МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т M.3016.2

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2005)

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

Сеть управления электросвязью

Безопасность для плоскости управления: услуги по обеспечению безопасности

Рекомендация МСЭ-Т M.3016.2

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.3016.2

Безопасность для плоскости управления: услуги по обеспечению безопасности

Резюме

В настоящей Рекомендации определяются услуги по обеспечению безопасности для плоскости управления в управлении электросвязью. В частности, внимание в Рекомендации сконцентрировано на аспекте обеспечения безопасности плоскости управления для элементов сети (ЭС) и систем управления (СУ), которые являются частью инфраструктуры электросвязи.

Источник

Рекомендация МСЭ-Т M.3016.2 утверждена 13 апреля 2005 года 4-й Исследовательской комиссией (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 жизненно важная инфраструктура для глобальной связи и экономики. Особое значение имеет надлежащая безопасность для функций управления, контролирующая эту инфраструктуру. Существует множество стандартов для обеспечения безопасности управления сетью электросвязи. Однако они мало соответствуют требованиям, и их внедрение в различное телекоммуникационное оборудование и элементы программного обеспечения недостаточно. В настоящей Рекомендации определяются услуги по обеспечению безопасности, с тем чтобы позволить разработчикам, учреждениям и поставщикам услуг внедрить безопасную инфраструктуру управления электросвязью. Хотя данный набор услуг и механизмов по обеспечению безопасности отражает существующее понимание современного технического уровня, технологии будут развиваться, а условия изменяться. Для обеспечения результативности настоящая Рекомендация должна развиваться по мере создания условий. Эта Рекомендация задумана как основа. Поставщики услуг могут включить дополнительные услуги и механизмы по обеспечению безопасности для удовлетворения их конкретных потребностей в дополнение к представленным в настоящей Рекомендации.

Эта Рекомендация является частью Рекомендаций МСЭ-Т серии M.3016.x, предназначенных для предоставления руководящих указаний и рекомендаций по обеспечению безопасности плоскости управления развивающихся 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.3016.2

Безопасность для плоскости управления: услуги по обеспечению безопасности

1 Область применения

В Рек. МСЭ-Т M.3016.1, M.3016.2 и M.3016.3 задается набор требований, услуг и механизмов для обеспечения надлежащей безопасности функций управления, необходимых для поддержки инфраструктуры электросвязи. Поскольку различным администрациям и организациям требуются разные уровни поддержки обеспечения безопасности, в Рек. МСЭ-Т M.3016.1–M.3016.3 не устанавливается, является ли требование/услуга/механизм обязательным(ой) или необязательным(ой).

В настоящей Рекомендации определяются услуги по обеспечению безопасности для плоскости управления в управлении электросвязью. В частности, внимание в Рекомендации сконцентрировано на аспекте обеспечения безопасности плоскости управления для элементов сети (ЭС) и систем управления (СУ), которые являются частью инфраструктуры электросвязи.

Эта Рекомендация является обобщенной по своему характеру и не занимается выявлением или рассмотрением требований к конкретному интерфейсу сети управления электросвязью (СУЭ).

В настоящей Рекомендации не определяются требования к обеспечению безопасности или механизмы обеспечения безопасности для поддержки требований к услугам по обеспечению безопасности.

Настоящая Рекомендация является частью серии Рекомендаций МСЭ-Т M.3016x. Требования к обеспечению безопасности, механизмы и проформы структуры заданы в других частях серии Рек. МСЭ-Т M.3016x.

Проформа, определенная в Рек. МСЭ-Т M.3016.4, предоставляется для оказания содействия организациям, администрациям и другим национальным/международным организациям, установления обязательной и необязательной поддержки требований, а также диапазонов значений, самих значений и т. п., с тем чтобы помочь внедрению их политики в области обеспечения безопасности.

2 Ссылки

Нижеследующие Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники являются предметом пересмотра; поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания Рекомендаций и других ссылок, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т публикуется регулярно. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

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

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

3 Определения

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

– управление доступом;
– аутентификация;
– конфиденциальность;
– целостность данных;
– неотвергаемость.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

СУ Система управления

ЭС Элемент сети

ЭУОиО Эксплуатация, управление, техническое обслуживание и обеспечение

ВОС Взаимодействие открытых систем

СУЭ Сеть управления электросвязью

5 Условные обозначения

В Рек. МСЭ-Т M.3016.1, M.3016.2 и M.3016.3 используется ключевое слово для установления различных требований, услуг и механизмов. Ключевое слово состоит из одного из приведенных ниже трехбуквенных обозначений, за которым следует номер:

– REQ – для требования;
– SER – для услуги;
– MEC – для механизма.

6 Услуги обеспечения безопасности

На рисунке 1 описывается взаимосвязь между целями обеспечения безопасности, угрозами, рисками, требованиями к обеспечению безопасности и услугами. Рисунок описывает процесс получения "требований к обеспечению безопасности" на основе "угроз" и "целей обеспечения безопасности", которые будут последовательно осуществляться набором услуг по обеспечению безопасности. Эти "услуги", направленные на противодействие угрозам, будут использовать "механизмы", которые, в свою очередь, будут применять "алгоритмы обеспечения безопасности".

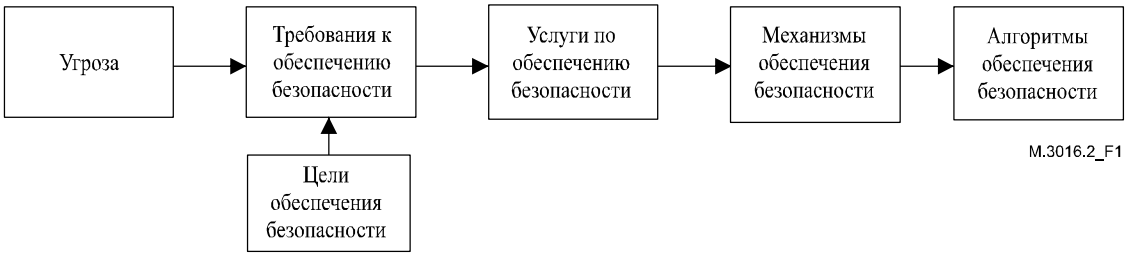

Рисунок 1/M.3016.2 – Структура обеспечения безопасности

Приведенная ниже таблица 1 воспроизведена из Рек. МСЭ-Т M.3016.0 (таблица 4 – из Рек. МСЭ-Т M.3016.0). Эта таблица дает обзор взаимосвязи между требованиями и услугами по обеспечению безопасности и используется в качестве основы для формирования других рекомендаций этой серии. Например, в Рек. МСЭ-Т M.3016.1 обсуждаются функциональные требования к обеспечению безопасности, в настоящей Рекомендации (Рек. МСЭ-Т M.3016.2) обсуждаются услуги по

обеспечению безопасности, и в Рек. МСЭ-Т М.3016.3 обсуждаются конкретные механизмы обеспечения безопасности, соответствующие услугам по обеспечению безопасности.

В этом пункте определяются услуги по обеспечению безопасности, которые обеспечиваются стандартными решениями; другие возможные услуги (например, обнаружение отказа в обслуживании) были исключены.

Таблица 1/М.3016.2 – Отображение требований к обеспечению безопасности и услуг по обеспечению безопасности

Функциональное требование	Услуга по обеспечению безопасности
Идентификационная проверка	аутентификация пользователя аутентификация однорангового объекта аутентификация источника данных
Контролируемые доступ и авторизация	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
Учет действий	неотвергаемость
Регистрация деятельности	контрольный журнал
Аварийная сигнализация в системе безопасности	аварийный сигнал в системе безопасности
Контроль обеспечения безопасности	контрольный журнал
Защита СПД	проверка пакетов

В таблице 2 рассматривается организация этого пункта:

Таблица 2/М.3016.2 – Организация пункта 6

Пункт	Содержание
6.1	Обсуждает услуги аутентификации, включая аутентификацию пользователя, аутентификацию однорангового объекта и аутентификацию источника данных.
6.2	Обсуждает услугу управления доступом.
6.3	Обсуждает услугу обеспечения конфиденциальности данных.
6.4	Обсуждает услугу обеспечения целостности данных.
6.5	Обсуждает услугу обеспечения неотвергаемости.
6.6	Обсуждает услугу контрольного журнала.
6.7	Обсуждает услугу аварийной сигнализации в системе безопасности.

6.1 Аутентификация

СУЭ должна обеспечивать возможность установления и проверки заявленной идентификационной информации любого действующего в СУЭ субъекта.

Действующими субъектами могут быть физические пользователи или объекты в рамках СУЭ. Проверенная идентификационная информация обеспечивает основу для учета действий и носит принципиально важный характер для удовлетворения большинства требований к обеспечению безопасности, перечисленных в этом пункте.

Аутентификация – это услуга по обеспечению безопасности, направленная на поддержку требования. Услуга аутентификации предоставляет доказательство того, что идентификационная информация объекта или субъекта действительно является заявляемой им идентификационной информацией. В зависимости от типа действующего субъекта и цели идентификации могут иметь место следующие виды аутентификации:

– аутентификация пользователя, устанавливающая доказательство подлинности физического пользователя или процесса;

– аутентификация однорангового объекта, устанавливающая доказательство подлинности однорангового объекта в процессе связи;

– аутентификация источника данных, устанавливающая доказательство подлинности, ответственной за конкретную единицу данных.

Использование услуги аутентификации устанавливает доказательство подлинности в определенный момент времени. Постоянное доказательство подлинности обеспечивается путем повторения аутентификации или ее соединения с услугой обеспечения целостности.

Примерами механизмов, используемых для внедрения услуги аутентификации, являются пароли и личные идентификационные номера (ЛИН) (простая аутентификация) и методы, основанные на шифровании (строгая аутентификация).

Аутентификация служит двум целям обеспечения безопасности **плоскости управления**:

1) она гарантирует подлинность сторон, установивших связь, обеспечивая основу для установления частной связи с полной целостностью данных и конфиденциальностью между двумя системами; и

2) она предоставляет основной механизм для случаев регистрации в системе управления и/или контроля за деятельностью по управлению в любой системе.

Данная услуга предоставляется следующими уровнями (согласно Рек. МСЭ-Т X.800):

– сетевым уровнем (удостоверение подлинности одноранговых субъектов транспортного уровня);

– транспортным уровнем (удостоверение подлинности одноранговых субъектов сеансового уровня);

– прикладным уровнем (удостоверение подлинности прикладных процессов);

– внешнее ВОС: в самом прикладном процессе.

Что касается стека ВОС, то учитывая, что требование к СУЭ идентифицирует и аутентифицирует управляющие устройства и исполнительные устройства, а также линию аутентификации с управлением доступом, рекомендуемыми позициями являются прикладной уровень и прикладной процесс.

6.1.1 Аутентификация пользователя

Аутентификация касается **аутентификации** клиентов, участвующих в управлении сетью. В этом случае **аутентификация** удостоверяет подлинность законного пользователя и предотвращает атаки нелегальных пользователей. При правильной **аутентификации** возможно отследить деятельность и ограничить пользователей предварительно санкционированными деятельностью или ролями.

УСЛУГА 1: Каждая СУ/каждый СЭ, обеспечивающая(ий) доступ пользователя, должна/должен поддерживать услугу строгой аутентификации для доказательства подлинности.

Следует отметить, что в этой Рекомендации не требуется предоставление единой услуги по вхождению в систему, но она может быть предусмотрена в будущей рекомендации. Однако, если такая услуга будет внедрена, протокол должен продолжать запрашивать имя пользователя и пароль у объекта(ов). Пользователь может не вводить имя пользователя и пароль, если они надежно закрыты тем или иным способом (например, механизмом Кербероса).

6.1.2 Аутентификация однораногового объекта

Аутентификация однорангового объекта имеет отношение к **аутентификации** однорангового объекта в процессе связи между такими объектами, как приложения, системы или устройства. **Аутентификация** доказывает подлинность однорангового субъекта и предотвращает атаки нелегальных устройств.

Аутентификация одноранговой объекта обеспечивает **аутентификацию** в ходе передачи данных между системами (например, между системами, приложениями) и является основой для установления частной связи с полной целостностью данных. **Аутентификация** в ходе передачи данных позволяет получателю сообщения установить источник сообщения. В канале скрытой связи зашифрованная **аутентификация** должна быть связана с каждым сообщением, с тем чтобы закрепить за сообщением идентификационную информацию объекта-отправителя. Получатель проконтролирует зашифрованную информацию, подаваемую вместе с сообщением, для проверки достоверной идентификационной информации объекта-отправителя.

УСЛУГА 2: Каждая СУ/каждый СЭ, обеспечивающая(ий) передачу данных между системами, должна/должен поддерживать **аутентификацию** одноранговой объекта для связи и должна/должен использовать для **аутентификации** или **защищенной аутентификации** системы на основе сертификата X.509.

6.1.3 Аутентификация источника данных

Аутентификация источника данных касается установления доказательства подлинности системного объекта, заявленного в качестве исходного источника принимаемых данных. Эта **аутентификация** предоставляет доказательное подтверждение заявленного источника данных. Эта услуга обычно связана с услугой обеспечения целостности данных. Эта услуга не зависит от любых взаимосвязей между отправителем и получателем, и данные, о которых идет речь, могли появиться ранее в любое время.

УСЛУГА 3: Каждая СУ/каждый СЭ, обеспечивающая(ий) идентификацию системного объекта с доказательным подтверждением источника данных, должна/должен поддерживать услугу **аутентификации** данных источника.

6.2 Управление доступом

СУЭ должна предоставлять возможности для предотвращения доступа действующих субъектов к информации или ресурсам, доступ к которым для них не санкционирован.

Услугой обеспечения безопасности, которая соответствует этому требованию, является **управление доступом**. Услуга управления доступом предоставляет средства для обеспечения того, чтобы субъекты законным образом получали доступ к ресурсам. Ими могут быть повторная аутентификация, требуемая вследствие перерывов в работе, или требования изменения пароля. Рассматриваемыми ресурсами могут быть физическая система, программное обеспечение системы, приложения и данные. Услуга управления доступом может быть определена и внедрена на различных уровнях структуры СУЭ: уровне исполнительного устройства, уровне объекта или уровне атрибута.

Ограничения в доступе заложены в информацию об управлении доступом, которая устанавливает:

– средства для определения того, для каких объектов доступ санкционирован;

– какой вид доступа допускается (чтение, написание, изменение, создание, уничтожение);

– средства сопоставления масштаба времени с аутентифицированными объектами и "маркерами", которые они используют для аутентификации.

Более конкретно управление доступом в СУЭ может подразделяться на три типа:

– *Контроль доступа к управлению взаимосвязью*

  Эта услуга предоставляет возможность управления доступом на уровне управления взаимосвязью, означающую, что права доступа связаны с самой взаимосвязью, т. е. правом установления взаимосвязи.

– *Контроль доступа к уведомлениям управления*

  Эта услуга предоставляет возможность управления доступом в отношении уведомлений, т. е. обеспечения того, чтобы уведомления были открыты только для тех объектов, у которых есть санкция на их получение.

– *Контроль доступа к управляемому ресурсу*

  Эта услуга обеспечивает управление доступом в отношении самих ресурсов.

Идентификационная информация объекта, пытающегося получить доступ, должна быть проверена перед предоставлением доступа к ресурсу. Это означает, что использование управления доступом всегда связано с использованием услуги аутентификации.

УСЛУГА 4: Каждая СУ/каждый СЭ должна/должен поддерживать услуги контроля доступа для управления взаимосвязью, уведомлениями управления и контроля доступа к ресурсу управления.

6.3 Конфиденциальность данных

СУЭ должна предоставлять возможности для обеспечения конфиденциальности сохраненных и переданных данных.

Для поддержки требования предусмотрены следующие услуги обеспечения безопасности: **управления доступом** для сохраненных данных и **обеспечения конфиденциальности данных** для переданных данных.

Услуга обеспечения конфиденциальности предоставляет защиту от несанкционированного раскрытия данными обмена. Различают следующие виды услуг обеспечения конфиденциальности:

– *Конфиденциальность отдельных полей*

  Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, поскольку он является прикладным процессом, который может проводить различия между полями.

– *Конфиденциальность при соединении и в отсутствии соединения*

  С учетом того, что необходима сквозная конфиденциальность, ее обеспечение, исключая физический уровень и уровень линии передачи данных, возможно на сетевом уровне, транспортном уровне, представительном уровне, прикладном уровне или в прикладном процессе.

УСЛУГА 5: Каждая СУ/каждый СЭ должна/должен поддерживать услугу обеспечения конфиденциальности данных для защиты от несанкционированного раскрытия обменов данными, ориентированных на соединение или при его отсутствии, и обеспечивать конфиденциальность по отдельным полям.

6.4 Целостность данных

СУЭ должна быть способна гарантировать целостность сохраненных и переданных данных.

Для поддержки требования предусмотрены следующие услуги обеспечения безопасности: **управление доступом** для сохраненных данных и **обеспечение целостности данных** для переданных данных.

Услуга обеспечения целостности данных предоставляет средства для обеспечения правильности данных обмена. Различают следующие виды услуг обеспечения целостности:

– целостность отдельных полей;

– целостность соединения без восстановления;

– целостность соединения с восстановлением.

Услуга обеспечения целостности данных требует использования секретной величины, известной только поддерживающим связь сторонам. Секретная величина используется в нескольких протоколах для создания дайджеста HMAC-MD5. Этот дайджест добавляется к каждому сообщению.

УСЛУГА 6: Каждая СУ/каждый СЭ должна/должен поддерживать услугу обеспечения целостности данных для защиты от изменения, уничтожения, вставки и повторного использования данных обмена.

6.5 Неотвергаемость

СУЭ должна предоставлять возможность того, чтобы объект не мог отказаться от ответственности за любое из выполненных действий, а также за их результаты.

Требование поддерживается услугой обеспечения неотвергаемости, связывая субъект (или объект) с выполненной операцией. Услуги обеспечения неотвергаемости предоставляют средства для доказательства того, что обмен данными действительно имеет место. Это сводится к двум формам:

– неотвергаемости: доказательства происхождения;

– неотвергаемости: доказательства доставки.

Для достижения другой, более общей реализации неотвергаемости могут использоваться соответствующие сочетания услуг аутентификации, управления доступом и контрольного журнала.

УСЛУГА 7: Каждая СУ/каждый СЭ должна/должен поддерживать услугу неотвергаемости для обеспечения того, чтобы ни один из объектов не мог отказаться от ответственности за свои действия и за результаты этих действий.

6.6 Контрольный журнал

СУЭ должна быть способна сохранять информацию о действиях над системой с возможностью отслеживания пути этой информации к субъектам или объектам. СУЭ должна также предоставлять возможность анализа регистрируемых данных в случаях, имеющих отношение к безопасности, с целью их проверки на нарушение принципов обеспечения безопасности.

Журнал является хранилищем записей: он является абстракцией ВОС зарегистрированных ресурсов в реальных открытых системах. Записи содержат зарегистрированную информацию.

В целях обеспечения многих функций управления необходимо иметь возможность сохранения информации о произошедших событиях или об операциях, которые были выполнены, или о предпринятых попытках их выполнения различными ресурсами или над различными ресурсами.

К тому же, когда такая информация извлекается из журнала регистрации, управляющее устройство должно в любое время иметь возможность определить, были ли потеряны какие-либо записи или были ли изменены характеристики записей, сохраненных в журнале.

Контроль должен расцениваться как независимые анализ и проверка системных записей и действий с целью испытания управляющих устройств системы на пригодность для гарантирования соответствия установленным принципам обеспечения безопасности и эксплуатационным процедурам и для обнаружения нарушений безопасности. В результате контроля выявляются изменения в управлении, политике и процедурах.

Важно, чтобы каждая СУ/каждый СЭ предоставляла/предоставлял соответствующие возможности для расследования, контроля и действий по обнаружению и анализу в реальном времени, с тем чтобы можно было предпринять надлежащие восстановительные действия. В этом пункте рассматриваются контрольные журналы обеспечения безопасности, однако конкретные детали содержания и форматов журналов обеспечения безопасности находятся вне сферы применения этой Рекомендации.

Отметим, что действия, связанные с расследованием и криминалистическим анализом, могут включать изучение не относящихся к безопасности сообщений ЭУОиО, а также информации, сохраненной в контрольных журналах обеспечения безопасности, описанных в этом пункте. Для любых контролируемых действий требуется регистрация не относящихся к безопасности сообщений ЭУОиО, которые иногда называют сообщениями о "последних изменениях".

УСЛУГА 8: СУ/СЭ должна/должен иметь возможность регистрации любого действия, которое изменяет атрибуты и услуги обеспечения безопасности, управление доступом, параметры конфигурации устройств, и каждую попытку входа в систему и ее результат, вызывающий запуск таймера бездействия, и любое действие, которое требует проведения контроля. Каждая СУ/каждый СЭ должна/должен обеспечивать возможность контроля этих журналов.

Рекомендуется, чтобы записи в контрольном журнале направлялись в неизменяемый сервер контроля после того, как последовательность будет промаркирована и аутентифицирована (подписана) СУ/СЭ на основе шифрования.

6.7 Аварийная сигнализация

СУЭ должна обеспечивать возможность создания уведомлений об аварии, касающихся выбранных событий. Пользователь должен иметь возможность определять критерии выбора.

Функция управления контролем обеспечения безопасности является функцией управления системами, описывающей уведомление для сбора информации о событиях в системе безопасности. Уведомление об аварийных сигналах в системе безопасности, определяемое этой функцией управления системами, предоставляет информацию, касаемую условий эксплуатации, относящихся к обеспечению безопасности.

УСЛУГА 9: Каждая СУ/каждый СЭ должна/должен поддерживать услугу предоставления уведомлений об аварийных сигналах для предупреждения администраторов службы безопасности об условиях эксплуатации, относящихся к обеспечению безопасности.

6.8 Проверка пакетов

СУЭ должна предоставлять возможность проверки пакетов трафика, основанного на пакетной передаче и предназначенного для плоскости управления любого устройства СУЭ. Пользователь должен иметь возможность определить фильтрацию на основе адресов сетей источника и назначения, протокол и порты источника и назначения пакета.

Проверка пакетов является процессом анализа величин заголовков каждого пакета, который проходит через элемент сети, на основе конкретных критериев соответствия. На основе результатов проверки пакетов может быть предпринято какое-либо действие.

УСЛУГА 10: Каждая СУ/каждый СЭ должна/должен поддерживать услугу проверки пакетов для защиты плоскости управления СУЭ от любого трафика, который не удовлетворяет политике обеспечения безопасности.

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.