Утвержден и введен в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 1 декабря 2011 г. N 683-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ СЕТЕЙ

ЧАСТЬ 1

ОБЗОР И КОНЦЕПЦИИ

**Information technology. Security techniques.
Network security. Part 1. Overview and concepts**

**ISO/IEC 27033-1:2009
Information technology - Security techniques -
Network security - Part 1: Overview and concepts
(IDT)**

ГОСТ Р ИСО/МЭК 27033-1-2011

ОКС 35.040

Дата введения
1 января 2012 года

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения".

Сведения о стандарте

1. Подготовлен Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл"), Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России") и "Газпромбанк" [Открытое акционерное общество (ГПБ (ОАО)] на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4.

2. Внесен Техническим комитетом по стандартизации ТК 362 "Защита информации".

3. Утвержден и введен в действие Приказом Федерального агентства по техническому

регулированию и метрологии от 1 декабря 2011 г. N 683-ст.

4. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27033-1:2009 "Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции" (ISO/IEC 27033-1:2009 "Information technology - Security techniques - Network security - Part 1: Overview and concepts").

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации и межгосударственные стандарты, сведения о которых приведены в дополнительном Приложении ДА.

5. Взамен ГОСТ Р ИСО/МЭК 18028-1-2008.

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования - на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет.

Введение

В современном мире информационные системы большинства коммерческих и государственных организаций связаны сетями (см. рисунок 1), при этом сетевые соединения могут относиться к следующим (одному или нескольким) видам:

- в пределах организации;

- между различными организациями;

- между организацией и неограниченным кругом лиц.

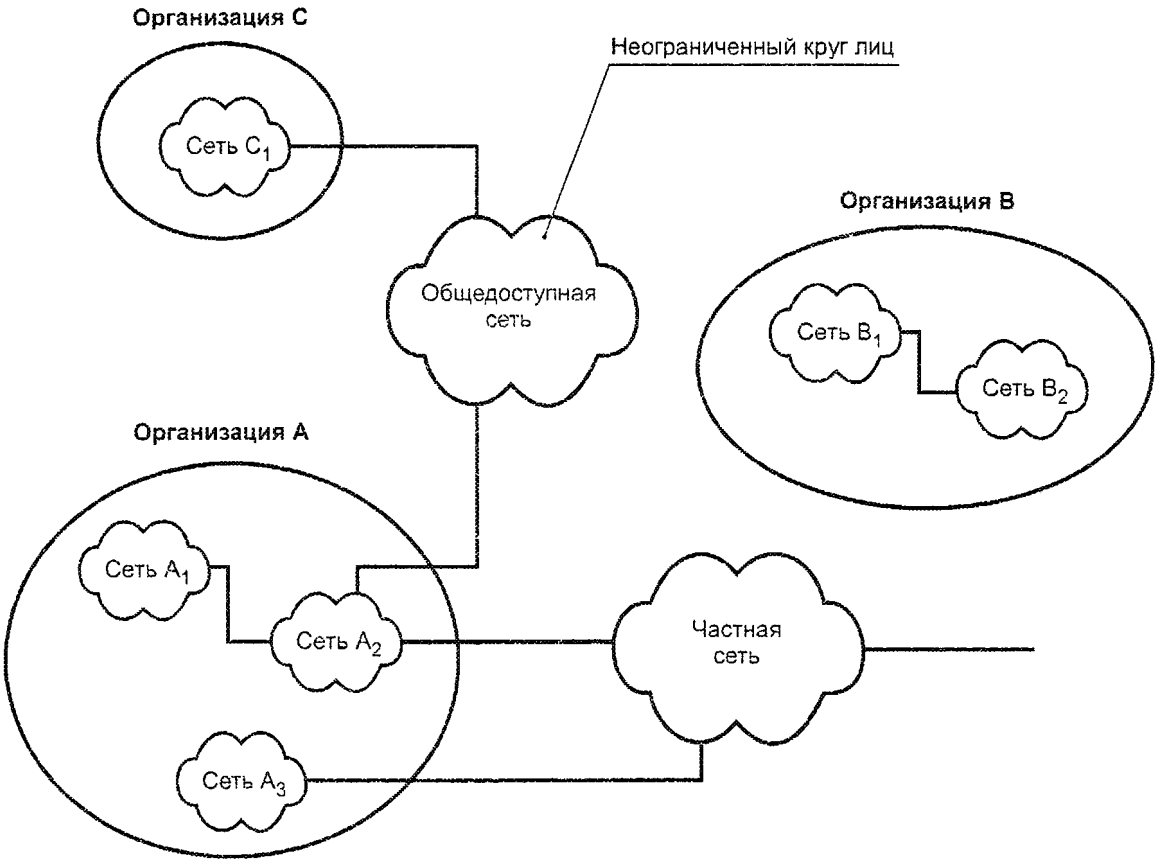


Рисунок 1. Разнообразные виды сетевых соединений

Кроме того, при бурном развитии общедоступной сетевой технологии (в особенности Интернета), предлагающей значительные возможности для ведения бизнеса, организации все больше занимаются электронной торговлей в глобальном масштабе и предоставляют общедоступные услуги в режиме реального времени (далее - в режиме on-line). Эти возможности обеспечивают более дешевый способ передачи данных с использованием Интернета в качестве глобального средства связи благодаря услугам, предоставляемым провайдерами Интернет-услуг. Это может означать использование относительно дешевых локальных точек подключения на каждом конце линии связи к полномасштабным системам электронной торговли и предоставление услуг, использующих сервисы и приложения, основанные на Интернет-технологии. Кроме того, новые технологии (включающие объединение данных, речи и видео) расширяют возможности для удаленной работы (также известной как "дистанционная работа"), позволяющей сотрудникам работать значительную часть времени дома. Они могут поддерживать контакт путем использования средств дистанционного доступа к сетям организации и сообщества, а также к информации и услугам, связанным с поддержкой основной деятельности организации.

Однако в то время как среда, образованная новыми технологиями, способствует получению значительных преимуществ для деятельности организации, также появляются новые риски безопасности, требующие управления. Утрата конфиденциальности, целостности и доступности информации и услуг может оказывать существенное неблагоприятное влияние на деятельность организации, поскольку организации в значительной степени зависят от использования информации и связанных с нею сетей для ведения своей деятельности. Следовательно, основным требованием является обеспечение надлежащей защиты сетей и связанных с ними информационных систем и информации. Другими словами реализация и

поддержка адекватной сетевой безопасности абсолютно необходима для успеха операций основной деятельности любой организации.

В этом контексте для индустрии телекоммуникаций и информационных технологий ведется поиск рентабельных всесторонних программных и технических средств и услуг по обеспечению безопасности, направленных на защиту сетей от злонамеренных атак и непреднамеренных неверных действий и обеспечение конфиденциальности, целостности и доступности информации и услуг в соответствии с потребностями организации. Обеспечение безопасности сети также важно в случае необходимости обеспечения точности информации об учете или использовании услуг. Возможности обеспечения безопасности в продуктах <1> являются необходимыми для общей сетевой безопасности (включая приложения и сервисы). Однако когда все больше продуктов комбинируется для обеспечения общих решений, их функциональная совместимость - или ее отсутствие - будет определять успех решения. Безопасность должна быть не только одним из поводов для беспокойства в отношении каждого продукта или услуги, но и разработана так, чтобы способствовать интегрированию возможностей продукта или услуги по обеспечению безопасности в общее решение по обеспечению безопасности организации.

<1> В настоящем стандарте под "продуктом" следует понимать "изделия/средства (программные, технические или программно-технические)".

Назначение ИСО/МЭК 27033 состоит в том, чтобы предоставить подробные рекомендации по аспектам безопасности менеджмента, функционирования и использования сетей информационных систем и их соединений. Лица, отвечающие за обеспечение в организации информационной безопасности в целом и сетевой безопасности в частности, должны быть способны адаптировать материал настоящего стандарта для соответствия своим конкретным требованиям. Основными целями частей стандарта ИСО/МЭК 27033 являются:

- для ИСО/МЭК 27033-1 "Обзор и концепция" - определение и описание концепций, связанных с сетевой безопасностью, и предоставление рекомендаций по менеджменту сетевой безопасности. Стандарт содержит общий обзор сетевой безопасности и связанных с ней определений, рекомендации по идентификации и анализу рисков сетевой безопасности, и, кроме того, определение требований сетевой безопасности. Он также знакомит с тем, как добиваться высокого качества специализированных архитектур безопасности, а также с аспектами риска, проектирования, аспектами мер и средств контроля и управления, связанными с типичными сетевыми сценариями и областями сетевых "технологий" (которые подробно рассматриваются в следующих частях стандарта ИСО/МЭК 27033);

- для ИСО/МЭК 27033-2 "Рекомендации по проектированию и реализации сетевой безопасности" - определение того, каким образом организации должны добиваться требуемого качества специализированных архитектур сетевой безопасности, проектирования и реализации, которые обеспечат уверенность в сетевой безопасности, соответствующей их среде деятельности, используя при необходимости последовательный подход к планированию, проектированию и реализации сетевой безопасности с применением моделей/систем (в данном контексте термины "модель/система" используются для формулирования в общих чертах представления или описания, показывающего структуру и высокоуровневую деятельность некоторого вида специализированной архитектуры/проекта безопасности). Данный стандарт предназначен для всего персонала, вовлеченного в планирование, проектирование и реализацию аспектов архитектуры сетевой безопасности (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за сетевую безопасность);

- для ИСО/МЭК 27033-3 "Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления, для типовых сетевых сценариев" - определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, связанных с типовыми сетевыми сценариями. Данный стандарт предназначен для персонала, вовлеченного в планирование, проектирование и реализацию аспектов архитектуры сетевой безопасности (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за сетевую безопасность).

Предполагается, что следующие части ИСО/МЭК 27033 будут рассматривать:

ИСО/МЭК 27033-4 "Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления, для обеспечения безопасности передачи информации между сетями с использованием шлюзов безопасности" - определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления для обеспечения безопасности информационных потоков между сетями с использованием шлюзов безопасности. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию шлюзов безопасности (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за сетевую безопасность);

ИСО/МЭК 27033-5 "Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления для обеспечения безопасности виртуальных частных сетей" - определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности соединений, установленных с использованием VPN. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности виртуальных частных сетей (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за сетевую безопасность);

ИСО/МЭК 27033-6 "IP-конвергенция" - определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности сетей с IP-конвергенцией, т.е. с конвергенцией данных, речи и видео. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности сетей с IP-конвергенцией (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за сетевую безопасность);

ИСО/МЭК 27033-7 "Беспроводная связь" - определение конкретных рисков, методов проектирования и вопросов, касающихся мер и средств контроля и управления, для обеспечения безопасности беспроводных сетей и радиосетей. Данный стандарт будет представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности беспроводных сетей и радиосетей (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за сетевую безопасность).

Следует подчеркнуть, что ИСО/МЭК 27033 предоставляет дополнительные детализированные рекомендации по реализации мер и средств контроля и управления сетевой безопасностью, определенных в базовом стандарте ИСО/МЭК 27002.

Если в будущем появятся другие части стандарта, они могут представлять интерес для всего персонала, вовлеченного в детальное планирование, проектирование и реализацию сетевых аспектов, охватываемых этими частями (например, для проектировщиков и разработчиков сетевой архитектуры, сетевых менеджеров и сотрудников, ответственных за

сетевую безопасность).

Следует отметить, что настоящий стандарт не является справочным или нормативным документом для регулирующих и законодательных требований безопасности. Хотя в нем подчеркивается важность этих оказывающих влияние факторов, они не могут быть сформулированы конкретно, так как зависят от страны, вида основной деятельности и т.д.

Если не указано иное, требования настоящего стандарта применимы к действующим в настоящее время и (или) планируемым сетям, но в тексте настоящего стандарта будут применены только термины "сети" или "сеть".

1. Область применения

Настоящий стандарт содержит обзор сетевой безопасности и связанных с ней определений. Стандарт определяет и описывает концепции, связанные с сетевой безопасностью, и предоставляет рекомендации по менеджменту сетевой безопасности. (В дополнение к безопасности информации, передаваемой по линиям связи, сетевая безопасность затрагивает безопасность устройств, безопасность деятельности по менеджменту данных устройств, приложений/услуг, а также безопасность конечных пользователей).

Настоящий стандарт предназначен для лиц, владеющих, управляющих или использующих сети. Помимо руководителей и администраторов, имеющих конкретные обязанности по обеспечению информационной и (или) сетевой безопасности и функционированию сети или отвечающих за разработку общей программы обеспечения безопасности и политики безопасности организации, стандарт предназначен и для представителей высшего руководства и других руководителей или пользователей, не имеющих технической подготовки. Настоящий стандарт также предназначен для всех вовлеченных в планирование, проектирование и реализацию аспектов архитектуры сетевой безопасности.

Настоящий стандарт также:

- представляет рекомендации по идентификации и анализу рисков сетевой безопасности и дает определение требований сетевой безопасности, основанных на этом анализе;

- представляет обзор мер и средств контроля и управления, поддерживающих специализированные архитектуры сетевой безопасности, и связанные с ними технические меры и средства контроля и управления, а также технические и нетехнические меры и средства контроля и управления, применяемые не только к сетям;

- знакомит с тем, как добиться высокого качества специализированных архитектур сетевой безопасности, а также с аспектами риска, проектирования, мер и средств контроля и управления, связанными с типичными сетевыми сценариями и областями сетевых "технологий" (которые детально рассматриваются в следующих частях ИСО/МЭК 27033);

- содержит краткое рассмотрение вопросов, связанных с реализацией и функционированием мер и средств контроля и управления сетевой безопасностью, постоянным мониторингом и проверкой их реализации.

В целом, в настоящем стандарте представлен обзор существующих частей ИСО/МЭК 27033, и он является "путеводителем" по остальным частям стандарта.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные

стандарты. Для датированных стандартов применяют только указанное издание. Для недатированных стандартов применяют последнее издание упомянутого стандарта (включая опубликованные изменения).

ИСО/МЭК 7498 (все части). Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель (ISO/IEC 7498 (all parts), Information technology - Open Systems Interconnection - Basic Reference Model)

ИСО/МЭК 27000:2009. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология (ISO/IEC 27000:2009. Information technology - Security techniques - Information security management systems - Overview and vocabulary)

ИСО/МЭК 27001:2005. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements)

ИСО/МЭК 27002:2005. Информационная технология. Методы и средства обеспечения безопасности. Свод правил для менеджмента информационной безопасности (ISO/IEC 27002:2005. Information technology - Security techniques - Code of practice for information security management)

ИСО/МЭК 27005:2008. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности (ISO/IEC 27005:2008. Information technology - Security techniques - Information security risk management).

3. Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 7498, ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27005, а также следующие термины с соответствующими определениями.

Примечание. Приведенные ниже термины и определения будут также применены в следующих частях ИСО/МЭК 27033.

3.1. Предупреждение об опасности (alert): "немедленное" оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или человеческой ошибки.

3.2. Архитектура (architecture): базовая организация системы, воплощенная в ее компонентах, их отношениях между собой и с окружением, а также принципы, определяющие проектирование и развитие системы.

[ИСО/МЭК 15288:2008, определение 4.5]

3.3. Нарушитель (attacker): любое лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем и сетей, или снижения доступности ресурсов информационной системы и сетевых ресурсов для законных пользователей.

3.4. Ведение контрольных журналов (audit logging): фиксирование данных о событиях, связанных с информационной безопасностью, в целях проверки, анализа и постоянного мониторинга.

3.5. Инструментальные средства аудита (audit tools): автоматизированные инструментальные средства, помогающие анализировать содержание журналов событий.

3.6. Центр сертификации [открытых ключей] (certification authority; CA): орган, которому доверяет один или более пользователей в вопросе создания и распределения сертификатов открытого ключа.

Примечания. 1. Факультативно орган сертификации может создавать ключи пользователей.

2. Роль органа сертификации в этом процессе заключается в обеспечении уверенности, что лицо, которому выдан уникальный сертификат, на самом деле является тем, кем оно себя заявляет. Обычно это означает, что орган сертификации имеет соглашение с учреждением, предоставляющим ему информацию для подтверждения предъявленной идентификационной информации в отношении лица. Органы сертификации являются важнейшим компонентом в информационной безопасности и электронной коммерции, потому что они гарантируют, что две стороны, обменивающиеся информацией, действительно являются теми, кем они себя заявляют.

3.7. Корпоративная политика информационной безопасности (corporate information security policy): документ, отражающий позицию руководства по обеспечению информационной безопасности в соответствии с требованиями основной деятельности организации и правовыми и регулирующими нормами.

Примечание. Документ, описывающий высокоуровневые требования информационной безопасности, которые должны соблюдаться в организации.

3.8. Демилитаризованная зона (demilitarized zone; DMZ); ДМЗ: пограничный сегмент сети (также известный как защищенная подсеть), выполняющий функции "нейтральной зоны" между сетями.

3.9. Отказ в обслуживании (denial of service; DoS): прекращение санкционированного доступа к ресурсам системы или задержка операций и функций системы, приводящее в итоге к потере доступности для авторизованных пользователей.

3.10. Экстранет (extranet): расширение сети Интранет организации, особенно через инфраструктуру общедоступной сети, делающее возможным совместное использование ресурсов организацией, другими организациями и лицами, с которыми она имеет дело, с предоставлением ограниченного доступа к своей сети Интранет.

Примечание. Например, клиентам организации может предоставляться доступ к некоторым частям ее сети Интранет посредством создания Экстранет, но клиентов нельзя считать "доверенными" с точки зрения безопасности.

3.11. Фильтрация (filtering): процесс приема или отклонения потоков данных в сети в соответствии с определенными критериями.

3.12. Межсетевой экран (firewall): вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности.

3.13. Концентратор (hub): сетевое устройство, которое функционирует на первом уровне эталонной модели взаимодействия открытых систем.

Примечание. Сетевые концентраторы не являются интеллектуальными устройствами, они обеспечивают только точки физического соединения для сетевых систем или ресурсов.

3.14. Интернет (the Internet): глобальная система взаимосвязанных сетей общедоступного пользования.

3.15. Интерсеть (internet): совокупность взаимосвязанных сетей, называемая "объединенной сетью" или просто "интерсетью".

3.16. Интранет (intranet): частная компьютерная сеть, использующая Интернет-протоколы и возможность сетевого соединения для безопасного коллективного использования части информации или операций организации ее сотрудниками.

3.17. Вторжение (intrusion): несанкционированный доступ к сети или подсоединенной к сети системе, т.е. преднамеренный или случайный несанкционированный доступ к информационной системе, включая злонамеренную деятельность против информационной системы или несанкционированное использование ресурсов в информационной системе.

3.18. Обнаружение вторжений (intrusion detection): формальный процесс обнаружения вторжений, обычно характеризующийся сбором сведений об аномальном характере использования, а также о том, какая уязвимость была использована и каким образом, включая то, когда и как это произошло.

Примечание. См. ИСО/МЭК 18043.

3.19. Система обнаружения вторжений (intrusion detection system); IDS: специализированная система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования на вторжение в информационные системы и сети.

Примечание. См. ИСО/МЭК 18043.

3.20. Предотвращение вторжений (intrusion prevention): формальный процесс активного реагирования с целью предотвращения вторжений.

3.21. Система предотвращения вторжений (intrusion prevention system); IPS: вид систем обнаружения вторжений, специально предназначенных для обеспечения активной возможности реагирования.

Примечание. См. ИСО/МЭК 18043.

3.22. Вредоносное программное средство (malware): вредоносное программное средство, специально разработанное для повреждения или разрушения системы посредством нарушения ее конфиденциальности, целостности и (или) доступности.

Примечание. Примерами вредоносного программного средства являются вирусы и "троянские кони".

3.23. Многопротокольная коммутация на основе меток (multi protocol label switching - MPLS): метод, разработанный для использования в межсетевой маршрутизации, в соответствии с которым индивидуальным трактам передачи данных или потокам данных присваиваются метки, и который используется для коммутации соединений на более низком уровне и в дополнение к обычным механизмам протоколов маршрутизации.

Примечание. Коммутация на основе меток может использоваться как один из методов создания туннелей.

3.24. Сетевое администрирование (network administration): повседневная эксплуатация и управление сетевыми процессами и средствами, используемыми сетью.

3.25. Сетевой анализатор (network analyzer): устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика.

Примечание. До проведения анализа информационного потока информация должна быть собрана определенным образом, например, путем использования сетевого анализатора пакетов.

3.26. Сетевой элемент (network element): информационная система, подсоединенная к сети.

3.27. Сетевой менеджмент (network management): процесс планирования, разработки, реализации, эксплуатации, мониторинга и поддержки сети.

3.28. Сетевой мониторинг (network monitoring): процесс постоянного наблюдения и проверки зафиксированных данных о сетевой деятельности и операциях, включая контрольные журналы и предупреждения об опасности, и связанный с этим анализ.

3.29. Политика сетевой безопасности (network security policy): совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как должна обеспечиваться защита ее сетевой инфраструктуры и сервисов.

3.30. Сетевой анализатор пакетов (network sniffer): устройство или программное средство, используемое для сбора информации, проходящей через сети.

3.31. Порт (port): конечная точка соединения.

Примечание. В контексте Интернет-протокола порт представляет собой конечную точку логического канала TCP или UDP соединения. Протоколы приложений на основе TCP или UDP обычно имеют назначенные по умолчанию номера портов, например, порт 80 для HTTP протокола.

3.32. Удаленный доступ (remote access): процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ.

3.33. Удаленный пользователь (remote user): пользователь, находящийся на объекте (площадке, филиале), отличном от того, на котором размещаются используемые сетевые ресурсы.

3.34. Маршрутизатор (router): сетевое устройство, используемое для установления и управления потоками данных между различными сетями путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации.

Примечания. 1. Сети сами могут быть основаны на разных протоколах.

2. Информация о маршрутизации хранится в таблице маршрутизации.

3.35. Домен безопасности (security domain): совокупность активов и ресурсов, подчиняющихся единой политике безопасности.

3.36. Шлюз безопасности (security gateway): точка соединения между сетями, между сегментами сетей или между программными приложениями в различных доменах безопасности, предназначенная для защиты сети в соответствии с существующей политикой безопасности.

3.37. Спам (spam): незапрашиваемые сообщения электронной почты, содержание которых может быть вредоносным и (или) мошенническим.

3.38. Спуфинг (spoofing): маскировка под легального пользователя или сетевой ресурс.

3.39. Коммутатор (switch): устройство, обеспечивающее соединение сетевых устройств посредством внутренних механизмов коммутации, с технологией коммутации, обычно реализованной на втором или третьем уровне эталонной модели взаимодействия открытых систем.

Примечание. Коммутаторы отличаются от других соединительных устройств локальной сети (например, концентраторов), так как используемая в коммутаторах технология устанавливает соединения на основе "точка - точка".

3.40. Туннель (tunnel): канал передачи данных между сетевыми устройствами, который устанавливают через существующую сетевую инфраструктуру.

Примечание. Туннели могут устанавливать путем использования таких технических приемов, как протокольная инкапсуляция, коммутация на основе меток или виртуальный канал.

3.41. Виртуальная локальная вычислительная сеть (virtual local area network): независимая сеть, созданная с логической точки зрения внутри физической сети.

4. Сокращения

Примечание. Перечисленные ниже сокращения применяют во всех частях ИСО/МЭК 27033.

3G - система цифровой мобильной связи третьего поколения;

AAA - аутентификация, авторизация и учет;

ACL - список контроля доступом;

ADSL - асимметричная цифровая абонентская линия;

AES - улучшенный стандарт шифрования;

ATM - асинхронный режим передачи;

BPL - широкополосная передача через линии электропередачи;

CA - центр сертификации [открытых ключей];

CDMA - многостанционный доступ с кодовым разделением каналов;

CDPD - сотовая цифровая передача пакетов данных;

CLID - идентификатор линии вызова;

CLNP - протокол сетевого обслуживания без установления соединения;

CoS - класс обслуживания (услуг);

CRM - управление взаимосвязями с клиентами;

DEL - прямая линия обмена информацией;

DES - стандарт шифрования данных;

DNS - служба доменных имен;

DoS - отказ в обслуживании;

DPNSS - цифровая сигнальная система частных сетей;

DSL - цифровая абонентская линия;

EDGE - улучшенные скорости передачи данных для развития GSM-стандарта;

EDI - электронный обмен данными;

EGPRS - улучшенный общий сервис пакетной радиопередачи;

EIS - информационная система предприятия;

FiOS - сервис с применением волоконной оптики;

FTP - протокол передачи файлов;

FTTH - сеть с доведенным до пользователя оптическим кабелем;

GPRS - общий сервис пакетной радиопередачи;

GSM - глобальная система мобильной связи;

HIDS - система обнаружения вторжений на базе хостов/серверов;

HTTP - протокол передачи гипертекста;

IDS - система обнаружения вторжений;

IG - Руководство по реализации;

IP - Интернет-протокол;

IPS - система предупреждения вторжений;

ISP - провайдер Интернет-услуг;

MPLS - многопротокольная коммутация на основе меток;

MRP - планирование производственных ресурсов;

NAT - трансляция сетевых адресов;

NIDS - система обнаружения сетевых вторжений;

NTP - синхронизирующий сетевой протокол;

OOB - внеполо́сный ;

PABX - учрежденческая АТС с исходящей и входящей связью;

PIN - личный идентификационный номер;

PKI - инфраструктура открытых ключей;

PSTN - телефонная коммутируемая сеть общего пользования;

QoS - качество обслуживания;

RAID - матрица независимых дисковых накопителей с избыточностью;

RAS - сервис удаленного доступа;

RTP - протокол реального времени;

SDSL - симметричная цифровая абонентская линия;

SecOPs - операционные процедуры безопасности;

SIM - модуль идентификации абонента;

SNMP - простой протокол сетевого управления;

SPIT - спам через IP-телефонию;

SSH - безопасная оболочка;

TCP - протокол управления передачей;

TDMA - многостанционный доступ с временным разделением каналов;

TETRA - наземное транкинговое радио;

TKIP - протокол целостности временного ключа;

UDP - протокол передачи дейтаграмм пользователя;

UMTS - универсальная система мобильной связи;

USB - универсальная последовательная шина;

VLAN - виртуальная локальная вычислительная сеть;

VoIP - передача речи по IP;

VPN - виртуальная частная сеть;

WAP - протокол приложений для беспроводной связи;

WEP - безопасность, эквивалентная проводной сети;

WLAN - беспроводная локальная вычислительная сеть;

WORM - с однократной записью и многократным считыванием;

WPA - защищенный доступ в беспроводных сетях;

ГВС (WAN) - глобальная вычислительная сеть;

ДМЗ (DMZ) - демилитаризованная зона;

ИБП (UPS) - источник бесперебойного питания;

ИТ (IT) - информационная технология;

КПК (PDA) - "карманный" персональный компьютер;

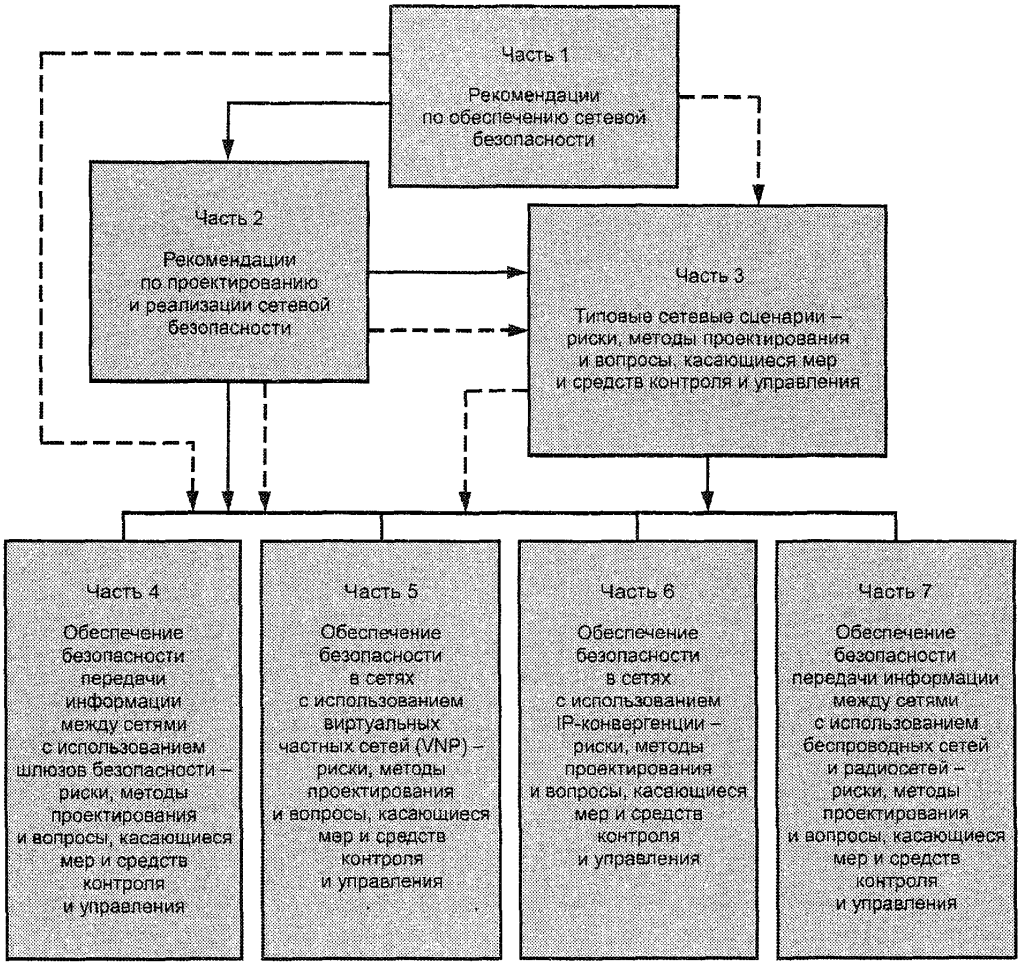
ЛВС (LAN) - локальная вычислительная сеть;

ОВЧ (VHF) - очень высокая частота;

ПК (PC) - персональный компьютер.

5. Структура

Структура серии стандартов ИСО/МЭК 27033 представлена в виде схемы или "путеводителя" на рисунке 2.



Примечание. Следует отметить, что в будущем возможно появление и других частей ИСО/МЭК 27033. Примеры возможных тем, охватываемых будущими частями ИСО/МЭК 27033, включают в себя локальные, глобальные и широкополосные сети; размещение информации на сервере веб-узлов; электронную почту в Интернете и маршрутизированный доступ для сторонних организаций. Основными пунктами всех этих частей должны быть риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления.

Рисунок 2. "Путеводитель" по ИСО/МЭК 27033

Сплошными линиями на рисунке 2 отмечена естественная иерархия частей ИСО/МЭК 27033. Пунктирными линиями отмечено, что, следуя процессам:

a) описанным в части 1, - можно обращаться за информацией по вопросу, касающемуся рисков безопасности, к частям 3 - 7 ИСО/МЭК 27033;

b) описанным в части 2, - можно обращаться за информацией по вопросам, касающимся методов проектирования и мер и средств контроля и управления, к частям 3 - 7 ИСО/МЭК 27033.

Кроме того, в части 3 ИСО/МЭК 27033 есть ссылки на конкретные аспекты, содержащиеся в частях 4 - 7 ИСО/МЭК 27033, с тем, чтобы избежать дублирования (т.е. при использовании части 3 возможно обращение к частям 4 - 7).

Таким образом, любой организации, начинающей с "нуля" или проводящей серьезную

проверку существующей сети (сетей), следует в первую очередь использовать настоящий стандарт, а затем ИСО/МЭК 27033-2 и, по мере необходимости, обращаться к информации о рисках безопасности, методах проектирования и вопросах, касающихся мер и средств контроля и управления, содержащихся в частях 3 - 7 ИСО/МЭК 27033.

Например, организация рассматривает реализацию новой сетевой среды, включающей в себя применение IP-конвергенции, шлюзов безопасности, частичное применение беспроводной связи, а также размещение информации на сервере веб-узлов и использование Интернета (например, для электронной почты и доступа в режиме on-line).

Используя описанные в настоящем стандарте процессы определения рисков безопасности для новой сетевой среды, организация будет учитывать относящуюся к риску информацию из других соответствующих частей ИСО/МЭК 27033, т.е. тех частей, которые определяют конкретные риски безопасности (а также методы проектирования и вопросы, касающиеся мер и средств контроля и управления), относящиеся к IP-конвергенции, шлюзам безопасности, частичному применению беспроводной связи, а также размещению информации на сервере веб-узлов и использованию Интернета (например, для электронной почты и доступа в режиме on-line).

При использовании ИСО/МЭК 27033-2 для определения требуемой специализированной архитектуры сетевой безопасности организации следует учитывать информацию о методах проектирования и вопросах, касающихся мер и средств контроля и управления из других соответствующих частей ИСО/МЭК 27033, т.е. тех частей, которые определяют конкретные методы проектирования и вопросы, касающиеся мер и средств контроля и управления (а также риски безопасности), относящиеся к IP-конвергенции, шлюзам безопасности, частичному применению беспроводной связи, а также размещению информации на сервере веб-узлов и использованию Интернета (например, для электронной почты и доступа в режиме on-line).

Структура настоящего стандарта включает в себя:

- обзор подхода к обеспечению сетевой безопасности (см. раздел 6);

- краткое изложение процесса идентификации рисков, связанных с сетями, и подготовки к идентификации мер и средств контроля и управления безопасностью, т.е. установлению требований сетевой безопасности (см. раздел 7);

- обзор мер и средств контроля и управления, поддерживающих специализированные архитектуры сетевой безопасности и связанные с ними технические меры и средства контроля и управления, т.е. обзор других мер и средств контроля и управления (технических и нетехнических), которые применимы не только к сетям (см. раздел 8). Представляются соответствующие ссылки на ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005;

- ознакомление с возможностями специализированных архитектур безопасности, которые будут обеспечивать сетевую безопасность, соответствующую среде основной деятельности организаций, применяя последовательный подход к планированию и проектированию сетевой безопасности с использованием при необходимости моделей/систем (т.е. введение к ИСО/МЭК 27033-2) (см. раздел 9);

- знакомство с конкретными рисками, методами проектирования и вопросами, касающимися мер и средств контроля и управления, связанными с типовыми сетевыми сценариями (т.е. введения к содержанию ИСО/МЭК 27033-3) (см. раздел 10);

- знакомство с конкретными рисками, методами проектирования и вопросами, касающимися мер и средств контроля и управления для сетевой "технологии" (т.е. введения к

частям 4 - 7 ИСО/МЭК 27033 и к другим частям ИСО/МЭК 27033, появление которых возможно в будущем) (см. раздел 11 и Приложение А);

- краткое изложение вопросов, связанных с разработкой, реализацией и тестированием комплекса программных и технических средств и услуг по обеспечению сетевой безопасности (см. раздел 12), эксплуатацией комплекса программных и технических средств и услуг по обеспечению сетевой безопасности (см. раздел 13) и постоянным мониторингом и проверкой реализации сетевой безопасности (см. раздел 14);

- таблицу, содержащую перекрестные ссылки между разделами ИСО/МЭК 27001, ИСО/МЭК 27002 и разделами настоящего стандарта, где рассматриваются меры и средства контроля и управления, связанные с сетевой безопасностью (см. Приложение В).

6. Обзор

6.1. Вводная информация

Пример сетевой среды, которую в настоящее время можно видеть во многих организациях, представлен на рисунке 3 (рисунок 3 приведен в настоящем разделе в качестве примера).

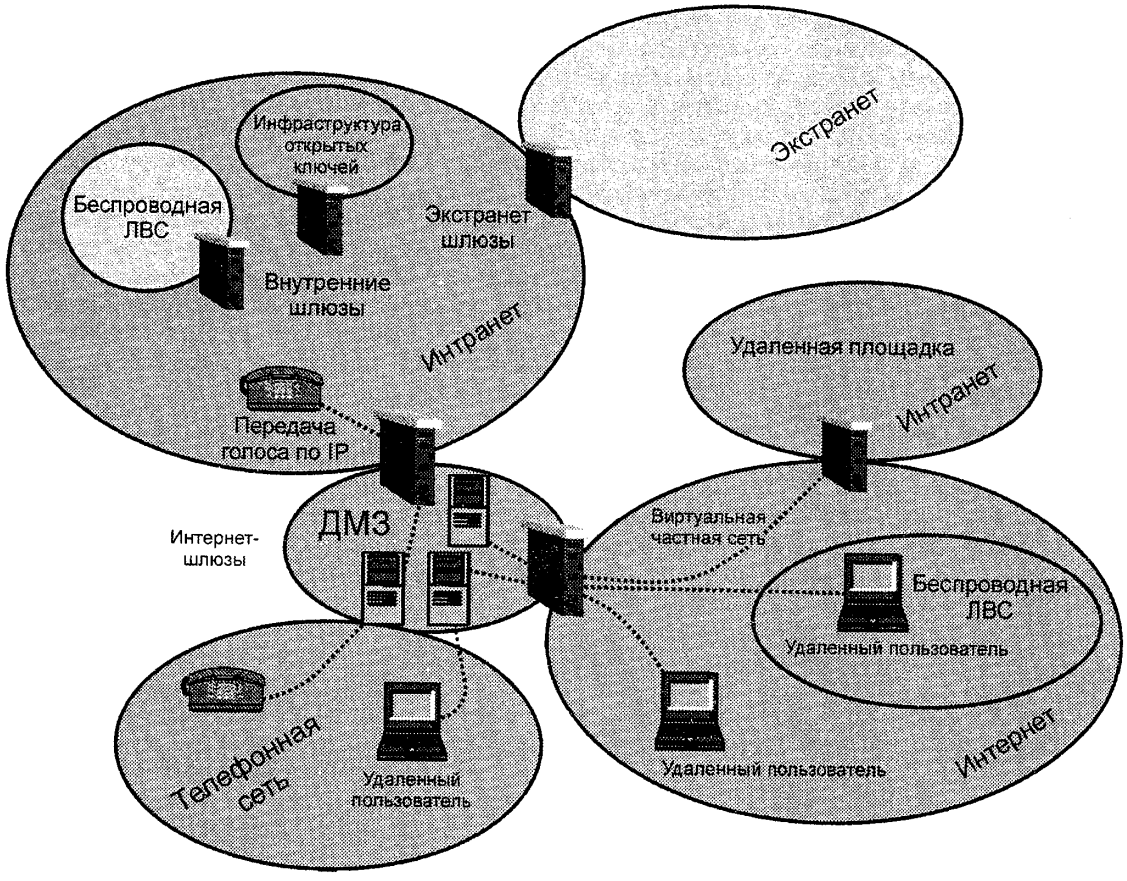


Рисунок 3. Пример сетевой среды

Интранет является внутренней сетью, используемой и поддерживаемой организацией. Обычно только работающие в организации лица имеют прямой физический доступ к этой сети, а поскольку сеть располагается в пределах помещений, являющихся собственностью

организации, можно легко обеспечить определенный уровень физической защиты. В большинстве случаев сеть Интранет является неоднородной в отношении использованных технологий и требований безопасности; она может включать в себя инфраструктуры, нуждающиеся в более высоком уровне защиты, чем предоставляемый сетью Интранет.

Управление такими инфраструктурами, например важнейшими частями среды PKI (инфраструктуры открытых ключей), может осуществляться в выделенном сегменте сети Интранет. С другой стороны, определенные технологии [например, инфраструктуры WLAN (беспроводной локальной вычислительной сети)] могут потребовать некоторого изолирования и аутентификации, так как они вносят дополнительные риски. Во всех ситуациях для реализации такого сегментирования могут использоваться внутренние шлюзы безопасности.

Потребности основной деятельности большинства организаций делают необходимыми связь и обмен данными с внешними партнерами и другими организациями. Часто связь с большинством важнейших деловых партнеров осуществляется способом, непосредственно расширяющим Интранет в сторону сети организации-партнера; для таких расширений обычно используется термин "Экстранет". Поскольку доверие к подключенным организациям-партнерам в большинстве случаев ниже, чем к сотрудникам самой организации, для устранения рисков, вносимых этими соединениями, используются шлюзы безопасности Экстранет.

Кроме того, общедоступные сети, наиболее распространенным примером которых является Интернет, используются сегодня для предоставления экономически оправданных средств связи и обмена данными с партнерами, клиентами и широкой публикой и обеспечения различных форм расширения сети Интранет. Из-за низкого уровня доверия в общедоступных сетях, особенно в Интернете, для содействия менеджменту соответствующих рисков необходимы усовершенствованные шлюзы безопасности. Эти шлюзы безопасности включают в себя специфические компоненты для учета требований различных форм расширения сети Интранет, а также связи с партнерами и клиентами.

Удаленные пользователи могут быть подсоединены посредством технологии виртуальных частных сетей. Кроме того, они могут использовать беспроводные средства связи, такие, например, как общедоступные точки доступа к WLAN, для получения доступа к Интернету. В качестве альтернативы для установления прямых коммутируемых соединений по телефонной линии с сервером удаленного доступа, который часто размещается в ДМЗ межсетевого экрана Интернет, удаленные пользователи могут задействовать телефонную сеть.

Если организация решает использовать технологии передачи речи по IP (VoIP) для реализации внутренней телефонной сети, то, как правило, используются соответствующие шлюзы безопасности для телефонной сети.

Благоприятные возможности для основной деятельности организации, предлагаемые новыми видами сетевой среды, должны сопоставляться с рисками, которые привносят новые технологии. Например, Интернет имеет ряд технических свойств, которые могут вызывать беспокойство с точки зрения безопасности, так как он первоначально проектировался в расчете на установление соединения, а не исходя из соображений безопасности - и многие из его обычно используемых основных протоколов не являются безопасными по своей природе. В глобальной сетевой среде насчитывается большое число людей, обладающих способностями, знаниями и склонностью к получению доступа к лежащим в ее основе механизмам и протоколам и созданию инцидентов безопасности от несанкционированного доступа до крупномасштабного отказа в обслуживании.

6.2. Планирование и менеджмент сетевой безопасности

При рассмотрении вопроса о сетевых соединениях все сотрудники организации, чьи

обязанности связаны с обслуживанием соединений сети, должны отчетливо сознавать важность требований и выгод основной деятельности организации, взаимосвязанных рисков безопасности и взаимосвязанных аспектов специализированной архитектуры безопасности/методы проектирования и области действия мер и средств контроля и управления безопасностью. Требования и выгоды основной деятельности организации влияют на многие решения и действия, предпринимаемые в процессе рассмотрения вопроса сетевых соединений, идентификации аспектов специализированной архитектуры безопасности/методов проектирования и потенциальных областей действия мер и средств контроля и управления безопасностью и, в конечном счете, выбора, проектирования, реализации и поддержки безопасных сетей.

Общий процесс достижения и поддержки необходимой сетевой безопасности можно кратко изложить следующим образом:

а) определение области/контекста, а затем оценка рисков безопасности:

1) сбор информации о текущей и (или) планируемой сетевой среде:

i) рассмотрение корпоративной политики информационной безопасности на предмет формулировок о рисках, связанных с сетями, которые всегда будут считаться высокими, а также мерах и средствах контроля и управления сетевой безопасностью, которые должны быть реализованы независимо от оцененных рисков;

Примечание. Следует отметить, что эта политика должна также отражать позицию организации в отношении (см. перечисление 1) регулирующих и законодательных требований безопасности, связанных с сетевыми соединениями, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти) (см. перечисление 2), значимости данных, которые будут храниться в сети или передаваться по сети.

ii) сбор и проверка информации о текущей и (или) планируемой сети (сетях) - архитектура (архитектуры), приложения, услуги, виды соединений и другие характеристики, что будет иметь отношение к идентификации и оценке рисков и определению того, что является возможным с точки зрения специализированной архитектуры/проекта сетевой безопасности;

iii) сбор другой информации с тем, чтобы иметь возможность оценить потенциальное неблагоприятное влияние на основную деятельность организации, угрозы и уязвимости (представляет ценность для операций основной деятельности организации, касающихся информации, которая должна передаваться через сетевые соединения, и любой другой информации, потенциально доступной несанкционированным образом через эти соединения, а также для предоставляемых услуг);

2) идентификация и оценка рисков сетевой безопасности и соответствующих потенциальных областей действия мер и средств контроля и управления:

i) осуществление оценки риска сетевой безопасности и проводимой руководством проверки с использованием информации о риске, связанном с требуемыми сетевыми сценариями и вопросами сетевых "технологий" (см. разделы 10 и 11) - определение требований безопасности. [Следует обратить внимание на то, что это будет включать в себя (см. перечисление 1) оценку рисков, связанных с потенциальными нарушениями значимых предписаний и законов, касающихся сетевых соединений, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти) (см. перечисление 2), использование установленных потенциальных неблагоприятных влияний на основную деятельность организации, подтверждающих значимость/секретность данных, которые будут

храниться или передаваться по сети];

b) идентификация поддерживающих мер и средств контроля и управления безопасностью - технических и нетехнических - применяемых не только к сетям (см. раздел 8);

c) рассмотрение вариантов специализированной архитектуры/проекта сетевой безопасности с учетом сетевых сценариев и вопросов сетевых "технологий", выбором и документированием предпочтительной специализированной архитектуры/проекта безопасности и связанных с ними мер и средств контроля и управления безопасностью (см. разделы 9 - 11 и Приложение A). [Следует отметить, что это будет касаться мер и средств контроля и управления, необходимых для соблюдения соответствующих предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти)];

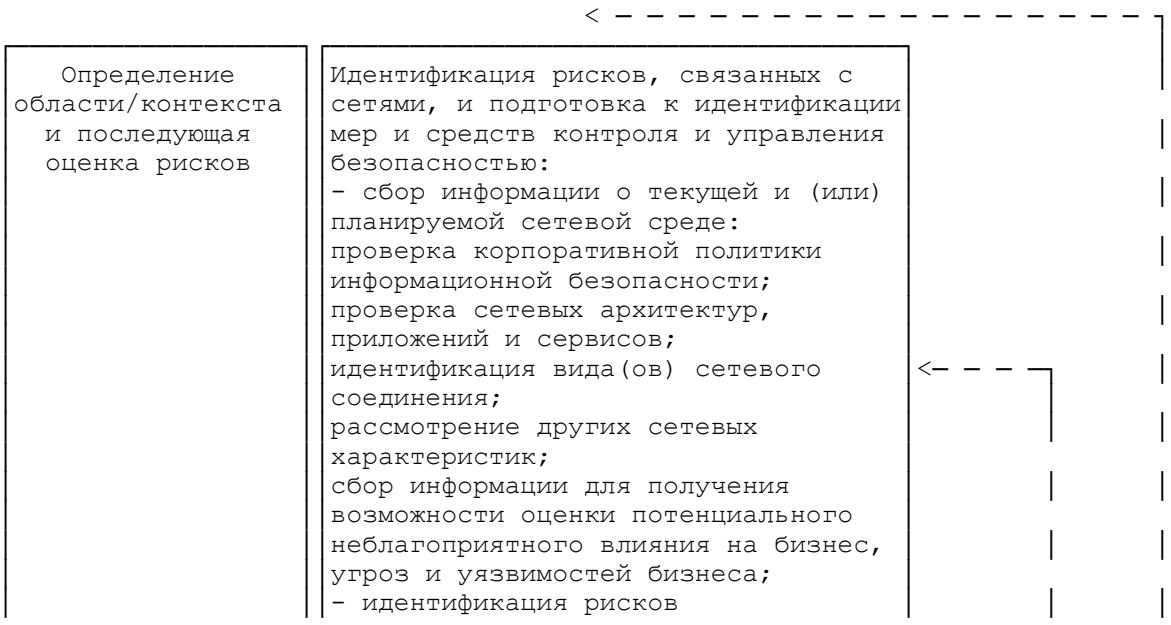
d) разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности (см. раздел 12);

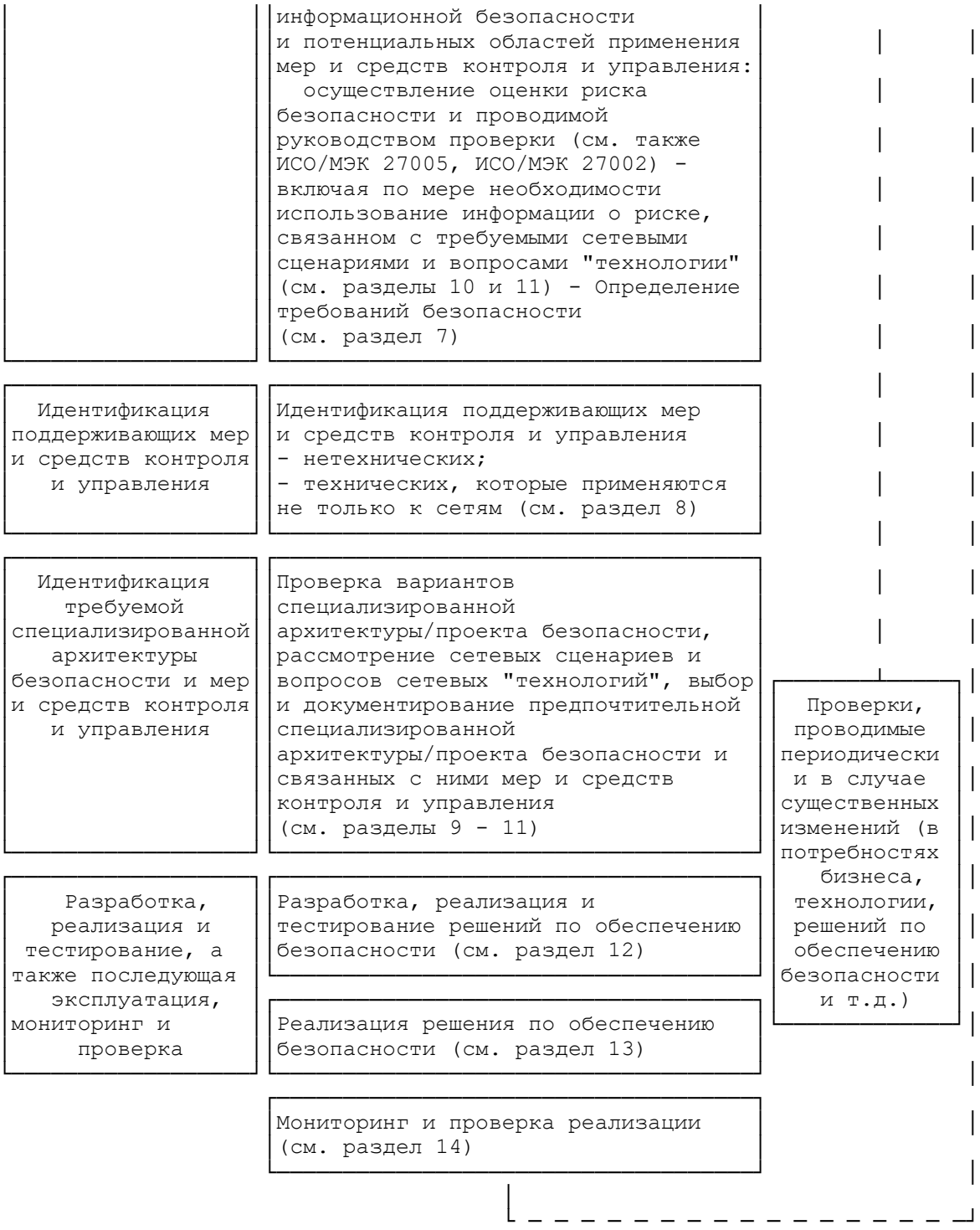
e) реализация и эксплуатация мер и средств контроля и управления безопасностью (см. раздел 13);

f) мониторинг и проверка реализации (см. раздел 14). [Следует отметить, что процесс будет включать мониторинг и проверку мер и средств контроля и управления, необходимых для соблюдения соответствующих предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти)]:

1) проверки должны проводиться периодически, а также в случае существенных изменений (в потребностях основной деятельности организации, технологии, решений по обеспечению безопасности и т.д.), и по мере необходимости должны пересматриваться и корректироваться результаты описанных выше предыдущих этапов.

Схема процесса планирования и менеджмента сетевой безопасности представлена на рисунке 4.





Примечание. См. также ИСО/МЭК 27001 - ИСО/МЭК 27005.

Рисунок 4. Процесс планирования
и менеджмента сетевой безопасности

Следует подчеркнуть, что на протяжении этого процесса, по мере необходимости и для получения общих рекомендаций по идентификации мер и средств контроля и управления

безопасностью, необходимо обратиться к ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005. Настоящий стандарт дополняет эти стандарты, предоставляя вводную информацию к тому, как следует идентифицировать соответствующие меры и средства контроля и управления сетевой безопасностью и, следовательно, к ИСО/МЭК 27033-2 - ИСО/МЭК 27033-7.

7. Идентификация рисков и подготовка к идентификации мер и средств контроля и управления безопасностью

7.1. Введение

Как показано в разделе 6, первым этапом идентификации и оценки рисков, связанных с сетями, и подготовки к идентификации мер и средств контроля и управления безопасностью является сбор информации о текущей и (или) планируемой сетевой среде.

Рекомендации по сбору информации о текущей и (или) планируемой сетевой среде представлены в 7.2. Вторым этапом является идентификация и оценка рисков сетевой безопасности и соответствующих потенциальных областей действия мер и средств контроля и управления, рекомендации по которому представлены в 7.3.

7.2. Информация о текущем и (или) планируемом построении сети

7.2.1. Требования безопасности в корпоративной политике информационной безопасности

Корпоративная политика информационной безопасности организации (или сообщества) может включать в себя утверждение о необходимости обеспечения конфиденциальности, целостности, неотказуемости и доступности, а также суждения о видах угроз и рисков и мерах и средствах контроля и управления сетевой безопасностью, которые должны быть реализованы независимо от оцененных рисков. Первым шагом построения сети должно быть рассмотрение корпоративной политики информационной безопасности с целью получения подробностей о любых связанных с сетями рисках, которые всегда будут рассматриваться как высокие, и мерах, средствах контроля и управления сетевой безопасностью, которые должны быть реализованы.

Например, такая политика может констатировать, что:

- главной задачей является доступность определенных видов информации или услуг;

- все соединения через коммутируемые линии запрещены;

- все соединения с Интернетом должны осуществляться через шлюз безопасности;

- должен использоваться определенный вид шлюза безопасности;

- платежное поручение недействительно без цифровой подписи.

Данные требования должны учитываться при осуществлении оценки риска и проводимой руководством организации проверки и идентификации аспектов специализированной архитектуры/проекта безопасности и потенциальных мер и средств контроля и управления безопасностью. Любые подобные требования должны быть документированы в предварительном списке потенциальных областей применения мер и средств контроля и управления и, при необходимости, отражены в вариантах специализированной архитектуры/проекта безопасности.

Рекомендации по политике информационной безопасности изложены в ИСО/МЭК 27002 и ИСО/МЭК 27005.

7.2.2. Информация о текущем/планируемом построении сети

7.2.2.1. Введение

Следующим шагом должен быть сбор и проверка информации о текущей(их) и (или) планируемой(ых) сети(ях) - архитектур(ы), приложениях, услугах, видах соединений и других характеристиках - это будет иметь отношение к идентификации и оценке рисков и определению того, что является возможным с точки зрения специализированной архитектуры/проекта сетевой безопасности. Указанные характеристики представлены ниже.

7.2.2.2. Сетевые архитектуры, приложения и сервисы

Должны быть получены подробности о соответствующей текущей и (или) планируемой сетевой архитектуре, приложениях и сервисах, которые должны быть проверены в целях обеспечения необходимого понимания и контекста для осуществления оценки риска сетевой безопасности и проводимой руководством проверки и, исходя из этого, рассмотрения вариантов специализированной архитектуры сетевой безопасности. В результате прояснения этих аспектов на самой ранней стадии процесс идентификации и оценки рисков безопасности, соответствующих мер и средств контроля и управления безопасностью, вариантов специализированной архитектуры сетевой безопасности и принятия решения о том, какой из этих вариантов следует выбрать, должен стать более эффективным и в итоге привести к более рациональному решению по обеспечению безопасности.

Кроме того, рассмотрение текущих и (или) планируемых аспектов сетевой архитектуры, приложений и сервисов на ранней стадии предоставит время для проверки и возможной модификации этих аспектов, если приемлемое решение по обеспечению безопасности не может быть практически достигнуто в пределах существующей и (или) планируемой среды.

В зависимости от охватываемой области сети можно классифицировать как:

- локальные вычислительные сети (ЛВС), используемые для локального соединения систем;

- ГВС, используемые для соединения систем, распространенных по всему миру.

(Некоторые источники также дают отдельное определение термина "региональная вычислительная сеть" (Metropolitan Area Network; MAN) для локально-ограниченной глобальной вычислительной сети, например, в пределах города. Однако в настоящее время для таких сетей используются те же технологии, что и для глобальных вычислительных сетей, поэтому существенных различий между региональной и глобальной вычислительной сетью больше не существует. Кроме того, для целей данного стандарта ПВС (Personal Area Network; PANs) будут классифицироваться как ЛВС. Еще одним термином, используемым в настоящее время, является термин "всемирная вычислительная сеть" (Global Area Network; GAN), т.е. всемирная ГВС. Следует отметить, что в настоящее время существуют термины, используемые для сетей, связанных с хранением данных, такие, например, как "сеть устройств хранения данных" (Storage Area Network; SAN) и "сетевая система хранения данных" (Network Attached Storage; NAS), но они выходят за рамки ИСО/МЭК 27033).

Различные протоколы имеют различные характеристики безопасности и подлежат особому рассмотрению. Например:

- протоколы разделяемой среды - в основном используются в локальных сетях и обеспечивают механизмы регулирования совместного использования ресурсов среды между соединенными системами. При использовании разделяемой среды вся информация в сети

физически доступна всем подсоединенным системам. Примером служит концентратор Ethernet;

- протоколы управления доступом, предназначенные для разрешения входа в сеть. Примерами являются IEEE 802.1x и защищенный доступ в беспроводных сетях;

- протоколы маршрутизации - используются для определения маршрутов через различные узлы, по которым передается информация через сегменты ЛВС или ГВС. Информация физически доступна для всех систем по маршруту передачи, и маршрутизация может быть случайно или намеренно изменена;

- протоколы MPLS, на которых основаны многие основные сети, предоставляющие услуги связи - позволяют многим частным сетям совместно использовать базовую сеть, предоставляющую услуги связи, причем ни один из пользователей какой-либо частной сети не знает о существовании других частных сетей, совместно использующих эту базовую сеть. Основным применением является реализация виртуальных частных сетей, где для идентификации и разделения трафика, принадлежащего разным виртуальным частным сетям, используют метки-признаки (виртуальная частная сеть, основанная на MPLS, не основана на механизмах шифрования данных). Использование меток-признаков дает возможность корпоративным клиентам передавать свою внутреннюю сеть провайдеру услуг и таким образом избегать необходимости развертывать и осуществлять управление собственной базовой сетью на основе IP-адресов. Основное преимущество состоит в возможности объединения сетевых услуг, таких как передача речи и данных по одной сети с использованием механизмов качества обслуживания для обеспечения функционирования в режиме реального времени.

Многие протоколы, используемые в сетях, не обеспечивают ее безопасность. Например, злоумышленники обычно используют инструментальные средства для извлечения паролей из сетевого трафика. Использование злоумышленниками инструментальных средств для извлечения паролей делает протоколы, посылающие незашифрованные пароли через общедоступные сети, подобные протоколу Telnet, крайне уязвимыми.

Примечание. Telnet - это программа эмуляции терминала для работы в режиме on-line на удаленном компьютере.

Многие протоколы могут быть использованы совместно с различными средами и топологиями сети, а также путем использования проводных и беспроводных технологий. Во многих случаях это оказывает дополнительное влияние на характеристики безопасности.

Используемые в сети виды приложений должны рассматриваться в контексте безопасности. Эти виды могут включать в себя:

- приложения для "тонкого" клиента;

- настольные приложения;

- приложения на основе эмуляции терминала;

- инфраструктуры и приложения обмена сообщениями;

- приложения "Сохранить и переслать" или приложения, основанные на буферизации;

- приложения "Клиент-сервер".

Приведенные ниже примеры показывают, как характеристики приложений влияют на требования безопасности сетевой среды, которую они могут использовать:

- приложения обмена сообщениями (обеспечивающие шифрование и электронные цифровые подписи для сообщений) могут обеспечивать адекватный уровень безопасности без реализации специальных мер и средств контроля и управления безопасностью в сети;

- для реализации соответствующих функциональных возможностей приложений для "тонкого" клиента может потребоваться загрузка мобильной программы. В то время как конфиденциальность может не быть важной проблемой в этом контексте, важным аспектом является целостность, и для ее обеспечения сеть должна предоставлять соответствующие механизмы. В качестве альтернативы при необходимости выполнения более высоких требований электронная цифровая подпись мобильной программы должна обеспечить целостность и дополнительную аутентификацию. Часто это осуществляется в самой структуре приложения, поэтому необходимость предоставления этих сервисов в сети может не возникать;

- приложения "Сохранить и переслать" или приложения, основанные на буферизации, обычно временно хранят важные данные в промежуточных узлах для дальнейшей обработки. При появлении требований целостности и конфиденциальности для обеспечения защиты данных во время транзита в сети потребуются соответствующие меры и средства контроля и управления. Однако из-за временного хранения данных на промежуточных узлах этих мер и средств контроля и управления может быть недостаточно. Таким образом, может потребоваться применение дополнительных мер и средств контроля и управления для обеспечения также защиты данных, хранящихся на промежуточных узлах.

Виды используемых в сети сервисов (например, служба доменных имен, электронная почта, передача речи) тоже должны рассматриваться в контексте безопасности.

При проверке сетевой архитектуры, приложений и сервисов следует также обращать внимание на сетевые соединения, существующие внутри организаций/сообществ, исходящие или входящие по отношению к ним, а также на сеть, с которой предполагается осуществить соединение. Существующие соединения организации/сообщества могут ограничивать или не допускать создание новых соединений, например, из-за имеющихся соглашений или договоров. Существование других соединений с сетью, к которой требуется подсоединение, может вносить дополнительные уязвимости и, следовательно, вызывать более высокие риски, оправдывая, вероятно, применение более строгих и (или) дополнительных мер и средств контроля и управления.

(Общее руководство по сетевым архитектурам и архитектурам приложений приведено в ИСО/МЭК 7498).

7.2.2.3. Виды сетевых соединений

Существует много общих видов сетевых соединений, использование которых может требоваться организации/сообществу. Некоторые из этих видов соединений могут осуществляться через частные сети (доступ к которым ограничен известным сообществом), а некоторые могут осуществляться через общедоступные сети (доступ к которым может получить практически любая организация или любое лицо). Кроме того, эти виды сетевых соединений могут применяться для различных услуг, например, электронной почты, и могут использовать средства сетей Интернет, Интранет или Экстранет, отличающиеся различными аспектами, связанными с обеспечением безопасности. Каждый из видов соединений может иметь различные уязвимости и, следовательно, связанные с ними риски безопасности, поэтому в конечном итоге будет требоваться различный набор мер и средств контроля и управления.

Способами классификации общих видов сетевых соединений, которые могут потребоваться для деятельности организации, являются:

- соединение между различными частями одной и той же организации в пределах одного и того же контролируемого местоположения, т.е. единственного контролируемого строения или площадки;

- соединение между различными территориально разбросанными частями одной и той же организации, например, региональными офисами с центральной площадкой, через глобальную вычислительную сеть. Большинство (если не все) пользователи имеют возможность получения доступа к информационным системам, доступным через сеть, но не всем пользователям в пределах организации разрешен доступ ко всем приложениям или информации;

- соединения между площадкой организации и персоналом, работающим вдали от организации, или установление удаленной связи с вычислительными системами организации сотрудниками, работающими дома или на других удаленных площадках, не связанных сетью, поддерживаемой организацией;

- соединения между разными организациями в пределах замкнутого сообщества, например, вследствие договорных или других юридически обязательных ситуаций или вследствие сходных интересов деятельности, например, банковских услуг или страхования. Такие соединения не будут предоставлять доступ к полному спектру приложений, используемых каждой из организаций-участниц;

- соединения с другими организациями, например, с целью получения доступа к удаленным базам данных, поддерживаемым другими организациями. При таком виде сетевого соединения все пользователи, включая пользователей подключаемой организации, индивидуально предварительно авторизованы той внешней организацией, к чьей информации предоставляется доступ;

- соединения с общедоступным доменом, при которых пользователями организации инициируется доступ к общедоступным базам данных, веб-сайтам и (или) службам электронной почты (например, через Интернет);

- соединения с телефонной сетью общего пользования из IP-среды, при которых инициируется доступ к коммутируемой сети общего пользования с телефона в IP-сети. Такие соединения являются неконтролируемыми, так как звонки могут приниматься из любой точки мира.

Какой бы из способов классификации не использовался, различные виды соединений в текущей и (или) планируемой сетевой среде должны быть проверены на предмет их последствий для безопасности, и полученная информация должна быть использована в процессе идентификации и оценки рисков безопасности, связанных с ними мер и средств контроля и управления безопасностью, вариантов специализированной архитектуры сетевой безопасности и принятия решения о том, какой из способов следует выбрать.

7.2.2.4. Другие сетевые характеристики

Должны быть проверены другие характеристики текущей и (или) планируемой сети (сетей). Особенно важно определить, является ли используемая/планируемая сеть общедоступной - сетью, которая доступна каждому, или частной сетью, например, сетью, состоящей из находящихся в собственности или выделенных линий и потому считающейся более безопасной, чем общедоступная сеть. Также важно знать вид передаваемых сетью данных, например:

- сеть передачи данных - передает, главным образом, данные и использует протоколы передачи данных;

- сеть передачи речи - сеть предназначена для телефонной связи, но также пригодна для передачи данных или

- "гибридная" сеть - объединяет передачу данных, речи, и, возможно, видео. Также значимой является следующая информация:

- является ли сеть пакетной, коммутируемой или сетью с многопротокольной коммутацией на основе признаков;

- поддерживается ли качество обслуживания, например, в сети с многопротокольной коммутацией на основе меток. (Качество обслуживания означает согласованное функционирование, достоверность и доступность. Сетевые услуги считают пригодными при обеспечении минимального уровня функционирования. Например, в случае неадекватности полосы пропускания при предоставлении услуги передачи голоса речь будет прерываться и искажаться. Качество обслуживания относится к способности сетевой системы поддерживать данную услугу на требуемом минимальном уровне функционирования или выше него).

Кроме того, следует установить, является ли соединение постоянным или оно устанавливается по мере необходимости.

Когда данные характеристики текущей и (или) планируемой сети идентифицированы и, как минимум, установлено, является ли сеть общедоступной или частной, стоит рассмотреть нижеперечисленные факторы в качестве входной информации для оценки риска сетевой безопасности и проводимой руководством проверки, т.е. примерно определить категорию сети, в чем-то подобной сети с:

- неизвестным кругом пользователей;

- известным кругом пользователей и в пределах замкнутого сообщества (нескольких организаций);

- известным кругом пользователей только в пределах организации.

Затем рассматривают полученную категорию на предмет того, является ли используемая/планируемая сеть общедоступной или частной сетью, и далее классифицируют ее как сеть:

- с неизвестным кругом пользователей и использованием общедоступной сети;

- с известным кругом пользователей в пределах замкнутого сообщества и с использованием общедоступной сети;

- с известным кругом пользователей только в пределах организации и использованием общедоступной сети;

- с неизвестным кругом пользователей и использованием частной сети;

- с известным кругом пользователей в пределах замкнутого сообщества и использованием частной сети;

- с известным кругом пользователей только в пределах организации и использованием частной сети.

Каким бы способом категории сетей не проверялись, следует сознавать, что определенные

комбинации, вероятно, будут означать более низкие уровни риска сетей. Полученная информация должна использоваться в процессе идентификации и оценки рисков безопасности, связанных с ними мер и средств контроля и управления безопасностью, вариантов специализированной архитектуры сетевой безопасности и принятия решения о том, какой из способов должен быть выбран.

7.2.2.5. Дополнительная информация

Наконец, должна быть собрана дополнительная информация для надлежащей подготовки к оценке риска сетевой безопасности и проводимой руководством проверке в соответствии с требованиями ИСО/МЭК 27001 и ИСО/МЭК 27002, включая тщательное определение границ/области проверки. Выполнение этого при первой возможности позволит избежать дальнейшей неопределенности и ненужной работы и повысит сосредоточенность и эффективность проверки. Определение границ/области должно ясно показать, что из приведенного ниже следует рассматривать при осуществлении оценки риска сетевой безопасности и проводимой руководством проверки:

- виды информации;

- процессы основной деятельности;

- фактические или потенциальные аппаратные компоненты, программные средства, услуги, соединения и подобные детали (если они неизвестны конкретно, то - в общих чертах);

- фактическую или потенциальную среду (например, площадки, помещения);

- виды деятельности (операции).

Эта информация вместе с собранной в соответствии с 7.2, которая должна использоваться при оценке риска сетевой безопасности и проводимой руководством проверке, а также связанная с ними деятельность - обобщены в 7.3.

7.3. Риски информационной безопасности и потенциальные области применения мер и средств контроля и управления

В настоящее время большинство организаций зависит от использования сетей и связанных с ними информационных систем и информации для поддержки функционирования своей деятельности. Кроме того, во многих случаях существует четко выраженная потребность основной деятельности в отношении использования сетей между информационными системами на каждой площадке организации, а также в других местах как внутри организации, так и за ее пределами, включая соединение с общедоступной сетью. При установлении соединения с другой сетью следует проявлять значительную осторожность для обеспечения того, чтобы организация не подвергалась дополнительным рискам (вследствие потенциальных угроз, использующих уязвимости). Эти риски могут исходить, например, от самого соединения или от абонента на другом конце сети.

Некоторые из этих рисков могут быть связаны с обеспечением соблюдения соответствующего законодательства и предписаний. (Особое внимание следует уделять законам о неприкосновенности частной жизни и защите данных. В некоторых странах приняты законы, устанавливающие меры и средства контроля и управления сбором, обработкой и передачей персональных данных, т.е. данных, которые могут быть связаны с конкретным лицом или лицами. В зависимости от соответствующего национального законодательства такие меры и средства контроля и управления могут налагать определенные обязанности на лиц, собирающих, обрабатывающих и распространяющих персональную информацию через сети, и

даже могут ограничивать возможность передачи этих данных в определенные страны, приводя к дополнительным серьезным проблемам, связанным с безопасностью. Менее наглядными примерами данных, которые могут стать объектом такого законодательства, являются некоторые сведения об отдельных категориях аппаратных средств и IP-адреса).

Таким образом, риски, с которыми сталкивается организация, могут быть связаны с проблемами несанкционированного доступа к информации, несанкционированной передачи информации, внесения вредоносной программы, отказа от факта приема или источника информации, отказа в обслуживании и недоступности информации или услуг. Указанные угрозы могут быть связаны с утратой:

- конфиденциальности информации и программы (в сетях и системах, соединенных с сетями);

- целостности информации и программы (в сетях и системах, соединенных с сетями);

- доступности информации и сетевых услуг (и систем, соединенных с сетями);

- неотказуемости сетевых транзакций (обязательств);

- подотчетности сетевых транзакций;

- подлинности информации (а также аутентичности сетевых пользователей и администраторов);

- достоверности информации и программы (в сетях и системах, соединенных с сетями);

- способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов, включая осуществление контроля в контексте политики безопасности организации (например, продажа полосы пропускания или использование полосы пропускания для собственной выгоды) и выполнение обязательств в отношении законодательства и предписаний (например, в отношении хранения детской порнографии);

- способности контролировать злоупотребление санкционированным доступом.

Концептуальная модель сетевой безопасности, показывающая, где могут возникать разные виды рисков безопасности, представлена на рисунке 5.

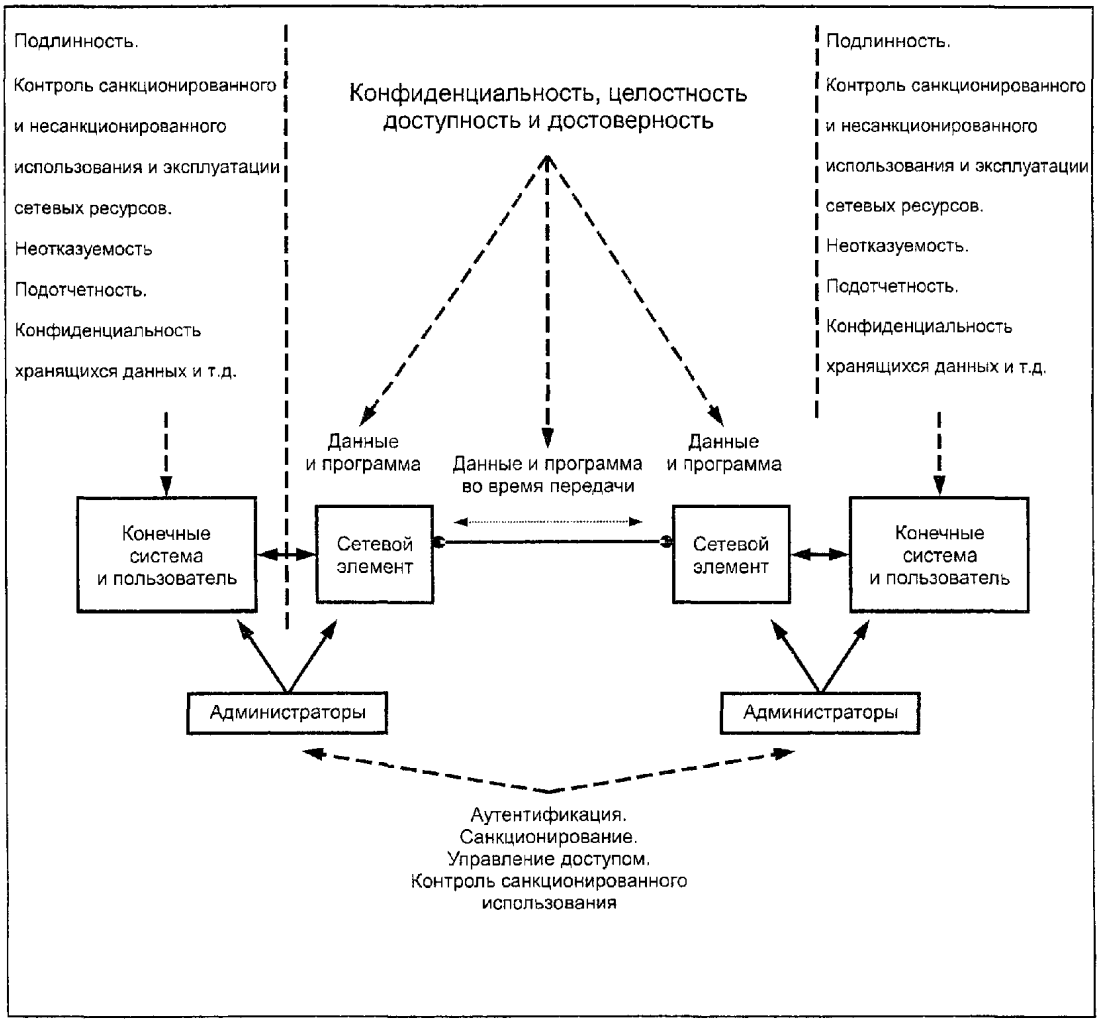


Рисунок 5. Концептуальная модель
областей риска сетевой безопасности

Таким образом, для идентификации и подтверждения технических мер и средств контроля и управления безопасностью, аспектов специализированной архитектуры/проекта безопасности и поддерживающих нетехнических мер и средств контроля и управления безопасностью должна проводиться оценка риска сетевой безопасности и, руководством организации, - проверка обеспечения безопасности в соответствии с рекомендациями, представленными в ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005. Для этого должны быть выполнены следующие основные действия:

- определение степени значимости информации и услуг, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность организации в случае возникновения нежелательных инцидентов (оценка активов). К оценке активов относится рассмотрение ценности информации для деятельности организации, передаваемой по сети, и любой другой информации, к которой можно получить несанкционированный доступ посредством сети, а также рассмотрение ценности предоставляемых услуг;

- идентификация и оценка вероятности или уровней угроз, направленных против информации и услуг;

- идентификация и оценка степени серьезности или уровня уязвимостей (слабых мест), которые могли бы быть использованы идентифицированными угрозами;

- оценка величины рисков, основывающихся на определенных последствиях потенциального неблагоприятного воздействия на операции деятельности организации и уровнях угроз и уязвимостей;

- идентификация аспектов специализированной архитектуры/проекта безопасности и оправданных потенциальных областей действия мер и средств контроля и управления безопасностью, необходимых для обеспечения того, чтобы оцененные риски оставались в допустимых пределах.

Основные процессы оценки и менеджмента риска сетевой безопасности показаны ниже на рисунке 6 (в сущности, это является расширением представленного на рисунке 4 блока "Определение области/контекста и последующая оценка рисков" и связанного с ним блока "Идентификация рисков, связанных с сетями, и подготовка к идентификации мер и средств контроля и управления безопасностью").

Рисунок 6. Процессы оценки и менеджмента риска сетевой безопасности

Примечание 1. Определение значимости информации и услуг также известно как "оценивание активов".

Примечание 2. Термины, использующиеся в ИСО/МЭК 27001 и взаимосвязанных стандартах, выделены курсивом.

Примечание 3. Подробную информацию об осуществлении оценки риска сетевой безопасности и проводимых руководством проверок см. в ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005.

Первые два ряда блоков, представленные на рисунке 6 "Установление границ/области проверки" и "Идентификация активов", соответствуют подготовительным мероприятиям. Следующие два ряда блоков соответствуют мероприятиям по оценке риска, а нижние два ряда блоков - мероприятиям по выбору мер и средств контроля и управления информационной безопасностью и принятию (остаточного) риска.

Необходимо подчеркнуть, что при проведении таких проверок следует использовать (где необходимо) информацию о риске (а также о мерах и средствах контроля и управления безопасностью), связанную с необходимыми сетевыми сценариями и вопросами сетевых "технологий" (см. разделы 10 - 11 и Приложение А настоящего стандарта, а также ИСО/МЭК 27033-3 - ИСО/МЭК 27033-7).

8. Поддерживающие меры и средства контроля и управления

8.1. Введение

В настоящем разделе представлен общий обзор мер и средств контроля и управления, поддерживающих специализированные архитектуры сетевой безопасности, и связанных с ними технических мер и средств (технических и нетехнических) контроля и управления, т.е. других мер и средств контроля и управления, применимых не только к сетям. Информация о многих этих мерах и средствах контроля и управления в ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005. Меры и средства контроля и управления, являющиеся особенно важными по отношению к использованию сетей, подробно изложены в 8.2 - 8.9, где рассматриваются менеджмент сетевой безопасности (деятельность по менеджменту сетевой безопасности, роли и обязанности, связанные с обеспечением сетевой безопасности, мониторинг сети и оценка сетевой безопасности), управление техническими уязвимостями, идентификация и аутентификация, ведение контрольных журналов и мониторинг сети, а также обнаружение и предотвращение вторжений, защита от вредоносной программы, криптографические услуги и управление непрерывностью деятельности, а также представлены (где необходимо) ссылки на ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005.

8.2. Менеджмент сетевой безопасности

8.2.1. Вводная информация

Общий менеджмент сетевой безопасности должен быть безопасным, при этом необходимо уделять внимание различным доступным сетевым протоколам и связанным с ними сервисам безопасности. В поддержку безопасности организация должна рассмотреть ряд мер и средств контроля и управления сетевой безопасностью, большая часть которых может быть идентифицирована посредством применения требований ИСО/МЭК 27002 и ИСО/МЭК 27005. Меры и средства контроля и управления, которые требуют более подробного изложения в контексте сетевой безопасности, представлены в 8.2.2 - 8.2.5.

8.2.2. Деятельность по менеджменту сетевой безопасности

8.2.2.1. Введение

Ключевым требованием, предъявляемым к любой сети, является поддержание ее посредством деятельности по менеджменту безопасности, которое инициирует и контролирует

реализацию и функционирование безопасности. Эта деятельность должна осуществляться для обеспечения безопасности всех информационных систем организации/сообщества. Деятельность по менеджменту сетевой безопасности должна включать в себя:

- определение всех обязанностей, связанных с сетевой безопасностью, и назначение лица, ответственного за обеспечение безопасности;

- документально оформленную политику сетевой безопасности вместе с документированной специализированной архитектурой безопасности;

- документированные SecOPs;

- проверку соответствия требованиям безопасности, включая тестирование безопасности, для обеспечения уверенности в том, что безопасность поддерживается на требуемом уровне;

- документированные условия обеспечения безопасности для сетевого соединения, которые должны быть соблюдены, прежде чем будет получено, при необходимости, разрешение на соединение с сотрудниками организации или сторонними организациями или лицами;

- документированные условия обеспечения безопасности для удаленных сетевых пользователей;

- план менеджмента инцидентов сетевой безопасности;

- документально оформленные и проверенные планы по обеспечению непрерывности деятельности/восстановлению после прерывания.

Подробную информацию по этим вопросам см. в ИСО/МЭК 27002, ИСО/МЭК 27005 и ИСО/МЭК 18044 <1>. В настоящем разделе предоставлено дальнейшее руководство только по тем вопросам, которые особенно важны в отношении использования сетей.

<1> В тексте ИСО/МЭК 27033-1:2009 даны ссылки на ИСО/МЭК 27035 - это опечатка.

8.2.2.2. Политика сетевой безопасности

Обязанностью руководства организации является принятие и обеспечение поддержки политики сетевой безопасности организации (см. ИСО/МЭК 27002). Политика сетевой безопасности должна следовать из политики информационной безопасности организации и быть согласована с ней. Политика сетевой безопасности организации должна быть реализуемой, легко доступной для уполномоченных сотрудников организации и должна содержать четкие формулировки:

- с точки зрения руководства организации в отношении приемлемого использования сети;

- правил безопасного использования конкретных сетевых ресурсов, услуг и приложений;

- последствий невыполнения правил безопасности;

- отношения организации к неправильному использованию сети;

- логического обоснования политики и конкретных правил безопасности.

[При необходимости эти формулировки могут быть включены в политику информационной безопасности, если это более удобно для организации и (или) это делает политику более понятной для персонала].

Содержание политики сетевой безопасности должно включать в себя краткое изложение результатов оценки риска сетевой безопасности и проводимой руководством проверки (что служит обоснованием расходов на меры и средства контроля и управления) с детализацией всех выбранных мер и средств контроля и управления безопасностью, соразмерных оцененным рискам (см. 7.3).

8.2.2.3. Операционные процедуры сетевой безопасности

В поддержку политики сетевой безопасности необходимо разработать документы по осуществлению процедур безопасности. Документы должны содержать детализированные операционные процедуры, связанные с обеспечением сетевой безопасности, а также сведения о лицах, ответственных за их применение и менеджмент. Примерный образец представлен в Приложении С.

8.2.2.4. Проверка соответствия требованиям сетевой безопасности

Для всех сетей должна проводиться проверка соответствия требованиям безопасности по комплексному контрольному перечню, составленному из мер и средств контроля и управления, определенных в:

- политике сетевой безопасности;

- соответствующих SecOPs;

- специализированной архитектуре безопасности;

- политике (безопасности) доступа к сервису шлюза безопасности;

- планах обеспечения непрерывности деятельности;

- условиях обеспечения безопасности соединения (при необходимости).

Проверка должна проводиться до введения любой сети в действие, до нового основного варианта исполнения (связанного со значительными изменениями, имеющими отношение к основной деятельности организации или сети) и ежегодно - во всех иных случаях.

Проверка должна включать в себя проведение тестирования безопасности в соответствии с заранее разработанными стратегией тестирования безопасности и связанными с ней планами, точно определяющими, какие тесты должны проводиться, с чем, где и когда. Обычно проверка должна сочетать в себе поиск уязвимостей и тестирование на проникновение. Перед началом любого такого тестирования необходимо проверить план тестирования, с тем чтобы обеспечить его проведение в полном соответствии с национальным законодательством. При проведении этой проверки не следует забывать о том, что сеть может не ограничиваться распространением только в одной стране, она может распространяться на другие страны с иным законодательством. После проведения тестирования в отчетах должны указываться особенности обнаруженных уязвимостей, необходимые меры по их устранению и приоритет их принятия.

8.2.2.5. Условия обеспечения безопасности сетевых соединений со многими организациями

При отсутствии согласованных в договоре условий обеспечения безопасности соединений организация фактически принимает риски, связанные с другой оконечностью сетевого соединения, находящегося вне сферы ее действия. Такие риски могут включать в себя риски, связанные с неприкосновенностью частной жизни/защитой данных, если сетевые соединения используются для обмена персональными данными, подчиняющегося национальному законодательству на одном или обоих концах, и если другой конец сетевого соединения (находящийся вне сферы действия организации) находится в другой стране и законодательство может быть другим.

Например, организация А может потребовать, чтобы перед подключением к ее системам через сетевое соединение, организация В поддерживала и наглядно показывала конкретный уровень обеспечения безопасности для своей системы, участвующей в этом соединении. Таким образом, организация А может убедиться в том, что организация В осуществляет менеджмент своих рисков приемлемым способом. В подобных случаях организация А должна представить документ, содержащий условия обеспечения безопасности соединения и детально описывающий меры и средства контроля и управления, которые должны существовать на конце соединения организации В. Меры и средства контроля и управления должны быть реализованы организацией В, после чего организация подписывает обязательное соглашение о поддержании безопасности. Организация А сохраняет за собой право на назначение или проведение проверки соответствия в организации В.

Также бывают случаи, когда организации в сообществе обоюдно согласуют документ "Условия обеспечения безопасности соединения", в котором фиксируют обязательства и ответственность всех сторон, включая взаимную проверку соответствия.

8.2.2.6. Документированные условия обеспечения безопасности для удаленных сетевых пользователей

Пользователям, получившим разрешение на выполнение удаленной работы, должен выдаваться документ "Условия обеспечения безопасности для удаленных сетевых пользователей". В нем должна быть изложена ответственность пользователя за аппаратные и программные средства и данные относительно сети и ее безопасности.

8.2.2.7. Менеджмент инцидентов сетевой безопасности

Инциденты информационной безопасности происходят с большей вероятностью и оказывают более серьезное негативное воздействие на основную деятельность организации в случае использования сетей (в отличие от случаев их отсутствия). Кроме того, особенно в случае сетевого соединения с другими организациями, возможны значительные юридические последствия, связанные с инцидентами безопасности.

Следовательно, организация, имеющая сетевые соединения, должна обладать хорошо документально оформленной и реализованной схемой менеджмента инцидентов информационной безопасности и связанной с ней инфраструктурой, чтобы иметь возможность быстро реагировать на идентифицированные инциденты, сводить к минимуму их воздействие и извлекать из них уроки, для предотвращения их повторного появления. Следуя этой схеме, должна быть обеспечена возможность реагирования как на события информационной безопасности (идентифицированные возникновения состояния системы, услуги или сети, указывающие на возможное нарушение политики информационной безопасности, или отказ

средств защиты, или прежде неизвестную ситуацию, которая может иметь значение для безопасности), так и на инциденты информационной безопасности (на единичное событие или серии нежелательных или неожиданных событий информационной безопасности, которые со значительной вероятностью могут подвергнуть операции основной деятельности организации и угрожать информационной безопасности). Более подробная информация о менеджменте инцидентов информационной безопасности представлена в ИСО/МЭК 18044 <1>.

<1> В тексте ИСО/МЭК 27033-1:2009 даны ссылки на ИСО/МЭК 27035 - это опечатка.

8.2.3. Роли и обязанности, связанные с обеспечением сетевой безопасности

В связи с менеджментом сетевой безопасности должны выполняться следующие роли и обязанности. (Следует отметить, что в зависимости от численности организации эти роли могут комбинироваться).

Высшее руководство должно:

- определять цели безопасности организации;

- инициировать, утверждать, доводить до сведения персонала и устанавливать политику, процедуры и правила безопасности организации;

- инициировать, утверждать, доводить до сведения персонала и устанавливать политику допустимого использования сетевых ресурсов организации;

- обеспечивать и приводить в исполнение политику обеспечения безопасности и допустимого использования сетевых ресурсов.

Примечание. Высшее руководство включает в себя владельцев основной деятельности.

Руководители, осуществляющие сетевой менеджмент, должны:

- разрабатывать детальную политику сетевой безопасности;

- реализовывать политику сетевой безопасности;

- реализовывать политику допустимого использования сетевых ресурсов;

- управлять взаимодействием с внешними заинтересованными сторонами/внешними провайдерами услуг для обеспечения соответствия внутренней и внешней политикам сетевой безопасности;

- обеспечивать разделение операционных обязанностей, связанных с сетями, и компьютерных операций при необходимости.

Группа обеспечения сетевой безопасности должна:

- приобретать, разрабатывать, тестировать, проверять и поддерживать компоненты и инструментальные средства сетевой безопасности;

- поддерживать инструментальные средства и компоненты сетевой безопасности для тщательного слежения за эволюцией угроз [например, путем обновления файлов сигнатур

вредоносной программы (в том числе вирусов)];

- устанавливать, обновлять, использовать и обеспечивать защиту сервисов и компонентов сетевой безопасности;

- выполнять необходимые ежедневные задачи по применению спецификаций, правил и параметров сетевой безопасности, требуемых действующими политиками сетевой безопасности;

- принимать соответствующие меры по обеспечению защиты компонентов сетевой безопасности (например, резервное копирование, мониторинг сетевой деятельности, реагирование на инциденты безопасности или сигналы тревоги и т.д.).

Пользователи сети должны:

- сообщать о своих требованиях к безопасности;

- соблюдать корпоративную политику безопасности;

- соблюдать корпоративные политики допустимого использования сетевых ресурсов;

- сообщать о событиях и инцидентах сетевой безопасности;

- обеспечивать обратную связь по вопросам эффективности сетевой безопасности.

Аудиторы [внутренние и (или) внешние] должны:

- проводить проверки и аудит (например, периодически проверять эффективность сетевой безопасности);

- проверять соблюдение политики сетевой безопасности;

- проверять и тестировать совместимость действующих правил сетевой безопасности с текущими требованиями основной деятельности организации и правовыми ограничениями (например, списки пользователей на получение доступа к сети).

8.2.4. Сетевой мониторинг

Сетевой мониторинг является очень важной частью менеджмента сетевой безопасности. Сетевой мониторинг обсуждается в 8.5.

8.2.5. Оценка сетевой безопасности

Сетевая безопасность является динамичным понятием. Персонал, отвечающий за обеспечение безопасности, должен быть осведомлен о самых современных разработках в этой области и должен обеспечивать уверенность в непрерывности работы сетей с установленными актуальными версиями предоставленных поставщиками исправлений программ, обеспечивающих безопасность. Необходимо периодически предпринимать шаги по проведению аудита имеющихся мер и средств контроля и управления безопасностью в отношении установленных контрольных точек, включая тестирование безопасности - поиск уязвимостей и т.д. Безопасность должна быть основным фактором при оценке новой сетевой технологии и сетевой среды.

8.3. Менеджмент технических уязвимостей

Сетевые среды, как и другие сложные системы, не свободны от погрешностей. Технические уязвимости присутствуют в компонентах и публикуются для компонентов, часто используемых в сетях. Использование этих технических уязвимостей может оказывать серьезное влияние на безопасность сетей, что чаще всего наблюдается при обеспечении доступности и конфиденциальности. Таким образом, менеджмент технических уязвимостей должен существовать, охватывая все компоненты сети, включая:

- своевременное получение информации о технических уязвимостях;

- оценку подверженности сетей подобным уязвимостям;

- определение соответствующих мер и средств контроля и управления безопасностью для решения вопросов, связанных с этими уязвимостями рисков;

- реализацию и проверку определенных мер и средств контроля и управления безопасностью. Необходимым условием для управления техническими уязвимостями должна быть доступность актуального и полного списка всех компонентов сети, обеспечивающего необходимую техническую информацию, например, о виде устройства, поставщике, номере версии аппаратных, программно-аппаратных или программных средств, а также организационную информацию, например, об ответственных административных лицах.

Если организация уже разработала общую программу управления техническими уязвимостями, предпочтительным решением вопроса должна стать интеграция управления сетевыми техническими уязвимостями в общую задачу. (Более подробную информацию об управлении техническими уязвимостями, включая рекомендацию по реализации, см. в ИСО/МЭК 27002).

8.4. Идентификация и аутентификация

Важно иметь возможность ограничения доступа через соединения, разрешая доступ только уполномоченному персоналу (являющемуся внутренним или внешним для организации). Например, распространенным требованием политики является то, чтобы доступ к определенным сетевым сервисам и связанной с ними информации был разрешен только для уполномоченного персонала. Подобные требования не являются единственными для использования сетевых соединений, и поэтому более подробная информация, относящаяся к использованию сетей, может быть получена из ИСО/МЭК 27002 и ИСО/МЭК 27005.

Областями применения мер и средств контроля и управления безопасностью, которые могут иметь отношение к использованию сетей и связанных с ними информационных систем, являются:

- удаленный вход в систему - вход в систему уполномоченного персонала, работающего вне организации, удаленного обслуживающего персонала или персонала других организаций, осуществляемый через коммутируемое соединение с организацией, Интернет-соединения, выделенные каналы связи из других организаций либо посредством коллективного доступа через Интернет. Эти соединения устанавливают при необходимости внутренними системами либо партнерами по договору с помощью общедоступных сетей. Каждый вид удаленного входа в систему должен иметь дополнительные меры и средства контроля и управления безопасностью, соответствующие характеру рассматриваемой сети. Например, непредоставление прямого доступа к системному и сетевому программным обеспечениям при учетных записях, использующихся для удаленного доступа, за исключением случаев обеспечения дополнительной аутентификации (см. усиленная аутентификация) и, возможно, сквозного шифрования, а также обеспечение защиты от несанкционированного доступа к информации, связанной с программным средством электронной почты и данными каталога,

хранящимися в персональных и дорожных компьютерах, используемых персоналом организации за пределами ее офисов;

- усиленная аутентификация - в то время как использование пар "идентификатор пользователя/пароль пользователя" является простым способом аутентификации пользователей, эти пары можно скомпрометировать или разгадать. Следовательно, должны быть рассмотрены другие (более безопасные) способы аутентификации пользователей - особенно удаленных, и (или) при наличии высокой вероятности получения доступа неуполномоченным лицом к защищенным и важным системам - вследствие того, что доступ, инициированный через общедоступные сети, или доступ к системе (например, через лэптоп), может оказаться вне непосредственного контроля организации. Простыми примерами являются использование CLID (но поскольку CLID открыт для спуфинга, его не следует использовать в качестве подтвержденного идентификатора без дополнительной аутентификации) и связей через модемы, которые отключаются, если не используются, и инициируются только после подтверждения идентификатора вызывающей стороны. Примерами более сложного, но намного более безопасного использования - особенно в контексте удаленного доступа - является использование других средств идентификации поддержки аутентификации пользователей, таких как дистанционно проверенные маркеры и смарт-карты, и обеспечение функционирования маркера или смарт-карты только вместе с аутентифицированной учетной записью уполномоченного пользователя (и предпочтительно, ПК этого пользователя, а также местоположения/точки доступа этого пользователя) и, например, любой соответствующий PIN-код или биометрический профиль. Обычно это называется "строгой, двухфакторной, аутентификацией";

- безопасное одноразовое предъявление пароля - там, где дело касается сетей, пользователи, вероятно, будут сталкиваться с многочисленными проверками идентификации и аутентификации. При таких обстоятельствах у пользователей может возникнуть соблазн использовать небезопасные методы, такие, например, как запись паролей или повторное использование одних и тех же данных аутентификации. Безопасное одноразовое предъявление пароля может снизить риски, связанные с таким поведением, путем сокращения числа паролей, которые пользователь должен запомнить. Наряду со снижением рисков это может улучшить продуктивность работы пользователя и уменьшить рабочие нагрузки "справочного стола", связанные с повторной установкой паролей. Однако следует отметить, что последствия сбоя системы безопасного одноразового предъявления пароля могут быть серьезными, так как не одна, а много систем и приложений подвергнутся риску и будут открыты для компрометации (это иногда называют "риском "ключей от царства"). Следовательно, могут потребоваться более мощные, по сравнению с обычными, механизмы идентификации и аутентификации, что желательно для исключения идентификации и аутентификации в смысле функций с высокой степенью привилегированности (системный уровень) из режима безопасного одноразового предъявления пароля.

8.5. Ведение контрольных журналов и мониторинг сети

Очень важно обеспечивать эффективность сетевой безопасности посредством ведения контрольных журналов и постоянного мониторинга с быстрым обнаружением, исследованием событий безопасности и оповещением и реагированием на них, а затем - на инциденты. Без ведения контрольных журналов и постоянного мониторинга нельзя быть уверенным в постоянной эффективности мер и средств контроля и управления сетевой безопасностью, а также в том, что не будут происходить инциденты безопасности с результирующими неблагоприятными воздействиями на операции основной деятельности организации.

В контрольных журналах должно фиксироваться достаточное количество информации об аварийных состояниях и действительных событиях, с тем чтобы можно было осуществлять

тщательный анализ предполагаемых и фактических инцидентов. Однако, признавая, что фиксирование огромного объема информации, связанной с сетевыми событиями, может затруднить управление анализом и повлиять на его продуктивность, со временем следует обращать внимание на то, что фиксируется на самом деле. Для сетей необходимо поддерживать контрольные журналы, фиксирующие следующие виды событий:

- неудавшиеся попытки входа в систему с указанием даты и времени;

- неудачные повторные аутентификации (или использования маркера);

- нарушения трафика через шлюзы безопасности;

- дистанционные попытки получения доступа к контрольным журналам сетевых событий;

- предупреждения об опасности или аварийные сообщения системы управления с последствиями для безопасности (например, дублирование IP-адреса, нарушения физической цепи).

В контексте сетей информация для контрольных журналов должна быть получена из различных источников, таких, например, как маршрутизаторы, межсетевые экраны, системы обнаружения вторжений, и передана на центральный сервер регистрации для объединения и тщательного анализа. Все контрольные журналы должны изучаться как в режиме реального времени, так и в автономном режиме. В режиме реального времени регистрационные записи могут быть отображены на экране в режиме прокрутки и использованы для предупреждения о потенциальных атаках. Автономный анализ является важным, поскольку он позволяет определять общую картину с помощью анализа тенденции. Первыми признаками атаки на сеть могут быть значительные "следы" в журналах межсетевых экранов, указывающие на действие по зондированию потенциальной цели. Система обнаружения вторжений может также обнаруживать это в реальном времени по сигнатуре атаки.

Следует подчеркнуть, что в аналитических и исследовательских целях должны использоваться соответствующие утвержденные программные средства анализа и менеджмента контрольных журналов для хранения и восстановления журналов, прослеживаемости и отчетности по контрольным журналам (в отношении конкретных пользователей, приложений и видов информации, а также временного периода, особенно если это необходимо в исследовательских целях) с быстрыми, сфокусированными и легко понятными результатами. Отчеты об анализе контрольных журналов должны архивироваться и храниться в безопасном месте в течение установленного периода времени. Кроме того, для самих контрольных журналов должна обеспечиваться защита в виде идентификации, аутентификации и управления доступом.

Постоянный мониторинг должен охватывать:

- контрольные журналы межсетевых экранов, маршрутизаторов, серверов и т.д.;

- предупреждения об опасности или аварийные сообщения из контрольных журналов, заранее сконфигурированные для уведомления об определенных видах событий, например, от межсетевых экранов, маршрутизаторов, серверов и т.д.;

- выходные данные систем обнаружения вторжений;

- результаты деятельностей по сканированию сетевой безопасности;

- информацию о событиях и инцидентах, о которых сообщили пользователи и

вспомогательный персонал;

- результаты проверок соответствия безопасности.

Контрольные журналы должны быть доступны в режиме on-line в течение периода времени, соответствующего потребностям организации, и все контрольные журналы должны дублироваться и архивироваться способом, обеспечивающим их целостность и доступность, например, с помощью носителей с однократной записью и многократным считыванием, таких, например, как компакт-диски. Кроме того, контрольные журналы должны содержать конфиденциальную информацию или информацию, пригодную для тех, кто может захотеть атаковать систему через сетевые соединения, а обладание контрольными журналами может предоставлять доказательство передачи данных по сети в случае возникновения спора. Поэтому контрольные журналы особенно необходимы в контексте обеспечения целостности информации и неотказуемости доступа к ней. Следовательно, все контрольные журналы должны быть надлежащим образом защищены, включая утилизацию архивных компакт-дисков в установленные сроки. Контрольные журналы должны храниться безопасным образом в течение периода времени, соответствующего требованиям конкретной организации и действующему законодательству. Также важно, чтобы во всех контрольных журналах и связанных с ними серверах надлежащим образом учитывалась временна́я синхронизация, например, путем использования NTP-протоколов, особенно в целях расследования и в случае возможного судебного преследования.

Следует подчеркнуть, что мониторинг сети должен проводиться способом, полностью согласующимся с соответствующим национальным и международным законодательством и предписаниями, в том числе и с законодательством по защите данных и регулированию следственных полномочий (согласно которому все пользователи должны быть проинформированы о мониторинге до его проведения). В общих чертах мониторинг должен проводиться ответственно и не использоваться, например, для анализа поведения сотрудников в странах с жесткими нормами права, охраняющими неприкосновенность частной жизни. Очевидно, что проводимые действия должны согласовываться с политиками безопасности и секретности организации/сообщества, и быть установлены соответствующие режиму процедуры и связанные с ними обязанности. Ведение сетевых контрольных журналов и мониторинг сети также должны проводиться безопасным с точки зрения права образом, с учетом того, что данные контрольных журналов могут использоваться при уголовном или гражданском преследовании.

Бо́льшую часть мер и средств контроля и управления безопасностью по ведению контрольных журналов и мониторингу, требующихся в отношении использования сетей и связанных с ними информационных систем, можно определить с помощью ИСО/МЭК 27002 и ИСО/МЭК 27005.

8.6. Обнаружение и предотвращение вторжений

С увеличением использования сетей злоумышленникам стало проще находить многочисленные способы проникновения в информационные системы и сети организации или сообщества, маскировать свои исходные точки доступа и получать доступ через сети и целевые внутренние информационные системы. Кроме того, злоумышленники становятся все более изощренными, а в Интернете или в открытой литературе легко доступны усовершенствованные методы и средства атак на информационные системы. Действительно, многие из средств атаки на информационные системы являются автоматизированными, могут быть очень эффективны и просты в использовании, включая применение их лицами с ограниченным опытом проникновения в информационные системы.

Для большинства организаций экономически невозможно предотвратить все потенциальные проникновения. Следовательно, существует вероятность осуществления некоторых проникновений в информационные системы организации. Риски, связанные с большинством проникновений в информационные системы организации, должны рассматриваться через реализацию обоснованной идентификации и аутентификации, логического контроля доступа, мер и средств контроля и управления учетом и аудитом и, если это оправдано, вместе с возможностями обнаружения и предотвращения вторжений. Такие возможности обеспечивают способы прогнозирования вторжений, идентификации вторжений в режиме реального времени, соответствующего предупреждения об опасности и предотвращения вторжений, а также дают возможность локального сбора информации, касающейся вторжений, последующего ее обобщения и анализа, а также анализа обычных моделей поведения/использования информационных систем организации.

Система обнаружения вторжений "прослушивает" весь трафик во внутренних сетях с целью определения того, что предпринимается: попытка вторжения, вторжение происходит, вторжение уже произошло и, возможно, осуществляется реагирование на вторжение и предупреждается об опасности соответствующий персонал. Существуют два вида систем обнаружения вторжений:

- NIDS - система, осуществляющая контроль пакетов в сети и пытающаяся обнаружить злоумышленника посредством сопоставления модели атаки с базой данных известных моделей атак;

- HIDS - система, осуществляющая контроль деятельности на серверах путем мониторинга журналов регистрации событий безопасности или проверки на предмет изменений в системе, таких, например, как изменения в критических файлах системы или реестре систем.

Система предотвращения вторжений проверяет весь трафик перед его переходом во внутренние сети и автоматически блокирует все распознанные атаки; другими словами, система предупреждения вторжений специально предназначена для обеспечения возможности активного реагирования.

Подробная информация об обнаружении и предупреждении вторжений представлена в ИСО/МЭК 18043.

8.7. Защита от вредоносных программ

Вредоносные программы (вирусы, черви, троянские кони, шпионские программные средства и т.д., которые часто обозначают общим термином "вредоносные программные средства") могут быть введены через сетевые соединения. Конкретная вредоносная программа может заставить компьютер выполнять несанкционированные функции (например, "бомбардировать" указанную цель сообщениями в указанное число и время) или фактически уничтожить важные ресурсы (например, удалить файлы). Будучи продублированной, вредоносная программа пытается обнаружить другие уязвимые серверы. Вредоносная программа не может быть обнаружена до нанесения ею ущерба, если только не применяются специальные меры и средства контроля и управления. Вредоносная программа может привести к компрометации мер и средств контроля и управления безопасностью (например, к захвату и раскрытию паролей), непреднамеренному раскрытию информации, непреднамеренным ее изменениям, уничтожению информации и (или) несанкционированному использованию ресурсов системы.

Некоторые формы вредоносной программы могут обнаруживаться и удаляться специальным сканирующим программным средством. Для некоторых видов вредоносной

программы существуют сканеры для межсетевых экранов, файловых серверов, почтовых серверов, ПК/рабочих станций. Кроме того, для создания возможности обнаружения новой вредоносной программы очень важно обеспечить постоянное соответствие сканирующих программных средств уровню современных требований, желательно посредством проведения ежедневных обновлений. Однако пользователи и администраторы должны осознавать, что не следует рассчитывать на то, что сканеры обнаружат все вредоносные программы (или даже все вредоносные программы конкретного вида), поскольку постоянно появляются новые формы вредоносных программ. Обычно для усиления защиты, обеспечиваемой сканерами (при наличии), требуются другие меры и средства управления и контроля.

Основной задачей программных средств защиты от вредоносной программы является сканирование данных и программ с целью идентификации подозрительных моделей, связанных с вредоносным программным средством. Библиотека сканируемых моделей, известных как "сигнатуры", должна обновляться через определенные промежутки времени или каждый раз, когда становятся доступными новые сигнатуры для предупреждения о вредоносном программном средстве с высокой степенью риска. В контексте удаленного доступа программное средство защиты от вредоносной программы должно работать на удаленных системах, а также на серверах центральной системы - особенно на серверах операционной системы Windows и электронной почты.

Сетевые пользователи и администраторы должны осознавать, что при взаимодействии с внешними сторонами по внешним каналам связи существуют риски более значительные по сравнению с обычными, связанные с вредоносным программным средством. Должны быть разработаны рекомендации для пользователей и администраторов, определяющие процедуры и практические приемы сведения к минимуму возможности внедрения вредоносной программы.

Пользователи и администраторы должны особо позаботиться о конфигурировании систем и приложений, связанных с сетевыми соединениями, с тем чтобы блокировать функции, не являющиеся необходимыми при данных обстоятельствах. (Например, приложения ПК могут конфигурироваться так, чтобы макрокоманды блокировались по умолчанию или требовали подтверждения пользователя перед выполнением макрокоманд).

Более подробная информация о защите от вредоносных программ представлена в ИСО/МЭК 27002 и ИСО/МЭК 27005.

Примечание. В ИСО/МЭК 11889 представлена технология, широко применяемая в клиентских и серверных системах, которая может быть использована для обнаружения и изолирования программ вредоносного или неизвестного происхождения.

8.8. Услуги, основанные на криптографии

В условиях, когда большое значение имеет сохранение конфиденциальности, для шифрования информации, проходящей через сети, следует рассмотреть меры и средства контроля и управления, связанные с шифрованием. В условиях, когда большое значение имеет сохранение целостности информации, для защиты информации, проходящей по сетевым соединениям, следует рассмотреть меры и средства контроля и управления, связанные с цифровой подписью и (или) целостностью сообщения. Меры и средства контроля и управления, связанные с цифровой подписью, способны обеспечивать защиту, сходную с той, которая обеспечивается мерами и средствами контроля и управления аутентификацией сообщений. Также меры и средства контроля и управления, связанные с цифровой подписью, обладают способностью неотказуемости.

В случае, если существует требование обеспечения возможности предоставления

убедительного доказательства прохождения информации по сети (неотказуемость), необходимо рассмотреть следующие меры и средства контроля и управления:

- коммуникационные протоколы, предоставляющие подтверждение передачи данных;

- протоколы приложений, требующие предоставления адреса или идентификатора инициатора и проверяющие наличие этой информации;

- шлюзы, проверяющие форматы адреса отправителя и получателя на точность синтаксиса и непротиворечивость информации в соответствующих каталогах;

- протоколы, подтверждающие доставку из сетей и позволяющие определять порядок следования информации.

Когда важна возможность доказательства передачи или получения информации в случае возникновения спорной ситуации (другая форма неотказуемости), необходимо дополнительное обеспечение уверенности путем использования стандартного метода цифровой подписи. Если требуется подтверждение источника, то отправители информации должны скреплять информацию цифровой подписью по общему стандарту. Если требуется подтверждение доставки, то отправители должны запросить ответ, скрепленный цифровой подписью.

При принятии решения об использовании шифрования, цифровой подписи, целостности сообщения или других мер и средств контроля и управления безопасностью, основанных на шифровании, необходимо принимать во внимание соответствующие законы и предписания органов исполнительной власти, соответствующие инфраструктуры открытого ключа, требования к менеджменту ключей, пригодность использующихся механизмов шифрования для задействованного типа сетевого соединения и необходимую степень защиты, а также надежную и доверенную регистрацию пользователей или объектов, связанных с ключами (при необходимости, сертифицированными), использующимися в протоколах цифровой подписи.

Механизмы шифрования представлены в ИСО/МЭК 18033 <1>. Один из широко используемых методов шифрования известен как "блочный шрифт", а способы использования блочных шрифтов для криптографической защиты, известные как режимы работы, представлены в ИСО/МЭК 10116 <2>. Меры и средства контроля и управления целостностью сообщений, известные как коды аутентификации сообщений (или MAC), представлены в ИСО/МЭК 9797 <3>. Методы цифровой подписи представлены в ИСО/МЭК 9796 <4> и ИСО/МЭК 14888 <5>. Более подробная информация о неотказуемости представлена в ИСО/МЭК 14516 и ИСО/МЭК 13888.

<1> ISO/IEC 18033. Information technology - Security techniques - Encryption algorithms.

<2> ISO/IEC 10116. Information technology - Security techniques - Modes of operation for an n-bit block cipher.

<3> ISO/IEC 9797. Information technology - Security techniques - Message Authentication Codes (MACs).

<4> ISO/IEC 9796. Information technology - Security techniques - Digital signature schemes giving message recovery.

<5> ISO/IEC 14888. Information technology - Security techniques - Digital signatures with appendix.

Менеджмент ключей, как основная услуга из всех других криптографических услуг, обеспечивает уверенность в управлении всеми необходимыми ключами шифрования в течение их полного жизненного цикла и их использовании безопасным способом. За информацией о менеджменте ключей и по другим связанным с ним вопросам, таким как, например, инфраструктура открытых ключей, или по более общим, таким как "менеджмент идентификационных данных", следует обращаться к следующим стандартам:

ИСО/МЭК 11770 - менеджмент ключей;

ИСО/МЭК 9594-8 - каталог: схемы сертификата открытого ключа и атрибута;

ИСО 11166-2 - банковское дело, менеджмент ключей средствами асимметричных алгоритмов;

ИСО 11568 - банковское дело - менеджмент ключей (для розничной торговли);

ИСО 11649 - финансовые услуги - структурированная кредиторская справка, содержащая информацию о переводе денежной суммы;

ИСО 13492 - элементы данных менеджмента ключей (розничная торговля);

ИСО 2118 <1> - инфраструктура открытых ключей в банковском секторе.

<1> В тексте ИСО/МЭК 27033-1:2009 даны ссылки на ИСО/МЭК 21118 - это опечатка.

Следует обратить внимание на то, что криптография должна также использоваться для управления сетевыми устройствами. Кроме того, журналы сетевого менеджмента и управления доступом должны передаваться при проведении безопасных шифрованных сеансов для обеспечения защиты конфиденциальных данных.

8.9. Менеджмент непрерывности деятельности

Важно, чтобы меры и средства контроля и управления применялись для обеспечения уверенности организации в непрерывности функционирования в случае бедствия путем предоставления условий для возможности восстановления каждой из частей процесса основной деятельности организации после нарушения его хода за соответствующий интервал времени. Таким образом, у организации должна быть программа менеджмента непрерывности деятельности, включающая в себя процессы, охватывающие все этапы обеспечения непрерывности деятельности: проверку анализа воздействий на деятельность организации, проверку оценки рисков, установление требований к восстановлению деятельности организации, формулирование стратегии обеспечения непрерывности деятельности, разработку плана обеспечения непрерывности деятельности, тестирование плана обеспечения непрерывности деятельности организации, обеспечение осведомленности всего персонала о необходимости непрерывности деятельности, постоянную поддержку плана обеспечения непрерывности деятельности организации и снижение риска. Только следуя всем этапам программы менеджмента непрерывности деятельности, можно обеспечить:

- согласование необходимых приоритетов деятельностей организации и временных интервалов с ее потребностями;

- соответствие идентифицированных предпочтительных вариантов стратегии обеспечения непрерывности деятельности этим приоритетам и временным интервалам;

- наличие и тестирование надлежащих и необходимых планов и средств, охватывающих информацию, процессы основной деятельности организации, информационные системы и услуги, передачу данных и речи, людей и оборудование.

Руководство по менеджменту непрерывности деятельности в целом, включая разработку соответствующей стратегии обеспечения непрерывности деятельности и связанных с ней планов и их последующее тестирование, см. ИСО/ОТУ 22399.

Что касается сети, следует рассматривать вопросы поддержания сетевых соединений, реализации альтернативных соединений с достаточной пропускной способностью и восстановления соединений после нежелательных событий. Данные аспекты и требования должны основываться на важности сетевых соединений для функционирования организации в течение продолжительного времени и прогнозируемых неблагоприятных воздействиях на основную деятельность организации в случае нарушения процессов ее деятельности. В то время как возможность сетевых соединений может дать много преимуществ организации в отношении гибкости и способности использовать инновационные подходы в случае нарушения процесса основной деятельности, сетевые соединения могут представлять точки уязвимости и компоненты, отказ которых приводит к отказу всей системы, которые могут оказывать сильное разрушающее воздействие на организацию.

9. Рекомендации по проектированию и реализации сетевой безопасности

9.1. Вводная информация

В настоящем разделе рассматриваются различные аспекты специализированной архитектуры/проекта сетевой безопасности и связанные с ними потенциальные области применения мер и средств контроля и управления. Риски, методы проектирования и области применения мер и средств контроля и управления безопасностью для типовых сетевых сценариев представлены в разделе 10. Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления безопасностью для определенных аспектов "технологий", представляющих интерес для современных организаций, представлены в разделе 11. Конкретное решение по обеспечению сетевой безопасности фактически может охватывать ряд вопросов и областей применения мер и средств контроля и управления, представленных в разделах 10 и 11. Таблица, содержащая перекрестные ссылки между разделами ИСО/МЭК 27001 и ИСО/МЭК 27002 и настоящего стандарта, отражающими/определяющими меры и средства контроля и управления, связанные с сетевой безопасностью, представлена в Приложении В.

В соответствии с разделами 8 - 11 (и Приложением А) необходимо тщательно рассмотреть предлагаемую специализируемую архитектуру/проект сетевой безопасности и список идентифицированных мер и средств контроля и управления в контексте соответствующих сетевых архитектур и приложений. Затем, при необходимости, следует скорректировать архитектуру и список мер и средств контроля и управления и затем использовать их как основу для разработки, реализации и тестирования комплекса программных и технических средств и услуг по обеспечению безопасности (см. раздел 12). После того как специализированная архитектура безопасности и, следовательно, реализация мер и средств контроля и управления безопасностью одобрены, следует начинать их реализацию (см. раздел 13) при постоянном мониторинге и с их проверкой (см. раздел 14).

9.2. Специализированная архитектура/проект сетевой безопасности

Документирование возможных вариантов специализированной архитектуры/проекта

сетевой безопасности и реализации обеспечивает способ изучения различных решений и анализа с целью выбора компромиссного решения. К тому же документирование облегчает разрешение часто возникающих проблем, связанных с техническими ограничениями и конфликтами между требованиями основной деятельности организации и требованиями безопасности.

Документируя возможные варианты, следует надлежащим образом учитывать любые требования корпоративной политики информационной безопасности (см. 7.2.1), соответствующие сетевые архитектуры, приложения, сервисы, виды соединений и другие характеристики (см. 7.2.2), а также перечень потенциальных мер и средств контроля и управления, установленных в результате оценки риска безопасности и проводимой руководством проверки (см. 7.3). При выполнении необходимых при документировании действий следует учитывать любые существующие специализированные архитектуры/проекты безопасности. После того как варианты будут документально оформлены и проверены как часть процесса проектирования специализированной архитектуры, предпочтительная архитектура безопасности должна быть согласована и представлена в документации по определению мер и средств контроля и управления специализированной архитектуры/проекта безопасности (совместимой или несовместимой с проектом специализированной архитектуры). Затем могут быть проведены изменения сетевой архитектуры, приложений и услуг (для обеспечения совместимости с предпочтительной специализированной архитектурой/проектом безопасности) и (или) перечня потенциальных мер и средств контроля и управления [например, создавая необходимость альтернативы идентифицированным мерам и средствам контроля и управления, поскольку достигнута договоренность о том, что проект/архитектура безопасности может быть технически реализован(а) только определенным образом].

Следует отметить, что в ИСО/МЭК 27033-2 определено, как организации должны достигать качества специализированных архитектур/проектов безопасности, которые обеспечат сетевую безопасность, соответствующую среде их основной деятельности, используя последовательный подход к планированию, проектированию и реализации сетевой безопасности.

Входная информация для процесса разработки специализированной архитектуры/проекта сетевой безопасности, представленного в ИСО/МЭК 2703322, включает в себя:

- документированные требования услуг организации/сообщества;

- документацию любой существующей или планируемой архитектуры, проекта и (или) реализации;

- текущую политику сетевой безопасности (или соответствующие части связанной с ней политики безопасности информационных систем), предпочтительно основанную на результатах оценки риска или проводимой руководством проверки;

- определение активов, требующих защиты;

- текущие и планируемые требования функционирования, включая связанный с ним трафик;

- текущую информацию о продукции организации.

Выходная информация процесса проектирования включает в себя:

- документацию специализированной архитектуры/проекта сетевой безопасности;

- документацию требований (безопасности) доступа к услугам для каждой системы шлюза

безопасности/межсетевого экрана [включающую в себя базу(ы) правил межсетевого экрана];

- операционные процедуры безопасности;

- условия безопасного сетевого соединения для сторонних организаций (при необходимости);

- руководства пользователей для сторонних пользователей, при необходимости.

Документирование специализированной архитектуры/проекта сетевой безопасности подробно рассмотрено в ИСО/МЭК 27033-2, приложение D которого также включает в себя типовой образец документации, содержащей требования (безопасности) доступа к услугам. Дальнейшую информацию (2-4 дефис выходной информации процесса проектирования) можно найти в 8.2.2 и ИСО/МЭК 27033-2.

Кроме того, после того как необходимая специализированная архитектура/проект сетевой безопасности документально оформлена и реализована, должны быть разработаны планы тестирования безопасности и проведено тестирование. При получении приемлемых результатов тестирования с любыми корректировками, осуществленными с учетом обнаруженных во время тестирования проблем, должно быть получено формальное одобрение руководством специализированной архитектуры/проекта сетевой безопасности и одобрение завершения реализации (см. раздел 12).

Информация о каждом из следующих видов деятельности представлена в ИСО/МЭК 27033-2 (и потому не приводится):

- подготовка к техническому проектированию и реализации сетевой безопасности:

инициирование проекта об обеспечения сетевой безопасности,

подтверждение общих сетевых требований организации/сообщества,

проверка существующей и (или) планируемой специализированной архитектуры и реализации. [Все существующие и (или) планируемые специализированные архитектуры и реализации должны быть описаны и проведены проверки их согласования с функциональными требованиями и потребностями организации/сообщества - см. предыдущее перечисление],

идентификация/утверждение активов,

подтверждение результатов оценки риска безопасности и проводимой руководством проверки, проверка в контексте этих результатов существующих и (или) планируемых мер и средств контроля и управления сетевой безопасностью и выбор потенциальных меры и средства контроля и управления безопасностью,

проверка требований функционирования сети и подтверждение критериев [должны быть проверены требования функционирования, решены спорные вопросы и формально согласованы критерии функционирования, которым должны удовлетворять специализированная архитектура и связанная(ый) с ней специализированная(ый) архитектура/проект сетевой безопасности. Соответственно требуются данные, позволяющие идентифицировать конфигурации линий связи, серверов, шлюзов безопасности и т.д., которые обеспечат требуемую доступность услуг];

- специализированный проект сетевой безопасности, охватывающий все применимые технические вопросы (рассматриваемые в соответствии с заголовками в ИСО/МЭК 27001:2007) и:

использование руководств по сетевым "сценариям" и "технологиям" (которые представлены в ИСО/МЭК 27033-3 - ИСО/МЭК 27033-6) (см. также разделы 10 и 11),

использование моделей/структур (включая ITU-T X.805 и др.),

выбор продуктов [который должен проводиться как итеративный процесс не изолированно, а в связи с разработкой специализированной архитектуры сетевой безопасности, основываясь на многих факторах (включая техническую пригодность, качество функционирования, расширяемость, средства управления, логическую безопасность и, конечно, возможности поставщиков, их репутацию и т.д.)],

подтверждение концепции [осуществление проверки концепции рекомендуется в случаях, если специализированная архитектура сетевой безопасности и связанная с ней совокупность продуктов не были подготовлены заранее и (или) предусматривается сложный набор услуг (не следует забывать о том, что продукты не всегда соответствуют предоставляемым поставщиком данным)],

завершение разработки специализированной архитектуры/проекта сетевой безопасности и связанной с ней документации,

- подготовка к тестированию (должна быть разработана документация стратегии тестирования безопасности, описывающая предпринимаемый подход тестирования для проверки специализированной архитектуры сетевой безопасности, главным образом направленная на то, как должны тестироваться основные технические меры и средства контроля и управления безопасностью. Затем для специализированной архитектуры сетевой безопасности должен быть разработан план тестирования, охватывающий больше подробностей, включая виды проводимого тестирования, кем и каким образом они должны проводиться);

- формальное одобрение специализированной архитектуры сетевой безопасности.

Общие принципы проектирования [применяемые в большинстве (если не во всех) случаев] приведены в ИСО/МЭК 27033-2. Кроме того, следует упомянуть о приложениях ИСО/МЭК 27033-2 - примерной модели/системе <1> ("типовой" архитектуре) сетевой безопасности, разборе конкретного случая модели/системы и типовых образцов документации.

<1> В контексте ИСО/МЭК 27033 использована для представления или описания модели/системы показанной структуры и высокоуровневой разработки вида архитектуры/проекта безопасности, реализуемой техническим способом.

Следует подчеркнуть, что должно быть проведено полное документирование и согласование специализированной архитектуры/проекта безопасности для любого проекта перед окончательным оформлением списка мер и средств контроля и управления безопасностью для реализации.

10. Типовые сетевые сценарии - риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления

10.1. Введение

Описание рисков, методов проектирования и вопросов, касающиеся мер и средств контроля и управления, связанных с типовыми сетевыми сценариями, приведены в ИСО/МЭК

27033-3. Некоторые примеры этих сценариев приведены в 10.2 - 10.10. В ИСО/МЭК 27033-3 предоставлены подробные рекомендации по рискам безопасности, методам проектирования безопасности и мерам и средствам контроля и управления, необходимым для уменьшения последствий этих рисков во всех конкретных сценариях. Там, где это необходимо, в ИСО/МЭК 27033-3 даны ссылки на ИСО/МЭК 27033-4 - ИСО/МЭК 27033-7, чтобы избежать дублирования содержания этих стандартов.

10.2. Услуги доступа сотрудников в Интернет

Практически все организации сегодня предоставляют услуги доступа своих сотрудников в Интернет и, предоставляя такие услуги, должны рассматривать вопрос доступа для четко идентифицированных и санкционированных целей, а не в общий открытый доступ. В конкретной политике должно быть определено, какие услуги предоставляются и для каких целей. Доступ в Интернет обычно разрешается в интересах организации, а в зависимости от политики организации может также разрешаться (обычно в ограниченной форме) для частных целей. Необходимо учитывать, какие услуги разрешено использовать - разрешены ли базовые услуги, например, услуги www (http & https), разрешен ли только поиск информации и (или) сотрудников, разрешено ли участвовать в чате, форумах и т.д., разрешены ли расширенные услуги совместной работы, - если да, то они вносят собственную совокупность рисков, которые рассматриваются в рамках конкретного сценария.

Базовым принципом должен быть принцип, разрешающий только те услуги, которые служат потребностям организации, но часто операции основной деятельности организации требуют использования услуг, в большей степени связанных с рисками безопасности. Даже при наличии ограничительной политики услуги доступа в Интернет для сотрудников вносят существенные риски безопасности.

10.3. Расширенные услуги совместной работы

Расширенные услуги совместной работы (такие, например, как мгновенный обмен сообщениями - чат, видеоконференции и среды коллективного использования документов), объединяющие различные возможности связи и коллективного использования документов, становятся все более значимыми в современной среде основной деятельности организации. Услуги совместной работы обычно объединяют видеотелефонию, телефонную связь с чат-каналами, системы электронной почты, а также среды коллективного использования документов и вспомогательные службы, работающие в режиме on-line. Существуют следующие основные способы использования таких услуг организацией:

- исключительно как внутренние услуги, но недостаток этого способа состоит в том, что услуги не могут быть использованы совместно с внешними партнерами и т.д.;

- как внутренние услуги и услуги, являющиеся внешними для организации. Использование таких услуг предлагает гораздо больше преимуществ, но в то же время с ним связано больше рисков безопасности по сравнению с исключительно внутренним использованием.

Услуги могут быть реализованы внутренними силами организации или приобретены у сторонней организации. В тех случаях, когда услуги используются только для внутренних целей, наиболее вероятной будет их реализация внутренними силами организации. Если услуги будут использоваться внутри и вне организации, то более приемлемым решением может стать приобретение услуг совместной работы у сторонней организации. Риски безопасности и рекомендации по методам проектирования безопасности и мерам и средствам контроля и управления безопасностью для уменьшения этих рисков описываются как для внутреннего, так и для внутреннего и внешнего использования.

10.4. Услуги "бизнес - бизнес"

Традиционно услуги "бизнес - бизнес" реализовывались путем использования выделенных линий или сегментов сети. Интернет и связанные с ним технологии предоставляют больше вариантов использования, но также вносят новые риски безопасности, связанные с реализацией таких услуг. Обычно услуги "бизнес - бизнес" предполагают собственные требования к ним. Например, очень важны требования доступности и достоверности, так как организации часто напрямую зависят от функционирования услуг "бизнес - бизнес".

Если в качестве основного сетевого соединения для реализации услуг "бизнес - бизнес" используется Интернет, то с такими требованиями, как доступность и достоверность, следует обращаться иначе, чем раньше. Испытанные меры, такие как используемые предположения о качестве услуг, например в соединении по выделенным линиям, в этих условиях уже не работоспособны. Новые риски безопасности необходимо снижать с помощью соответствующих методов проектирования и мер и средств контроля и управления.

10.5. Услуги "бизнес - клиент"

В услуги "бизнес - клиент" входят электронные торговля и банковские услуги. Их требования включают в себя конфиденциальность (особенно в отношении электронных банковских услуг), аутентификацию [возможными сейчас способами (например, двухфакторную, на базе сертификатов и т.д., основанную на взаимосвязи между затратами на реализацию), обычно высокими по причине очень большого числа клиентов и снижением рисков, таких как финансовые потери, потеря репутации/доверия к деятельности организации], целостность и стойкость к изощренным атакам, таким как "атакующий посередине" или "атакующий в браузере".

Характеристики услуги "бизнес - клиент" включают в себя:

- безопасность; "гарантируется" только на конечной платформе, обычно находящейся под контролем организации, обеспечивающей надежную среду для реализации мер и средств контроля и управления и поддержки достаточной безопасности на уровне платформы;

- безопасность на платформе клиента (обычно ПК); может быть недостаточной. В такой среде труднее достичь реализации мер и средств контроля и управления, поэтому платформы клиентов будут представлять значительные риски в этом сценарии (без совокупности требований "условия обеспечения безопасного соединения" зафиксированные в договоре, которые может быть трудно установить в такой среде).

10.6. Услуги аутсорсинга

Из-за сложности современных ИТ-сред многие организации используют предоставляемые внешним образом услуги ИТ-поддержки или полностью/частично передают сторонним подрядчикам поддержку своей ИТ-инфраструктуры и (или) используют другие услуги, предоставляемые с привлечением внешних ресурсов. У многих поставщиков также имеется необходимость прямого доступа к своим продуктам, используемым организациями-клиентами с тем, чтобы иметь возможность соответствующим образом справляться с вопросами поддержки и (или) менеджмента инцидентов.

В то время как многие услуги, осуществляемые с привлечением внешних ресурсов, требуют прав постоянного доступа, например, к поддерживаемой инфраструктуре, другие услуги могут потребовать только временного доступа. В некоторых случаях услуги, осуществляемые с привлечением внешних ресурсов, нуждаются в правах доступа с высоким уровнем привилегированности для того, чтобы выполнять необходимые задачи, особенно в сценариях

менеджмента инцидентов.

10.7. Сегментация сети

Для многих организаций, особенно транснациональных, характерные для разных стран законы оказывают огромное влияние на требования информационной безопасности. Международные организации обычно осуществляют свою деятельность в ряде стран и, соответственно, обязаны соблюдать законы, действующие в разных странах, результатом чего может возникнуть различие в требованиях информационной безопасности в зависимости от страны, в которой функционирует организация. Например, законы конкретной страны могут конкретной определенной защиты данных потребителей/клиентов и не разрешать передачу таких данных в другую страну. Различие в законодательстве разных стран обычно требует дополнительных мер и средств контроля и управления информационной безопасностью.

Для выполнения различных требований информационной безопасности тех стран, где международная организация осуществляет свою деятельность, эффективным общим решением может стать сегментация сети, фактически совпадающая с границами стран. Во многих случаях такое общее решение может использоваться для создания отдельного защитного барьера в дополнение, например, к управлению доступом на прикладном уровне.

10.8. Мобильная связь

Этот типовой сетевой сценарий относится к персональным устройствам мобильной связи, например, смартфонам или КПК, которые становятся очень популярными (руководство по аспектам безопасности связи через сети с такими устройствами представлено в ИСО/МЭК 27033-7, в котором рассматривается обеспечение безопасности связи через беспроводные сети и радиосети).

Несмотря на то, что быстрое развитие новых свойств персональных устройств мобильной связи наблюдается на потребительском рынке, эти свойства используются также в основной деятельности организаций. Согласно определению термина "персональный", эти устройства часто находятся в личной собственности и используются как организациями, так и в личных целях. Даже устройства, предназначенные для делового рынка, должны иметь введенные для потребительского рынка свойства, так как поставщики хотят добиться как можно большего расширения коммерческой деятельности на конкурентном рынке.

Многие из новых свойств устройств, которые становятся доступными при их использовании, например, увеличение объема памяти и общедоступная постоянная возможность связи через Интернет, предполагают как существенные риски информационной безопасности, так и ситуации, когда человек использует одно и то же устройство для частных целей и для целей организации.

Кроме того, при большой популярности персональных устройств мобильной связи и их статуса "персональной технической новинки" ограничительные политики, направленные на использование только ограниченного набора свойств или на разрешение только ограниченного числа устройств, во многих случаях потерпят неудачу или будут обойдены, что приведет к снижению эффективности обеспечения информационной безопасности.

10.9. Сетевая поддержка для пользователей, находящихся в разъездах

Пользователи, находящиеся в разъездах, ожидают в настоящее время возможностей связи, сравнимой со связью на стационарном объекте, как, например, в основном офисе. Решения и предложения в этой области часто сосредотачиваются на функциональных возможностях. С точки зрения информационной безопасности предлагаемые уровни функциональных возможностей вносят новые риски, например, оказывая влияние на ожидания, связанные с информационной безопасностью, или делая их несостоятельными. Например, ожидание поддержки хорошо управляемого и защищенного (извне) Интранета может в значительной степени ставиться под сомнение, если доступ находящегося в разъездах пользователя Интранета не реализован с применением соответствующих мер и средств контроля и управления.

10.10. Сетевая поддержка домашних офисов и офисов малых предприятий

Домашние офисы и офисы малых предприятий часто требуют расширения внутренней сети организации для их охвата. Критичным вопросом является стоимость расширения внутренней сети с целью охвата домашних офисов или офисов малых предприятий, поскольку для отображения соотношения "затраты/выгоды" обычно не требуется высоких затрат на реализацию. Это означает стоимостные ограничения на меры и средства контроля и управления безопасностью, которые должны использоваться для защиты такого расширения сети, и обычно препятствуют использованию признанных мер и средств контроля и управления безопасностью межсетевого взаимодействия, используемых для соединения больших сегментов Интранета.

Во многих сценариях, связанных с домашними офисами или офисами малых предприятий, инфраструктура может также использоваться для частных целей и целей деятельности организации, что может привести к дополнительным рискам информационной безопасности. Для таких сценариев определяются риски безопасности и описываются рекомендации по методам проектирования безопасности и мерам и средствам контроля и управления для снижения этих рисков.

11. Аспекты "технологии" - риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления

Подробности, касающиеся рисков безопасности, методов проектирования и вопросов мер и средств контроля и управления, связанных с аспектами "технологии", представлены в Приложении А и охватывают следующие темы:

- локальные вычислительные сети (см. А.1, Приложение А);

- глобальные вычислительные сети (см. А.2, Приложение А);

- беспроводные сети (см. А.3, Приложение А);

- радиосети (см. А.4, Приложение А);

- широкополосные сети (см. А.5, Приложение А);

- шлюзы безопасности (см. А.6, Приложение А);

- виртуальные частные сети (см. А.7, Приложение А);

- сети телефонной связи (см. А.8, Приложение А);

- IP-конвергенция (см. А.9, Приложение А);

- размещение информации на сервере веб-узлов (см. А.10, Приложение А);

- электронная почта в Интернете (см. А.11, Приложение А);

- маршрутизированный доступ к сторонним организациям (см. А.12, Приложение А);

- центр обработки и хранения данных (см. А.13, Приложение А).

12. Разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности

После того как специализированная архитектура безопасности полностью документально оформлена и согласована, включая одобрение высшего руководства, должен быть разработан комплекс программных и технических средств и услуг по обеспечению безопасности, который должен быть реализован в "экспериментальном режиме", тщательно протестирован, и должна быть проведена проверка его соответствия.

Общая проверка комплекса программных и технических средств и услуг на "соответствие назначению" должна проводиться в соответствии с документацией по стратегии тестирования, описывающей метод тестирования и позволяющей испытывать комплекс программных и технических средств и услуг, и планом тестирования. В результате идентификации недостатков в ходе такого тестирования могут потребоваться внесение изменения и проведение любого необходимого повторного тестирования.

После того как тестирование на "соответствие назначению" успешно проведено и осуществлены какие-либо необходимые изменения, должна быть проведена проверка реализации на предмет соответствия документированной специализированной архитектуры безопасности необходимым мерам и средствам контроля и управления безопасностью, определенным в следующих документах:

- специализированная архитектура безопасности;

- политика сетевой безопасности;

- документы, связанные с SecOPs;

- политика (безопасности) доступа к услуге шлюза безопасности;

- план(ы) обеспечения непрерывности деятельности;

- условия обеспечения безопасности соединения (при необходимости).

Проверка соответствия комплекса программных и технических средств и услуг должна проводиться до начала фактического функционирования. Проверка комплекса программных и технических средств и услуг будет завершена, когда все недостатки идентифицированы, исправлены и признаны высшим руководством.

Следует подчеркнуть, что проверка соответствия комплекса программных и технических средств и услуг должна включать в себя проведение тестирования безопасности по соответствующим национальным стандартам, стандартам организации (в отсутствие национальных стандартов) в соответствии с заранее разработанной стратегией тестирования безопасности и связанными с ней планами тестирования безопасности, точно определяющими, какое тестирование должно проводиться, с помощью чего, где и когда (примерный образец плана тестирования безопасности приведен в ИСО/МЭК 27033-2). Обычно тестирование должно

сочетать в себе поиск уязвимостей и тестирование на проникновение. Перед началом любого такого тестирования необходимо проверить план тестирования с тем, чтобы обеспечить уверенность в проведении тестирования в полном соответствии с релевантными законодательством и инструкциями. При проведении этой проверки не следует забывать о том, что сеть может не ограничиваться одной страной, а распространяться на другие страны с различными законодательствами. После проведения тестирования в отчетах должны указываться особенности обнаруженных уязвимостей, необходимые меры по их устранению, и приоритет их принятия, а в приложении должно подтверждаться, что все согласованные меры по их устранению применены. Такие отчеты должны быть подписаны высшим руководством организации.

Наконец, когда все результаты будут признаны удовлетворительными, реализация должна быть одобрена и принята, включая одобрение высшего руководства организации.

13. Реализация комплекса программных и технических средств и услуг по обеспечению безопасности

Понятие "реализация" означает (повседневное) функционирование действующей сети с применением согласованного комплекса программных и технических средств и услуг по обеспечению безопасности, результатов проведенного тестирования безопасности и связанными с ним заблаговременно выполненными необходимыми действиями. Другими словами, после того как специализированная архитектура безопасности и, соответственно, реализация мер и средств контроля и управления безопасностью одобрены, должны начаться фактические операции. С течением времени и в случае существенных изменений должны быть проведены дополнительная проверка и тестирование реализации (см. также раздел 14).

14. Мониторинг и проверка эксплуатации комплекса программных и технических средств и услуг

После начала эксплуатации должны проводиться действия по текущему мониторингу и проверке соответствия требованиям национальных стандартов, стандартов организации (при отсутствии национальных стандартов). Такие мероприятия должны проводиться ежегодно до появления новой основной версии (комплекса программных и технических средств и услуг), связанной со значительными изменениями потребностей деятельности организации, технологии, решений по обеспечению безопасности и т.д. При этом также необходимо соблюдать рекомендации раздела 12.

Приложение А
(справочное)

АСПЕКТЫ "ТЕХНОЛОГИИ" - РИСКИ, МЕТОДЫ ПРОЕКТИРОВАНИЯ И ВОПРОСЫ, КАСАЮЩИЕСЯ МЕР И СРЕДСТВ КОНТРОЛЯ И УПРАВЛЕНИЯ

А.1. Локальные вычислительные сети

А.1.1. Вводная информация

ЛВС представляет собой сеть для соединения компьютеров и серверов на небольшом географическом пространстве. Размеры сети варьируются от нескольких связанных систем,

например формирующих домашнюю сеть, до нескольких тысяч систем, например, в сети университетского городка. Обычные реализуемые услуги включают в себя коллективное использование ресурсов, таких как принтер, и совместное использование файлов и приложений. Обычно ЛВС также обеспечивают централизованные услуги, подобные обмену сообщениями или электронному календарю. В некоторых случаях ЛВС также используются для замены традиционной функции других сетей, например, если протоколы и сервисы передачи речи по IP предоставляются в качестве замены телефонной сети на основе офисной АТС. ЛВС могут иметь проводную или беспроводную основу.

Проводные ЛВС обычно состоят из узлов, соединенных в сеть через сетевой коммутатор посредством сетевых кабелей, способных обеспечивать возможности высокоскоростной передачи данных. Наиболее широко применяемой технологией проводных ЛВС является Ethernet (IEEE 802.3).

Беспроводные ЛВС используют радиоволны высокой частоты для передачи сетевых пакетов. Их гибкость заключается в быстроте организации локальной сети без необходимости прокладки проводов. Широко известные технологии беспроводных ЛВС включают в себя реализации IEEE 802.11 и Bluetooth.

При использовании ЛВС в пределах физически защищенных областей, например, только в пределах собственных помещений организации, риски, вероятно, будут таковы, что потребуются только базовые технические меры и средства контроля и управления. Однако в случае использования ЛВС в более широкой среде, а также при использовании беспроводных технологий одна только физическая защита вряд ли будет гарантировать достаточный уровень безопасности.

Настольный компьютер представляет собой уязвимую область, так как является пользовательским интерфейсом. Если настольный компьютер не блокируется, существует вероятность установки пользователем несанкционированного программного обеспечения в ЛВС. Серверы, используемые в корпоративной сети, предназначенные для Интернета, и внутренние серверы, не имеющие непосредственного соединения с Интернетом, могут служить источником существенных рисков безопасности, к которым необходимо относиться очень серьезно. Например, несмотря на то, что большинство сотрудников ИТ-отделов утверждает, что они внимательно относятся к осуществлению исправлений в используемом организацией программном обеспечении, даже крупным организациям не удавалось своевременно осуществить такие исправления программного обеспечения на всех серверах, что приводило к разрушению внутреннего сетевого трафика "червями" и вирусами.

А.1.2. Риски безопасности

В проводных ЛВС риски безопасности создаются узлами, физически соединенными с сетью. В общем, основные риски безопасности, имеющие отношение к ЛВС, включают в себя риски, связанные с:

- несанкционированным доступом и изменениями, вносимыми в ПК, серверы и другие соединенные с ЛВС устройства;

- устройствами, в которых не осуществлены исправления программного обеспечения;

- паролями низкого качества;

- хищением аппаратных средств;

- нарушениями энергоснабжения;

- импортом вредоносной программы через электронную почту и доступ к веб-страницам;

- неудачным резервным копированием локальных жестких дисков;

- отказом аппаратных средств, таких, например, как жесткие диски;

- несанкционированными соединениями с инфраструктурой ЛВС, например, коммутаторами и коммутационными стойками;

- несанкционированными соединениями с выходными устройствами, например дорожными компьютерами;

- паролями по умолчанию на портах управления сетевых устройств;

- вторжениями, при которых происходит раскрытие информации или при которых в дальнейшем не могут быть гарантированы целостность и (или) доступность данных;

- DoS-атаками, когда ресурсы становятся недоступными для уполномоченных пользователей;

- длительным запаздыванием, которое будет оказывать влияние на передачу речи через IP сервисы;

- сбоем устройств;

- повреждением кабеля;

- недостаточной физической защитой.

Риски безопасности, связанные с беспроводными ЛВС, представлены в А.3.2.

А.1.3. Меры и средства контроля и управления безопасностью

Поддержание безопасности пространства ЛВС требует обеспечения защиты компонентов ЛВС и подсоединенных устройств. Таким образом, меры и средства контроля и управления для защиты среды ЛВС могут включать в себя:

- физические меры и средства контроля и управления безопасностью и меры и средства контроля и управления безопасностью, связанные с влиянием среды:

использование систем стальных тросов для защиты центральных процессоров, мониторов и клавиатур от хищения,

использование замков на устройствах для предотвращения хищения таких частей, как запоминающие устройства,

использование устройств неконтактного действия для предотвращения несанкционированного выноса оборудования с территории организации,

обеспечение хранения устройств ЛВС, таких как коммутаторы и маршрутизаторы, в физически защищенных шкафах в безопасных помещениях связи,

использование ИБП с автоматическим отключением для критических устройств и ПК пользователей, если пользователи не хотят потерять результаты выполняемой работы;

- аппаратные и программные меры и средства контроля и управления безопасностью:

конфигурирование устройств с частными (например, IP) адресами,

строгая политика паролей,

требование регистрации на каждом ПК/рабочей станции с использованием, по крайней мере, пары идентификатор пользователя/пароль,

отображение времени последней успешной регистрации,

запрет повторного отображения имени пользователя в последней успешной регистрации или любого списка ранее использованных имен пользователей,

установка программных средств защиты от вредоносной программы (включая антивирусные программные средства) и регулярное автоматическое их обновление,

реализация безопасных установок конфигурации,

блокировка дисковода для жестких дисков, дисковода для компакт-дисков и портов универсальной последовательной шины,

зеркальное копирование накопителей сервера (или реализация матрицы независимых дисковых накопителей с избыточностью) для обеспечения избыточности,

удаление ненужного программного обеспечения,

обеспечение обоснованного управления интерактивной средой;

- операционные меры и средства контроля и управления безопасностью:

документирование установок программного обеспечения и безопасности для использования в будущем при конфигурировании новых ПК/рабочих станций,

планирование периодического получения и осуществления исправлений программного обеспечения для операционной системы,

создание и поддержка текущих дисков аварийного восстановления и хранение их в контролируемом месте,

реализация протокола для фиксирования проблем технического обслуживания и ненадлежащего использования ПК/рабочих станций,

хранение в архиве всей документации компонентов ПК/рабочей станции (документы/руководства/диски) для использования специалистами по обслуживанию оборудования,

обеспечение режима резервного копирования,

обеспечение изменения паролей по умолчанию на всех сетевых устройствах,

простановка соответствующих имен сообщества/паролей в протоколе сетевого менеджмента,

шифрование сетевого трафика,

надлежащее конфигурирование (в случае доступности) контрольных журналов и реализация процедур их мониторинга,

планирование периодической установки обновленных версий встроенных программ,

документирование настройки оборудования для использования в будущем при повторном его конфигурировании; создание резервной копии конфигурационного файла маршрутизатора и хранение его в безопасном месте,

тестирование всех подсоединенных к локальной вычислительной сети устройств на предмет наличия уязвимостей.

Меры и средства контроля и управления безопасностью, связанные с беспроводными локальными вычислительными сетями, представлены в А.3.3.

А.2. Глобальные вычислительные сети

А.2.1. Вводная информация

ГВС используются для соединения удаленных пунктов и их ЛВС. ГВС могут быть созданы с использованием кабелей и каналов связи провайдера услуг или посредством аренды услуги у провайдера сетей связи. Технологии ГВС дают возможность передачи и маршрутизации сетевого трафика на большие расстояния и обычно обеспечивают широкие возможности маршрутизации для направления сетевых пакетов в ЛВС нужного пункта назначения. Обычно для связи между ЛВС используется физическая общедоступная сетевая инфраструктура, например, выделенные линии, спутниковая связь, или волоконно-оптические кабели. ГВС могут иметь проводную или беспроводную основу.

Проводные ГВС обычно состоят из устройств маршрутизации (например, маршрутизаторов), соединенных с общедоступной или частной сетью телекоммуникационными кабелями. Беспроводные ГВС обычно используют радиоволны для передачи сетевых пакетов на большие расстояния - 10 километров и более.

Хотя традиционные ГВС были первоначально созданы с использованием арендуемых у провайдеров стационарных (магистральных) линий связи, причем провайдер услуг выполнял минимальную управленческую деятельность, связанную с этими линиями связи, помимо обеспечения их функционирования, развитие технологии ГВС привело к перекладыванию ответственности за управление на провайдера услуг, что принесло организациям выгоду, заключающуюся в отсутствии необходимости развертывания собственной сети и управления ею, то есть ответственность в обеспечении уверенности в безопасности менеджмента сети возлагается на провайдера услуг. Кроме того, поскольку ГВС главным образом используются для направления сетевого трафика на большие расстояния, функция маршрутизации должна быть хорошо защищена для обеспечения того, чтобы сетевой трафик не был направлен в ЛВС, представляющую неверный пункт назначения. Поэтому проходящий через ГВС трафик может подвергаться перехвату лицами, имеющими доступ к инфраструктуре ГВС. Поскольку инфраструктура ГВС, по-видимому, более доступна, чем инфраструктура ЛВС, следует соблюдать осторожность, обеспечивая шифрование передаваемой через среду ГВС значимой информации. В договоре с провайдером услуг должен быть оговорен уровень безопасности, необходимый организации, который должен продемонстрировать провайдер.

А.2.2. Риски безопасности

Хотя проводные ГВС разделяют основные риски безопасности с проводными ЛВС (см. А.1), у проводной ГВС существует больше рисков безопасности вследствие более значительной

подверженности риску сетевого трафика в ГВС, что означает необходимость наличия мер и средств контроля и управления, включая средства управления доступом, для обеспечения того, чтобы проводную ГВС было нелегко скомпрометировать, вызывая тем самым широко распространяющееся нарушение. Аналогично, хотя беспроводные ГВС разделяют основные риски безопасности с беспроводной ЛВС (см. А.3), они более подвержены нарушениям из-за возможностей преднамеренных помех в системе, используемой для передачи сетевых пакетов. В целом, к основным рискам безопасности, имеющим отношение к ГВС, относятся риски, связанные с:

- вторжением, при котором происходит раскрытие информации или не могут быть гарантированы целостность и (или) доступность данных;

- DoS-атаками, когда ресурсы становятся недоступными для авторизованных пользователей;

- длительным запаздыванием, которое будет оказывать влияние на такие услуги, как передача речи через IP сервисы;

- неустойчивой синхронизацией в сети, которая будет оказывать влияние на качество передачи речи (вызываемой главным образом использованием медных кабелей для поставки услуг);

- сбоем устройств;

- повреждением кабеля;

- устройствами с неосуществленными исправлениями программного обеспечения;

- потерей электроснабжения на транзитной площадке, затрагивающей многие другие риски;

- средствами сетевого менеджмента провайдера услуг.

А.2.3. Меры и средства контроля и управления безопасностью

Основные меры и средства контроля и управления безопасностью, необходимые для обеспечения защиты ГВС, должны включать в себя:

- использование безопасных протоколов управления, таких как SSH, SCP или SNMPv3;

- шифрование каналов управления;

- шифрование сетевого трафика;

- реализацию безопасной аутентификации для получения доступа к устройствам ГВС с соответствующей подачей сигнализации для устройств;

- обеспечение безопасности физического оборудования ГВС на каждой площадке, например, использование запираемых шкафов с сигнализацией доступа;

- использование ИБП для обеспечения защиты от нарушения энергоснабжения;

- двойное соединение узлов сети/связи с использованием разных маршрутов;

- профилактический последовательный опрос устройств ГВС;

- составление схемы размещения сетевых устройств для идентификации несанкционированных устройств;

- менеджмент осуществления исправлений программного обеспечения;

- шифрованные оверлеи для значимых данных;

- получение от провайдера услуг гарантий предоставления услуг по таким вопросам, как доступность, запаздывание и неустойчивая синхронизация;

- реализацию процесса аудита и ведения учета сетевых ресурсов для доступа к устройствам ГВС;

- использование межсетевых экранов, отвергающих любой неожиданный входящий трафик;

- обеспечение уверенности в том, что инфраструктура и адреса являются скрытыми;

- присвоение IP-адресов, которые не могут быть маршрутизированы через Интернет;

- использование программных средств для того, чтобы помешать вредоносному программному обеспечению ("троянские кони", вирусы, шпионское ПО и черви) открывать лазейки в безопасности изнутри сети;

- использование систем обнаружения вторжений для идентификации подозрительного трафика;

- обеспечение логической безопасности систем сетевого менеджмента;

- внеполосный сетевой менеджмент;

- обеспечение физической безопасности мест управления сетью;

- обеспечение резервного копирования устройств;

- проведение проверок надежности персонала, занимающегося сетевым менеджментом.

А.3. Беспроводные сети

А.3.1. Вводная информация

Беспроводные сети определяют как "сети, охватывающие небольшие в географическом отношении области и использующие беспроводные средства связи, такие как радиоволны или инфракрасные волны". Обычно беспроводные сети используют для реализации связности, эквивалентной той, что обеспечивается в ЛВС, и поэтому их также называют "беспроводной локальной вычислительной сетью" (WLAN). Основные используемые технологии стандартизированы в IEEE 802.11 и Bluetooth. Следует подчеркнуть, что беспроводные сети составляют категорию сетей, отличную от радиосетей, таких как GSM, 3G и ОВЧ, так как радиосети используют антенные мачты для передачи (см. А.4). Кроме того, рассматривая беспроводные сети, следует принимать в расчет инфракрасные соединения или любой другой вид соединений, поддерживающих беспроводные сети.

WLAN подвержены всем уязвимостям проводных ЛВС и, вдобавок, от некоторых особых уязвимостей, связанных с характеристиками беспроводной связи. Для рассмотрения этих дополнительных уязвимостей были разработаны некоторые специфические технологии

(главным образом основанные на шифровании), хотя у более ранних версий этих технологий (например, WEP) имелись слабые места в архитектуре, и поэтому они не отвечали ожиданиям в отношении требований конфиденциальности.

А.3.2. Риски безопасности

Основные риски безопасности, имеющие отношение к использованию WLAN, включают в себя риски, связанные с:

- подслушиванием;

- несанкционированным доступом;

- взаимными и преднамеренными помехами;

- неправильной конфигурацией;

- отключением по умолчанию безопасного режима доступа;

- небезопасными протоколами шифрования;

- небезопасными протоколами управления, используемыми для управления WLAN;

- не всегда существующей возможностью идентифицировать пользователей WLAN;

- неисправными устройствами (например, в точках доступа).

А.3.3. Меры и средства контроля и управления безопасностью

Меры и средства контроля и управления, необходимые для WLAN, могут включать в себя:

- конфигурирование инфраструктуры с соответствующими техническими мерами безопасности (включая, например, организацию межсетевой защиты WLAN от корпоративной инфраструктуры);

- шифрование связи и данных при обмене, например, путем реализации виртуальной частной сети на основе IPsec через WLAN между клиентом и межсетевым экраном периметра;

- рассмотрение вопроса повышения безопасности каждого устройства WLAN путем конфигурирования персональных межсетевых экранов, программных средств обнаружения вторжений и защиты от вредоносной программы (включая антивирусы), установленных на клиентском устройстве;

- использование аутентификации;

- контроль уровня передаваемого сигнала для исключения распространения за пределы физической территории организации;

- конфигурирование простого протокола сетевого управления (SNMP) доступом только для чтения;

- сбор и анализ журналов регистрации с целью обнаружения любого искажения или несанкционированного использования;

- управление сетью по дополнительному шифрованному каналу, например, с

использованием SSH;

- поддержку физической безопасности точек беспроводного доступа;

- повышение прочности любых сетевых элементов;

- тестирование системы;

- рассмотрение использования системы обнаружения вторжений между корпоративной и беспроводной сетями.

А.4. Радиосети

А.4.1. Вводная информация

Радиосети определяют как "сети, использующие радиоволны в качестве средства связи для охвата географически обширных областей". Типичными примерами радиосетей являются сети сотовой связи, использующие такие технологии, как GSM или UMTS, и предоставляющие общедоступные сервисы передачи речи и данных.

Следует подчеркнуть, что сети, использующие радиоволны для охвата небольших областей, считают относящимися к другой категории и приведены в А.3.

К радиосетям, например, относятся:

- TETRA;

- GSM;

- 3G (включая UMTS);

- GPRS;

- CDPD;

- CDMA.

А.4.2. Риски безопасности

Основные риски безопасности, имеющие отношение к использованию радиосетей, в целом включают риски, связанные с:

- подслушиванием;

- перехватом сеанса связи;

- представлением себя другим лицом;

- угрозами прикладного уровня, например, мошенничеством;

- отказом в обслуживании.

Риски безопасности, имеющие отношение к GSM, включают в себя риски, связанные с тем фактом, что:

- Comp128-1 и алгоритмы A5/x являются слабыми;

Примечание. Запатентованный алгоритм, первоначально использовался по умолчанию в SIM-картах.

- GSM шифрование, как правило, обычно отключено;

- клонирование SIM-карт является реальностью.

Риски безопасности, имеющие отношение к 3G, включают в себя риски того, что:

- телефоны уязвимы для электронных атак, включая внесение вредоносной программы, например, вирусов;

- возможности атак высоки, так как телефоны зачастую включены;

- услуги могут стать объектами подслушивания;

- в радиосетях могут быть преднамеренные помехи;

- возможно введение ложных базовых станций;

- шлюзы могут подвергаться несанкционированному доступу;

- услуги могут подвергаться атакам и несанкционированному доступу через Интернет;

- возможно внесение спама;

- системы управления могут подвергаться несанкционированному доступу через RAS;

- услуги могут подвергаться атакам посредством потерянного или похищенного оборудования инженерно-технической помощи, включая портативные компьютеры.

UMTS является основным представителем глобального семейства технологий мобильной связи третьего поколения (3G) и предоставляет существенные возможности широкополосной передачи и пропускной способности для поддержки передачи данных и речи большому числу клиентов. UMTS использует несущую полосу частот 5 МГц для достижения значительно более высоких скоростей передачи данных и увеличения пропускной способности, обеспечивая оптимальное использование радиоресурсов, особенно для операторов с широкими смежными участками спектра, обычно от 2 x 10 до 2 x 20 МГц, для снижения расходов на развертывание 3G сетей. Пакетная радиосвязь общего назначения (GPRS) является существенным шагом вперед к сетям мобильной связи третьего поколения, улучшая функциональные возможности GSM-сети. GPRS - это спецификация передачи данных в GSM-сетях, дающая возможность существования в GSM-инфраструктуре и пакетного трафика и трафика с коммутацией каналов. GPRS использует до восьми 9,05 Кбит или 13,4 Кбит TDMA таймслотов с общей пропускной способностью 72,4 или 107,2 Кбит. GPRS поддерживают протоколы TCP/IP и X.25. GSM-сети с технологией EDGE могут реализовывать EGPRS - улучшенную версию GPRS, которая увеличивает пропускную способность каждого таймслота до 60 Кбит. GPRS делает возможным "постоянно включенное" Интернет-соединение, являющееся потенциальной проблемой безопасности. GPRS-провайдер обычно старается повысить безопасность связи, обеспечивая межсетевой экран между GPRS-сетью и Интернетом, но обеспечение межсетевого экрана должно быть сконфигурировано так, чтобы сделать возможной работу допустимых сервисов, и, следовательно, возможность использования сторонними организациями.

Сотовая цифровая передача пакетов данных (CDPD) представляет собой спецификацию для поддержки беспроводного доступа к Интернету и другим общедоступным сетям с коммутацией пакетов через сотовые телефонные сети. CDPD поддерживает TCP/IP и CLNP. CDPD использует поточный шифр RC4 с 40-битовыми ключами для шифрования. CDPD определена в стандарте IS-732. Алгоритм не является стойким и может быть дешифрован методом грубого прямого подбора.

CDMA - форма расширенного спектра - является семейством методов цифровой связи, который использовался в течение многих лет. Основным принципом расширенного спектра является использование шумоподобных несущих частот, имеющих гораздо бо́льшую ширину полосы пропускания, чем требуется для простой прямой связи при одной и той же скорости передачи данных. Технология цифрового кодирования позволяет CDMA предупреждать намеренное или случайное подслушивание. Технология CDMA разбивает звук на "кусочки", проходящие по расширенному спектру частот. Каждый "кусочек" разговора (или данных) идентифицируется по цифровому коду, известному только CDMA-телефону и базовой станции. Это означает, что фактически никакое другое устройство не может принять звонок. Наличие миллионов кодовых комбинаций, доступных для любого звонка, обеспечивает защиту от подслушивания.

А.4.3. Меры и средства контроля и управления безопасностью

Существует ряд технических мер и средств контроля и управления безопасностью для осуществления менеджмента рисков радиосетей от идентифицированных угроз, включая:

- надежную аутентификацию;

- шифрование с эффективными алгоритмами;

- защищенные базовые станции;

- межсетевые экраны;

- защиту от вредоносной программы (вирусы, "троянские кони" и т.д.);

- антиспам.

А.5. Широкополосные сети

А.5.1. Вводная информация

Широкополосные сети могут брать начало от группы технологий, позволяющих индивидуальным абонентам осуществлять высокоскоростной доступ к точке наличия Интернета. Широкополосные технологии включают в себя, например:

3G;

кабельную (оптическую, коаксиальную);

спутниковую;

xDSL;

FiOS;

BPL;

FTTH.

Что касается xDSL, существуют два основных вида: ADSL, скорость потока которого от пользователя ниже (от четверти до половины скорости потока к пользователю), и SDSL, скорости потоков в которых в обоих направлениях одинаковы. В любом случае скорость потока к пользователю обычно составляет от 128 Кбит/с до 2 - 8 Мбит/с, в зависимости от продукта. Кабельная и спутниковая технологии также имеют сходные виды продукта.

Основные причины выбора широкополосных технологий заключаются в том, что они являются высокоскоростными технологиями постоянного подключения, которые дешевле традиционных систем связи и могут поддерживать приложения, требующие широкой полосы пропускания (например, HDTV требует 15 - 20 Мб при текущей компрессии). Все технологии делают возможным доступ к Интернету и, следовательно, действуют только в диапазоне от Интернета до помещений абонента. Использование Интернета в качестве универсального транспортного средства связи позволяет быстро и дешево организовывать связь, возможно, с развертыванием виртуальной частной сети для безопасных линий связи.

А.5.2. Риски безопасности

Широкополосная связь - это просто высокоскоростная линия связи "постоянного подключения" между абонентом и Интернетом. Эти свойства облегчают хакеру задачу подключения к широкополосной системе связи. К основным рискам безопасности, имеющим отношение к использованию широкополосных сетей, относятся риски, связанные с:

- раскрытием, модификацией или удалением информации в результате несанкционированного удаленного доступа;

- распространением вредоносной программы;

- приемом/передачей и выполнением несанкционированных программ;

- кражей идентификаторов;

- неправильным конфигурированием систем клиента;

- внесением программных уязвимостей;

- перегрузкой сети;

- отказом в обслуживании.

А.5.3. Меры и средства контроля и управления безопасностью

Существует ряд технических мер и средств контроля и управления безопасностью для осуществления менеджмента рисков широкополосной связи от идентифицированных угроз, которые могут включать в себя:

- межсетевые экраны для малого офиса/домашнего офиса;

- шифрование данных;

- программные средства защиты от вредоносной программы (включая антивирусы);

- системы обнаружения вторжений, включая системы предупреждения вторжений;

- виртуальные частные сети;

- обновление версий/осуществление исправлений программного обеспечения.

А.6. Шлюзы безопасности

А.6.1. Вводная информация

Соответствующий механизм шлюза безопасности должен обеспечивать защиту внутренних систем организации и осуществлять безопасные управление и контроль проходящего через него трафика в соответствии с документально оформленной политикой доступа к сервису шлюза безопасности (см. А.6.3).

А.6.2. Риски безопасности

С каждым днем хакеры предпринимают все более изощренные попытки взлома сетей, используемых для целей деятельности организаций, и в центре их внимания находятся шлюзы. Попытки несанкционированного доступа могут быть злонамеренными, ведущими, например, к DoS атаке; атаки могут быть направлены на злоупотребление ресурсами или получение ценной информации. Шлюзы должны защищать организацию от таких вторжений извне, например, из Интернета или сетей сторонней организации. Неконтролируемое, исходящее из организации информационное наполнение, приводит к правовым проблемам и потенциальной потере интеллектуальной собственности. К тому же, по мере того как все больше организаций устанавливают связь с Интернетом для удовлетворения своих организационных потребностей, они сталкиваются с необходимостью контроля доступа к несоответствующим или нежелательным веб-сайтам. Без такого контроля организации рискуют стать непродуктивными, подвергнуться неприятностям и неправильно распределить пропускную способность из-за непродуктивного "блуждания" по веб-сайтам. Таким образом, требующие рассмотрения основные риски безопасности включают в себя риски, связанные с:

- возможностью недоступности соединения с внешним миром;

- повреждением данных;

- несанкционированным раскрытием, которому могут подвергнуться ценные активы организации;

- размещением данных на веб-сайтах или передачей их иным способом без надлежащих полномочий, приводящим к правовым проблемам (например, инсайдерская торговля).

А.6.3. Меры и средства контроля и управления безопасностью

Шлюз безопасности должен:

- разделять логические сети;

- выполнять функции ограничения и анализа информации, проходящей между логическими сетями;

- пользоваться организацией в качестве средства контроля доступа к информации, поступающей в сеть организации и выходящей из нее;

- обеспечивать наличие единственной контролируемой и управляемой точки входа в сеть;

- осуществлять политику безопасности организации относительно сетевых соединений;

- обеспечивать наличие единственной точки регистрации данных.

Для каждого шлюза безопасности должен быть разработан отдельный документ, касающийся политики (безопасности) доступа к услугам, и его требования должны выполняться, чтобы обеспечить прохождение только санкционированного трафика. Этот документ должен содержать набор правил, которые должны применяться к шлюзу и конфигурации шлюза. Должна существовать возможность по отдельности определять разрешенные соединения согласно протоколу связи и другим деталям. Таким образом, для обеспечения уверенности в том, что только санкционированные пользователи и трафик получают разрешение на доступ к соединениям для передачи данных, в политике, где должны быть определены и подробно зафиксированы ограничения и правила, применяемые к трафику, входящему в шлюз безопасности и исходящему из него, а также параметры управления и конфигурации.

Для всех шлюзов безопасности необходимо полностью использовать доступные средства идентификации и аутентификации, логического контроля доступа и аудита. Кроме того, они должны регулярно проверяться на наличие несанкционированных программных средств и (или) данных, а при их обнаружении должны составляться отчеты об инцидентах в соответствии со схемой менеджмента инцидентов информационной безопасности организации и (или) сообщества (см. ИСО/МЭК 18044 <1>).

<1> В тексте ИСО/МЭК 27033-1:2009 даны ссылки на ИСО/МЭК 27035 - это опечатка.

Следует подчеркнуть, что подключение к сети должно осуществляться только после проверки соответствия выбранного шлюза безопасности требованиям организации и (или) сообщества и возможности безопасного менеджмента всех рисков от подобного соединения. Должна обеспечиваться невозможность обхода шлюза безопасности.

Хорошим примером шлюза безопасности является межсетевой экран. Межсетевые экраны обычно должны обладать соответствующей степенью доверия, соизмеримого с оцененным риском, и стандартным набором правил для межсетевого экрана, обычно начинающихся с запрещения любого доступа к внутренним и внешним сетям и добавляющих определенные требования для обеспечения соответствия только необходимым каналам связи.

Более подробная информация о шлюзах безопасности представлена в ИСО/МЭК 27033-4 (а также в ИСО/МЭК 27002 и ИСО/МЭК 27005).

Следует отметить, что хотя аспекты сетевой безопасности персональных межсетевых экранов (специального вида межсетевых экранов) в ИСО/МЭК 27033-4 не обсуждаются, они также подлежат рассмотрению. В отличие от большинства центральных площадок, защищенных специальными межсетевыми экранами, удаленные системы могут не оправдать расходы и уровень специалистов, обеспечивающих поддержку таких устройств. Вместо специальных межсетевых экранов может использоваться персональный межсетевой экран, контролирующий поток информации в удаленный компьютер (и иногда из него). Администрирование правил (политик) межсетевого экрана может удаленно осуществляться персоналом на центральной площадке, освобождая удаленного пользователя системы от необходимости изучения технической стороны процесса, но если это невозможно, следует позаботиться об обеспечении эффективной конфигурации, особенно если персонал на удаленной площадке не имеет специальных знаний в сфере ИТ. Некоторые персональные межсетевые экраны также могут

ограничивать способность передавать санкционированные программы (даже библиотеки) по сети, ограничивая возможность распространения вредоносного программного средства.

А.7. Виртуальные частные сети

А.7.1. Вводная информация

Виртуальные частные сети представляют собой частные сети, которые реализуются при помощи инфраструктуры существующих сетей. С точки зрения пользователя, виртуальные частные сети функционируют как частные сети и предлагают аналогичные выполняемые функции и услуги. Конкретная виртуальная частная сеть может использоваться в различных ситуациях, таких, например, как:

- реализация удаленного доступа к организации для сотрудников, которым приходится много перемещаться, или находящихся за пределами организации;

- осуществление связи между различными площадками организации, включая избыточные связи для реализации инфраструктуры восстановления;

- установление подсоединений к сети организации других организаций/партнеров по основной деятельности.

Другими словами, виртуальные частные сети позволяют двум компьютерам или сетям обмениваться информацией в такой передающей среде, как Интернет. Такой обмен ранее осуществлялся с большими затратами путем использования арендуемых линий с шифраторами в канале связи. Однако с появлением высокоскоростных каналов связи Интернет и подходящего оконечного оборудования на каждом конце сети появилась возможность установления надежных связей между узлами сети с помощью виртуальных частных сетей.

А.7.2. Риски безопасности

Ключевым риском безопасности, присущим передаче данных в незащищенной сети, является риск, связанный с конфиденциальной информацией, потенциально доступной для несанкционированных сторон, что может приводить к ее несанкционированному раскрытию и (или) изменению. В дополнение к рискам безопасности, обычно связанным с локальными и глобальными сетями (см. А.1 и А.2 соответственно), типичные риски безопасности, имеющие отношение к виртуальным частным сетям, включают в себя риски, связанные с:

- небезопасной реализацией в результате:

не прошедшего тестирование или дефектного набора шифров,

слабого совместно используемого пароля, который может быть легко разгадан,

неуверенности в безопасности удаленного клиента,

неуверенности в аутентификации пользователей;

- неуверенностью в безопасности основного провайдера услуг;

- плохим функционированием или доступностью сервиса;

- несоответствием нормативным и законодательным требованиям, предъявляемым к применению шифрования в некоторых странах.

А.7.3. Меры и средства контроля и управления безопасностью

Для реализации функциональных возможностей безопасности и услуг в виртуальных частных сетях обычно используются криптографические технологии и (или) протоколы приложений, особенно если сеть, на которой построена виртуальная частная сеть, является общедоступной сетью (например, Интернет). В большинстве случаев реализации для обеспечения конфиденциальности каналы связи между участниками шифруют, а для подтверждения идентичности систем, подключенных к виртуальной частной сети, используют протоколы аутентификации. Обычно зашифрованная информация проходит по безопасному "туннелю", который соединяется со шлюзом организации, с сохранением конфиденциальности и целостности этой информации. Затем шлюз идентифицирует удаленного пользователя и делает возможным его доступ только к той информации, которую он уполномочен получить.

Таким образом, виртуальная частная сеть представляет собой механизм, основанный на туннелировании протокола - обработке одного полного протокола (клиентского протокола) как простого потока битов, и на заключении его в другой протокол (протокол несущей частоты). Обычно протокол несущей частоты виртуальной частной сети обеспечивает безопасность (конфиденциальность и целостность) клиентского протокола(ов). При рассмотрении использования виртуальной частной сети следует учитывать следующие аспекты архитектуры:

- безопасность конечной точки;

- безопасность завершения;

- защита от вредоносного программного средства;

- строгая аутентификация;

- обнаружение вторжений;

- шлюзы безопасности (включая межсетевые экраны);

- шифрование данных;

- проектирование сети;

- другая возможность соединения;

- раздельное туннелирование;

- ведение контрольных журналов и мониторинг сети;

- технический менеджмент уязвимостей.

Более подробная информация о виртуальных частных сетях, включая каждый из приведенных выше аспектов архитектуры, представлена в ИСО/МЭК 27033-5.

А.8. Сети телефонной связи

А.8.1. Вводная информация

На сегодняшний день имеются учрежденческие АТС с исходящей и входящей связью, поддерживающие традиционную канальную телефонию, соединенную с телефонной коммутируемой сетью общего пользования. Информация для наладки вызова проходит между

ними, используя DPNSS (промышленный стандартный интерфейс между учрежденческой АТС с исходящей и входящей связью и сетью доступа). Цифровая сигнальная система частных сетей распространяет возможности, которые обычно доступны только между абонентскими добавочными телефонными номерами единственной учрежденческой АТС с исходящей и входящей связью, на все абонентские добавочные телефонные номера учрежденческих АТС с исходящей и входящей связью, соединенных друг с другом в частной сети. Однако несколько лет назад параллельно с цифровой сигнальной системой частных сетей был разработан новый протокол передачи информации между учрежденческими АТС с исходящей и входящей связью, а также между учрежденческой АТС с исходящей и входящей связью и телефонной коммутируемой сетью общего пользования. Новый протокол связан с архитектурой для частных цифровых сетей связи с комплексными услугами и протоколом межстанционной передачи сигналов, основанным на концепциях цифровой сети связи с комплексными услугами, определенных в рекомендациях ITU-T. Этот межстанционный протокол, основанный на рекомендации ITU-T Q.931, известен как QSIG. Протоколы передачи сигналов считались надежными и ранее не вызывали никаких проблем в области безопасности, однако появился ряд рисков безопасности, связанных с традиционными телефонными системами учрежденческих АТС с исходящей и входящей связью.

А.8.2. Риски безопасности

Риски безопасности, имеющие отношение к традиционной телефонии, включают в себя риски, связанные с:

- отсутствием мер и средств контроля и управления резервным копированием информации, характерной для узла, что при определенных обстоятельствах может оказать влияние на доступность;

- подслушиванием, если может быть получен физический доступ к кабельной системе;

- уязвимостью портов управления к несанкционированному вторжению, поскольку они плохо защищены простыми системами с обратным вызовом, что может приводить к перепрограммированию учрежденческой АТС с исходящей и входящей связью и использованию ее с мошенническими целями или к ее отключению;

- мошенничеством, связанным с несанкционированными междугородними звонками, поскольку реестры запрета междугородней связи плохо поддерживаются, позволяя вручную маршрутизировать звонки через сеть, а затем отправлять в телефонную коммутируемую сеть общего пользования (в ряде случаев это обстоятельство приводит к серьезному мошенничеству, заключающемуся в совершении вызовов с оплатой по повышенному тарифу, и, как результат, существенным финансовым потерям);

- мошенничеством, являющимся результатом неэффективного запрета соединений между каналами прямой связи (trunk to trunk), позволяющим осуществлять несанкционированное изменение маршрута вызова и настройку вызова (мошенничество происходит с использованием взаимосвязанной системы передачи речевых сообщений для перенаправления вызовов в телефонную коммутируемую сеть общего пользования);

- недостатком устойчивости и (или) пропускной способности, который может влиять на доступность.

А.8.3. Меры и средства контроля и управления безопасностью

Меры и средства контроля и управления безопасностью сетей телефонной связи должны обеспечивать уверенность в:

- невозможности получения физического доступа к кабельной системе, распределительным коробкам и стойкам;

- надлежащем использовании реестров запрета соединений между каналами прямой связи (trunk to trunk) для предотвращения несанкционированной маршрутизации вызовов;

- невозможности доступа пользователей к кодам маршрутизации;

- частом резервном системном копировании с хранением копий во внешнем хранилище;

- конфигурировании учрежденческих АТС с исходящей и входящей связью со многими процессорами с тем, чтобы отсутствовали компоненты, отказ которых приводит к отказу всей системы;

- наличии резервных аккумуляторов или ИБП;

- наличии многих маршрутов к телефонной коммутируемой сети общего пользования с выбранными резервными аналоговыми линиями для использования в аварийной ситуации;

- использовании строгой аутентификации на всех каналах управления (это может означать использование дополнительного оборудования сторонних организаций);

- невозможности осуществления мошенничества, связанного с несанкционированными междугородними звонками, либо путем использования несанкционированной маршрутизации, либо посредством взаимосвязанных систем передачи речевых сообщений;

- наличии устройств антиспама;

- установке системы анализа вызовов и регулярной проверке затрат, связанных с вызовами;

- регулярном проведении проверок соответствия услуг требованиям и тестирования с принятием необходимых мер по их результатам.

Следует отметить, что "традиционные" телефонные системы учрежденческих АТС с исходящей и входящей связью устаревают и их либо частично переводят на системы передачи речи по IP - VoIP, либо заменяют этими системами (см. А.9 <1>).

<1> По тексту ИСО/МЭК 27033-1:2009 даны ссылки на подраздел 11.10, что является опечаткой.

А.9. IP-конвергенция

А.9.1. Вводная информация

По мере завоевания популярности IP-конвергенцией (данные, речь и видео), появилась необходимость в выявлении и рассмотрении связанных с ней проблем безопасности. Хотя текущие реализации телефонии нуждаются в мерах и средствах контроля и управления безопасностью для предотвращения мошенничества, связанного с международными разговорами, и других инцидентов безопасности, эти системы не интегрированы в корпоративную сеть данных и не подвержены тем же рискам, что сети данных IP. При конвергенции речи и данных для снижения риска атак необходима реализация мер и средств

контроля и управления безопасностью.

Приложение VoIP обычно состоит из специализированного программного обеспечения, размещенного на открытых или коммерчески доступных аппаратных средствах и операционных системах. Число серверов зависит от поставщика, а также от фактического их размещения. Эти компоненты сообщаются посредством IP по сети Интернет и соединены через коммутаторы и маршрутизаторы.

А.9.2. Риски безопасности

Основные сферы рисков безопасности могут быть связаны с IP-атаками, основанными на характерных уязвимостях программного средства, и аппаратными средствами или платформой операционной системы, на которых размещено приложение VoIP. Риски безопасности, имеющие отношение к компонентам приложения VoIP, включают в себя риски, связанные с атаками на сетевые устройства и приложения, и им могут содействовать уязвимости в проектировании или реализации решения, связанного с VoIP. Основные риски безопасности, имеющие отношение к IP-конвергенции, включают в себя риски, связанные с:

- качеством обслуживания - без общего обеспечения качества обслуживания возможны потеря качества или прерывание вызовов из-за потери пакета и задержки распространения сигнала в сети;

- недоступностью услуг из-за атак отказа в обслуживании или изменений в таблицах маршрутизации;

- влиянием на целостность и доступность вредоносных программ (включая вирусы), которая(ые) может(гут) проникнуть в сеть через незащищенные системы VoIP и ухудшить функционирование или даже вызвать потерю сервиса, а также распространиться на серверы в сети, что приведет к повреждению "памяти" для хранения данных;

- спамом через IP-телефонию (SPIT);

- программофонами, установленными на клиентских ПК, создающими существенный риск, так как они могут являться точками проникновения вредоносной программы (включая вирусы) и вторжения;

- подверженностью риску серверов VoIP и систем управления VoIP, если они не защищены межсетевыми экранами;

- возможностью ухудшения безопасности сети передачи данных из-за многочисленных портов, открытых на межсетевых экранах для поддержки VoIP. Сеанс VoIP использует множественные протоколы и связанные с ними номера портов. H.323 использует многочисленные протоколы для передачи сигналов, а H.323 и SIP используют протоколы RTP. В результате сеанс H.323 может использовать до 11 различных портов;

- мошенничеством, являющимся ключевой проблемой телефонии, и возможностью увеличения рисков при отсутствии внимания к проблемам безопасности при использовании VoIP. Хакеры могут получить несанкционированный доступ к услуге VoIP посредством атак имитации соединения, воспроизведения или нападения на соединения. Мошенничество, связанное с международными разговорами или несанкционированными вызовами с оплатой по повышенному тарифу, может привести к существенным убыткам;

- нарушениями конфиденциальности, которые могут возникнуть вследствие перехвата информации, например, в результате атаки "атакующий посередине" - проведенной в сети

сотрудниками и другим персоналом, имеющим доступ к сети;

- прослушиванием речевых вызовов;

- потребностями IP-телефонов в питании для их работы, так как телефонная сеть не может функционировать в случае нарушений энергоснабжения;

- наличием более существенной вероятности сбоя сервисов, связанных с передачей речи и данных из-за использования общих компонентов, например ЛВС.

А.9.3. Меры и средства контроля и управления безопасностью

Существует ряд следующих технических мер и средств контроля и управления безопасностью менеджмента рисков от идентифицированных угроз сетям с IP-конвергенцией:

- в сети с IP-конвергенцией должны быть реализованы средства обеспечения качества обслуживания, в противном случае существует вероятность ухудшения качества речи. Оказание сетевых услуг и там, где это возможно, предоставление IP-каналов связи должно осуществляться по волоконно-оптическому кабелю для минимизации неустойчивой синхронизации (которая влияет на качество речи);

- все серверы VoIP должны конфигурироваться с защитой от вредоносного программного средства;

- ПК, поддерживающие программофоны, должны быть оснащены персональными межсетевыми экранами; должны часто обновляться программные средства проверки наличия вредоносной программы (включая вирусы);

- защита VoIP-серверов и систем управления VoIP должна быть реализована за межсетевыми экранами, чтобы оградить их от атак;

- для каждой услуги должны использоваться специальные виртуальные частные сети и должно осуществляться шифрование различных потоков данных;

- проектировщики должны обеспечивать открытие только минимального числа портов межсетевых экранов для поддержки услуг по VoIP;

- для борьбы с мошенничеством, связанным с международными разговорами, должны реализовываться меры и средства контроля и управления, направленные на защиту от повторного воспроизведения и имитации соединения (спуфинг), для предотвращения нападения на соединения;

- доступ к серверам управления должен быть аутентифицирован;

- для серверов, поддерживающих услуги по VoIP, должен быть рассмотрен вопрос реализации систем обнаружения вторжений;

- должна рассматриваться возможность шифрования канала прохождения данных, если в сети VoIP обсуждается конфиденциальная информация;

- IP-телефоны должны получать электроэнергию через коммутаторы, поддерживаемые ИБП;

- для использования в аварийных ситуациях может потребоваться предоставление

обычного речевого сервиса с автономным источником питания.

А.10. Размещение информации на сервере веб-узлов

А.10.1. Вводная информация

Услуги по размещению информации на сервере веб-узлов предлагаются многими провайдерами сетевых услуг в форме стандартизированной услуги, часто включающей в себя средства баз данных для обработки длительно хранимых данных, а также основную среду выполнения приложения. Хотя большинство компонентов, необходимых для реализации и предложения услуг по размещению информации на сервере веб-узлов, находятся вне области рассмотрения настоящего стандарта (такие, например, как веб-сервер или база данных), в настоящем стандарте представлены некоторые мнения об услуге в целом, так как многие считают размещение информации на сервере веб-узлов сети составной частью предложения сетевых услуг.

Сервер веб-узлов размещения информации подвергается риску со стороны разнообразных угроз, особенно там, где они подсоединены к Интернету, и где, например, известные организации могут быть атакованы группами, готовыми на крайние действия. Таким образом, важно идентифицировать все потенциальные угрозы, а затем блокировать все уязвимости, которые могли бы эксплуатироваться этими угрозами. Наилучшим образом это достигается исключением уязвимостей при проектировании. Рассмотрение таких проблем в соответствии с представленной рекомендацией должно сделать возможным проектирование безопасного, надежного веб-узла с низкой вероятностью нанесения ущерба.

А.10.2. Риски безопасности

К основным рискам безопасности, имеющим отношение к размещению информации на серверах веб-узлов, относятся риски, связанные с:

- доступом злоумышленника к приложению и данным через единственную брешь в защите периметра;

- подверженностью компонента инфраструктуры уязвимостям;

- многочисленными компонентами, отказ которых приводит к отказу системы;

- потерей обслуживания из-за сбоя аппаратных средств;

- невозможностью вывода из эксплуатации для технического обслуживания;

- непреднамеренным доступом широкой пользовательской аудитории к местам хранения данных;

- атаками, направленными на целостность данных (например, нанесение ущерба веб-узлу или размещение несанкционированного информационного наполнения);

- загрузкой в систему вредоносного программного средства;

- компрометацией веб-узла с использованием функциональной возможности коммутации;

- неспособностью получения резервных копий без воздействия на работу веб-узла;

- несанкционированным раскрытием плана IP-адресации, облегчающим атаку на веб-узел;

- использованием соединений между станциями управления и веб-узлом;

- необнаруженной атакой;

- трудностью отслеживания вторжений между устройствами;

- неспособностью восстановления данных;

- неспособностью выполнять требования соглашения об уровне услуг;

- неспособностью поддерживать непрерывность обслуживания;

- несанкционированным использованием веб-услуг, включая нарушение политики организации (например, использование серверов в личных целях) и несоответствие законам и предписаниям (например, хранение материала, который нарушает авторские права, или детской порнографии).

А.10.3. Меры и средства контроля и управления безопасностью

Технические меры и средства контроля и управления безопасностью менеджмента рисков от идентифицированных угроз для веб-узлов могут включать в себя:

- обеспечение зонирования и углубленной безопасности для ограничения влияния успешной атаки;

- спецификацию различных видов межсетевых экранов для противодействия возможным уязвимостям межсетевых экранов (более подробная информация о межсетевых экранах представлена в А.6 и ИСО/МЭК 27033-4);

- устойчивость; проект должен быть проверен на наличие потенциальных компонентов, отказ которых приводит к отказу системы; они должны быть устранены;

- преодоление отказа/разделение нагрузки для защиты от сбоя в работе оборудования;

- кластеризацию там, где требованием является высокий уровень доступности в среде "24 x 7" (24 часа семь дней в неделю);

- предоставление посреднических услуг для ограничения доступа к веб-узлу и обеспечения высокой степени протоколирования;

- регулярные проверки целостности на предмет несанкционированных изменений данных;

- меры и средства контроля и управления, направленные на защиту от вредоносной программы (включая антивирусы), используемые на загрузках для предотвращения импорта вредоносного программного средства;

- коммутацию уровня 2 <1>, обычно используемую в проекте веб-узла. Коммутация уровня 3 <2> не должна использоваться, если это не является требованием деятельности организации, таким, например, как требование разделения нагрузки. Кроме того, один и тот же физический коммутатор не должен использоваться обеими сторонами межсетевого экрана. В проект коммутатора следует включать контрольные точки;

- виртуальные локальные вычислительные сети, разделенные функцией для упрощения настройки системы обнаружения вторжений, так как существует сокращенный протокол,

настроенный на любую виртуальную локальную вычислительные сеть. Кроме того, внедрение резервной виртуальной локальной вычислительные сети позволяет выполнять резервное копирование в любое время суток, не подвергая опасности работу сайта;

- насколько это необходимо для операций основной деятельности организации, план IP-адресации для сведения к минимуму числа общедоступных адресов с планом IP-адресации, хранящимся "под строжайшим секретом", так как осведомленность о его существовании может использоваться для инициирования атаки на веб-узел;

- места подсоединения каналов управления к общедоступным сетям должны шифроваться (более подробная информация об удаленном доступе приведена в ИСО/МЭК 27033-4). Это включает, по меньшей мере, наличие предупреждений об опасности/ловушек SNMP на соединениях портов пульта управления;

- копирование всех журналов регистрации событий и транзакций каждого устройства на контрольный сервер, а затем на носители резервных копий, такие, например, как компакт-диски;

- реализованную услугу временной синхронизации, поскольку она является основой анализа несанкционированного доступа и способности отслеживания по системным журналам. Для этого требуется синхронизация всех системных журналов и, следовательно, серверов, с точностью до +1 с или более (здесь уместен протокол NTP; более подробную информацию см. в 10.6 ИСО/МЭК 27002);

- конфигурирование устройств ЛВС для контроля неуправляемых изменений MAC-адресов;

- предпочтительность услуги централизованного резервного копирования, так как существует наибольшая вероятность ее выполнения должным образом;

- необходимость круглосуточного функционирования веб-узлов; функционирование требует высококачественных аппаратных средств, которые могут выдерживать такой режим. Для поддержки функционирования в режиме "24 x 7" в веб-узле должна быть определена инфраструктура сервера. Вспомогательные операционные системы должны быть укреплены, затем все серверы и другие устройства должны быть протестированы на предмет безопасности для обеспечения полной защищенности всех устройств;

- внедренное надежное прикладное программное средство, программа которого проверена в отношении структуры, являющейся логически корректной и использующей утвержденное программное средство аутентификации.

<1> Уровень 2 - канальный уровень семиуровневой модели взаимосвязи открытых систем (примечание разработчика).

<2> Уровень 3 - сетевой уровень семиуровневой модели взаимосвязи открытых систем (примечание разработчика).

Также следует отметить, что при проектировании веб-узла часто не полностью рассматриваются вопросы менеджмента непрерывности деятельности. В отношении веб-узлов деятельности, связанные с менеджментом непрерывности деятельности, должны проводиться полностью.

А.11. Электронная почта в Интернете

А.11.1. Вводная информация

Ставшие возможными для организаций/сообществ Интернет-услуги, способные удовлетворять законные требования их деятельности, привносят с собой разнообразные угрозы, которые могут использовать уязвимости эксплуатируемых систем. Таким образом, электронная почта в Интернете может подвергаться риску, связанному с различными угрозами, и целью обеспечения безопасности является разработка и реализация безопасного и надежного решения. Пример решения для электронной почты в Интернете приведен на рисунке А.1.

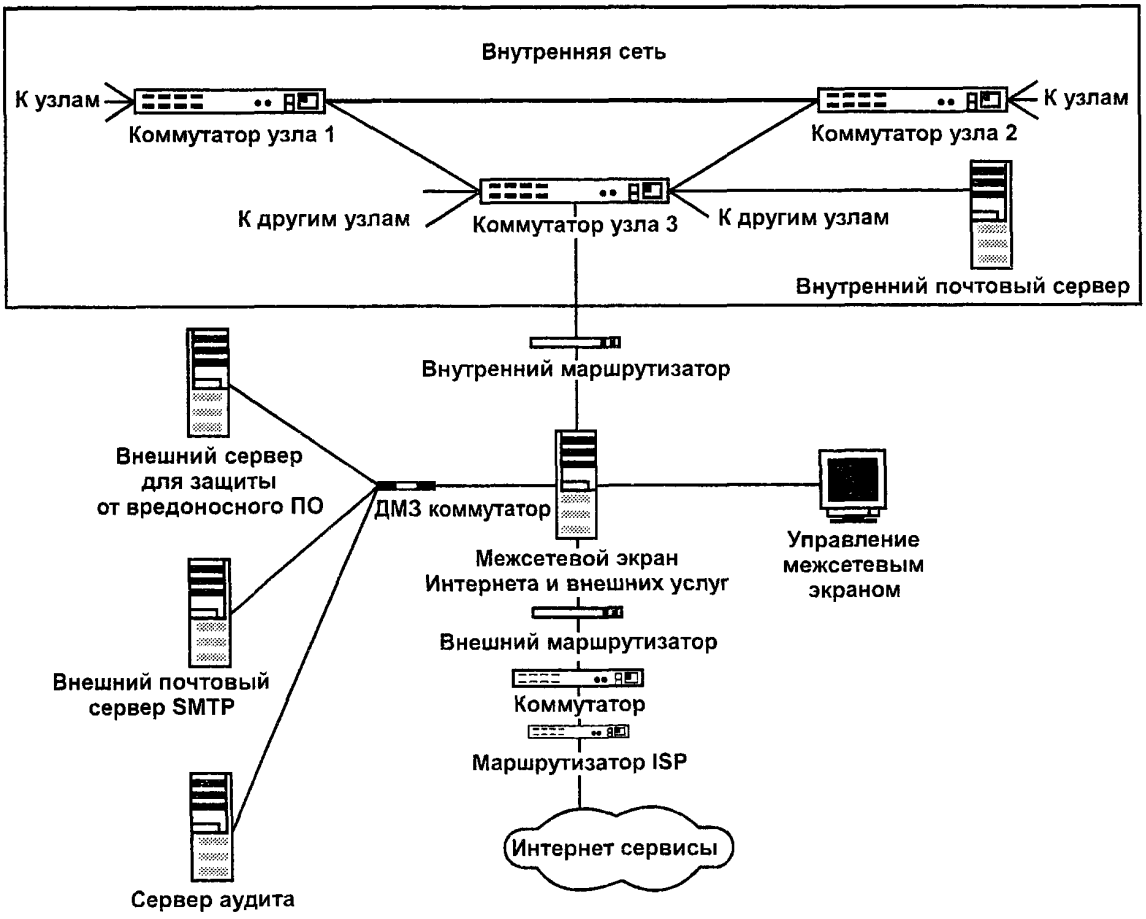


Рисунок А.1. Пример решения
для электронной почты в Интернете

Почтовые системы Интернета (SMPT) можно довольно просто рассматривать в специализированной архитектуре сетевой безопасности, поскольку от них требуется только проверять и пересылать полученную почту. Подлежащая сбору информация должна включать в себя:

- ожидаемое число почтовых сообщений в день, пересылаемых в каждом направлении;

- разрешенные виды сообщений и содержание сообщений;

- число и размер почтовых сообщений в день, пересылаемых в каждом направлении;

- средний и максимальный размеры разрешенных сообщений;

- подробности о внутренней почтовой системе;

- подробности о внутреннем шлюзе в системе электронной почты, который будет обмениваться информацией с определенным в специализированной архитектуре безопасности шлюзом в системе электронной почты;

- подробности о внешней почтовой системе(ах) которая(ые) может(гут) быть с любым ретранслятором в системе электронной почты в Интернете или может(гут) быть определенным(и) почтовыми серверами, принадлежащим(и) провайдеру услуг;

- подробности о требованиях аутентификации почтового сервера для внутренних сообщений и сообщений электронной почты в Интернете;

- подробности о внутренних средствах WINS/DNS;

- подробности о средствах DNS в Интернете;

- подробности о том, какого рода доступ требуется к телеконференциям и (если доступ нужен) должны ли накладываться какие-либо ограничения в отношении телеконференций, к которым возможен доступ;

- подробности о том, потребуется ли временная синхронизация электронной почты/сервера из Интернета;

- подробности о том, должно ли быть более одного маршрута к Интернету;

- требования поиска вредоносной программы (включая вирусы).

А.11.2. Риски безопасности

К основным рискам безопасности, имеющим отношение к электронной почте в Интернете, относятся риски, связанные с:

- несанкционированным вторжением в сеть организации/сообщества. Попытки несанкционированного доступа, включая представление себя другим пользователем, могут происходить в любое время суток, они становятся более "творческими" и изощренными и могут быть злонамеренными, например, приводя к DoS-атаке, злоупотреблению ресурсами или получению ценной информации;

- пересылкой вредоносной программы, которая может вносить "троянского коня", собирающего такую информацию, как пароли, и посылающего их на удаленный объект, или средства, захватывающие управление удаленным устройством. Таким образом, следует обращать внимание на современные "комплексные атаки", где вредоносная программа содержит "начинку";

- пересылкой спама (спам представляет собой существенную угрозу для почтовых услуг - он может оказывать неблагоприятное влияние на почтовую деятельность, расходуя сетевые ресурсы для передачи спама, а также ресурсы системы для почтовых шлюзов, или может использоваться для распространения вредоносного программного средства);

- транслированием спама (если конфигурация почтового сервера допускает наличие анонимного транслятора в системе электронной почты, он может использоваться пользователями-спамерами для рассылки спама через Интернет от лица организации, которой принадлежит почтовый сервер);

- почтовым спуфингом (когда очень просто выдать себя за любого пользователя, притворяясь лицом, посылающим электронное письмо);

- фальсификацией содержания;

- неконтролируемым информационным наполнением, исходящим из организации без ведома персонала, отвечающего за информационную безопасность, что может привести к правовым проблемам и потенциальной потере интеллектуальной собственности;

- прямой DoS-атакой, направленной на почтовую систему;

- распределенной DoS-атакой, когда тысячи почтовых сообщений посылаются из многих мест, буквально заваливая почтовый сервер.

А.11.3. Меры и средства контроля и управления безопасностью

Меры и средства контроля и управления безопасностью для электронной почты в Интернете могут включат в себя:

- использование межсетевых экранов с уровнями доверия и наборами правил, соответствующих оцененным рискам. Для большинства целей безопасности начальным набором правил межсетевого экрана должен быть отказ в прохождении всего трафика через межсетевой экран. В системе электронной почты почтовый сервер обычно посылает данные в Интернет и получает приходящие из Интернета данные. В системе электронной почты следует устанавливать набор правил для межсетевого экрана, разрешающих передачу почтовых данных в обоих направлениях. Как упоминалось ранее, рекомендуется иметь два последовательно установленных межсетевых экрана от разных поставщиков или имеющих различные операционные системы;

- возможности хранения данных и проверок, поддерживаемые полностью синхронизированной службой времени во всех компонентах инфраструктуры, межсетевых экранах и серверах. Эта временная синхронизация должна быть рассмотрена при проектировании с описанием главного генератора синхронизирующих импульсов плана иерархии серверов и сети(ей). Часто генератор синхронизирующих импульсов будет синхронизироваться при помощи системы глобального позиционирования (GPS) или наземной радиослужбы времени;

- надлежащим образом установленную систему простого протокола электронной почты для выполнения необходимых, связанных с обеспечением безопасности, задач, включая предоставление организации/сообществу интерфейса из Интернета, передачу почтовых сообщений из Интернета на внутренний почтовый сервер и в обратном направлении, предотвращение трансляции почты из Интернета на другие адреса в Интернете и обеспечение уверенности в том, что почтовые сообщения и вложения не содержат вредоносной программы, независимо от направления;

- проверку для любой входящей почты в результате просмотра на DNS-сервере Интернета сообщений, направляемых на адрес межсетевого экрана организации, а при получении из Интернета проверку внешним маршрутизатором на предмет нахождения поля адреса источника вне внутреннего адресного пространства перед направлением на межсетевой экран. На межсетевом экране сообщение должно быть проверено на предмет нахождения поля адреса вне внутреннего адресного пространства и адреса назначения почтового сервера (и, конечно, на принадлежность к электронной почте), а затем направлено на почтовый сервер SMTP. На почтовом сервере SMTP должно быть проверено, что сообщение поступило из Интернета и что адрес назначения соответствует внутреннему адресу, а затем сообщение должно быть

направлено на внешний сервер защиты от вредоносной программы с целью проверки на наличие вирусов и любого иного вредоносного наполнения. Наконец, оно должно быть направлено на внутренний почтовый сервер для распределения внутренней почтовой системой. Любые полученные сообщения с неверным адресом должны отклоняться с включением в протокол соответствующей записи. Любые полученные сообщения, содержащие вирусы или другое вредоносное наполнение, должны быть отклонены, и об этом должно быть проинформировано соответствующее лицо или группа лиц;

- для любой исходящей почты направление сообщений, посылаемых через Интернет, сначала с внутреннего почтового сервера на внешний сервер защиты от вредоносной программы в целях проверки на вирусы и любое другое вредоносное наполнение перед отправкой на внешний почтовый сервер SMTP для направления в Интернет. Внешний почтовый сервер SMTP должен проверить, находится ли адрес вне внутреннего адресного пространства, и предназначен ли он для каких-либо других почтовых маршрутов, а затем направить сообщение в Интернет;

- выбор одного из вариантов: отправка сообщения внешним почтовым сервером SMTP на единственный почтовый сервер Интернет-провайдера для предстоящей маршрутизации или на любой достоверный почтовый адрес на любом почтовом сервере. Первый вариант должен быть наиболее безопасным, поскольку он предполагает, что Интернет-провайдер (предположительно, специалист в сфере электронной почты) отвечает за организацию и поддержку пересылки почты, но он может вызывать задержки, связанные с пересылкой почты. Второй вариант является более гибким и не вызывает задержек, связанных с пересылкой, осуществляемой Интернет-провайдером, но он может стать менее безопасным в случае ненадлежащего управления, при этом организация/сообщество должна поддерживать пересылку почты на многие почтовые серверы и подвергаться риску отказа, если ее ретранслятор не будет признан удаленным почтовым сервером, что может быть преодолено посредством процедур аутентификации между соответствующими почтовыми серверами. Выбираемый вариант зависит от технических достоинств решения и уровня квалификации лиц, которые будут поддерживать почтовую систему;

- реализацию мер управления доступом на основе принципа наименьшего уровня привилегий;

- конфигурирование почтового сервера для блокирования или удаления почтовых сообщений, содержащих вложения, которые обычно используются для распространения вредоносной программы, таких, например, как файлы с расширениями vbs, bat, exe, pif и scr;

- быстрое устранение инфицированных компьютеров из сети для предотвращения дальнейшей компрометации, проведение судебной экспертизы и восстановления с использованием доверенных носителей данных;

- обучение тому, чтобы персонал не открывал вложения, пока они не проверены, и не запускал скаченные из Интернета программы, если не проведена проверка на наличие вредоносных программ;

- использование на маршрутизаторах списка контроля доступа (ACL). ACL на маршрутизаторах определяет на обращение с входящим IP-пакетом. Обычные действия при этом включают пересылку, протоколирование и отбрасывание (или отказ). В сочетании с соответствующей политикой маршрутизатора по умолчанию (например, отказ в прохождении всего трафика) можно определить набор правил для маршрутизатора, оказывающих существенную помощь в поддержке безопасности базовой сети;

- активизацию антиспуфинга. Спуфинг обычно относят к ситуации, когда исходный адрес сообщения имеет вид, как будто сообщение исходит от кого-то или откуда-то, но не от его подлинного автора. Меры антиспуфинга принимают форму непринятия сообщения из Интернета, если в нем утверждается, что оно исходит изнутри организации, и наоборот (более подробную информацию см. в RFC 2827 "Фильтрация на входе сети. Отражение атак отказа в обслуживании");

- активизацию модулей доступа электронной почты. Прокси-сервер представляет собой сервер, действующий в качестве посредника между пользователем ПК/рабочей станции и Интернетом так, чтобы предприятие могло обеспечить безопасность, административный контроль и услугу кэширования. Безопасность осуществляется с применением:

- сканирования данных по известным образцам (например, проверка на значимые слова для обеспечения соответствия);

- перемещения между внутренними и внешними адресами;

- создания журнала регистрации запросов и запрашивающих сторон;

- средств защиты от вредоносной программы, основанных на модулях доступа.

Прокси-серверы также могут проводить проверку на предмет вредоносного наполнения простой обработкой запроса. Если запрос является вредоносным, на самом прокси-сервере, вероятно, произойдет аварийный отказ. Поскольку прокси-серверы обычно реализуются в ДМЗ, полудоверенной зоне, такие действия выполняют функцию "предохранителя" с тем, чтобы обеспечить защиту реальной запрашивающей стороны или сервера;

- реализацию защитных мер и средств контроля и управления вредоносной программой на модулях доступа электронной почты. После того, как выявлено, что информационные системы свободны от вредоносной программы (включая вирусы), единственным маршрутом внесения вредоносной программы является внесение ее в качестве данных (или программ). Почтовые средства являются основными "кандидатами" на передачу вредоносной программы и основными точками реализации защитных мер и средств контроля и управления вредоносной программой. Обычные меры и средства контроля и управления безопасностью включают в себя средства, изолирующие подозрительные файлы (например, по типу информационного наполнения) и отсеивающие запрошенные адреса электронной почты, попавшие в "черный" список. Кроме того, для борьбы с самыми последними комплексными угрозами, когда вредоносная программа содержит "начинку", необходимо рассмотреть вопрос блокирования определенных вложений, содержащих исполняемую программу;

- использование технологий антиспама и обучение пользователей защите адресов электронной почты при доступе к сайтам;

- реализацию антиретранслятора на серверах электронной почты и обратных просмотров DNS. Один из возможных способов эксплуатации почтового сервера из Интернета состоит в том, чтобы послать на него сообщение, предназначенное на самом деле сторонней организации. Тогда, если почтовый сервер принимает сообщение, оно будет направлено сторонней организации, по-видимому, от организации/сообщества, а не от истинного отправителя. Эти механизмы могут быть использованы пользователями-спамерами или в целях разрушения сети сторонней организации атакой отказа в обслуживании. Меры и средства контроля и управления антиретранслятора определяют, предназначается ли входящее электронное письмо организации/сообществу. Если это не так, электронное письмо протоколируется (или изолируется), и почтовый сервер не предпринимает дальнейших действий;

- использование предупреждений об опасности и "ловушек" протокола SNMPv3. Протокол SNMP может использоваться для дистанционного управления сетевым устройством и для отправки устройством сообщений (или "ловушек") с целью уведомления станции мониторинга о состоянии этого устройства. Протокол относительно небезопасен, и существует тенденция не использовать его для целей управления устройством. Тем не менее, SNMP-"ловушки" широко используются и передаются по сети для уведомления центральной станции о статистике или состояниях ошибки;

- реализацию управления аудитом. Все журналы регистрации, относящиеся к электронной почте, должны быть собраны на сервере аудита и должны ежедневно проверяться для обнаружения необычной деятельности, что включает в себя журналы регистрации межсетевого экрана и почтового модуля доступа SMTP. Журналы регистрации следует изучать, используя качественные инструментальные средства анализа и корреляции событий;

- установление внеполосного управления межсетевым экраном. Установление внеполосного управления межсетевым экраном связано с практикой использования разных сетей для передачи данных и управления, чтобы сделать невозможным подключение злоумышленника к целевому устройству (в данном случае межсетевому экрану). Существует несколько механизмов реализации внеполосного управления:

управление только путем физического доступа,

отдельная сеть управления,

использование виртуальных локальных сетей для создания отдельных каналов в сети данных, позволяющих разделить поток данных и трафик управления.

В иных случаях управление должно осуществляться только путем физического доступа.

А.12. Маршрутизированный доступ к сторонним организациям

А.12.1. Вводная информация

Число соединений со сторонними организациями увеличивается по мере стремления организаций к совместной работе, требующей прямой связи и шлюзов между организациями. Пример технического решения по обеспечению безопасности для маршрутизированного доступа к сторонним организациям представлен на рисунке А.2.

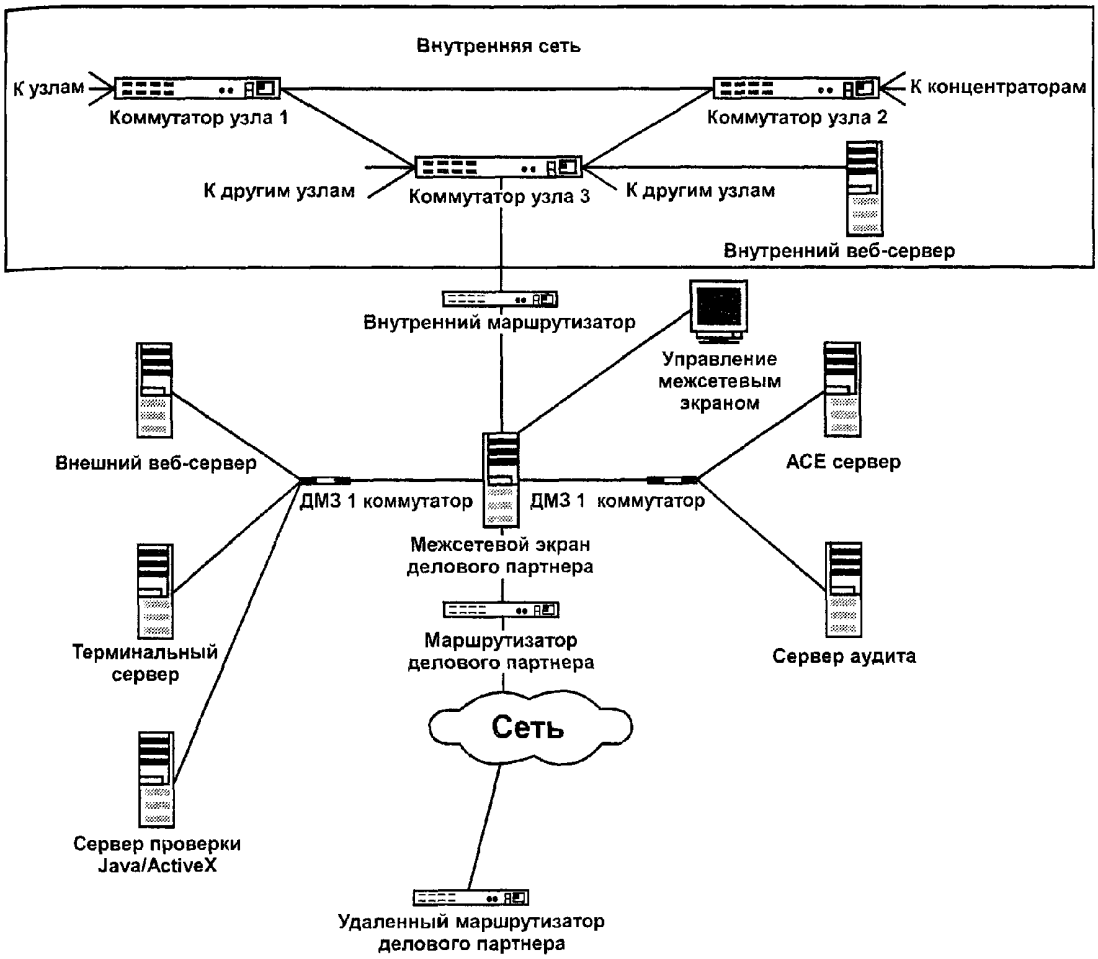


Рисунок А.2. Пример технического решения
по маршрутизированному доступу к сторонним организациям

Маршрутизированный доступ к другим организациям может осуществляться с помощью технологий глобальных или широкополосных сетей и требоваться по многим причинам, например, может потребоваться доступ к приложениям баз данных в любом направлении - в этом случае может быть введен несанкционированный код с любой стороны, или пользователями любой сети может быть предпринята попытка несанкционированного доступа к другой сети. Подлежащая сбору информация должна, например, включать в себя:

- сведения о том, какие приложения подлежат поддержке через маршрутизированную связь;

- подробности о взаимодействующих серверах и их местоположении;

- подробности о ПК пользователей и их местоположении;

- подробности о маршрутизаторе сторонней организации, при наличии (включая IP-адрес, метод аутентификации, например, цифровые сертификаты, совместно используемые пароли, RADIUS, TACACS+);

- вид и скорость линии связи, например, виртуальная частная сеть в широкополосной сети, ретрансляция кадров, частная проводная связь, коммутируемое соединение по телефонной

линии и цифровая сеть связи с комплексными услугами.

Целесообразно также разработать для доступа каждой сторонней организации документацию конфигурации (при ее отсутствии), включающую в себя обзор требований, сетевой график, информацию о конфигурации и подробности об IP-адресации и аутентификации.

(При рассмотрении маршрутизированного доступа к сторонним организациям целесообразно обратиться к ИСО/МЭК ТО 14516:1999).

А.12.2. Риски безопасности

Основные риски безопасности, имеющие отношение к маршрутизированному доступу к сторонним организациям, в основном связаны с тем фактом, что любая сторонняя организация представляет собой отдельную сферу безопасности с собственными политиками и может не отличаться такой же безопасностью, как собственная организация. Таким образом, основные риски безопасности, имеющие отношение к маршрутизированному доступу к сторонним организациям, включают риски, связанные с:

- несанкционированным доступом к вашей сети и связанным с ней "системам" и информации;

- введением вредоносной программы через кажущийся доверенным шлюз;

- DoS-атакой через стороннюю организацию;

- убеждением, что сеть сторонней организации предлагает более высокий уровень безопасности, чем Интернет.

А.12.3. Меры и средства контроля и управления безопасностью

Меры и средства контроля и управления безопасностью для маршрутизированного доступа к сторонним организациям могут включать в себя:

- изоляцию всех соединений с внешней стороной посредством межсетевого экрана, отличающегося от используемого для Интернета и других классов внешних соединений;

- программное средство защиты от вредоносных программ для проверки программ Java и ActiveX вместо программного средства, работающего на межсетевых экранах [как упоминалось ранее, программы Java и ActiveX не распознаются стандартными программными средствами защиты от вредоносных программ (включая антивирусы) и, следовательно, не могут быть обнаружены и проверены на предмет их достоверности];

- наличие строгой аутентификации на основе маркеров или карточек в виде цифровых сертификатов на токенах или смарт-картах либо двухфакторной аутентификации с маркерами;

- использование идентификатора линии вызова в качестве дополнительного метода аутентификации, ее соединения осуществляются с помощью маршрутизированного доступа цифровой сети связи с комплексными услугами;

- аутентификацию маршрутизаторов, включая маршрутизаторы на удаленном конце соединения, с помощью сервера аутентификации, такого, например, как TACACS+. Однако если со сторонней организацией не может быть достигнуто соглашение о методе аутентификации, то при малом числе применений могут использоваться совместно используемые пароли - обмен

паролями. Для большого числа соединений должны использоваться цифровые сертификаты, поскольку они могут регулярно меняться;

- использование маршрутизатором сторонней организации таких же средств аутентификации, например, цифровых сертификатов, совместно используемых секретных данных, RADIUS, TACACS+;

- обеспечение физической безопасности маршрутизаторов на обоих концах соединения;

- включение всех соединений со сторонней организацией в документированные условия обеспечения безопасного соединения, которые подписываются каждой сторонней организацией до разрешения любого соединения;

- рассмотрение вопроса об использовании системы обнаружения вторжений/системы предупреждения вторжений;

- реализацию аудита и подотчетности;

- разработку и согласование документации по конфигурации для доступа каждой сторонней организации, которая включает в себя обзор требований, сетевой график, информацию о конфигурации и подробности об IP-адресации и аутентификации.

А.13. Центр обработки (и хранения) данных сети Интранет

А.13.1. Вводная информация

Центр обработки (и хранения) данных Интранета содержит приложения и данные, наиболее важные для организации. Центр обработки (и хранения) данных может быть критической частью инфраструктуры организации, и его деятельность может быть связана с решением задач, выходящих за пределы сетевых аспектов, рассматриваемых в других частях настоящего приложения. Хотя хранение (сети хранения данных) и отдельные аспекты, касающиеся серверов в центре обработки (и хранения) данных, выходят за область применения настоящего стандарта (например, повышение надежности серверов или баз данных); здесь приведены некоторые соображения об общей безопасности центра обработки (и хранения) данных.

Угрозы, с которыми сталкиваются в настоящее время администраторы безопасности ИТ, из относительно тривиальных попыток причинить ущерб сетям превратились в изощренные атаки, направленные на получение прибыли и хищение конфиденциальных корпоративных данных. Реализация возможностей обеспечения безопасного надежного центра обработки (и хранения) данных для защиты значимых и необходимых для целевой задачи приложений и данных служит краеугольным камнем усилий, направленных на обеспечение безопасности сетей предприятия.

Поскольку основной задачей обеспечения безопасности центра обработки (и хранения) данных является поддержание доступности услуг, необходимо тщательно рассмотреть, как обеспечение безопасности влияет на потоки данных, масштабируемость и сбои.

А.13.2. Риски безопасности

В настоящее время увеличились векторы атак, направленные на разрушение защиты сети и нацеленные непосредственно на приложения. Атаки на базе HTTP, XML и SQL оказываются успешными для большинства злоумышленников, потому что этим протоколам обычно разрешается проходить через сеть организации и входить в центр обработки (и хранения) данных Интранета.

Ниже приведены некоторые векторы угроз, оказывающие влияние на центр обработки (и хранения) данных Интранета:

- несанкционированный доступ к данным;

- несанкционированный доступ к приложениям;

- несанкционированный доступ к устройствам;

- нарушение важнейших услуг в результате DoS-атак;

- необнаруженные атаки;

- потеря данных;

- невозможность восстановления данных;

- целевые атаки для модификации данных;

- повышение привилегий;

- установка вредоносного программного средства;

- несанкционированное использование услуг, в том числе нарушение политики организации.

А.13.3. Меры и средства контроля и управления безопасностью

Технические меры и средства контроля и управления безопасностью для центров обработки (и хранения) данных могут включать в себя:

- шлюзы безопасности для управления доступом к центру обработки (и хранения) данных;

- использование в центре обработки (и хранения) данных системы обнаружения вторжений/предупреждения вторжений;

- защитные меры и средства контроля и управления вредоносной программой (включая антивирусы) на серверах;

- менеджмент безопасности устройств инфраструктуры;

- возможности регистрации и проверки, поддерживаемые полностью синхронизированной службой времени во всех частях центра обработки (и хранения) данных;

- план обеспечения непрерывности деятельности при аварийных ситуациях;

- гибкое проектирование;

- регулярные проверки целостности для выявления несанкционированных изменений данных;

- виртуальные ЛВС для разделения услуг в центре обработки (и хранения) данных с целью защиты более уязвимых услуг;

- конфигурирование устройств ЛВС для контроля неуправляемых изменений MAC-адресов;

- использование протоколов менеджмента безопасности.

Приложение В
(справочное)

ПЕРЕКРЕСТНЫЕ ССЫЛКИ МЕЖДУ ИСО/МЭК 27001, ИСО/МЭК 27002 И РАЗДЕЛАМИ НАСТОЯЩЕГО СТАНДАРТА, ОТРАЖАЮЩИМИ МЕРЫ И СРЕДСТВА КОНТРОЛЯ И УПРАВЛЕНИЯ, СВЯЗАННЫЕ С СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

Таблица В.1

Перекрестные ссылки между ИСО/МЭК 27001, ИСО/МЭК 27002 и разделами настоящего стандарта

Разделы, подразделы, пункты, подпункты ИСО/МЭК 27001 и ИСО/МЭК 27002	Меры	Разделы, подразделы, пункты, подпункты настоящего стандарта
10.4.1. Меры защиты от вредоносного кода	Должны быть реализованы меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей	8.7. Защита от вредоносной программы
10.4.2. Меры защиты от мобильного кода	Там, где разрешено использование мобильного кода, конфигурация должна обеспечивать уверенность в том, что авторизованный мобильный код функционирует в соответствии с четко определенной политикой безопасности, а исполнение операций с использованием неавторизованного мобильного кода будет предотвращено	7.2.2.2. Сетевые архитектуры, приложения и сервисы
10.6.1. Средства контроля сети	Сети должны быть адекватно управляемыми и контролируемыми в целях защиты от угроз и поддержания безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям	См. ниже для разделов ИСО/МЭК 27001 и ИСО/МЭК 27002, пункты 10.6.1 IG, перечисления а) - е)
10.6.1. IG <1>, перечисление а)	Эксплуатационные обязанности, связанные с сетями, должны быть	8.2. Менеджмент сетевой

	отделены от компьютерных операций (где необходимо)	безопасности
10.6.1. IG, перечисление b)	Должны быть установлены обязанности и процедуры менеджмента удаленного оборудования, включая оборудование в зоне пользователя	Более подробная информация приведена в ИСО/МЭК 27033-5
10.6.1. IG, перечисление c)	Должны быть установлены специальные меры и средства контроля и управления для защиты конфиденциальности и целостности данных, передаваемых по общедоступным или беспроводным сетям, и для защиты соединенных с ними систем и приложений (см. 11.4 и 12.3); могут также потребоваться специальные меры и средства контроля и управления для поддержки доступности сетевых услуг и подсоединенных компьютеров	Все меры и средства контроля и управления безопасностью см. в разделе 11 "Аспекты "технологий" - риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления"
10.6.1. IG, перечисление d)	Должны использоваться соответствующие регистрация (данных) и мониторинг, чтобы сделать возможным фиксирование деятельности, связанной с обеспечением безопасности	8.5. Ведение контрольных журналов и мониторинг сети
10.6.1. IG, перечисление e)	Деятельность по осуществлению менеджмента должна быть согласована должным образом, чтобы оптимизировать услуги для организации и обеспечить последовательное применение мер и средств контроля и управления в инфраструктуре обработки информации	8.2. Менеджмент сетевой безопасности
10.6.2. Безопасность сетевых сервисов	Обеспечение безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в любой договор о сетевых услугах, независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией	8.2. Менеджмент сетевой безопасности (имеющий отношение к другим подпунктам раздела 8 и разделам 9 - 11)
10.8.1. Политики и процедуры обмена информацией	Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов	6.2. Планирование и менеджмент сетевой безопасности
10.8.4. Электронный обмен сообщениями	Информация, используемая в электронном обмене сообщениями, должна быть надлежащим образом	A.11. Электронная почта в Интернете

	защищена	
10.9.1. Электронная торговля	Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания контрактов, а также от несанкционированного разглашения и модификации	10.4. Услуги "бизнес - бизнес" 10.5. Услуги "бизнес - клиент"
10.9.2. Транзакции в режиме реального времени (on-line)	Информация, используемая в транзакциях в режиме реального времени (on-line), должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного копирования или повторного отправления сообщений	10.5. Услуги "бизнес - клиент"
10.9.3. Общедоступная информация	Информация, предоставляемая через общедоступную систему, должна быть защищена от несанкционированной модификации	A.10. Размещение информации на сервере веб-узлов
11.4.1. Политика в отношении использования сетевых услуг	Пользователям следует предоставлять доступ только к тем услугам, по отношению к которым они специально были авторизованы	8.2.2.2. Политика сетевой безопасности
11.4.2. Аутентификация пользователей для внешних соединений	Для контроля доступа удаленных пользователей должны применяться соответствующие методы аутентификации	8.4. Идентификация и аутентификация
11.4.3. Идентификация оборудования в сетях	Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием	
11.4.4. Защита портов конфигурации и диагностики при удаленном доступе	Физический и логический доступ к портам конфигурации и диагностики должен быть контролируемым	
11.4.5. Принцип разделения в сетях	В сетях должны применяться принципы разделения групп информационных услуг, пользователей и информационных систем	
11.4.6. Контроль сетевых соединений	Подключение пользователей к совместно используемым сетям, особенно к выходящим за территорию организации, необходимо ограничивать в соответствии	11. Аспекты сетевых "технологий" - риски, методы проектирования и вопросы,

	с политикой контроля доступа и требованиями бизнес-приложений	касающиеся мер и средств контроля и управления
11.4.7. Контроль маршрутизации в сети	Должны быть внедрены средства управления и контроля маршрутизации в сети с целью исключения нарушений правил контроля доступа для бизнес-приложений, вызываемых соединениями и потоками информации	A.6. Шлюзы безопасности

<1> IG - Руководство по реализации, т.е. стандарт ИСО/МЭК 27002.

Таблица В.2

Перекрестные ссылки между разделами настоящего стандарта и разделами ИСО/МЭК 27001, ИСО/МЭК 27002

Разделы, подразделы, пункты, подпункты настоящего стандарта	Наименования разделов	Разделы, подразделы, пункты, подпункты ИСО/МЭК 27001 и ИСО/МЭК 27002
6	Обзор	
6.2	Планирование и менеджмент сетевой безопасности	10.8.1. Политики и процедуры обмена информацией
7	Идентификация рисков и подготовка к идентификации мер и средств контроля и управления безопасностью	
7.2	Информация о текущем и (или) планируемом построении сети	
7.2.1	Требования безопасности в корпоративной политике информационной безопасности	
7.2.2	Информация о текущем/планируемом построении сети	
7.2.2.2	Сетевые архитектуры, приложения и сервисы	10.4.2. Меры защиты от мобильного кода
7.2.2.3	Виды сетевых соединений	
7.2.2.4	Другие сетевые характеристики	
7.2.2.5	Дополнительная информация	

7.3	Риски информационной безопасности и потенциальные области действия мер и средств контроля и управления	
8.2	Менеджмент сетевой безопасности	10.6.1. Средства контроля сети
8.2.2	Деятельности по менеджменту сетевой безопасности	
8.2.2.2	Политика сетевой безопасности	5.1. Политика информационной безопасности 11.4.1. Политика в отношении использо-вания сетевых услуг
8.2.2.3	Операционные процедуры сетевой безопасности	
8.2.2.4	Проверка соответствия требованиям сетевой безопасности	
8.2.2.5	Условия обеспечения безопасности сетевых соединений со многими организациями	
8.2.2.6	Документированные условия обеспечения безопасности для удаленных сетевых пользователей	
8.2.2.7	Менеджмент инцидентов сетевой безопасности	13. Управление инцидентами информационной безопасности
8.2.3	Роли и обязанности, связанные с обеспечением сетевой безопасности	8.1.1. Функции и обязанности персонала по обеспечению безопасности
8.2.4	Сетевой мониторинг	10.10. Мониторинг
8.2.5	Оценка сетевой безопасности	
8.3	Менеджмент технических уязвимостей	12.6. Менеджмент тех-нических уязвимостей
8.4	Идентификация и аутентификация	11.4.2. Аутентифика-ция пользователей для внешних соединений 11.5.2. Идентификация и аутентификация пользователей
8.5	Ведение контрольных журналов и мониторинг сети	10.6.1. Средства контроля сети 10.10.1. Ведение

		журналов аудита
8.6	Обнаружение и предотвращение вторжений	
8.7	Защита от вредоносных программ	10.4. Защита от вредоносного кода и мобильного кода
8.8	Услуги, основанные на криптографии	12.3. Криптографичес-кие средства защиты
8.9	Менеджмент непрерывности деятельности	14. Менеджмент непрерывности бизнеса
9	Рекомендации по проектированию и реализации сетевой безопасности	
9.2	Специализированная архитектура/проект сетевой безопасности	
10	Типовые сетевые сценарии - риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления	
10.2	Услуги доступа сотрудников к Интернету	
10.3	Расширенные услуги совместной работы	
10.4	Услуги "бизнес-бизнес"	10.9.1. Электронная торговля
10.5	Услуги "бизнес-клиент"	10.9.1. Электронная торговля 10.9.2. Транзакции в режиме реального времени (on-line)
10.6	Услуги аутсорсинга	
10.7	Сегментация сети	
10.8	Мобильная связь	
10.9	Сетевая поддержка для находящихся в разъездах пользователей	
10.10	Сетевая поддержка для домашних офисов и офисов малых предприятий	
11	Аспекты сетевых "технологий" - риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления	10.6.1. Средства контроля сети 11.4.6. Контроль сетевых соединений
12	Разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности	

13	Реализация комплекса программных и технических средств и услуг по обеспечению безопасности	
14	Мониторинг и проверка эксплуатации комплекса программных и технических средств и услуг	
Приложение A	Аспекты сетевых "технологий" - риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления	
A.1	Локальные вычислительные сети	
A.2	Глобальные вычислительные сети	
A.3	Беспроводные сети	
A.4	Радиосети	
A.5	Широкополосные сети	
A.6	Шлюзы безопасности	11.4.7. Контроль маршрутизации в сети
A.7	Виртуальные частные сети	
A.8	Сети телефонной связи	
A.9	IP-конвергенция	
A.10	Размещение информации на сервере веб-узлов	10.9.3. Общедоступная информация
A.11	Электронная почта в Интернете	10.8.4. Электронный обмен сообщениями
A.12	Маршрутизированный доступ к сторонним организациям	

Приложение C
(справочное)

ПРИМЕРНЫЙ ОБРАЗЕЦ ДОКУМЕНТА, КАСАЮЩЕГОСЯ SecOPs

1. Введение

1.1. Предпосылки

1.2. Структура документа

2. Область применения

2.1. Объекты

2.2. Техническая инфраструктура

2.2.1. ИТ-среда

2.2.2. Сетевая архитектура

2.2.3. Объект 1

2.2.4. Объект 2

2.2.5. Объект 3

2.2.6. Внешние соединения

3. Политика безопасности

4. Организация обеспечения информационной безопасности

4.1. Введение

4.2. Менеджмент безопасности - структура и обязанности

4.2.1. Должностное лицо службы безопасности организации

4.2.2. Заместитель должностного лица службы безопасности организации

4.2.3. Должностное лицо службы информационной безопасности организации

4.2.4. <1> Группа поддержки ИТ (при необходимости)

<1> В тексте оригинала ИСО/МЭК 27033-1:2009 отсутствует пункт 4.2.4 (т.е. после 4.2.3 следует 4.2.5).

4.2.5. Руководители основной деятельности

4.2.6. Персонал

4.2.7. Совет директоров организации

4.3. Отчетность об инцидентах и недостатках информационной безопасности

4.4. Распределение операционных процедур безопасности

4.5. Оценка рисков, связанных со сторонними организациями

4.6. Соглашения о доступе сторонней организации

4.7. Аутсорсинг

5. Управление активами

5.1. Инвентаризация активов

5.2. Допустимое использование информации и других активов

5.3. Классификация информации

6. Кадровая безопасность

6.1. Минимальная кадровая безопасность, включая допуск и требования

6.2. Условия

6.3. Информирование и обучение обеспечению информационной безопасности

6.4. Дисциплинарный процесс

6.5. Контроль над персоналом

6.6. Окончание работы по найму

6.7. Карточки доступа/прохода в здания

6.8. Физический доступ к системам и сетям ИТ

7. Физическая безопасность и защита от влияния окружающей среды

7.1. Реализация физических мер и средств контроля и управления и мер и средств контроля и управления влиянием окружающей среды

7.2. Физический периметр защиты

7.3. Физические меры и средства контроля и управления входом

7.4. Работа в основных помещениях/зонах

7.5. Размещение оборудования

7.6. Ключи и комбинации

7.7. Сигналы тревоги при обнаружении нарушителей

7.8. Защита оборудования от хищения

7.9. Снятие оборудования с эксплуатации

7.10. Средства управления доступом к аппаратным средствам

7.11. Обнаружение искажений

7.12. Техническое обслуживание и ремонт

7.13. Защита энергопитания

7.14. Пожаробезопасность

7.15. Защита от протечек

7.16. Предупреждение об опасности

7.17. Безопасность ПК

8. Менеджмент связи и операций

8.1. Операционные процедуры и обязанности

8.1.1. Процедуры контроля внесения изменений

8.1.2. Разделение обязанностей и сферы ответственности

8.2. Планирование и приемка системы

8.2.1. Планирование мощностей

8.2.2. Приемка системы

8.3. Защита от вредоносной и мобильной программы

8.3.1. Предупреждение

8.3.2. Обнаружение

8.3.3. Восстановление

8.3.4. Мобильная программа

8.4. Резервное копирование и восстановление

8.5. Запуск и остановка ИТ-компонентов (в том числе сетевых компонентов)

8.6. Обеспечение безопасности носителей данных (в том числе документов)

8.6.1. Менеджмент сменных носителей данных

8.6.2. Печатные документы

8.6.3. Безопасное повторное использование или уничтожение носителей данных

8.7. Обмен информацией

8.8. Мониторинг

8.8.1. Учет и аудит

8.8.2. Журналы учета, заполняемые вручную

8.8.3. Временная синхронизация

8.9. Протоколы данных оператора

8.10. Протоколирование данных об ошибках

8.11. Планы развития ИТ и средств связи

9. Управление доступом

9.1. Менеджмент учетных записей пользователей

9.1.1. Запросы по учетным записям пользователей

9.1.2. Создание учетных записей пользователей

9.1.3. Проверка, блокирование и удаление учетных записей пользователей

9.2. Конфигурация управления доступом

9.3. Менеджмент паролей

9.3.1. Реализация и контроль

9.3.2. Генерация паролей

9.3.3. Хранение и передача паролей

9.3.4. Смена паролей

9.3.5. Проверка паролей

9.3.6. Пароли для технического обслуживания

9.3.7. Пароли привилегированного пользователя/пароли персонала, наблюдающего за управлением системой

9.4. Маркеры доступа

9.5. Управление сетевым доступом

9.5.1. Общая информация

9.5.2. Внешние соединения

9.6. Условия обеспечения безопасности соединений

9.7. Удаленный доступ

9.8. Управление доступом к операционной системе, приложениям и информации

9.9. Мобильные компьютерные среды и дистанционная работа

9.9.1. Общая информация

9.9.2. Безопасность дорожных компьютеров

9.9.3. Безопасность КПК

10. Приобретение, разработка и поддержка систем

10.1. Безопасность системных файлов

10.1.1. Контроль системного программного обеспечения

10.1.2. Защита данных тестирования системы

10.1.3. Защита исходных текстов программ

10.2. Обеспечение безопасности процессов разработки и поддержки

10.2.1. Целостность системного и прикладного программного обеспечения

10.2.2. Разработка программных средств по субдоговору/с привлечением внешних ресурсов

10.3. Сопровождение программного обеспечения

10.4. Журналы программных ошибок

10.5. Управление техническими уязвимостями

11. Менеджмент инцидентов информационной безопасности

11.1. Инциденты и слабые места информационной безопасности

11.2. Сбои ИТ (включая сети)

12. Менеджмент непрерывности деятельности

12.1. Планирование обеспечения непрерывности деятельности

12.2. Процедуры резервирования

12.3. Аварийные ситуации и сбои

12.3.1. Аппаратные сбои

12.3.2. Программные сбои

12.3.3. Эвакуация при возгорании/эвакуация из здания

13. Соответствие

13.1. Соответствие правовым требованиям

13.2. Соответствие политикам и стандартам информационной безопасности, техническое соответствие

13.3. Защита инструментальных средств аудита систем

14. Структура документа

14.1. Обратная связь

14.2. Изменения SecOPs

Приложение A. Справочная информация.

БИБЛИОГРАФИЯ

[1] ISO/IES 7498-1:1994	Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model
[2] ISO 7498-2:1989	Information processing systems - Open Systems Interconnection - Basic Reference Model - Security Architecture
[3] ISO/IEC 7498-3:1997	Information technology - Open Systems Interconnection - Basic Reference Model: Naming and Addressing
[4] ISO/IEC 7498-4:1989	Information processing systems - Open Systems Interconnection - Basic Reference Model - Management Framework
[5] ISO/IEC 9594-8	Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate trameworks
[6] ISO/IEC 10181-1:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview
[7] ISO 11166-2	Banking - Key management by means of asymmetric algorithms - Part 2: Approved algorithms using the RSA cryptosystem
[8] ISO 11568 (all parts)	Banking - Key management (retail)
[9] ISO 11649	Financial services - Core banking - Structured creditor reference to remittance information
[10] ISO/IEC 11770 (all parts)	Information technology - Security techniques - Key management
[11] ISO/IEC 11889-1	Information technology - Trusted Platform Module - Part 1: Overview
[12] ISO/IEC 11889-2	Information technology - Trusted Platform Module - Part 2: Design principles
[13] ISO/IEC 11889-3	Information technology - Trusted Platform Module - Part 3: Structures
[14] ISO/IEC 11889-4	Information technology - Trusted Platform Module - Part 4: Commands
[15] ISO 13492	Financial services - Key management related data element - Application and usage of ISO 8583 data elements 53 and 96
[16] ISO/IEC 13888 (all parts)	Information technology - Security techniques - Non-repudiation
[17] ISO/IEC TR 14516:1999	Information technology - Security techniques - Guidelines for the use and Management of Trusted Third Party services
[18] ISO/IEC 15288:2008	Systems and software engineering - System life cycle processes
[19] ISO/IEC 18043:2006	Information technology - Security techniques - Selection, deployment and

operations of intrusion detection systems (IDS)
[20] ISO/IEC TR 18044:2004 <1> Information technology - Security techniques - Information security incident management
[21] ISO 21188 <2> Banking Public Key Infrastructure

<1> ISO/IEC TR 18044 будет отменен и заменен новой редакцией ISO/IEC 27035.

<2> В тексте ISO указан ISO/IEC 21118 (Information to be included in specification sheets - Data projectors) - это опечатка.

[22] ISO/PAS 22399:2007 Societal security - Guidelines for incident preparedness and operational continuity management
[23] ISO/IEC 27003 Information technology - Security techniques - Information security management systems implementation guidance
[24] ISO/IEC 27004 Information technology - Security techniques - Information security management - Measurement
[25] IETF Site Security Handbook (RFC 2196), September 1997
[26] IETF IP Security Document Roadmap (RFC 2411), November 1998
[27] IETF Security Architecture for the Internet Protocol (RFC 2401), November 1998
[28] IETF Address Allocation for Private Internets (RFC 1918), February 1996
[29] IETF SNMP Security Protocols (RFC 1352), July 1992
[30] IETF Internet Security Glossary (RFC 2828), May 2000
[31] IETF Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (RFC 2827), May 2000
[32] NIST Special Publications (800 series) On Computer Security
[33] NIST Special Publication 800-10: Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, December 1994.

Приложение ДА
(справочное)

СВЕДЕНИЯ О СООТВЕТСТВИИ ССЫЛОЧНЫХ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ССЫЛОЧНЫМ НАЦИОНАЛЬНЫМ СТАНДАРТАМ РОССИЙСКОЙ ФЕДЕРАЦИИ

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименования соответствующего национального стандарта
ИСО/МЭК 7498-1:1994	IDT	ГОСТ Р ИСО/МЭК 7498-1-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель"

ИСО 7498-2:1989	IDT	ГОСТ Р ИСО 7498-2-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации"
ИСО/МЭК 7498-3:1997	-	<*>
ИСО/МЭК 7498-4:1989	IDT	ГОСТ Р ИСО/МЭК 7498-4-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления"
ИСО/МЭК 27000:2009	-	<*>
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"
ИСО/МЭК 27002:2005	-	<*>
ИСО/МЭК 27005:2008	IDT	ГОСТ Р ИСО/МЭК 27005-2010 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности"

<*> Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание. В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:
IDT - идентичные стандарты.