МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т M.3016.3

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2005)

СЕРИЯ M: УПРАВЛЕНИЕ ЭЛЕКТРОСВЯЗЬЮ, ВКЛЮЧАЯ СУЭ И ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ СЕТЕЙ

Сеть управления электросвязью

Безопасность для плоскости административного управления: Механизм безопасности

Рекомендация МСЭ-Т M.3016.3

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ M

УПРАВЛЕНИЕ ЭЛЕКТРОСВЯЗЬЮ, ВКЛЮЧАЯ СУЭ И ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ СЕТЕЙ

Введение и общие принципы технической эксплуатации и организации технического обслуживания	M.10–M.299
Международные системы передачи	M.300–M.559
Международные телефонные каналы	M.560–M.759
Системы сигнализации по общему каналу	M.760–M.799
Международные системы телеграфной и фототелеграфной передачи	M.800–M.899
Международные арендованные первичные и вторичные групповые тракты	M.900–M.999
Международные арендованные каналы	M.1000–M.1099
Системы и службы подвижной электросвязи	M.1100–M.1199
Международная телефонная сеть общего пользования	M.1200–M.1299
Международные системы передачи данных	M.1300–M.1399
Обозначения и обмен информацией	M.1400–M.1999
Международная сеть транспортировки сообщений	M.2000–M.2999
Сеть управления электросвязью	**M.3000–M.3599**
Цифровые сети с интеграцией служб	M.3600–M.3999
Системы сигнализации по общему каналу	M.4000–M.4999

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

Рекомендация МСЭ-Т M.3016.3

Безопасность для плоскости административного управления: Механизм безопасности

Резюме

В настоящей Рекомендации определены механизмы обеспечения безопасности для плоскости административного управления в сети управления электросвязью. Особое внимание в ней обращается на аспект безопасности плоскости административного управления для сетевых элементов (NE) и систем управления (MS), которые являются частью инфраструктуры электросвязи.

Источник

Рекомендация МСЭ-Т M.3016.3 утверждена 13 апреля 2005 года 4-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (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 положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соответствие данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой 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 получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет 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

Введение

Электросвязь – это крайне важная инфраструктура глобальной связи и экономики. Существенным является обеспечение надлежащей безопасности для функций административного управления этой инфраструктурой. Существует много стандартов обеспечения безопасности управления сетью электросвязи. Однако согласованность их низка, а различное оборудование электросвязи и компоненты программного обеспечения несовместимы между собой. Настоящая Рекомендация определяет механизмы обеспечения безопасности, с тем чтобы создать для поставщиков оборудования, организаций и поставщиков услуг возможность реализации безопасной инфраструктуры управления электросвязью. Рассматриваемый набор механизмов безопасности соответствует современному представлению о состоянии техники, однако технологии будут развиваться, и условия будут меняться. Для успешного выполнения поставленных задач данная Рекомендация должна совершенствоваться по мере изменения условий. Настоящая Рекомендация предназначена служить в качестве базовой. Для выполнения своих конкретных потребностей поставщики услуг могут включать дополнительные механизмы безопасности сверх рассмотренных в данной Рекомендации.

Настоящая Рекомендация является частью серии Рекомендаций МСЭ-Т M.3016.x, которые разработаны в качестве руководящих указаний и с целью выработки рекомендаций по обеспечению безопасности для плоскости административного управления разрабатываемых сетей:

Рек. МСЭ-Т M.3016.0 – *Безопасность для плоскости административного управления*: *Обзор.*

Рек. МСЭ-Т M.3016.1 – *Безопасность для плоскости административного управления*: *Требования по безопасности.*

Рек. МСЭ-Т M.3016.2 – *Безопасность для плоскости административного управления*: *Услуги по обеспечению безопасности.*

Рек. МСЭ-Т M.3016.3 – *Безопасность для плоскости административного управления: Механизм безопасности.*

Рек. МСЭ-Т M.3016.4 – *Безопасность для уровня управления*: *проформа структуры.*

Рекомендация МСЭ-Т M.3016.3

Безопасность для плоскости административного управления: Механизм безопасности

1 Область применения

Рекомендации МСЭ-Т M.3016.1–M.3016.3 задают набор требований, услуг и механизмов для обеспечения надлежащей безопасности функций управления, необходимых для поддержки инфраструктуры электросвязи. Так как различным администрациям и организациям требуется поддержка разных уровней безопасности, в Рекомендациях МСЭ-Т M.3016.1–M.3016.3 не указывается, являются ли требование, услуга или механизм обязательными или необязательными.

Настоящая Рекомендация определяет механизмы безопасности для плоскости административного управления электросвязью. В ней особое внимание обращается на аспект безопасности плоскости административного управления для сетевых элементов (NE) и систем управления (MS), которые являются частью инфраструктуры электросвязи.

Настоящая Рекомендация является обобщенной по своему характеру и не определяет требований или не рассматривает требования для конкретного интерфейса сети управления электросвязью (СУЭ).

Форма, определенная в Рекомендации МСЭ-Т M.3016.4, служит для содействия организациям, администрациям и другим национальным/международным организациям при указании обязательной и необязательной поддержки требований, а также при определении диапазонов значений, конкретных значений и т. д. для помощи в реализации их политики обеспечения безопасности.

2 Ссылки

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

– ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the Automatically Switched Optical Network (ASON)*, plus Amendment 2 (2005).

– ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

– Рекомендация МСЭ-Т M.3016.0 (2005 г.), *Безопасность для плоскости административного управления*: *Обзор*.

– Рекомендация МСЭ-Т M.3016.2 (2005 г.), *Безопасность для плоскости управления: услуги по обеспечению безопасности.*

– Рекомендация МСЭ-Т M.3016.3 (2005 г.), *Безопасность для плоскости административного управления*: *Механизм безопасности*.

– Рекомендация МСЭ-Т M.3016.4 (2005 г.), *Безопасность для уровня управления*: *проформа структуры.*

– ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection*: *The Directory: Public-key and attribute certificate frameworks,* plus Corrigendum 1 (2001), Corrigendum 2 (2002), and Corrigendum 3 (2004).

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT Applications*, plus Amendment 1 (1996).

– Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.

3 Определения

В настоящей Рекомендации не определены никакие новые термины.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

CORBA	Обобщенная архитектура посредника объектных запросов
DoS	Отказ в обслуживании
EMS	Система управления элементами
FTP	Протокол пересылки файлов
HTTP	Протокол передачи гипертекста
IETF	Целевая группа по инженерным проблемам сети Интернет
IP	Межсетевой протокол
IPSec	Безопасность межсетевого протокола
ИСО/МЭК	Международная организация по стандартизации/Международная электротехническая комиссия
МСЭ-Т	Международный союз электросвязи – Сектор стандартизации электросвязи
MS	Система управления; любая EMS, NMS или OSS[1]
NE	Сетевой элемент
NE/MS	NE или MS
NMS	Система управления сетью
NTP	Протокол сетевого времени
NTPv3	Протокол сетевого времени (NTP), версия 3
OAM&P	Эксплуатация, управление, техническое обслуживание и обеспечение
OS	Операционная система
OSS	Система эксплуатационной поддержки
RFC	Запрос для комментариев
SAML	Язык разметки положений безопасности
SNMP	Простой сетевой протокол управления
SNMPv3	Простой сетевой протокол управления, версия 3
SOAP	Простой протокол доступа к объекту
SSH	Безопасная оболочка
SSL	Уровень защищенных гнезд

[1] В общем случае OSS могут использоваться в том же контексте, что и MS, на любом уровне иерархии сети управления электросвязью.

TCP	Протокол управления передачей
TLS	Безопасность транспортного уровня
СУЭ	Сеть управления электросвязью
XML	Расширяемый язык разметки текста

5 Условные обозначения

Для идентификации различных требований, услуг и механизмов в Рекомендациях МСЭ-Т M.3016.1, M.3016.2 и M.3016.3 используется описатель. Описатель содержит одну из следующих трехбуквенных меток, за которыми следует число:

– REQ для требования;

– SER для услуги;

– MEC для механизма.

6 Механизмы безопасности

В данном пункте описываются конкретные механизмы безопасности для эксплуатации, управления, технического обслуживания и обеспечения (OAM&P) и для системы эксплуатационной поддержки (OSS), как они, в частности, применяются в целях обеспечения безопасности плоскости административного управления для инфраструктуры, услуг и приложений.

Приведенная ниже таблица 1 воспроизведена из Рекомендации МСЭ-Т M.3016.0 (таблица 4 в Рекомендации МСЭ-Т M.3016.0). В этой таблице приведен обзор взаимосвязи между требованиями по безопасности и услугами безопасности, и она используется в качестве основы для разработки других Рекомендаций в данной серии. Например, в Рекомендации МСЭ-Т M.3016.1 обсуждаются функциональные требования по безопасности, в Рекомендации МСЭ-Т M.3016.2 – услуги безопасности, а в настоящей Рекомендации (Рекомендация МСЭ-Т M.3016.3) – конкретные механизмы безопасности, соответствующие услугам безопасности.

В данном пункте определены только услуги безопасности, относящиеся к стандартным решениям; другие возможные услуги (например, обнаружение отказа в обслуживании) опущены.

Таблица 1/M.3016.3 – Соответствие требований по безопасности и услуг безопасности

Функциональное требование по безопасности	Услуга безопасности
Проверка идентичности	аутентификация пользователя аутентификация равноправного объекта аутентификация источника данных
Управляемый доступ и санкционирование	управление доступом
Защита конфиденциальности – сохраняемые данные	управление доступом конфиденциальность
Защита конфиденциальности – передаваемые данные	конфиденциальность
Защита целостности данных – сохраняемые данные	управление доступом
Защита целостности данных – передаваемые данные	целостность
Возможность ведения учета	невозможность отказа от участия
Регистрация действий	данные проверки
Отчеты о нарушениях безопасности	аварийная сигнализация о нарушениях безопасности
Проверка безопасности	данные проверки
Защита DCN	контроль пакетов

В приведенной ниже таблице 2 показана структура данного пункта:

Таблица 2/M.3016.3 – Структура данного пункта

Пункт	Содержание
6.1	Обсуждаются механизмы безопасности аутентификации, включая аутентификацию пользователя, аутентификацию равноправного объекта.
6.2	Обсуждается аутентификация источника данных.
6.3	Обсуждаются механизмы безопасности управления доступом.
6.4	Обсуждаются механизмы безопасности конфиденциальности данных.
6.5	Обсуждаются механизмы безопасности целостности данных.
6.6	Обсуждаются механизмы безопасности данных проверки.

6.1 Аутентификация пользователя

Аутентификация пользователя – это акт проверки заявленной идентичности личности. Аутентификация пользователя может основываться на механизмах безопасности, которые включают:

– Идентификатор (ID) пользователя и комбинацию паролей (из подходящих сложных паролей), где пароль может быть разовым паролем (например, SecureID).

– Многофакторная аутентификация.

– Аутентификация с разовым предъявлением пароля.

В данном пункте обсуждаются механизмы безопасности аутентификации пользователя.

6.1.1 Аутентификация по ID пользователя и паролям

Для аутентификации пользователя могут использоваться ID пользователя и статические пароли. Аутентификация пользователя включает в себя соответствующую проверку идентичности законного пользователя системы и предотвращение маскировки незаконных пользователей-злоумышленников. При надлежащей аутентификации можно прослеживать действия и использовать управление доступом для ограничения пользователей заранее санкционированными действиями или ролями, как это обсуждается в п. 6.2.

Аутентификация по ID пользователя и паролю включает в себя назначение каждому пользователю уникального ID пользователя, а затем назначение подходящего сложного секретного пароля, который используется для проверки идентичности в комбинации с ID пользователя.

Пароли должны содержать достаточное число знаков и других случайных показателей для предотвращения раскрытия лицами или посредством машинных автоматизированных методов. Примеры характеристик сложных паролей могут включать приведенные ниже требования:

MEC 1: Может потребоваться, чтобы пароли имели длину, равную минимальному числу знаков (например, восемь знаков).

MEC 2: Может запрещаться использование в паролях некоторых знаков.

MEC 2a: Может запрещаться повторение или реверсирование в паролях соответствующего ID пользователя.

MEC 2b: Может запрещаться использование в любом месте внутри пароля набора упорядоченных последовательностей знаков (например, слов из словаря или названий продуктов).

MEC 3: Может потребоваться, чтобы пароли содержали не более заданного числа одних и тех же знаков, используемых последовательно.

MEC 4: Может потребоваться, чтобы пароли содержали как минимум определенное число знаков алфавита в нижнем и/или верхнем регистрах.

MEC 5: Может потребоваться, чтобы пароли содержали как минимум определенное число цифровых знаков.

MEC 6: Может потребоваться, чтобы пароли содержали как минимум определенное число специальных знаков.

Для обеспечения безопасной системы аутентификации также очень важно администрирование паролями. Могут быть желательны, например следующие возможности системного администрирования паролями:

MEC 7: Система администрирования паролями может потребовать ввода старого пароля для предотвращения изменения другим пользователем зарегистрированного пароля пользователя без ведома его владельца.

MEC 8: Системой может выполняться автоматическая проверка для обеспечения того, чтобы каждый новый пароль регистрации отличался от предыдущего пароля. (Так как обычно пароли сохраняются посредством одностороннего шифрования, ввод старого пароля может также потребоваться, чтобы позволить системе определять степень различия старого и нового паролей[2].)

MEC 9: Для предотвращения повторного использования паролей системой может вестись перечень использованных паролей.

MEC 10: Система может потребовать изменения паролей через определенные интервалы времени.

MEC 11: После некоторого числа попыток ввода недействительного пароля система может запрещать последующие попытки на заданный период времени (например, 60 минут) или включать блокировку пользователей. Заблокированным пользователям может потребоваться обращение к персоналу администрирования безопасностью для выяснения условий блокировки.

6.1.2 Многофакторная аутентификация

Многофакторная аутентификация относится к процедурам аутентификации, для которых требуются два или более различных типов информации или факторов для проверки идентичности при аутентификации пользователя. Потребность в нескольких факторах повышает безопасность системы аутентификации за счет отказа от использования только одного фактора, который можно проще раскрыть.

Факторы аутентификации, используемые обычно в системах многофакторной аутентификации, представляют собой:

Что-либо, что пользователь **знает**:	например, знание секретного пароля или подходящей фразы.
Что-либо, что пользователь **имеет**:	например, жетон, смарт-карта, генератор разового пароля.
Что-либо, что **является признаком** пользователя:	например, отпечаток пальца или другой биометрический показатель.

Общеизвестным механизмом многофакторной аутентификации является двухфакторная аутентификация, при которой для аутентификации требуются два удостоверяющих признака. Типичным примером двухфакторной аутентификации является банковская карточная система, в которой пользователь должен владеть карточкой, а также знать секретный PIN-код, связанный с карточкой.

MEC 12: Многофакторная аутентификация с заданным числом факторов.

6.1.3 Аутентификация пользователя в случае разового предъявления пароля

Аутентификация пользователя может поддерживать методы безопасного разового предъявления пароля и инфраструктуры открытых ключей сертификатов X.509. При безопасном разовом предъявлении пароля протокол все же запрашивает у объекта(ов) удостоверяющие признаки (например, имя пользователя и пароль); пользователь может не вводить удостоверяющие признаки, так как они могут быть безопасно сохранены каким-либо способом (например, посредством технологии "Керберос"). Методы безопасного разового предъявления пароля используются с целью исключения для пользователя необходимости несколько раз выполнять процедуру аутентификации в системе, что может быть неудобно.

MEC 13: Аутентификация в случае разового предъявлением пароля.

6.2 Аутентификация равноправного объекта и источника данных

Механизмы аутентификации равноправного объекта используются для проверки заявленной идентичности между равноправными системами. Механизмы безопасности аутентификации источника данных используются для обеспечения того, чтобы сообщения принимались от системы, которая заявила,

---

[2] В качестве исключения для одностороннего шифрования для паролей могут использоваться пароли симметричного шифрования, которые необходимо дешифровать для внутреннего, временного использования в защищенной связи от системы к системе или при разовом предъявлении пароля.

что она отправила их. Аутентификация равноправного объекта и аутентификация источника данных тесно взаимосвязаны и могут базироваться на механизмах безопасности, которые включают:

– Механизмы криптографической аутентификации.

– Механизмы аутентификации защищенного маршрута.

Эти механизмы безопасности аутентификации обсуждаются в нижеследующем пункте.

6.2.1 Криптографическая аутентификация

Механизмы криптографической аутентификации обеспечивают аутентификацию во время передачи данных между системами (например, от системы к системе, от приложения к приложению) и являются основой для организации частной связи с полным сохранением целостности данных. Во время передачи данных криптографическая аутентификация передающего объекта позволяет получателю сообщения аутентифицировать идентичность отправителя (аутентификация равноправного объекта) и удостовериться в источнике сообщения (аутентификация источника данных). В защищенном канале связи аутентификация равноправного объекта и источника данных может быть основана на криптографической информации, связанной с каждым сообщением, для привязки идентичности передающего объекта к сообщению. Получатель проверяет криптографическую информацию, поставляемую с сообщением, для подтверждения точной идентичности передающего объекта.

Криптографические методы, которые могут использоваться для аутентификации равноправного объекта и источника данных, включают шифрование с открытым ключом, шифрование с симметричным ключом, цифровые подписи и методы цифрового хеширования[3]. Криптографическая аутентификация может быть односторонней, когда аутентифицируется только один конец разговора, или двусторонней, когда аутентифицируются оба конца. Двусторонняя аутентификация является более защищенной и может использоваться для содействия предотвращению активных атак.

MEC 14: Аутентификация равноправного объекта и источника данных на основе шифрования с открытым ключом.

MEC 15: Аутентификация равноправного объекта и источника данных на основе шифрования с симметричным ключом.

MEC 16: Аутентификация равноправного объекта и источника данных на основе цифровых подписей.

MEC 17: Аутентификация равноправного объекта и источника данных на основе методов цифрового хеширования.

MEC 18: Двусторонняя криптографическая аутентификация.

6.2.2 Аутентификация пользователя достоверного маршрута

Аутентификация достоверного маршрута – это механизм безопасности, при котором защита любых взаимодействий по аутентификации между двумя системами обеспечивается на достоверном маршруте связи. Этот механизм может быть активизирован только системой и не может имитироваться. Достоверный маршрут может быть либо выделенным физическим маршрутом (т. е. терминал непосредственно подсоединен к системе), либо шифрованным маршрутом, который реализует целостность и защиту от повторного воспроизведения (например, виртуальная частная сеть IPsec, туннель уровня защищенных гнезд/безопасности транспортного уровня (SSL/TLS) или безопасная оболочка (SSH))[4]. Что касается обсуждения протоколов безопасности IPsec, SSL/TLS и SSH, см. Дополнение I.

MEC 19: Аутентификация равноправного объекта и источника данных на основе достоверного маршрута.

6.3 Управление доступом

Сеть СУЭ может предоставлять возможности для обеспечения предотвращения доступа действующих объектов к информации или ресурсам, доступ к которым не санкционирован для этих объектов. Механизмы безопасности управления доступом обеспечивают возможность управления ресурсами безопасности системы только санкционированными пользователями.

---

[3] American National Standards Institute T1.243-1995, *Operations, Administration, Maintenance*.

[4] Адаптировано из Документа National Computer Security Centre, NCSC-TG-004-88, *Glossary of Computer Security Terms*, October 1998 (доступно по адресу: http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

Механизмы безопасности управления доступом могут обеспечиваться централизованной системой, часто в сочетании с системой аутентификации. Например, централизованный сервер системы удаленного доступа пользователей по телефонным линиям (Remote Access Dial-In User System, RADIUS) может использоваться в сочетании с базой данных облегченного протокола доступа к каталогам (Lightweight Directory Access Protocol, LDAP) для обеспечения централизованной системы аутентификации и управления доступом.

Механизмы безопасности управления доступом могут иметь некоторые из следующих характеристик:

MEC 20: Все административные действия могут быть связаны с конкретными лицами.

MEC 21: Механизм безопасности управления доступом может поддерживать концепцию "минимальная привилегия" (т. е. лицо должно иметь роль и иметь разрешение на просмотр данных, изменение данных или на инициирование действий по управлению только для тех функций, которые допускаются этой ролью).

MEC 22: По крайней мере для некоторых учетных записей администратора может отсутствовать разрешение на блокировку из-за связанных с паролем действий, таких как сбои или перерывы в регистрации.

MEC 23: Может быть определен ряд ролей администратора, каждая с разным уровнем привилегий в части неотложных действий по управлению безопасностью. Например, системой могут быть определены пять ролей пользователя-администратора. Другой системой могут быть определены три роли пользователя-администратора. В каждом случае могут быть определены роли для разрешения различных привилегий в отношении следующих действий по безопасности:

MEC 23a: Определение и назначение привилегий пользователя.

MEC 23b: Добавление и исключение идентификаторов (ID) пользователя.

MEC 23c: Инициализация и сброс паролей для регистрации.

MEC 23d: Инициализация и изменение криптографических ключей.

MEC 23e: Установление системного срока действия паролей для регистрации.

MEC 23f: Установление системного предела числа неудачных попыток регистрации для каждого ID пользователя.

MEC 23g: Отмена блокировки или изменение значения системного таймера блокировки.

MEC 23h: Установление значения системного таймера неактивности.

MEC 23i: Установление конфигурации регистрации событий и аварийной сигнализации безопасности системы.

MEC 23j: Управление процессами регистрации событий безопасности системы.

MEC 23k: Модернизация программного обеспечения безопасности.

MEC 23l: Завершение любого сеанса пользователя или системы.

MEC 23m: Определение и назначение новых привилегий пользователя и группы на уровне приложения.

MEC 23n: Ведение записи всех запросов доступа к приложению.

MEC 23o: Добавление и исключение пользователей на уровне приложения.

MEC 23p: Контроль всех регистрационных записей безопасности приложения.

MEC 23q: Конфигурирование регистрации и аварийных сигналов безопасности приложения.

MEC 23r: Управление процессами регистрации безопасности приложения.

MEC 23s: Завершение любого сеанса приложения пользователя.

6.4 Конфиденциальность данных

Механизмы безопасности в отношении конфиденциальности данных используются для предотвращения несанкционированного получения передаваемых данных. В этом пункте обсуждаются криптографические механизмы безопасности, служащие для обеспечения конфиденциальности данных.

Конфиденциальность данных базируется на криптографических принципах. Криптография использует специальные алгоритмы, основанные на стандартах, и общедоступные, что делает возможным их тщательное изучение и простую реализацию. Криптографическая "сила" определяется как используемым криптографическим алгоритмом, так и размером используемого ключа (т. е. сила имеет отношение к

количеству времени, необходимому для обратного определения (т. е. нахождения или угадывания) значения(ий) ключа, используемого с конкретным алгоритмом).

Протоколы безопасности (например, IPsec, SSL/TLS, SSH) в типовом варианте обеспечивают аутентификацию источника данных, целостность данных и конфиденциальность данных. (По вопросам обсуждения протоколов безопасности IPsec, SSL/TLS и SSH см. Приложение А.) Расширения безопасности других протоколов, таких как простой сетевой протокол управления, версия 3 (SNMPv3)[5], обобщенная архитектура посредника объектных запросов (CORBA), протокол пограничного шлюза (Border Gateway Protocol) и открытый протокол маршрутизации с выбором кратчайшего пути (Open Shortest Path First) разработаны для обеспечения аутентификации и целостности данных.

Методы, используемые для генерации, хранения, распространения, уничтожения и аннулирования криптографических ключей для обеспечения конфиденциальности данных, имеют первостепенную важность. Кроме того, такие факторы, как длина ключа, выбор ключа и выбор алгоритма, непосредственно влияют на степень безопасности конкретной криптосистемы.

6.4.1 Симметричная конфиденциальность данных

Симметричное шифрование, или шифрование с секретным ключом, относится к криптографической системе, в которой шифровальный и дешифровальный ключи одни и те же. Симметричные криптосистемы требуют проведения начальных мероприятий для отдельных лиц, чтобы они могли совместно использовать уникальный секретный ключ (например, шифровальный ключ). Ключ должен распространяться между отдельными лицами с использованием защищенных средств или генерироваться внутри (например, на основе совместно используемого секретного ключа дерева), поскольку знание шифровального ключа подразумевает знание дешифровального ключа и наоборот.

Механизмы безопасности в отношении конфиденциальности данных могут базироваться на симметричных криптографических алгоритмах, таких как стандарт шифрования данных (Data Encryption Standard, DES), усовершенствованный стандарт шифрования (Advanced Encryption Standard, AES), тройной алгоритм шифрования данных (Triple Data Encryption Algorithm, 3DES) и другие алгоритмы.

DES – 56-битовый симметричный алгоритм шифрования, который используется уже много лет. Из-за короткой длины своего ключа DES допускает возможность раскрытия ключа посредством массовых параллельных вычислений и в данное время считается слабым алгоритмом. Рейтинг DES был снижен Национальным институтом стандартов и технологий США (US National Institute of Standards and Technology, NIST).

Для приложений правительства США NIST выбрал AES для замены DES в качестве стандартного симметричного алгоритма шифрования. Ключи AES имеют длину 128, 192 и 256 битов.

Алгоритм 3DES является фактически алгоритмом DES, который запускается трижды с двумя или тремя 56-битовыми ключами. 3DES определен в публикации 46-3 Федерального стандарта обработки информации (Federal Information Processing Standard (FIPS) Publication 46-3, *Data Encryption Standard*, October 1999, Appendix 2, Page 22 (доступен по адресу: http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)).

3DES может выполняться с использованием двух или трех независимых 56-битовых ключей, ожидаемая "сила" которых может составлять 112 и 168 битов, соответственно. Однако 3DES подвержен атаке "встреча на середине" ("meet in the middle"), которая может уменьшить силу двух ключей DES лишь до 57 битов вместо ожидаемых 112 битов. Та же атака может уменьшить силу трех ключей 3DES лишь до 112 битов вместо ожидаемых 168 битов. Следовательно, для большей безопасности следует использовать 3DES с тремя независимыми ключами и предполагать, что для наихудшего случая его сила будет равна 112 битам.

Алгоритм DES может выполняться относительно быстро благодаря его короткому 56-битовому ключу, в то время как 3DES должен фактически выполнять DES три раза и поэтому является гораздо более медленным. AES, который имеет минимальную длину ключа 128 битов, криптографически сильнее, чем 3DES, и, кроме того, может выполняться быстро как аппаратными, так и программными средствами. Например, программная реализация AES может быть обработана приблизительно так же быстро, как DES, на той же самой платформе, но при значительно большей криптографической силе, чем DES.

МЕС 24: Симметричная конфиденциальность данных на базе криптографического алгоритма DES.

---

[5] SNMPv3 может также обеспечивать конфиденциальность.

MEC 25: Симметричная конфиденциальность данных на базе криптографического алгоритма AES.

MEC 26: Симметричная конфиденциальность данных на базе криптографического алгоритма 3DES.

6.4.2 Асимметричная конфиденциальность данных

Система асимметричного шифрования – это одна из систем, в которой шифровальный и дешифровальный ключи связаны между собой, но различны. Один из них делается открытым, в то время как другой держится в секрете. Открытый ключ отличается от частного ключа, и не существует приемлемого способа получения частного ключа из открытого ключа. Открытые ключи распространяются свободно, частный ключ всегда держится в секрете.

Механизмы безопасности в отношении конфиденциальности данных могут базироваться на асимметричных криптографических алгоритмах, таких как алгоритм Ривеста, Шамира и Адлмана (RSA), шифрование методом эллиптических кривых (Elliptic Curve Cryptography, ECC) и другие.

Алгоритм RSA – это широкораспространенный асимметричный алгоритм, который может использоваться для шифрования и цифровых подписей. RSA базируется на математической трудности разложения на множители больших простых чисел. Ключи для алгоритма RSA имеют общую длину 1024 бита и 2048 битов. Следует отметить, что RSA с длиной ключа 2048 битов приблизительно эквивалентен по криптографической силе 128-битовому симметричному шифрованию.

Шифрование методом эллиптических кривых (ECC) – это новый метод реализации криптографии с открытым ключом (т. е. он сравним с алгоритмом RSA). Посредством ECC эллиптическая кривая определяется в некотором поле; затем в этом поле решается проблема дискретного логарифма эллиптической кривой. Главным преимуществом ECC по сравнению с другими алгоритмами с открытым ключом является размер ключа. 160-битовый ключ ECC приблизительно эквивалентен по защищенности 1024-битовому ключу алгоритма RSA, а 210-битовый ключ ECC приблизительно эквивалентен по защищенности 2048-битовому ключу алгоритма RSA. Благодаря меньшей длине ключа ECC требуется меньший объем вычислений для служебного заголовка и реализуется более эффективная криптосистема[6].

MEC 27: Асимметричная конфиденциальность данных на базе криптографического алгоритма RSA с заданной длиной ключа.

MEC 28: Асимметричная конфиденциальность данных на базе криптографического алгоритма ECC с заданной длиной ключа.

6.4.3 Конфиденциальность данных – Резюме

Примеры алгоритмов, которые могут использоваться для обеспечения конфиденциальности данных, в табличном формате представлены в таблице 3. Также должны быть рассмотрены такие вопросы, как форматирование, дополнение нулями, обработка ошибочных состояний, выбор подходящих простых чисел и размера открытой экспоненты, а в случае ECC – выбор базового поля и кривой; однако эти вопросы выходят за рамки настоящей Рекомендации.

Таблица 3/M.3016.3 – Примеры криптографических алгоритмов для обеспечения конфиденциальности данных

Категория	Алгоритм	Комментарии
Симметричные алгоритмы шифрования	AES	Усовершенствованный стандарт шифрования
	3-DES	Тройной алгоритм шифрования данных
	DES	Стандарт шифрования данных
Асимметричные алгоритмы шифрования	RSA	Ривест, Шамир и Адлман
	ECC	Шифрование методом эллиптических кривых

[6] См. *Digital Signature Standard*, November 2002 (доступно на http://csrc.nist.gov/cryptval/dss.htm) для получения дополнительных подробных сведений об алгоритмах RSA, Диффи-Хеллмана и ECC.

6.5 Целостность данных

Механизмы безопасности в отношении целостности данных используются для гарантирования отсутствия изменений передаваемых данных.

Целостность данных базируется на криптографических принципах. Криптография использует специальные алгоритмы, основанные на стандартах и публично доступные, что делает возможным их тщательное изучение и простую реализацию. Протоколы безопасности (например, IPsec, SSL/TLS, SSH) в типовом варианте обеспечивают услуги целостности данных на базе лежащих в их основе криптографических алгоритмов в дополнение к другим услугам безопасности, таким как конфиденциальность данных и аутентификация источника данных. (Для обсуждения протоколов безопасности IPsec, SSL/TLS и SSH см. Дополнение I.)

Методы, используемые для генерации, хранения, распространения, уничтожения и аннулирования криптографических ключей в целях обеспечения целостности данных, имеют первостепенную важность. Кроме того, такие факторы, как длина ключа, выбор ключа и выбор алгоритма, непосредственно влияют на уровень безопасности конкретной криптосистемы.

6.5.1 Симметричная целостность данных

Симметричная целостность данных, или целостность данных с секретным ключом, относится к криптографической системе, в которой ключи, используемые для обеспечения целостности данных, одни и те же для отправителя и получателя информации. Симметричные криптосистемы требуют проведения начальных мероприятий для отдельных лиц, чтобы они могли совместно использовать уникальный секретный ключ (например, ключ верификации). Ключ должен распространяться между отдельными лицами с использованием защищенных средств или генерироваться внутри (например, на основе совместно используемого секретного ключа дерева).

Механизмы безопасности в отношении симметричной целостности данных для сообщений произвольной длины могут базироваться на ключевых алгоритмах с дайджестом сообщения, объединенных с функциями хеширования. Примерами ключевых алгоритмов с кратким изложением сообщения являются хешированный код аутентификации сообщения с дайджестом сообщения MD5 (HMAC-MD5-96)[7] и хешированный код аутентификации сообщения с алгоритмом безопасного хеширования 1 (HMAC-SHA-1-96)[8].

MEC 29: Симметричная целостность данных на базе криптографического алгоритма HMAC-MD5-96.

MEC 30: Симметричная целостность данных на базе криптографического алгоритма HMAC-SHA-1-96.

6.5.2 Асимметричная целостность данных

Система асимметричной целостности данных – это одна из систем, в которой ключи подписи и верификации связаны между собой, но различны. Ключ верификации делается открытым, в то время как ключ подписи держится в секрете. Ключ подписи отличается от ключа верификации, и не существует приемлемого способа получения ключа подписи из ключа верификации. Ключи верификации распространяются свободно, однако ключ подписи всегда держится в секрете.

Механизмы безопасности в отношении целостности данных могут базироваться на асимметричных криптографических алгоритмах, таких как алгоритм цифровой подписи (Digital Signature Algorithm, DSA) и алгоритм (Ривеста Шамира и Адлмана, RSA).

Посредством механизмов безопасности в отношении асимметричной целостности данных отправитель подписывает дайджест сообщения ключом подписи (частным ключом), а ключ верификации (открытый ключ) используется получателем для проверки того, что дайджест сообщения был подписан заявленным отправителем.

MEC 31: Асимметричная целостность данных на базе криптографического алгоритма DSA с заданной длиной ключа.

MEC 32: Асимметричная целостность данных на базе криптографического алгоритма RSA с заданной длиной ключа.

---

[7] Internet Engineering Task Force Request for Comment 2403, *The Use of HMAC-MD5-96 within ESP and AH*, C. Madson, R. Glenn, November 1998.

[8] Internet Engineering Task Force Request for Comment 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*, C. Madson, R. Glenn, November 1998.

6.5.3 Целостность данных – Резюме

Примеры алгоритмов, которые могут использоваться для обеспечения целостности данных, в табличном формате представлены в таблице 4. Также должны быть рассмотрены такие вопросы, как форматирование, дополнение нулями, обработка ошибочных состояний и выбор подходящих простых чисел; однако эти вопросы выходят за рамки настоящей Рекомендации.

Таблица 4/M.3016.3 – Примеры криптографических алгоритмов для обеспечения целостности данных

Категория	Алгоритм	Комментарии
Асимметричные алгоритмы проверки сообщения	DSA	Алгоритм цифровой подписи.
Симметричные алгоритмы проверки сообщения	HMAC-MD5-96	Хешированный код аутентификации сообщения с дайджестом сообщения MD5.
	HMAC-SHA-1-96	Хешированный код аутентификации сообщения с алгоритмом защищенного хеширования 1.

6.6 Данные проверки

Сетевые элементы и системы управления должны обеспечивать достаточные возможности, позволяющие выполнять действия по изучению, проверке, обнаружению в реальном времени, анализу и защите, чтобы могли быть предприняты надлежащие действия по устранению сбоев. В данном пункте рассматриваются механизмы безопасности, используемые для выполнения таких регистрационных записей проверки безопасности. Конкретные подробные сведения о содержимом и формате регистрационных записей проверки безопасности выходят за рамки настоящей Рекомендации.

Регистрационные записи проверки безопасности могут вестись сетевым элементом и системами управления. Эти регистрационные записи проверки безопасности могут храниться на месте и могут передаваться в централизованное хранилище регистрационных записей и/или в устройство анализа регистрационных записей.

Системная регистрация (Syslog) является одним из общепринятых механизмов, используемых для передачи регистрационных записей безопасности из местной памяти в централизованное хранилище записей.

В общем случае устройство может обладать способностью дистанционно или с консоли регистрировать любое действие, которое изменяет атрибуты и услуги безопасности, настройки доступа или другие параметры конфигурации устройств; каждую попытку регистрации и ее результат; каждый выход из системы или окончание сеанса. Регистрация не связанных с безопасностью сообщений OAM&P, относимых иногда к сообщениям "о текущем изменении", требуется для любых доступных для проверки действий.

Регистрационные записи проверки могут быть отправлены на постоянный сервер проверки после присвоения им последовательной метки и криптографической аутентификации (подписи) сетевым элементом или системой управления. Регистрационные записи проверки безопасности могут быть отправлены в центральное хранилище по защищенному маршруту. Для обеспечения правильного анализа действий должны быть точно и надежно синхронизированы дата и время многочисленных источников регистрации (например, NTPv3).

MEC 33: Регистрация проверки безопасности на основе Syslog.

MEC 34: Регистрационная запись проверки безопасности, содержащая следующую информацию:

MEC 34a: Описание действия или фактическое действие, которое регистрируется.

MEC 34b: Уровень идентичности и защищенности пользователя или процесса, который инициировал данное действие.

MEC 34c: Дата и время состоявшегося действия.

MEC 34d: Информация о сетевом источнике и сетевом пункте назначения, если она применима (например, когда производится вхождение в систему).

MEC 34e: Индикация успеха или неудачи действия.

MEC 34f: Любое действие, которое требует проверки.

MEC 35: Регистрационные записи проверки безопасности, отправленные на постоянный сервер проверки.

MEC 36: Криптографически подписанные регистрационные записи проверки безопасности.

MEC 37: Регистрационные записи проверки безопасности, отправленные в центральное хранилище по защищенному маршруту.

6.7 Обмен ключами

Для приложений с симметричной конфиденциальностью данных и с симметричной целостностью данных должен производиться безопасный обмен криптографическими ключами между конечными пунктами. В нормальном варианте обмен ключами для таких симметричных алгоритмов должен осуществляться в процессе, тесно связанном с аутентификацией, чтобы не позволять атакующему объекту вторгаться между процессами аутентификации и распространения ключей.

Методы, используемые для генерации, хранения, распространения, уничтожения и аннулирования криптографических ключей в целях обеспечения целостности данных, имеют первостепенную важность. Кроме того, такие факторы, как длина ключа, выбор ключа и выбор алгоритма, непосредственно влияют на степень безопасности обеспечиваемой криптосистемы.

Для обеспечения криптографических ключей и/или их обмена могут использоваться различные методы. Одним из концептуально простых методов является обмен предварительно назначенными общими ключами, когда ключи посылаются вне полосы и предоставляются каждому конечному пункту при необходимости. Например, ключи могут быть выбраны и сконфигурированы в конечных пунктах сетевыми администраторами после ввода в эксплуатацию. Обмен предварительно назначенными ключами применим при малом числе конечных пунктов, однако он плохо подходит при большом числе конечных пунктов, так как генерирование и конфигурирование большого числа ключей становится весьма трудоемким.

Для поддержки услуг обмена ключами могут использоваться асимметричные алгоритмы, такие как Ривеста Шамира и Адлмана (RSA). Используя RSA, один конечный пункт выбирает симметричные криптографические ключи и распределяет их другим конечным пунктам под защитой алгоритма шифрования RSA. При использовании этого метода асимметричный алгоритм должен иметь подходящую длину ключа, достаточную для защиты отправляемых симметричных ключей. Например, для защиты 128-битового симметричного ключа в алгоритме RSA должен использоваться ключ длиной 2048 битов или больше, чтобы криптографическая сила была примерно эквивалентна 128-битовому шифрованию с симметричным ключом.

Общим методом распространения ключей является алгоритм соглашения о ключах Диффи-Хеллмана. Используя алгоритм Диффи-Хеллмана, конечные пункты независимо получают секретные криптографические ключи по сети общего пользования. Во время процедуры Диффи-Хеллмана между конечными пунктами посылаются только промежуточные результаты, а секретный ключ никогда не показывается. При надлежащем выборе простого числа Диффи-Хеллмана для атакующих объектов с точки зрения вычислений невозможно раскрыть секретный ключ по промежуточным результатам.

Для алгоритмов RSA и Диффи-Хеллмана также должны быть рассмотрены такие вопросы, как выбор подходящих простых чисел, выбор открытых экспонент и обработка состояний возникновения ошибки.

MEC 38: Обмен криптографическими ключами на базе предварительно заданных общих ключей.

MEC 39: Обмен криптографическими ключами на базе асимметричного алгоритма RSA с заданной длиной ключа RSA.

MEC 40: Обмен криптографическими ключами на базе алгоритма соглашения о ключах Диффи-Хеллмана с заданной группой простых чисел Диффи-Хеллмана.

6.8 Предоставление отчетов о нарушениях безопасности

Аварийные сигналы в системе безопасности должны посылаться администраторам при обнаружении любого нарушения безопасности или при неспособности продолжать записи регистрационных сведений о проверке.

MEC 41: Механизмы предоставления отчетов о нарушениях безопасности, такие как X.736.

6.9 Фильтрация пакетов

Для защиты DCN от атаки и от потери информации об DCN для устройств с организацией соединений на основе пакетов должна использоваться фильтрация пакетов.

MEC 42: Фильтрация пакетов на основе одного или нескольких следующих критериев контроля:

MEC 42a: IP-адрес источника

MEC 42b: IP-адрес пункта назначения

MEC 42c: Протокол

MEC 42d: Порт источника

MEC 42e: Порт пункта назначения

и обеспечение одного или нескольких следующих действий:

MEC 42f: Передача

MEC 42g: Исключение

MEC 42h: Изменение

MEC 42i: Пересылка

с потенциальной возможностью учета предыдущих решений (т. е. с использованием информации содержимого).

Дополнение I

Механизмы безопасности IPsec, SSL/TLS и SSH

I.1 IPsec

IPsec поддерживает безопасность на уровне IP посредством использования комбинации криптографических и протокольных механизмов безопасности. Протокол IPSec функционирует между сетевым уровнем (уровень 3) и транспортным уровнем (уровень 4), он может использоваться для защиты трафика данных любого типа (TCP или UDP) и не зависит от приложений. IPsec предназначен для обеспечения совместимой, высокого качества и основанной на криптографических методах безопасности для протоколов IPv4 и IPv6. Набор услуг безопасности, предоставляемых протоколом IPsec, включает следующие услуги:

a) целостность данных;

b) аутентификация источника данных на основе IP-адреса;

c) аутентификация машина-машина;

d) защита от повторного воспроизведения информации;

e) конфиденциальность данных;

f) обмен криптографическими ключами.

Эти задачи выполняются за счет использования двух услуг безопасности трафика – заголовок аутентификации (Authentication Header, AH) и полезная нагрузка с встроенной защитой информации (Encapsulating Security Payload, ESP) – и процедур и протоколов управления криптографическими ключами. Услуга AH обеспечивает аутентификацию источника данных, аутентификацию машина-машина и целостность данных для IP-пакетов. Услуга ESP обеспечивает услугу конфиденциальности данных в дополнение к аутентификации источника данных, аутентификации машина-машина и целостности данных для IP-пакетов. Механизмы IPsec предназначены также для обеспечения независимости от криптографических алгоритмов, чтобы допускать выбор различных комплектов алгоритмов без влияния на другие части реализации.

Управление ключами обеспечивается протоколом обмена ключами в сети Интернет (Internet Key Exchange, IKE). Предусматриваются как ручной, так и автоматический механизмы для согласования ключей между конечными пунктами. Автоматическое согласование ключей может основываться на предварительно задаваемых общих ключах (например, пароли) или на сертификатах X.509.

Ссылки [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197].

I.2 SSL/TLS

Протокол безопасности "Уровень защищенных гнезд" (SSL) обеспечивает шифрование данных, аутентификацию сервера, целостность сообщения и необязательную аутентификацию клиента для соединения TCP/IP на транспортном уровне (уровень 4). SSL в данное время имеет версию 3.0. Безопасность транспортного уровня (TLS) – это стандартизованная IETF версия SSL, включающая следующие усовершенствования безопасности по отношению к SSL:

- Поддержка требуемых алгоритмов Диффи-Хеллмана и цифровых подписей (DSA) с необязательной поддержкой RSA.
- Использование более сильного алгоритма аутентификации хеширования сообщения (HMAC) вместо нестандартного алгоритма MAC, определяемого SSL.
- Модифицированный алгоритм генерации ключей, в котором используется MD5 (дайджест сообщения MD5) и SHA-1 (Secure Hash Algorithm 1, алгоритм безопасного хеширования 1) с HMAC.

Протокол SSL/TLS функционирует выше сетевого уровня (уровень 4), он работает только с протоколом управления транспортировкой (Transport Control Protocol, TCP) и не может работать с протоколом дейтаграмм пользователя (User Datagram Protocol, UDP). Протоколами прикладного уровня, которые обычно функционируют поверх SSL/TLS, являются (но это не полный список) протокол передачи гипертекста (HTTP), облегченный протокол доступа к сетевым каталогам (LDAP) и протокол доступа к сообщениям в сети Интернет (Internet Messaging Access Protocol). Протокол более высокого прикладного уровня может работать поверх SSL/TLS без какой-либо связи с SSL/TLS; однако прикладной уровень должен быть связан с SSL/TLS посредством использования обратных вызовов ввода/вывода (I/O).

Протокол SSL/TLS обеспечивает три функции безопасности для трафика TCP: конфиденциальность данных, целостность данных и аутентификация.

Архитектура протокола безопасности SSL/TLS обеспечивает два уровня, которые функционируют поверх TCP:

- протоколы верхнего уровня SSL/TLS;
- протокол записи SSL/TLS.

Протоколы верхнего уровня SSL/TLS включают в себя протокол установления связи (Handshake Protocol) SSL/TLS, протокол изменения шифра (Cipher Change Protocol) SSL/TLS и протокол сигнализации (Alert Protocol) SSL/TLS для оповещений. Сеансы связи SSL/TLS сначала организуются протоколом установления связи SSL/TLS, который обеспечивает:

a) Согласование механизмов аутентификации и безопасности.

b) Аутентификацию клиента и сервера. (Используя открытые/частные ключи сервера и клиента.)

c) Установление ключей безопасности.

После установления сеанса SSL/TLS протокол записи SSL/TLS используется для услуг транспортировки массивов данных. Протокол записи SSL/TLS обеспечивает:

a) Аутентификацию источника данных на основе ключей сервера.

b) Целостность данных.

c) Конфиденциальность.

Следует отметить, что SSL в настоящее время имеет версию 3 (SSLv3), а TLS – версию 1. Использование более ранних версий SSL и TLS не рекомендуется.

SSL/TLS позволяет проводить либо одностороннюю аутентификацию, когда только сервер удостоверяет подлинность клиента, либо двустороннюю аутентификацию, когда как клиент, так и сервер удостоверяют подлинность друг друга. Односторонняя аутентификация – это обычный метод, используемый в сети Интернет общего пользования. Для приложений управления сетью рекомендуется двусторонняя аутентификация, чтобы позволить обеим сторонам узнать, связываются ли они с желаемым конечным пунктом.

Ссылки [RFC 2246], [RFC 3546], [SSL V3].

I.3 SSH

SSH – это протокол безопасности прикладного уровня (уровень 7), используемый обычно для непосредственной замены небезопасных протоколов Telnet и FTP (протокол пересылки файлов). Telnet и FTP являются небезопасными протоколами, которые передают пароли и все другие данные в открытом виде. SSH может также использоваться для защиты других протоколов посредством перенаправления портов, так что этот протокол может использоваться в качестве общего протокола безопасности сети.

Существуют две версии SSH: SSHv1 и SSHv2. SSHv1 был разработан в 1998 году и сейчас считается небезопасным/вышедшим из употребления.

Свойствами защищенной оболочки 2 являются:

- Полная замена протоколов Telnet, Rlogin, Rsh, Rcp и FTP для обеспечения безопасной пересылки файлов и безопасного копирования файлов.
- Автоматическая аутентификация пользователей. (Пароли не посылаются открытым текстом.)
- Двусторонняя аутентификация (удостоверяется подлинность как сервера, так и клиента).
- Туннелирование произвольных приложений на основе TCP/IP посредством использования перенаправления портов.
- Шифрование данных для обеспечения конфиденциальности данных.
- Несколько вариантов аутентификации, включая аутентификацию по паролям, по открытому ключу и по идентификатору SecureID.
- Доступность нескольких наборов шифров.

Архитектура SSHv2 состоит из трех важных компонентов:

- Протокол транспортного уровня (Transport Layer Protocol) [SSH-TRANS] обеспечивает аутентификацию сервера, конфиденциальность данных и целостность данных. Он может также факультативно предусматривать компрессию.
- Протокол аутентификации пользователя (User Authentication Protocol) [SSH-USERAUTH] удостоверяет подлинность пользователя на стороне клиента для сервера.
- Протокол соединения (Connection Protocol) [SSH-CONNECT] мультиплексирует зашифрованный туннель в несколько логических каналов.

Протокол соединения обеспечивает каналы, которые могут использоваться для широкого спектра задач. Стандартные методы обеспечиваются для организации интерактивных сеансов связи в режиме защищенной оболочки и для перенаправления ("туннелирования") произвольных портов и соединений TCP/IP.

Порт с номером 22 зарегистрирован IANA в качестве стандартного порта для использования приложениями SSHv2.

Ссылки [SSH-ARCH], [SSH-TRANS], [SSH-USERAUTH], [SSH-CONNECT].

Дополнение II

В данном Дополнении описывается механизм фильтрации пакетов для повышения безопасности сети передачи данных (DCN). Сеть передачи данных (DCN) – это сеть, используемая для соединения приложений управления (обычно расположенных в оперативном центре управления сетью (Network Operations Centre)) с сетевыми элементами для централизованного предоставления услуг, контроля аварийных сигналов, тестирования, выставления счетов и другой деятельности по управлению сетью. В разделах 2.8–2.10 Документа RFC 3871 содержится набор требований к фильтрации пакетов для большой инфраструктуры IP-сети поставщика услуг Интернет. В рассматриваемом дополнении используется документ RFC 3871 для определения рекомендаций по фильтрации для DCN.

Фильтрация пакетов – это процесс принятия решения по существу каждого пакета, который проходит через сетевой элемент, на основе заданного критерия соответствия[9]. Может быть несколько вариантов решения, например передача, удаление, перенаправление (направление пакета куда-то в другое место) и т. д. Фильтрация пакетов обеспечивает базовый механизм защиты, определяющий, какой трафик передается в сетевой элемент или систему управления или проходит через них.

Основной интерес представляет фильтрация трафика, поступающего из других сетей (например, сети, переносящие трафик потребителя, равноправные сети управления) в DCN. Дополнительно может потребоваться отделение некоторых элементов DCN от других элементов. Поэтому фильтрация может использоваться между разными подсетями (или областями) DCN.

II.1 Задачи

Основными задачами механизма фильтрации пакетов являются:

1) Защита инфраструктуры DCN от трафика потребителя. Защита должна включать в себя надлежащее совместное использование общих ресурсов для предотвращения ухудшения обслуживания или отказа в обслуживании.

2) Защита инфраструктуры DCN от равноправных сетей.

3) Предотвращение любого дальнейшего распространения через инфраструктуру DCN трафика DCN, не отвечающего применяемой политике безопасности.

II.2 Соображения по проектированию сети, влияющие на фильтрацию пакетов

В данном Дополнении не содержатся требования к проектированию DCN; однако проектирование и развертывание DCN будут оказывать влияние на организацию фильтрации пакетов в сети и на требования к фильтрации пакетов в сети. На рисунке II.1 показана типичная схема построения сети DCN.

[9] Это описание фильтрации пакетов очень похоже на маршрутизацию пакетов, однако в данном Дополнении обращается внимание на фильтрацию пакетов, и в нем не рассматривается маршрутизация пакетов.

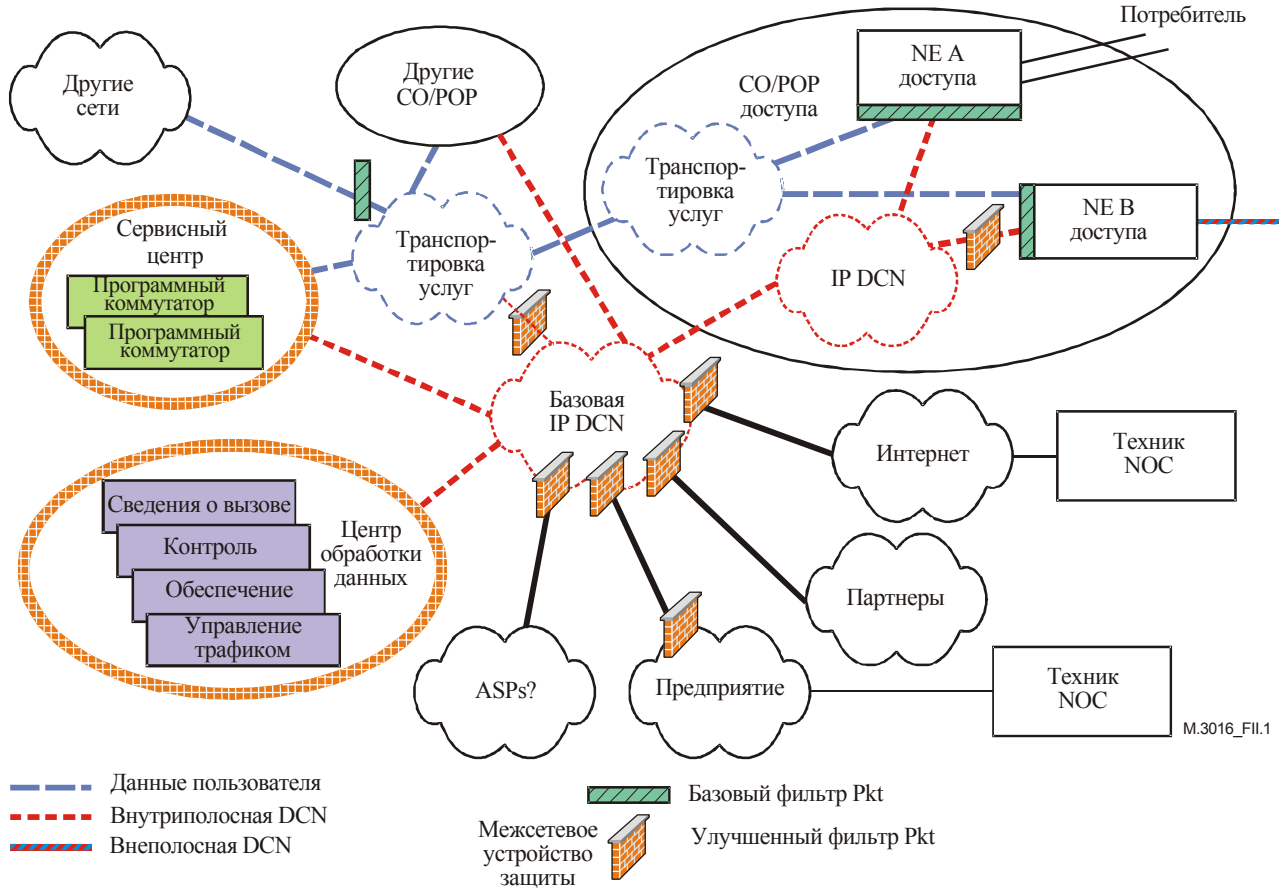

Рисунок II.1/M.3016.3 – Общая иллюстрация сети DCN

Общепризнанными являются три типа построения DCN:

- Внутриполосное управление: DCN использует зарезервированную полосу из сервисной сети, применяемой для переноса данных потребителя. Например, для трафика управления в канале Ethernet может быть выделена сеть VLAN либо соединение IPSec или SSH может использоваться поверх соединения Интернет (например, для техника NOC на рисунке II.1, подсоединенного через Интернет).
- Внеполосное управление: DCN полностью отличается от сервисной сети, переносящей трафик потребителя. Эта сеть может быть наложена сверху на ту же физическую сеть, которая также переносит трафик данных пользователя.
- Гибридное управление: сочетает внутриполосный и внеполосный подходы.

Сравнение и общее обсуждение этих типов архитектур управления выходят за рамки настоящей Рекомендации (см. раздел 2.2 RFC 3871); однако использование одной или другой из архитектур будет влиять на требования к фильтрации.

Логическое обоснование, используемое при создании сетей DCN, будет меняться для типа поддерживаемых сетевых элементов, рабочих процедур и предпочтений, топологий сети, экономики и т. д. Пропускная способность сети, устойчивость и безопасность являются вопросами, которые рассматриваются для каждого подхода.

Предлагаемые управляемые услуги следующего поколения будут реализовываться с использованием транспортного оборудования на основе пакетов (например, ретрансляции кадров, ATM, IP, MPLS, Ethernet). Возникновение таких услуг делает необходимым управление оборудованием доступа (CPE).

Может потребоваться использование гибридной модели, в которой применяется внеполосное управление до точки входа в сеть (POP) и внутриполосное управление от POP до устройств доступа CPE, поскольку может оказаться экономически нецелесообразным расширение внеполосного управления на весь маршрут до устройства доступа CPE. Элемент NE B доступа иллюстрирует последнее соображение на рисунке II.1.

В этом случае улучшенная фильтрация (например, межсетевое устройство защиты) может быть использована для защиты DCN от CPE. Другими примерами использования внутриполосного соединения являются управление удаленной, изолированной POP, когда нецелесообразно создавать отдельную сеть, и использование сервисной сети в качестве резерва для DCN.

Использование фильтрации пакетов подразумевает также, что используемое DCN адресное пространство отделено от адресного пространства, выделенного потребителям, и что отсутствует необходимость в потоке трафика между этими двумя областями. Разделение адресных пространств упрощает разработку пакетных фильтров для блокировки доступа трафика потребителей к ресурсам управления. Самым простым подходом является блокирование всего идущего в DCN трафика, источник которого находится вне DCN, для защиты инфраструктуры управления от трафика потребителя. Однако в некоторых случаях может оказаться необходимым обмен определенным объемом трафика между внешними сетями и DCN, например, обмен информацией управления между двумя поставщиками услуг (например, DCC в средней точке соединения между двумя SP).

Следовательно, требуется принять меры, чтобы обеспечить прохождение некоторого ограниченного объема трафика между областями, и требуется больше настроек (например, улучшенная фильтрация пакетов) для обеспечения адекватной безопасности сетей DCN.

Рисунок II.1 иллюстрирует схему построения сети DCN на основе сделанных выше допущений. Транспорт услуги (синий цвет) переносит трафик потребителя. DCN (красный цвет) переносит трафик управления. Сервисный центр содержит серверы и другие устройства, которые предоставляют услуги потребителям и к которым потребители имеют доступ (например, программные коммутаторы). Центр обработки данных содержит серверы и другие рабочие системы, используемые для управления и контроля сети и непосредственно не доступные для потребителей. В соединениях от DCN к сетевым элементам может использоваться IP, X.25, асинхронная передача или ИСО CLNS (сетевое обслуживание без установления соединения).

Базовым требованием для обеспечения безопасности DCN в NE доступа является возможность фильтрации входящих пакетов на границе DCN/сервисная сеть. Однако такая базовая фильтрация пакетов может быть недостаточной, поскольку атаки могут также исходить от скомпрометированного NE или хоста внутри DCN. Поэтому может потребоваться, чтобы подходящие механизмы фильтрации пакетов были стратегически реализованы во многих пунктах в DCN для обеспечения соответствия применяемой политике безопасности. Кроме того, может потребоваться улучшенная фильтрация пакетов, когда DCN соединяется с внешними сетями (например, Интернет, сеть предприятия поставщика услуг (SP), партнеры и т. д.).

Несмотря на то что фильтрация пакетов является компонентом стратегии сетевой безопасности, она должна использоваться в контексте общих принципов и стратегий сетевой безопасности, включая, например, разделение на изолированные части и углубленную защиту. Таким образом, хотя хорошая стратегия безопасности включает требования по безопасности к самим хостам (например, программным коммутаторам) и разделение сети на изолированные части, эти вопросы выходят за рамки настоящей Рекомендации.

Для защиты инфраструктуры управления и DCN в общем случае для сетевого оператора полезно отбрасывать некоторые пакеты, полученные извне периметра DCN (т. е. от равноправных сетей и потребителей). Например, пакеты с недействительными IP-адресами источника и пакеты, предназначенные для IP-адресов, используемых исключительно в DCN, не должны допускаться внутрь периметра DCN. Эта функция называется входящей фильтрацией. Данные требования взяты из [RFC 3871] и [RFC 2827].

Существуют две категории фильтрации пакетов:

- Базовая фильтрация пакетов на основе информации заголовка пакета, включая способность обнаруживать и блокировать пакеты с ложными адресами источника.
- Улучшенная фильтрация пакетов, включающая:
  - Контроль состояния пакетов с учетом их содержимого, когда контекст или состояние информации также используется при принятии решений о фильтрации.
  - Динамическая фильтрация для конкретных протоколов, когда фильтры открываются динамически на основе информации, переносимой в полезной нагрузке протокола.
  - Углубленный контроль пакетов, когда протоколы прикладного уровня проверяются на наличие каких-либо аномалий протокола, необычного или подозрительного содержимого.

II.3 Базовая фильтрация пакетов

Оборудование, подсоединенное к DCN, должно иметь возможность отбрасывать полученные от внешних интерфейсов (например, потребителей или равноправных сетей) пакеты, содержащие недействительные IP-адреса источника. Недействительные IP-адреса источника могут состоять из:

- Адресов Bogon (IP-адреса источника, невыделенные IANA или региональными регистрами Интернета) (см. раздел 1.8 RFC 3871).
- Martians (имена пакетов с IP-адресами Bogon) (см. раздел 1.8 RFC 3871).
- IP-адресов, неназначенных потребителю (или недействительных для отправки равноправной сетью).

Механизм фильтрации пакетов должен обладать способностью фильтровать трафик, адресованный выделенным DCN блокам адресов и приходящий извне (например, от потребителей), на основе атрибутов, заданных в MEC 42.

Механизм фильтрации пакетов должен обеспечивать получение точной статистики трафика на каждый интерфейс. Уровень детальности статистики может меняться в зависимости от механизма фильтрации пакетов.

Оборудование должно обладать способностью фильтровать трафик, поступающий извне DCN (например, от потребителей), т. е. адресованный непосредственно сетевому элементу через любой из его интерфейсов, включая интерфейсы шлейфа, на основе атрибутов, заданных в MEC 42.

Механизм фильтрации пакетов может поддерживать концепцию многих областей безопасности модели СУЭ, когда все элементы в области безопасности обязаны придерживаться общей политики безопасности.

Оборудование может обладать способностью генерировать соответствующие аварийные сигналы на основании трафика, изъятий трафика и своих рабочих состояний.

II.4 Улучшенная фильтрация пакетов

Эти рекомендации должны приниматься во внимание, когда существует высокая степень перекрытия трафика пользователя и трафика управления, то есть когда трафики пользователя и управления не разделяются прямо на границе сети и когда DCN непосредственно соединена с другими сетями. Кроме того, эти возможности фильтрации должны использоваться на границах защищенных подсетей (например, между DCN и центром обработки данных).

Данный механизм фильтрации должен контролировать прикладные протоколы, используемые в DCN, на наличие каких-либо аномалий протокола или аномального режима работы и должен обладать способностью блокировки такого трафика.

Механизм должен контролировать содержимое трафика DCN на наличие злоумышленного содержимого, такого как вирусы, "черви", атаки типа "Троянский конь" и т. д., где это возможно.

Должен обеспечивать защиту от применяемых атак типа "отказ в обслуживании" (DoS).

Должен обладать способностью фильтрации с учетом содержимого пакетов, т. е. для фильтрации пакетов используется информация сеанса связи. Пропуск обратного трафика сеанса связи должен быть разрешен во всех случаях.

Должен поддерживать возможность динамического пропуска для всех протоколов, используемых в сети, переносящей информацию порта в своей полезной нагрузке, например FTP, SIP и т. д. Механизм фильтрации пакетов должен контролировать информацию порта в полезной нагрузке и открывать связь в заданном порте (динамический пропуск) на время сеанса связи. На случай внезапного прекращения сеанса связи должен быть реализован соответствующий механизм тайм-аута для закрытия порта.

Должен поддерживать исполнение протокола, включая отбрасывание неправильно сформированных пакетов или прекращение неправильно сеанса связи и т. д.

Другие рекомендации по возможностям фильтрации можно найти в разделах 2.7–2.10 RFC 3871.

БИБЛИОГРАФИЯ

[RFC 2827] IETF RFC 2827 (2000), *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*.

[RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt?number=2401

[RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks*.

[RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[NDS/IP] 3GPP TS 33.210 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security*.

[RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header*, http://www.ietf.org/rfc/rfc2402.txt?number=2402

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2403.txt?number=2403

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2404.txt?number=2404

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV*, http://www.ietf.org/rfc/rfc2405.txt?number=2405

[RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, http://www.ietf.org/rfc/rfc2406.txt?number=2406

[RFC 2407] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*, http://www.ietf.org/rfc/rfc2407.txt?number=2407

[RFC 2408] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*, http://www.ietf.org/rfc/rfc2408.txt?number=2408

[RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*, http://www.ietf.org/rfc/rfc2409.txt?number=2409

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use with IPsec*, http://www.ietf.org/rfc/rfc2410.txt?number=2410

[RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*, http://www.ietf.org/rfc/rfc2411.txt?number=2411

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*, http://www.ietf.org/rfc/rfc2412.txt?number=2412

[RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt

[RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*, http://www.ietf.org/rfc/rfc2451.txt

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol, Version 1.0*, ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

[RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*, ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt

[SSL V3] *Secure Socket Layer Version 3.0 Specification*, Netscape Communications. http://wp.netscape.com/eng/ssl3/

[SSH-ARCH] YLONEN (T.): *SSH Protocol Architecture*, I-D draft-ietf-architecture-15.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt

[SSH-TRANS] YLONEN (T.): *SSH Transport Layer Protocol*, I-D draft-ietf-transport-17.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt

[SSH-USERAUTH] YLONEN (T.): *SSH Authentication Protocol*, I-D draft-ietf-userauth-18.txt, September 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt

[SSH-CONNECT] YLONEN (T.): *SSH Connection Protocol*, I-D draft-ietf-connect-18.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt

[FIPS-46-3] Data Encryption Standard. (Описываются как DES, так и 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-197] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[RFC 2437] IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0*, http://www.ietf.org/rfc/rfc2437.txt?number=2437

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
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 и 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	**Управление электросвязью, включая СУЭ и техническое обслуживание сетей**
Серия N	Техническое обслуживание: 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, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2005 г.