МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т M.3016.1

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2005)

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

Сеть управления электросвязью

Безопасность для плоскости административного управления: Требования по безопасности

Рекомендация МСЭ-Т M.3016.1

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.3016.1

Безопасность для плоскости административного управления: Требования по безопасности

Резюме

Данная Рекомендация определяет требования по 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.

Источник

Рекомендация МСЭ-Т M.3016.1 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.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются 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 соблюдение положений 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 вероятность того, что практическое применение или реализация этой 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 получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения 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 требования по безопасности, с тем чтобы создать для поставщиков оборудования, организаций и поставщиков услуг возможность реализации безопасной инфраструктуры управления электросвязью. Настоящий набор требований соответствует современному представлению о состоянии техники, однако технологии развиваются, и условия меняются. 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 требования 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:

– ITU-T Rec. M.3016.0 – Security for the management plane: Overview.
– ITU-T Rec. M.3016.1 – Security for the management plane: Security requirements.
– Рек. МСЭ-Т M.3016.2 – Безопасность для плоскости управления: Услуги по обеспечению безопасности.
– ITU-T Rec. M.3016.3 – Security for the management plane: Security mechanism.
– Рек. МСЭ-Т M.3016.4 – Безопасность для уровня управления: Проформа структуры.

Рекомендация МСЭ-Т M.3016.1

Безопасность для плоскости административного управления: Требования по безопасности

1 Область применения

Рекомендации МСЭ-Т M.3016.1–3 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.3016.1–3 не указывается, является ли требование, услуга или механизм обязательным или необязательным.

Настоящая Рекомендация определяет требования по 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.

Данная 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, значений и т. д. для помощи в реализации их политики обеспечения безопасности.

1.1 Назначение

В Рекомендации МСЭ-Т M.3016.0 определяется ряд целевых функций для обеспечения безопасности сети управления, а также угрозы, которые создают риски при выполнении этих целевых функций. В данной Рекомендации требования выведены из целевых функций, направленных против этих угроз, и определены услуги безопасности, которые противодействуют угрозам. При определении услуг используются механизмы, основанные на некоторых алгоритмах. Другие Рекомендации этой серии базируются на структуре, заданной в обзоре Рекомендации МСЭ-Т M.3016.0. Она добавляет различные действия, требуемые для обеспечения безопасности плоскости административного управления.

1.2 Взаимосвязь с архитектурой безопасности X.805

В Рекомендации МСЭ-Т X.805 определена архитектура безопасности для обеспечения сквозной безопасности сети. Архитектура безопасности X.805 логически разделяет комплексный набор свойств, связанных со сквозной безопасностью сети, на три отдельных архитектурных компонента, а именно, параметры безопасности (Security Dimensions), слои безопасности (Security Layers) и плоскости безопасности (Security Planes) (см. рисунок 2/X.805). Параметр безопасности – набор мер по безопасности, выработанных для рассмотрения конкретного аспекта безопасности сети. В Рекомендации МСЭ-Т X.805 определяются три слоя безопасности: слой безопасности инфраструктуры, слой безопасности услуг и слой безопасности приложений, причем эти уровни располагаются друг за другом для обеспечения общесетевых решений. Плоскость безопасности представляет собой некоторый тип деятельности сети, защищенной параметрами безопасности. В Рекомендации МСЭ-Т X.805 определены три плоскости безопасности, а именно, плоскость административного управления, плоскость оперативного управления и плоскость конечного пользователя. Для обеспечения законченного решения меры безопасности (например, управление доступом, аутентификация) должны быть применены к каждому типу деятельности сети (то есть к работе в плоскости административного управления, к работе в плоскости оперативного управления и к работе в плоскости конечного пользователя) для инфраструктуры сети, услуг сети и приложений сети. В настоящей Рекомендации обращается особое внимание на аспект безопасности плоскости административного управления для сетевых элементов (NE) и систем управления (MS), которые являются частью инфраструктуры сети.

1.3 Взаимосвязь с требованиями по безопасности сетей электросвязи E.408

В Рекомендации МСЭ-Т E.408 предоставлены обзор требований по безопасности и структура, которая определяет угрозы безопасности сетей электросвязи в общем (как для фиксированной, так и для подвижной связи; как для передачи голоса, так и для передачи данных) и дает руководящие указания по

планированию контрмер, которые могут быть применены для уменьшения рисков, возникающих из-за угроз. Эта Рекомендация является обобщенной по своему характеру и не определяет или не рассматривает требования для конкретных сетей. Серия M.3016.x определяет требования, услуги и механизмы безопасности для сети электросвязи, то есть плоскость административного управления в общем случае при управлении электросвязью.

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.

– Рекомендация МСЭ-Т E.408 (2004 г.), *Требования к безопасности сетей электросвязи*.

– 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*.

– ITU-T Recommendation M.3013 (2000), *Considerations for a telecommunications management network*.

– ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.

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

– ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.

– 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 Technical Cor.1 (2001), Technical Cor.2 (2002) and Technical Cor.3 (2003).

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*, plus Amendment 1 (1996), *Layer Two Security Service and Mechanisms for LANs*.

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

– IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

3 Термины и определения

В данной Рекомендации используются следующие термины из Рекомендации МСЭ-Т G.8080/Y.1304:

– плоскость оперативного управления;

– плоскость административного управления;

– транспортная плоскость.

В данной Рекомендации используются следующие термины из Рекомендации МСЭ-Т M.3010:

– система управления;

– сетевой элемент.

В данной Рекомендации используется следующий термин из Рекомендации МСЭ-Т M.3013:

– система управления элементами.

В данной Рекомендации используется следующий термин из Рекомендации МСЭ-Т X.509:

– строгая аутентификация.

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

– управление доступом;

– аутентификация.

В данной Рекомендации определен следующий термин:

3.1 неотложные административные действия по безопасности (critical security administration actions); которые включают (но не ограничиваются этим):

a) определение и назначение привилегий пользователей;

b) добавление и удаление идентификаторов (ID) пользователей;

c) запрет использования конкретных ID пользователей в качестве регистрационного ID в системе;

d) инициализация и сброс паролей для регистрации в системе;

e) инициализация и изменение криптографических ключей;

f) задание срока действия в системе паролей для регистрации в системе;

g) задание системного предела числа неудачных попыток регистрации для каждого регистрационного ID;

h) отмена блокировки или изменение значения системного таймера блокировки;

i) установление значения системного таймера неактивности;

j) установление конфигурации регистрации событий и аварийной сигнализации безопасности системы;

k) управление процессами регистрации событий безопасности;

l) модернизация программного обеспечения безопасности;

m) завершение любого сеанса пользователя или системы.

4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения:

AAA	Аутентификация, авторизация и учет
ACS	Сервер управления доступом
ALE	Потери, ожидаемые в течение года
ANSI	Американский национальный институт стандартов
CO	Центральная АТС
CORBA	Обобщенная архитектура посредника объектных запросов
CSI	Общее защищенное взаимодействие
DoS	Отказ в обслуживании
EMS	Система управления элементами
FTP	Протокол передачи файлов
HAZMAT	Опасные материалы

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
LAES	Узаконенное электронное наблюдение
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
OAM&P	Эксплуатация, управление, техническое обслуживание и обеспечение
OASIS	Организация по совершенствованию стандартов структурированной информации
OEM	Изготовитель оригинального оборудования
ORB	Посредник объектных запросов
OS	Операционная система
OSS	Система эксплуатационной поддержки
RFC	Запрос для комментариев
SAML	Язык разметки заявлений системы безопасности
SNMP	Простой сетевой протокол управления
SOAP	Простой протокол доступа к объекту
SSH	Безопасная оболочка
SSL	Уровень защищенных гнезд
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.3016.1–3 используется описатель. Описатель содержит одну из следующих трехбуквенных меток, за которыми следует число:

– REQ для требования;

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

– SER для услуги;

– MEC для механизма.

6 Требования по безопасности

В данном пункте содержатся требования по безопасности для эксплуатации, управления, технического обслуживания и обеспечения (OAM&P) и для системы эксплуатационной поддержки (OSS) **плоскости административного управления**.

На рисунке 1/M.3016.0 приведены взаимосвязи между целевыми функциями безопасности, угрозами, рисками, требованиями по безопасности и услугами. На нем показан процесс определения "Требований по безопасности" из "Угроз" и "Целевых функций безопасности", которые, в свою очередь, реализуются посредством набора услуг безопасности. Эти "Услуги", противодействующие угрозам, используют "Механизмы", которые сами используют "Алгоритмы безопасности". В таблице 1 (которая является таблицей 4/M.3106.0) приведена взаимосвязь между требованиями по безопасности и услугами безопасности. Описываемые в данном пункте требования по безопасности согласно таблице 1 имеют следующий состав:

– проверка идентичности;

– управляемый доступ и санкционирование;

– защита конфиденциальности;

– защита целостности данных;

– возможность ведения учета;

– регистрация и проверка безопасности;

– отчет об нарушениях безопасности.

ПРИМЕЧАНИЕ. – Восстановление после нарушения безопасности является темой для дальнейшего изучения.

Таблица 1/M.3016.1 – Соответствие требований по безопасности и услуг безопасности (Таблица 4/M.3016.0)

Функциональное требование	Услуга безопасности
Проверка идентичности	Аутентификация пользователя Аутентификация равноправного объекта Аутентификация источника данных
Управляемый доступ и санкционирование	Управление доступом
Защита конфиденциальности – сохраненные данные	Управление доступом Конфиденциальность
Защита конфиденциальности – переданные данные	Конфиденциальность
Защита целостности данных – сохраненные данные	Управление доступом
Защита целостности данных – переданные данные	Целостность
Возможность ведения учета	Невозможность отказа от участия
Регистрация действий	Данные проверки
Отчет о нарушениях безопасности	Аварийная сигнализация о нарушениях безопасности
Проверка безопасности	Данные проверки

6.1 Проверка идентичности

Аутентификация служит двум целям при обеспечении безопасности в **плоскости административного управления**:

1) она обеспечивает идентификацию сторон, участвующих в коммуникации, создает базу для установления частных соединений при обеспечении полной целостности данных и конфиденциальности между двумя системами; и

2) она обеспечивает базовый механизм для регистрации в системе управления и/или проверки деятельности по управлению в любой системе.

6.1.1 Аутентификация пользователя, пароли и ID пользователя

Аутентификация пользователя относится к **аутентификации** клиентов, вовлеченных в управление сетью. В этом случае **аутентификация** проверяет идентичность законного пользователя и предотвращает попытки нелегального проникновения незаконных пользователей. При помощи надлежащей **аутентификации** возможно отслеживание деятельности и ограничение пользователей предварительно санкционированными действиями или ролями, как это обсуждается в п. 6.3.

Минимальными требованиями для **аутентификации** являются использование ID пользователя и статического **сложного пароля**. Могут использоваться и другие механизмы, если администраторы NE/MS уверены, что уровень безопасности как минимум так же высок, как уровень, обеспечиваемый ID пользователя и статическим **сложным паролем**. Другие механизмы, которые могут быть рассмотрены, включают:

– ID пользователя и **двухфакторную аутентификацию** с использованием генератора разового пароля[2]; и

– **двухфакторную аутентификацию** с использованием смарткарты с сохраненными на ней с применением защиты именем пользователя и паролем.

REQ 1: Для входа в систему NE/MS, регистрации и проверки должна поддерживаться строгая аутентификация.

REQ 1 представляет собой требование по безопасности. Описание общего механизма аутентификации приведено в Рекомендации МСЭ-Т M.3016.3. Ожидается, что методы **аутентификации** и простые технологии разового предъявления пароля будут продолжать совершенствоваться.

При безопасном разовом предъявлении пароля протокол по-прежнему запрашивает у объекта(ов) имя пользователя и пароль; однако пользователь может не вводить имя пользователя и пароль, так как они могут быть безопасно сохранены определенным способом (например, посредством системы аутентификации "Керберос").

Следующие требования помогают обеспечить сложность пароля и полезны при проверке и регистрации.

REQ 2: Каждый NE/MS должен проводить **аутентификацию** в соответствии с организационной политикой.

REQ 3: Каждый NE/MS должен поддерживать минимальные требования сложности для **аутентификации** в соответствии с организационной политикой.

REQ 4: NE/MS должен предотвращать попытки изменения зарегистрированного пароля другим пользователем без своего информирования.

REQ 5: Каждый NE/MS должен автоматически обеспечивать, чтобы каждый новый пароль для регистрации отличался от предыдущего пароля. Степень отличия должна конфигурироваться в соответствии с организационной политикой.

Так как в типовом варианте пароли сохраняются посредством одностороннего шифрования, также требуется запись старого пароля, чтобы NE/MS мог определить степень различия старого и нового паролей.

REQ 6: Каждый NE/MS должен обеспечивать предотвращение попыток повторного использования пароля. Параметры предотвращения попыток использования пароля должны конфигурироваться в соответствии с организационной политикой.

REQ 7: Каждый ID пользователя должен иметь свой собственный устанавливаемый пароль для регистрации.

REQ 8: Должна быть обеспечена возможность изменения паролей пользователем по своему усмотрению через минимальный интервал после последнего изменения. Минимальный интервал должен конфигурироваться в соответствии с организационной политикой и устанавливаться **системным администратором безопасности**.

---

[2] В этом пункте не обсуждаются динамические пароли, так как их рассмотрение выходит за рамки данной Рекомендации.

REQ 9: Каждый NE/MS должен поддерживать многоуровневое управление паролем. Некоторые пользователи могут быть заблокированы (например, из-за устаревания пароля или ошибки при регистрации), в то время как некоторые пользователи не могут быть заблокированы.

6.1.2 Варианты аутентификации по умолчанию

Правильное применение паролей по умолчанию детально обсуждалось в литературе по безопасности. Исторически, пароли по умолчанию варьировались в диапазоне от жестко заданных в программе до паролей по умолчанию, связанных с каждой версией или модернизацией программы. Ниже приводятся требования к **аутентификации** по умолчанию.

REQ 10: Должно применяться одно из следующих требований:

- Программное обеспечение конфигурации должно создавать уникальный пароль инициализации для каждого приложения в новой версии или при модернизации[3] программного обеспечения.
- Если используется пароль по умолчанию, то перед вводом устройства в эксплуатацию система должна потребовать замены пароля по умолчанию на уникальный пароль.
- Если устройство поставлено без пароля или с нулевым паролем, то во время процесса инсталляции перед вводом устройства в эксплуатацию должен быть назначен уникальный пароль.

REQ 11: Системный срок службы паролей для регистрации должен быть конфигурируемым, если эта функциональная возможность также встроена в приложение. По истечении срока службы пароль для регистрации соответствующего приложения должен быть заменен на исходное значение по умолчанию, определенное в REQ 10. Все привилегии на изменение пароля должны быть отменены для всех пользователей, за исключением роли пользователя, которая имеет самый высокий уровень полномочий по безопасности для того или иного варианта системы или приложения.

REQ 12: Значение системного таймера неактивности должно быть конфигурируемым, если эта функциональная возможность также встроена в приложение. Если работа системного таймера неактивности разрешена, то доступ в систему для данного ID пользователя должен быть заблокирован, а процесс регистрации для этого пользователя должен быть запрещен.

REQ 13: Предельное число последовательных неудачных регистраций в системе для данного ID пользователя должно быть конфигурируемым, если эта функциональная возможность также встроена в приложение. Когда достигнуто предельное значение числа последовательных неудачных регистраций в системе для данного ID пользователя, то должен быть запущен системный таймер неактивности, определенный в REQ 12.

6.2 Управляемый доступ и санкционирование

Каждый NE/MS должен поддерживать концепцию "минимальная привилегия" (то есть то или иное лицо должно иметь свою роль и должно быть санкционировано на просмотр данных, изменение данных или на инициирование **действий по управлению** только для тех функций, которые разрешены этой ролью). В данном пункте определяются базовые требования для реализации "минимальной привилегии" посредством надлежащего административного обеспечения безопасности системы.

6.2.1 Административное обеспечение безопасности

Каждый NE/MS должен обеспечить, чтобы только санкционированным пользователям разрешалось управлять ресурсами безопасности системы. Все административные действия связываются с ролями пользователя, и эти роли пользователя назначаются конкретным лицам. Хотя обсуждаются только несколько типов ролей пользователя, могут существовать многие другие роли пользователя с изменяющимися степенями привилегий, особенно в отношении неотложных **действий по управлению** безопасностью. Целью является обеспечение возможности управления критическими ресурсами безопасности только для санкционированных привилегированных пользователей.

REQ 14: Каждый NE/MS должен поддерживать многие определяемые пользователем типы ролей пользователя, а **действия по управлению** могут назначаться каждой роли пользователя.

---

[3] Это аналогично практике, когда для каждого проданного компакт-диска имеется уникальный разрешающий пароль.

Роли пользователя могут образовывать иерархию ролей так, что каждая роль будет иметь различные или меньшие задачи, назначенные таким образом, чтобы они содержали меньшие полномочия, чем более привилегированная роль пользователя. Примером иерархии является такая иерархия, в которой роль пользователя обладает способностью выполнять все **действия по управлению** подобно "привилегированному пользователю" компьютера. Другая роль пользователя поддерживает доступ только для чтения, чтобы осуществлять контроль устройств так, как это делает оператор.

REQ 15: Каждый NE/MS должен поддерживать тип пользователя по умолчанию, который имеет минимальные или ограниченные **действия по управлению**.

REQ 16: Каждый NE/MS должен поддерживать следующие **неотложные действия по административному обеспечению безопасности**, но не ограничиваться ими:

- Определение и назначение привилегий пользователя и группы.
- Ведение записи всех запросов идентификаторов (ID) для регистрации в системе.
- Добавление и удаление идентификаторов (ID) пользователя.
- Запрет и разрешение использования конкретных ID пользователя в качестве ID для регистрации.
- Инициализация и переустановка паролей для регистрации.
- Инициализация и изменение криптографических ключей.
- Установка срока действия паролей для регистрации в системе.
- Установка предельного числа неудачных регистраций в системе для каждого регистрационного ID.
- Отмена блокировки или изменение значения системного таймера блокировки.
- Установка значения системного таймера неактивности.
- Установка конфигурации регистрации безопасности системы и аварийной сигнализации.
- Контроль всех регистрационных записей по безопасности системы.
- Управление процессами регистрации безопасности системы.
- Модернизация программного обеспечения безопасности.
- Завершение любого сеанса пользователя или системы.
- Делегирование полномочий по безопасности конкретным лицам в других ролях.
- Установление требований сложности пароля.

REQ 17: Каждый NE/MS должен поддерживать следующие **действия по управлению** безопасностью приложения, но не ограничиваться ими:

- Определение и назначение новых привилегий пользователя и группы на прикладном уровне.
- Ведение записи всех запросов в отношении регистрационных идентификаторов (ID) для приложения.
- Добавление и удаление пользователей на прикладном уровне.
- Контроль всех регистрационных записей по безопасности приложения.
- Конфигурирование регистрации и аварийных сигналов безопасности приложения.
- Управление процессами регистрации безопасности приложения.
- Завершение сеанса приложения пользователя.

6.2.2 Использование и работа NE/MS

Требования, приведенные в данном пункте, применимы как к удаленному доступу к NE/MS, так и к доступу к NE/MS с консоли. Эти обязательные требования представляют собой базовый набор для NE/MS, который фактически хранит идентификаторы (ID) и пароли пользователя. Многие NE/MS ссылаются на централизованную ACS для хранения идентификаторов и паролей пользователя. Обязательные требования, сформулированные в данной Рекомендации, применимы к NE/MS, если в этих объектах содержатся идентификаторы и пароли пользователя и если идентификаторы и пароли пользователя хранятся в ACS.

REQ 18: NE/MS должен синхронизировать время с помощью заверенного способа (например, версия 3 NTP).

REQ 19: Для NE/MS каждое **действие по управлению** должно быть связано с отдельным санкционированным СЕАНСОМ.

REQ 20: Каждый СЕАНС должен быть организован с помощью надлежащей **аутентификации**, как подробно описывается в требовании REQ 1.

REQ 21: Соединения между NE/MS и ACS для целей переноса данных (имени пользователя и пароля) **аутентификации** должны устанавливаться по **защищенному маршруту**.

REQ 22: NE/MS должен использовать **управление доступом** и разграничения для разрешения, запрета или другого управления доступом пользователя, группы пользователей или удаленной системы к NE/MS и должен обеспечивать функциональные возможности, ограничивающие для пользователей данные, транзакции и оборудование, необходимые для выполнения их ролей. Разрешения на доступ должны включать в себя режимы "только чтение" и "чтение-запись", но не ограничиваться этим.

6.2.3 Процесс регистрации в системе

REQ 23: NE/MS должен поддерживать способность назначения каждому лицу уникального идентификатора (ID) для регистрации в приложении или в системе главного компьютера.

REQ 24: NE/MS должен обладать способностью, при необходимости, автоматически заставлять пользователя изменять свой пароль при первом доступе после создания учетной записи и при первом доступе после сброса пароля.

ПРИМЕЧАНИЕ. – В следующем требовании (REQ 25) идет речь об учете различий при управлении сетевого элемента (NE) по сравнению с системой управления (MS). Для управления сетевых элементов при проведении изменений конфигурации требуется контроль устройства посредством нескольких механизмов, возможно одновременно. В случае MS это не обязательно.

Назначением этого требования является управление возможностью пользователей использовать все доступные ресурсы NE/MS. Эксплуатационный персонал должен настроить NE по умолчанию так, как это требуется для конкретных ситуаций, и должен контролировать и изучать попытки превышения этих пределов, поскольку они могут указывать на дефект в работе или на попытку злонамеренных действий.

REQ 25: NE/MS должен предотвращать, регулировать или ограничивать одновременное активное использование одного и того же ID пользователя, когда это требуется. Число одновременных активных сеансов должно быть конфигурируемым на основе ID пользователя.

REQ 26: Для нормальной работы приложение NE/MS должно учитывать требуемые привилегии доступа **привилегированного пользователя**.

REQ 27: NE/MS должен обладать способностью отображать для пользователя во время начала сеанса, когда это требуется, время и дату последней успешной **аутентификации** данного пользователя.

REQ 28: Ориентированное на потребителя служебное информационное сообщение и предупреждение о недопустимости злоупотреблений должны отображаться на начальном экране ввода до разрешения какого-либо логического доступа. Оборудование должно поддерживать минимальную длину сообщения 1600 знаков. Должно обеспечиваться сообщение по умолчанию.

Ниже приведен пример предупредительной заставки.

```
ВНИМАНИЕ! Данная компьютерная система и сеть являются
ЧАСТНЫМИ и представляют собой СОБСТВЕННОСТЬ фирмы, и доступ
к ним возможен только для санкционированных пользователей.
Несанкционированное использование данной компьютерной
системы или сети строго запрещено и может иметь следствием
судебное преследование, вплоть до наказания служащего,
включая штраф, или прекращение контракта с
поставщиком/службой. Владелец или его агенты могут
контролировать любое действие или связь в компьютерной
системе или сети. Владелец или его агенты могут обращаться
к любой информации, сохраненной в компьютерной системе или
сети. При доступе к этой компьютерной системе или сети или
пользовании ею Вы даете согласие на такой контроль и
обращение к информации для целей судебного расследования
```

или других целей. Пользователи не должны ожидать конфиденциальности какой-либо связи или информации, хранящейся в компьютерной системе или сети, включая информацию, хранящуюся локально или дистанционно на жестком диске или на другом носителе информации, используемом в этой компьютерной системе или сети.

Рекомендуется, чтобы каждый объект создал подходящую предупредительную заставку.

REQ 29: О каждой неудачной попытке регистрации пользователю следует сообщать только то, что процесс регистрации неуспешен или недействителен. Такая информация, как "недействительный ID пользователя" или "недействительный пароль", не должна сообщаться.

REQ 30: NE/MS должен **заблокировать** регистрацию учетной записи пользователя после достижения устанавливаемого порогового числа неудачных регистраций. **Блокировка** должна охватывать интерфейс консоли. **Блокировка** НЕ должна распространяться на исходную учетную запись по умолчанию, которая поддерживает все действия по управлению.

REQ 31: NE/MS НЕ должен иметь механизма для обхода **аутентификации** регистрации и текущих процессов регистрации.

REQ 32: Никакой NE/MS не должен когда-либо отображать открытым текстом удостоверяющую информацию, как, например, пароль, на любом носителе, включая отображение на экранах терминалов, вывод на печать и сохранение в регистрационных записях.

REQ 33: NE/MS должен ограничивать срок действия пароля порогом с перестраиваемой конфигурацией.

Общей и приемлемой реализацией REQ 33 для системы является немедленное требование от пользователя установить новый пароль после аутентификации пользователя при помощи старого пароля. В качестве альтернативного варианта, система может потребовать от администратора надлежащим образом изменить пароль. Если учетная запись не использовалась в течение определенного периода, она считается неактивной.

REQ 34: Если время существования пароля для регистрации превысил предельный срок для системы, тогда NE/MS должен **заблокировать** регистрацию для этого ID пользователя до тех пор, пока пароль не будет изменен надлежащим образом.

REQ 35: Если учетная запись не использовалась в течение перестраиваемого порогового периода времени, то каждый NE/MS должен генерировать предупреждение.

REQ 36: Если учетная запись не использовалась в течение перестраиваемого порогового периода времени, то NE/MS должен запретить учетную запись после генерации предупреждения "запретить". Процесс ЗАПРЕЩЕНИЯ НЕ должен распространяться на учетную запись **системного администратора**, на учетную запись **системного администратора безопасности** и на учетную запись **привилегированного пользователя**.

REQ 37: Чтобы повторно разрешить использование **запрещенного** ID для регистрации, требуется надлежащим образом зарегистрированный в системе администратор с назначенными неотложными действиями по административному обеспечению безопасности для инициализации и сброса регистрационных паролей.

Опции для повторного разрешения на использование регистрационных идентификаторов могут быть сконфигурированы как общесистемный параметр на уровне роли.

REQ 38: Для сброса регистрационного ЗАБЛОКИРОВАННОГО ID и для отмены состояния **блокировка** требуется надлежащим образом зарегистрированный в системе администратор с назначенными неотложными действиями по административному обеспечению безопасности для отмены блокировки или изменения значения таймера "блокировка" системы.

Опции для отмены **блокировки** регистрационных идентификаторов могут быть сконфигурированы как общесистемный параметр на уровне роли.

6.2.4 Процесс прекращения сеанса

REQ 39: Каждый надлежащим образом начатый **сеанс** должен быть прекращен пользователем или при неактивности системы.

REQ 40: NE/MS должен прекратить надлежащим образом начатый **сеанс**, когда время, прошедшее с завершения последней активности для этого **сеанса** превышает конфигурируемое значение системного таймера неактивности.

6.2.5 Приложения

REQ 41: Тип роли пользователя должен оставаться неизменным во время работы какого-либо приложения NE/MS и после прекращения его работы.

Пользователь не должен иметь возможности задействования механизма управляющей последовательности, например, перевода оболочки в режим **привилегированного пользователя**. Или, если приложение выходит из строя, оно не должно оставлять пользователя в другой роли с бóльшим числом привилегий. Для получения другой роли пользователь должен выполнить повторную аутентификацию (повторную регистрацию).

6.3 Защита конфиденциальности

В данном пункте задаются требования к криптографическим алгоритмам и управлению ключами для содействия обеспечения безопасности системы и сети. Для обеспечения как конфиденциальности, так и целостности услуг, как правило, используются симметричные алгоритмы. Обмен ключами для симметричных алгоритмов обычно должен происходить в процессе, тесно связанном с аутентификацией. При поддержке услуг аутентификации и обмена ключами могут использоваться также несимметричные алгоритмы. Методы, используемые для генерации, хранения, распространения, уничтожения и аннулирования этих ключей, имеют первостепенную важность. Кроме того, такие факторы, как длина ключа, выбор ключа и выбор алгоритма, непосредственно влияют на степень безопасности конкретной криптосистемы.

Защищенная аутентификация и конфиденциальность данных базируются на криптографических принципах. Криптография использует специальные алгоритмы, основанные на стандартах и публично доступные, что делает возможным их тщательное исследование и простоту реализации. Криптографическая "сила" зависит как от используемого криптографического алгоритма, так и от размера используемого ключа (то есть сила имеет отношение к количеству времени, требующемуся для обратного определения (то есть нахождения или угадывания) значения(ий) ключа, используемого с конкретным алгоритмом).

Протоколы безопасности (например, IPsec, SSL, SSH) в типовом варианте обеспечивают **аутентификацию**, целостность и конфиденциальность. Расширения безопасности других протоколов, таких как простой сетевой протокол управления, версия 3 (SNMPv3)[4], обобщенная архитектура посредника объектных запросов (CORBA), протокол пограничной маршрутизации (Border Gateway Protocol) и открытый протокол маршрутизации с выбором кратчайшего пути (Open Shortest Path First) разработаны для обеспечения **аутентификации** и целостности. **Защищенная аутентификация** и целостность необходимы между NE/MS, а также там, где, в зависимости от обстоятельств, требуется конфиденциальность.

6.3.1 Симметричные алгоритмы шифрования

Симметричное шифрование или шифрование с секретным ключом, относится к криптографической системе, в которой ключи шифрования и дешифрования 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 безопасных средств или генерироваться внутри (например, на основе совместно используемого секретного корневого ключа), так как знание шифровального ключа подразумевает знание дешифровального ключа и наоборот.

REQ 42: Для всех приложений симметричного шифрования сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.

---

[4] SNMPv3 может также обеспечивать конфиденциальность.

6.3.2 Несимметричные алгоритмы шифрования

Система несимметричного шифрования – это система, в которой шифровальный и дешифровальный ключи связаны между собой, но различны. Один делается открытым, в то время как второй остается секретным. Открытый ключ отличается от частного ключа, и возможный путь получения частного ключа из открытого ключа неизвестен. Открытые ключи свободно распространяются; однако частный ключ всегда остается секретным. Применение несимметричного шифрования обычно ограничивается шифрованием симметричных ключей для обмена ключами и подписанием выборок сообщений для цифровых подписей. При обмене ключами используется открытый ключ получателя, а при подписании выборок сообщений используется частный ключ подписывающего лица.

REQ 43: Для всех приложений несимметричного шифрования сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.

REQ 44: Для всех приложений с обменом ключами сила алгоритма должна быть согласована с национальной, промышленной или организационной политикой.

6.3.3 Управление криптографическими ключами

Правильное управление содержимым криптографических ключей является трудным, зачастую и сложным процессом, так как управление ключами в дополнение к генерации ключей охватывает контроль срока действия, безопасный обмен и безопасную публикацию. Дополнительные правила содержатся в документе IETF RFC 1750, Randomness Recommendations for Security (*Рекомендации по случайной структуре для обеспечения безопасности*).

6.3.4 Связь

Безопасная связь является основой для защиты **плоскости административного управления** в современной сети. В Приложении A обсуждаются архитектуры и протоколы в целях реализации безопасной **связи для управления**. Определенные в этом пункте обязательные требования применимы ко всем интерфейсам СУЭ, как описывается в Рекомендации МСЭ-Т M.3010, *Принципы построения сети управления электросвязью*.

REQ 45: Для каждого физического или логического интерфейса, который переносит какой-либо **трафик управления** в NE/MS, NE/MS должен быть конфигурируемым в целях достижения защищенного **трафика управления** с помощью **строгой аутентификации** и криптографической защиты для обеспечения конфиденциальности, целостности и защиты от воспроизведения.

REQ 46: Какой-либо пароль, переданный открытым текстом, должен передаваться только по **защищенному маршруту**, если не используется механизм одноразового пароля. Если используются одноразовые пароли, то они могут передаваться открытым текстом, пока отсутствует промежуточный хост.

6.4 Защита целостности данных

6.4.1 Алгоритмы обеспечения целостности данных

Для обеспечения целостности данных в сообщениях произвольной длины могут использоваться ключевые алгоритмы выборок сообщений, комбинированные с функциями хэширования.

REQ 47: Для всех симметричных безопасных приложений обеспечения целостности данных сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.

REQ 48: Для всех несимметричных безопасных приложений обеспечения целостности данных сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.

6.4.2 Разработка и доставка NE/MS

Безопасность NE/MS зависит от полного процесса в течение жизненного цикла. Безопасность является проблемой во время концептуального проектирования и остается проблемой во время детального проектирования, разработки, развертывания и вывода продукта из эксплуатации. Крайне важными для обеспечения приемлемых уровней безопасности являются надлежащие контроль и тестирование полного процесса в течение жизненного цикла. В пп. I.5.2 и I.5.3 рассмотрены дополнительные соображения в отношении жизненного цикла.

REQ 49: Все программное обеспечение, поставляемое поставщику услуг или другому клиенту, должно содержать, когда это требуется, криптографическую **аутентификацию** и механизмы защиты целостности, такие как цифровые подписи или симметричная **аутентификация** сообщения, как указано в Рекомендации МСЭ-Т М.3016.3.

REQ 50: Все получаемое программное обеспечение NE/MS должно быть способно интерпретировать криптографическую **аутентификацию** и механизмы защиты целостности и при необходимости проверять источник и целостность программного обеспечения.

REQ 51: Все обновления программного обеспечения, включая заплатки, должны передаваться получающему NE/MS по **защищенному маршруту**.

NE/MS должен быть способен электронным способом определять свои текущие версии программного обеспечения и аппаратуры и проверять достоверность соответствующих конфигураций программного обеспечения/встроенного программного обеспечения.

6.5 Возможность ведения учета

Целью ведения учета является обеспечение того, чтобы любой объект нес ответственность за любые инициируемые им действия.

REQ 52: Все NE/MS должны обеспечивать возможность того, чтобы объект не мог отрицать свою ответственность за любые выполненные им действия, а также за их результаты.

См. также REQ 49 и REQ 50 для ознакомления с требованиями к возможности ведения учета, связанными с разработкой и поставкой NE/MS.

6.6 Регистрация и проверка безопасности

Важно обеспечить каждый NE/MS адекватными возможностями, позволяющими выполнять действия по исследованию, проверке, определению реального времени, анализу и защите с тем, чтобы могли быть предприняты надлежащие корректирующие действия. В этом пункте рассматриваются регистрационные записи проверки безопасности; однако конкретные детали содержимого и формата регистрационных записей безопасности выходят за рамки данной Рекомендации.

Отметим, что действия по изучению и анализу спорных ситуаций могут включать в себя изучения не связанных с безопасностью сообщений OAM&P, а также информации, сохраненной в регистрационных записях проверки безопасности, описываемых в этом пункте. Регистрация не связанных с безопасностью сообщений OAM&P, называемых иногда сообщениями "о последних изменениях", требуется для любых доступных для проверки действий.

REQ 53: NE/MS должен быть способен регистрировать любое действие, которое изменяет атрибуты и услуги безопасности, настройки доступа, параметры конфигурации устройств.

REQ 54: NE/MS должен обеспечивать способность конфигурировать те **неотложные действия по административному обеспечению безопасности**, которые будут включены в регистрационную запись безопасности.

REQ 55: NE/MS должен быть способен регистрировать каждую попытку регистрации и ее результат; каждую отмену регистрации или завершение сеанса (дистанционное или с консоли) и каждую попытку регистрации и ее результат, которые вызывают активизацию системного таймера неактивности, определенного в REQ 12.

Рекомендуется отправлять регистрационные записи проверки на постоянный сервер проверки после выполнения NE/MS присвоения последовательной метки и криптографической аутентификации (подписи).

REQ 56: NE/MS должен обладать способностью дистанционной регистрации по **защищенному маршруту**.

REQ 57: Каждая регистрационная запись должна содержать следующую информацию:

- описание действия или фактического действия, которое регистрируется;
- уровень идентичности и безопасности пользователя или процесса, который инициировал данное действие;
- дата и время состоявшегося действия;
- сетевой источник и информация о пункте назначения, если она применима (например, когда производится вхождение в систему);
- Индикация успеха или неудачи действия.

6.7 Отчет об аварийных сигналах безопасности

Для некоторых событий требуется составлять отчеты об аварийных сигналах безопасности, например, см. REQ 35. Однако определение конкретных событий, о которых требуется составлять отчеты, выходит за рамки данной Рекомендации.

REQ 58: Все NE/MS должны обеспечивать возможность генерирования уведомлений об аварийных сигналах для выбранных событий.

REQ 59: Все NE/MS должны обеспечивать возможность, которая позволяет пользователю определять критерий выбора для событий, генерирующих уведомления об аварийных сигналах.

6.8 Защита DCN

Для защиты инфраструктуры управления и DCN в общем для сетевого оператора представляется полезным осуществлять проверку определенного трафика, получаемого от адресов или передаваемого на адреса вне DCN (например, от равноправных сетей и клиентов), и выполнять действия над этим трафиком. Например, пакеты с адресами IP источника, которые совпадают с адресным пространством DCN, не должны допускаться внутрь DCN от внешних сетей.

REQ 60: Все NE/MS с возможностями соединения на основе пакетов должны не допускать трафик, который не соответствует требованиям политики обеспечения безопасности DCN.

Приложение A

Соответствие требований, услуг и механизмов безопасности

В данном Приложении показано соответствие требований по безопасности услугам безопасности, определенным в Рекомендации МСЭ-Т M.3016.2, и механизмам безопасности, определенным в Рекомендации МСЭ-Т M.3016.3.

Требования по безопасности M.3016.1		Услуги безопасности M.3016.2	Механизмы безопасности M.3016.3
REQ 1:	Для входа в систему, регистрации и проверки NE/MS должна поддерживаться строгая аутентификация.	**SER 1, SER 2, SER 3, SER 8**	**MEC 1-MEC 13**
REQ 2:	Каждый NE/MS должен проводить **аутентификацию** в соответствии с организационной политикой.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 3:	Каждый NE/MS должен поддерживать минимальные требования сложности для **аутентификации** в соответствии с организационной политикой.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 4:	NE/MS должен предотвращать попытки изменения зарегистрированного пароля другим пользователем без своего информирования.	**SER 8**	**MEC 7-MEC 11**
REQ 5:	Каждый NE/MS должен автоматически обеспечивать, чтобы каждый новый пароль для регистрации отличался от предыдущего пароля. Степень отличия должна конфигурироваться в соответствии с организационной политикой.	**SER 1**	**MEC 7-MEC 11**
REQ 6:	Каждый NE/MS должен обеспечивать предотвращение попыток повторного использования пароля. Параметры предотвращения попыток использования пароля должны конфигурироваться в соответствии с организационной политикой.	**SER 1**	**MEC 7-MEC 11**
REQ 7:	Каждый ID пользователя должен иметь свой собственный устанавливаемый пароль для регистрации.	**SER 1**	**MEC 7-MEC 11**

Требования по безопасности M.3016.1		Услуги безопасности M.3016.2	Механизмы безопасности M.3016.3
REQ 8:	Должна быть обеспечена возможность изменения паролей пользователем по своему усмотрению через минимальный интервал после последнего изменения. Минимальный интервал должен конфигурироваться в соответствии с организационной политикой и устанавливаться **системным администратором безопасности**.	**SER 1**	**MEC 7-MEC 11**
REQ 9:	Каждый NE/MS должен поддерживать многоуровневое управление паролем. Некоторые пользователи могут быть заблокированы (например, из-за устаревания пароля или ошибки при регистрации), в то время как некоторые пользователи не могут быть заблокированы.	**SER 1, SER 2, SER 3, SER 4**	**MEC 20-MEC 23**
REQ 10:	Должно применяться одно из следующих требований: • Программное обеспечение конфигурации должно создавать уникальный пароль инициализации для каждого приложения в новой версии или при модернизации программного обеспечения. • Если используется пароль по умолчанию, то перед вводом устройства в эксплуатацию система должна потребовать замены пароля по умолчанию на уникальный пароль. • Если устройство поставлено без пароля или с нулевым паролем, то во время процесса инсталляции перед вводом устройства в эксплуатацию должен быть назначен уникальный пароль.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 11:	Системный срок службы паролей для регистрации должен быть конфигурируемым, если эта функциональная возможность также встроена в приложение. По истечении срока службы пароль для регистрации соответствующего приложения должен быть заменен на исходное значение по умолчанию, определенное в REQ 10. Все привилегии на изменение пароля должны быть отменены для всех пользователей, за исключением роли пользователя, которая имеет самый высокий уровень полномочий по безопасности для того или иного варианта системы или приложения.	**SER 4**	**MEC 7-MEC 11**
REQ 12:	Значение системного таймера неактивности должно быть конфигурируемым, если эта функциональная возможность также встроена в приложение. Если работа системного таймера неактивности разрешена, то доступ в систему для данного ID пользователя должен быть заблокирован, а процесс регистрации для этого пользователя должен быть запрещен.	**SER 4**	**MEC 7-MEC 11**
REQ 13:	Предельное число последовательных неудачных регистраций в системе для данного ID пользователя должно быть конфигурируемым, если эта функциональная возможность также встроена в приложение. Когда достигнуто предельное значение числа последовательных неудачных регистраций в системе для данного ID пользователя, то должен быть запущен системный таймер неактивности, определенный в REQ 12.	**SER 4**	**MEC 7-MEC 11**
REQ 14:	Каждый NE/MS должен поддерживать многие определяемые пользователем типы ролей пользователя, а **действия по управлению** могут назначаться каждой роли пользователя.	**SER 4**	**MEC 20-MEC 23**
REQ 15:	Каждый NE/MS должен поддерживать тип пользователя по умолчанию, который имеет минимальные или ограниченные **действия по управлению**.	**SER 4**	**MEC 20-MEC 23**

Требования по безопасности М.3016.1	Услуги безопасности М.3016.2	Механизмы безопасности М.3016.3
REQ 16: Каждый NE/MS должен поддерживать следующие **неотложные действия по административному обеспечению безопасности**, но не ограничиваться ими: • Определение и назначение привилегий пользователя и группы. • Ведение записи всех запросов идентификаторов (ID) для регистрации в системе. • Добавление и удаление идентификаторов (ID) пользователя. • Запрет и разрешение использования конкретных ID пользователя в качестве ID для регистрации. • Инициализация и переустановка паролей для регистрации. • Инициализация и изменение криптографических ключей. • Установка срока действия паролей для регистрации в системе. • Установка предельного числа неудачных регистраций в системе для каждого регистрационного ID. • Отмена блокировки или изменение значения системного таймера блокировки. • Установка значения системного таймера неактивности. • Установка конфигурации регистрации безопасности системы и аварийной сигнализации. • Контроль всех регистрационных записей по безопасности системы. • Управление процессами регистрации безопасности системы. • Модернизация программного обеспечения безопасности. • Завершение любого сеанса пользователя или системы. • Делегирование полномочий по безопасности конкретным лицам в другие ролях. • Установка требований сложности пароля.	**SER 4, SER 8**	**MEC 20-MEC 23**
REQ 17: Каждый NE/MS должен поддерживать следующие **действия по управлению** безопасностью приложения, но не ограничиваться ими: • Определение и назначение новых привилегий пользователя и группы на прикладном уровне. • Ведение записи всех запросов в отношении регистрационных идентификаторов (ID) для приложения. • Добавление и удаление пользователей на прикладном уровне. • Контроль всех регистрационных записей по безопасности приложения. • Конфигурирование регистрации и аварийных сигналов безопасности приложения. • Управление процессами регистрации безопасности приложения. • Завершение сеанса приложения пользователя.	**SER 4, SER 8**	**MEC 20-MEC 23**
REQ 18: NE/MS должен синхронизировать время с помощью заверенного способа (например, версия 3 NTP).	**SER 8**	**Нет данных**
REQ 19: Для NE/MS каждое **действие по управлению** должно быть связано с отдельным санкционированным СЕАНСОМ.	**SER 4**	**MEC 20-MEC 23**
REQ 20: Каждый СЕАНС должен быть организован с помощью надлежащей **аутентификации**, как подробно описывается в требовании REQ 1.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 12**
REQ 21: Соединения между NE/MS и ACS для целей переноса данных (имени пользователя и пароля) **аутентификации** должны устанавливаться по **защищенному маршруту**.	**SER 5, SER 6**	**MEC 19**

Требования по безопасности M.3016.1		Услуги безопасности M.3016.2	Механизмы безопасности M.3016.3
REQ 22:	NE/MS должен использовать **управление доступом** и разграничения для разрешения, запрета или другого управления доступом пользователя, группы пользователей или удаленной системы к NE/MS и должен обеспечивать функциональные возможности, ограничивающие для пользователей данные, транзакции и оборудование, необходимые для выполнения их ролей. Разрешения на доступ должны включать в себя режимы "только чтение" и "чтение-запись", но не ограничиваться этим.	**SER 4**	**MEC 20-MEC 23**
REQ 23:	NE/MS должен поддерживать способность назначения каждому лицу уникального идентификатора (ID) для регистрации в приложении или в системе главного компьютера.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 24:	NE/MS должен обладать способностью, при необходимости, автоматически заставлять пользователя изменять свой пароль при первом доступе после создания учетной записи и при первом доступе после сброса пароля.	**SER 4**	**MEC 7-MEC 11**
REQ 25:	NE/MS должен предотвращать, регулировать или ограничивать одновременное активное использование одного и того же ID пользователя, когда это требуется. Число одновременных активных сеансов должно быть конфигурируемым на основе ID пользователя.	**SER 1, SER 2, SER 3, SER 4**	**MEC 7-MEC 11**
REQ 26:	Для нормальной работы приложение NE/MS должно учитывать требуемые привилегии доступа **привилегированного пользователя**.	**SER 4**	**MEC 20-MEC 23**
REQ 27:	NE/MS должен обладать способностью отображать для пользователя во время начала сеанса, когда это требуется, время и дату последней успешной **аутентификации** данного пользователя.	**SER 4, SER 8**	**MEC 7-MEC 11**
REQ 28:	Ориентированное на потребителя служебное информационное сообщение и предупреждение о недопустимости злоупотреблений должны отображаться на начальном экране ввода до разрешения какого-либо логического доступа. Оборудование должно поддерживать минимальную длину сообщения 1600 знаков. Должно обеспечиваться сообщение по умолчанию.	**SER 4**	**Нет данных**
REQ 29:	О каждой неудачной попытке регистрации пользователю следует сообщать только то, что процесс регистрации неуспешен или недействителен. Такая информация, как "недействительный ID пользователя" или "недействительный пароль", не должна сообщаться.	**SER 8**	**MEC 7-MEC 11**
REQ 30:	NE/MS должен **заблокировать** регистрацию учетной записи пользователя после достижения устанавливаемого порогового числа неудачных регистраций. **Блокировка** должна охватывать интерфейс консоли. **Блокировка** НЕ должна распространяться на исходную учетную запись по умолчанию, которая поддерживает все действия по управлению.	**SER 4**	**MEC 7-MEC 11**
REQ 31:	NE/MS НЕ должен иметь механизма для обхода **аутентификации** регистрации и текущих процессов регистрации.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 32:	Никакой NE/MS не должен когда-либо отображать открытым текстом удостоверяющую информацию, как, например, пароль, на любом носителе, включая отображение на экранах терминалов, вывод на печать и сохранение в регистрационных записях.	**SER 8**	**MEC 7-MEC 11**
REQ 33:	NE/MS должен ограничивать срок действия пароля порогом с перестраиваемой конфигурацией.	**SER 4**	**MEC 7-MEC 11**
REQ 34:	Если время существования пароля для регистрации превысил предельный срок для системы, тогда NE/MS должен **заблокировать** регистрацию для этого ID пользователя до тех пор, пока пароль не будет изменен надлежащим образом.	**SER 4**	**MEC 7-MEC 11**
REQ 35:	Если учетная запись не использовалась в течение перестраиваемого порогового периода времени, то каждый NE/MS должен генерировать предупреждение.	**SER 4, SER 8, SER 9**	**MEC 7-MEC 11 MEC 33-MEC 37**

Требования по безопасности М.3016.1		Услуги безопасности М.3016.2	Механизмы безопасности М.3016.3
REQ 36:	Если учетная запись не использовалась в течение перестраиваемого порогового периода времени, то NE/MS должен запретить учетную запись после генерации предупреждения "запретить". Процесс ЗАПРЕЩЕНИЯ НЕ должен распространяться на учетную запись **системного администратора**, на учетную запись **системного администратора безопасности** и на учетную запись **привилегированного пользователя**.	**SER 4, SER 8**	**MEC 7-MEC 11 MEC 20-MEC 23**
REQ 37:	Чтобы повторно разрешить использование **запрещенного** ID для регистрации, требуется надлежащим образом зарегистрированный в системе администратор с назначенными неотложными действиями по административному обеспечению безопасности для инициализации и сброса регистрационных паролей.	**SER 4**	**MEC 7-MEC 11 MEC 20-MEC 23**
REQ 38:	Для сброса регистрационного ЗАБЛОКИРОВАННОГО ID и для отмены состояния **блокировка** требуется надлежащим образом зарегистрированный в системе администратор с назначенными неотложными действиями по административному обеспечению безопасности для отмены блокировки или изменения значения таймера "блокировка" системы.	**SER 4**	**MEC 7-MEC 11 MEC 20-MEC 23**
REQ 39:	Каждый надлежащим образом начатый **сеанс** должен быть прекращен пользователем или при неактивности системы.	**SER 4**	**MEC 33-MEC 37**
REQ 40:	NE/MS должен прекратить надлежащим образом начатый **сеанс**, когда время, прошедшее с завершения последней активности для этого **сеанса** превышает конфигурируемое значение системного таймера неактивности.	**SER 4**	**MEC 7-MEC 11**
REQ 41:	Тип роли пользователя должен оставаться неизменным во время работы какого-либо приложения NE/MS и после прекращения его работы.	**SER 4**	**MEC 20-MEC 23**
REQ 42:	Для всех приложений симметричного шифрования сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.	**SER 5, SER 6**	**MEC 24-MEC 26**
REQ 43:	Для всех приложений несимметричного шифрования сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.	**SER 5, SER 6**	**MEC 27-MEC 28**
REQ 44:	Для всех приложений с обменом ключами сила алгоритма должна быть согласована с национальной, промышленной или организационной политикой.	**SER 5, SER 6**	**MEC 38-MEC 40**
REQ 45:	Для каждого физического или логического интерфейса, который переносит какой-либо **трафик управления** в NE/MS, NE/MS должен быть конфигурируемым в целях достижения защищенного **трафика управления** с помощью **строгой аутентификации** и криптографической защиты для обеспечения конфиденциальности, целостности и защиты от воспроизведения.	**SER 2, SER 3, SER 5, SER 6**	**MEC 24-MEC 32**
REQ 46:	Какой-либо пароль, переданный открытым текстом, должен передаваться только по **защищенному маршруту**, если не используется механизм одноразового пароля. Если используются одноразовые пароли, то они могут передаваться открытым текстом, пока отсутствует промежуточный хост.	**SER 1, SER 2, SER 3, SER 5, SER 6**	**MEC 19**
REQ 47:	Для всех симметричных безопасных приложений обеспечения целостности данных сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.	**SER 5**	**MEC 29-MEC 30**
REQ 48:	Для всех несимметричных безопасных приложений обеспечения целостности данных сила алгоритмов должна быть согласована с национальной, промышленной или организационной политикой.	**SER 5**	**MEC 31-MEC 32**

Требования по безопасности M.3016.1		Услуги безопасности M.3016.2	Механизмы безопасности M.3016.3
REQ 49:	Все программное обеспечение, поставляемое поставщику услуг или другому клиенту, должно содержать, когда это требуется, криптографическую **аутентификацию** и механизмы защиты целостности, такие как цифровые подписи или симметричная **аутентификация** сообщения, как указано в Рекомендации МСЭ-Т M.3016.3.	**SER 7**	**MEC 29-MEC 32**
REQ 50:	Все получаемое программное обеспечение NE/MS должно быть способно интерпретировать криптографическую **аутентификацию** и механизмы защиты целостности и при необходимости проверять источник и целостность программного обеспечения.	**SER 7**	**MEC 29-MEC 32**
REQ 51:	Все обновления программного обеспечения, включая заплатки, должны передаваться получающему NE/MS по **защищенному маршруту**.	**SER 5, SER 6**	**MEC 19**
REQ 52:	Все NE/MS должны обеспечивать возможность того, чтобы объект не мог отрицать свою ответственность за любые выполненные им действия, а также за их результаты.	**SER 7**	**MEC 29-MEC 32**
REQ 53:	NE/MS должен быть способен регистрировать любое действие, которое изменяет атрибуты и услуги безопасности, настройки доступа, параметры конфигурации устройств.	**SER 8**	**MEC 33-MEC 37**
REQ 54:	NE/MS должен обеспечивать способность конфигурировать те неотложные **действия по административному обеспечению безопасности**, которые будут включены в регистрационную запись безопасности.	**SER 4**	**MEC 33-MEC 37**
REQ 55:	NE/MS должен быть способен регистрировать каждую попытку регистрации и ее результат; каждую отмену регистрации или завершение сеанса (дистанционное или с консоли) и каждую попытку регистрации и ее результат, которые вызывают активизацию системного таймера неактивности, определенного в REQ 12.	**SER 8**	**MEC 33-MEC 37**
REQ 56:	NE/MS должен обладать способностью дистанционной регистрации по **защищенному маршруту**.	**SER 5, SER 6, SER 8**	**MEC 33-MEC 37 MEC 19**
REQ 57:	Каждая регистрационная запись должна содержать следующую информацию: • описание действия или фактического действия, которое регистрируется; • уровень идентичности и безопасности пользователя или процесса, который инициировал данное действие; • дата и время состоявшегося действия; • сетевой источник и информация о пункте назначения, если она применима (например, когда производится вхождение в систему); • индикация успеха или неудачи действия.	**SER 8**	**MEC 33-MEC 37**
REQ 58:	Все NE/MS должны обеспечивать возможность генерирования уведомлений об аварийных сигналах для выбранных событий.	**SER 9**	**MEC 41**
REQ 59:	Все NE/MS должны обеспечивать возможность, которая позволяет пользователю определять критерий выбора для событий, генерирующих уведомления об аварийных сигналах.	**SER 9**	**MEC 41**
REQ 60:	Все NE/MS с возможностями соединения на основе пакетов должны не допускать трафик, который не соответствует требованиям политики обеспечения безопасности DCN.	**SER 10**	**MEC 42**

Дополнение I

Дополнительные соображения по безопасности

Процедуры обеспечения безопасности, детально описываемые в последующих пунктах, по своему характеру являются учебным материалом. Они выходят за рамки подробных требований, предусматриваемых данной Рекомендацией, но должны приниматься в рассмотрение для обеспечения безопасных систем. В некоторых случаях используется обязательный язык; однако он задается для информационных целей и должен служить только в качестве примера. Протоколы и рекомендации, включенные в данное Дополнение, являются предметом будущих обсуждений и вкладов. Они не представляют собой никаких предложений о включении или исключении содержимого существующих или создаваемых стандартов.

I.1 Возможность применения к функционированию, администрированию, техническому обслуживанию и обеспечению предприятия

Сегодня предприятия вышли за рамки традиционных изолированных сетей предприятия прошлого. Предприятия выросли до многофилиальных организаций, распространившихся на большие географические районы, для которых требуются сетевые соединения экстрасети с клиентами и партнерами по бизнесу. Предприятия должны обеспечивать партнерам и клиентам возможность доступа к внутренним данным и принятия оперативных деловых решений на основе этих данных.

Сети предприятий разрабатываются и управляются самими предприятиями или приобретаются как управляемые сети у поставщика сетевых услуг. Создаваемые поставщиками услуги позволяют предприятию управлять своей частью более широкой сетевой структуры.

По мере прогресса промышленности, требования доступа к данным о неисправностях и о рабочих характеристиках и поддержки возможности конфигурирования разнообразных компонентов сети предприятием-подрядчиком делают необходимым применение на месте надлежащих механизмов обеспечения безопасности. Эти механизмы должны обеспечить надлежащее управление для защиты не только управляемой предприятием сети, но также и собственной внутренней сети поставщика. Внутренняя сеть может быть соединена с этими сетями предприятий и может быть частью инфраструктуры электросвязи. В итоге, требования по безопасности для функционирования, администрирования, технического обслуживания и обеспечения трафиком, охарактеризованные в данном Дополнении, полностью применимы к предприятиям и к сетям поставщика/переносчика услуг.

I.2 Обобщенная архитектура посредника объектных запросов, простой сетевой протокол управления, расширяемый язык разметки текста и простой протокол доступа к объекту

Следующие соображения следует принимать во внимание в отношении безопасности для обобщенной архитектуры посредника объектных запросов (CORBA), простого сетевого протокола управления (SNMP), расширяемого языка разметки текста (XML) и простого протокола доступа к объекту (SOAP). Кроме того, имеются другие протоколы, которые могут также использоваться, как, например, расширяемый протокол обмена блоками. Хотя для этих развиваемых протоколов изменения не предложены, последующее обсуждение может быть использовано для повышения безопасности.

I.2.1 CORBA

Услуга безопасности CORBA содержит функциональные возможности обеспечения безопасности посредством основной аутентификации принципалов (пользователей-людей и объектов), санкционирование доступа принципалов к объектам, проверки безопасности, безопасности связи, невозможности отказа от участия и администрирования. Хотя применение всех этих возможностей может быть излишним для многих приложений. Вместо этого для приложений, по причинам доступности и простоты, могут потребоваться только функциональные возможности обеспечения безопасности связи и аутентификации системного уровня на основе технологии безопасности транспортного уровня (TLS) (и ее предшественника, уровня защищенных гнезд (SSL)). Наконец, для некоторых приложений может не требоваться защита. Поэтому приведенные ниже необязательные требования отражают три возможных варианта выбора:

– Обеспечение защиты не предусмотрено.

– Посредники объектных запросов (ORB) используют TLS (или SSL) для обеспечения безопасности связи и аутентификации системного уровня, которая по существу является обеспечением безопасности "сеанса".

– ORB используют услугу безопасности CORBA для обеспечения безопасности связи, аутентификации, невозможности отказа от участия и ведения списков управления доступом для групп или отдельных лиц, осуществляющих доступ к отдельным объектам и операциям.

Дополнительную информацию о безопасности в структуре CORBA можно найти в Рекомендации МСЭ-Т Q.816, *Услуги СУЭ на базе CORBA,* и Рекомендации МСЭ-Т Q.816.1, *Услуги СУЭ на базе CORBA*: *Расширения для поддержки направленно-гранулированных (course-grained) интерфейсов*.

Если CORBA используется в интерфейсах сетевого элемента/системы управления (NE/MS), то должны применяться механизмы обеспечения безопасности CORBA. Уровень соответствия реализации услуги безопасности CORBA должен быть полным. В последующем обсуждении приводятся руководящие указания относительно безопасности CORBA. Не следует считать это попыткой идентификации стандартов. Когда поставляются продукты или системы, базирующиеся на услуге CORBA, базовыми уровнями безопасности являются следующие уровни:

– Уровень 0: Защита приложения не обеспечивается, и программы не содержат информации о безопасности. Должны обеспечиваться аутентификация, шифрование, целостность данных, санкционирование активизации объекта, данные проверки и администрирование сферы безопасности.
– Уровень 1: Программы могут содержать информацию о безопасности, это означает, что они могут вызывать интерфейс прикладного программирования для доступа к дополнительным услугам, таким как проверка подписей, контроль доступа к объектам и создание записей проверки безопасности.
– Уровень 2: Обеспечивает поддержку цифровых подписей, позволяющих подписывать документы и не дающих возможности отказа от участия при транзакциях. Это важно, в частности, при совместной работе разных организаций, например, при взаимодействии "бизнес–бизнес" или одноранговой структуре сетевого управления.

Спецификация общего защищенного взаимодействия (CSI) определяет стандарты посредством шифрования спецификации для защищенного взаимодействия, когда используется общий протокол между ORB/межсетевой протокол между ORB:

– Уровень 1 CSI: Идентичность инициирующего ответственного лица передается от отправителя к получателю.
– Уровень 2 CSI: Идентичность инициирующего ответственного лица передается от отправителя к получателю, но идентичность может быть делегирована другим объектам, так что другие объекты могут выдавать себя за пользователя.
– Уровень 3 CSI: В дополнение к переносу идентичности атрибуты инициирующего ответственного лица (принципала), переносимые от клиента к цели, могут включать другую информацию санкционирования, такую как принадлежность ролей или групп.

Обязанностями, возложенными на поставщиков, являются:

– быть полностью осведомленными о возможностях безопасности выбранной технологии ORB;
– обеспечивать их соответствие требованиям по безопасности, сформулированным в другом месте данной Рекомендации.

В соответствии со своим названием, CORBA занимается объектами. Безопасность объекта – это предотвращение несанкционированного использования объектов посредством активации набора правил управления доступом. Безопасность CORBA обеспечивает пользователю возможность ведения учета своих действий на объекте или с объектом и обеспечивает доступность объектов.

Безопасность объекта отличается от многих других аспектов безопасности. Часто разработчику не нужно знать подробности обеспечения безопасности, поскольку безопасность применяется на более позднем этапе, в качестве "упаковки". Поэтому некоторые аспекты являются жизненно важными. В CORBA имена могут дублироваться или могут вообще не существовать; могут существовать только номера ссылок. Должна существовать возможность определять политику объекта без знания его имени. Аналогично, должно быть возможным определение политики даже в объектах со многими именами, и политика должна применяться независимо от имени, используемого для защиты объекта.

Типовые объектно-ориентированные системы содержат десятки тысяч объектов, и нецелесообразно ожидать определения безопасности для отдельных объектов. Следовательно, должна существовать возможность группирования объектов и определения политики для группы объектов, имеющих одинаковые требования к защите.

– *Сквозная аутентификация*: CORBA может передавать контекст пользователя другому приложению. Там, где установлены строго доверительные взаимоотношения между этими системами, может оказаться возможным принятие этой информации без дополнительной проверки. Однако там, где другие механизмы не существуют, для безопасности других систем может оказаться необходимой тесная связь с безопасностью CORBA. Очень важна сквозная аутентификация, и имеет смысл проверить, поддерживает ли ее поставщик.
– *Управление доступом*: CORBA поддерживает идею регистрации на основе роли. Системы всегда должны разрабатываться с использованием этой функции, так как это не только сокращает расходы на администрирование, но и упрощает его, что означает меньшую вероятность наличия ошибок в конфигурации.
– *Шифрование*: Использование шифрования внутри CORBA должно удовлетворять требованиям, зафиксированным в данной Рекомендации. Следует полностью использовать функции CORBA для целостности, конфиденциальности и аутентификации источника, в особенности при организации связи в сети любого типа.
– *Административное управление политикой*: Административное управление политикой CORBA отвечает за формирование информации о доменах, пользователях, ролях, политике доступа к объектам, политике защиты сообщений и политике проверки. Должно существовать четкое представление на всем протяжении проектирования обо всех аспектах именования доменов и объектов. Роли должны быть четко определены с целью обеспечения надлежащего распределения функций.

I.2.2 Безопасность протокола SNMP

SNMP – широко используемый метод администрирования разнообразным процессорным оборудованием, предоставляет возможность для:

– получения параметров конфигурации устройства;
– установки параметров конфигурации устройства;
– отправки предупреждений от управляемого устройства к системе централизованного анализа.

Многие развернутые версии SNMP имеют существенные слабые места в системе безопасности. В версиях 1 и 2 пароль (известный как строка общего пользования) передается открытым текстом. Дополнительно, хотя могут производиться проверки действительности адреса межсетевого протокола (IP) клиента, обнаруживаемый с умеренной вероятностью злонамеренный абонент может фальсифицировать адреса IP. Версии 1 и 2 SNMP создают существенное ослабление степени защищенности в нескольких сетях. Поэтому версии 1 и 2 SNMP следует использовать только в крайнем случае. 4-я Исследовательская комиссия МСЭ-Т обсуждает создание двух новых пакетов протоколов:

– SNMPv3 или V2C с TLS посредством протокола управления передачей (нет управления доступом); и
– SNMPv3 с моделью безопасности пользователя посредством протокола дейтаграмм пользователя (в качестве стека с просмотром в прямом направлении).

Там, где развернут SNMP, предпочтительным уровнем является версия 3. Протокол SNMP версии 3 более защищен и должен использоваться во всех новых системах, так как он обеспечивает защиту от изменения данных, нелегального проникновения, переупорядочения следования сообщений и потери конфиденциальности. Для защиты доступа SNMPv3 к NE должны приниматься следующие контрмеры:

– Агент SNMP должен посылать предупреждение администратору, если он получает команду, исходящую из незнакомого источника.
– Для разрешения сообщений SNMP только от санкционированного администратора следует использовать системы управления доступом. Сообщения SNMP от всех других источников должны подавляться и обрабатываться в соответствии с надлежащей политикой обеспечения безопасности. Может оказаться желательным блокировать несанкционированные запросы в устройстве и по периметру сети.
– Не должна использоваться общая строка по умолчанию.
– Должны регистрироваться нарушения доступа и ошибки доступа.
– По умолчанию SNMPv3 использует стандарт шифрования данных; однако могут использоваться более защищенные алгоритмы.

– SNMPv3 должен использоваться по крайней мере с AuthNoPriv, который обеспечивает аутентификацию, но не обеспечивает конфиденциальность транзакций. Предпочтительно использование AuthPriv.
– Должна быть разрешена регистрация агента SNMP.
– Должна быть запрещена любая услуга или возможность, которая явно не требуется, включая протокол SNMP, если это разрешено.

I.2.3 XML

Стандарт XML обеспечивает язык для определения структур данных. Текущий стандарт имеет версию 1.0. Версия 1.1 является рассматриваемым проектом Рекомендации. Организация по совершенствованию стандартов структурированной информации (OASIS) Технического комитета служб безопасности ищет пути расширения функциональных возможностей обеспечения безопасности, используя XML. OASIS работает над завершением языка разметки заявлений системы безопасности (SAML). SAML базируется на четырех положениях:

– *аутентификация* – выпускающий осуществляет аутентификацию объекта;
– *атрибут* – специфический унифицированный идентификатор ресурса или схема расширения, которая определяет атрибут;
– *решение* – отчет о действительности аутентификации; и
– *санкционирование* – субъект имеет разрешение на доступ к ресурсу(ам).

Положения XML должны включать в себя следующее:

– *базовая информация* – уникальный идентификатор или имя положения, обычно включает дату и время создания и временной интервал его действия;
– *заявление* – документ, описывающий использование положения;
– *условие* – положение может подвергаться воздействию условий, которые делают его действительным или недействительным; и
– *совет* – обеспечивает дополнительную информацию, такую как положения, используемые для принятия решения о политике.

I.2.4 SOAP

SOAP 1.1 – это текущая форма рекомендации консорциума "Всемирной паутины" (World Wide Web). SOAP является форматом сообщения, не связанным с конкретным протоколом. В большинстве случаев он использует протокол передачи гипертекста (HTTP), но может использовать другие протоколы, такие как SMTP или протокол передачи файлов (FTP). Когда протокол SOAP используется с HTTP, брандмауэр "видит" SOAP как HTTP и, как правило, разрешает его прохождение. Потенциально SOAP может быть отфильтрован брандмауэром, даже когда SOAP ему неизвестен. Однако эта фильтрация является непростой задачей и чувствительна к ошибкам. Фильтрация является проблемой, так как шифрование может скрыть содержимое и контекст транспортируемых данных (то есть XML), и SOAP не имеет унифицированной схемы адресации или внутренней структуры (то есть заголовки и имена метода являются необязательными).

I.3 Узаконенное электронное наблюдение

Операторы электросвязи должны учитывать следующие соображения по безопасности при реализации узаконенного электронного наблюдения (LAES).

Практика по безопасности для действий LAES должна быть надежной и той же самой, что и для любого критического NE, или системы эксплуатационной поддержки (OSS), или MS, с некоторыми перечисленными ниже исключениями. Эта практика связана с необходимостью обеспечения конфиденциальности действий LAES.

– В действиях LAES участвуют только санкционированные сотрудники.
– Информация LAES, включая идентичность цели, вовлеченный(ые) правоохранительный(ые) орган(ы), содержимое вызова и идентификационную информацию вызова, должна быть защищена от раскрытия несанкционированным персоналом.
– Доступ к командам и процессам LAES должен иметь только санкционированный персонал.
– Должен вестись постоянно обновляемый список персонала, которому разрешены доступ, эксплуатация, администрирование и управление в отношении действий, процессов и процедур LAES.

– Действия, политика и процедуры обеспечения безопасности LAES должны документироваться надлежащим образом и быть доступны для санкционированного персонала.

– Регистрационные записи по безопасности и записи действий, относящиеся к LAES, должны вестись и сохраняться в защищенном оборудовании.

– Для идентификации и аутентификации правоохранительных органов и обработки запросов LAES должен быть реализован строго документируемый процесс.

I.4 Соображения, касающиеся физической безопасности

Для обеспечения физической безопасности должны быть приняты во внимание следующие соображения. При подготовке требований по безопасности важным компонентом является физическая безопасность. В большинстве архитектур безопасности предполагается защита физической среды. Раньше все NE находились в зданиях центральных АТС (CO). В этих зданиях круглосуточно находились сотрудники для управления, обеспечения, администрирования и технического обслуживания этого оборудования. Сотрудники знали друг друга, и посторонние не могли проникнуть в здания, не будучи замеченными и спрошенными ими. Однако, физическая среда в настоящее время совершенно другая. Существует тенденция установки беспроводного оборудования снаружи в незащищенных условиях. Также многие центральные АТС, если не большинство, управляются без обслуживающего персонала, и большую часть времени в них отключается освещение. Дежурный персонал и лица, управляющие с центрального пункта, выполняют задачи плановой модернизации и технического обслуживания. В настоящее время ежедневная круглосуточная охрана объектов является редким исключением. Центральные АТС используются также внешним линейным персоналом в качестве удобного места для встреч и хранения инструментов и оборудования. Далее приведены характеристики защищенного объекта:

– Все приходы и уходы персонала регистрируются, и об этом делаются записи.

– Поставщики и сотрудники других организаций, размещенных на объекте (co-located personnel), проверяется, их приходы и уходы регистрируются, и об этом делаются записи.

– Физический доступ к NE разрешен только для санкционированных сотрудников.

– На сотрудников других организаций, размещенных на объекте, распространяются те же требования к доступу, что и на действующего поставщика услуг.

– Никто из лиц, имеющих право законного физического доступа в здание, не должен получать логический доступ к NE, консолям, оборудованию сетевого доступа OSS без прохождения защитной аутентификации.

– Несанкционированный доступ должен обнаруживаться, и должны своевременно приниматься соответствующие ответные меры.

– Должны обеспечиваться такие службы, как водоснабжение, электроснабжение и электросвязь.

– Объекты наблюдаются посредством случайных посещений охранным персоналом, систем аварийной сигнализации, которые контролируют и регистрируют открывание и закрывание дверей и окон, данные детекторов перемещения и целевых (inferred) детекторов, а также дистанционного видеоконтроля критических мест.

– Содержимое носителей записей и журналов регистрации наблюдения должно документироваться. Объем содержимого может меняться в зависимости от уровня риска.

В следующих пунктах приведена дополнительная информация относительно обеспечения физической безопасности. Подробное описание проблем обеспечения физической безопасности можно найти в документе Национальной системы связи (National Communication System), *Public Switched Network Security Assessment Guidelines*, September 2000.

I.4.1 Физическая безопасность помещений

Организации обычно реализуют различные уровни средств управления доступом в здание в соответствии с важностью имущества, находящегося на объекте. Крупные корпорации часто строят отдельные объекты с высоким уровнем безопасности для особо важных компонентов сети, таких как коммутаторы или центры сбора данных. Важность находящегося в них имущества определяет уровень безопасности. Это определение производится на этапе развертывания и во время анализа оценки имущества. В следующих пунктах приводятся оцениваемые позиции для объекта, в котором размещается очень ценное или особо важное имущество. Для менее важного оборудования проводится менее детальный анализ. Полная оценка физической безопасности должна определять требуемый уровень защиты и относительное качество защитных механизмов на месте.

I.4.1.1 Обеспечение общей безопасности здания

Хотя двери и окна здания всегда рассматриваются в качестве основных точек доступа, в зависимости от видов угроз должны быть рассмотрены другие точки (например, вентиляционные отверстия, места ввода для воды, газа, связи и электричества и дренажные каналы). В качестве дополнительных точек входа должны рассматриваться кабельные шахты центральных АТС, а также и другие места, где существует потенциальная возможность причинения повреждений. Кроме того, должно рассматриваться буферное пространство снаружи вокруг самого здания. Газоны, ландшафт, освещение и ограждения могут вносить вклад в первый уровень защиты периметра, так как они могут сдерживать попытки доступа или препятствовать им. Для предотвращения попыток въезда легковых и грузовых автомобилей или других транспортных средств с потенциальным намерением разрушения могут использоваться физические препятствия, такие как бетонные столбы или большие ландшафтные бетонные плиты. Наружные видеокамеры и наблюдательное оборудование дополнительно усиливают или расширяют это буферное пространство.

I.4.1.2 Охрана, замки и идентификационные знаки

Охрана здания защищает внешний периметр, а иногда и внутренние зоны. Для особо важных объектов анализ должен обеспечить следующее:

– Все двери, дающие доступ к объекту, должны быть постоянно закрыты на замок или охраняться.

– Любые двери, которые обычно не используются, такие как аварийные выходы, оборудуются аварийной сигнализацией. Проведенный анализ должен обеспечить правильное функционирование аварийной сигнализации и наличие процедур реагирования на аварийные сигналы.

– Двери устанавливаются надлежащим образом так, чтобы они не могли быть удалены с наружной стороны (например, дверные петли и болты защищены от воздействия снаружи).

– Во время пиковых периодов входа и выхода сотрудников на входах и выходах должна присутствовать охрана. В остальное время двери должны контролироваться, и следует использовать некоторые другие существующие формы управления доступом (например, карточки для считывающих устройств, карточки бесконтактного считывания и ключи).

– Для доступа через неохраняемые двери используется метод запроса идентификации входящего.

– Неохраняемые двери, обеспечивающие доступ с помощью ключей или других средств, содержат механизмы для предотвращения "прохождения хвоста"[5]. Для предотвращения таких попыток доступа могут использоваться ловушки, вращающиеся двери и детекторы или посылка аварийного сигнала в случае такого проникновения.

– Методы определения квалификации при наборе, а также методы обучения и запоминания для нанимаемой охраны являются адекватными и соответствующими. В частности, это важно для подрядных охранных служб, которые широко распространены.

– Сотрудники, местные поставщики, подрядчики и другие санкционированные лица во время пребывания в здании имеют и постоянно держат на виду идентификационные карточки (бэджики).

– Посетителям, не являющимся сотрудниками, выдается временный идентификатор, такой как удостоверение посетителя, и от посетителей требуется, чтобы он был всегда хорошо виден.

– Существуют процедуры и условия, когда посетители могут входить и работать без сопровождающего лица, и условия, когда посетителей должны сопровождать.

– Идентификационные карточки сотрудников содержат цветную фотографию. Фотография должна иметь достаточно большие размеры, чтобы охраннику не нужно было брать карточки в руки, чтобы рассмотреть фотографию. Конструкция карточки должна быть такой, чтобы фотографию нельзя было изменить или заменить. Фотография должна быть достаточно четкой, чтобы охранник мог сравнить ее с лицом владельца карточки.

– На идентификационной карточке четко указывается имя сотрудника и другая идентификационная информация (например, номер, штриховой код).

– На идентификационную карточку наносится метка или указатель, который позволяет отличить сотрудников от не сотрудников, имеющих доступ в здания.

---

[5] "Прохождение хвоста" относится к действию несанкционированного лица, проходящего в дверь, открытую санкционированным лицом.

– Идентификационная карточка имеет срок действия и в максимально возможной степени защищена от изнашивания, повреждения или изменения.

– Идентификационная карточка содержит электронную или магнитную информацию, которая может потребоваться при наличии устройств для считывания карточек.

– Идентификационная карточка может содержать интеллектуальный чип, который хранит дополнительную информацию, такую как биометрические данные или сертификаты X.509.

– Системы аутентификации и выдачи разрешений на использование идентификационной карточки должны быть связаны с центральным каталогом безопасности для возможности немедленного изменения или удаления привилегий доступа.

– При необходимости, идентификационная карточка поддерживает возможность ограничения доступа в некоторые зоны корпоративной территории в противоположность полному доступу.

– На идентификационной карточке имеется адрес, по которому он может быть отправлен без оплаты почтовых расходов в случае ее утери и если она найдена не сотрудником.

– Система безопасности организации или здания может запретить или сделать недействительной любую идентификационную карточку, которая была утеряна или владельцу которой больше не разрешен вход в здание или на корпоративную территорию.

– При увольнении владельца идентификационной карточки то или иное лицо (руководитель, охрана здания, система безопасности организации) отбирает или уничтожает карточку, чтобы не допустить ее незаконное использование.

Охранники не являются единственными сотрудниками, ответственными за обеспечение внутренней безопасности здания. Санкционированные арендаторы часто повышают степень безопасности здания за счет бдительности и пассивного контроля. Путем анализа следует определить, уполномочены ли сотрудники на допуск несанкционированного персонала в контролируемые зоны. Полезным может оказаться проведение теста на проникновение для оценки степени понимания охраной и сотрудниками важности физической безопасности. Участники проведения такого теста могут попытаться пройти тайком, или попытаться "заговорить" охранника и пройти, или попытаться упросить сотрудников обеспечить доступ через неохраняемые входы.

I.4.1.3 Административное управление физическими и логическими ключами

Традиционные физические ключи редко используются на особо важных объектах, так как их трудно инвентаризовать и восстанавливать и они не обеспечивают данные для проверки пользователя. Часто использование физических ключей ограничивается доступом во внутренние части здания, такие как кладовые, комнаты охраны и кабельные шкафы. Однако теперь общепринятым стало использование на многих предприятиях и установках кодовых замков в качестве основного средства для входа в здание или для доступа в особо важные зоны внутри зданий. Если такие замки используются, то важно соблюдать следующие предосторожности:

– Должны существовать процедуры для санкционирования распределения ключей определенным лицам, включая контроль ключей и регистрацию доступа и распределения.

– Ключи должны иметь индивидуальную нумерацию.

– Должна вестись полная инвентаризация ключей и их владельцев и осуществляться их проверка.

– Должны быть определены критерии для замены замков в случае утери ключей.

– Должны проводиться периодические проверки инвентаризации ключей и должны существовать процедуры для устранения выявленных несоответствий.

– Должны существовать процедуры для восстановления ключей, когда доступ больше не требуется или изменились выданные разрешения.

Процедуры для использования логических ключей (например, карточек для бесконтактного считывания) должны оцениваться по тем же критериям. Процедуры восстановления ключей, регистрации входа и выхода и выдачи разрешений при использовании логических ключей упрощаются, так как эти системы имеют централизованное оборудование для использования контроля, выдачи разрешений и запрета ключей. Еще должны быть реализованы процедуры для обеспечения того, чтобы оборудование, ответственное за инвентаризацию ключей, и база данных о выданных разрешениях уведомлялись, когда отдельные лица увольняются или изменяются их требования к доступу. Должна производиться оценка комбинационных замков, особого варианта логических замков, для обеспечения того, чтобы комбинации не могли быть очевидно получены из используемых комбинаций или из записанных комбинаций. Комбинации должны быть изменены, если изменились разрешения на вход.

I.4.1.4 Функциональное разделение объектов и многоуровневое управление доступом

Обеспечение физической безопасности применяется как к внутренним частям здания, так и к внешнему периметру. Доступ во внутренние зоны, которые считаются засекреченным или особо важными с эксплуатационной точки зрения, должен управляться, когда доступ к их содержимому ограничен по какой-либо причине (например, они содержат засекреченные данные, результаты экспериментов или оборудование). В общем случае:

– Особо важное компьютерное и сетевое оборудование должно размещаться в зонах, имеющих отдельные механизмы управления физическим доступом. Доступ должен разрешаться только тем, кому это необходимо.
– Должны быть предусмотрены процедуры для обеспечения того, чтобы информация, являющаяся собственностью фирмы, когда ею не пользуются, сохранялась в защищенных устройствах. Офисы и помещения, где такие материалы обычно хранятся, должны быть заперты. Кабинеты, в которых имеется такая информация, также должны быть заперты.
– Все потенциальные точки доступа к особо важному компьютерному и сетевому оборудованию (например, консоли, рабочие центры) должны управляться способом, соответствующим управлению, осуществляемому над самим объектом.
– Должна вестись запись случаев доступа ко всем таким управляемым зонам.
– Носители данных, хранящие особо важную информацию, должны быть зашифрованы или помещены в запертые зоны ограниченного доступа.
– Физический адрес особо важной системы не должен сообщаться тем, кому не требуется его знать.

Управление внутренними зонами здания может быть улучшено посредством использования системы изолированных ролей и ответственностей. Например, административному персоналу не требуется доступ в компьютерные помещения организации. Также инженерам обычно не требуется доступ в помещение для работы с документами. С помощью проведенного анализ следует оценить, является ли подходящим существующее функциональное разделение. Дополнительно, если степень риска требует этого, может использоваться двойной входной ключ или комбинационные замки.

I.4.2 Службы здания

Функционирование организации находится в критической зависимости от доступности таких служб, как водоснабжение, электроснабжение, электросвязь и удаление отходов.

I.4.2.1 Коммунальные службы (водоснабжение, электроснабжение, электросвязь и удаление отходов)

Без служб водоснабжения, электроснабжения, электросвязи и удаления отходов организация не может работать эффективно, если может работать вообще. Зависимость от этих служб часто недооценивается. При оценке должен быть произведен анализ планируемых реакций организации на перерывы в работе коммунальных служб. Для служб, крайне важных для непрерывного выполнения производственных функций, существенными являются следующие шаги:

– Подача электроэнергии должна быть продублирована и быть географически разделена для предотвращения случайного пропадания электроэнергии.
– Должно быть доступно аварийное электропитание для обеспечения возможности продолжения работы в течение времени, превышающего среднюю продолжительность пропаданий электроэнергии. До исчерпания аварийного источника электропитания должны быть доступны для развертывания источники, генерирующие электроэнергию. (Мобильные генераторы могут быть собственными или взятыми в аренду.)
– Для поддержки продолжения работы особо важных компонентов оборудования должно иметься достаточное хранилище воды (или служба ее доставки).
– Для внешней связи должно иметься активное резервное оборудование или оборудование должно быть достаточно надежным, чтобы работать в кризисной ситуации, как должна работать внутренняя связь. Пропускная способность должна быть достаточной для обработки кризисного трафика.
– Во время кризисных ситуаций должны функционировать туалеты и оборудование очистки, или должны иметься соответствующие временные устройства (как минимум, арендуемые) с быстрой активацией.
– Кондиционирование воздуха для компьютерных помещений и других зон, для которых требуются регулируемые климатические условия, должно резервироваться для предотвращения отказов в работе оборудования или выхода его из строя из-за перегрева.

– Запертые контейнеры для удаления и уничтожения информации, являющейся собственностью фирмы, должны быть легко доступны, где бы такой материал не использовался. В ходе анализа должен быть прослежен путь удаления такого материала, чтобы гарантировать завершение этой процедуры.

Интерес для оценки представляет распределение этих служб внутри зданий. Должна быть произведена оценка общей устойчивости оборудования в случаях перерывов в работе службы от ее начала у поставщиков коммунальных служб до путей распределения внутри здания.

I.4.2.2 Аварийное оборудование

В ходе анализа следует оценить достаточность аварийных средств, таких как средства для обнаружения и тушения пожара, обеспечения требуемых норм электропитания, кондиционирования воздуха, вентиляции, а также другие системы защиты окружающей среды, необходимые для непрерывной работы особо важных систем. Эти системы должны реагировать так, чтобы позволить:

– эвакуировать людей из помещений;

– обеспечить защиту оборудования (как минимум в течение времени до прибытия пожарных команд или других служб);

– сохранить структурную целостность оборудования;

– в максимально возможной степени защитить внутреннее содержимое здания от внешней среды.

Аварийное оборудование необходимо как для устранения последствий "бреши" в системе безопасности, так и последствий аварий и стихийных бедствий, как предлагается в предыдущем пункте.

I.4.2.3 Резервирование транспорта и физическая защита особо важного оборудования

Особо важное оборудование компьютерных систем и систем связи должно быть по возможности географически разнесено без чрезмерного воздействия на эксплуатационные расходы, рабочие характеристики и безопасность. Кроме того, маршрутизация особо важных каналов связи (например, важные межофисные магистрали, каналы сигнализации) должна резервироваться и географически разноситься внутри и вне объекта так, чтобы сигналы связи, в случае необходимости, могли немедленно направляться по физически разнесенным резервным маршрутам. Сети связи, необходимые для поддержания обслуживания, должны быть спроектированы так, чтобы повреждение в одной точке не распространялось широко или не приводило к серьезным сбоям.

I.4.3 Угрозы от окружающей среды и географические угрозы

Должны быть проанализированы критические места расположения объектов для определения любых рисков из-за размещения оборудования в зонах, где оно с определенной вероятностью может подвергаться воздействию стихийных бедствий, серьезных аварий (например, утечки химических веществ, взрывы газопроводов), прерываниям в подаче электроэнергии и связанных с этим проблем. При анализе должны также учитываться воздействия таких простых факторов окружающей среды, как чрезвычайная жара или холод, повреждения от солей и растворов и суровые климатические условия.

Географические проблемы включают в себя реакции местного населения, такие как враждебные акты, быстрота реагирования местных аварийных служб и уровень защиты, обеспечиваемый персоналу на месте и на пути к объекту. Так как действия и мотивации людей изменяются во времени вследствие волнений, политических проблем, религиозных взглядов или других факторов, анализы должны производиться периодически в соответствии с заранее составленным расписанием. Хотя зачастую непрактично отказываться от объектов, где существуют такие риски, может оказаться целесообразным дублировать или переместить особо важные системы и ресурсы, находящиеся на объектах с высокой степенью риска.

Должны быть разработаны планы поддержания непрерывности выполнения производственных функций и восстановления в случае бедствий, ориентированные на проведение ответных мер в случае событий, являющихся следствием этих угроз и проблем. Планы должны включать в себя процедуры выдачи команд, управления и связи, и периодически должно проводиться их тестирование. Планы восстановления функционирования также должны включать условия и контракты, которые могут быть быстро выполнены в случае инцидентов с вредными материалами (HAZMAT). В этих планах должно также учитываться, что полное восстановление безопасной среды может препятствовать нормальному доступу к объекту в течение продолжительного периода времени. Возможно, что при восстановлении потребуется перемещение на резервный объект или наличие обученного и надлежащим образом оснащенного персонала для работы с вредными материалами (HAZMAT) в целях поддержания функционирования объекта в течение некоторого времени.

I.4.4 Процедуры совместного размещения

Совместное размещение относится к ситуациям, которые имеют место, когда предприятие, принадлежащее к нескольким поставщикам, физически является единым зданием. В частности, для целей анализа физической безопасности, предоставление доступа в таких случаях часто означает, что конкуренты (иногда несколько конкурентов) требуют доступа к физическим компонентам и оборудованию главного поставщика. При анализе следует учитывать, что:

– Особо важное оборудование должно быть ограждено физическими препятствиями; однако для сотрудников других организаций, размещающихся на объекте, должны действовать те же требования к доступу, что и для действующего поставщика услуг.

– Должны действовать процедуры распределения ключей, ведения учета и проверок. Должны действовать процессы, обеспечивающие возможность контроля изменений персонала во всех размещенных вместе компаниях.

– Особо важное оборудование и средства не должны привлекать к себе внимания. Традиционный метод четкой маркировки особо важного оборудования и транспортных средств (так называемая "красная маркировка"[6]) становится потенциально опасным в открытой среде и следует избегать его применения.

I.5 Процесс подготовки к эксплуатации

I.5.1 Режимы начальной загрузки, инсталляции и неисправности

Следующие соображения должны быть приняты во внимание для процедур обеспечения безопасности в режимах начальной загрузки, инсталляции и в случаях неисправностей.

Для защиты той или иной реализации объекта от "новой инсталляции" в течение срока службы этой реализации должны быть выполнены несколько отдельных операций. Для решения этих проблем важно начать с понимания угроз в отношении реализации. На эти угрозы даются ссылки в стандарте ANSI T1.233-2004, *Operations, Administration, Maintenance, and Provisioning – Security framework for Telecommunications Management Network Interfaces*, и в стандарте ISO/IEC 10181, *Open Systems Interconnection – Security frameworks for open systems*. Общая возможность соединения с открытыми системами приводит к таким угрозам, как:

– вирусы при начальной загрузке;

– несанкционированный доступ;

– нелегальное проникновение;

– угрозы целостности данных;

– угрозы конфиденциальности;

– отказ в обслуживании (DoS); и

– невозможность отказа от участия.

I.5.2 Процесс введения "заплаток"

Поставщики услуг заключают контракты с поставщиками, которые разрабатывают и обеспечивают как приложение, так и платформу, на которой инсталлировано приложение, или только прикладное программное обеспечение. В последнем случае поставщики услуг инсталлируют программное обеспечение на платформе, которую они предварительно приобрели.

В период между общими выпусками программного обеспечения поставщики разрабатывают "заплатки" для коррекции или модификации операционной системы (OS) или прикладного программного обеспечения, или того и другого. После надлежащего тестирования такая заплатка поставляется поставщику услуг. В некоторых случаях поставщик прикладного программного обеспечения может выпускать заплатки в "пакетах" с предусмотренной контрактом периодичностью. Часто выпуски создаются каждые шесть месяцев.

В общем случае заплатка OS не влияет на способ функционирования приложения; однако так бывает не всегда. Следовательно, в случае выпуска поставщиком платформы той или иной заплатки OS

---

[6] "Красная маркировка" предупреждает обслуживающий персонал, что оборудование является особо важным и следует соблюдать особые предосторожности, чтобы случайно не повредить его.

обязанностью провайдера является проверка совместно с поставщиком приложения того, что созданная заплатка OS не влияет неблагоприятно на работу приложения.

В ситуации, когда поставщик приложения поставляет и приложение и аппаратную платформу, но не является изготовителем оригинального оборудования (OEM) платформы, а заплатка для системы безопасности OS выпущена OEM платформы, поставщик приложения и поставщик услуг обязаны знать о выпуске заплатки для безопасности и своевременно организовать проведение тестирования заплатки, чтобы проверить отсутствие ее неблагоприятного влияния на приложение.

Применению заплаток для безопасности должен быть назначен приоритет при выполнении анализа поставщиком приложения (в течение недель, а не месяцев). В таком случае должна быть организована рутинная процедура, чтобы при обращении провайдера к поставщику приложения относительно заплатки для безопасности поставщик мог быстро произвести надлежащие действия. Кроме того, поставщик должен обеспечить, чтобы инсталляция этой заплатки не повредила ранее инсталлированные заплатки для безопасности.

Если тестирование заплатки для безопасности выявило ее влияние на приложение, то своевременно должны быть предприняты соответствующие корректирующие действия для определения проблемы и выработки планов устранения условия, вызвавшего нарушение работы приложения, и последующего использования заплатки для системы безопасности.

При введении заплаток в OS или в прикладное программное обеспечение должны быть приняты во внимание следующие соображения в плане безопасности.

– Поставщики оборудования или системные интеграторы должны предоставить указания по безопасности и учебные руководства для администраторов, содержащие подробные сведения об OS, функциях и процедурах обеспечения безопасности приложения и процедурах доступа пользователя.
– Должна быть проверена совместимость безопасности OS и других заплаток с приложениями NE и MS.
– Программное обеспечение OS: В рабочих сетевых элементах и в операционной системе платформы управления должны применяться только заплатки, утвержденные OEM.
– Прикладное программное обеспечение по управлению: В рабочем приложении по управлению должны применяться только заплатки, утвержденные поставщиком оригинального приложения по управлению.
– Заплатки, оказывающие сильное влияние, должны распространяться своевременно, а не в рамках регулярного процесса рассылки заплаток.
– Все загрузки или скачивания любого программного обеспечения или данных конфигурации должны быть защищены посредством строгой аутентификации источника данных и строгой защиты целостности. В идеальном случае оба этих вида защиты могли бы обеспечиваться посредством цифровой подписи поставщика программного обеспечения. Кроме того, поставщик программного обеспечения может выбрать шифрование программного обеспечения или данных конфигурации.
– Описание процедур(ы) получения и введения самых последних заплат в системы безопасности для системного и прикладного программного обеспечения, выполняемых в каждом элементе, должно поставляться одновременно с заплаткой.
– Описание процесса тестирования каждой заплатки для безопасности перед утверждением ее передачи поставщику услуг должно поставляться одновременно с заплаткой.
– Уровень обратной совместимости выпусков системного программного обеспечения и выпусков эксплуатационных заплаток для безопасности должен быть определен ко времени поставки.
– Системное программное обеспечение или определенная процедура должны отслеживать примененные заплатки и модернизации. Должна быть обеспечена возможность проверки статуса заплатки и модернизации.

I.5.3 Обеспечение безопасности в течение жизненного цикла

Безопасность продукта или услуги зависит от полного процесса в течение срока службы. Безопасность является проблемой во время концептуальной разработки и остается ею во время подробной разработки, проектирования, развертывания и вывода продукта из эксплуатации. Для продуктов и услуг, работающих с особо важной информацией, безопасность может требоваться даже после вывода продукта или услуги из

эксплуатации. Во время всего жизненного цикла крайне важными для обеспечения приемлемых уровней безопасности является работа соответствующих органов управления, а также выполнение тестирования.

I.5.3.1 Управление персоналом

Фундаментальной проблемой безопасности, которой зачастую не придают значения, является надежность персонала. Весь персонал, имеющий доступ к разработке, проектированию и тестированию должен быть надежным.

– Весь персонал, подрядчики, субподрядчики, консультанты и сотрудники, участвующие в проектировании и тестировании особо важных компонентов программного обеспечения, должны пройти негласную проверку.

I.5.3.2 Осведомленность и обучение вопросам обеспечения безопасности

Весь персонал должен быть информирован о политике и процедурах обеспечения безопасности и о необходимости защиты информационных активов. Зачастую самым слабым звеном в обеспечении безопасности является участвующий в этом человек. Осведомленность и обучение вопросам обеспечения безопасности существенно усилила это слабое звено. Информированность уменьшает число несанкционированных действий, предпринимаемых персоналом; повышается эффективность средств управления защитой; это помогает избежать мошенничества, потерь и неправильного использования вычислительных ресурсов.

– Осведомленность и обучение вопросам обеспечения безопасности должны предусматриваться в отношении всего персонала, включая подрядчиков, субподрядчиков, консультантов и сотрудников.

I.5.3.3 Управление рисками

Управление рисками является основой информационной безопасности. Управление рисками определено как идентификация, анализ, управление и минимизация потерь, связанных с "событием". Основные этапы идентификации риска включают в себя идентификацию фактических угроз, последствий реализованной угрозы, потенциальной частоты появления угрозы и вероятности реализации угрозы. Управление рисками охватывает не только анализ рисков с анализом стоимости и эффективности защитных мер, но также и реализацию, анализ и обслуживание защиты.

Анализ рисков идентифицирует риски и дает обоснование стоимости и эффективности контрмер. Эта информация используется для воздействия на процесс принятия решений на всех этапах срока службы, включая выбор места, проектирование здания и конструктивные решения. Для определения того, гарантирована ли защита, производится определение "ожидания потерь за один год" (ALE). (ALE до реализации защиты) – (ALE после реализации защиты) = уровень защиты. Отметим, что реализация защиты должна включать годовые затраты на работу и обслуживание.

– Анализ рисков должен проводиться для каждого нового продукта или услуги. Этот анализ должен включать составление формального документа, в котором описывается используемый подход и результаты анализа. Как минимум, в отчете должны быть идентифицированы все доступные данные и владелец данных (то есть корпоративный, поставщик услуг сети Интернет), определены количественные или качественные показатели данных или услуги, подвергающейся риску, а также потенциальное влияние угрозы в восходящем и нисходящем потоках на NE или OSS.

I.5.3.4 Требования

– Требования по безопасности должны быть задокументированы для продукта или услуги во время этапа сбора требований.

I.5.3.5 Проектирование

– Требования по безопасности должны быть рассмотрены на этапе проектирования и не добавляться после начала разработки.

– Должен быть выполнен анализ проектирования по вопросам безопасности для обнаружения недостатков проектирования, которые снижают безопасность.

– Все точки доступа в систему должны быть хорошо задокументированы и должны обеспечивать поддержку идентификации и аутентификации.

– НЕ должно допускаться использование служебных запасных дверей или люков, не соответствующих политике обеспечения безопасности.

I.5.3.6 Разделение обязанностей

Функции, являющиеся безопасными в надежной среде, могут создавать слабые места в плане безопасности в ненадежных средах. Например, интерпретатор языка "postscript" был разработан для просмотра документов. Ненадежный документ может использовать функции внутри интерпретатора злонамеренным образом, например, изготавливать копии или удалять файлы.

– Система должна поддерживать как минимум три уровня пользователей: пользователь, системный администратор/оператор и администратор по безопасности.

– Каждая функция должна иметь минимальный уровень привилегий, требуемых для выполнения производственной функции.

I.5.3.7 Реализация

– Перед повторным использованием повторно используемые ресурсы (то есть файлы, память, временная память) должны быть очищены от любой информации.

– Для защищенного программирования разработчики должны использовать самые лучшие используемые в практике методы (то есть такое управление буферами, чтобы исключить случаи переполнений).

– В средах разработки, тестирования и поддержки должны выполняться периодические проверки обеспечения безопасности.

– Среды разработки не должны использоваться для работ, не относящихся к компании.

– Программное обеспечение общего пользования не должно импортироваться, использоваться или распространяться для применения при разработках, тестировании или в системах поддержки, если оно не доступно в исходном коде и если исходный код был проверен на наличие злонамеренного кода.

I.5.3.8 Документация

– Там, где это требуется, на документацию должны быть нанесены фирменные маркировочные знаки.

– В документации конечного пользователя должны быть описаны функциональные возможности обеспечения безопасности, которые не прозрачны для пользователя, объяснены их функции и приведены руководящие указания по использованию.

– Руководство системного администратора должно включать в себя следующее:

  • предупреждения относительно функций и привилегий, которые требуют управления при работе в защищенном режиме;

  • документ об использовании функций проверки;

  • процедуры для проведения экспертизы и ведения регистрационных записей проверки;

  • подробные структуры регистрационной записи проверки;

  • процедуры для резервирования и удаления регистрационных записей проверки;

  • процедуры для контроля свободного места, доступного для регистрационных записей проверки.

I.5.3.9 Операционная система

Операционная система (OS) должна обладать способностью обеспечивать эффективные средства управления аппаратным и программным обеспечением для создания защиты, достаточной для управляемых данных и ресурсов. Для предложенной архитектуры безопасности предполагается, что OS обеспечивает уровень безопасности, необходимый для управляемых данных и ресурсов. Может потребоваться анализ этого предложения для конкретных потребностей поставщика услуг. Если OS не обеспечивает потребностей в обеспечении защиты поставщика услуг безопасности, то может потребоваться инсталлировать программное обеспечение в другой OS, которая поддерживает более высокий уровень безопасности.

– В OS должны быть инсталлированы надлежащие заплатки для системы безопасности.

– Должна быть установлена защищенная конфигурация OS, и она должна поставляться с конфигурацией привилегий доступа при ограниченной безопасности. Существуют несколько документов и Web-сайтов, где обсуждается безопасность OS. Хотя перечисление их выходит за

рамки данной Рекомендации, некоторые примеры включают в себя общие критерии и профили защиты OS[7, 8, 9].

– Разрешается только минимум услуг, которые требуются для функционирования по умолчанию.

I.5.3.10 Разработка программного обеспечения

Обеспечение безопасности является неотъемлемой частью разработки компьютерных программ. Для разработки защищенного продукта должны использоваться методы защищенного программирования и защищенные протоколы. Незащищенные методы программирования могут нейтрализовать самые лучшие протоколы и механизмы обеспечения безопасности. Например, если программист не управляет правильно буферами, может возникнуть переполнение буфера, и пользователю будет предоставлена большая привилегия, чем это требуется.

– Поставщики должны следовать формальным документированным процессам разработки, таким как "Модель зрелости процессов разработки" (Capability Maturity Model), разработанная Институтом техники программного обеспечения (Software Engineering Institute). Для проектирования, разработки, тестирования и распространения программного обеспечения должны использоваться наилучшие используемые в практике методы защищенного программирования.

I.5.3.11 Доступность и рабочие характеристики

Доступность и рабочие характеристики являются неотъемлемой частью защищенной системы. Рабочие характеристики могут ухудшиться до уровня, когда систему нельзя больше использовать.

– Проектирование, разработка и реализация должны минимизировать воздействия от атаки "отказ от обслуживания" (DoS).

– Проектирование, разработка и реализация должны обеспечивать высокую доступность.

– Архитектура и реализация сети не должны иметь ни одной точки сбоя.

I.5.3.12 Системное программное обеспечение

Программное обеспечение, используемое для управления и обслуживания компьютерных систем (OS, утилиты и MS), должно иметь возможность защищенного конфигурирования и обслуживания. Для гарантии того, что компоненты и параметры обеспечения безопасности были надежно реализованы и правильно сконфигурированы, должно быть проведено тестирование.

– Системное программное обеспечение и промежуточное программное обеспечение должны быть безопасно инсталлированы и сконфигурированы, включая инсталляцию заплаток для системы безопасности. Программное обеспечение должно поставляться с конфигурацией привилегий доступа при ограниченной безопасности.

I.5.3.13 Передача

– Опция обеспечения защищенной передачи данных должна быть доступна для использования по усмотрению поставщика услуг. Опции защищенной передачи должны быть доступны как для передачи "клиент–сервер", так и для передачи "система–система".

I.5.3.14 Безопасное хранение

– Должны обеспечиваться конфигурируемые поставщиком услуг опции безопасного хранения данных. Поставщик услуг должен иметь возможность указывать, какие области данных хранятся в безопасном режиме.

I.5.3.15 Гарантирование работы программного обеспечения

Гарантирование работы программного обеспечения должно рассматриваться по двум направлениям: тестирование параметров обеспечения безопасности и тестирование потенциальных нарушений политики обеспечения безопасности.

– Обязанности должны быть разделены между группами разработки программного обеспечения и группами тестирования программного обеспечения.

– План тестирования безопасности, тестовые процедуры и результаты должны документироваться.

---

[7] Общий критерий становится международно признанным стандартом для формальной оценки безопасности (http://www.commoncriteria.org/).

[8] Профили защиты операционной системы форума "Техническая структура информационной гарантии", http://www.iatf.net/protection_profiles/operating_systems.cfm.

[9] Национальный институт стандартов и технологии, Центр ресурсов компьютерной безопасности, http://csrc.nist.gov/.

– Должны тестироваться все параметры обеспечения безопасности.

– Тесты должны включать попытки обнаружения нарушений политики обеспечения безопасности (то есть слабые места, такие как управление доступом).

– В качестве части тестирования должна быть проведена проверка того, что вновь разработанная система или приложение не создает уязвимостей в существующих структурах, общих сетях и системах.

– Должна быть выполнена проверка методов защищенного программирования. Проверка может быть произведена путем анализа кода или с помощью программных средств.

– Все нарушения безопасности должны быть исправлены, устранены или нейтрализованы, и должно быть проведено повторное тестирование системы.

I.5.3.16 Упаковка и доставка

В течение срока службы продукта должна использоваться система управления конфигурацией программного обеспечения, реализующая управление изменениями исходного кода и документации.

– Разработчики не должны обслуживать систему управления конфигурацией программного обеспечения.

– Разработчики не должны иметь доступа к производственным системам, за исключением регулируемых положений об аварийных ситуациях, которые утверждаются и регистрируются.

– К поставляемой базе источника должны добавляться только санкционированные код и модификации кода.

– Все изменения должны документироваться и анализироваться.

– Должны существовать средства или процедуры для генерации новой версии системы из исходного кода.

– Должны существовать средства или процедуры для защиты исходного кода от несанкционированных изменений.

– Должны существовать средства или процедуры для проверки подходящих версий и уровней компонентных модулей источника, которые были использованы.

– Продукт должен содержать такие механизмы обеспечения целостности, чтобы можно было проверять совместимость инсталлированного программного обеспечения с поставляемым программным обеспечением (то есть отсутствие каких-либо несанкционированных изменений).

– Там, где имеются средства механизированного сканирования, после модернизаций или других существенных изменений OS или прикладного программного обеспечения, должно быть проведено сканирование уязвимости.

– Должны своевременно обеспечиваться способы устранения или "фиксации" нарушений безопасности, причем они должны соответствовать угрозе.

– Должна существовать главная база данных, содержащая копии всего поставленного программного обеспечения. Программное обеспечение должно иметь номер выпуска и спецификации соответствующих OS и аппаратных средств.

I.5.3.17 Защищенная инсталляция, конфигурация и работа

– Для программного обеспечения должны быть определены параметры защищенной конфигурации.

– Для программного обеспечения должны быть определены и задокументированы защищенные рабочие процедуры.

– Вся дистанционная поддержка программного обеспечения должна осуществляться безопасным способом.

– Все поставляемые с системой идентификаторы пользователя (ID) по умолчанию должны поставляться в неактивном состоянии, которое для использования требует явного действия инсталлятора администратора/программного обеспечения.

– Все процессы инсталляции должны быть защищены и не должны полагаться на доверительные взаимоотношения (т. е. общие дисководы).

Дополнение II

Структура и указания по проектированию

II.1 Структура и модель

В контексте настоящей Рекомендации обеспечение безопасности какого-либо объекта означает его защиту (то есть защита компьютеров, сетей, данных или других ресурсов) от несанкционированного доступа, использования или действия. Потеря данных, отказ в обслуживании (DoS) и хищение услуги – это только некоторые из результатов инцидентов в сфере безопасности. Системным и сетевым администраторам необходимо защищать системы и их составные элементы от внутренних и внешних пользователей и от злоумышленников. Хотя безопасность является многосторонним понятием (безопасность основных операций, физическая безопасность, безопасность связи, обработки и персонала), здесь рассматриваются проблемы обеспечения безопасности, возникающие из-за наличия слабых мест в используемых конфигурациях и технологиях. Угрозы включают в себя (но не ограничиваются этим) раскрытие информации, несанкционированное использование, изменения информационных элементов и отказ в обслуживании. В таблице II.1 перечислены некоторые угрозы безопасности.

Таблица II.1/M.3016.1 – Угрозы

Категория угрозы (Примечание)	**Примеры угроз**
Несанкционированный доступ	Хакерство Несанкционированный доступ в систему для проведения атак Хищение услуги
Нелегальное проникновение	Повторная передача сеанса Перехват сеанса "Посреднические" атаки
Угрозы целостности системы	Несанкционированная обработка файлов конфигурации системы Несанкционированная обработка системных данных
Угрозы целостности связи	Несанкционированная обработка данных при их транзите
Угрозы конфиденциальности	Подслушивание Запись и перехват сеансов связи Нарушения секретности
Отказ в обслуживании	Поток комбинаций SYN протокола управления передачей (TCP) Атаки посредством ложных пакетов Распределенный отказ в обслуживании (DoS)
ПРИМЕЧАНИЕ. – Взято из стандарта Американского национального института стандартов T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces* и стандарта Международной организации по стандартизации (ISO) 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*	

Эти угрозы безопасности могут быть минимизированы или уменьшены в сетевой системе, или в платформе NE, или в приложении путем включения услуг безопасности (как определено в стандарте ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*) для реализации следующего:

– идентификация и **аутентификация**;

– санкционирование и уровень **управления доступом**;

– целостность данных;

– секретность и конфиденциальность;

– невозможность отказа от участия.

Настоящая Рекомендация посвящена безопасности для плоскости административного управления, то есть параметрам безопасности для обеспечения того, чтобы административное управление и оперативное управление сетью могли осуществляться безопасным способом. Некоторая уязвимость все же может иметь место, даже после выполнения положений, содержащихся в данной Рекомендации. Следующие риски относятся к тем, для которых возможно достижение компромисса в плоскости административного управления:

– Несоответствующие действия санкционированных пользователей или злоумышленников. Эти действия могут быть злонамеренными или случайными.

– Перекрытие с плоскостью оперативного управления (например, протоколы сигнализации, маршрутизации, именования и обнаружения).

– Влияние слабых мест в определенных протоколах.

– Злонамеренные программы (например, вирусы, "Троянские кони", черви или другой встроенный код). Достигнув успешного компромисса с каким-либо NE/MS, злонамеренная программа может использовать защищенные каналы связи сети для передачи атак на другие компоненты NE/MS. Эти атаки могут продолжаться до тех пор, пока диспетчеры сети не обнаружат атаку и не предпримут действия для ее ликвидации.

Настоящая Рекомендация посвящена защите трафика управления, особенно в тех случаях, когда он передается по сетям совместно с трафиком конечных пользователей. На рисунке II.1 показана эталонная модель, которая используется для принятия решений по обеспечению безопасности сетевого управления. Эта модель используется для изучения логических маршрутов связи внутри всей сети и определения протоколов, которые применяются для связи на каждом маршруте. Используя эту модель, можно выявить угрозы и слабые места для каждого маршрута и применить для них надлежащие механизмы обеспечения безопасности.

В нижней части модели на рисунке II.1 показаны NE многих поставщиков. EMS, обеспечивающие определенные функции управления для конкретного NE, расположены выше NE. Сама система сетевого управления (NMS) помещена в верхней части модели. NMS обеспечивает все функции управления NE и EMS и содержит конкретные приложения управления услугами и приложения управления производственными операциями, такие как системы конфигурации и выставления счетов. В модели показаны также удаленные и местные операторы и маршруты связи со всеми другими системными элементами.

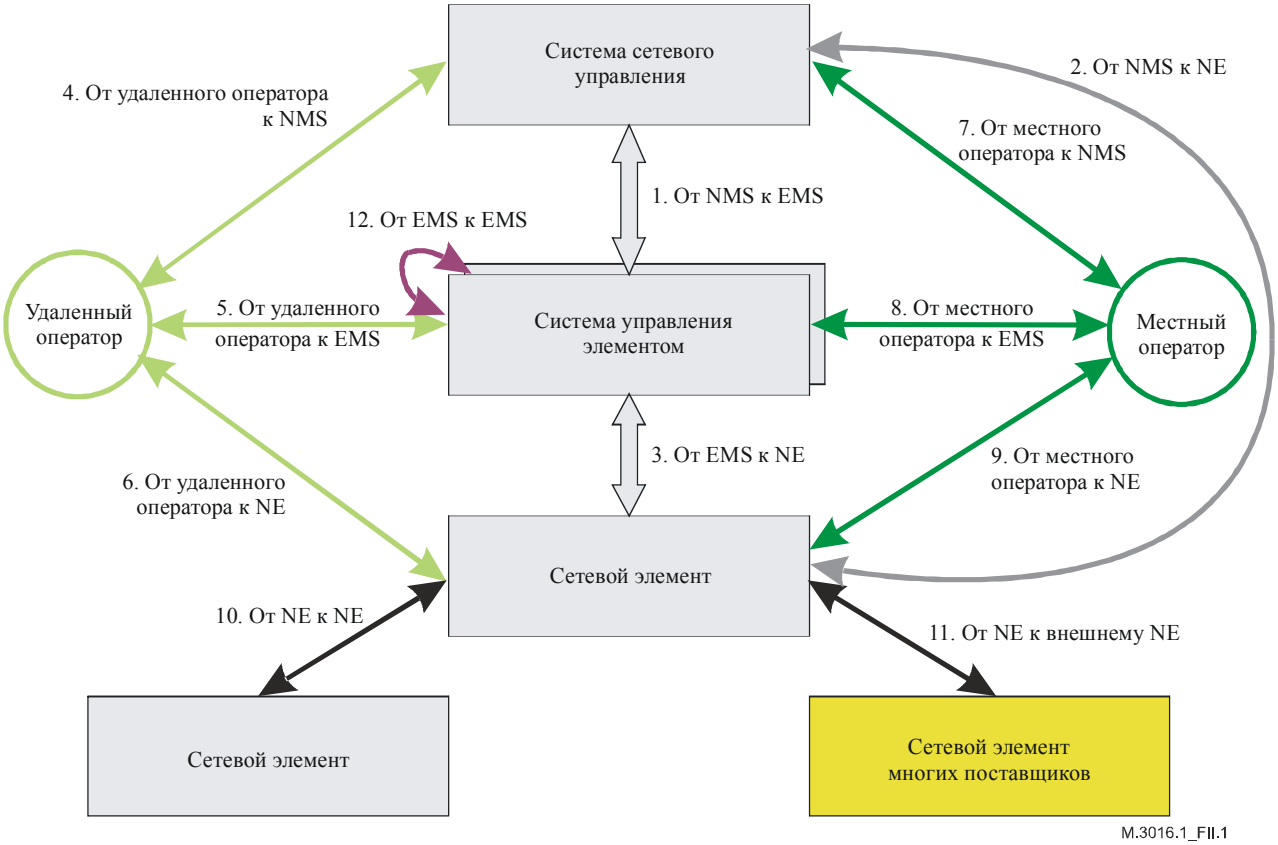

Рисунок II.1/M.3016.1 – Эталонная модель обеспечения безопасности сетевого управления

Эталонная модель обеспечения безопасности (рисунок II.1) может быть полезна также при определении взаимосвязи интерфейсов, определяемых сетью управления электросвязью (СУЭ), с моделью обеспечения безопасности. Сеть СЭУ определена в Рекомендации МСЭ-Т M.3010, *Принципы построения сети управления электросвязью*. Она определяется как архитектура для управления, включающего планирование, обеспечение, инсталляцию, техническое обслуживание, эксплуатацию и администрирование оборудования, сетей и услуг электросвязи.

II.2 Руководящие указания по проектированию

В таблице II.2 представлены задачи рекомендаций по проектированию, посредством которых предпринимается попытка выполнения требований пункта 6 по ослаблению угроз, приведенных в таблице II.1.

Таблица II.2/M.3016.1 – Рассмотренные направления по проектированию

Направление	Описание
Изоляция	Изоляция трафика управления от трафика пользователей.
Эффективная политика обеспечения безопасности	Требования и поддерживаемые архитектуры должны предусматривать политику, которая является определяемой, гибкой, осуществимой, проверяемой, верифицируемой, надежной и практичной.
Строгая **аутентификация**, санкционирование и учет (AAA)	Надежный учет надлежащим образом санкционированных сеансов между аутентифицированными объектами.
Извлечение максимальной пользы при данных затратах	Повышение безопасности посредством реализации механизмов обеспечения безопасности, которые стандартизованы, имеют широко доступные и широко применяемые реализации, что позволяет произвести оценку механизмов безопасности, используя опыт их применения.
Способы усовершенствования	Рассматриваются следующие шаги для повышения и усовершенствования безопасности сетевого управления для дальнейшего удовлетворения заданных требований с использованием развиваемых технологий и механизмов или для выполнения вновь определенных требований по безопасности.

Направление	Описание
Техническая осуществимость	Требования должны удовлетворяться с помощью доступных в настоящее время продуктов, решений и/или технологий.
Действия по обслуживанию	Требования должны быть совместимы со стандартными рабочими процедурами организованных операций сетевого управления.
Открытые стандарты	Использование идей или концепций, которые уже стандартизованы или процесс стандартизации которых осуществляется организациями по стандартизации (например, безопасность межсетевого протокола (IPsec), цифровые подписи). Должны учитываться все аспекты открытых стандартов, включая систему, протоколы, режимы, алгоритм, опцию, размер ключа и кодирование.

Дополнение III

Семантика терминов, используемых в серии M.3016.x

Следующие термины выделяются **жирным шрифтом**, когда они используются в формулировке требования.

III.1 управление доступом: Предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным способом[10].

III.2 сервер управления доступом (ACS): Вспомогательный сетевой элемент, который развертывается для обеспечения и аутентификации доступа к MS на основе **сложных паролей**, если NE не может непосредственно обеспечивать эту функциональную возможность.

III.3 администратор приложения: Роль, отвечающая за правильную активацию, техническое обслуживание и использование приложения NE/MS. Задачи администратора приложения включают в себя модернизацию прикладного программного обеспечения[11].

III.4 администратор по безопасности приложения: Роль, отвечающая за правильную активацию, техническое обслуживание и использование параметров обеспечения безопасности прикладного уровня NE/MS. Представляет собой самый высокий уровень органа по обеспечению безопасности для частного случая приложения NE/MS. Задачи могут включать:

– определение и назначение новых привилегий пользователя и группы на прикладном уровне;

– ведение записи всех запросов к приложению относительно идентификаторов (ID) для регистрации;

– добавление и удаление пользователей на прикладном уровне;

– контроль всех регистрационных записей по безопасности приложения;

– конфигурирование регистрации и аварийных сигналов по безопасности приложения;

– управление процессами регистрации по безопасности приложения;

– завершение сеанса приложения пользователя.

III.5 аутентификация: **Аутентификация** – акт проверки заявленной идентичности.

III.6 сложные пароли: Пароль характеризуется как "сложный", когда он состоит из некоторой комбинации буквенных, цифровых и специальных знаков, что делает трудным или маловероятным раскрытие пароля посредством бытовых приемов или автоматизированных средств.

III.7 плоскость оперативного управления: **Плоскость оперативного управления** выполняет функции управления вызовом и управления соединением. С помощью сигнализации **плоскость**

---

[10] Взято из стандарта ANSI T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces*, раздел 3.1.

[11] Эта задача может быть функцией **системного администратора**, если для ее выполнения необходимы полномочия **привилегированного пользователя**. Могут быть разработаны процессы для управления доступом к учетной записи **привилегированного пользователя**.

оперативного управления устанавливает и отключает соединения и может восстановить соединение в случае его прерывания[12].

III.8 неотложные административные действия по обеспечению безопасности: **Системный администратор безопасности** отвечает за осуществление неотложных административных действий по безопасности, которые делают возможной правильную активацию, техническое обслуживание и использование параметров безопасности системы (NE/MS). **Неотложные административные действия по безопасности** включают (но не ограничиваются этим):

– определение и назначение привилегий пользователя;

– добавление и удаление идентификаторов (ID) пользователя;

– запрет использования конкретных ID пользователя в качестве регистрационного ID;

– инициализация и сброс паролей для регистрации;

– инициализация и изменение криптографических ключей;

– установка системного порога срока действия паролей для регистрации;

– установка системного предельного числа неудачных регистраций для каждого регистрационного ID;

– отмена блокировки или изменение значения системного таймера блокировки;

– установка значения системного таймера неактивности;

– установка конфигурации регистрации и аварийных сигналов для безопасности системы;

– управление процессами регистрации в системе безопасности;

– модернизация программного обеспечения в системе безопасности;

– завершение любого сеанса пользователя или системы.

III.9 запретить/запрещенный: Если данный термин относится к ID пользователя, то это состояние, в котором ID пользователя не может использоваться для регистрации до тех пор, пока ID не будет разрешен посредством конкретного действия от другого ID пользователя с соответствующими привилегиями санкционирования (например, **системный администратор безопасности** или **администратор по безопасности приложения**).

III.10 система управления элементами (EMS): Система, выполняющая функцию OS на уровне управления элементами.

III.11 сила ключа: Различные криптографические алгоритмы имеют разные степени безопасности в зависимости от того, как трудно их раскрыть. Криптографический алгоритм считается сильным, если его нельзя раскрыть с помощью вычислений, то есть он обладает достаточной сложностью, которую нельзя раскрыть в течение "разумного" интервала времени с помощью ресурсов, доступных в настоящее время или в обозримом будущем. Вычислительная сложность наиболее часто измеряется в контексте сложности обработки или количества времени и объема памяти, необходимой для проведения атаки. Хотя сложность атаки остается постоянной для конкретного алгоритма и размера ключа, вычислительные возможности постоянно возрастают. Хорошие криптографические системы проектируются так, чтобы их было невозможно раскрыть с использованием вычислительных мощностей, создание которых ожидается через много лет. Как следствие быстрого развития новых технологий и криптоаналитических методов, правильный размер ключа для конкретного приложения постоянно изменяется.

III.12 блокировка/блокированный: Если данный термин относится к ID пользователя, то это состояние, в котором ID пользователя не может использоваться для регистрации до тех пор, пока состояние блокировки не будет отменено посредством одного или нескольких надлежащих действий. Надлежащие действия включают следующее (но не ограничиваются этим):

– автоматический сброс после истечения порогового периода времени (например, через 60 минут);

---

[12] Рек. МСЭ-Т G.8080/Y.1304, *Архитектура для автоматически коммутируемой оптической сети (ASON)*, ноябрь 2001 г. (имеется в электронном книжном магазине МСЭ).

– автоматический сброс после успешного выполнения предварительно определенного процесса сброса (например, после правильных ответов владельца на подготовленный набор вопросов); или

– сброс посредством определенного действия от другого ID пользователя с соответствующими привилегиями санкционирования (например, **системный администратор безопасности** или **администратор по безопасности приложения**).

III.13 действие по управлению: Действия, которые выполняются **системным администратором** или от его имени.

III.14 связь управления: Любая связь **действия по управлению**.

III.15 плоскость административного управления: **Плоскость административного управления** выполняет функции управления для **транспортной плоскости**, **плоскости оперативного управления** и системы в целом. Она также обеспечивает координацию между всеми этими плоскостями. Функциональные области рабочих характеристик, неисправности, конфигурации, учета и управления по безопасности, определенные в Рекомендации МСЭ-Т M.3010, *Принципы построения сети управления электросвязью,* выполняются в **плоскости административного управления**[13].

III.16 сетевой элемент (NE): См. Рекомендацию МСЭ-Т M.3010.

III.17 система сетевого управления (NMS): Система, выполняющая функцию OS на уровне сетевого управления.

III.18 сетевой элемент/система управления (NE/MS): Общий термин, используемый для описания общности элементов внутри сети электросвязи, включающей NE, EMS, NMS и OSS.

III.19 защищенная аутентификация: Включает **строгую аутентификацию**, **двухфакторную аутентификацию**, **аутентификацию защищенного маршрута**, криптографическую аутентификацию третьей стороны (например, система Керберос) или разовую аутентификацию пароля.

III.20 сеанс: Последовательность операций "машина–машина" или "машина–человек", которые связаны с уникальным процессом или идентификатором (ID) пользователя.

III.21 строгая аутентификация: **Строгая аутентификация** – это **аутентификация**, которая основана на использовании криптографических методов (например, шифрование с открытым ключом, шифрование с симметричным ключом, цифровые подписи и методы цифрового хэширования). **Строгая аутентификация** должна включать в себя двухстороннюю аутентификацию, которая может использоваться для предотвращения активных атак.

III.22 криптостойкое шифрование: Грубая форсированная атака имеет место, когда злоумышленник пытается перебрать все возможные комбинации ключа, используя имеющиеся вычислительные ресурсы, чтобы раскрыть шифрованное сообщение. В этом режиме правильный ключ может быть найден в среднем после перебора половины всех возможных комбинаций ключа. Ожидаемое время проверки половины комбинаций ключа является мерой криптостойкого шифрования. Поэтому в любое заданное время механизмы **криптостойкого шифрования** используют алгоритмы и ключи так, что любому злоумышленнику потребуется более 2 лет для раскрытия с использованием современной технологии.

III.23 системный администратор: Роль, которая отвечает за процессы на уровне OS и процедуры в отношении инсталляции, работы, технического обслуживания операционной платформы, инсталляции программного обеспечения на платформу и управления полномочиями **привилегированного пользователя**. Задачи могут включать:

– координирование инсталляции новой платформы;

– определение и назначение новых привилегий пользователю и группе на уровне OS;

– ведение записи всех запросов к OS для регистрационных идентификаторов (ID);

– добавление и удаление пользователей на уровне OS;

---

[13] Архитектура TMN описывается в Рекомендации МСЭ-Т M.3010, *Принципы построения сети управления электросвязью,* а дополнительные подробности относительно ПЛОСКОСТИ АДМИНИСТРАТИВНОГО УПРАВЛЕНИЯ приведены в Рекомендациях серии M. Рекомендация МСЭ-Т G.8080/Y.1304, *Архитектура для автоматически коммутируемой оптической сети (ASON)*, ноябрь 2001 г. (имеется в электронном книжном магазине МСЭ).

– запрет использования конкретных ID в качестве регистрационных ID (bin, sys, uucp);
– инсталляция модернизаций и заплаток OS;
– инсталляция в OS программного обеспечения приложения и базы данных;
– контроль всех регистрационных записей системы;
– обслуживание и контроль доступа и изменений пароля **привилегированного пользователя**;
– управление доступом к учетной записи **привилегированного пользователя**, позволяющее выполнять надлежащий доступ согласно требованием производственной деятельности;
– процессы регистрации управления системой;
– делегирование полномочий по административному управлению конкретным лицам с другими ролями, включая **администраторов приложения**;
– завершение любого сеанса пользователя или системы.

III.24 Системный администратор безопасности: Роль, отвечающая за правильную активацию, техническое обслуживание и использование параметров безопасности системы NE/MS. Представляет собой самый высокий уровень полномочий по безопасности для частного случая системы/приложения. Задачи могут включать:

– определение и назначение новых привилегий пользователю и группе на уровне OS;
– ведение записи всех запросов к OS для регистрационных идентификаторов (ID);
– добавление и удаление пользователей на уровне OS;
– запрет использования конкретных ID в качестве регистрационных ID (bin, sys, uucp);
– контроль всех регистрационных записей системы;
– инициализация и изменение криптографических ключей;
– установка системного порога срока действия паролей для регистрации;
– установка системного предельного числа неудачных регистраций для каждого регистрационного ID;
– отмена блокировки или изменение значения системного таймера блокировки;
– установка значения системного таймера неактивности;
– конфигурирование регистрации и аварийных сигналов системы;
– управление процессами регистрации по безопасности системы;
– делегирование полномочий по обеспечению безопасности конкретным лицам с другими ролями, включая **администраторов безопасности приложения**;
– завершение любого сеанса пользователя или системы.

III.25 транспортная плоскость: **Транспортная плоскость** обеспечивает двунаправленный или однонаправленный перенос информации пользователя от одного сетевого элемента другому. Она может также обеспечивать перенос некоторой информации управления и сетевого управления. **Транспортная плоскость** содержит уровни; она эквивалентна транспортной сети, определенной в Рекомендации МСЭ-Т G.8080/Y.1304, *Архитектура для автоматически коммутируемой оптической сети (ASON)*[12].

III.26 защищенный маршрут: Механизм, посредством которого системой могут быть защищены любые взаимодействия "пользователь/оператор–система" или "система–система". Этот механизм может быть активирован только пользователем/оператором или системой и не может имитироваться. **Защищенный маршрут** может быть либо выделенным физическим маршрутом (то есть терминал непосредственно подсоединен к системе) или шифрованным маршрутом, который предусматривает целостность и защиту от повторной передачи (например, "защищенная" виртуальная частная сеть, туннель уровня защищенных гнезд (SSL), безопасная оболочка (SSH))[14].

[14] Адаптировано из работы National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*, October 1998 (имеется на сайте http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

III.27 двухфакторная аутентификация: **Двухфакторная аутентификация** – общеиспользуемый термин для описания процесса **аутентификации**, который требует владения физическим объектом (например, жетон или карточка) и знания секрета (например, пароль или идентификационная фраза).

БИБЛИОГРАФИЯ

Документы в этом разделе содержат дополнительную информацию по многим вопросам, рассмотренным в Дополнениях I и II.

– ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance.*

– ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation* (доступно по адресу: ANSI X9 Electronic Standards Store, http://webstore.ansi.org/ansidocstore/ dept.asp?dept_id=80).

– ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)* (доступно по адресу: ANSI X9 Electronic Standards Store, http://webstore. ansi.org/ansidocstore/dept.asp?dept_id=80).

– ANSI T1.210-2004, *OAM&P – Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces.*

– ANSI T1.233-2004, *OAM&P – Security Framework for Telecommunications Management Network (TMN) Interfaces*.

– ANSI T1.252-1996 (R2002), *Operations, Administration, Maintenance and Provisioning OAM&P – Security for the Telecommunications Management Network (TMN) Directory.*

– ANSI T1.261-1998 (R2004), *OAM&P – Security for TMN Management Transactions over the TMN Q3 Interface.*

– ANSI T1.268-2000, *TMN – PKI – Digital Certificates and Certificate Revocation Lists Profile*.

– ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*.

– ATM Forum. AF-SEC-0179.000 (April 2002), *Methods of Securely Managing ATM Network Elements – Implementation Agreements Version 1.1* (доступно по адресу: ftp://ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).

– BARRETT (D.), SILVERMAN (R.): SSH, The Secure Shell: The Definitive Guide, *O'Reilly*, January 2001.

– BELLOVIN (S.): An Issue With DES-CBC When Used Without Strong Integrity, *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, April 1995.

– BLEICHENBACHER (D.): Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, pp. 1-12, 1998.

– BONEH (D.): Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the American Mathematical Society (AMS)*, Vol. 46, No. 2, pp. 203-213, February 1999 (доступно по адресу: http://www.ams.org/notices/199902/boneh.pdf).

– BONEH (D.), JOUX (A.), NGUYEN (P.): Why Textbook RSA and ElGamal Encryption Are Insecure, *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, pp. 30-43, 2000.

– Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, September 1999.

– General Requirements (GR)-815, *Generic Requirements for Network Element/Network System Security*, March 2002 (доступно по адресу: Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GR-1194, *Bellcore Operations Systems Security Requirements*, December 1998 (доступно по адресу: Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GUTMANN (P.): Software Generation of Practically Strong Random Numbers, *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, pp. 243-257, 1998 (доступно по адресу: http://www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/ gutmann.pdf).

– Information Assurance Technical Framework Forum (IATF), http://www.commoncriteria.org/ and http://www.iatf.net/protection_profiles/profiles.cfm.

– IEEE 1363-2000, *IEEE Standard Specifications for Public Key Cryptography* (доступно по адресу: IEEE Standards Online, http://standards.ieee.org/catalog/olis/ busarch.html).

– IETF RFC 768, *User Datagram Protocol*, J. Postel, August 1980 (доступно по адресу: http://www.ietf.org/rfc/rfc0768.txt?number=768).

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification* (доступно по адресу: http://www.ietf.org/rfc/ rfc0791.txt?number=791).

– IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program Protocol Specification* (доступно по адресу: http://www.ietf.org/rfc/rfc0792.txt?number=792).

– IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program Protocol Specification* (доступно по адресу: http://www.ietf.org/rfc/rfc0793.txt?number=793).

– IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware* (доступно по адресу: http://www.ietf.org/rfc/rfc0826.txt?number=826).

– IETF RFC 859 (1983), *Telnet Status Option* (доступно по адресу: http://www.ietf.org/rfc/rfc0859.txt?number=859).

– IETF RFC 959 (1985), *File Transfer Protocol (FTP)* (доступно по адресу: http://www.ietf.org/rfc/rfc0959.txt?number=959).

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP)* (доступно по адресу: http://www.ietf.org/rfc/rfc1157.txt?number=1157).

– IETF RFC 1288 (1991), *The Finger User Information Protocol* (доступно по адресу: http://www.ietf.org/rfc/rfc1288.txt?number=1288).

– IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* (доступно по адресу: http://www.ietf.org/rfc/rfc1905.txt?number=1905).

– IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies* (доступно по адресу: http://www.ietf.org/rfc/rfc2045.txt?number=2045).

– IETF RFC 2202 (1997), *Test Cases for HMAC-MD5 and HMAC-SHA-1* (доступно по адресу: http://www.ietf.org/rfc/rfc2202.txt?number=2202).

– IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)* (доступно по адресу: http://www.ietf.org/rfc/rfc2222.txt?number=2222).

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0* (доступно по адресу: http://www.ietf.org/rfc/rfc2246.txt?number=2246).

– IETF RFC 2271 (1998), *An Architecture for Describing SNMP Management Frameworks* (доступно по адресу: http://www.ietf.org/rfc/rfc2271.txt?number=2271).

– IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (доступно по адресу: http://www.ietf.org/rfc/rfc2272.txt?number=2272).

– IETF RFC 2273 (1998), *SNMPv3 Applications* (доступно по адресу: http://www.ietf.org/rfc/rfc2273.txt?number=2273).

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* (доступно по адресу: http://www.ietf.org/rfc/rfc3414.txt?number=3414).

– IETF RFC 2275 (1998), *View-based Access Control Model for the Simple Network Management Protocol* (*SNMP)* (доступно по адресу: http://www.ietf.org/rfc/rfc2275.txt?number=2275).

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

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

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

– IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms* (доступно по адресу: http://www.ietf.org/rfc/rfc2451.txt?number=2451).

– IETF RFC 2616 (1999), *Hypertext Transfer Protocol (HTTP) – HTTP/1.1* (доступно по адресу: http://www.ietf.org/rfc/rfc2616.txt?number=2616).

– IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method* (доступно по адресу: http://www.ietf.org/rfc/rfc2631.txt?number=2631).

– IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core* (доступно по адресу: http://www.ietf.org/rfc/rfc3080.txt?number=3080).

– IETF RFC 3081 (2001), *Mapping the BEEP Core onto TCP* (доступно по адресу: http://www.ietf.org/rfc/rfc3081.txt?number=3081).

– ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture* (доступно по адресу: ISO Online Store, http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1=35&ICS2=100&ICS3=1).

– ITU-T Recommendation M.3010 (2000), *Principles for a Telecommunications Management Network* (можно приобрести в электронном книжном магазине МСЭ).

– ITU-T Recommendation M.3013 (2000), *Considerations for a Telecommunications Management Network* (можно приобрести в электронном книжном магазине МСЭ).

– JANSEN (W.A.): A Revised Model for Role Based Access Control, *NIST-IR 6192*, July 1998 (доступно по адресу: http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf).

– JONSSON (J.), KALISKI (B.): On the Security of RSA Encryption in TLS, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 127-142, August 2002.

– KELSEY (J.), SCHNEIER (B.), FERGUSON (N.): Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator, *Sixth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1999 (доступно по адресу: http://www.counterpane.com/yarrow-notes.html).

– KRAWCZYK (H.): Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 143-161, August 2002.

– LENSTRA (A.), VERHEUL (E.): Selecting Cryptographic Key Sizes, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.

– National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*. October 1988 (доступно по адресу:http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

– National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000 (доступно по адресу: http://www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification*, *Version 1.8*, March 2002 (доступно по адресу: http://cgi.omg.org/docs/formal/02-03-11.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7,* March 2001 (доступно по адресу: http://cgi.omg.org/docs/formal/01-03-08.pdf).

– Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, September 2001 (доступно по адресу: http://www.pcis.org/library.cfm?urlSection=WG).

– RESCORLA (E.): SSL and TLS, Addison-Wesley, 2001.

– SCHNEIER (Bruce.): Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

– SILVERMAN (R.): The Mythical MIPS Year, *IEEE Computer*, August 1999.

– SILVERMAN (R.): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, *RSA Laboratories Bulletin*, No. 13, April 2000.

– VAUDENAY (S.): Security Flaws Induced by CBC Padding – Applications to SSL, IPsec, WTLS, *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, pp. 534-545, April-May 2002.

– World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, February 1998 (доступно по адресу: http://www.w3.org/TR/1998/REC-xml-19980210).

– World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, May 2000 (доступно по адресу: http://www.w3.org/TR/SOAP/).

– WU (T.): The Secure Remote Password Protocol, *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, pp. 97-111, March 1998 (доступно по адресу: http://www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

– YLÖNEN, T.: SSH – Secure Login Connections Over the Internet, *Sixth USENIX Security Symposium Proceedings*, pp. 37-42, July 1996 (доступно по адресу: http://www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html).

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.