МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т M.3016.0

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(05/2005)

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

Сеть управления электросвязью

Безопасность для плоскости административного управления: обзор

Рекомендация МСЭ-Т M.3016.0

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.3016.0

Безопасность для плоскости административного управления: обзор

Резюме

Данная Рекомендация содержит обзор и структуру для идентификации угроз в отношении СУЭ; в ней показано, как доступные услуги безопасности могут быть использованы в рамках функциональной архитектуры СУЭ.

Источник

Рекомендация МСЭ-Т M.3016.0 утверждена 22 мая 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

Рекомендация МСЭ-Т M.3016.0

Безопасность для плоскости административного управления: обзор

1 Область применения

Данная Рекомендация содержит обзор и структуру для идентификации угроз безопасности в отношении СУЭ; в ней показано, как доступные услуги безопасности могут быть использованы в рамках функциональной архитектуры СУЭ, описанной в Рекомендации МСЭ-Т M.3010.

Данная Рекомендация является обобщенной по своему характеру и не определяет требований или не рассматривает требования для конкретного интерфейса СУЭ.

В данной Рекомендации не делается попытки определения новых услуг безопасности, а используются существующие услуги безопасности, определенные в других Рекомендациях МСЭ-Т и стандартах ИСО.

Настоящая Рекомендация является частью Рекомендаций МСЭ-Т серии M.3016.x, предназначенных для предоставления руководящих указаний и выработки рекомендаций по обеспечению безопасности для плоскости административного управления развиваемых сетей:

Рек. МСЭ-Т M.3016.0 − *Безопасность для плоскости административного управления: обзор.*

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

Рек. МСЭ-Т M.3016.2 − *Безопасность для плоскости 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.*

В Рекомендациях 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. Так как различным администрациям и организациям требуется поддержка разных уровней безопасности, в Рекомендациях МСЭ-Т M.3016.1, M.3016.2 и M.3016.3 не указывается, является ли требование, услуга или механизм обязательным или необязательным.

Форма, определенная в Рекомендации МСЭ-Т M.3016.4, предназначена для оказания помощи 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.

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 M.3010 (2000), *Principles for a telecommunications management network*.

– ITU-T Recommendation M.3400 (2000), *TMN management functions*.

– ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

– ITU-T Recommendation X.741 (1995), *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control*.

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

– ITU-T Recommendation X.802 (1995), *Information technology – Lower layers security model*.

– ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.812 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

– ITU-T Recommendation X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

– ITU-T Recommendation X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.

– ITU-T Recommendation X.815 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.

– ITU-T Recommendation X.816 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.

– ISO/IEC 9979:1999, *Information technology – Security techniques – Procedures for the registration of cryptographic algorithms*.

3 Определения

В данной Рекомендации не определены никакие новые термины.

4 Сокращения и акронимы

В данной Рекомендации используются следующие сокращения:

МККТТ	Международный консультативный комитет по телеграфии и телефонии
DCN	Сеть передачи данных
FC	Функциональные классы
ИСО	Международная организация стандартизации
МСЭ-Т	Международный союз электросвязи – Сектор стандартизации электросвязи
LLA	Логическая многоуровневая архитектура
MF	Функция устройства сопряжения
NEF	Функция сетевого элемента
OSF	Функция операционной системы
ВОС	Взаимосвязь открытых систем
PIN	Персональный идентификационный номер
TF	Функция преобразования

СУЭ Сеть управления электросвязью

TTP Пользующаяся доверием третья сторона

WSF Функция рабочей станции

5 Логическое обоснование

Требования по безопасности в СУЭ исходят от различных источников:

– **Потребителям**/**абонентам** требуется соблюдение конфиденциальности в сети и в предоставляемых услугах, включая правильное выставление счетов.

– **Обществу**/**полномочным органам** требуется безопасность согласно директивам и законодательству для обеспечения доступности услуг и сохранения тайны.

– Самим **сетевым операторам**/**поставщикам услуг** требуется безопасность для защиты своих рабочих и деловых интересов и для выполнения обязанностей по отношению к потребителям и обществу.

СУЭ предназначена для управления базовой сетью электросвязи; следовательно, обеспечение безопасности СУЭ является существенно необходимым для правильного функционирования сети электросвязи. К тому же сеть электросвязи может обладать возможностями обеспечения безопасности, которым требуется управление со стороны СУЭ. В Рекомендации МСЭ-Т M.3400 перечислены эти функции управления безопасностью.

Стандарты по безопасности СУЭ предпочтительно должны базироваться на международно согласованных стандартах по безопасности, так как выгоднее повторно использовать существующие стандарты, чем создавать новые. Предоставление и использование услуг безопасности вполне может оказаться более дорогостоящим по отношению к ценности защищаемых деловых операций. Поэтому важным фактором является способность адаптации обеспечиваемой безопасности к защищаемым операциям СУЭ. Услуги и механизмы безопасности, которые используются для защиты операций СУЭ, должны обеспечиваться способом, позволяющим такую адаптацию. Вследствие наличия большого числа возможных комбинаций параметров безопасности желательно иметь **профили безопасности** (см. Дополнение I), охватывающие широкий спектр приложений обеспечения безопасности СУЭ.

Стандартизация облегчает **повторное использование решений и полученных результатов**, а это значит, что обеспечение безопасности может быть осуществлено быстрее и с меньшими затратами.

Аналогично этому, важным преимуществом стандартизованных решений для поставщиков и пользователей систем является масштабная экономия при разработке систем безопасности и при осуществлении взаимодействия компонентов внутри системы СУЭ в части обеспечения безопасности.

Необходимо обеспечить услуги и механизмы безопасности для защиты операций СУЭ между объектами СУЭ (как определено в Рекомендации МСЭ-Т M.3010) от таких злонамеренных атак, как подслушивание, спуфинг, намеренное искажение сообщений (изменение, задержка, уничтожение, вставка, повторное воспроизведение, перемаршрутизация, неправильная маршрутизация или изменение порядка следования сообщений), отрицание участия или подделка документов. Защита включает в себя предотвращение, обнаружение атак и восстановление после атак, а также управление связанной с безопасностью информацией. Стандарты должны охватывать как внутридоменные интерфейсы (Q и F), так и междоменные интерфейсы (X).

6 Описание системы

Задачей настоящей Рекомендации является построение абстрактной конструкции, которая сделает возможным избежать многих деталей реализации и согласовать результаты, которые могут быть полезными позднее при отображении в конкретные реализации.

Описание СУЭ выполняется с точки зрения функциональной архитектуры, информационной архитектуры и физической архитектуры (Рекомендация МСЭ-Т M.3010).

В Рекомендации МСЭ-Т M.3010 отмечается, что составляющие блоки СУЭ могут поддерживать и другие интерфейсы в дополнение к интерфейсам Q, X и F. Аналогично, физическое оборудование может обладать другими функциональными возможностями в дополнение к тем, которые относятся к информации, получаемой через Q, X и F. Эти дополнительные интерфейсы и связанные с ними

функциональные возможности выходят за рамки СУЭ и, следовательно, за пределы области стандартизации безопасности СУЭ.

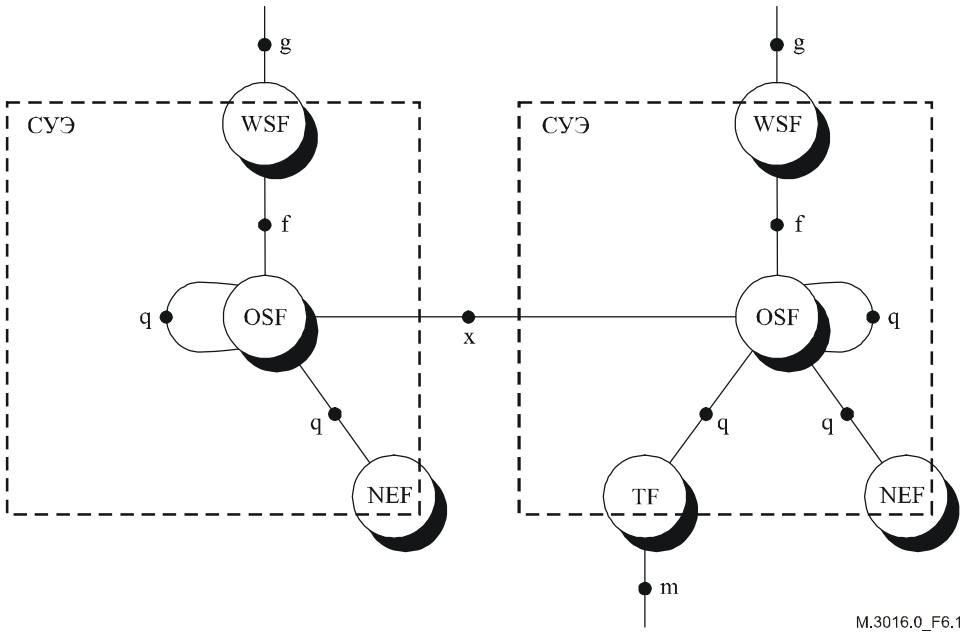

Рисунок 1/M.3016.0 – Функциональная архитектура СУЭ

6.1 Действующие объекты и роли

В целях стандартизации безопасности СУЭ будет рассматриваться только техническая безопасность, а это означает, что надлежащими действующими объектами следует считать *пользователей СУЭ*. Пользователь СУЭ – это лицо или процесс, применяющие услуги управления СУЭ для цели выполнения операций управления. Пользователи СУЭ могут быть далее разделены на категории в зависимости от того, относятся ли они к организации, эксплуатирующей СУЭ (внутренние пользователи), или получают доступ в СУЭ как внешние пользователи.

При каждом доступе пользователя СУЭ к услуге управления он берет на себя ту или иную роль. В некоторых случаях имеет место взаимно-однозначное соответствие между пользователем СУЭ и ролью, то есть пользователь СУЭ всегда остается в той же самой роли. В других случаях имеет место взаимно-многозначное соответствие между конкретным пользователем СУЭ и возможными ролями, которые пользователь СУЭ может выполнять.

Далее приведена высокоуровневая классификация некоторых общих ролей:

– сетевые операторы (*частных сетей или сетей общего пользования*);
– поставщики услуг (*поставщики услуг по переносу информации или поставщики дополнительных услуг*);
– абоненты услуг/потребители услуг;
– конечные пользователи услуг;
– поставщики оборудования/программного обеспечения;
– пользующаяся доверием третья сторона (то есть третья сторона, которой доверяют обе стороны и которая функционирует согласно соответствующим национальным законам и регламентарным положениям для обеспечения сертификации, аутентификации и связанных с этим услуг).

При обеспечении безопасности СУЭ недостаточно управлять режимом работы известных пользователей СУЭ. Следует также учитывать возможность попыток злоумышленников получить нелегальный доступ в СУЭ.

Некоторые меры безопасности требуют от действующих объектов выполнения роли пользующейся доверием третьей стороны (TTP). Важной проблемой безопасности является способ допуска этих действующих объектов к взаимодействию с СУЭ.

6.2 Домены безопасности

В Рекомендации МСЭ-Т М.3010 введена концепция "логической многоуровневой архитектуры" (LLA), в которой функциональные возможности управления разделены на уровни. На каждом уровне выполняется четко ограниченное множество общих действий по управлению. Каждый функциональный уровень является отдельным *доменом управления*, находящимся под управлением функции операционной системы (OSF), называемой доменом OSF. Функции сетевого элемента (NEF), управляемые OSF, являются частью домена OSF. СУЭ, как таковая, состоит из одного или нескольких доменов OSF, где разные домены OSF могут либо соседствовать, либо взаимодействовать, либо накладываться друг на друга, либо находиться в сети.

Домен безопасности определен как совокупность объектов или сторон, по отношению к которым проводится единая политика обеспечения безопасности и применяется единое управление безопасностью. Нормальным допущением было бы рассмотрение СУЭ как единого домена безопасности. Это часто имеет место, но не может подходить для принятия в качестве общего допущения. В более крупных СУЭ, состоящих из множества разнообразных систем управления, в разных частях СУЭ могут проводиться различные стратегии безопасности, и к ним могут предъявляться различные требования по безопасности. Поэтому представляется более подходящим считать, что домен безопасности СУЭ охватывает один единый домен OSF или совокупность доменов OSF.

При использовании этого допущения могут применяться следующие междоменные и внутридоменные взаимосвязи по безопасности:

Возможные внутридоменные взаимосвязи по безопасности:

– q (OSF-NEF, OSF-OSF).

Возможные междоменные взаимосвязи по безопасности:

– x (OSF-OSF);
– f (WSF-OSF, WSF-MF);
– q (OSF-OSF, OSF-TF).

Отметим, что приведенные выше взаимосвязи относятся к доменам безопасности, а не к доменам управления. Важным фактом, который следует отметить, является то, что опорная точка q может участвовать как во внутридоменных, так и в междоменных взаимосвязях безопасности. Одним из главных отличий между внутридоменными и междоменными взаимосвязями является степень доверия, существующая между участвующими объектами.

7 Общие задачи обеспечения безопасности для СУЭ

Задачей этого пункта является описание основной цели мер безопасности, принимаемых в среде, соответствующей СУЭ. Главным здесь является степень достигнутой безопасности, а не способ ее достижения.

Задачи безопасности должны быть получены исходя из интересов, деловых связей, законодательных и регламентарных ограничений, договорных ограничений и т. д. оператора и других действующих объектов.

Задачами безопасности для СУЭ являются:

– Возможность доступа и работы с имеющимися средствами в СУЭ должны иметь только легальные действующие объекты.
– Легальные действующие объекты должны иметь возможность доступа и работы с имеющимися средствами, если они санкционированы для доступа.
– Все действующие объекты должны быть подотчетны за свои и только свои действия в СУЭ.
– Доступность СУЭ должна быть защищена от незатребованного доступа или операций.
– Должна быть обеспечена возможность поиска в СУЭ информации, связанной с безопасностью.
– В случае обнаружения случаев нарушения безопасности их обработка должна вестись контролируемым способом, минимизируя тем самым нанесенный ущерб.
– Должна быть обеспечена возможность восстановления нормальных уровней безопасности после обнаружения "бреши" в системе безопасности.
– Архитектура безопасности СУЭ должна обладать определенной гибкостью для возможности поддержки различных стратегий безопасности, например применения механизмов безопасности с разной степенью надежности.

Термин "доступ к имеющимся средствам" понимается как возможность не только выполнения функций, но и считывания информации.

Общие задачи формулируются в соответствии с видом и языком управления предприятием. Следующие пункты требуют изложения в более технических терминах, обеспечивающих возможность реализации услуг и функций безопасности. Соответствие между двумя языками не всегда очевидно.

Можно показать, что при выполнении следующей совокупности задач по безопасности могут быть реализованы первые пять из указанных в этом пункте, выше, задач по безопасности для СУЭ:

– конфиденциальность;
– целостность данных;
– подотчетность;
– доступность.

Угрозы и риски, определенные в п. 9, а также функциональные требования в п. 6 должны основываться на этих более формальных терминах. См. определения в п. 9.

8 Вопросы, связанные с законодательством

Инфраструктура безопасности СУЭ должна обладать способностью приспособления к ограничениям, налагаемым государственными законами, положениями договоров, договорами и регламентарными положениями. Эти ограничения могут включать в себя обязательные услуги безопасности (такие как обеспечение конфиденциальности информации клиентов), исключение некоторых механизмов обеспечения безопасности (как, например, некоторых типов шифрования) и/или поддержку секретного прослушивания правоохранительными органами.

9 Угрозы и риски

Данный пункт посвящен рассмотрению угроз и рисков для СУЭ. Здесь не преследуется цель проведения оценок риска или анализа угроз для отдельных реализаций СУЭ. Это локальные вопросы, которые могут решаться по-разному каждым поставщиком услуг без влияния на способность взаимодействия.

Угроза – это потенциальная возможность нарушения безопасности. Согласно определенным общим задачам обеспечения безопасности в СУЭ угрозы могут относиться к четырем различным аспектам:

– **конфиденциальность** (конфиденциальность хранимой и передаваемой информации);
– **целостность данных** (защита хранимой и передаваемой информации);
– **подотчетность** (любой объект должен нести ответственность за любое инициированное им действие); и
– **доступность** (все легитимные объекты должны иметь возможность правильного доступа к оборудованию СУЭ).

В данной Рекомендации различаются три вида угроз:

– случайная угроза: угроза, источник которой не является злонамеренным;
– административная угроза: угроза, возникающая из-за отсутствия административного управления безопасностью; и
– преднамеренная угроза: угроза от злонамеренного объекта, который может атаковать либо саму связь, либо сетевые ресурсы.

Случайные и административные угрозы могут учитываться в работе по стандартизации СУЭ, когда их последствия те же, что и от преднамеренных угроз. Учитывая архитектуру СУЭ для проведения более точного анализа угроз, в настоящей Рекомендации основное внимание уделяется преднамеренным угрозам, относящимся к связи между различными действующими объектами СУЭ. Целью этого подхода является определение более короткого перечня угроз, который может быть непосредственно использован в работе по стандартизации СУЭ. Таким образом, на основании Рекомендации МСЭ-Т X.800 анализ угроз СУЭ должен быть посвящен следующим позициям:

– **маскировка под законного пользователя** (**"спуфинг"**): обманная попытка объекта выдать себя за другой объект;

- **подслушивание**: нарушение конфиденциальности посредством контроля связи;
- **несанкционированный доступ**: попытки доступа объекта к данным в нарушение действующей политики безопасности;
- **потеря или повреждение информации**: нарушение целостности передаваемых данных посредством несанкционированного удаления, вставки, изменения, переупорядочения, повторного воспроизведения или задержки;
- **отрицание участия**: участвовавший в обмене связью объект впоследствии отказывается от признания этого факта;
- **подделка**: объект фабрикует информацию и заявляет, что такая информация была получена от другого объекта или была послана другому объекту;
- **отказ в обслуживании**: это происходит, когда объект не может выполнять свою функцию или препятствует другим объектам выполнять их функции. Это может включать в себя отказ в доступе к СУЭ и отказ в связи путем переполнения СУЭ трафиком. В совместно используемой сети эта угроза может быть распознана как фабрикация дополнительного трафика, который переполняет сеть, мешая использовать ее другим посредством задержки их трафика.

В таблице 1 показано соответствие между угрозами и задачами.

Таблица 1/M.3016.0 – Соответствие угроз и задач

Угроза	Конфиден-циальность	Целостность данных	Подотчетность	Доступность
Маскировка под законного пользователя	x	x	x	x
Подслушивание	x			
Несанкционированный доступ	x	x	x	x
Потеря или повреждение (передаваемой) информации		x		x
Отрицание участия			x	
Подделка		x	x	
Отказ в обслуживании				x

Потенциальная угроза не наносит системе вреда до тех пор, пока в системе нет соответствующих слабых мест и пока не наступит момент времени, в который возможно использование этого слабого места. Каждая угроза заключает в себе риск. Оценка риска может быть разделена на оценку вероятности каждой угрозы и на оценку воздействия, которое может оказать угроза. Оценка угрозы и риска должна быть частью итеративного процесса: новые угрозы могут появиться, когда выработаны контрмеры; например, угрозы для криптографических ключей, когда используются меры по защите криптографических методов.

10 Требования и услуги безопасности

На рисунке 2 показаны взаимосвязи между задачами по безопасности, угрозами, требованиями по безопасности и услугами. Они описывают процесс получения "требований по безопасности" из "угроз" и "задач по безопасности", которые, в свою очередь, реализуются посредством набора услуг безопасности. Эти "услуги", которые противодействуют угрозам, используют "механизмы", которые сами используют "алгоритмы безопасности".

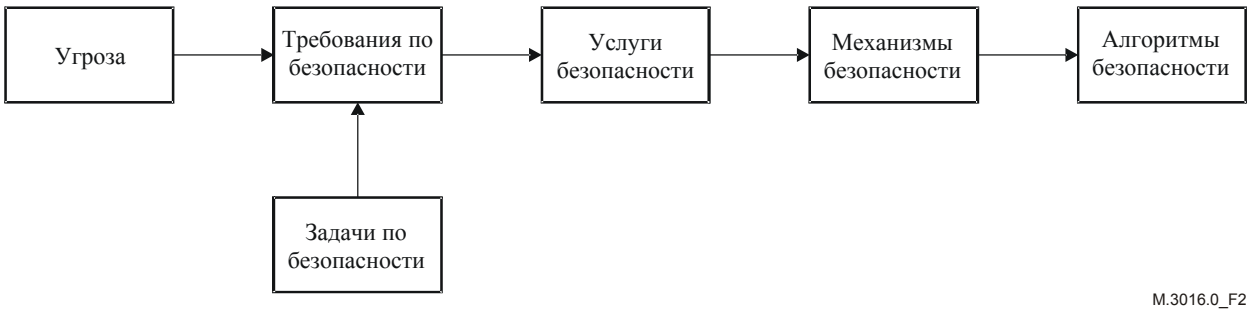

Рисунок 2/M.3016.0 – Структура обеспечения безопасности

Такие требования по безопасности перечислены в п. 10.1. Если не оговорено особо, слово "требование" в настоящей Рекомендации не означает, что та или иная функциональная возможность всегда является обязательной в каждой СУЭ; скорее, оно означает, что функциональная возможность может быть сделана администрацией СУЭ обязательной для некоторых конкретных приложений и/или интерфейсов этой СУЭ. Фактический выбор будет зависеть от задач по безопасности, определенных в политике безопасности оператора.

В дополнение к требованиям и услугам безопасности в этом пункте приведены также некоторые общие требования для управления услугами безопасности (см. п. 10.2) и архитектурные требования по управлению интеграцией услуг безопасности в архитектуру СУЭ (см. п. 10.3). Административные требования и требования к жизненному циклу являются важными, но они не влияют на архитектуру и не включены в этот пункт.

10.1 Требования по безопасности и соответствующие услуги

В этом пункте описывается набор общих функциональных требований и соответствующих услуг, которые могут использоваться для противодействия угрозам СУЭ.

10.1.1 Соответствие функциональных требований, угроз и задач по безопасности

В этом пункте определяются функциональные требования по безопасности для преодоления угроз, перечисленных в п. 9. Это выполнено в таблице 2. С ее помощью устанавливается соответствие требований по безопасности (таблица 3) задачам по безопасности, сформулированным в п. 7. Перечень ограничен требованиями, которые являются общими по своему характеру и оказывают существенное влияние на компоненты и архитектуру.

Таблица 2/M.3016.0 – Соответствие функциональных требований и угроз

Функциональное требование	Маскировка под законного пользователя	Подслушивание	Несанкционированный доступ	Потеря или искажение информации	Отрицание участия	Подделка	Отказ в обслуживании
Проверка идентичности	x		x				
Управляемый доступ и санкционирование			x				x
Защита конфиденциальности		x	x				
Защита целостности данных				x			
Подотчетность					x	x	
Регистрация действий	x		x		x	x	x
Отчет об авариях	x		x	x			x
Проверка	x		x		x	x	x

Используемыми задачами являются четыре формальные задачи, определенные в п. 3, каждая с колонкой в таблице 3, указывающей набор функциональных требований для выполнения рассматриваемой задачи.

10.1.2 Описание функциональных требований и соответствующих услуг

Функциональные требования из таблиц 2 и 3 обсуждаются далее в тексте, и для каждого из требований определяются соответствующие услуги безопасности. Отметим, что требования для каждой из этих функций не вызывают автоматически услугу безопасности, как определено ИСО. Однако на практике в некоторых случаях имеет место совпадение.

Таблица 3/M.3016.0 – Соответствие задач по безопасности и функциональных требований

Функциональное требование	Конфиден-циальность	Целостность данных	Подотчетность	Доступность
Проверка идентичности	x	x	x	
Управляемый доступ и санкционирование	x	x	x	x
Защита конфиденциальности	x			
Защита целостности данных		x		
Подотчетность			x	
Регистрация действий			x	x
Отчет об авариях	x	x	x	x
Проверка			x	x

10.1.2.1 Проверка идентичности

СУЭ должна обеспечивать возможности установления и проверки объявленной идентичности любого действующего объекта в СУЭ.

Действующими объектами могут быть люди или объекты в пределах СУЭ. Проверенные идентичности обеспечивают базу для подотчетности и являются основой для выполнения большинства требований по безопасности, перечисленных в этом пункте.

Услугой безопасности для поддержки этого требования является **аутентификация**. Услуга аутентификации предоставляет доказательство того, что идентичность объекта или субъекта на самом деле является объявленной им идентичностью. В зависимости от типа действующего объекта и от цели идентификации могут потребоваться следующие виды аутентификации:

– аутентификация пользователя, предоставляющая доказательство идентичности пользователя-человека или прикладного процесса;

– аутентификация равноправного объекта, предоставляющая доказательство идентичности равноправного объекта во время взаимоотношений при связи;

– аутентификация источника данных, предоставляющая доказательство идентичности, отвечающей за конкретный элемент данных.

Использование услуги аутентификации предоставляет доказательство для конкретного момента времени. Для обеспечения длительного доказательства аутентификация должна повторяться или быть связана с услугой обеспечения целостности.

Примерами механизмов, используемых для реализации услуги аутентификации, являются пароли и персональные идентификационные номера (PIN) (простая аутентификация), а также методы на основе криптографии (строгая аутентификация).

10.1.2.2 Управляемый доступ и санкционирование

СУЭ должна предоставлять возможности обеспечения того, чтобы предотвращалось получение доступа к информации или ресурсам действующими объектами, которые не санкционированы для доступа.

Услугой безопасности для выполнения этого требования является **управление доступом**. Услуга управления доступом предоставляет средства для обеспечения доступа субъектов к ресурсам только санкционированным способом. Такими ресурсами может быть физическая система, системное

программное обеспечение, приложения и данные. Услуга управления доступом может быть определена и реализована на различных уровнях структурированности в СУЭ: на уровне агента, на уровне объекта или на уровне атрибута. Ограничения доступа содержатся в информации управления доступом, которая указывает:

– средства для определения того, каким объектам разрешено иметь доступ;

– какой вид доступа допускается (чтение, запись, изменение, создание, удаление).

Более конкретно управление доступом в СУЭ может быть разделено на три типа:

– *Управление доступом на уровне ассоциации административного управления*

  Эта услуга разрешает управление доступом на уровне ассоциации административного управления, это означает, что права доступа связаны с самой ассоциацией, то есть с правом создания ассоциации.

– *Управление доступом к оповещениям административного управления*

  Эта услуга разрешает управление доступом в отношении оповещений, то есть обеспечивает, чтобы оповещения показывались только объектам, имеющим санкцию на их получение.

– *Управление доступом к административно управляемым ресурсам*

  Эта услуга обеспечивает управление доступом в отношении самих ресурсов.

Идентичность объекта, пытающегося получить доступ, должна быть проверена до того, как будет предоставлен доступ к ресурсу. Это означает, что использование управления доступом всегда связано с использованием услуги аутентификации.

10.1.2.3 Защита конфиденциальности

СУЭ должна предоставлять возможности обеспечения конфиденциальности сохраненных и переносимых при связи данных.

Услугами безопасности для поддержки этого требования являются: **управление доступом** для сохраненных данных и **конфиденциальность данных** для переносимых при связи данных. **Конфиденциальность данных** может также требоваться для некоторых видов сохраненных данных, таких как пароли.

Услуга конфиденциальности обеспечивает защиту от несанкционированного раскрытия данных обмена. Различаются следующие виды услуг конфиденциальности:

– конфиденциальность выбранного поля;

– конфиденциальность соединения;

– конфиденциальность потока данных.

10.1.2.4 Защита целостности данных

СУЭ должна быть способна обеспечивать целостность сохраненных и переносимых при связи данных.

Услугами безопасности для поддержки этого требования являются: **управление доступом** и **целостность данных** для сохраненных данных и **целостность данных** для переносимых при связи данных.

Услуга целостности предоставляет средства для обеспечения правильности данных обмена, защиты от изменения, удаления, создания (вставки) и повторного воспроизведения данных обмена. Различаются следующие виды услуг целостности:

– целостность выбранного поля;

– целостность соединения без восстановления;

– целостность соединения с восстановлением.

10.1.2.5 Подотчетность

СУЭ должна обеспечивать возможность того, чтобы объект не мог отказаться от ответственности за любое из произведенных им действий, а также от результатов этих действий.

Это требование поддерживается услугой **невозможности отказа от участия**, связывающей лицо (или объект) с выполненной операцией. Услуги невозможности отказа от участия предоставляют средства для доказательства того, что обмен данными фактически имел место. Они реализуются в двух формах:

– невозможность отказа от участия: доказательство источника;

– невозможность отказа от участия: доказательство доставки.

Другая, более общая и, возможно, менее убедительная реализация подотчетности достигается посредством соответствующих комбинаций услуг **аутентификации**, **управления доступом** и **контрольного журнала**.

10.1.2.6 Регистрация действий, отчеты об авариях и аудиторская проверка

Эти требования охватывают потребности в хранении и анализе информации о действиях, связанных с безопасностью, в пределах СУЭ. Кроме того, оповещения об аварии должны генерироваться при некоторых управляемых событиях. Соответствующими услугами являются **контрольный журнал** и **отчеты об авариях**. Каждое из требований обсуждается ниже с некоторыми подробностями.

10.1.2.6.1 Регистрация действий

СУЭ должна обеспечивать возможность сохранения информации о действиях в системе с возможностью отслеживания этой информации в отношении лиц или объектов.

Хранилищем для записей является журнал регистрации: это абстрактная структура ВОС для регистрации ресурсов в реальных открытых системах. Записи содержат зарегистрированную информацию.

Для целей многих функций административного управления необходимо иметь возможность сохранять информацию о событиях, которые имели место, или об операциях над различными ресурсами, которые были выполнены или попытка выполнения которых предпринималась.

Кроме того, при считывании этой информации из журнала регистрации администратор должен иметь возможность определить, не были ли утеряны некоторые записи или не были ли изменены в какое-либо время данные сохраненных в журнале записей.

10.1.2.6.2 Отчеты о сигналах нарушения безопасности

СУЭ должна обеспечивать возможность генерирования оповещений о сигналах тревоги для выбранных событий. Пользователь должен иметь возможность определения критериев выбора.

Функция управления проверкой системы безопасности является функцией административного управления системами, описывающей оповещение для совокупности событий по безопасности. Оповещение о сигналах нарушения безопасности, определенное этой функцией административного управления системами, обеспечивает информацию о режиме эксплуатации, относящемся к обеспечению безопасности.

10.1.2.6.3 Проверка системы безопасности

СУЭ должна обеспечивать возможность анализа зарегистрированных данных о событиях, относящихся к обеспечению безопасности, для контроля их на наличие нарушений политики безопасности.

Проверка должна представлять собой независимый анализ и изучение записей и действий системы для тестирования адекватности средств контроля системы, для обеспечения соответствия принятой политике безопасности и рабочим процедурам и для обнаружения нарушений безопасности. Результат проверки выявляет изменения в управлении, политике и процедурах.

В таблице 4 приведен обзор взаимосвязи между требованиями по безопасности и услугами безопасности. В данном пункте определены только услуги безопасности, относящиеся к стандартным решениям; другие возможные услуги (например, обнаружение отказа в обслуживании) опущены.

Таблица 4/M.3016.0 – Соответствие требований по безопасности и услуг безопасности

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 – переносимые данные	Конфиденциальность
Защита целостности данных – сохраненные данные	Управление доступом
Защита целостности данных – переносимые данные	Целостность
Подотчетность	Невозможность отказа от участия
Регистрация действий	Данные контрольного журнала
Отчеты о сигналах нарушения безопасности	Сигналы нарушения безопасности
Проверка системы безопасности	Данные контрольного журнала
Защита DCN	Контроль пакетов

ПРИМЕЧАНИЕ. – Следующие требования не являются требованиями того же типа, как те, которые были представлены до таблицы 4, и не могут рассматриваться в качестве очевидных кандидатов для стандартизации. Однако они должны учитываться на этапе проектирования наряду с реализацией представленных выше ключевых требований СУЭ.

10.1.2.6.4 Целостность системы

Необходимо, чтобы программная и аппаратная среда реализуемых функций обеспечения безопасности поддерживала требуемый уровень безопасности.

Это включает в себя правильную конфигурацию операционных систем и исключение системных дефектов.

Эти аспекты сами не входят в состав функционального профиля обеспечения безопасности, но они должны быть точно определены вместе с их спецификациями для гарантирования надежности функций в реальной среде.

10.1.2.6.5 Замечания о готовности

Для требования готовности не имеется какой-то одной услуги безопасности или ограниченного набора таких услуг, которые способны выполнить это требование. Все перечисленные здесь услуги безопасности должны формировать согласованный набор, в котором они вместе способны обеспечивать готовность. Однако одни услуги безопасности никогда не могут быть способны обеспечить готовность: это является также вопросом надежности аппаратных средств и программного обеспечения (с точки зрения как проектирования, так и реализации).

10.1.2.7 Защита DCN

СУЭ должна обеспечивать защиту DCN от трафика клиентов и равноправной сети.

СУЭ должна обеспечивать отделение трафика DCN от трафика других типов, особенно в пакетной DCN.

10.2 Требования по управлению безопасностью

СУЭ должна содержать информационные модели и иметь возможности управления услугами, используемыми для обеспечения безопасности СУЭ.

Подробные требования по управлению безопасностью определяют, какие приложения по обеспечению безопасности должны быть введены и как они должны быть спроектированы. Это делается для обеспечения администратора по безопасности надлежащими средствами для

эффективного и правильного контроля и управления услугами по безопасности. Задачи и цели управления безопасностью представлены на трех различных уровнях системы электросвязи, которые соответствуют управлению безопасностью системы, услугам по безопасности и механизмам обеспечения безопасности, соответственно.

Операции и информация, относящиеся к управлению услугами безопасности в СУЭ, требуют особого рассмотрения с точки зрения безопасности. Секретные шифровальные ключи, информация по аутентификации и списки управления доступом являются примерами случаев, когда требуемая сила защиты может быть выше, чем при управлении сетью.

Управление безопасностью должно осуществляться согласованно с функциями управления безопасностью, определенными в Рекомендации МСЭ-Т М.3400.

Должна поддерживаться функция восстановления безопасного состояния системы после возникновения нарушения безопасности.

Когда бы не возникло нарушение в системе безопасности, СУЭ должна быть способна обработать эту попытку контролируемым способом, означающим, что данная попытка не должна привести к серьезному ухудшению работы СУЭ в плане готовности.

10.3 Архитектурные требования

Наиболее важными требованиями, которые должны быть удовлетворены посредством мер обеспечения безопасности, соответствующих структуре СУЭ, являются следующие:

– Меры должны базироваться на принципах функциональной модели СУЭ.

– Меры должны соответствовать объектно-ориентированным данным и информационной модели СУЭ.

– Меры должны быть применимы ко всем областям работы СУЭ в общественном и частном секторах.

– Решения должны быть масштабируемыми для применения в малых и больших сетях СУЭ.

– Решения должны быть совместимыми с внутренней архитектурой рассматриваемых опорных точек СУЭ.

– Решения должны учитывать интересы всех внутренних и внешних пользователей СУЭ.

– Решения должны учитывать аспекты устойчивости.

– Решения должны поддерживать реконфигурацию путем добавления или удаления пользователей или приложений.

Неизбежно появление конфликтов между областью обеспечения безопасности и другими функциональными областями. Например, целостность и конфиденциальность данных о тарификации должны быть сбалансированы с требованиями на пропускную способность огромного объема информации, необходимого для выписки квитанций на оплату. Соответствующий действительности набор требований по безопасности должен оказывать воздействие на характеристики других рассматриваемых функциональных областей.

Другие архитектурные требования могут возникнуть при анализе конкретных сценариев СУЭ.

10.4 Услуги безопасности и уровни ВОС

В данном пункте описывается, какие уровни ВОС используются для предоставления услуг безопасности, и поэтому показывается, как они могут быть обоснованно предоставлены для СУЭ.

Предполагается, что если на каком-то уровне предоставляется та или иная услуга безопасности, то эта услуга предоставляется для уровня, расположенного выше рассматриваемого уровня. Предоставление услуг уровнями, изложенное в Рекомендации МСЭ-Т X.800, используется в качестве основы для ограничения возможностей.

10.4.1 Аутентификация пользователя

Эта услуга зависит от взаимодействия с пользователем. Поэтому она выходит за рамки модели ВОС.

10.4.2 Аутентификация (равноправного объекта и источника данных)

Эта услуга может быть предоставлена на следующих уровнях (согласно Рекомендации МСЭ-Т X.800):

– сетевой уровень (подтверждение идентичности равноправных объектов транспортного уровня);

– транспортный уровень (подтверждение идентичности равноправных объектов сеансового уровня);

– прикладной уровень (подтверждение идентичности прикладных процессов);

– вне ВОС: в самом прикладном процессе.

Учитывая, что для СУЭ требуются идентификация и аутентификация администраторов и агентов, а также связь аутентификации с управлением доступом, рекомендуемыми позициями в отношении стека ВОС являются прикладной уровень и прикладной процесс.

10.4.3 Управление доступом

– *Управление доступом на уровне ассоциации административного управления*

Эта услуга применима на тех уровнях, где существует ассоциация; это может быть на прикладном уровне (управление доступом для прикладных процессов) или в самом прикладном процессе.

Управление доступом на уровне ассоциации может обеспечиваться на сетевом уровне, например, используя услугу "замкнутая группа пользователей X.25". Кроме того, управление доступом на уровне ассоциации может обеспечиваться на прикладном уровне или в самом прикладном процессе.

– *Управление доступом к оповещениям административного управления*

Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, поскольку именно прикладной процесс, подобно администраторам и агентам, может различать объекты (прикладного процесса).

– *Управление доступом к административно управляемым ресурсам*

Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, поскольку именно прикладной процесс, подобно администраторам и агентам, может различать объекты (прикладного процесса).

10.4.4 Сигналы нарушения безопасности, контрольный журнал и восстановление безопасного состояния

Эти услуги связаны с другими услугами и поэтому представлены на тех уровнях, где обеспечиваются другие услуги.

10.4.5 Целостность

– *Целостность выбранного поля*

Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, поскольку именно прикладной процесс может различать поля.

– *Целостность соединения с восстановлением*

Может обеспечиваться на транспортном уровне, на прикладном уровне или в прикладном процессе.

– *Целостность соединения без восстановления*

Может обеспечиваться на сетевом уровне, на транспортном уровне, на прикладном уровне или в прикладном процессе.

10.4.6 Конфиденциальность

– *Конфиденциальность выбранного поля*

Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, поскольку именно прикладной процесс может различать поля.

– *Конфиденциальность соединения и без установления соединения*

Учитывая, что необходима межконцевая конфиденциальность, которая исключает физический уровень и уровень канала данных, конфиденциальность может быть обеспечена на сетевом уровне, на транспортном уровне, на уровне представления, на прикладном уровне или в прикладном процессе.

– *Конфиденциальность потока трафика*

Эта услуга может предоставляться на сетевом, транспортном или прикладном уровнях или в прикладном процессе.

10.4.7 Невозможность отказа от участия

– Невозможность отказа от участия – доказательство отправки.

– Невозможность отказа от участия – доказательство доставки.

Эта услуга может использоваться на уровне представления, на прикладном уровне или в самом прикладном процессе.

Вся эта информация сведена в таблицу 5.

Таблица 5/M.3016.0 – Связь услуг безопасности и эталонной модели ВОС

	Уровень						
Услуга	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Аутентификация пользователя	–	–	–	–	–	–	+
Аутентификация равноправного объекта	–	–	+	+	–	–	+
Аутентификация источника данных	–	–	+	+	–	–	+
Управление доступом на уровне ассоциации административного управления	–	–	+	–	–	–	+
Управление доступом к оповещению административного управления	–	–	–	–	–	–	+
Управление доступом к административно управляемому ресурсу	–	–	–	–	–	–	+
Сигнал нарушения безопасности, контрольный журнал и восстановление безопасного состояния	+	+	+	+	+	+	+
Целостность выбранного поля	–	–	–	–	–	–	+
Целостность соединения с восстановлением	–	–	–	+	–	–	+
Целостность соединения без восстановления	–	–	+	+	–	–	+
Конфиденциальность выбранного поля	–	–	–	–	–	–	+
Конфиденциальность соединения/без установления соединения	–	–	+	+	–	+	+
Конфиденциальность потока трафика	–	–	+	+	–	+	+
Невозможность отказа от участия – доказательство отправки	–	–	–	–	–	+	+
Невозможность отказа от участия – доказательство доставки	–	–	–	–	–	+	+

10.5 Управление безопасностью

Управление безопасностью включает все действия по организации, обслуживанию и завершающему этапу обеспечения безопасности системы.

Охватываются следующие вопросы:

– управление услугами безопасности;

– инсталляция механизмов безопасности;

– управление ключами (часть управления);

– установление идентичности, ключи, информация управления доступом и т. д.;

– управление данными контрольного журнала безопасности и сигналами нарушения безопасности.

Дополнение I

Функциональные классы и подпрофили обеспечения безопасности

I.1 Группирование мер безопасности

Меры безопасности могут быть сгруппированы в "функциональные классы" (FC). Следующее определение не включает в себя надежности меры безопасности:

Функциональный класс – это согласованный набор мер безопасности, предназначенных для выполнения требований меняющихся функциональных уровней.

I.1.1 Использование функциональных классов в случае междоменных действий

Безопасность СУЭ не должна испытывать отрицательного влияния результатов междоменных действий. Правила взаимодействия доменов должны быть определены в междоменной политике безопасности. Эти правила определяют, какие меры безопасности должны использоваться в каждом случае. Для упрощения достижения соглашения между взаимодействующими доменами эти меры безопасности можно отнести к отдельному функциональному классу.

I.1.2 Использование функциональных классов в случае внутридоменных действий

В случае внутридоменных действий функциональные классы могут упростить определение безопасности. FC могут также использоваться в целях обеспечения безопасности. Для достижения этого функциональные классы должны быть связаны с уровнем обеспечения, объявленным изготовителем средств управления. Этот вопрос находится в тесной связи с формальными критериями оценки.

Возможно, что для цели междоменного взаимодействия один оператор может потребовать применения отдельного FC для случая междоменных действий другого оператора. Причиной для этого может быть то, что не со всеми угрозами можно эффективно бороться в интерфейсе между двумя доменами. Решением для этого случая может быть обеспечение существования минимального уровня внутренней безопасности для взаимодействующих СУЭ. Стандарт безопасности СУЭ не должен предписывать, чтобы требовались FC, но должен разрешать возможность запроса некоторых FC посредством определения подходящих позиций для выбора.

I.2 Функциональные классы

Функциональные классы используются для определения сокращенной группы услуг безопасности, предназначенных для обеспечения некоторого уровня безопасности. В данном пункте создан набор функциональных классов, который служит примером того, каким образом можно определить функциональные классы. Функциональные классы *для X-интерфейса* предложены для трех различных уровней безопасности:

1) минимальный функциональный класс: (FC 1);

2) базовый функциональный класс: (FC 2);

3) улучшенный функциональный класс: (FC 3).

Для практических целей количество FC не должно быть слишком большим. С другой стороны, должна существовать возможность согласования требований различных организаций. Функциональные классы могут изменяться следующими способами:

– Функциональные классы, определенные только для X-интерфейса, могут также включать интерфейсы Q.

– Предполагается, что конфиденциальность должна быть необязательным свойством для всех классов по двум причинам:

  • это менее строгое требование;

  • обязательное включение в функциональный класс может иметь правовые последствия в отношении возможностей использования данного класса.

В таблице I.1 приведен обзор функциональных классов.

Таблица I.1/M.3016.0 – Функциональные классы услуг безопасности

FC 1	FC 2	FC 3
Основное назначение: обеспечение целостности сохраненных управляемых ресурсов	Основное назначение: обеспечение целостности сохраненных управляемых ресурсов и целостности переносимых данных	FC 2 плюс подотчетность операций по управлению
• Аутентификация (равноправный объект и пользователь) • Управление доступом на уровне ассоциации административного управления • Управление доступом к административно управляемым ресурсам • Сигналы нарушения безопасности, контрольный журнал и восстановление безопасного состояния	• Аутентификация (равноправный объект и пользователь) • Управление доступом на уровне ассоциации административного управления • Управление доступом к административно управляемым ресурсам • Аутентификация источника данных • Целостность выбранного поля • Целостность соединения • Сигналы нарушения безопасности, контрольный журнал и восстановление безопасного состояния	• Аутентификация (равноправный объект и пользователь) • Управление доступом на уровне ассоциации административного управления • Управление доступом к административно управляемым ресурсам • Аутентификация источника данных • Целостность выбранного поля • Целостность соединения • Невозможность отказа от участия в качестве источника • Невозможность отказа от участия в качестве пункта назначения • Сигналы нарушения безопасности, контрольный журнал и восстановление безопасного состояния
Необязательные свойства: • Целостность соединения • Конфиденциальность соединения	Необязательные свойства: • Конфиденциальность соединения • Конфиденциальность выбранного поля	Необязательные свойства: • Конфиденциальность соединения • Конфиденциальность выбранного поля

Кроме того, следует отличать FC, применимые для междоменного случая, от FC для внутридоменного случая. В обоих случаях требования будут различными, по этой причине меры безопасности также могут быть различными.

В следующей части представлен обзор различных случаев, что дает возможность выяснить, какие FC требуются и какие FC являются подходящими.

Допущение

Для каждого домена существует орган, ответственный за принятие решения о том, какие меры безопасности должны применяться в домене.

Различают три случая:

1) FC определяются органом домена и применимы в своем домене (внутри домена);
2) FC определяются органом домена и применимы при взаимодействиях доменов (между доменами). Выбор этих FC является результатом соглашения между органами взаимодействующих доменов;
3) FC определяются органом домена как требования по внутренней безопасности другого домена.

В каждом случае может быть определено количество FC для различных уровней безопасности.

Количество уровней безопасности подлежит дальнейшему изучению.

Набор мер безопасности, которые образуют FC, подлежит дальнейшему изучению.

В различных случаях FC могут быть одинаковыми, при этом сокращается общее количество FC.

Может быть также рассмотрен компромисс между различными случаями, например, когда междоменная безопасность находится на высоком уровне, требования по внутренней безопасности могут быть низкими, и наоборот. Другой возможностью может быть, что FC представляет минимальный набор мер безопасности, который может быть расширен введением дополнительных мер, когда это необходимо.

I.3 Профили безопасности

Функциональные классы не требуют использования стандартизованных механизмов безопасности; могут применяться любые механизмы, которые удовлетворяют этим требованиям.

Для обеспечения взаимодействия между мерами безопасности в различных доменах эти меры должны соответствовать стандартам. Предписание об использовании конкретных стандартов, которые вместе обеспечивают функциональный класс, называется профилем 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.