертификаты безопасности, содержащие один или более классов данных, относящихся к обеспечению безопасности.	X.509 X.810
Путь сертификата	**certification path**	Упорядоченная последовательность сертификатов объектов в информационном дереве каталога, которая вместе с открытым ключом первоначального объекта данного пути может быть обработана для получения открытого ключа конечного объекта данного пути.	X.509
Сервер управления вызовами	**challenge**	Изменяемый во времени параметр, создаваемый верификатором.	X.811
Шифр	**cipher**	1. Криптографический алгоритм, математическое преобразование 2. Алгоритм, осуществляющий преобразование данных между нешифрованным текстом и шифротекстом.	H.235 J.170
Шифротекст	**ciphertext**	Данные, созданные с применением шифрования. Семантическое содержание результирующих данных не доступно. *Примечание.* – Шифротекст может тоже пройти процедуру шифрования, в результате чего будут созданы супершифрованные данные.	X.800
Заявитель	**claimant**	Объект, который является *администратором доступа* в целях аутентификации или представляет его. Заявитель выполняет функции, необходимые для осуществления обменов данными аутентификации от имени администратора доступа	X.811
Незашифрованный текст	**cleartext**	Открытые данные, семантическое содержание которых доступно.	X.800
Скомпрометированные фактические данные	**compromised evidence**	Фактические данные, которые одно время были удовлетворительными, но которым больше не доверяет пользующаяся доверием третья сторона или арбитр.	X.813
Конфиденциальность	**confidentiality**	Свойство, которое служит для предотвращения раскрытия информации объектами или процессами, не имеющими разрешения на это.	X.800

Термин	Термин	Определение	Ссылка
Услуга обеспечения конфиденциальности	**confidentiality service**	Услуга обеспечения конфиденциальности предоставляет защиту от неразрешенного раскрытия данных обмена. Различают следующие виды услуг обеспечения конфиденциальности: конфиденциальность отдельных полей; конфиденциальность соединений; конфиденциальность потока данных.	M.3016.2
Целостность содержания	**content integrity**	1. Дает возможность получателю сообщения удостовериться в том, что исходное содержание сообщения не было изменено. 2. Данный элемент обслуживания позволяет отправителю сообщения предоставить получателю сообщения способ, с помощью которого получатель может убедиться в том, что содержание сообщения не было изменено. Целостность содержания обеспечивается на основе каждого получателя с возможным использованием асимметричного или симметричного методов шифрования.	X.400 X.400
Подпись, скрепляющая документ	**counter-signature**	Цифровая подпись добавляется к блоку данных, который уже был подписан другим объектом (например, TTP).	X.813
Полномочия	**credentials**	Данные, которые передаются для установления заявленной идентификации объекта.	X.800
Криптоанализ	**cryptanalysis**	1. Анализ криптографической системы и/или входных и выходных данных для извлечения секретных переменных и/или уязвимых данных, включая открытый текст. 2. Процесс восстановления незашифрованного текста сообщения или ключа шифрования без доступа к ключу. 3. Наука восстановления незашифрованного текста сообщения или ключа шифрования без доступа к ключу (к электронному ключу в электронных криптографических системах).	X.800 J.170 J.93
Криптографический алгоритм	**cryptographic algorithm**	Математическая функция, которая вычисляет результат по одному или нескольким входным значениям.	H.235
Криптографическое сцепление	**cryptographic chaining**	Режим использования криптографического алгоритма, при котором преобразование осуществляется алгоритмом, который зависит от значений предыдущих входных или выходных данных.	X.810
Криптографическое контрольное значение	**cryptographic checkvalue**	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.	X.800
Криптографическая система, криптосистема	**cryptographic system, cryptosystem**	1. Набор преобразований из незашифрованного текста в шифротекст и наоборот. Конкретное(ые) преобразование(я), которое(ые) должно(ы) использоваться, выбирается(ются) ключами. Преобразования обычно описывается математическим алгоритмом. 2. Криптосистема – это просто алгоритм, который может преобразовывать входные данные в нечто нераспознаваемое (шифрование) и обратно преобразовывать нераспознаваемые данные в их исходную форму (дешифрование). Методы шифрования RSA описаны в Рек. МСЭ-Т X.509.	X.509 Q.815
Криптография	**cryptography**	Дисциплина, включающая принципы, средства и методы для преобразования данных, для того чтобы скрыть содержащуюся в них информацию, предотвратить их скрытое изменение и/или предотвратить несанкционированное использование. *Примечание.* – Криптография определяет методы, используемые при шифровании и дешифровании. Воздействие на криптографический принцип, средство или метод называется криптоанализом.	X.800
Конфиденциальность данных	**data confidentiality**	Данная услуга может использоваться для обеспечения защиты данных от несанкционированного раскрытия их содержания. Услугу обеспечения конфиденциальности данных поддерживает структура аутентификации. Может применяться для защиты данных от несанкционированного перехвата.	X.509

Термин	Термин	Определение	Ссылка
Целостность данных	**data integrity**	Показатель того, что данные не были изменены или разрушены несанкционированным образом.	X.800
Аутентификация источника данных	**data origin authentication**	1. Подтверждение того, что источник полученных данных соответствует заявленному. 2. Подтверждение идентификации администратора доступа, ответственного за конкретный блок данных.	X.800 X.811
Дешифрование	**decipherment**	Инверсия соответствующего обратимого шифрования.	X.800
Дешифрация	**decryption**	См. *Дешифрование*.	X.800
Делегирование	**delegation**	Передача полномочия от одного объекта, который владеет данным полномочием, другому объекту.	X.509
Отказ в обслуживании	**denial of service**	Недопущение санкционированного доступа к ресурсам или задержка выполнения операций, критических по времени.	X.800
Дескремблирование	**descrambling**	1. Восстановление характеристик сигнала видеоизображения/звука/данных для предоставления возможности приема в четкой форме. Данное восстановление является определенным процессом, управляемым системой условного доступа (приемный конец). 2. Процесс, обратный функции скремблирования (см. "скремблирование"), с целью получения пригодных для использования услуг передачи изображений, звука и данных.	J.96 J.93
Цифровой "отпечаток"	**digital fingerprint**	Характеристика элемента данных, например, криптографическое контрольное значение или результат выполнения односторонней функции хеширования в отношении данных, которая достаточно индивидуальна для этого элемента данных, и вследствие этого невозможно путем вычислений найти другой элемент данных, обладающий теми же характеристиками.	X.810
Цифровая подпись	**digital signature**	1. Данные, добавленные к блоку данных, или криптографическое преобразование (см. *Криптография*) блока данных, которое позволяет получателю данных удостовериться в происхождении и целостности блока данных и обеспечить защиту от мошенничества, например, получателем. 2. Криптографическое преобразование блока данных, которое позволяет получателю блока данных удостовериться в происхождении и целостности блока данных и обеспечить защиту отправителя и получателя блока данных от мошенничества со стороны третьих сторон, а также отправителя от мошенничества со стороны получателя.	X.800 X.843
Прямая попытка нарушения защиты	**direct attack**	Попытка нарушения защиты системы, основанная на недостатках базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.	X.814
Услуга каталога	**directory service**	Услуга поиска и извлечения из каталога информации о хорошо определенных объектах, которая может содержать данные о сертификатах, номерах телефонов, условиях доступа, адресах и т. д. Примером является услуга справочника, соответствующая Рекомендации МСЭ-Т X.500.	X.843
Метод двойной оболочки	**double enveloping technique**	Дополнительная защита полного сообщения, включая параметры оболочки, может быть обеспечена благодаря возможности определять, что само сообщение является полным сообщением, т. е. метод двойной оболочки доступен благодаря использованию аргумента типа информационного наполнения, который позволяет определять, что информационное наполнение сообщения является внутренней оболочкой.	X.402
Перехват информации	**eavesdropping**	Нарушение конфиденциальности путем слежения за связью.	M.3016.0
Электронный ключ	**electronic key**	Термин, относящийся к сигналам данных, которые используются для управления процессом дескремблирования в абонентских декодерах. *Примечание.* – Существует, по меньшей мере, три типа электронных ключей: ключи, используемые для потоков телевизионных сигналов; ключи, используемые для защиты работы систем управления и ключи, используемые для рассылки электронных ключей по кабельной системе.	J.93

Термин	Термин	Определение	Ссылка
Шифрование	**encipherment**	1. Криптографическое преобразование данных (см. *Криптография*) для создания шифротекста. *Примечание.* – Шифрование может быть необратимым, и в этом случае выполнение соответствующего процесса дешифрования невозможно. 2. Шифрование (зашифровывание) – это процесс превращения данных в нечитаемые для несанкционированных объектов данные путем применения криптографического алгоритма (алгоритма шифрования). Дешифрование (дешифрация) является обратной операцией, в результате которой криптотекст преобразуется в открытый текст.	X.800 H.235
Зашифровывание	**encryption**	1. Метод, используемый для преобразования информации в форме открытого текста в шифротекст. 2. Процесс скремблирования сигналов для недопущения несанкционированного доступа (см. также *Шифрование*)	J.170 J.93
Конечный объект	**end entity**	Субъект, который имеет сертификат и использует свой личный ключ не для целей подписи сертификатов, или объект, который является доверенной стороной.	X.509
Сквозное шифрование	**end-to-end encipherment**	Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения. (См. также *Межканальное шифрование*)	X.800
Объект	**entity**	1. Человек, организация, компонент аппаратного обеспечения или элемент программного обеспечения. 2. Любой конкретный или абстрактный предмет интереса. В то время как обычно слово "объект" может использоваться для именования чего-либо, в контексте моделирования оно относится к объектам моделирования в предметной области	X.842 X.902
Аутентификация объекта	**entity authentication**	Подтверждение идентификации администратора доступа в контексте взаимоотношений в области связи. *Примечание.* – Аутентифицированная идентификация администратора доступа удостоверяется только когда данная услуга аннулирована. Обеспечение непрерывности аутентификации может быть достигнуто с помощью методов, описанных в п. 5.2.7 Рек. МСЭ-Т X.811.	X.811
Определитель события	**event discriminator**	Функция, которая обеспечивает первоначальный анализ события, имеющего отношение к обеспечению безопасности, и вызывает, по мере необходимости, проверку безопасности и/или сигнал тревоги.	X.816
Доказательство	**evidence**	Информация, которая сама по себе или при использовании вместе с другой информацией, может применяться для разрешения спора. *Примечание.* – Конкретными формами доказательств являются цифровые подписи, защитные оболочки и маркеры безопасности. Цифровые подписи используются вместе с методами открытых ключей, тогда как защитные оболочки и маркеры безопасности применяются вместе с методами секретных ключей.	X.813
Генератор доказательств	**evidence generator**	Объект, который создает доказательство фиксации авторства. *Примечание.* – Данный объект может быть инициатором запроса услуги обеспечения фиксации авторства, отправителем, получателем или совместно работающими многими сторонами (например, лицо, подписавшее сообщение, и поручитель).	X.813
Мошенничество	**forgery**	Объект фабрикует информацию и заявляет, что такая информация была получена от другого объекта или направлена другому объекту.	M.3016.0
Хеш-функция	**hash function**	Функция (математическая), которая отображает значения из крупного (возможно очень крупного) набора значений в меньший диапазон значений.	X.810
Скрывать	**hide**	Операция, применяющая защиту конфиденциальности для незащищенных данных или дополнительную конфиденциальность для уже защищенных данных.	X.814

Термин	Термин	Определение	Ссылка
Стратегия обеспечения безопасности на основе идентификации	**identity-based security policy**	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.	X.800
Непрямая попытка нарушения защиты системы	**indirect attack**	Попытка нарушения защиты системы, не основанная на недостатках конкретного механизма обеспечения безопасности (например, попытки нарушения защиты в обход механизма или попытки нарушения защиты, рассчитанные на систему, неправильно использующую механизм).	X.814
Целостность	**integrity**	Показатель того, что данные не были изменены несанкционированным образом. (См. также *Целостность данных*)	H.235
Услуга обеспечения целостности	**integrity service**	Услуга обеспечения целостности предоставляет способы гарантирования правильности данных обмена, защиту от изменения, удаления, создания (вставки) и повторного использования данных обмена. Различают следующие виды услуг обеспечения безопасности: целостность отдельных полей; целостность соединения без восстановления; целостность соединения с восстановлением.	M.3016.2
Канал с защитой целостности	**integrity-protected channel**	Канал связи, к которому была применена услуга обеспечения безопасности. (См. *Целостность при соединении* и *Целостность при отсутствии соединения*)	X.815
Данные с защитой целостности	**integrity-protected data**	Данные и все соответствующие атрибуты в среде с защитой целостности.	X.815
Среда с защитой целостности	**integrity-protected environment**	Среда, в которой предотвращаются или обнаруживаются несанкционированные изменения данных (включая создание и удаление).	X.815
Намеренные угрозы	**intentional threats**	К таким угрозам относятся угрозы от случайного просмотра с использованием легко доступных инструментов слежения до изощренных попыток нарушения защиты с использованием специальных знаний о системе. Намеренная угроза, если она реализована, может считаться "попыткой нарушения защиты".	X.800
Сопротивление вмешательству	**intrusion resistance**	Способность объекта аппаратного обеспечения отказывать неуполномоченным сторонам в физическом, электрическом или основанном на излучении доступе к внутренним функциональным возможностям.	J.93
Система IPCablecom	**IPCablecom**	Проект МСЭ-Т, включающий архитектуру и серию рекомендаций, который обеспечивает возможность доставки реально временных услуг по сетям кабельного телевидения с использованием кабельных модемов.	J.160
Протокол Kerberos	**Kerberos**	Протокол сетевой аутентификации с секретным ключом, который использует на выбор криптографические алгоритмы шифрования и централизованную базу данных ключей для аутентификации.	J.170
Ключ	**Key**	1. Последовательность символов, которые управляют операциями шифрования и дешифрования. 2. Математическая величина, введенная в выбранный криптографический алгоритм.	X.800 J.170
Система рассылки ключей	**key distribution service**	Услуга безопасной рассылки ключей уполномоченным объектам выполнятся центром рассылки ключей и описана в стандарте ИСО/МЭК 11770-1.	X.843
Обмен ключами	**key exchange**	Обмен между объектами открытыми ключами, которые должны использоваться для кодирования связи между этими объектами.	J.170
Управление ключами	**key management**	Создание, хранение, рассылка, удаление, архивирование и применение ключей в соответствии со стратегией обеспечения безопасности.	X.800
Утечка информации	**leakage of information**	Если информация была получена неуполномоченной стороной путем слежения за передачами, с помощью неразрешенного доступа к информации, хранящейся в любой системе MHS, или путем подмены, это может быть следствием маскировки под законного пользователя или неправильного использования системы MTS или принуждения агента MTA к неправильной работе. Угрозы утечки информации включают следующее: потерю конфиденциальности; потерю анонимности; незаконное присвоение сообщений; анализ трафика.	X.402

Термин	Термин	Определение	Ссылка
Межканальное шифрование	**link-by-link encipherment**	Индивидуальное применение шифрования к данным на каждом участке системы связи. (См. также *Сквозное шифрование*.) *Примечание.* – В результате межканального шифрования данные на объектах ретрансляции будут находиться в форме открытого текста.	X.800
Потеря или искажение информации	**loss or corruption of information**	Нарушение целостности переданных данных путем несанкционированного удаления, вставки, изменения, изменения порядка следования, повторного использования или задержки	M.3016.0
Контроль работы с данными	**manipulation detection**	Механизм, используемый для определения случаев изменения блока данных (непредумышленно или намеренно).	X.800
Подмена	**masquerade**	Предпринимаемая объектом попытка представить себя другим объектом.	X.800
Код аутентификации сообщения (MAC)	**message authentication code (MAC)**	Криптографическое проверочное значение, используемое для обеспечения аутентификации происхождения данных и целостности данных.	X.813
Аутентификация исходного сообщения	**message origin authentication**	Предоставляет возможность получателю или любому агенту MTA, через которого проходит сообщение, аутентифицировать идентификацию отправителя сообщения.	X.400
Целостность последовательности сообщений	**message sequence integrity**	1. Позволяет отправителю предоставлять получателю доказательство того, что последовательность сообщений была передана. 2. Данный элемент услуги позволяет отправителю сообщения предоставлять получателю сообщения средство, с помощью которого получатель может убедиться в том, что последовательность сообщений от отправителя к получателю была сохранена (без потери сообщений, изменения порядка их следования или повторного использования). Целостность последовательности сообщений обеспечивается на основе каждого получателя и может использовать асимметричный или симметричный методы шифрования.	X.400
Установление последовательности сообщения	**message sequencing**	Имеет место, когда все сообщение или его часть повторяется, сдвигается во времени или имеет другой порядок следования, например для использования аутентификационной информации в действительном сообщении и изменения порядка следования или сдвига во времени действительного сообщения. Несмотря на то, что предотвратить повторное использование с помощью услуг обеспечения безопасности системы MHS невозможно, это можно обнаружить и устранить влияние угрозы. Установление последовательности сообщения включает: повторное использование сообщений; изменение порядка следования сообщений; передачу сообщений ранее назначенного времени; задержку сообщений.	X.402
Контролирующая роль	**monitoring role**	Роль, в которой пользующаяся доверием третья сторона контролирует действие или событие. Этой стороне доверено предоставлять доказательство в отношении того, что было проконтролировано.	X.813
Взаимная аутентификация	**mutual authentication**	Обеспечение идентификации обоих администраторов доступа.	X.811
Фиксация авторства	**non-repudiation**	1. Способность предотвратить последующее непризнание отправителем факта отправки сообщения или выполнения действия. 2. Защита от отказа признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи. 3. Процесс, обеспечивающий невозможность непризнания отправителем сообщения (например, запроса на услугу "разовая плата за просмотр программы") факта его направления.	J.170 H.235 J.93
Заверение	**notarization**	Регистрация данных с участием пользующейся доверием третьей стороны, которая позволяет впоследствии удостоверить соответствие характеристик таких данных, как информационное наполнение, источник, время и доставка.	X.800

Термин	Термин	Определение	Ссылка
Нотариус	**notary**	Пользующаяся доверием третья сторона, которая зарегистрировала данные; таким образом, в дальнейшем может быть обеспечена точность характеристик данных.	X.813
Пассивная угроза	**passive threat**	Угроза несанкционированного раскрытия содержания информации без изменения состояния системы.	X.800
Пароль	**password**	1. Конфиденциальная аутентификационная информация, состоящая, как правило, из строки символов. 2. Относится к строке пароля, вводимого пользователем: понимается, что он является присвоенным ключом безопасности, который совместно используется подвижным пользователем и его домашним доменом. Данный пароль пользователя и полученный совместно используемое секретное значение пользователя применяются в целях аутентификации пользователя.	X.800 H.530
Аутентификация однорангового объекта	**peer-entity authentication**	1. Подтверждение того, что равноправный объект в ассоциации является заявленным объектом. 2. Представление доказательства идентификации однорангового объекта в ходе взаимодействия с целью осуществления связи.	X.800 M.3016.0
Среда личной безопасности (PSE)	**personal security environment (PSE)**	Безопасное местное хранилище для личного ключа объекта, ключ органа сертификации, пользующегося непосредственным доверием и возможно другие данные. В зависимости от стратегии обеспечения безопасности объекта или требований к системе эта среда может быть, например, криптографически защищенным файлом или маркером аппаратных средств, защищённых от умышленных повреждений.	X.843
Физическая безопасность	**physical security**	Меры, предпринимаемые для обеспечения физической защиты ресурсов от умышленных и случайных угроз.	X.800
Администратор доступа	**principal**	Объект, идентификация которого может быть аутентифицирована.	X.811
Секретность	**privacy**	1. Право частного лица контролировать или воздействовать на то, какая касающаяся его информация может быть собрана и сохранена, а также кем и кому содержание этой информация может быть открыто. *Примечание.* – Учитывая, что данный термин относится к правам частных лиц, он не может быть предельно точным и следует воздерживаться от его использования за исключением случаев обоснования уровня необходимой безопасности. 2. Режим связи, при котором расшифровывать сообщения могут только имеющие на это разрешение стороны. Как правило, это достигается с помощью шифрования и использования коллективного(ых) ключа(ей) к шифру.	X.800 H.235
Личный ключ; секретный ключ (исключенный)	**private key; secret key (deprecated)**	1. Это ключ (в криптосистеме с открытым ключом) из пары ключей пользователя, который известен только пользователю. 2. Ключ, который используется с асимметричным криптографическим алгоритмом и количество владельцев которого ограничено (обычно единственным объектом). 3. Ключ, который используется в криптографии с открытым ключом, принадлежит конкретному объекту и должен оставаться секретным.	X.509 X.810 J.170
Полномочие	**privilege**	Атрибут или свойство, назначенное объекту соответствующим органом.	X.509
Инфраструктура управления полномочиями (PMI)	**Privilege Management Infrastructure (PMI)**	Инфраструктура, способная поддерживать управление полномочиями при поддержке комплексной услуги авторизации и при взаимодействии с инфраструктурой открытых ключей.	X.509

Термин	Термин	Определение	Ссылка
Открытый ключ	**public key**	1. Это ключ (в криптосистеме с открытым ключом) из пары ключей пользователя, который известен всем. 2. Ключ, который используется с асимметричным криптографическим алгоритмом и доступ к которому может быть открытым. 3. Ключ, используемый в криптографии с открытым ключом, который принадлежит конкретному объекту и распространяется открытым способом. Другие объекты используют этот ключ для кодирования данных, подлежащих отправке владельцу ключа.	X.509 X.810 J.170
Сертификат открытого ключа	**public key certificate**	1. Открытый ключ пользователя и некоторая другая информация, не поддающиеся подделке благодаря шифрованию, вместе с личным ключом выдавшего его органа сертификации. 2. Значения, представляющие собой открытый ключ владельцев (и другую факультативную информацию), которые проверены и подписаны доверенным органом в формате, не поддающемся подделке. 3. Увязывание открытого ключа объекта с одним или более атрибутами, связанными с его идентификационной информацией, также называемое цифровой подписью.	X.509 H.235 J.170
Криптография с открытым ключом	**Public Key Cryptography**	Криптографический метод, основанный на алгоритме личного и открытого ключей, при котором сообщение кодируется с помощью открытого ключа, но может быть декодировано только при помощи личного ключа. Известен также как система личного-открытого ключа (PPK). *Примечание.* – Знание открытого ключа не раскрывает личного ключа. Пример: Сторона А хотела бы разделить личный и открытый ключи и публично направить открытый ключ всем, кто пожелал бы связаться со Стороной А, но сохранить в секрете личный ключ. Далее, в то время как любой, кто имеет открытый ключ, сможет закодировать сообщения для Стороны А, раскодировать их можно будет только при наличии личного ключа, имеющегося у Стороны А.	J.93
Инфраструктура открытых ключей (PKI)	**Public Key Infrastructure (PKI)**	Инфраструктура, способная поддерживать управление открытыми ключами, обеспечивающее поддержку услуг аутентификации, кодирования, целостности и фиксации авторства.	X.509
Орган регистрации (OP)	**Registration Authority (RA)**	1. Какой-либо объект, отвечающий за идентификацию и аутентификацию субъектов сертификатов, но не являющийся органом сертификации и органом по присвоению атрибутов, и, следовательно, не занимающийся подписью и выдачей сертификатов. *Примечание*. – OP может оказывать содействие процессу применения сертификатов, процессу аннулирования или обоим процессам. 2. Орган, которому предоставлено право и доверено предоставлять услугу регистрации.	X.842 X.843
Злонамеренное воздействие с ретрансляцией	**relay attack**	Злонамеренное воздействие на аутентификацию, при котором осуществляется перехват обмена аутентификационной информацией и немедленная ее ретрансляция.	X.811
Доверяющая сторона	**relying party**	Пользователь или агент, который при принятии решения полагается на данные сертификата.	X.509
Повторное использование	**replay**	Сообщение или его часть повторяется для создания неразрешенного результата. Например, действительное сообщение, содержащее аутентификационную информацию, может быть повторно использовано другим объектом в целях своей аутентификации (как тем, чем он не является)	X.800
Непризнание авторства	**repudiation**	1. Отказ признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи. 2. Объект, задействованный в обмене информацией, последовательно отрицает этот факт. 3. Если пользователь системы MHS (в случае системы MHS) или система MTS в дальнейшем могут отрицать факт представления, приема или создания сообщения, включая отрицание происхождения, отрицание представления, отрицание доставки.	X.800 M.3016.0 X.402

Термин	Термин	Определение	Ссылка
Раскрытие	**reveal**	Операция частичного или полного удаления ранее примененной защиты.	X.814
Сертификат аннулирования	**revocation certificate**	Сертификат безопасности, выданный органом безопасности для указания, что конкретный сертификат безопасности был аннулирован.	X.810
Сертификат списка аннулирования	**revocation list certificate**	Сертификат безопасности, определяющий список сертификатов безопасности, которые были аннулированы.	X.810
Управление маршрутизацией	**routing control**	Применение правил в процессе маршрутизации для выбора или обхода конкретных сетей, линий или ретрансляторов.	X.800
Стратегия безопасности на основе правил	**rule-based security policy**	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.	X.800
Печать	**seal**	Криптографическое контрольное значение, которое обеспечивает поддержку целостности, но не защищает от подлога, осуществляемого получателем (т. е. не обеспечивает фиксацию авторства). Если печать связана с элементом данных, то 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 пользующимися доверием третьими сторонами.	X.810
Секретный ключ	**secret key**	Ключ, используемый с асимметричным криптографическим алгоритмом. Обладание секретным ключом ограничено (обычно двумя объектами).	X.810
Безопасность	**security**	Термин "*безопасность*" используется в смысле минимизации не незащищенности активов и ресурсов. Активом является что-либо представляющее ценность. *Незащищенность* - это любое слабое место, которое может использоваться для нарушения работы системы или содержащееся в ней информации. Какая-либо *угроза* является потенциальным нарушением безопасности.	X.800
Администратор безопасности	**security administrator**	Лицо, ответственное за определение или выполнение требований одной или более частей стратегии обеспечения безопасности.	X.810
Сигнал о нарушении безопасности	**security alarm**	Сообщение, создаваемое в случае обнаружения события, имеющего отношение к безопасности, которое, в соответствии со стратегией обеспечения безопасности, определяется как условие нарушения безопасности. Сигнал о нарушении безопасности имеет целью своевременно обратить внимание соответствующих объектов.	X.816
Ассоциация по безопасности	**security association**	Отношения между двумя или более объектами, для которых существуют атрибуты (информация о состоянии или правила) для управления предоставлением услуг обеспечения безопасности, задействующих эти объекты. Отношения между установившими связь объектами низшего уровня, в отношении которых существуют соответствующие атрибуты ассоциации по безопасности .	X.803 X.802
Проверка безопасности	**security audit**	Независимый анализ или рассмотрение системных записей и действий для проверки на соответствие управляющих функций системы, с целью обеспечения соответствия установленным стратегическим и эксплуатационным процедурам, для выявления нарушения безопасности и для предложения каких-либо изменений в управлении, стратегии или процедурах.	X.800
Данные проверки безопасности	**security audit trail**	Данные, которые собраны и могут быть использованы для содействия проведению проверки безопасности.	X.800
Аудитор безопасности	**security auditor**	Лицо или процесс, которому разрешен доступ к данным проверки безопасности и создание отчетов о проверке.	X.816

Термин	Термин	Определение	Ссылка
Орган безопасности	**security authority**	1. Объект, ответственный за определение, реализацию и выполнение стратегии обеспечения безопасности. 2. Объект, ответственный за управление стратегией обеспечения безопасности в домене обеспечения безопасности. 3. Администратор, ответственный за реализацию стратегии обеспечения безопасности.	X.810 X.841 X.903
Сертификат безопасности	**security certificate**	Набор связанных с безопасностью данных, выданных органом безопасности или пользующейся доверием третьей стороной, вместе с информацией безопасности, которая используется для обеспечения услуг целостности и аутентификации источника данных. *Примечание.* – Все сертификаты считаются сертификатами безопасности. Термин "сертификат безопасности" в серии Рекомендаций МСЭ-Т X.800 принят во избежание терминологического несоответствия с Рекомендацией МСЭ-Т X.509.	X.810
Домен безопасности	**security domain**	1. Совокупность пользователей и систем, подчиняющихся общей стратегии обеспечения безопасности. 2. Набор ресурсов, подчиняющихся одной стратегии обеспечения безопасности.	X.841 X.411
Обмен данными безопасности	**security exchange**	Передача или последовательность передач данных управления-протокола-приложения между открытыми системами, являющихся частью работы одного или нескольких механизмов обеспечения безопасности.	X.803
Информация о безопасности (ИБ)	**security information (SI)**	Информация, необходимая для реализации услуг обеспечения безопасности.	X.810
Метка безопасности	**security label**	Маркировка, связанная с ресурсом (которым может быть блок данных), определяющая имя или обозначение атрибутов безопасности данного ресурса.	X.800
Управление обеспечением безопасности	**security management**	Управление обеспечением безопасности включает любую деятельность по установлению, поддержанию и удалению аспектов системы, связанных с обеспечением безопасности. Тематика охватывает: управление услугами обеспечения безопасности; установку механизмов обеспечения безопасности; управление ключами защиты (часть управления); установление идентификации, ключи, данные управления доступом и т. д.; управление данными проверки безопасности и сигналами нарушения безопасности.	M.3016.0
Модель обеспечения безопасности	**security model**	Основа для описания услуг обеспечения безопасности, которые противодействуют потенциальным угрозам системе MTS, и элементов обеспечения безопасности, которые поддерживают эти услуги.	X.402
Стратегия обеспечения безопасности	**security policy**	1. Набор правил, установленных органом безопасности, который управляет использованием и предоставлением услуг и средств обеспечения безопасности. 2. Набор критериев для предоставления услуг обеспечения безопасности. *Примечание.* – См. *Стратегия обеспечения безопасности на основе идентификации* и *на основе правил*. Полная стратегия обеспечения безопасности неизбежно затрагивает многие вопросы, выходящие за рамки ВОС (взаимодействие открытых систем).	X.509 X.800
Security policy rules	**security rules**	Местная информация, которая с учетом выбранных услуг обеспечения безопасности определяет механизмы обеспечения безопасности для применения, включая все параметры, необходимые для работы данного механизма. *Примечание.* – Правила обеспечения безопасности имеют вид правил безопасного взаимодействия, определенных в модели обеспечения безопасности высшего уровня.	X.802
Услуга безопасности	**security service**	Услуга, предоставляемая каким-либо уровнем открытых систем связи, которая гарантирует достаточную защиту систем или процессов передачи данных.	X.800
Состояние безопасности	**security state**	Информация о состоянии, которая хранится в открытой системе и требуется для предоставления услуг обеспечения безопасности.	X.803

Термин	Термин	Определение	Ссылка
Маркер безопасности	**security token**	Набор данных, передаваемых между объектами связи, который защищен одной или несколькими услугами обеспечения безопасности, вместе с информацией о безопасности, которая используется при их предоставлении.	X.810
Преобразование данных о безопасности	**security transformation**	Набор функций (обеспечения безопасности системы и обеспечения безопасности связи), которые вместе воздействуют на элементы данных пользователя для защиты особым образом этих элементов данных в период осуществления связи и хранения.	X.803
Защита отдельных полей	**selective field protection**	Защита конкретных полей в сообщении, которое подлежит передаче.	X.800
Критичность	**sensitivity**	Характеристика ресурса, которая косвенно выражает его значение или важность.	X.509
Коллективное секретное значение	**shared secret**	Относится к ключу системы защиты для криптографических алгоритмов; может быть получено исходя из пароля.	H.530
Защита	**shield**	Преобразование данных в данные с защищенной целостностью.	X.815
Подпись	**signature**	См. *Цифровая подпись*.	X.800
Простая аутентификация	**simple authentication**	Аутентификация посредством соглашений о простых паролях.	X.509
Источник полномочий (ИП)	**Source of Authority (SOA)**	Орган по присвоению атрибутов, которому верификатор полномочий для конкретного ресурса доверяет как высшему органу по назначению набора полномочий.	X.509
Рассылка спама	**spamming**	Злонамеренное воздействие 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 ценные ресурсы системы.	H.235
Строгая аутентификация	**strong authentication**	Аутентификация с помощью криптографически полученных полномочий.	X.509
Симметричный метод аутентификации	**symmetric authentication method**	Метод аутентификации, при котором оба объекта совместно используют общую информацию об аутентификации.	X.811
Симметричный криптографический алгоритм	**symmetric cryptographic algorithm**	Алгоритм выполнения шифрования или соответствующий алгоритм выполнения дешифрования, в котором для шифрования и дешифрования требуется один и тот же ключ.	X.810
Угроза	**threat**	Потенциальное нарушение безопасности.	X.800
Услуга отметки времени	**time stamping service**	Услуга, которая подтверждает существование электронных данных в определенный момент времени. *Примечание.* – Услуги отметки времени полезны и, возможно, совершенно необходимы для поддержки проверки подписей в течение длительного срока.	X.842
Анализ трафика	**traffic analysis**	Извлечение сведений посредством анализа открытой информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота).	X.800
Конфиденциальность потоков трафика	**traffic flow confidentiality**	Услуга обеспечения конфиденциальности для защиты от анализа трафика, т. е. услуга обеспечения безопасности для предоставления защиты информации, которая может быть получена на основе наблюдения за потоками трафика.	X.800

Термин	Термин	Определение	Ссылка
Подстановка трафика	**traffic padding**	Генерирование ложных событий связи, ложных блоков данных и/или ложных данных в пределах блоков данных.	X.800
Путь обхода системы защиты	**Trapdoor**	Результат действия, при котором объект системы претерпевает изменение, для того чтобы позволить злоумышленнику оказать несанкционированное влияние на команду или на предопределенное событие или на последовательность событий. Например, проверка пароля может быть изменена таким образом, что помимо своего обычного результата она подтверждает также правильность пароля злоумышленника.	X.800
Троянский конь	**Trojan horse**	При проникновении в систему "троянский конь" помимо разрешенной функции обладает несанкционированной функцией. "Троянский конь" – это ретрансляция, при которой происходит также копирование сообщений по неразрешенному каналу.	X.800
Доверие	**trust**	Говорят, что объект X доверяет объекту Y в отношении ряда действий, если и только если объект X полагается на объект Y, который ведет себя определенным образом по отношению к этим действиям.	X.810
Доверенный объект	**trusted entity**	Объект, который может нарушить стратегию обеспечения безопасности путем выполнения непредполагаемых действий либо путем невыполнения предполагаемых действий.	X.810
Функциональная возможность, пользующаяся доверием	**trusted functionality**	Функциональная возможность, воспринимаемая как подходящая по определенным критериям, например как установленная в соответствии со стратегией обеспечения безопасности.	X.800
Пользующаяся доверием третья сторона	**trusted third party (TTP)**	Орган безопасности или его агент, пользующийся доверием (других объектов) в отношении некоторых связанных с безопасностью действий (в контексте стратегии обеспечения безопасности).	X.810
Несанкционированный доступ	**unauthorized access**	Объект пытается осуществить доступ к данным в нарушение действующей стратегии обеспечения безопасности.	M.3016.0
Незащищенный	**unshield**	Преобразование данных с защищенной целостностью в данные с исходной защищенностью.	X.815
Аутентификация пользователя	**user authentication**	Установление доказательства идентификации пользователя-человека или прикладного процесса.	M.3016.0
Проверять	**validate**	Проверка данных с защищенной целостностью для обнаружения потери целостности.	X.815
Верификатор	**verifier**	Является объектом, требующим аутентифицированной идентификации, или представляет его. Верификатор включает в себя функции, необходимые для осуществления обменов в целях аутентификации.	X.811
Незащищенность	**vulnerability**	Любое слабое место, которое может быть использовано для нарушения системы или информации, которая в ней содержится.	X.800
Сертификат X.509	**X.509 certificate**	Спецификация сертификата открытого ключа, разработанная как часть каталога стандартов МСЭ-Т X.500.	J.170

B.2 Сокращения, относящиеся к тематике обеспечения безопасности

Сокращение	Определение
AA	[X.509] Орган по присвоению атрибутов
ACI	[SANCHO] Информация управления доступом
AE	[M.3010] Прикладной объект
AES	[H.235] [J.170] Усовершенствованный стандартный алгоритм шифрования
APS	[SANCHO] Автоматическая коммутация с защитой данных
ASN.1	[H.680] Абстрактная синтаксическая нотация версии один
ASON	[SANCHO] Оптическая сеть автоматической коммутацией
ASP	[X.805] [X.1121] Поставщик прикладных услуг
CA	[H.234] [H.235] [J.170] [X.509] Орган сертификации. Доверенная организация, которая принимает приложения сертификатов от объектов, аутентифицирует приложения, выдает сертификат и осуществляет ведение информации о статусе сертификатов. [J.170] Агент вызова. Часть CMS, которая поддерживает состояние установленной связи и управляет связью со стороны линии связи.
CME	[X.790] Согласованный объект управления.
CMIP	[M.3010] Протокол передачи общей управляющей информации.
CMS	[J.170] Криптографический 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).
CORBA	[SANCHO] Общая архитектура посредника запросов объектов.
COS	[SANCHO] Класс услуги.
CP	Стратегия в отношении сертификатов.
CPS	[SANCHO: X.842] Свидетельство о практике проведения сертификации [SANCHO: Q.817] Свидетельство о порядке проведения сертификации
CRL	[H.235] [X.509] Список аннулирования сертификатов
DCN	[SANCHO] Сеть передачи данных
DES	[SANCHO] Стандарт шифрования данных, стандарт зашифровывания данных
DHCP	[SANCHO] Протокол динамической конфигурации узлового компьютера
DOCSIS	[SANCHO] Спецификация интерфейса службы передачи данных по кабелю
DSA	[X.509] Агент системы каталогов [SANCHO] Алгоритм цифровой подписи
DSL	[SANCHO] Цифровой абонентский шлейф
DSP	[SANCHO] Процессор цифрового сигнала [SANCHO] Протокол услуги справочника
FDS	[SANCHO] 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
GK	[H.235] [H.510] [H.530] Пропускной пункт
GW	[H.235] Шлюз
HFC	[SANCHO] Комбинированный волоконно-коаксиальный кабель
HFX	[T.30] [T.36] Факсимильный шифр Hawthorne
HKM	[T.30] [T.36] Алгоритм управления ключами Hawthorne

Сокращение	Определение
ICN	Информационно-коммуникационная сеть
ICT	Информационно-коммуникационные технологии
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 обеспечивающим весьма высокую защиту. Относится к числу наиболее популярных алгоритмов. В течение нескольких лет его использования не появилось ни одного официального сообщения о предпринятых в отношении него практических попыток злонамеренного воздействия, несмотря на ряд попыток их обнаружения (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html).
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
IKE+	[J.170] Нотация, определенная с целью указания механизма IKE, для которого требуются сертификаты открытых ключей.
IMT-2000	[M.3210.1] Международная подвижная электросвязь 2000
IP	[X.805] Протокол Internet
IPSec	[H.235] [H.530] [J.170] [X.805] Безопасность протокола Internet.
IVR	[J.170] Интерактивная система речевой связи
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 называемый MIC. [J.170] Управление доступом к среде. Подуровень уровня канала передачи данных. Обычно работает непосредственно над физическим уровнем.
MCU	[H.235] Многоадресный блок. [H.323] Многопунктовый 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] База информационных данных
MIS	[M.3010] Система передачи управляющей информации
MS	[M.3210.1] Система управления Хранилище сообщений Участок мультиплексирования
MSP	[SANCHO] Защита участка мультиплексирования
MS-SPRing	Кольцо коллективной защиты участка мультиплексирования
MTA	[J.170] Адаптер медиатерминала Адаптер мультимедийного терминала Агент передачи сообщения
NAT	[H.235] Трансляция сетевых адресов
OAM&P	[SANCHO] Эксплуатация, администрирование, техническое обслуживание и обеспечение
OS	[M.3010] [X.790] Операционная система
OSF	[M.3010] Функция операционных систем
OSI	[SANCHO] Взаимодействие открытых систем

Сокращение	Определение
OSS	[J.170] Поддержка операционной системы. Программное обеспечение поддержки, которое используется для конфигурирования, управления качеством, устранения отказов, учета и управления безопасностью.
PDA	Электронный секретарь, хранящий персональные данные
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 управления процессами выдачи сертификатов.
PKINIT	[J.160] Первоначальная аутентификация с помощью криптографии с открытым ключом [J.191] Криптография с открытым ключом для первоначальной аутентификации
PMI	[X.509] Инфраструктура управления полномочиями
QoS	[SANCHO] Качество обслуживания
RA	Орган регистрации
RADIUS	[J.170] Служба удаленной аутентификации пользователей по телефонным линиям
RAS	[SANCHO] Регистрация, допуск и статус [SANCHO] Протокол регистрации, допуска и статуса
RBAC	[X.509] Управление доступом по ролевому признаку
RKS	[J.170] Сервер ведения записей. Устройство, которое собирает сообщения о событиях и выполняет их корреляцию.
RSA	[H.235] [T.30] [T.36] Алгоритм Ривеста, Шамира и Адлмана (алгоритм шифрования с открытыми ключами)
RTP	[H.225.0] [H.235] [J.170] Протокол реального времени
SHA1	[H.235] Защищенный алгоритм хеширования № 1
SG	Шлюз сигнализации
SIP	[J.170] [X.805] Протокол инициирования сеанса связи. Протокол управления (сигнализация) прикладного уровня для создания, изменения и завершения сеансов с одним или более участниками.
SNC	[SANCHO] Соединение по подсети
SNMP	[J.170] [X.805] Простой протокол управления сетью
SoA	[X.509] Источник полномочий
SRTP	[H.235] Защищенный протокол реального времени
SS7	[J.170] [X.805] Система сигнализации номер 7 – это архитектура и набор протоколов для выполнения внеполосной сигнализации вызовов с телефонной сетью.
SSL	[H.235] [X.805] Уровень защищенных разъемов
TFTP	[SANCHO] Тривиальный протокол передачи файлов
TGS	[J.160] Сервер выдачи разрешения
TLS	[H.235] Безопасность транспортного уровня
TMN	[M.3010] [M.3210.1] [X.790] Сеть управления электросвязью
TTP	[X.810] Пользующаяся доверием третья сторона
UDP	[J.170] Протокол пользовательских дейтаграмм
VA	Проверяющий орган
VoIP	[X.805] Передача речи по протоколу Internet
VPN	[X.805] Виртуальная частная сеть

Приложение C

Перечень исследовательских комиссий и Вопросов, связанных с проблемой безопасности

Деятельность МСЭ–Т в области стандартизации осуществляется исследовательскими комиссиями (ИК), в которых представители членов МСЭ-Т разрабатывают Рекомендации (стандарты) для различных областей международной электросвязи. ИК ведут свою работу в форме изучения Вопросов. Каждый из них предполагает проведение технических исследований в конкретной области стандартизации электросвязи. Ниже перечислены исследовательские комиссии МСЭ-Т на исследовательский период 2005–2008 годов, их наименования и мандаты, а также перечень Вопросов для изучения, связанных с деятельностью в области обеспечения безопасности.

ИК2	Эксплуатационные аспекты предоставления услуг, сети и характеристики работы *Ведущая исследовательская комиссия по вопросам определения услуг, нумерации и маршрутизации*
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 обеспечением безопасности:	
– **Q.1/2** – Применение планов нумерации, наименования и адресации для электросвязи и услуг и эксплуатационных аспектов нумерации, включая определение услуг (F.851)	
– **Q.4/2** – Эксплуатационные аспекты качества обслуживания в сетях электросвязи (E.408, E.409 (совместно с ИК17))	

ИК3	Принципы тарификации и расчетов, включая соответствующие экономические и стратегические вопросы электросвязи
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 обеспечением безопасности: Нет	

ИК4	Управление электросвязью *Ведущая исследовательская комиссия по вопросам управления электросвязью*

Отвечает за проведение исследований, касающихся управления службами, сетями и оборудованием электросвязи, включая поддержку сетей последующих поколений (СПП) и применение и развитие структуры сети управления электросвязью (СУЭ). Кроме того, на нее возложена ответственность за проведение других исследований в области управления электросвязью, относящихся к обозначениям, процедурам работ, связанных с транспортным протоколом, а также к контрольно-измерительным методам и приборам.

Работа ИК4 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 на 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 рамках одной или нескольких администраций. Исходя из принципов архитектуры, в действующих Рекомендациях определены конкретные требования, механизмы и поддерживающие протоколы, а также разрабатывается еще ряд Рекомендаций.

Недавно утвержденная серия Рекомендаций M.3016 заменяет исходную Рекомендацию МСЭ-Т M.3016 (1998 г.). В ней описывается значимость и применимость вопросов обеспечения безопасности в контексте языка СУЭ. В данной серии рекомендаций конкретным организациям предоставляется основа для создания соответствующей спецификации использования имеющихся в распоряжении механизмов, а не указывается набор услуг для защиты от угроз.

В серии Рекомендаций M.3016 рассматриваются следующие угрозы в СУЭ: осуществление подмены, перехват информации, несанкционированный доступ, Потеря или искажение информации, непризнание авторства, мошенничество и отказ от обслуживания. Она охватывает также следующие функции безопасности: обеспечение конфиденциальности, целостности данных, отчетность и готовность.

Вопросы, относящиеся к обеспечению безопасности:

– **Q.6/4** – Принципы и архитектура управления (M.3010, серия M.3016, M.3400)

– **Q.7/4** – Требования к интерфейсам управления бизнес-бизнес и абонент-бизнес (M.3320)

– **Q.10/4** – Относящиеся к конкретным приложениям информационные модели (M.3210.1)

– **Q.11/4** – Протоколы для интерфейсов управления (Q.813, Q.815, Q.817)

ИК5	Защита от электромагнитных воздействий окружающей среды

Отвечает за проведение исследований, относящихся к защите сетей и оборудования электросвязи от помех и ударов молний, а также за исследования, касающиеся электромагнитной совместимости (ЭМС), безопасности и последствий для здоровья, связанных с влиянием электромагнитных полей, которые создаются установками и устройствами электросвязи, включая сотовые телефоны.

Выполняя свою задачу, ИК5 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 искусственного происхождения, 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 из оборудования.

Природа умышленных угроз и соответствующие средства их смягчения аналогичны тем, которые применяются к естественным или непреднамеренным электромагнитным возмущениям. У HEMP и электромагнитного импульса, создаваемого молнией, существуют общие черты. Методы экранирования и фильтрации, которые уменьшают передачу энергии нежелательного радиоизлучения оборудования, снижают также возможность непреднамеренной утечки энергии. Следовательно, традиционная деятельность 5-й Исследовательской комиссии, касающаяся защиты от ударов молнии и контроля электромагнитных помех (ЭМП), содействует обеспечению защиты сети от умышленно создаваемых угроз искусственного происхождения. В ходе текущего исследовательского периода аспекты работы ИК, связанные с безопасностью, рассматриваются в рамках нового Вопроса 15/5 – *Защита систем электросвязи и информации от электромагнитного воздействия окружающей среды.*

Электромагнитные угрозы включают злонамеренно создаваемые нестационарные процессы большой мощности искусственного происхождения, такие как возникновение электромагнитного импульса в результате высотного ядерного взрыва (HEMP) и излучения электромагнитных генераторов высокой мощности (HPEM), включая мощное сверх высокочастотное излучение (HPM) и излучения сверхширокополосных источников (UWB). Наряду с этим электромагнитная защита охватывает проблему утечки информации в сетях электросвязи вследствие непредвиденного радиоизлучения оборудования.

Вопросы, относящиеся к обеспечению безопасности:

- **Q.2/5** – ЭМС, связанная с широкополосными сетями доступа (Управление нежелательными излучениями систем широкополосного доступа содействует снижению вероятности утечки информации).
- **Q.4/5** – Устойчивость оборудования связи (Устойчивость оборудования к ударам молнии повышает устойчивость оборудования к перенапряжениям, наводимым HEMP).
- **Q.5/5** – Защита систем электросвязи от ударов молний (Методы, используемые для защиты от ударов молний, повышают степень устойчивости оборудования к воздействиям HEMP и HPE).
- **Q.6/5** – Конфигурации соединений и заземление систем электросвязи в глобальной окружающей среде (Принятие надлежащих мер по соединению и заземлению также помогает повысить степень устойчивости 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 проводимых и излучаемых HEMP, а также в среде излучаемых HPE. Также ЭМС оборудования электросвязи снижает вероятность утечки информации).
- **Q.15/5** – Защита систем электросвязи и информации от электромагнитного воздействия окружающей среды (Устойчивость оборудования к ударам молний повышает устойчивость оборудования к перенапряжениям, наводимым HEMP).

ИК6	Внешние линейно-кабельные сооружения и связанные с ними установки в помещениях

Отвечает за проведение исследований, касающихся линейно-кабельных сооружений и связанных с ними установок в помещениях, в таких областях как сооружение, прокладка, соединение, оконечная нагрузка, защита всех типов наземных 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.

Вопросы, относящиеся к обеспечению безопасности:

- **Q.6/6** – Процедуры в отношении внешних линейно-кабельных сооружений, касающиеся вопросов окружающей среды и безопасности
- **Q.6/6** – Техническое обслуживание волоконно-оптической кабельной сети

ИК9	Интегрированные широкополосные кабельные сети и передача телевизионных и звуковых программ *Ведущая исследовательская комиссия по вопросам интегрированных широкополосных кабельных и телевизионных сетей.*

Отвечает за проведение исследований, касающихся:

a) использования 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 критических по времени услуг, видеопрограмм по заказу, интерактивных услуг и т. д.;

b) использования систем электросвязи для трансляции, первичного распределения и вторичного распределения телевизионных и звуковых программ, а также предоставления других аналогичных услуг передачи данных.

В качестве ведущей исследовательской комиссией по вопросам интегрированных широкополосных кабельных и телевизионных сетей ИК9 проводит оценку угроз и уязвимости широкополосных сетей и услуг, ведет документирование объектов защиты, оценивает меры противодействия и определяет архитектуру безопасности.

Деятельность, связанная с безопасностью, строится по следующим направлениям:

a) *Безопасные широкополосные услуги:* предоставление услуг обеспечения безопасности для сетей широкополосного доступа, а именно, аутентификация кабельного модема, управление криптографическими ключами, секретность и целостность передаваемых данных и безопасная загрузка программного обеспечения кабельного модема.

b) *Безопасные услуги VoIP:* IPCablecom является специальным проектом по нормируемым по времени интерактивным услугам, предоставляемым по кабельным телевизионным сетям с использованием протокола IP, в частности по передаче звука 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, безопасную инициализацию и конфигурацию устройства, безопасные управление устройствами, безопасную сигнализацию и безопасную среду передачи.

c) *Безопасные 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, безопасное управление брандмауэрами и безопасную загрузку программного обеспечения усовершенствованного кабельного модема.

d) *Безопасная среда приложений для интерактивных телевизионных служб:* Интерактивные телевизионные службы базируются на услугах обеспечения безопасности, определенных в спецификации Java и мультимедийной домашней платформы (MHP).

Вопросы, относящиеся к обеспечению безопасности:

– **Q.3/9** – Методы и практическое применение ограниченного доступа, защиты от несанкционированного копирования и несанкционированного перераспределения ("управление перераспределением" для распределения программ цифрового кабельного телевидения в жилых помещениях)

– **Q.8/9** – Предоставление цифровых услуг кабельного телевидения и прикладных программ с использованием протокола Internet (IP) и/или данных в пакетном режиме (J.112)

– **Q.9/9** – Прикладные программы передачи речевых и видеосигналов с использованием IP по сетям кабельного телевидения (J.160, J.170, J.191)

– **Q.10/9** – Расширение услуг, предоставляемых по кабельным широкополосным сетям, на сети бытового использования

ИК11	Требования к сигнализации и протоколы *Ведущая исследовательская комиссия по вопросам сигнализации, протоколов и интеллектуальных сетей*

Отвечает за проведение исследований, касающихся требований к сигнализации и протоколов, связанных с функциями протокола Internet (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.

Большинство существующих Рекомендаций ИК11 были разработаны для пользующихся доверием сетей на основе ВРК, в которых межпунктовые соединения могут быть использованы для обеспечения безопасности связи. ИК11 признала, что внедрение на сети IP-технологии ставит новые задачи по обеспечению безопасности. В 2004 году ИК11, признавая внедрение IP-технологии и необходимость возможности безопасного предоставления информации управления и сигнализации в этой развивающейся сети, разработала ряд Вопросов, относящихся к требованиям к сигнализации и протоколу, которые учитывают эти новые задачи в области обеспечения безопасности.

Вопросы, относящиеся к обеспечению безопасности:

– **Q.1/11** – Функциональная архитектура сигнализации сети и управления в условиях появления СПП

– **Q.7/11** – Требования к сигнализации и управлению и протоколы в поддержку подсоединения в условиях СПП

ИК12	Характеристики работы и качество обслуживания *Ведущая исследовательская комиссия по вопросам качества обслуживания и характеристик*

Отвечает за разработку Рекомендаций по характеристикам сквозной передачи оконечного оборудования и сетей в зависимости от воспринимаемого качества и приемлемости для пользователя текста, речи и мультимедийных приложений. Несмотря на то, что данная работа включает связанные с этим вопросы передачи для всех сетей (например, базирующихся на ПЦИ, СЦИ, АРП и IP, а также СПП) и всех оконечных устройств электросвязи (например, микротелефонной трубки, громкоговорящего телефона, телефонной гарнитуры, мобильного телефона, видеотелефонного устройства и устройства интерактивного речевого ответа), а также вопросы, относящиеся к характеристикам работы и управлению ресурсами, особое внимание уделяется вопросам качества обслуживания при использовании IP, взаимодействия и последствиям для СПП.

Вопросы, относящиеся к обеспечению безопасности:

– **Q.10/12** – Вопросы, касающиеся планирования и осуществления передачи для речевых телефонных услуг, доставки данных и мультимедийных услуг

– **Q.13/12** – Требования в отношении характеристик качества обслуживания/качества опыта мультимедийных служб и методы оценки

– **Q.17/12** – Характеристики сетей на базе IP

ИК13	Сети последующих поколений *Ведущая исследовательская комиссия по вопросам СПП и спутников*

Отвечает за исследования, относящиеся к архитектуре, развитию и конвергенции сетей последующих поколений (СПП), включая структуры и функциональную архитектуру, требования к сигнализации для СПП, координацию управления проектами СПП в исследовательских комиссиях и осуществление планирования, сценарии внедрения и модели развертывания, возможности сетей и обслуживания, взаимодействие, воздействие **IPv6**, мобильность в СПП и конвергенция сетей, аспекты сети передачи открытых данных.

Признавая, что безопасность является одной из ключевых особенностей СПП, ИК13 установила специальный Вопрос, относящийся к обеспечению безопасности: Вопрос 15/13, Безопасность СПП. Особое внимание в Вопросе уделяется исследованиям проблем обеспечения безопасности, относящихся к СПП, и разработке решений по обеспечению безопасности для СПП. Одной из важнейших целей ИК13 является ввод в действие набора стандартов, который в максимальной мере будет гарантировать безопасность инфраструктуры электросвязи по мере преобразования унаследованных сетей в СПП.

13-я Исследовательская комиссия приняла также решение включать в каждую новую или, со временем, пересмотренную рекомендацию раздел, посвященный вопросам обеспечения безопасности, в котором даются ссылки на те разделы данной рекомендации, в которых рассматриваются аспекты обеспечения безопасности.

13-я Исследовательская комиссия проводит работу по вопросам, относящимся к обеспечению безопасности в сотрудничестве с другими исследовательскими комиссиями, а также другими организациями по разработке стандартов (ОРС). Наиболее важными внешними ОРС, имеющими большое значение для исследований ИК13 в области обеспечения безопасности, являются IETF (в областях интернета, безопасности и транспортирования), 3GPP, 3GPP2 и Форум DSL.

Вопросы, относящиеся к обеспечению безопасности:

– **Q.2/13** – Требования и сценарии осуществления, касающиеся появляющихся услуг в СПП

– **Q.3/13** – Принципы и функциональная архитектура в СПП

– **Q.4/13** – Требования и инфраструктура, касающиеся качества обслуживания в СПП

– **Q.5/13** – OAM и управление сетями в СПП

– **Q.6/13** – Мобильность СПП и конвергенция сетей фиксированной и подвижной связи

– **Q.7/13** – Взаимодействие сетей и услуг в условиях СПП

– **Q.8/13** – Сценарии обслуживания и модели развертывания СПП

– **Q.9/13** – Влияние IPV6 на СПП

– **Q.10/13** – Функциональная совместимость спутниковых и наземных сетей и сетей следующих поколений (СПП)

– **Q.12/13** – Протокол Frame Relay (X.272)

– **Q.13/13** – Общедоступные сети передачи данных

– **Q.14/13** – Протоколы и механизмы обслуживания для многофункциональных сетей передачи данных (MSDN)

– **Q.15/13** – Безопасность СПП

Задачи по обеспечению безопасности включают:

- Играть ведущую роль при решении вопросов, относящихся к уровню проектов по обеспечению безопасности СПП, в рамках ИК13 и вместе с другими исследовательскими комиссиями. Признавая общую роль ИК17 как ведущей исследовательской комиссии по вопросам обеспечения безопасности в электросвязи, консультировать и оказывать содействия ИК17 по вопросам координации работы в области обеспечения безопасности СПП.
- Определить, каким образом применять Рекомендацию МСЭ-Т X.805, Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами в контексте среды СПП.
- Обеспечить, чтобы разрабатываемая архитектура СПП соответствовала принятым принципам обеспечения безопасности.
- Обеспечить, чтобы при необходимости принципы AAA были внедрены на СПП.

ИК15	Оптические и другие транспортные сетевые инфраструктуры *Ведущая исследовательская комиссия по транспортным аспектам сети доступа* *Ведущая исследовательская комиссия по оптическим технологиям*

В МСЭ-Т 15-я Исследовательская комиссия является координатором деятельности по разработке стандартов инфраструктур оптических и других транспортных сетей, систем, оборудования, оптических волокон и соответствующих технологий плоскости управления для обеспечения возможности развития в направлении создания интеллектуальных транспортных сетей. Эта работа охватывает создание соответствующих стандартов, относящихся к помещениям клиентов, доступу, городским и протяженным участкам сетей связи.

В соответствии с Вопросом 14/15 Комиссия отвечает за определение требований в отношении управления и контроля, а также поддержку информационных моделей для оборудования, осуществляющего транспортные функции. Вопрос 14/15 следует установленным в МСЭ-Т понятию и структуре СУЭ для определения указанных требований и моделей. Управление обеспечением безопасности является одной из пяти ключевых функциональных категорий управления СУЭ. Управление обеспечением безопасности входит в сферу охвата и изучается в рамках Q.14/15:

a) Требования к управлению оборудованием, осуществляющему транспортные функции: в Рекомендациях МСЭ-Т G.7710/Y.1701, G.784, и G.874 рассматриваются функции управления оборудованием (EMF) внутри элементов транспортных сетей, которые являются общими для множества технологий, характерными для сетевых элементов СЦИ и для сетевых элементов оптических транспортных систем (ОТС), соответственно. Дается описание приложений для управления датой и временем, управления устранением неисправностей, управления конфигурацией, управления учетом, управления качеством функционирования и управления обеспечением безопасности. С учетом этих приложений устанавливаются спецификации функций EMF и требования к ним. Требования к управлению обеспечением безопасности, входящие в эти рекомендации, в настоящее время исследуются.

b) 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 (СУЭ), распределенную передачу сигнализации, относящуюся к оптической сети с автоматической коммутацией (ASON), и иную распределенную передачу (например, служебный канал или передача речи, загрузка программного обеспечения). Для разных приложений (например, СУЭ, ASTN и т. д.) требуется сеть передачи в пакетном режиме для транспортирования информации между различными компонентами. Например, для СУЭ необходима сеть связи, которая является сетью передачи для управления (MCN), для транспортирования управляющих сообщений между компонентами СУЭ (например, компоненты NEF и OSF). Для ASON 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 дается ссылка на серию Рекомендаций МСЭ-Т M.3016. Требования к безопасности SCN описаны в Рекомендации МСЭ-Т G.7712/Y.1703.

c) 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 установления связи через интерфейсы для осуществления автоматических операций с вызовами и соединениями. Наряду с прочими определены атрибуты безопасности, позволяющие проводить проверку операций с вызовами и соединениями (например, это может быть информация, разрешающая аутентификацию запроса вызова и, возможно, проверку целостности запроса вызова).

ИК15	Оптические и другие транспортные сетевые инфраструктуры *Ведущая исследовательская комиссия по транспортным аспектам сети доступа* *Ведущая исследовательская комиссия по оптическим технологиям*

d) Архитектура и требования для маршрутизации в ASON: в Рекомендации МСЭ-Т G.7715/Y.1706 определяются требования и архитектура для функций маршрутизации, используемых для установления коммутируемых соединений (SC) и программируемых постоянных соединений (SPC) в рамках 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, относящихся к безопасности, в данной Рекомендации даются ссылки на серии Рекомендаций МСЭ-Т M.3016 и X.800. В частности, говорится, что в зависимости от условий применения протокола маршрутизации степень важности общих целей в области безопасности, определенных в Рекомендациях МСЭ-Т серии M.3016, – конфиденциальности, целостности данных, контролируемости и готовности, – может изменяться. Анализ предлагаемого протокола маршрутизации в отношении угроз, исходя из Рекомендации МСЭ-Т X.900, должен учитывать следующие события: подмену, подслушивание, несанкционированный доступ, потерю или искажение информации (включая злонамеренные воздействия типа повторной передачи перехваченных сообщений), фиксацию авторства, мошенничество и отказ в обслуживании.

e) Структура управления ASON: в Рекомендации МСЭ-Т G.7718/Y.1709 рассматриваются аспекты управления плоскости контроля ASON и взаимодействие между плоскостью управления и плоскостью контроля ASON. Будут включены требования к управлению устранением неисправностей, управлению конфигурацией, управлению учетом, управлению качеством функционирования и управлению обеспечением безопасности для компонентов плоскости контроля.

Вопросы, относящиеся к обеспечению безопасности:

– **Q.3/15** – Общие характеристики оптических транспортных сетей (G.911)

– **Q.9/15** – Транспортное оборудование и защита/восстановление сети (G.808.1, G.841, G.842, G.873.1)

– **Q.14/15** – Управление и контроль в отношении транспортных систем и оборудования

ИК16	Мультимедийные службы, системы и оконечное оборудование *Ведущая исследовательская комиссия по вопросам мультимедийного оконечного оборудования, систем, приложений и повсеместно используемых приложений ("электронное все что угодно", например, электронное здравоохранение и электронный бизнес)*

16-я Исследовательская комиссия является ведущей исследовательской комиссией по вопросам мультимедийного оконечного оборудования, систем, приложений и повсеместно используемых приложений ("электронное все что угодно", например электронное здравоохранение и электронный бизнес). Вопрос 25/16 (РГ 2/16) охватывает "Безопасность мультимедийной связи в сетях последующих поколений" и в его рамках рассматриваются следующие вопросы обеспечения безопасности.

Развитые мультимедийные (ММ) приложения, такие как телефония по сетям с коммутацией пакетов, передача речи по протоколу Internet, интерактивные (видео) конференции и групповая работа; передача сообщений ММ, потоковая транспортировка аудио/видеоданных и другие подвержены разнообразным серьезным угрозам в неоднородных средах. Умышленные воздействия, заключающиеся в злоупотреблении, злонамеренном искажении, подслушивании и отказе в обслуживании, представляют лишь небольшую, но существенную часть возможных и опасных рисков для обеспечения безопасности, особенно в сетях, базирующихся на IP.

Общепризнано, что указанные приложения имеют общие потребности в защите, которые могут быть удовлетворены с помощью характерных мер защиты, например обеспечения безопасности сети или аутентификации в масштабах сети. Вместе с тем, ММ приложения, как правило, имеют потребности в обеспечении безопасности, обусловливаемые конкретным приложением, которые наилучшим образом удовлетворяются на прикладном уровне. Вопрос 25/16 посвящен проблемам безопасности ММ приложений в сетях последующих поколений (Б-ММ-СПП) и при необходимости в нем принимаются в расчет дополнительные меры по обеспечению безопасности в сетях. В рамках Вопроса 25/16 намечено создать рекомендации по вопросу обеспечения безопасности, в которых будут рассмотрены потребности рынка в этом отношении.

Вопросы, относящиеся к обеспечению безопасности:

– **Q.1/16** – Мультимедийные системы, терминалы и многоадресная передача данных

– **Q.2/16** – Аудиовизуальная связь и передача данных в режиме реального времени по сетям с коммутацией пакетов (H.323)

– **Q.4/16** – Свойства усовершенствованных мультимедийных услуг связи на базе определенных МСЭ-Т платформ мультимедийных систем (H.350.2)

– **Q.25/16** – Безопасность мультимедийных средств в сетях последующих поколений (Б-ММ-СПП) (серия Рекомендаций МСЭ-Т H.235.x)

– **Q.29/16** – Мобильность мультимедийных систем и услуг (H.530)

ИК17	Безопасность, языки и программное обеспечение систем электросвязи *Ведущая исследовательская комиссия по вопросам обеспечения безопасности связи, языкам и методам описания*

17-я Исследовательская комиссия отвечает за проведение исследований, относящихся к обеспечению безопасности, к применению открытых систем связи, включая организацию сетей и каталог, к языкам технических описаний и методам их использования, а также к прочим вопросам, связанным с аспектами программного обеспечения систем электросвязи.

17-я Исследовательская комиссия является ведущей исследовательской комиссией по вопросам безопасности электросвязи. Работа МСЭ-Т по стандартизации в области обеспечения безопасности координируется в рамках нового проекта МСЭ-Т по обеспечению безопасности, организованного в рамках Вопроса 4/17. Частью этой работы стали разработка и постоянное обновление каталога Рекомендаций МСЭ-Т, относящихся к вопросам обеспечения безопасности, и каталога определений по тематике безопасности, взятых из утвержденных Рекомендаций МСЭ-Т. Семинары-практикумы и симпозиумы по кибербезопасности состоялись в мае 2002 года в Сеуле (Корея), в октябре 2004 года во Флорианополисе (Бразилия), в марте 2005 года в Москве (Россия) и в октябре 2005 года в Женеве (Швейцария). Другие семинары-практикумы будут организованы по мере необходимости.

Разработанная в РГ 1/17, Рекомендация МСЭ-Т X.509, *Структуры сертификатов атрибутов и открытых ключей* предоставляет основу для инфраструктур открытых ключей (PKI) и инфраструктур управления полномочиями (PMI). Продолжается работа по улучшению Рекомендации X.509 с целью удовлетворения возникающих потребностей. РГ 2/17 отвечает за Рекомендации по вопросам общепризнанной базовой архитектуры обеспечения безопасности, структуры и протокола, в частности за Рекомендации серии X.800. В течение последнего исследовательского периода был подготовлен комплект новых рекомендаций по вопросам обеспечения безопасности, включая Рекомендацию X.805, в которой определяется архитектура безопасности для обеспечения сквозной безопасности сети. Данная архитектура может применяться к различным видам сетей независимо от технологии, лежащей в основе сети. Эта рекомендация может использоваться в качестве инструмента для обеспечения полноты соображений в отношении обеспечения безопасности при разработке рекомендаций и для проведения оценки безопасности сетей. В другой фундаментальной Рекомендации X.1051 определяются требования к системе управления информационной безопасностью (ISMS) в контексте электросвязи. В ней указываются требования для установления, внедрения, эксплуатации, контроля, анализа, технического обслуживания и совершенствования документированной ISMS в контексте общих рисков предприятия электросвязи, связанных с его коммерческой деятельностью. Рекомендация X.1081 является базовой рекомендацией, устанавливающей основу для будущих телебиометрических спецификаций. Рекомендации X.1121 и X.1122 сосредоточены на подвижной сквозной передаче данных. В Рекомендации X.1121 анализируются угрозы безопасности в среде подвижной связи и средства защиты, рассматриваемые с точки зрения пользователя подвижной связи и поставщика прикладных услуг. В Рекомендации X.1122 содержится руководство для использования при создании безопасных подвижных систем на основе технологии инфраструктуры открытых ключей (PKI). С имеющейся в настоящее время информацией можно ознакомиться на веб-странице ИК17 веб-сайта МСЭ по адресу: www.itu.int/ITU-T/studygroups/com17/tel-security.html.

Вопросы, относящиеся к обеспечению безопасности:

WP 1/17 Технология открытых систем

– **Q.1/17 –** Сквозная многоадресная связь с возможностью управления качеством обслуживания

В рамках данного Вопроса рассматриваются аспекты требований, архитектуры, управления группой и сеансом связи и протокол для сквозной многоадресной связи. Рассмотрено распространение протокола обеспечения безопасности на протоколы сквозной многоадресной связи с целью осуществления безопасной связи среди членов группы. Текущая работа сосредоточена на применении соответствующих механизмов обеспечения безопасности и создании процедур для обеспечения безопасной связи.

– **Q.2/17** – Службы каталогов, системы каталогов и сертификаты открытых ключей/атрибутов

В рамках данного Вопроса осуществляется разработка и ведение вопросов, относящихся к Рекомендациям X.509, в которых рассматриваются сертификаты открытых ключей, сертификаты атрибутов, аннулирование сертификатов и спецификация инфраструктур поддержки (инфраструктуры открытых ключей и инфраструктуры управления полномочиями). Сертификаты открытых ключей и инфраструктура поддержки являются основой для осуществления аутентификации и применяются, в частности, для цифровых подписей.

– **Q.16/17** – Интернационализированные имена доменов

Вопросы обеспечения безопасности являются частью работы над интернационализированными именами доменов (IDN). Вопрос 16/17 имеет целью выявление существующей документации, в которой формулируются основы IDN, включая документацию, относящуюся к рискам, которые связаны с безопасностью сетей электросвязи и сопутствуют внедрению IDN. Эта задача решается при консультации с соответствующими объединениями, включая ИСО/МЭК, консорциум UNICODE, IETF, ICANN и CENTR.

WP 2/17 Безопасность электросвязи

– **Q.4/17** – Проект по обеспечению безопасности систем связи

Данный Вопрос посвящен формированию представления, а также координации и организации всей деятельности в области обеспечения безопасности сетей электросвязи, проводимой в рамках МСЭ-Т. В работе по данному Вопросу безопасности, которая будет проводиться в сотрудничестве с другими исследовательскими комиссиями и ОРС, будет использован метод нисходящего проектирования. Данный проект направлен на достижение более целенаправленной работы на проектном и стратегическом уровнях.

– **Q.5/17** – Архитектура и структура безопасности

Для получения эффективных по затратам всеобъемлющих решений в области обеспечения безопасности, которые можно применять к различным типам сетей, услуг и приложений в среде многих поставщиков, безопасность сетей должно строиться по стандартным архитектурам обеспечения безопасности и стандартным технологиям обеспечения безопасности. С учетом угроз для безопасности среды связи и существующего развития относящихся к безопасности мер противодействия этим угрозам в данном проекте рассматриваются новые требования к обеспечению безопасности и соответствующие решения, а также то, каким образом могут развиваться архитектуры и структуры обеспечения безопасности для отражения развивающейся среды.

– **Q.6/17** – Кибербезопасность

В данном Вопросе рассматриваются аспекты кибербезопасности в контексте международной стандартизации. В частности, Вопрос касается следующих областей кибербезопасности:

- процесс распределения, совместного использования и раскрытия информации о незащищенности;
- стандартная процедура для операций управления случаями нарушения безопасности в киберпространстве;
- стратегия защиты особо важной сетевой инфраструктуры.

– **Q.7/17** – Управление безопасностью

Целью данного Вопроса является разработка комплекта Рекомендаций по управлению обеспечением безопасности для МСЭ-Т с учетом необходимости сотрудничества с ОЦГ1 ИСО/МЭК. Вопрос, в частности, концентрируется на определении риска и его управлении в системах электросвязи и приведении в соответствие системы управления информацией о безопасности (ISMS) для операторов связи с существующими стандартами ISMS.

– **Q.8/17** – Телебиометрия

Основой данного Вопроса является ведущаяся работа, которая относится к персональной идентификации и аутентификации с использованием телебиометрии, проводимая в тесном сотрудничестве с другими ОРС, разрабатывающими соответствующие стандарты. В частности, Вопрос концентрируется на том, каким образом улучшить идентификацию и аутентификацию пользователей путем использования безопасных и защищенных телебиометрических методов и как могут быть выделены проблемы, касающиеся технологии биометрической аутентификации в электросвязи.

– **Q.9/17** – Безопасные услуги связи

Из-за некоторых конкретных характеристик подвижной связи (например, передачи по эфиру, ограниченных вычислительной мощности и размера памяти небольших устройств подвижной связи) обеспечение безопасности является чрезвычайно сложной задачей, заслуживающей особого внимания и проведения исследования. В данном Вопросе рассматривается, каким образом могут быть выявлены и определены безопасные услуги подвижной связи или услуги, связанные с использованием веб-сети, каким образом можно выявить угрозы в отношении услуг связи и как обращаться с ними, и каким образом можно сохранить возможность безопасного присоединения служб связи.

– **Q.17/17** – Противодействие спаму с помощью технических средств

Данный Вопрос сконцентрирован на технических требованиях, структурах, руководящих принципах и новых технологиях противодействия спаму. Частью работы, проводимой в рамках этого Вопроса, является создание набора Рекомендаций по противодействию спаму в электронной почте и мультимедийных приложениях с учетом необходимости осуществления совместной работы с другими исследовательскими комиссиями МСЭ-Т и сотрудничества с другими ОРС.

WP 3/17 Языки и программное обеспечение электросвязи

– **Q.10/17** – Абстрактная (ASN.1) и другие языки данных

Данный Вопрос имеет целью ведение и совершенствование ASN.1 и ее правил кодирования, включая DER (отличительные правила кодирования), которые используются при создании цифровых сертификатов или цифровых подписей X.509. Нотация ASN.1 является важной частью представления информации в такой форме, чтобы она могла быть надежно зашифрована/расшифрована и подписана/проверена. В рамках данного Вопроса продолжается совершенствование нотации ASN.1 для удовлетворения изменяющихся требований в современных условиях связи.

ИК19	Сети подвижной электросвязи *Ведущая исследовательская комиссия по сетям подвижной электросвязи и по вопросам мобильности*.
Отвечает за проведение исследований, относящихся к сетевым аспектам сетей подвижной электросвязи, включая систему международной подвижной связи 2000 (IMT-2000) и последующие системы, беспроводный интернет, конвергенцию сетей подвижной и фиксированной связи, управление мобильностью, функции подвижной мультимедийной связи, межсетевую организацию, взаимодействие и усовершенствование существующих Рекомендаций МСЭ-Т по IMT-2000.	
Вопросы, относящиеся к обеспечению безопасности:	
– **Q.1/19** – Требования к возможностям обслуживания и к сети и архитектура сети	
– **Q.3/19** – Определение существующих и развивающихся систем IMT-2000 (Q.1741.1, Q.1741.2, Q.1741.3, Q.1742.1, Q.1742.2, Q.1742.3)	
– **Q.5/19** – Конвергенция развивающихся сетей IMT-2000 с развивающимися сетями фиксированной связи	

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.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

Безопасность управления сетью

M.3010 – Принципы построения сети управления электросвязью

M.3016.x – Безопасность СУЭ (Рекомендация в нескольких частях)

M.3210.1 – Управление безопасностью для категории IMT2000 – Требования

M.3320 – Требования к интерфейсу X

M.3400 – Функции управления СУЭ

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

Безопасность в электросвязи

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

X.1051 – Система управления информационной безопасностью – Требования к электросвязи (ISMS-T)

X.1081 – Телебиометрическая мультимодальная модель – Структура для спецификации аспектов безопасности и защищенности в телебиометрике

X.1121 – Структура технологий безопасности для подвижной передачи данных от конца до конца

X.1122 – Руководящие указания по созданию безопасных подвижных систем на основе инфраструктуры открытого ключа (PKI)

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

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.x – Безопасность H.323 (Рекомендация в нескольких частях)

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

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

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

Системы обработки сообщений (MHS)

X.400/F.400 – Обзор систем и служб обработки сообщений

X.402 – Общая архитектура

X.411 – Информационная технология – Системы обработки сообщений (MHS) – Система передачи сообщений: Определение абстрактных услуг и процедуры

X.413 – Накопитель сообщений: определение абстрактной системы

X.419 – Информационные технологии – Системы обработки сообщений (MHS): спецификации протоколов

X.420 – Информационные технологии – Системы обработки сообщений (MHS) – Система межперсональных сообщений

X.435 – Система передачи сообщений на основе электронного обмена данными

X.440 – Системы обработки сообщений: система передачи голосовых сообщений

Рекомендации МСЭ-Т доступны через веб-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, кибербезопасность, безопасность домашних сетей, безопасность СПП, борьба со спамом, электросвязь в чрезвычайных ситуациях

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

Отпечатано в Швейцарии
Женева, 2006 г.