МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

E.408

(05/2004)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ E: ОБЩАЯ ЭКСПЛУАТАЦИЯ СЕТИ, ТЕЛЕФОННАЯ СЛУЖБА, ФУНКЦИОНИРОВАНИЕ СЛУЖБ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ

Управление сетью – Управление международной сетью

Требования к безопасности сетей электросвязи

Рекомендация МСЭ-Т E.408

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ E

ОБЩАЯ ЭКСПЛУАТАЦИЯ СЕТИ, ТЕЛЕФОННАЯ СЛУЖБА, ФУНКЦИОНИРОВАНИЕ СЛУЖБЫ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ

МЕЖДУНАРОДНАЯ ЭКСПЛУАТАЦИЯ	
Определения терминов	E.100–E.103
Общие положения, касающиеся администраций	E.104–E.119
Общие положения, касающиеся пользователей	E.120–E.139
Эксплуатация международных телефонных служб	E.140–E.159
План нумерации в международной телефонной службы	E.160–E.169
Международный план маршрутизации	E.170–E.179
Тональные сигналы в национальных системах сигнализации	E.180–E.189
План нумерации для международной телефонной службы	E.190–E.199
Морская подвижная служба и сухопутная подвижная служба общего пользования	E.200–E.229
ЭКСПЛУАТАЦИОННЫЕ ПОЛОЖЕНИЯ, ОТНОСЯЩИЕСЯ К НАЧИСЛЕНИЮ ПЛАТЫ И РАСЧЕТАМ В МЕЖДУНАРОДНОЙ ТЕЛЕФОННОЙ СЛУЖБЕ	
Начисление платы в международной телефонной службе	E.230–E.249
Измерение и регистрация продолжительности разговора для целей расчетов	E.260–E.269
ИСПОЛЬЗОВАНИЕ МЕЖДУНАРОДНОЙ ТЕЛЕФОННОЙ СЕТИ ДЛЯ НЕТЕЛЕФОННЫХ СЛУЖБ	
Общие положения	E.300–E.319
Фототелеграфия	E.320–E.329
ПОЛОЖЕНИЯ ПО ЦСИС, ОТНОСЯЩИЕСЯ К ПОЛЬЗОВАТЕЛЯМ	E.330–E.349
МЕЖДУНАРОДНЫЙ ПЛАН МАРШРУТИЗАЦИИ	E.350–E.399
УПРАВЛЕНИЕ СЕТЬЮ	
Статистические данные по международной службе	E.400–E.404
Управление международной сетью	**E.405–E.419**
Контроль качества международной телефонной службы	E.420–E.489
ТЕХНИЧЕСКИЕ АСПЕКТЫ ТРАФИКА	
Измерение и регистрация трафика	E.490–E.505
Прогнозирование трафика	E.506–E.509
Определение числа каналов при ручном обслуживании	E.510–E.519
Определение числа каналов при автоматическом и полуавтоматическом обслуживании	E.520–E.539
Качество обслуживания трафика	E.540–E.599
Определения терминов	E.600–E.649
Технические аспекты трафика для IP-сетей	E.650–E.699
Технические аспекты трафика в ЦСИС	E.700–E.749
Технические аспекты трафика в сети подвижной связи	E.750–E.799
КАЧЕСТВО УСЛУГ ЭЛЕКТРОСВЯЗИ: ПОНЯТИЯ, МОДЕЛИ, НОРМЫ И ПЛАНИРОВАНИЕ НАДЕЖНОСТИ РАБОТЫ	
Термины и определения, связанные с качеством услуг электросвязи	E.800–E.809
Модели для услуг электросвязи	E.810–E.844
Нормы на качество обслуживания и понятия, связанные с услугами электросвязи	E.845–E.859
Использование норм на качество обслуживания для планирования сетей электросвязи	E.860–E.879
Сбор данных по эксплуатации и оценка рабочих характеристик оборудования, сетей и служб	E.880–E.899

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

Рекомендация МСЭ-Т E.408

Требования к безопасности сетей электросвязи

Резюме

В настоящей Рекомендации приводятся обзор требований к безопасности и структура, которая опознает угрозы безопасности для сетей электросвязи в общем виде (как для фиксированной, так и для подвижной связи; как для голоса, так и для данных), а также дается руководство по планированию мер противодействия, которые могут быть приняты для уменьшения рисков, создаваемых угрозами.

Источник

Рекомендация МСЭ-Т E.408 утверждена 28 мая 2004 года 2-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т E.408

Требования к безопасности сетей электросвязи

1 Введение

1.1 Область применения

В настоящей Рекомендации приводятся обзор и структура, которая опознает угрозы безопасности для сетей электросвязи в общем виде (как для фиксированной, так и для подвижной связи; как для голоса, так и для данных), а также дается руководство по планированию мер противодействия, которые могут быть приняты для уменьшения рисков, создаваемых угрозами.

Данная Рекомендация является общей по своему характеру, она не определяет требований для конкретных сетей и не ссылается на них.

В настоящей Рекомендации не предпринимается попытка определения новых услуг безопасности, а используются существующие услуги безопасности, определенные в других Рекомендациях МСЭ-Т и соответствующих стандартах других органов.

Данная Рекомендация предназначена в помощь при международном сотрудничестве в следующих областях безопасности сетей электросвязи:

- совместное использование и распространение информации;
- координация при инциденте и ответные действия при кризисе;
- набор и обучение специалистов по безопасности;
- координация правоприменения;
- защита основной инфраструктуры и основных услуг;
- разработка соответствующего законодательства.

Для достижения такого сотрудничества в отношении национальных компонентов сети необходима реализация требований данной Рекомендации на национальном уровне.

1.2 Ссылки

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

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

– ITU-T Recommendation M.3016 (1998), *TMN security overview*.

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

– ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

– ITU-T Recommendation X.741 (1995) | ISO/IEC 10164-9:1995, *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) | ISO/IEC TR 13594:1995, *Information technology – Lower layers security model*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

– ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

– ITU-T Recommendation X.814 (1995) | ISO/IEC 10181-5:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.

– ITU-T Recommendation X.815 (1995) | ISO/IEC 10181-6:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.

– ITU-T Recommendation X.816 (1995) | ISO/IEC 10181-7:1996, *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*.

– IETF RFC 2535 (1999), *Domain Name System Security Extensions*.

– IETF RFC 2870 (2000), *Root Name Server Operational Requirements*.

– IETF RFC 3013 (2000), *Recommended Internet Service Provider Security Services and Procedures*.

1.3 Использование термина "service"

Термин "service" (служба/услуга), встречающийся в данной Рекомендации, не относится к каким-либо службам/услугам, определенным МСЭ. Он используется в качестве общего термина при обсуждении вопросов и/или функций безопасности и должен быть определен в будущем.

1.4 Обоснование

Требования к общей структуре сетевой безопасности обусловлены совокупностью различных факторов:

– **Потребителям/абонентам** необходимо испытывать доверие к предлагаемым сетям и услугам, включая готовность услуг (особенно экстренного обслуживания) в условиях крупных катастроф (включая террористические акты).

– **Органы/объединения государственной власти** предъявляют требования к безопасности, издавая директивы и применяя законодательство, с тем чтобы обеспечить готовность услуг, добросовестную конкуренцию и защиту частной жизни.

– **Операторы сетей и поставщики услуг** сами нуждаются в обеспечении безопасности для защиты своих эксплуатационных и коммерческих интересов и выполнения своих обязательств перед потребителями и населением.

Требования к безопасности сетей и услуг электросвязи должны базироваться преимущественно на согласованных на международном уровне стандартах безопасности, поскольку выгоднее использовать уже существующие, чем разрабатывать новые. Предоставление и использование услуг и механизмов, обеспечивающих безопасность, может быть довольно дорогим относительно стоимости защищаемых транзакций. Таким образом, важным фактором является возможность определить параметры безопасности в соответствии с услугами, подлежащими защите. Используемые услуги и механизмы обеспечения безопасности должны предоставляться таким образом, который допускает указанную параметризацию. Учитывая большое количество возможных сочетаний функций обеспечения безопасности, желательно иметь **профили безопасности** (см. Добавление II), охватывающие широкий диапазон сетевых услуг электросвязи.

Содействовать **повторному применению решений и продуктов** будет стандартизация, ускоряющая обеспечение безопасности и делающая ее менее дорогой.

Существенными преимуществами применения стандартизованных продуктов и для продавцов, и для пользователей систем являются экономия масштаба при разработке продуктов и функциональная совместимость компонентов в среде сети электросвязи в отношении безопасности.

Услуги и механизмы обеспечения безопасности, которые могут быть использованы в сетях электросвязи или поставщиками услуг, относятся к средствам защиты от преднамеренных атак, таких как отказ в обслуживании, подслушивание, имитация соединения, искажение сообщений (изменение, задержка, удаление, вставка, повторная передача перехваченного сообщения, перемаршрутизация, неправильная маршрутизация или изменение порядка следования сообщений), непризнание участие или подлог. Защита включает предупреждение, локализацию и восстановление после атаки, а также управление связанной с безопасностью информацией. Защита также должна включать меры по предотвращению прерываний в обслуживании вследствие естественных событий (погодные условия и т. д.). Должны быть определены условия, разрешающие подслушивание и наблюдение по запросу должным образом уполномоченных правоприменительных органов.

2 Описание системы

Для эффективного обеспечения безопасности в сети рекомендуется реализовать уровни безопасности; чем больше уровней введено, тем более эффективно обеспечивается безопасность. Этот метод построения уровней можно проанализировать снизу вверх:

АУДИТ БЕЗОПАСНОСТИ
ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭЛЕКТРОСВЯЗИ
МОНИТОРИНГ
ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ
СЕТЕВОЙ АДМИНИСТРАТОР

Рисунок 1/E.408 – Шесть уровней для обеспечения безопасности сети

Термин "уровень", используемый в настоящей Рекомендации, служит лишь для описания некоторых соображений в отношении безопасности, которые касаются организации сетевой безопасности. Уровни в настоящей Рекомендации не следует рассматривать в качестве элементов архитектуры и их не следует путать с уровнями безопасности из Рекомендации МСЭ-Т X.805.

Подобно фундаменту дома первый уровень – сетевые администраторы – является основой конфигурации сетевой безопасности. Ежегодное расходование дополнительных средств на хорошего сетевого администратора более эффективно, чем покупка дорогого брандмауэра. Хорошие сетевые администраторы понимают операционную систему, в которой они работают, и знают, как проводить каждую машину по сети, с тем чтобы разрешить проход только через те порты и процессы, через которые следует пройти. Административное управление должно обеспечивать администраторам сети

возможность непрерывного обучения и время, чтобы предвидеть сетевые сбои и обеспечивать рациональное использование сети.

Вторым уровнем является физическая безопасность. Любой нарушитель в мире знает, что самый легкий путь получения доступа в сеть – путь изнутри. Отмечено очень много случаев "социально-технических нападений", когда нарушители просто обращались в службу помощи, заявляли, что забыли свой пароль и просили службу помощи сменить его на xxxxx. Физическая безопасность охватывает все: от предоставления только определенным лицам (системным администраторам) доступа к пультам до принятия решения о том, какую информацию о сети организации делать открытой. Верная политика в отношении допустимого использования, паролей и установки программного обеспечения весьма эффективно помогает организациям управлять доступом к своим сетям.

Третьим уровнем является мониторинг. Очень редко атака завершается успешно с первой попытки. Большинство атак возможно остановить, если по меньшей мере раз в день тщательно анализировать системные журналы регистрации. Это не потребует так много времени, как может показаться вначале. Человеческий глаз является лучшим прибором для выявления закономерностей в журналах регистрации. Существуют несколько хороших программ мониторинга журналов регистрации, и несмотря на то, что эти программы могут быть весьма полезными, системному администратору следует прочитывать журнал регистрации его главной машины каждый день.

Четвертым уровнем является программное обеспечение электросвязи. Каждая часть программного обеспечения, установленная на серверах, должна оцениваться в аспекте безопасности. Системный администратор должен знать, например, какие порты TCP и UDP будет использовать это программное обеспечение, с какими пользовательскими счетами будет взаимодействовать программа, и какие разрешения доступа к каталогу требует программа. Рекомендуется также перед приобретением провести проверку известных недостатков системы безопасности. Это должно стать частью процесса оценки при приобретении любого программного обеспечения.

Пятым уровнем являются инструменты обеспечения безопасности. После того как приняты подходящие политика и практика в отношении предыдущих четырех уровней, следует приступать к анализу брандмауэров, программного обеспечения обнаружения проникновений и посреднических программ. Установка лучшего в мире брандмауэра с неподходящей политикой в отношении межсетевой защиты будет хуже, чем полное отсутствие брандмауэра. Слишком часто можно встретить сетевые серверы с неудовлетворительными методами обеспечения безопасности, зависящими от одного брандмауэра, который должен все время держать нарушителей под контролем. Как только такой брандмауэр оказывается вскрытым, все серверы широко открываются для атаки.

Шестым уровнем является аудит безопасности. Сетевая безопасность представляет собой движущуюся цель. Каждый день кто-то где-то находит новый метод взлома сетевой безопасности. Важно, чтобы организации регулярно пытались постигать свои собственные сети. Некоторый контрольный механизм (аудит) должен проверять каждый аспект сетевой безопасности. Рекомендуется тестирование устойчивости сети к физическим атакам ее системы безопасности, а некоторый "боевой номеронабиратель" должен набирать все телефонные номера, с тем чтобы гарантировать, что в компьютер не установлены модемы без ведома сетевого администратора. Аудит следует выполнять для почтового сервера, DNS, домена, Web и FTP серверов.

2.1 Участники и функции

Для целей стандартизации сетей электросвязи следует рассматривать только техническую безопасность; то есть рассматриваемыми участниками являются *Участники электросвязи* (Telecommunication Actors, TAs). ТА – это лицо (физическое или юридическое), либо процесс, ответственный за определенные операции в сети.

Каждый раз при выполнении действия ТА берет на себя определенную функцию. В некоторых случаях это будет взаимо-однозначное соответствие между ТА-пользователем и функцией, то есть ТА всегда будет оставаться в одной роли. В других случаях это будет взаимоотношение "один–множество" между конкретным ТА-пользователем и возможными функциями, которые способен выполнять ТА.

Ниже приводится классификация на высоком уровне для некоторых общих функций:

– оператор сети (*государственный или частный*);

– поставщик услуг (*поставщик услуг переноса или поставщик дополнительных услуг*);

– абонент услуги/клиент услуги;

– конечный пользователь услуги;

– продавец аппаратного/программного обеспечения;

– доверенная третья сторона.

2.2 Домены безопасности для сетей электросвязи

Домен безопасности – это набор объектов или сторон, который является объектом одной политики безопасности и одной администрации безопасности.

При проектировании сетевой безопасности могут рассматриваться различные домены и субдомены, с тем чтобы определить и разграничить ответственности по административному управлению сетью и управлению безопасностью.

Для разделения сети на домены должны быть учтены по меньшей мере следующие аспекты:

- Физические границы сети
- Области ответственности
- Функциональные области
- Критичность приложений и данных, передаваемых по сетям
- Потенциальные географические границы (в помещении, для региона и т. д.)
- Потребные/доступные трафик и пропускная способность
- Потребности в непрерывной работе и восстановлении
- Домен бизнес-приложений
- Домен бизнес-поддержки (выставление счетов, управление людскими ресурсами и т. д.)
- Домены развития и тестирования
- Домены производства
- Домен управления при авариях
- Ответственности управляющих и диспетчеров за сетевую безопасность.

Интерфейсы основного уровня обычно находятся в зоне изменения ответственности. Интерфейсами между рабочей средой и офисной средой или тестирующей средой обычно являются границы между сетевыми функциями. Каждая точка доступа к домену и субдомену нуждается в шлюзе, который может обеспечить разные услуги безопасности, такие как управление трафиком, управление доступом и т. д.

3 Общие задачи безопасности для сетей электросвязи

Назначением данного раздела является описание конечной цели мер безопасности, используемых в сетях электросвязи. Акцент делается на требования безопасности, которые должны выполняться, а не на то, как это сделать.

Задачи безопасности для сетей электросвязи формулируются следующим образом.

– Только легитимные участники должны иметь возможность доступа к сетям электросвязи и их использования.

– Легитимные участники должны иметь возможность доступа и работы с ресурсами, доступ к которым был им разрешен.

– Сети электросвязи должны обеспечивать секретность на уровне, определенном политикой безопасности в данной сети.

– Все участники должны нести ответственность за свои, и только свои действия в сетях электросвязи.

– Чтобы обеспечить доступность, сети электросвязи должны быть защищены от непредусмотренных доступа или действия.

– Должна быть обеспечена возможность получения от сетей электросвязи информации, относящейся к безопасности (но только легитимные участники должны иметь возможность запросить такую информацию).
– При обнаружении нарушений безопасности они должны обрабатываться управляемым способом согласно заранее определенному плану, с тем чтобы минимизировать потенциальный ущерб.
– При обнаружении взлома безопасности должна существовать возможность восстановления нормальных уровней безопасности.
– Архитектура безопасности сетей электросвязи должна обеспечивать определенную гибкость, чтобы поддерживать разные стратегии безопасности, например различную эффективность механизмов безопасности.

Термин "доступ к ресурсам" следует понимать как возможность не только выполнять функции, но также читать информацию.

Общие задачи формируются согласно точке зрения и языку менеджмента предприятия. Последующие разделы следует излагать в более технических терминах, сводящихся к реализуемым услугам и функциям безопасности. Взаимосвязь между этими двумя языками не всегда очевидна.

Может быть показано, что решение следующей ниже совокупности задач обеспечит решение первых пяти перечисленных выше в данном разделе задач безопасности для сетей электросвязи:

– конфиденциальность;
– целостность данных (несомненно, требуется также целостность системных программ, иначе вероятны атаки типа "отказ в обслуживании");
– отчетность, включая аутентификацию, фиксацию авторства и управление доступом;
– готовность.

В основе определений угроз и рисков, данных в разделе 5, ниже, а также функциональных требований в разделе 6 лежат эти более формальные термины. Определения терминов см. в разделе 5.

Остальные задачи относятся к контролю и управлению состоянием безопасности системы. Они будут рассмотрены в соответствующих разделах, посвященных восстановлению, архитектуре и управлению безопасностью применительно к реализуемой стратегии безопасности.

4 Вопросы законодательства

Инфраструктура безопасности в сети электросвязи должна обладать способностью приспосабливаться к ограничениям, которые налагаются государственными законами, контрактным законодательством, договорами и правилами. Эти ограничения могут включать обязательные услуги безопасности (такие как гарантии секретности информации о клиенте), исключать некоторые механизмы безопасности (такие как некоторые типы шифрования) и/или разрешать прослушивание правоохранительными органами.

5 Угрозы и риски

Целью данного раздела является анализ угроз и рисков для сетей электросвязи. Не ставится задача давать оценки конкретных рисков или анализировать угрозы для отдельных типов сетей электросвязи. Это – частные вопросы, которые могут решаться отдельно каждым оператором и не влиять на взаимодействие.

Угроза – это потенциальное нарушение безопасности. Согласно определенным общим задачам безопасности угрозы могут быть направлены на задачи четырех разных типов:

– **конфиденциальность** (конфиденциальность хранимой или переносимой информации);
– **целостность данных** (защита хранимой или переносимой информации);
– **целостность системы** (защиты операционной системы);
– **отчетность** (каждый объект должен быть ответственен за любые инициированные им действия); и

– **готовность** (все легитимные объекты должны получать корректный доступ к сетям электросвязи).

В настоящей Рекомендации различаются три вида угроз:

– случайная угроза: угроза, источник которой не преследует злого умысла;

– административная угроза: угроза, которая возникает из-за отсутствия администрирования безопасности; и

– намеренная угроза: угроза, которую создает объект, имеющий злой умысел, который может атаковать либо саму сеть электросвязи, либо сетевые ресурсы.

Случайные и административные угрозы могут быть учтены при стандартизации, поскольку их последствия такие же, как у намеренных угроз. Для более точного анализа угроз в данной Рекомендации рассматриваются в основном намеренные угрозы. Цель такого подхода – дать более короткий список угроз, который можно непосредственно использовать в деятельности по стандартизации. Вследствие этого анализ угроз должен охватывать следующие вопросы, исходя из Рекомендации МСЭ-Т X.800:

– **нелегальное проникновение (имитация соединения)**: объект предпринимает попытку представить себя другим объектом;

– **подслушивание**: нарушение конфиденциальности путем наблюдения за электросвязью;

– **несанкционированный доступ**: объект пытается получить доступ к данным в нарушение действующей стратегии безопасности;

– **потеря или искажение информации**: целостность переносимых данных поставлена под угрозу из-за несанкционированных уничтожения данных, вставки, изменения, изменения порядка следования, повторный передачи или задержки;

– **непризнание авторства**: объект, который участвовал в обмене по сети электросвязи, впоследствии отрицает этот факт;

– **подлог**: объект подделывает информацию и заявляет, что эта информация была получена от другого объекта или передана другому объекту;

– **отказ в обслуживании**: происходит, когда объект не выполняет свою функцию или препятствует другим объектам выполнять их функции. Может включать отказ в доступе к сетям электросвязи и отказ в проведении связи путем лавинной загрузки сетей электросвязи или компонентов сети. В коллективно используемой сети эта угроза может быть распознана как подделка дополнительного трафика, который перегружает сеть, препятствуя другим объектам в использовании сети из-за задержки их трафика.

В таблице 1 показано взаимоотношение угроз и задач.

Таблица 1/E.408 – Взаимоотношение угроз и задач

Угрозы	**Задачи**			
	Конфиден-циальность	**Целостность системы или данных**	**Отчетность**	**Готовность**
Нелегальное проникновение	x	x	x	x
Подслушивание	x			
Несанкционированный доступ	x	x	x	x
Потеря или искажение информации (переносимой)		x		x
Непризнание участия			x	
Подлог		x	x	
Отказ в обслуживании				x

Потенциальная угроза для системы необязательно вредна, если отсутствует соответствующее слабое место в системе или если такое слабое место не используется угрозой.

Каждая угроза означает риск. Оценка риска может быть разделена на оценку вероятности каждой угрозы и оценку воздействия, которое может иметь угроза. Оценки угрозы и риска должны быть частями итеративного процесса: появление новых угроз возможно при принятии контрмер, например угрозы криптографическим ключам возникают в результате реализации криптографических мер.

6 Требования к безопасности

На рисунке 2 показаны взаимоотношения между задачами безопасности: угрозы, риски, требования к безопасности и услуги. Он отображает процесс получения "Требований к безопасности" из "Угроз" и "Задач безопасности", которые, в свою очередь, будут реализованы набором услуг безопасности. Эти "Услуги", которые противодействуют угрозам, будут использовать "Механизмы", которые сами используют "Алгоритмы безопасности". Данный процесс показан на рисунке 2.

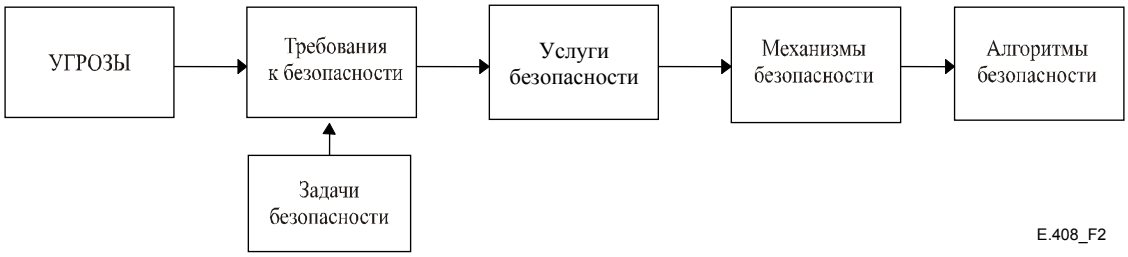

Рисунок 2/E.408 – Полученные требования к безопасности

В разделе 6.1 перечислены такие требования к безопасности. Если не указано иное, то слово "требование" в данной Рекомендации не означает, что какая-либо функциональная возможность всегда обязательна в каждой сети электросвязи; оно означает, что какая-либо функциональная возможность может быть сделана обязательной сетевым диспетчером для некоторых конкретных услуг, приложений и/или интерфейсов этой сети. Фактический выбор будет зависеть от задач безопасности, определенных оператором в стратегии обеспечения безопасности.

Кроме требований к безопасности и услуг безопасности в данном разделе определяются некоторые общие требования к административному управлению услугами безопасности (см. п. 6.2) и архитектурные требования, регулирующие интеграцию услуг безопасности в общую сетевую архитектуру (см. п. 6.3). Административные требования и требования к сроку службы важны, но они не будут влиять на архитектуру и не рассматриваются в настоящем разделе.

Рассматриваемые требования к безопасности могут применяться к любой концепции безопасности в архитектуре безопасности, стандартизованной в Рекомендации МСЭ-Т X.805. Параметры безопасности (также введенные в Рекомендации МСЭ-Т X.805) разработаны для удовлетворения требований к безопасности для каждой концепции безопасности. Услуги безопасности, механизмы безопасности и алгоритмы безопасности, рассматриваемые в настоящей Рекомендации, следует рассматривать как неотъемлемые части каждого параметра безопасности.

6.1 Требования к безопасности и соответствующие услуги

В данном разделе описывается набор общих функциональных требований и соответствующие услуги, которые могут использоваться для противодействия угрозам в сетях электросвязи.

6.1.1 Взаимоотношения функциональных требований, угроз и задач безопасности

В данном разделе определяются функциональные требования к безопасности для охвата тех угроз, которые перечислены в разделе 5. Они представлены в таблице 2. Требования к безопасности далее отображаются (таблица 3) в задачи безопасности, определенные в разделе 3. Список ограничен требованиями, которые по своему характеру являются общими и существенно влияют на компоненты и архитектуру.

Таблица 2/E.408 – Взаимосвязь функциональных требований и угроз

Функциональные требования	Угрозы						
	Нелегальное проникновение	Подслу-шивание	Несанкцио-нированный доступ	Потеря или искажение информации	Непризна-ние участия	Подлог	Отказ в обслужи-вании
Подтверждение идентификационной информации	x		x				
Управляемый доступ и авторизация			x				x
Защита конфиденциальности		x	x				
Защита целостности данных				x			
Отчетность					x	x	
Регистрация действий	x		x		x	x	x
Аварийное уведомление	x		x	x			x
Аудит	x		x		x	x	x

Поставленные задачи являются четырьмя формальными задачами, определенными в разделе 3, они помещены в столбцах таблицы 3, показывающей набор функциональных требований для решения рассматриваемых задач.

6.1.2 Описание функциональных требований и соответствующих функций

Функциональные требования из таблиц 2 и 3 подробнее обсуждаются далее, и для каждого требования определяются соответствующие функции безопасности. Заметим, что требования к любой из этих функций не означают автоматического введения какой-либо услуги безопасности, определенной ИСО. На практике, однако, в некоторых случаях наблюдается соответствие.

Таблица 3/E.408 – Взаимосвязь задач безопасности и функциональных требований

Функциональные требования	Задачи безопасности			
	Конфиден-циальность	Целостность системы данных	Отчетность	Готовность
Подтверждение идентификационной информации	x	x	x	
Управляемый доступ и авторизация	x	x	x	x
Защита конфиденциальности	x	x		
Защита целостности системы или данных		x		
Отчетность			x	
Регистрация действий			x	x
Аварийное извещение	x	x	x	x
Аудит			x	x

ПРИМЕЧАНИЕ. – Соблюдение конфиденциальности данных является достаточным условием для поддержания целостности данных, это означает, что если данные можно сохранить конфиденциальными, то они будут защищены от изменения. Однако защита от изменения необязательно защищает их от разглашения.

6.1.2.1 Подтверждение идентификационной информации

Сеть электросвязи должна обеспечивать возможность установления и подтверждения представленной идентификационной информации любого участника в этой сети электросвязи.

Участниками могут быть пользователи – лица или объекты внутри сети электросвязи. Подтверждаемая идентификационная информация составляет базу отчетности и является важнейшим фактором для удовлетворения большинства требований к безопасности, перечисленных в данном разделе.

Услугой безопасности для поддержки этого требования является **аутентификация**. Функция аутентификации предоставляет доказательство того, что объект или субъект на самом деле имеет ту идентификационную информацию, которую он предъявил. В зависимости от типа участника и цели идентификации могут потребоваться следующие виды аутентификации:

– аутентификация пользователя, обеспечивающая подтверждение идентификационной информации пользователя-человека или прикладного процесса;

– аутентификация равноправного объекта, обеспечивающая подтверждение идентификационной информации равноправного объекта при взаимодействии по электросвязи;

– аутентификация отправителя данных, обеспечивающая подтверждение идентификационной информации ответственного за конкретный блок данных.

Использование функции аутентификации обеспечивает подтверждение для определенного момента времени. Для того чтобы гарантировать непрерывное подтверждение, аутентификация должна выполняться повторно или связываться с услугой обеспечения целостности.

Примерами механизмов, используемых для реализации услуги аутентификации, являются пароли или персональные идентификационные номера (Personal Identification Numbers, PINs) (простая аутентификация) и методы на основе криптографии (жесткая аутентификация).

6.1.2.2 Управляемый доступ и авторизация

Сеть электросвязи должна гарантировать предотвращение получения участниками доступа к информации или ресурсам, доступ к которым им не разрешен.

Услугой безопасности, которая отвечает этому требованию, является **управление доступом**. Услуга управления доступом обеспечивает средства гарантирования того, что ресурсы будут доступны субъектам только разрешенным образом. Рассматриваемыми ресурсами могут быть физическая система, системное программное обеспечение, приложения и данные. Функция управления доступом может быть определена и реализована на разных уровнях детализации в сети электросвязи: на уровне агента, объекта или атрибута. Ограничения на доступ размещаются в информации управления доступом, которая указывает:

– средства, которые определяют, каким объектам разрешено иметь доступ;

– какой вид доступа разрешен (чтение, запись, изменение, создание, уничтожение).

Более конкретно, управление доступом в сети электросвязи может быть разделено на три типа:

– *Управление доступом к ассоциации административного управления*

  Дает возможность управлять доступом на уровне ассоциаций административного управления; это означает, что права доступа относятся к самой ассоциации, то есть означает право установить эту ассоциацию.

– *Управление доступом к извещениям административного управления*

  Дает возможность управлять доступом в части извещений, то есть гарантирует, что эти извещения раскрываются только тем объектам, которые имеют разрешение принимать их.

– *Управление доступом к управляемым ресурсам*

  Обеспечивает управление доступом в отношении самих ресурсов.

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

6.1.2.3 Защита конфиденциальности

Сеть электросвязи должна обеспечивать возможности гарантирования конфиденциальности хранимых и передаваемых данных.

Это требование поддерживается следующими услугами безопасности: **управление доступом** для систем, **управление доступом** для хранимых данных и **конфиденциальность данных**, передаваемых с помощью электросвязи.

Взлом конфиденциальности системы не следует игнорировать, так как он часто является предшественником атак на целостность системы или данных (помогает нарушителю в отыскании уязвимости типа "отказ в обслуживании").

Услуга конфиденциальности обеспечивает защиту от несанкционированного раскрытия хранимых или передаваемых данных. Различают следующие виды конфиденциальности:

– конфиденциальность системы (включая различную информацию, такую как информация об архитектуре и конфигурации, используемые алгоритмы, номера версий программного обеспечения, типы используемой аппаратуры и т. д.);

– выборочная конфиденциальность полей;

– конфиденциальность соединения;

– конфиденциальность потока данных.

6.1.2.4 Защита целостности системы или данных

Сеть электросвязи должна быть в состоянии гарантировать целостность систем, а также хранимых и передаваемых данных.

Услугами безопасности, которые удовлетворяют этому требованию, являются: **управление доступом** для систем, **управление доступом** для хранимых данных и **целостность данных** для передаваемых данных.

Услуга целостности обеспечивает средства, гарантирующие корректность системных файлов и пересылаемых данных, что защищает их от изменения, уничтожения, создания (вставки) и повторной передачи данных обмена. Различают следующие виды целостности:

– целостность операционной системы;

– выборочная целостность полей;

– целостность соединения без восстановления;

– целостность соединения с восстановлением.

6.1.2.5 Отчетность

Сеть электросвязи должна обладать неким свойством, гарантирующим, что любой объект не может отказаться от ответственности за любые выполненные им действия, а также за их последствия. Например, сеть электросвязи должна обеспечивать средства, подтверждающие, что объект выполнил определенные действия.

Это требование удовлетворяется услугой **защиты от непризнания участия**, которая связывает человека (или объект) с выполненной операцией. Услуги защиты от непризнания участия обеспечивают средства, которые гарантируют, что перенос данных осуществлен фактически и что пользователи осведомлены об использовании услуги или продукта в легитимной среде (например, осведомленность о том, что использование контролируется и т. д., обычно достигается с помощью регистрационных заголовков). Это сводится к трем формам:

– защита от непризнания участия: доказательство источника;

– защита от непризнания участия: доказательство доставки;

– защита от непризнания участия: доказательство знания легитимной среды.

Другая более общая и, возможно, менее эффективная реализация отчетности достигается соответствующей комбинацией услуг **аутентификации**, **управления доступом** и **данных проверки**.

6.1.2.6 Регистрация действий, аварийное извещение и аудит

Эти требования обусловливают необходимость сохранять и анализировать информацию о действиях, связанных с безопасностью, внутри сети электросвязи. Соответствующими услугами являются **регистрация действий**, **аудиторский журнал** и **аварийное извещение**. Каждое из этих требований подробно обсуждается ниже.

6.1.2.6.1 Регистрация действий

Сеть электросвязи должна обладать свойством сохранять информацию о действиях в системе с возможностью прослеживать эту информацию до конкретных лиц или объектов.

Журнал регистрации является хранилищем записей: он является согласно ВОС абстракцией ресурсов регистрации в реальных открытых системах. Записи содержат информацию, которая регистрируется.

Для многих функций административного управления необходимо обладать свойством сохранять информацию о событиях, которые произошли, или об операциях, которые были выполнены различными ресурсами или с различными ресурсами, либо об операциях, которые были выполнены или предпринималась попытка их выполнения ресурсами или с ресурсами.

Кроме того, когда такая информация запрашивается из журнала регистрации, диспетчер в любой момент времени должен иметь возможность обнаружить факт потери записи или факт изменения характеристики записей, сохраненных в журнале регистрации.

Поскольку файлы журнала регистрации составляют часть системных данных, это требование также обусловливает требования, определенные в п. 6.1.2.4 и, возможно, в п. 6.1.2.3.

6.1.2.6.2 Аварийное извещение безопасности

Сеть электросвязи должна обладать свойством генерировать аварийные извещения об отдельных событиях. Пользователь должен иметь возможность определять критерии для выбора.

Функция управления аудитом безопасности является одной из функций административного управления системами, описывающей уведомление о совокупности событий безопасности. Аварийное извещение безопасности, определенное этой функцией административного управления системами, дает информацию об эксплуатационном состоянии, влияющем на безопасность.

6.1.2.6.3 Аудит безопасности

Сеть электросвязи должна обладать способностью анализировать данные регистрации событий, относящихся к безопасности, с целью их проверки на наличие нарушений стратегии безопасности.

Аудит следует рассматривать в качестве независимого обзора и анализа системных записей и действий с целью контроля системных средств управления на адекватность, гарантирования соответствия принятым стратегии безопасности и эксплуатационным процедурам, а также обнаружения взломов систем безопасности. Результатом аудита может стать изменение в управлении, стратегии и процедурах.

В таблице 4 дается обзор взаимосвязи требований и услуг безопасности. В данном разделе определяются только те услуги безопасности, которые охватываются стандартными средствами, другие возможные услуги (например, обнаружение отказа в обслуживании) не включены.

Таблица 4/E.408 – Взаимосвязь требований к безопасности и услуг безопасности

Функциональное требование	Услуга безопасности
Подтверждение идентификационной информации	аутентификация пользователя аутентификация равноправного объекта аутентификация источника данных
Управляемый доступ и авторизация	управление доступом
Защита целостности системы	управление доступом
Защита конфиденциальности – хранимые данные	управление доступом
Защита конфиденциальности – переносимые данные	конфиденциальность
Защита целостности данных – хранимые данные	управление доступом
Защита целостности данных – переносимые данные	целостность
Отчетность	защита от непризнания участия
Регистрация действий	аудиторский журнал
Аварийное извещение безопасности	аварийный сигнал безопасности
Аудит безопасности	аудиторский журнал и восстановление

ПРИМЕЧАНИЕ. – Приведенные ниже требования не совпадают с теми, которые определялись ранее, выше таблицы 4, и не могут считаться безусловными объектами для какой-либо Рекомендации. Тем не менее, их следует учитывать на этапе проектирования вместе с реализацией базовых требований к безопасности сетей электросвязи, которые были определены выше.

6.1.2.6.4 Целостность системы

Критически важно, чтобы программная и аппаратная среда реализованных функций безопасности поддерживала запрошенный уровень безопасности.

Это включает корректную конфигурацию операционных систем и исключение системных дефектов.

Данные аспекты не формируют часть функционального профиля безопасности, но они учитываются в его спецификации, с тем чтобы гарантировать эффективность этих функций в реальной рабочей среде.

6.1.2.6.5 Замечания в отношении готовности

Требование в отношении готовности не подразумевают одну услугу или ограниченный набор услуг безопасности, которые способны выполнить это требование. Все перечисленные здесь услуги безопасности должны образовать согласованный набор услуг, которые в совокупности способны обеспечивать готовность. Услуги безопасности сами по себе, однако, не смогут гарантировать готовность: она зависит также от надежности аппаратных и программных средств (с точки зрения как проектирования, так и реализации).

6.2 Требования к административному управлению безопасностью

Сеть электросвязи должна содержать информационные модели и обладать функциями административного управления для услуг, используемых при обеспечении безопасности сети электросвязи.

Детальные требования к административному управлению безопасностью устанавливают, какие управляющие приложения следует ввести и как они должны быть спроектированы. Это делается для того, чтобы обеспечить администратора безопасности надлежащими инструментами контроля услуг безопасности и управления ими эффективным и корректным образом. Задачи и цели административного управления безопасностью ставятся для трех разных уровней системы электросвязи, которые соответствуют административному управлению безопасностью систем, услугам безопасности и механизмам безопасности, соответственно.

После взлома безопасности должно обеспечиваться восстановление безопасного состояния системы.

В случае взлома безопасности сеть электросвязи должна быть способна обработать эту попытку управляемым образом, то есть эта попытка не должна привести к значительному ухудшению работы сети электросвязи в аспекте готовности.

Операции и информация, относящиеся к административному управлению услугами электросвязи в сетях электросвязи, требуют специального рассмотрения с точки зрения безопасности. Секретные ключи шифрования, информация аутентификации и списки управления доступом служат примерами областей, для которых требуемая эффективность защиты может быть выше, чем для управления сетью.

6.3 Услуги безопасности и уровни ВОС

В данном разделе определено, какие уровни ВОС используются для обеспечения услуг безопасности и, следовательно, показано, как они могут обеспечиваться для сетей электросвязи эффективным образом.

Предполагается, что если какой-то уровень представляет услугу безопасности, то эта услуга оказывается уровню, находящемуся над рассматриваемым уровнем. Предоставление услуг уровнями согласно Рекомендации МСЭ-Т X.800 используется в качестве базы для ограничения возможных вариантов.

6.3.1 Аутентификация (равноправного объекта и источника данных)

Эту услугу могут обеспечить следующие уровни (согласно Рекомендации МСЭ-Т X.800):

– сетевой уровень (подтверждение идентификационной информации равноправных объектов транспортного уровня);

– транспортный уровень (подтверждение идентификационной информации равноправных объектов сеансового уровня);

– прикладной уровень (подтверждение идентификационной информации прикладных процессов);

– вне ВОС: в самом прикладном процессе.

6.3.2 Управление доступом

– *Управление доступом к ассоциации административного управления*

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

  Управление доступом к ассоциации может обеспечиваться на сетевом уровне. Кроме того, управление доступом к ассоциации может обеспечиваться на прикладном уровне или в самом прикладном процессе.

– *Управление доступом к извещению административного управления*

  Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, так как именно сам прикладной процесс может различать объекты (прикладного процесса), такие как диспетчеры и агенты.

– *Управление доступом к управляемому ресурсу*

  Эта услуга может использоваться на прикладном уровне или в самом прикладном процессе, так как именно сам прикладной процесс может различать объекты (прикладного процесса), такие как диспетчеры и агенты.

6.3.3 Аварийный сигнал безопасности, аудиторский журнал и восстановление

Эти услуги связаны с другими услугами и поэтому присутствуют на тех уровнях, на которых присутствуют эти другие услуги.

6.3.4 Целостность

– *Выборочная целостность поля*

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

– *Целостность соединения с восстановлением*

  Может обеспечиваться на транспортном уровне или в прикладном процессе.

– *Целостность соединения без восстановления*

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

6.3.5 Конфиденциальность

– *Выборочная конфиденциальность поля*

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

– *Конфиденциальность соединения и связи без соединения*

  Учитывая, что необходима "сквозная" конфиденциальность, которая исключает физический уровень и уровень звена данных, конфиденциальность может обеспечиваться на сетевом уровне, транспортном уровне, представительном уровне, прикладном уровне или в прикладном процессе.

– *Конфиденциальность потока трафика*

  Эта услуга может обеспечиваться на сетевом, транспортном или прикладном уровне, либо в прикладном процессе.

6.3.6 Защита от непризнания участия

– Защита от непризнания участия: доказательство передачи;

– защита от непризнания участия: доказательство доставки.

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

Все это кратко представлено в таблице 5. Таблица 5 не идентична таблице 2 из Рекомендации МСЭ-Т X.800, так как области применения этих двух Рекомендаций различаются.

Таблица 5/E.408 – Связь услуг безопасности с эталонной моделью ВОС

	Уровни						
Услуги	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Аутентификация пользователя	–	–	–	–	–	–	+
Аутентификация равноправного объекта	–	–	+	+	–	–	+
Аутентификация источника данных	–	–	+	+	–	–	+
Управление доступом к ассоциации административного управления	–	–	+	–	–	–	+
Управление доступом к извещению административного управления	–	–	–	–	–	–	+
Управление доступом к управляемому ресурсу	–	–	–	–	–	–	+
Аварийный сигнал безопасности, аудиторский журнал и восстановление	+	+	+	+	+	+	+
Выборочная целостность поля	–	–	–	–	–	–	+
Целостность соединения с восстановлением	–	–	–	+	–	–	+
Целостность соединения без восстановления	–	–	+	+	–	–	+
Выборочная конфиденциальность поля	–	–	–	–	–	–	+
Конфиденциальность соединения/связи без соединения	–	–	+	+	–	+	+
Конфиденциальность потока трафика	–	–	+	+	–	+	+
Защита от непризнания участия: доказательство передачи	–	–	–	–	–	+	+
Защита от непризнания участия: доказательство доставки	–	–	–	–	–	+	+

6.4 Административное управление обеспечением безопасности

Административное управление обеспечением безопасности охватывает все действия по введению, поддержанию и завершению действия аспектов безопасности системы.

Охватываются следующие области:

– административное управление услугами безопасности;

– ввод в действие механизмов безопасности;

– управление ключами (часть, связанная с административным управлением);

– установление идентификационной информации, ключей, информации управления доступом и т. д.;

– управление аудиторским журналом безопасности и аварийным сигналом безопасности;

– оповещение и обучение по вопросам безопасности;

– стратегия безопасности;

– политика и нормы безопасности;

– управление коллективной безопасностью.

Добавление I

Вопросы законодательства

I.1 Введение

В этом разделе описываются сферы законодательства, которые могут влиять на стандартизацию безопасности в сетях электросвязи, и делается попытка сформулировать некоторые следствия этого законодательства.

I.2 Применимые сферы законодательства

Определены следующие сферы законодательства, которые могут влиять на стандартизацию безопасности сетей электросвязи:

Секретность

– "секретность переписки": сохранение информации, которой обмениваются клиенты, недоступной для не имеющих разрешения третьих сторон;

– ограничение сбора, хранения и обработки данных личного характера: данные личного характера можно собирать, хранить и обрабатывать только в случаях, когда имеется взаимосвязь между такими данными и фактическим предоставлением услуг;

– раскрытие: обязанность сетевого оператора держать информацию о клиентах недоступной для не имеющих разрешения третьих сторон;

– "контроль и коррективы": право клиента контролировать информацию о себе, хранимую, если это оправданно, сетевым оператором, и вносить в нее коррективы.

Законодательство о секретности будет влиять в основном на требования к безопасности, относящиеся к управлению доступом, целостности и конфиденциальности.

Договорные отношения

– возможность использования информации, относящейся к электросвязи между объектами, в случае судебного разбирательства;

– признание контракта, доставленного электронным способом, в суде.

В основном влияние будет оказываться на требования к безопасности, касающиеся целостности и невозможности непризнания участия.

Международная безопасность и национальный общественный порядок

– требования к надлежащей защите информации и инфраструктуры: обеспечение доступности и целостности сети электросвязи;

– ограничения на использование криптографических методов: в некоторых странах действуют законы, ограничивающие использование шифрования;

– обязанность сетевых операторов сотрудничать и предоставлять информацию в случае законного перехвата для уголовного расследования.

Это законодательство может влиять на требования к безопасности. Влияние законодательства о законном перехвате на эти требования несколько неясно. Имеется, однако, взаимосвязь с секретностью, например следует предоставлять только информацию о личности, в отношении которой ведется расследование.

I.3 Источники законодательства

В предыдущем разделе законодательство классифицировалось по его предмету. Ниже указываются некоторые источники законодательства и их возможное влияние на безопасность сетей электросвязи.

– *Конституции*

  Охватывают тайну переписки, право на секретность, право на личную свободу и т. д. Не во всех конституциях конкретно упоминается электросвязь.

– *Международные договоры*

Двумя примерами являются Римский и Маастрихтский договоры. Для электросвязи здесь важны две сферы законодательства. Первая сфера относится к европейскому рынку (так называемый "первый столп") и имеет целью конкуренцию на рынке (электросвязи): для безопасности важными являются "обязательные требования" по безопасности и целостности сетей, а также по защите данных. Вторая сфера ("третий столп") относится к европейскому сотрудничеству в сфере юстиции: применительно к безопасности основными моментами в этой сфере являются требования к законному перехвату. Эти требования относятся к содержанию вызова, связанным с вызовом данным и местоположению объекта. Важными аспектами для безопасности сетей электросвязи могут быть следующие: *Специальные положения необходимы в отношении конфиденциальности, целостности и проверке процесса перехвата.*

– *Другие международные соглашения*

Многие из этих соглашений касаются прав человека: по отношению к электросвязи наиболее актуальными являются конфиденциальность и тайна переписки. Считается, что законы об авторском праве не сказываются на безопасности сетей электросвязи.

– *Национальные законы*

Применимые законы опять-таки относятся к конфиденциальности, тайне переписки и законному перехвату.

– *Правила, устанавливаемые Национальным регламентарным органом электросвязи (National Telecommunications Regulator, NTR)*

NTR – это национальный орган (назначенный национальным законодательством), которому даны полномочия издавать правила и регламентарные нормы в области электросвязи. Эти правила могут включать вопросы безопасности.

– *Кодексы практики*

Направления политики, согласованные компаниями и организациями электросвязи для урегулирования вопросов безопасности. В аспекте безопасности сетей электросвязи эти кодексы практики могут стать важной проблемой, когда сети электросвязи соединены между собой.

I.4 Возможные последствия для стандартизации в сфере безопасности сетей электросвязи

При стандартизации в сфере безопасности сетей электросвязи предвидятся следующие последствия применения законодательства, которые необходимо принимать во внимание.

– Законодательство может создавать требования, которые относятся к мощности и доступности услуг безопасности. В предыдущих разделах упоминалось об этих требованиях.

– Необходимость обеспечивать определенный уровень целостности сети электросвязи.

– Возможность поддерживать законный перехват и доступ к данным по управлению для департамента юстиции. Продолжительность времени хранения данных и процессы обеспечения уничтожения данных, когда это требуется.

– Законодательство может привести к запрету использования шифрования в некоторых странах.

– Законодательство в различных странах неодинаково. Это означает, что в разных странах могут возникать разные требования.

Добавление II

Функциональные классы и профили безопасности

II.1 Классификация мер безопасности

Меры безопасности можно классифицировать по "функциональным классам" (Functional Classes, FC). Приводимое здесь определение не охватывает эффективности меры безопасности.

Функциональный класс – это последовательный комплекс мер безопасности для удовлетворения требований к безопасности на различных уровнях (функциональных уровнях).

II.1.1 Использование FC в междоменном случае

На безопасность сети электросвязи не должна негативно влиять междоменная деятельность. Правила взаимодействия доменов должны быть определены в междоменной политике безопасности. Эти правила будут определять, какие меры безопасности следует применять в каком случае. Для упрощения достижения соглашения между взаимодействующими доменами эти меры безопасности могут обозначаться как конкретный функциональный класс.

II.1.2 Использование FC во внутридоменном случае

Во внутридоменном случае функциональные классы могут упрощать определение безопасности. FC могут также использоваться в целях гарантирования безопасности. Чтобы достичь этого, функциональные классы следует увязывать с уровнем гарантии, объявляемым изготовителем средств управления. Этот вопрос тесно связан с формальными критериями оценки.

Возможны ситуации, когда одному оператору для междоменного взаимодействия может потребоваться применение конкретного FC к внутридоменному случаю другого оператора. Причиной этого может быть то, что не все угрозы можно эффективно преодолеть на интерфейсе между двумя доменами. Одним из способов решения этой проблемы могло бы быть обеспечение минимального уровня внутренней безопасности во взаимодействующих сетях электросвязи. Стандарт на безопасность сети электросвязи должен не предписывать, какие FC требуются, а давать возможность затребования определенных FC путем определения соответствующих пунктов для выбора.

II.2 Функциональные классы

Функциональные классы используются для определения небольшой группы услуг безопасности, задачей которых является обеспечение определенного уровня безопасности. В данном разделе рассматривается комплекс функциональных классов, который служит примером того, как можно определить функциональные классы. Предложены функциональные классы *для X-интерфейса* на трех разных уровнях безопасности:

1) минимальный функциональный класс: (FC 1);

2) базовый функциональный класс: (FC 2);

3) усовершенствованный функциональный класс: (FC 3).

По практическим соображениям число FC не должно быть слишком велико. С другой стороны, должна существовать возможность удовлетворять требования многих разных организаций. Функциональные классы можно изменять следующими способами.

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

– Предполагается, что конфиденциальность будет факультативным свойством для всех классов по двумя причинам:

  • она является менее строгим требованием;

  • обязательное включение ее в какой-либо функциональный класс может привести к юридическим последствиям в отношении применимости этого класса.

В таблице II.1 дается обзор функциональных классов.

Таблица II.1/E.408 – Функциональные классы услуг безопасности

FC 1	FC 2	FC 3
Основное внимание уделяется целостности хранимых управляемых ресурсов	Основное внимание уделяется целостности хранимых управляемых ресурсов и целостности передаваемых данных	Как FC 2 плюс отчетность по операциям управления
• Аутентификация (равноправного объекта или пользователя) • Управление доступом к ассоциации административного управления • Управление доступом к управляемому ресурсу • Аварийный сигнал безопасности, проверка и восстановление	• Аутентификация (равноправного объекта и пользователя) • Управление доступом к ассоциации административного управления • Управление доступом к управляемому ресурсу • Аутентификация источника данных • Выборочная целостность поля • Целостность соединения • Аварийный сигнал безопасности, проверка и восстановление	• Аутентификация (равноправного объекта и пользователя) • Управление доступом к ассоциации административного управления • Управление доступом к управляемому ресурсу • Аутентификация источника данных • Выборочная целостность поля • Целостность соединения • Защита от непризнания участия источника • Защита от непризнания участия назначения • Аварийный сигнал безопасности, проверка и восстановление
Факультативно: • Целостность соединения • Конфиденциальность соединения	Факультативно: • Конфиденциальность соединения • Выборочная конфиденциальность поля	Факультативно: • Конфиденциальность соединения • Выборочная конфиденциальность поля

Кроме того, следует различать FC, применимые для междоменного случая, и FC для внутридоменного случая. Требования для этих двух случаев будут различаться, поэтому меры безопасности могут также быть различны.

Ниже приводится обзор различных случаев, дающий возможность понять, какие FC нужны и какие подходят.

Предполагаемая ситуация

В каждом домене имеется орган, который отвечает за решение о том, какие меры безопасности следует применять в домене.

Различаются три случая:

1) FC, определенные органом управления домена и применимые в собственном домене (внутридоменные);

2) FC, определенные органом управления домена и применимые к взаимодействию доменов (междоменные). Эти FC будут результатом соглашения между органами управления взаимодействующих доменов;

3) FC, определенные органом управления одного домена в виде требований к внутренней безопасности другого домена.

В каждом случае можно определить число FC для разных уровней безопасности.

Число уровней безопасности подлежит дальнейшему изучению.

Комплекс мер безопасности, формирующих тот или иной FC, подлежит дальнейшему изучению.

Классы FC в различных случаях могут быть равны, что уменьшает общее число FC.

Можно предусмотреть также координацию между разными случаями, например, если междоменная безопасность находится на высоком уровне, то требования к внутренней безопасности в другом домене могут быть низкими, и наоборот. Еще один возможный подход может состоять в том, что какой-либо FC представляет минимальный комплекс мер безопасности, который может по мере необходимости расширяться за счет дополнительных мер.

II.3 Профили безопасности

Функциональные классы не требуют использования стандартизованных механизмов безопасности; могут применяться любые отвечающие требованиям механизмы.

Чтобы обеспечить возможность взаимодействия между мерами безопасности в различных доменах, эти меры должны соответствовать стандартам. Предписание относительно использования конкретных стандартов, которые совместно обеспечивают тот или иной функциональный класс, называется профилем безопасности.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	**Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы**
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных 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	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
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 и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола (IP) и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2005 г.