МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т X.805

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(10/2003)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ И ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ

Безопасность

Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами

Рекомендация МСЭ-Т X.805

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ И ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	
Службы и услуги	X.1–X.19
Интерфейсы	X.20–X.49
Передача, сигнализация и коммутация	X.50–X.89
Сетевые аспекты	X.90–X.149
Техническая эксплуатация	X.150–X.179
Административные предписания	X.180–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	
Модель и обозначение	X.200–X.209
Определения служб	X.210–X.219
Спецификации протоколов в режиме с установлением соединений	X.220–X.229
Спецификации протоколов в режиме без установления соединений	X.230–X.239
Проформы PICS	X.240–X.259
Идентификация протоколов	X.260–X.269
Протоколы обеспечения безопасности	X.270–X.279
Управляемые объекты уровня	X.280–X.289
Испытания на соответствие	X.290–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	
Общие положения	X.300–X.349
Спутниковые системы передачи данных	X.350–X.369
IP-сети	X.370–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	
Организация сети	X.600–X.629
Эффективность	X.630–X.639
Качество обслуживания	X.640–X.649
Наименование, адресация и регистрация	X.650–X.679
Абстрактно-синтаксическая нотация 1 (ASN.1)	X.680–X.699
АДМИНИСТРАТИВНОЕ УПРАВЛЕНИЕ ВОС	
Структура и архитектура административного управления системами	X.700–X.709
Служба и протокол связи для административного управления	X.710–X.719
Структуры управляющей информации	X.720–X.729
Функции административного управления и функции ODMA	X.730–X.799
БЕЗОПАСНОСТЬ	**X.800–X.849**
ПРИЛОЖЕНИЯ ВОС	
Фиксация, параллельность и восстановление	X.850–X.859
Обработка транзакций	X.860–X.879
Удаленные операции	X.880–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999

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

Рекомендация МСЭ-Т X.805

Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами

Резюме

В настоящей Рекомендации определяются общие связанные с безопасностью элементы сетевой архитектуры, которые при соответствующем применении могут обеспечить сквозную сетевую защиту.

Источник

Рекомендация МСЭ-Т X.805 была утверждена 17-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) согласно процедуре Рекомендации МСЭ-Т A.8 29 октября 2003 года.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

Соблюдение настоящей Рекомендации носит добровольный характер. Однако Рекомендация может содержать определенные обязательные положения (например, по обеспечению возможности взаимодействия или применимости), и в этом случае соблюдение Рекомендации достигается при выполнении всех этих обязательных положений. Слово "должен" и обозначающие долженствование другие выражения, а также их отрицательные эквиваленты используются для выражения требований. Употребление этих слов не означает, что соблюдение Рекомендации требуется от какой-либо стороны.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое осуществление или реализация данной Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получал извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации данной Рекомендации. Однако те, кто будут применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

Стр.

Введение

Отрасли электросвязи и информационных технологий нуждаются в рентабельных решениях по обеспечению безопасности. Безопасная сеть должна быть защищена от преднамеренных и неумышленных нападений, а также должна быть легко доступна, иметь соответствующую скорость реагирования, надежность, целостность, универсальность и обеспечивать точную информацию для формирования счетов. Защитные возможности программ имеют решающее значение для безопасности сети в целом (включая приложения и службы). Вместе с тем, так как для обеспечения комплексных решений совместно используется большое количество программ, то их способность к взаимодействию или ее отсутствие определяет успех того или иного решения. Защита не должна быть вопросом, касающимся только каждой программы или службы, а должна быть разработана таким способом, который реализует сочетание возможностей защиты для полного сквозного решения по обеспечению безопасности. Для достижения такого решения в среде со многими поставщиками сетевая защита должна быть разработана на основе стандартной архитектуры защиты.

Рекомендация МСЭ-Т X.805

Архитектура защиты для систем, обеспечивающих связь между оконечными устройствами

1 Область применения

В настоящей Рекомендации определяется сетевая архитектура защиты для обеспечения сквозной сетевой защиты. Архитектура может применяться к различным видам сетей, где возникает вопрос сквозной защиты, независимо от основной технологии сети. В данной Рекомендации определяются общие связанные с защитой архитектурные элементы, которые являются необходимыми для обеспечения сквозной защиты. Цель настоящей Рекомендации состоит в том, чтобы служить основой для разработки детальных рекомендаций для сквозной сетевой защиты.

2 Ссылки

Следующие Рекомендации МСЭ-Т и другие документы содержат положения, которые путем ссылки в настоящем тексте составляют положения настоящей Рекомендации. Во время публикации указанные издания были в силе. Все Рекомендации и другие документы могут пересматриваться, и ввиду этого пользователи настоящей Рекомендации призываются изучать возможность применения последнего по времени издания Рекомендаций и других документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в рамках настоящей Рекомендации не придает этому документу самому по себе статус Рекомендации.

– Рекомендация МСЭ-Т X.800 (1991), *Архитектура защиты для взаимосвязи открытых систем для применений МККТТ.*

3 Термины и определения

В настоящей Рекомендации используются следующие термины Рекомендации МСЭ-Т X.800:

- управление доступом;
- доступность;
- аутентификация;
- конфиденциальность;
- целостность данных;
- сохранность информации;
- секретность.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

AAA Аутентификация, авторизация и учет
ASP Поставщик прикладных услуг
ATM Асинхронный режим передачи
DHCP Протокол динамического выбора хост-машины
DNS Служба имен доменов
DoS Отказ в обслуживании
DS-3 Уровень цифровых сигналов 3
FTP Протокол передачи файлов

IP Протокол Интернет

IPSec Протокол защиты IP

OAM&P Эксплуатация, управление, техническое облсуживание и обеспечение

ВОС Взаимодействие открытых систем

КТСОП Коммутируемая телефонная сеть общего пользования

PVC Постоянный виртуальный канал

QoS Качество обслуживания

SIP Протокол инициирования сеанса

SMTP Упрощенный протокол передачи сообщений электронной почты

SNMP Простой протокол управления сетью

SONET Синхронная оптоволоконная сеть связи

SS7 Сигнальная система 7

SSL Безопасный уровень сокета (Протокол кодирования и аутентификации)

VoIP Передача звука посредством IP

VPN Виртуальная частная сеть

5 Архитектура защиты

Архитектура защиты была создана для решения общих вопросов защиты поставщиков услуг, предприятий и потребителей и применяется к беспроводным, оптическим и проводным линиям связи сетей передачи речи, данных и интегрированных сетей. Эта архитектура защиты определяет вопросы защиты для управления, контроля и использования сетевой инфраструктуры, услуг и приложений. Архитектура защиты обеспечивает комплексную, сверху донизу сквозную область сетевой защиты и может применяться к элементам сети, услугам и приложениям, с тем чтобы обнаруживать, прогнозировать и исправлять уязвимость защиты.

Архитектура защиты логически делит сложный набор сквозных сетевых, связанных с защитой характеристик, на отдельные архитектурные компоненты. Такое разделение позволяет применять систематический подход к сквозной защите, который может использоваться как для планирования новых вариантов защиты, так и для оценки защищенности существующих сетей.

Архитектура защиты касается трех существенных вопросов сквозной защиты:

1) Какая защита необходима и от каких угроз?

2) Какие именно типы сетевого оборудования и совокупности средств должны быть защищены?

3) Какие именно типы сетевой активности должны быть защищены?

Эти вопросы относятся к трем компонентам архитектуры: измерения защиты, уровни защиты и плоскости защиты.

Принципы, задаваемые архитектурой защиты, могут применяться к широкому кругу сетей независимо от технологии сети или расположения в стеке протокола.

В следующих разделах подробно описываются элементы архитектуры и их функции относительно главных угроз безопасности.

6 Измерения защиты

Измерения защиты – это комплекс мер защиты, предназначенных для реализации конкретного аспекта сетевой защиты. В настоящей Рекомендации идентифицируется восемь таких комплексов, которые защищают от всех основных угроз. Эти измерения не ограничены сетью, но также распространяются на приложения и информацию конечного пользователя. Кроме того, измерения защиты применяются к поставщикам услуг и к организациям, предлагающим услуги по обеспечению безопасности своим клиентам. Измерения защиты:

1) управление доступом;
2) аутентификация;
3) сохранность информации;
4) конфиденциальность данных;
5) безопасность связи;
6) целостность данных;
7) доступность;
8) секретность.

Должным образом разработанные и осуществленные измерения защиты поддерживают политику защиты, которая определена для конкретной сети, и упрощают выполнение правил, установленных управлением защитой.

6.1 Измерение защиты: управление доступом

Измерение защиты – управление доступом – защищает от неправомочного использования сетевых ресурсов. Управление доступом гарантирует, что только уполномоченному персоналу или устройствам разрешен доступ к элементам сети, хранимой информации, потокам информации, услугам и приложениям. Кроме того, управление доступом на основе ролей (RBAC) обеспечивает различные уровни доступа для гарантии того, чтобы люди и устройства могли получать доступ и совершать операции только с теми элементами сети, с той хранимой информацией и с теми потокам информации, доступ к которым им разрешен.

6.2 Измерение защиты: аутентификация

Измерение защиты – аутентификация – предназначено для удостоверения личностей поддерживающих связь объектов. Аутентификация гарантирует подлинность заявляемой личности объектов, участвующих в связи (например, человека, устройства, услуги или приложения), и обеспечивает уверенность в том, что объект не пытается осуществлять подмену или неправомочно использовать предыдущий сеанс связи.

6.3 Измерение защиты: сохранность информации

Измерение защиты – сохранность информации – обеспечивает средства для предотвращения со стороны индивидуума или объекта отрицания выполнения конкретного действия, связанного с данными, обеспечивая наличие доказательств совершения различных действий, связанных с сетью (таких как доказательство обязательства, намерения или готовности; доказательство происхождения данных, доказательство собственности, доказательство использования ресурса). Гарантируется наличие данных, которые могут быть предоставлены третьей стороне и которые могут использоваться как доказательства того, что некоторое событие или действие имело место.

6.4 Измерение защиты: конфиденциальность данных

Измерение защиты – конфиденциальность данных – защищает данные от неправомочного раскрытия. Конфиденциальность данных гарантирует, что содержание данных не может быть понято объектами, которые не имеют на это права. Шифрование, списки контроля доступа и разрешение доступа к файлам – это методы, которые часто используются для обеспечения конфиденциальности данных.

6.5 Измерение защиты: безопасность связи

Измерение защиты – безопасность связи – гарантирует, что информация передается только между уполномоченными оконечными точками (информация не изменяет направления и не перехватывается при передаче между этими оконечными точками).

6.6 Измерение защиты: целостность данных

Измерение защиты – целостность данных – гарантирует правильность и точность данных. Данные защищены от несанкционированного изменения, удаления, создания и дублирования, а также обеспечивается обнаружение такой несанкционированной деятельности.

6.7 Измерение защиты: доступность

Направление защиты – доступность – гарантирует отсутствие какого-либо ограничения на санкционированный доступ к элементам сети, хранимой информации, потокам данных, к услугам и приложениям из-за событий, влияющих на сеть. Варианты восстановления после аварий включены в эту категорию.

6.8 Измерение защиты: секретность

Измерение защиты – секретность – обеспечивает защиту информации, которая могла бы быть получена, исходя из наблюдения сетевой деятельности. Примеры такой информации – Web-сайты, которые пользователь посетил, географическое расположение пользователя, IP-адреса и имена DNS в сети поставщика услуг.

7 Уровни защиты

Для обеспечения сквозной защиты измерения защиты, описанные в разделе 6, должны применяться к иерархии сетевого оборудования и групп средств, которые определяются как уровни защиты. В настоящей Рекомендации определяются три уровня защиты:

– уровень защиты инфраструктуры;

– уровень защиты услуг; и

– уровень защиты приложений.

Эти уровни в комплексе обеспечивают сетевые решения.

Уровни защиты – это ряд факторов, способствующих обеспечению сетевой защиты: уровень инфраструктуры делает возможным применение уровня услуг, а уровень услуг делает возможным применение уровня приложений. Архитектура защиты учитывает тот факт, что каждый уровень имеет различные точки уязвимости защиты, и предлагает гибкость в отражении потенциальных угроз наиболее приемлемым способом для конкретного уровня защиты.

Необходимо отметить, что уровни защиты (как определено выше) представляют отдельную категорию, и все три уровня защиты могут применяться к каждому уровню эталонной модели ВОС.

Уровни защиты определяют, где защита должна быть использована в программах и решениях, обеспечивая последовательную структуру сетевой защиты. Например, сначала уязвимость защиты рассматривается на уровне инфраструктуры, затем на уровне услуг и, наконец, уязвимость защиты рассматривается на уровне приложений. На Рисунке 1 показано как измерения защиты применяются к уровням защиты для уменьшения уязвимости, которая существует в каждом уровне, и таким образом смягчают последствия атак на защиту.

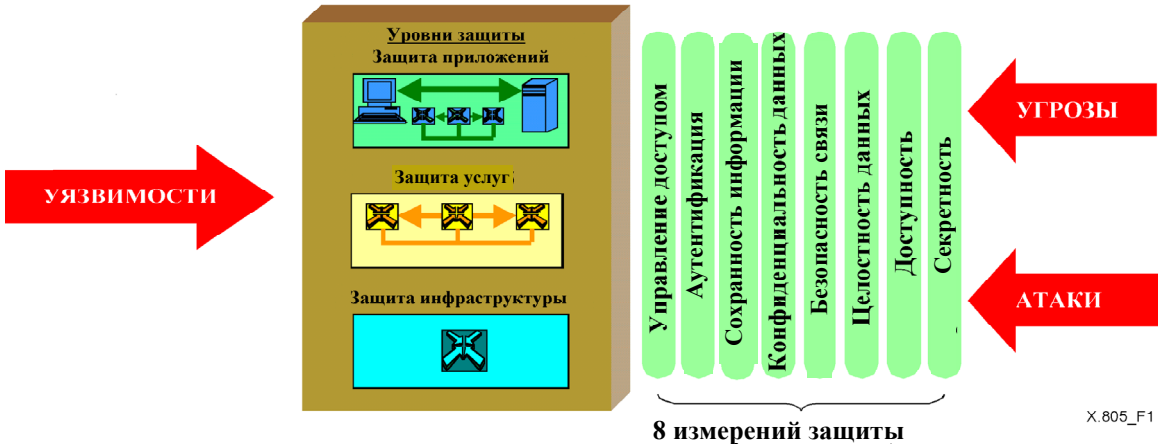

Рисунок 1/X.805 – Применение измерений защиты к уровням защиты

7.1 Уровень защиты инфраструктуры

Уровень защиты инфраструктуры состоит из сетевых средств передачи, а также из отдельных элементов сети, защищенных по измерениям защиты. Уровень инфраструктуры включает основные стандартные блоки сетей, их услуги и приложения. Примерами компонентов, которые принадлежат к уровню инфраструктуры, могут служить отдельные маршрутизаторы, коммутаторы и серверы, а также линии связи между отдельными маршрутизаторами, коммутаторами и серверами.

7.2 Уровень защиты услуг

Уровень защиты услуг определяет защиту услуг, которые поставщики услуг предоставляют своим клиентам. К таким услугам относятся как базовые транспорт и подключение к необходимым для обслуживания ресурсам, например необходимым для обеспечения доступа к Интернет (службы AAA, службы динамической конфигурации хостов, службы имен доменов и т. д.), так и дополнительные услуги, такие как услуги бесплатной телефонии, QoS, VPN, службы позиционирования, мгновенной передачи сообщений и т. д. Уровень защиты услуг используется для защиты поставщиков услуг и их клиентов, которые являются потенциальными объектами угроз защите. Например, нападающие могут пытаться лишить поставщика услуг возможности предоставлять услуги или прервать обслуживание отдельного клиента поставщика услуг (например, корпорации).

7.3 Уровень защиты приложений

На уровне защиты приложений обеспечивается главным образом защита сетевых приложений, к которым имеют доступ клиенты поставщика услуг. Работа таких приложений обеспечивается сетевыми службами и включает основной транспорт файлов (например, FTP) и приложения навигации в сети, основные приложения, такие как работа с директориями, сетевая передача речевых сообщений и электронная почта, а также более сложные приложения, такие как управление взаимодействием с клиентами, электронная торговля/торговля с помощью подвижной связи, профессиональная подготовка на основе сети, видеоконференции и т. д. Сетевые приложения могут предоставляться сторонними поставщиками прикладных услуг (ASP), поставщиками услуг, действующими также в качестве ASP, или организациями, эксплуатирующими их в собственных (или арендованных) центрах данных. На этом уровне имеются четыре потенциальных объекта нападения: пользователь приложений, поставщик приложений, связующее ПО, предоставленное сторонними интеграторами (например, службами хостинга сети), и поставщик услуг.

8 Плоскости защиты

Плоскость защиты – это определенный тип сетевой операции, защищенной измерениями защиты. В настоящей Рекомендации определяется три плоскости защиты для представления трех типов защищенных сетевых операций. Определяются следующие плоскости защиты:

1) плоскость управления;

2) плоскость контроля;

3) плоскость конечного пользователя.

Эти плоскости защиты относятся к конкретным потребностям в защите, связанным с управлением сетью, контролем за сетью или сигнальными операциями, а также операциями конечного пользователя, соответственно.

Сети следует проектировать таким образом, чтобы события в одной плоскости защиты были полностью изолированы от других плоскостей защиты. Например, приток поисков DNS в плоскости конечного пользователя, инициированный запросами конечного пользователя, не должен блокировать интерфейс OAM&P в плоскости управления, который позволит администратору решить данную проблему.

На Рисунке 2 показана архитектура защиты, включающая плоскости защиты. Каждый тип описанных сетевых операций имеет собственные конкретные потребности в области защиты. Концепция плоскостей защиты позволяет дифференцировать конкретные проблемы защиты, связанные с этими операциями, и дает возможность решать их независимо. Рассмотрим, например, службу VoIP, к которой относится уровень защиты услуг. Защита управления службой VoIP (например, подключения пользователей) не должна зависеть от защиты контроля за услугами (например, протоколов типа SIP), а также не должна зависеть от защиты данных конечного пользователя, передаваемых службой (например, речь пользователя).

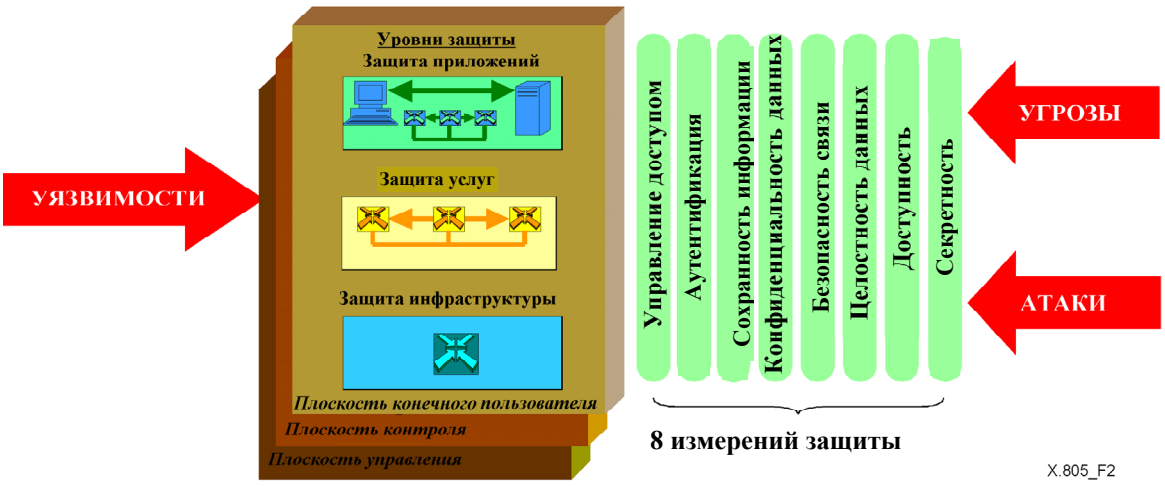

Рисунок 2/X.805 – Плоскости защиты отражают различные типы сетевых операций

8.1 Плоскость защиты управления

К плоскости защиты управления относится защита функций OAM&P элементов сети, средств передачи, систем поддержки (системы поддержки выполнения операций, системы поддержки деловых операций, системы работы с клиентом и т. д.), а также центров данных. Плоскость управления поддерживает функции работы с ошибками, обеспечения производительности, управления, обеспечения и защиты (FCAPS). Следует отметить, что сеть, по которой осуществляется трафик для этих операций, может находиться в полосе или вне полосы пользовательского трафика поставщика услуг.

8.2 Плоскость защиты контроля

К плоскости защиты контроля относится защита операций, которые обеспечивают эффективную доставку информации, услуг и приложений по сети. Обычно используется

передача информации с одного устройства на другое, что позволяет устройствам (например, коммутаторам или маршрутизаторам) определять оптимальный способ направления или переключения трафика через базовую транспортную сеть. Этот тип информации иногда называется управляющей или сигнальной информацией. Сеть, передающая такие типы сообщений, может находиться в полосе или вне полосы пользовательского трафика поставщика услуг. Например, IP-сети передают такую управляющую информацию в полосе, в то время как КТСОП передает свою управляющую информацию в отдельной внеполосной сигнальной сети (сети SS7). Примеры трафика такого типа включают протоколы маршрутизации, DNS, SIP, SS7, Megaco/H.248 и т. д.

8.3 Плоскость защиты конечного пользователя

К плоскости защиты конечного пользователя относится защита доступа клиентов к сети поставщика услуг и ее использования. К этой плоскости также относятся реальные потоки данных конечного пользователя. Конечные пользователи могут использовать сеть, которая только обеспечивает связь, и они могут также использовать ее для служб дополнительных услуг, таких как VPN, или они могут использовать эту сеть для доступа к сетевым приложениям.

9 Угрозы безопасности

Архитектура защиты определяет план и ряд принципов, которые описывают структуру защиты для варианта сквозной защиты. Архитектура определяет, какие проблемы защиты должны быть решены для предотвращения намеренных угроз, а также случайных угроз. Следующие угрозы описаны в Рекомендации МСЭ-Т X.800 (1991), *Архитектура защиты для взаимосвязи открытых систем для применений МККТТ:*

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

Пересечение каждого уровня защиты с каждой плоскостью защиты представляет область защиты, в которой измерения защиты применяются для противодействия угрозам. В Таблице 1 представлено схематическое соотношение измерений защиты применительно к угрозам безопасности. Соотношение идентично для каждой области защиты.

'Да' в ячейке, сформированной пересечением столбцов и строк таблицы, означает, что конкретной угрозе безопасности противостоит соответствующее измерение защиты.

Таблица 1/X.805 – Соотношение измерений защиты и угроз безопасности

Измерение защиты	Угроза безопасности				
	Уничтожение информации или других ресурсов	**Искажение или изменение информации**	**Кража, удаление или потеря информации и других ресурсов**	**Раскрытие информации**	**Прерывание обслужи-вания**
Управление доступом	ДА	ДА	ДА	ДА	
Аутентификация			ДА	ДА	
Сохранность информации	ДА	ДА	ДА	ДА	ДА
Конфиденциальность данных			ДА	ДА	
Безопасность связи			ДА	ДА	
Целостность данных	ДА	ДА			
Доступность	ДА				ДА
Секретность				ДА	

На Рисунке 3 показана архитектура защиты с элементами архитектуры и указанием угроз безопасности, описанных выше. На рисунке представлена концепция защиты сети по измерениям защиты в каждой плоскости защиты каждого уровня защиты, с тем чтобы представить комплексный вариант защиты. Следует отметить, что в зависимости от потребностей защиты данной сети не обязательно реализовывать все элементы архитектуры (т. е. иметь полную систему измерений защиты, уровней защиты и плоскостей защиты).

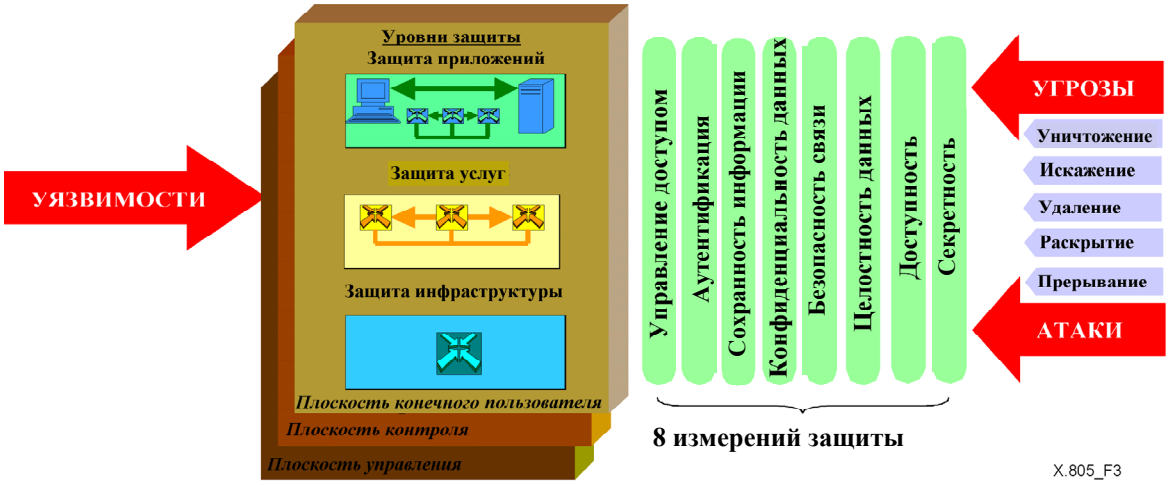

Рисунок 3/X.805 – Архитектура защиты для сквозной сетевой защиты

10 Описание целей, достигаемых применением измерений защиты к уровням защиты

Архитектура защиты может применяться ко всем аспектам и фазам программы защиты, как показано на Рисунке 4. Как явствует из Рисунка 4, программа защиты состоит из стратегий и процедур в дополнение к технологии и проходит через три фазы в течение срока своего действия:

1) фаза определения и планирования;

2) фаза реализации;

3) фаза эксплуатации.

Архитектура защиты может применяться к стратегиям и процедурам защиты, а также к технологии в течение всех трех фаз программы защиты.

Архитектура защиты может определять разработку комплексных определений политики защиты, реакции на происшествия и планов восстановления, а также архитектуры технологии, принимая во внимание каждое измерение защиты на каждом уровне и в каждой плоскости защиты в фазе определения и планирования. Архитектура защиты может также использоваться как основа для оценки защиты, в ходе которой исследовалось бы, как выполнение программы защиты соотносится с измерениями, уровнями и плоскостями защиты, по мере того как разрабатываются стратегии и процедуры и реализуется технология. Когда программа защиты развернута, она должна поддерживаться для сохранения адекватности в постоянно изменяющейся среде защиты. Архитектура защиты может помогать в управлении стратегиями и процедурами защиты, реакцией на происшествия и реализацией планов восстановления, а также в управлении архитектурой технологии, гарантируя, что модификации программы защиты применяются к каждому измерению защиты на каждом уровне и в каждой плоскости защиты.

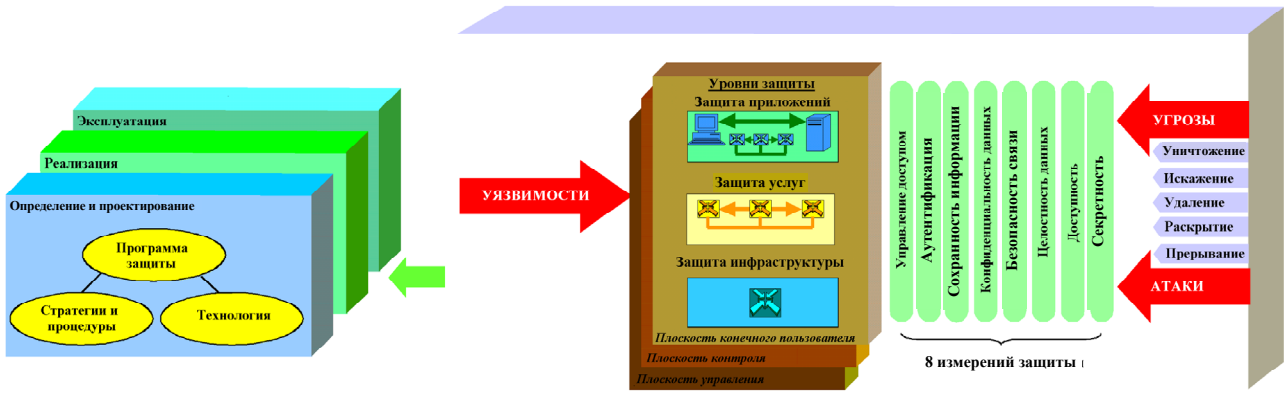

Рисунок 4/X.805 – Применение архитектуры защиты к программам защиты

Кроме того, архитектура защиты может применяться к любому типу сети на любом уровне стека протокола. Например, в IP-сети, которая находится на третьем уровне стека протокола, к уровню инфраструктуры относятся отдельные маршрутизаторы, прямые каналы связи между маршрутизаторами (например, SONET, ATM PVC и т. д.) и серверные платформы, используемые для обеспечения вспомогательных услуг, необходимых IP-сети. К уровню услуг относится непосредственно основная услуга IP (например, возможность подключения к Интернет), вспомогательные услуги IP (например, AAA, DNS, DHCP и т. д.) и расширенные дополнительные услуги, предлагаемых поставщиком услуг (например, VoIP, QoS, VPN и т. д.). Наконец, к уровню приложений относится защита приложений пользователя, доступ к которым обеспечивается по IP-сети (например, электронная почта и т. д.).

Аналогичным образом, для сети ATM, которая находится на втором уровне стека протокола, к уровню инфраструктуры относятся отдельные коммутаторы и прямые каналы связи между коммутаторами (средства передачи, например DS-3). К уровню услуг относятся различные классы транспорта, обеспечиваемого предлагаемой службой ATM (постоянная скорость передачи, переменная скорость передачи в режиме реального времени, переменная скорость передачи информации не в режиме реального времени, имеющаяся скорость передачи и неуказанная скорость передачи). Наконец, к уровню приложений относятся приложения, для доступа к которым конечный пользователь использует сеть ATM, например приложение видеоконференцсвязи.

На Рисунке 5 представлена схема архитектуры защиты в табличной форме и показан методический подход к обеспечению защиты сети. Как можно видеть на рисунке, пересечение уровня защиты с плоскостью защиты представляет единственную перспективу для рассмотрения восьми измерений защиты. Каждый из этих девяти модулей объединяет восемь измерений защиты, которые применяются к конкретному уровню защиты в определенной плоскости защиты. Следует отметить, что измерения защиты различных модулей имеют различные цели и, следовательно, включают различные комплексы мер защиты. Табличная форма представляет собой удобный способ описания целей измерений защиты для каждого модуля.

Рисунок 5/X.805 – Архитектура защиты в табличной форме

10.1 Защита уровня инфраструктуры

10.1.1 Защита плоскости управления уровня инфраструктуры предполагает защиту эксплуатации, управления, технического обслуживания и обеспечения (OAM&P) отдельных элементов сети, линий связи и серверных платформ, из которых состоит сеть. Конфигурация сетевых устройств и линий связи также считается операцией управления. Пример управления инфраструктурой, которое должно быть защищено, – это конфигурация отдельного маршрутизатора или коммутатора персоналом, отвечающим за сетевые операции. В Таблице 2 описаны цели применения измерений защиты к уровню инфраструктуры в плоскости управления.

Таблица 2/X.805 – Применение измерений защиты к уровню инфраструктуры в плоскости управления

Модуль 1: Уровень инфраструктуры, плоскость управления	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченному персоналу или устройствам (например, в случае SNMP – управляемым устройствам) разрешено выполнять административные действия или операции управления на сетевом устройстве или линии связи. Это применимо как к прямому управлению устройством через консольный порт, так и к дистанционному управлению устройством.
Аутентификация	Проверять личность человека или устройства, выполняющего административные действия или операции управления на сетевом устройстве или линии связи. В качестве элемента управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, которые выполняют каждое административное действие или операцию управления на сетевом устройстве или линии связи, и действие, которое было выполнено. Этот отчет может использоваться как подтверждение источника административных или управленческих действий.
Конфиденциальность данных	Защищать информацию о конфигурации сетевого устройства или линии связи от несанкционированного доступа и просмотра. Это применяется к информации о конфигурации, наличествующей в сетевом устройстве или линии связи, к информации о конфигурации, передаваемой на сетевое устройство или линию связи, а также к резервной информации о конфигурации, сохраняемой автономно. Защитить административную информацию об аутентификации (например, идентификацию администратора и пароли) от несанкционированного доступа и просмотра. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности данных.
Безопасность связи	В случае дистанционного управления сетевым устройством или линией связи гарантировать, что управленческая информация передается только между станциями дистанционного управления и устройствами или линиями связи, управление которыми осуществляется. Управленческая информация не изменяет направления и не перехватывается в ходе передачи между этими оконечными точками. Такие же меры принимаются по отношению к административной информации об аутентификации (например, идентификация администратора и пароли).
Целостность данных	Защищать информацию о конфигурации сетевых устройств и линий связи от несанкционированной модификации, удаления, создания и дублирования. Эта защита применяется к информации о конфигурации, содержащейся в сетевом устройстве или линии связи, а также к информации о конфигурации, которая передается транзитом или хранится автономно. Такие же меры принимаются по отношению к административной информации об аутентификации (например, идентификация администратора и пароли).
Доступность	Гарантировать, что уполномоченному персоналу или устройствам не может быть отказано в способности управлять сетевым устройством или линией связи. Это включает защиту от активных нападений, таких как отказ в обслуживании (DoS), а также защиту от пассивных нападений, таких как модификация или удаление административной информации об идентификации (например, идентификация администратора и паролей).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации сетевого устройства или линии связи, не доступна неуполномоченным персоналу или устройствам. Примеры такого типа информации включают IP-адрес сетевого устройства и имя домена DNS. Например, способность идентифицировать сетевое устройство дает целевую информацию атакующим.

10.1.2 Защита в плоскости управления уровня инфраструктуры заключается в защите управленческой или сигнальной информации, которая находится в элементах сети и серверных платформах, из которых состоит сеть, а также в защите получения и передачи управленческой или сигнальной информации сетью, элементами и серверными платформами. Например, таблицы коммутации, находящиеся в сетевых коммутаторах, должны быть защищены от вмешательства или неправомочного раскрытия. Еще в одном примере маршрутизаторы должны быть защищены от приема и распространения фальшивых модификаций маршрутизации и реакции на фальшивые запросы маршрутизации, исходящие от фиктивных маршрутизаторов. В Таблице 3 описаны цели применения измерений защиты к уровню инфраструктуры в плоскости контроля.

Таблица 3/X.805 – Применение измерений защиты к уровню инфраструктуры в плоскости контроля

Модуль 2: Уровень инфраструктуры, плоскость контроля	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченному персоналу и устройствам разрешен доступ к информации об управлении доступом, находящейся в сетевом устройстве (например, таблице маршрутизации) или в автономной памяти. Гарантировать, что сетевое устройство принимает сообщения об управлении только от уполномоченных сетевых устройств (например, корректировку маршрута).
Аутентификация	Проверять личность человека или устройства, читающего или изменяющего информацию об управлении, находящуюся в сетевом устройстве. Проверять личность устройства, посылающего информацию об управлении на сетевое устройство. В качестве элемента управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, которые читали или изменили информацию об управлении в сетевом устройстве или линии связи, а также действие, которое было ими выполнено. Этот отчет может использоваться как подтверждение доступа к информации об управлении или ее изменения. Формировать отчет, идентифицирующий устройство, от которого исходят сообщения об управлении, посылаемые сетевому устройству, а также действие, которое было им выполнено. Этот отчет может использоваться как доказательство того, что устройство явилось источником сообщения об управлении.
Конфиденциальность данных	Защищать информацию об управлении, находящуюся в сетевом устройстве или автономной памяти, от несанкционированного доступа и просмотра. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности информации об управлении, находящейся в сетевом устройстве. Защищать информацию об управлении, предназначенную для сетевого устройства, от несанкционированного доступа и просмотра при передаче по сети.
Безопасность связи	Гарантировать, что информация об управлении, передаваемая по сети (например, корректировки маршрута), передается только от источника информации об управлении до ее желательного адресата. Информация об управлении не изменяет направления и не перехватывается в ходе передачи между этими оконечными точками.
Целостность данных	Защищать информацию об управлении, находящуюся в сетевых устройствах и передаваемую по сети или хранимую автономно, от несанкционированной модификации, удаления, создания и дублирования.
Доступность	Гарантировать, что сетевые устройства всегда доступны для приема информации об управлении из уполномоченных источников. Это включает защиту от преднамеренных нападений, таких как отказ в обслуживании (DoS), а также от случайных происшествий (например, искажения маршрута).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации сетевого устройства или линии связи, не доступна неуполномоченным персоналу или устройствам. Примеры такого типа информации включают IP-адрес сетевого устройства и имя домена DNS. Например, способность идентифицировать сетевые устройства или линии связи дает атакующим целевую информацию.

10.1.3 Защита плоскости конечного пользователя уровня инфраструктуры заключается в защите информации и речевых сигналов пользователя, если они находятся в элементах сети или передаются через них, а также когда они передаются по линиям связи. Сюда также относится защита информации пользователя, находящейся на серверной платформе, как и защита информации пользователя от незаконного перехвата во время передачи по элементам сети или линиям связи. В Таблице 4 описаны цели применения измерений защиты к уровню инфраструктуры в плоскости конечного пользователя.

Таблица 4/X.805 – Применение измерений защиты к уровню инфраструктуры в плоскости конечного пользователя

Модуль 3: Уровень инфраструктуры, плоскость конечного пользователя	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченному персоналу или устройствам разрешен доступ к данным конечного пользователя, которые передаются по элементу сети или линии связи либо находятся в автономных устройствах памяти.
Аутентификация	Проверять личность человека или устройства, стремящегося получить доступ к данным конечного пользователя, которые передаются по элементу сети или линии связи либо находятся в автономных устройствах памяти. В качестве элемента управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий каждого человека или устройство, которые получают доступ к данным конечного пользователя, передаваемым по элементу сети или линии связи либо находящимся в автономных устройствах памяти, и действие, которое было выполнено. Этот отчет должен использоваться как подтверждение доступа к данным конечного пользователя.
Конфиденциальность данных	Защищать данные конечного пользователя, которые передаются по элементу сети или линии связи либо находятся в автономных устройствах памяти, от несанкционированного доступа и просмотра. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности данных конечного пользователя.
Безопасность связи	Гарантировать, что данные конечного пользователя, которые передаются по элементу сети или линии связи, не изменяют направления и не перехватываются без санкционированного доступа (например, законный перехват), при передаче между оконечными точками.
Целостность данных	Защищать данные конечного пользователя, которые передаются по элементу сети или линии связи либо находятся в автономных устройствах, от несанкционированной модификации, удаления, создания или дублирования.
Доступность	Гарантировать, что уполномоченный персонал (включая конечного пользователя) и устройства не могут быть лишены доступа к данным конечного пользователя в автономных устройствах. Сюда относится защита от активных нападений, таких как отказ в обслуживании (DoS), а также защиту от пассивных нападений, таких как модификация или удаление информации об аутентификации (например, идентификация пользователя и его пароли, идентификация администратора и его пароли).
Секретность	Гарантировать, что элементы сети не предоставляют информации, имеющей отношение к сетевой деятельности конечного пользователя (например, географическое местоположение пользователя, посещаемые Web-сайты и т. д.), неуполномоченному персоналу или устройствам.

10.2 Защита уровня услуг

Защита уровня услуг усложняется тем фактом, что услуги могут взаимно усиливаться для удовлетворения требований клиента. Например, чтобы обеспечить услугу VoIP, поставщик услуг должен сначала обеспечить базовую услугу IP с ее необходимыми вспомогательными услугами, такими как AAA, DHCP, DNS и т. д. Поставщику услуг также может быть необходимо обеспечить услугу VPN, чтобы удовлетворить потребности клиента в отношении QoS и безопасности для услуги VoIP. Поэтому рассматриваемая предлагаемая услуга должна быть разбита на составные услуги для обеспечения защиты в целом.

10.2.1 Защита плоскости управления уровня услуг состоит в защите функций OAM&P сетевых служб. Конфигурация сетевых услуг также считается операцией управления. Примером требующего защиты управления услугами является обеспечение уполномоченных пользователей IP-услуги занимающимся эксплуатацией сетей персоналом. В Таблице 5 описаны цели применения измерений защиты к уровню услуг в плоскости управления.

Таблица 5/X.805 – Применение измерений защиты к уровню услуг в плоскости управления

Модуль 4: Уровень служб, плоскость управления	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченному персоналу и устройствам разрешено выполнять административные действия и операции управления сетевой услуги (например, обеспечивать пользователей услуги).
Аутентификация	Проверять личность человека или устройства, стремящегося выполнить административные действия или операции управления сетевой услугой. Как часть управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, которые выполняют каждое административное или управленческое действие сетевой услуги, и действия, которые были выполнены. Этот отчет должен использоваться как подтверждение того, что указанные лицо или устройство выполнили административные или управленческие операции.
Конфиденциальность данных	Защищать информацию о конфигурации сетей услуги и управленческую информацию (например, загружаемые IPSec параметры настройки клиента для услуги VPN) от несанкционированного доступа и просмотра. Это применяется к информации об управлении и конфигурации, находящейся в сетевых устройствах и передаваемой по сети или сохраняемой автономно. Защищать административную и управленческую информацию сетевой услуги (например, идентификацию пользователя и его пароли, идентификацию администратора и его пароли) от несанкционированного доступа и просмотра.
Безопасность связи	В случае дистанционного управления сетевой услугой гарантировать, что административная и управленческая информация передается только от дистанционной станции управления к устройствам, управление которыми производится в рамках сетевой услуги. Административная и управленческая информация не меняет направления и не перехватывается при передаче между этими оконечными точками. Такие же меры принимаются в отношении информации об аутентификации сетевой услуги (например, идентификация пользователя и его пароли, идентификация администратора и его пароли).
Целостность данных	Защищать административную и управленческую информацию сетевых услуг от несанкционированной модификации, удаления, создания или дублирования. Эта защита применяется к административной и управленческой информации, находящейся в сетевых устройствах и передаваемой по сети или сохраняемой в автономных системах. Такие же меры принимаются в отношении информации об аутентификации сетевой услуги (например, идентификация пользователя и его пароли, идентификация администратора и его пароли).
Доступность	Гарантировать, что уполномоченный персонал и устройства не могут быть лишены способности управлять сетевой услугой. Сюда относится защита от активных нападений, таких как отказ в обслуживании (DoS), а также защита от пассивных нападений, таких как модификация или удаление административной информации об аутентификации сетевой услуги (например, идентификация администратора и его пароли).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации административной и управленческой систем сетевой услуги, не доступна неуполномоченному персоналу или устройствам. Примеры такого типа информации включают IP-адрес системы и имя домена DNS. Например, способность идентифицировать административные системы сетевой услуги дает атакующим целевую информацию.

10.2.2 Защита плоскости контроля уровня услуг заключается в защите информации об управлении или сигнальной информации, используемой сетевой услугой. Например, сюда

относятся проблемы защиты протокола SIP, который используется, чтобы инициировать и поддерживать сеансы VoIP. В Таблице 6 описаны цели применения измерений защиты к уровню услуг в плоскости контроля.

Таблица 6/X.805 – Применение измерений защиты к уровню услуг в плоскости управления

Модуль 5: Уровень услуг, плоскость управления	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что информация об управлении, получаемая сетевым устройством для сетевой услуги, исходит из уполномоченного источника (например, сообщение об инициировании сеанса VoIP поступило от уполномоченного пользователя или устройства), до ее принятия. Например, защищать от спуфинга несанкционированным устройством сообщение об инициировании сеанса VoIP.
Аутентификация	Проверять происхождение информации об управлении, посылаемой сетевым устройствам, участвующим в сетевой услуге. В качестве части управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, которые являются источником сообщений об управлении сетевой услугой, получаемых сетевым устройством, которое участвует в сетевой услуге, а также действие, которое было выполнено. Этот отчет может использоваться как подтверждение того, что человек или устройство стали источником сообщения об управлении сетевой услугой.
Конфиденциальность данных	Защищать информацию об управлении сетевой услугой, находящуюся в сетевом устройстве (например, базах данных о сеансах IPSec) и передаваемую по сети или хранимую автономно, от несанкционированного доступа и просмотра. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности данных об управлении сетевой услугой, находящихся в сетевом устройстве.
Безопасность связи	Гарантировать, что информация об управлении сетевой услугой, направляемая по сети (например, сообщения о согласовании ключа IPSec), передается только от источника информации об управлении ее желательному адресату. Информация об управлении сетевой услугой не меняет направления и не перехватывается при передаче между этими оконечными точками.
Целостность данных	Защищать информацию об управлении сетевой услугой, находящуюся в сетевых устройствах и передаваемую по сети или хранимую автономно, от несанкционированной модификации, удаления, создания или дублирования.
Доступность	Гарантировать, что сетевые устройства, участвующие в сетевой услуге, всегда доступны для приема информации об управлении из уполномоченных источников. Сюда относится также защита от активных нападений, таких как отказ в обслуживании (DoS).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации сетевых устройств или линий связи, участвующих в сетевой услуге, не доступна неуполномоченному персоналу или устройствам. К примерам такого типа информации относятся IP-адрес сетевого устройства и имя домена DNS. Например, способность идентифицировать сетевые устройства и линии связи дает атакующим целевую информацию.

10.2.3 Защита плоскости конечного пользователя уровня услуг заключается в защите информации и речевых сигналов пользователя при применении им сетевой услуги. Например, конфиденциальность разговора пользователя в рамках услуги VoIP должна быть защищена. Аналогичным образом услуга DNS должна гарантировать конфиденциальность пользователей услуги. В Таблице 7 описываются цели применения измерений защиты к уровню служб в плоскости конечного пользователя.

Таблица 7/X.805 – Применение измерений защиты к уровню услуг в плоскости конечного пользователя

Модуль 6: Уровень услуг, плоскость конечного пользователя	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченным пользователям и устройствам обеспечены доступ к сетевой услуге и ее использование.
Аутентификация	Проверять личность пользователя или устройства, стремящегося получить доступ к сетевой услуге и ее использовать. В качестве элемента управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий каждого пользователя и устройство, которые получили доступ к сетевой услуге и использовали ее, а также действие, которое было при этом выполнено. Этот отчет должен использоваться как подтверждение доступа к сетевой услуге и ее использования конечным пользователем или устройством.
Конфиденциальность данных	Защищать данные конечного пользователя, которые передаются, обрабатываются или сохраняются сетевой услугой, от несанкционированного доступа и просмотра. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности данных.
Безопасность связи	Гарантировать, что данные конечного пользователя, которые передаются, обрабатываются или сохраняются сетевой услугой, не меняют направления и не перехватываются без санкционированного доступа (например, законный перехват), во время передачи между этими оконечными точками.
Целостность данных	Защищать данные конечного пользователя, которые передаются, обрабатываются или сохраняются сетевой услугой, от несанкционированной модификации, удаления, создания или дублирования.
Доступность	Гарантировать, что уполномоченным конечным пользователям и устройствам не может быть отказано в доступе к сетевой услуге. Сюда относится защита от активных нападений, таких как отказ в обслуживании (DoS), а также защита от пассивных нападений, таких как модификация или удаление информации об аутентификации конечного пользователя (например, идентификация пользователя и пароли).
Секретность	Гарантировать, что сетевая услуга не предоставляет информацию, имеющую отношение к использованию услуги конечным пользователем (например, для услуги VoIP – вызываемые стороны), неуполномоченному персоналу или устройствам.

10.3 Защита уровня приложений

Защита плоскости управления уровня приложений состоит в защите функций OAM&P сетевого приложения. Конфигурация сетевых приложений также считается операцией управления. Для приложения электронной почты пример операции управления, которая нуждается в защите, – это обеспечение и управление почтовыми ящиками пользователей. В Таблице 8 описываются цели применения измерений защиты к уровню приложений в плоскости управления.

Таблица 8/X.805 – Применение измерений защиты к уровню приложений в плоскости управления

Модуль 7: Уровень приложения, плоскость управления	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченному персоналу и устройствам разрешается выполнять административные действия и операции управления сетевым приложением (например, управлять почтовыми ящиками пользователей для приложения электронной почты).
Аутентификация	Проверять личность человека или устройства, стремящегося осуществлять административные действия или операции управления сетевым приложением. Как часть управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, которые выполняют каждое административное действие или операцию по управлением сетевым приложением, а также действие, которое было выполнено. Этот отчет должен использоваться как подтверждение того, что административное действие или операция управления было выполнено, с указанием человека или устройства, которые это совершили.
Конфиденци-альность данных	Защищать все файлы, используемые при создании и выполнении сетевого приложения (например, исходные файлы, объектные файлы, исполняемые файлы, временные файлы и т. д.), а также файлы конфигурации приложения от несанкционированного доступа и просмотра. Это относится к файлам приложений, находящимся в сетевых устройствах и передаваемым по сети или сохраняемым автономно. Защищать административную и управленческую информацию сетевого приложения (например, идентификацию пользователя и его пароли, идентификацию администратора и его пароли) от несанкционированного доступа и просмотра.
Безопасность	В случае дистанционного управления сетевым приложением гарантировать, что административная и управленческая информация передается только от дистанционной удаленной станции управления до устройств, составляющих сетевое приложение. Административная и управленческая информация не меняет направления и не перехватывается при передаче между этими оконечными точками. Те же меры принимаются по отношению к административной и управленческой информации сетевого приложения (например, идентификация пользователя и его пароли, идентификация администратора и его пароли).
Целостность данных	Защищать все файлы, используемые при создании и выполнении сетевого приложения (например, исходные файлы, объектные файлы, исполняемые файлы, временные файлы и т. д.), а также файлы конфигурации приложения от несанкционированной модификации, удаления, создания или дублирования. Эта защита также обеспечивается файлам, находящимся в сетевых устройствах и передаваемым по сети или сохраняемым автономно. Те же меры применяются по отношению к административной и управленческой информации сетевого приложения (например, идентификация пользователя и его пароли, идентификация администратора и его пароли).
Доступность	Гарантировать, что уполномоченному персоналу и устройствам не может быть отказано в способности управлять сетевым приложением. Сюда относится защита от активных нападений, таких как отказ в обслуживании (DoS), а также защита от пассивных нападений, таких как модификация или удаление административной информации об аутентификации сетевого приложения (например, идентификация администратора и его пароли).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации административных или управленческих систем сетевого приложения, не доступна неуполномоченному персоналу и устройствам. Примеры такого типа информации включают IP-адрес сетевого устройства и имя домена DNS. Например, способность идентифицировать административные системы сетевого приложения дает атакующим целевую информацию.

10.3.1 Защита плоскости контроля уровня приложений заключается в защите контрольной или сигнальной информации, используемой сетевыми приложениями. Этот тип информации обычно побуждает приложение выполнять действие в ответ на прием информации. Например, здесь рассматриваются проблемы защиты протоколов SMTP и POP, используемых для управления доставкой электронной почты. В Таблице 9 описываются цели применения измерений защиты к уровню приложений в плоскости контроля.

Таблица 9/X.805 – Применение измерений защиты к уровню приложений в плоскости контроля

Модуль 8: Уровень приложений, плоскость контроля	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать до принятия сообщения, что информация об управлении приложением, полученная сетевым устройством, участвующим в сетевом приложении, происходит из уполномоченного источника (например, сообщение SMTP, запрашивающее передачу электронной почты). Например, защитить от спуфинга со стороны неуполномоченного устройства клиента SMTP.
Аутентификация	Проверять происхождение информации об управлении приложением, которая посылается сетевым устройствам, участвующим в сетевом приложении. Как часть управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, являющиеся источником сообщений об управлении приложением, получаемыми сетевым устройством, участвующим в сетевом приложении, а также действие, которое было выполнено. Этот отчет может использоваться как подтверждение того, что человек или устройство явились источником сообщения об управлении приложением.
Конфиденциальность данных	Защищать информацию об управлении приложением, находящуюся в сетевом устройстве (например, базы данных о сеансах SSL) и передаваемую по сети или сохраняемую автономно, от несанкционированного доступа и просмотра. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности данных об управлении сетевым приложением, которые находятся в сетевом устройстве.
Безопасность	Гарантировать, что информация об управлении приложением, передаваемая по сети (например, сообщения о согласовании SSL), передается только от источника информации об управлении до ее желательного адресата. Информация об управлении приложением не меняет направления и не перехватывается при передаче между этими оконечными точками.
Целостность данных	Защищать информацию об управлении сетевым приложением, находящуюся в сетевых устройствах и передаваемую по сети или сохраняемую автономно, от несанкционированной модификации, удаления, создания или дублирования.
Доступность	Гарантировать, что сетевые устройства, участвующие в сетевых приложениях, всегда доступны для приема информации об управлении из уполномоченных источников. Сюда относится защита от активных нападений, таких как отказ в обслуживании (DoS).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации сетевых устройств или линий связи, участвующих в сетевом приложении, не доступна неуполномоченному персоналу или устройствам. Примеры такого типа информации включают IP-адрес сетевого устройства и имя домена DNS. Например, способность идентифицировать сетевые устройства или линии связи дает атакующим целевую информацию.

10.3.2 Защита плоскости конечного пользователя уровня приложений заключается в защите информации пользователя, передаваемой сетевому приложению. Например, конфиденциальность номера кредитной карты пользователя должна быть защищена приложением электронной торговли. В Таблице 10 описываются цели применения измерений защиты к уровню приложений в плоскости конечного пользователя.

Таблица 10/X.805 – Применение измерений защиты к уровню приложений в плоскости конечного пользователя

Модуль 9: Уровень приложений, плоскость конечного пользователя	
Измерение защиты	**Цели защиты**
Управление доступом	Гарантировать, что только уполномоченным пользователям и устройствам разрешен доступ к сетевому приложению и его использование.
Аутентификация	Проверять личность пользователя или устройства, стремящегося получить доступ к сетевому приложению и использовать его. Как часть управления доступом могут потребоваться методы аутентификации.
Сохранность информации	Формировать отчет, идентифицирующий каждого пользователя и устройство, которые получили доступ к сетевому приложению и использовали его, а также действие, которое было выполнено. Этот отчет должен использоваться как подтверждение доступа к сетевому приложению и его использования конечным пользователем или устройством.
Конфиденци-альность данных	Защищать данные конечного пользователя (например, номер кредитной карты пользователя), которые передаются, обрабатываются или сохраняются сетевым приложением, от несанкционированного доступа и просмотра. Те же меры принимаются по отношению к данным пользователя при передаче их от пользователя сетевому приложению. Методы, используемые для управления доступом, могут способствовать обеспечению конфиденциальности данных конечного пользователя.
Безопасность	Гарантировать, что данные конечного пользователя, которые передаются, обрабатываются или сохраняются сетевым приложением, не меняют направления и не перехватываются без санкционированного доступа (например, перехвата) при передаче между этими оконечными точками. Те же меры принимаются по отношению к информации пользователя при передаче ее от пользователя сетевому приложению.
Целостность данных	Защищать данные конечного пользователя, которые передаются, обрабатываются или сохраняются сетевым приложением, от несанкционированной модификации, удаления, создания или дублирования. Те же меры принимаются по отношению к информации пользователя при передаче ее от пользователя сетевому приложению.
Доступность	Гарантировать, что уполномоченные конечные пользователи и устройства не могут быть лишены доступа к сетевому приложению. Сюда относится защита от активных нападений, таких как отказ в обслуживании (DoS), а также защита от пассивных нападений, таких как модификация или удаление информации об аутентификации конечного пользователя (например, идентификация пользователя и его пароли).
Секретность	Гарантировать, что сетевое приложение не предоставляет информацию, имеющую отношение к применению приложения конечным пользователем (например, посещенные Web-сайты), неуполномоченному персоналу и устройствам. Например, допустимо раскрытие такого типа информации только для персонала правоохранительных органов, имеющего ордер на обыск.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2004 г.