ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 18028-1— 2008

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Сетевая безопасность информационных технологий

Часть 1

Менеджмент сетевой безопасности

ISO/IEC 18028-1:2006
Information technology — Security techniques — IT network security — Part 1: Network security management
(IDT)

Издание официальное

Москва
Стандартинформ
2011

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 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 Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»), Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 523-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 18028-1:2006 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности» (ISO/IEC 18028:2006 «Information technology — Security techniques — IT network security — Part 1: Network security management»)

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

5 ВВЕДЕН ВПЕРВЫЕ

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, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2011

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Обозначения и сокращения . . . 5
5 Структура . . . 6
6 Цель . . . 7
7 Обзор . . . 7
7.1 Общие положения . . . 7
7.2 Процесс идентификации . . . 9
8 Рассмотрение требований корпоративной политики информационной безопасности . . . 12
9 Проверка сетевых архитектур и приложений . . . 12
9.1 Общие положения . . . 12
9.2 Виды сетей . . . 13
9.3 Сетевые протоколы . . . 13
9.4 Сетевые приложения . . . 13
9.5 Технологии, используемые для реализации сетей . . . 14
9.6 Другие соображения . . . 14
10 Идентификация видов сетевых соединений . . . 15
11 Проверка сетевых характеристик и взаимосвязанных доверительных отношений . . . 16
11.1 Сетевые характеристики . . . 16
11.2 Доверительные отношения . . . 17
12 Идентификация рисков информационной безопасности . . . 18
13 Идентификация соответствующих потенциальных сфер контроля . . . 23
13.1 Общие положения . . . 23
13.2 Архитектура сетевой безопасности . . . 23
13.3 Основа безопасного управления услугами . . . 38
13.4 Менеджмент сетевой безопасности . . . 40
13.5 Управление техническими уязвимостями . . . 42
13.6 Идентификация и аутентификация . . . 42
13.7 Протоколирование данных аудита и мониторинг сети . . . 44
13.8 Обнаружение вторжений . . . 45
13.9 Защита от вредоносного кода . . . 46
13.10 Криптографические услуги в общей инфраструктуре . . . 47
13.11 Управление непрерывностью бизнеса . . . 50
14 Реализация и функционирование мер безопасности . . . 51
15 Мониторинг и анализ ввода в эксплуатацию . . . 51
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 52
Библиография . . . 53

Введение

Индустрии телекоммуникаций и информационных технологий ищут рентабельные всесторонние решения по обеспечению безопасности. Безопасная сеть должна быть защищена от злонамеренных и непреднамеренных атак и должна отвечать требованиям бизнеса (деловым требованиям) в отношении конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и услуг. Обеспечение безопасности сети также важно для поддержания подотчетности или информации об использовании при необходимости. Возможности обеспечения безопасности продуктов необходимы для общей сетевой безопасности (включая приложения и сервисы). Однако с ростом числа комбинируемых в целях обеспечения общих решений продуктов функциональная совместимость (или ее отсутствие) будет определять успех решения. Безопасность должна быть не только одним из свойств продукта или услуги, но должна быть разработана таким образом, чтобы способствовать интегрированию возможностей безопасности в общее сквозное решение по обеспечению безопасности. Таким образом, назначение ИСО/МЭК 18028 состоит в том, чтобы предоставить подробное руководство по аспектам безопасности управления и использования сетей информационных систем и их соединений. Лица, отвечающие в организации за обеспечение информационной безопасности в целом и за сетевую безопасность в частности, должны быть способны адаптировать материал настоящего стандарта для своих конкретных потребностей. Его основные цели:

- в ИСО/МЭК 18028-1 — определение и описание концепций, связанных с сетевой безопасностью, и представление руководства по менеджменту сетевой безопасностью, включая методы идентификации и анализа связанных с системами связи факторов, которые следует принимать в расчет для установления требований сетевой безопасности, вместе с ознакомлением с возможными областями контроля и специфическими техническими областями (представленными в последующих частях ИСО/МЭК 18028);
- в ИСО/МЭК 18028-2 — определение стандартной архитектуры безопасности, описывающей последовательную структуру поддержки планирования, проектирования и реализации сетевой безопасности;
- в ИСО/МЭК 18028-3 — определение методов и средств обеспечения безопасности информационных потоков между сетями, использующими шлюзы безопасности;
- в ИСО/МЭК 18028-4 — определение методов и средств обеспечения безопасности удаленного доступа;
- в ИСО/МЭК 18028-5 — определение методов и средств обеспечения безопасности межсетевых соединений, установленных с использованием виртуальных частных сетей (VPN).

ИСО/МЭК 18028-1 представляет интерес для всех лиц, владеющих, управляющих сетями или использующих их, помимо руководителей и администраторов, имеющих конкретные обязанности по обеспечению информационной и/или сетевой безопасности и функционированию сети или же отвечающих за разработку общей программы обеспечения безопасности и политики безопасности организации. В их число входят представители высшего руководства и другие руководители и пользователи, не имеющие технической подготовки.

ИСО/МЭК 18028-2 представляет интерес для персонала, вовлеченного в планирование, проектирование и реализацию аспектов архитектуры сетевой безопасности (например, для сетевых менеджеров, администраторов, инженеров и ответственных за сетевую безопасность).

ИСО/МЭК 18028-3 представляет интерес для персонала, вовлеченного в детальное планирование, проектирование и реализацию шлюзов безопасности (например, для сетевых менеджеров, администраторов, инженеров и ответственных за сетевую безопасность).

ИСО/МЭК 18028-4 представляет интерес для персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности удаленного доступа (например, для сетевых менеджеров, администраторов, инженеров и ответственных за сетевую безопасность).

ИСО/МЭК 18028-5 представляет интерес для персонала, вовлеченного в детальное планирование, проектирование и реализацию безопасности VPN (например, для сетевых менеджеров, администраторов, инженеров и ответственных за сетевую безопасность).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Сетевая безопасность информационных технологий

Часть 1

Менеджмент сетевой безопасности

Information technology. Security techniques. IT network security.
Part 1. Network security management

Дата введения — 2009 — 10— 01

1 Область применения

Настоящий стандарт устанавливает правила по менеджменту сетей и систем связи, включая аспекты безопасности соединения самих сетей информационных систем и соединения удаленных пользователей с ними. Он предназначен для тех, кто отвечает за менеджмент информационной безопасности в целом и сетевую безопасность в частности. Настоящий стандарт дает определение методов идентификации и анализа связанных с системами связи факторов, которые следует принимать в расчет для установления требований сетевой безопасности, дает рекомендации, как идентифицировать соответствующие сферы контроля безопасности, связанные с соединениями сетей связи, а также представляет общий обзор возможных сфер контроля, включая те вопросы технического проектирования и реализации, которые подробно рассмотрены в ИСО/МЭК 18028-2 — ИСО/МЭК 18028-5.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК 13335-1:2004 Информационная технология — Методы и средства обеспечения безопасности — Управление безопасностью информационных и телекоммуникационных технологий — Часть 1: Концепции и модели управления безопасностью информационных и телекоммуникационных технологий (ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management)

ИСО/МЭК 17799:2005 Информационная технология — Методы и средства обеспечения безопасности — Свод правил по менеджменту информационной безопасности (ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management)

ИСО/МЭК 18028-2:2006 Информационная технология — Методы и средства обеспечения безопасности — Сетевая безопасность ИТ — Часть 2: Архитектура сетевой безопасности (ISO/IEC 18028-2:2006, Information technology — Security techniques — IT network security — Part 2: Network security architecture)

ИСО/МЭК 18028-3:2005 Информационная технология — Методы и средства обеспечения безопасности — Сетевая безопасность ИТ — Часть 3: Обеспечение безопасности соединений между сетями с применением шлюзов безопасности (ISO/IEC 18028-3:2005, Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways)

ИСО/МЭК 18028-4:2005 Информационная технология — Методы и средства обеспечения безопасности — Сетевая безопасность ИТ — Часть 4: Обеспечение безопасности удаленного доступа (ISO/IEC 18028-4:2005, Information technology — Security techniques — IT network security — Part 4: Securing remote access)

Издание официальное

ИСО/МЭК 18028-5:2006 Информационная технология — Методы и средства обеспечения безопасности — Сетевая безопасность ИТ — Часть 5: Обеспечение безопасности соединений между сетями с применением виртуальных частных сетей (ISO/IEC 18028-5:2006, Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks)

ИСО/МЭК 18043:2006 Информационная технология — Методы и средства обеспечения безопасности — Выбор, применение и использование систем обнаружения вторжений (ISO/IEC 18043:2006, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems)

ИСО/МЭК ТО 18044:2004 Информационная технология — Методы и средства обеспечения безопасности — Менеджмент инцидентов информационной безопасности (ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины и определения, приведенные в ИСО/МЭК 7498 (все части), ИСО/МЭК 17799 и ИСО/МЭК 13335-1, а также следующие термины с соответствующими определениями:

3.1 **сигнал тревоги** (alert): Моментальное оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие несчастного случая, сбоя или ошибки человека.

3.2 **злоумышленник** (attacker): Любое лицо, намеренно использующее уязвимости технических и нетехнических средств безопасности в целях захвата или компрометации информационных систем и сетей или затруднения доступа авторизованных пользователей к ресурсам информационной системы и сетевым ресурсам.

3.3 **аудит** (audit): официальное исследование, изучение или проверка фактических результатов в сопоставлении с ожидаемыми относительно предполагаемых результатов в целях соответствия и исполнения требований нормативных актов.

3.4 **протоколирование данных аудита** (audit logging): Сбор 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 протоколов аудита.

3.6 **управление непрерывностью бизнеса (деловой деятельностью)** (business continuity management): Процесс, который должен обеспечивать гарантированное восстановление операций в случае возникновения неожиданного или непредусмотренного инцидента, способного оказать негативное воздействие на реализацию важнейших функций бизнеса (деловых функций) и поддерживающих их элементов.

Примечание — Данный процесс должен также обеспечивать восстановление в требуемых порядке очередности и временных рамках, а также возвращение впоследствии всех функций бизнеса (деловых функций) и поддерживающих их элементов обратно в нормальное состояние. Основные элементы этого процесса должны обеспечивать, чтобы необходимые планы и ресурсы были введены и протестированы и чтобы они охватывали информацию, бизнес-процессы, информационные системы и услуги, передачу речевых сообщений и данных, людей и физические средства.

3.7 **Comp128-1**: Запатентованный алгоритм, первоначально использовавшийся по умолчанию в SIM-картах.

3.8 **демилитаризованная зона**; ДМЗ; *экранированная подсеть* (demilitarized zone; DMZ; *screened sub-net*): Пограничный сегмент сети, выполняющий функции «нейтральной зоны» между внешней и внутренней сетями.

Примечание — Она формирует буферную зону безопасности.

3.9 **отказ в обслуживании** (denial of service; DoS): Препятствие санкционированному доступу к ресурсам системы или задержка операций и функций системы.

3.10 **экстранет** (extranet): Расширение сети интранет организации, особенно через инфраструктуру общедоступной сети, делающее возможным коллективное использование ресурсов организацией и другими организациями и лицами, с которыми она имеет дело, предоставляя ограниченный доступ к своей сети интранет.

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 межсетевой экран пропускает 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 нельзя считать интеллектуальными устройствами в общепринятом смысле, они обеспечивают только точки физического соединения для сетевых систем или ресурсов.

3.14 **событие информационной безопасности** (information security event): Идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности.

Примечание — См. ИСО/МЭК ТО 18044.

3.15 **инцидент информационной безопасности** (information security incident): Единичное событие или серия нежелательных или неожиданных событий, связанных с информационной безопасностью, которые со значительной вероятностью способны нанести ущерб бизнес-операциям (деловым операциям) и поставить под угрозу информационную безопасность.

Примечание — См. ИСО/МЭК ТО 18044.

3.16 **менеджмент инцидентов информационной безопасности** (information security incident management): Формальный процесс реагирования на события и инциденты информационной безопасности и осуществления последующих действий.

Примечание — Рекомендации по процессу менеджмента инцидентов информационной безопасности приведены в ИСО/МЭК ТО 18044.

3.17 **Интернет** (internet): Глобальная система взаимосвязанных сетей общего пользования.

3.18 **интранет** (intranet): Частная сеть, развернутая внутри организации.

3.19 **вторжение** (intrusion): Несанкционированный доступ к сети или подсоединенной к сети системе, то есть преднамеренный или случайный несанкционированный доступ к информационной системе, включая злонамеренную деятельность против информационной системы и несанкционированное использование ресурсов в информационной системе.

3.20 **обнаружение вторжений** (intrusion detection): Формальный процесс обнаружения вторжений, обычно включающий сбор сведений об аномальном характере использования, а также о том, какая уязвимость была использована и каким образом, когда и как это произошло.

Примечание — См. ИСО/МЭК 18043.

3.21 **система обнаружения вторжений** (intrusion detection system — IDS): Техническая система, используемая для идентификации того, что была предпринята попытка вторжения, что вторжение происходит или произошло, а также для возможного реагирования на вторжения в информационные системы и сети.

Примечание — Рекомендации по выбору и использованию IDS приведены в ИСО/МЭК 18043.

3.22 **система предупреждения вторжений** (intrusion prevention system — IPS): Разновидность систем обнаружения вторжений, специально предназначенная для обеспечения возможности активного реагирования.

Примечание — См. ИСО/МЭК 18043.

3.23 **флуктуация фазы** (jitter): Одна из форм линейного искажения, вызываемого отклонением передаваемого сигнала от несущей частоты.

3.24 **вредоносное программное обеспечение** (malware): Вредоносное программное обеспечение, например вирусы или «троянский конь», специально разработанное для повреждения или разрушения системы.

3.25 **многопротокольная коммутация меток-признаков** (multiprotocol label switching — MPLS): Метод, разработанный для использования в межсетевой маршрутизации, в соответствии с которым индивидуальным трактам передачи данных или потокам данных присваивают метки и который используют для коммутации соединений на более низком уровне и в дополнение к обычным механизмам протоколов маршрутизации.

Примечание — Коммутацию с помощью меток можно использовать как один из методов создания туннелей.

3.26 **сетевое администрирование** (network administration): Повседневные эксплуатация и управление сетевыми процессами и пользователями.

3.27 **сетевой анализатор** (network analyzer): Устройство, используемое для перехвата и анализа сетевого трафика.

3.28 **сетевой элемент** (network element): Информационная система, которая подсоединена к сети.

Примечание — Подробное описание элемента безопасности дано в ИСО/МЭК 18028-2.

3.29 **сетевой менеджмент** (network management): Процесс планирования, разработки, реализации, эксплуатации, мониторинга и поддержки сети.

3.30 **сетевой мониторинг** (network monitoring): Процесс постоянного наблюдения и анализа зафиксированных данных о сетевой деятельности и операциях, включая протоколы аудита и сигналы тревоги, и взаимосвязанный с этим анализ.

3.31 **политика сетевой безопасности** (network security policy): Совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как следует обеспечивать защиту ее сетевой инфраструктуры и сервисов.

3.32 **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.

3.33 **неприкосновенность частной жизни** (privacy): Право каждого человека на конфиденциальность/неприкосновенность его/ее частной и семейной жизни, жилища и переписки.

Примечание — Власти не должны нарушать неприкосновенность частной жизни. Такое вмешательство происходит в соответствии с законом и является необходимым в демократическом обществе в интересах национальной и общественной безопасности или экономического благосостояния страны, для предотвращения беспорядков или преступлений, для защиты здоровья или моральных устоев или защиты прав и свобод других людей.

3.34 **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.

3.35 **удаленный пользователь** (remote user): Пользователь, находящийся на объекте (площадке, филиале), отличном от того, на котором размещены используемые сетевые ресурсы.

3.36 **маршрутизатор** (router): Сетевое устройство, используемое для организации и контроля потоков данных между различными сетями, которые могут быть основаны на разных сетевых протоколах, путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации. Информация о маршрутизации находится в таблице маршрутизации.

3.37 **параметр безопасности** (security dimension): Совокупность мер и средств безопасности, используемых при рассмотрении конкретного аспекта сетевой безопасности.

Примечание — Подробное описание параметров безопасности дано в ИСО/МЭК 18028-2.

3.38 **домен безопасности** (security domain): Совокупность активов и ресурсов, подчиненных единой политике безопасности.

3.39 **шлюз безопасности** (security gateway): Точка соединения между сетями, между сегментами сетей или между программными приложениями в различных областях безопасности, предназначенная для защиты сети в соответствии с единой политикой безопасности.

Примечание — Подробное описание шлюза безопасности дано в ИСО/МЭК 18028-3.

3.40 **уровни безопасности** (security layers): Иерархия групп сетевого оборудования и мощностей, защищаемых параметрами безопасности.

Примечание — Подробное описание уровней безопасности дано в ИСО/МЭК 18028-2.

3.41 **плоскость безопасности** (security plane): Определенный вид сетевой деятельности, защищаемой параметрами безопасности.

Примечание — Подробное описание плоскости безопасности дано в ИСО/МЭК 18028-2.

3.42 **спаминг** (spamming): Рассылка большого количества незатребованных сообщений, которые по получении неблагоприятно влияют на доступность ресурсов информационной системы.

3.43 **спуфинг** (spoofing): Имитация другого пользователя или сетевого ресурса посредством использования их идентификаторов (учетная запись, IP-адрес).

3.44 **коммутатор** (switch): Устройство, обеспечивающее возможность соединения сетевых устройств посредством внутренних механизмов коммутации.

Примечание — В отличие от других соединительных устройств локальной сети (например, концентраторов) используемая в коммутаторах технология устанавливает соединения на основе «точка–точка». Это обеспечивает возможность того, чтобы сетевой трафик был виден только адресованным сетевым устройствам, и делает возможным одновременное существование нескольких соединений. Технология коммутации обычно может быть реализована на втором или третьем уровне эталонной модели взаимодействия открытых систем.

3.45 **туннель** (tunnel): Тракт передачи данных между сетевыми устройствами, который устанавливают через существующую сетевую инфраструктуру путем использования таких технических приемов, как протокольная инкапсуляция, коммутация с помощью меток-признаков, или виртуальная линия.

3.46 **виртуальная частная сеть** (virtual private network): Логическая вычислительная сеть ограниченного пользования, созданная из системных ресурсов физической сети, например, путем использования шифрования и/или туннельных каналов виртуальной сети через реальную сеть.

4 Обозначения и сокращения

Примечание — Следующие приводимые обозначения и сокращения использованы во всех частях ИСО/МЭК 18028.

3G — Система цифровой мобильной связи третьего поколения
ACL — Список управления доступом
ADSL — Асимметричная цифровая абонентская линия
ATM — Асинхронный режим передачи
CDPD — Сотовая цифровая передача пакетов данных
CDMA — Многостанционный доступ с кодовым разделением каналов
CLID — Идентификатор линии вызова
CLNP — Протокол сетевого обслуживания без установления соединения
CRM — Управление взаимосвязями с клиентами
DNS — Служба доменных имен
DoS — Отказ в обслуживании
EDGE — Улучшенные скорости передачи данных для развития GSM-стандарта
EDI — Электронный обмен данными
EGPRS — Улучшенный общий сервис пакетной радиопередачи
EIS — Информационная система предприятия
FTP — Протокол передачи файлов
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
IP — Интернет-протокол
ISP — Интернет-провайдер
MPLS — Многопротокольная коммутация меток-признаков
MRP — Планирование производственных ресурсов
NAT — Трансляция сетевых адресов
NIDS — Система обнаружения сетевых вторжений
NTP — Синхронизирующий сетевой протокол
OOB — Внеполосный
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
SSH — Безопасная оболочка
TCP — Протокол передачи данных транспортного уровня с установлением сеанса связи
TDMA — Многостанционный доступ с временным разделением каналов
Telnet — Программа эмуляции терминала для работы в Интернете на удаленном компьютере
TETRA — Наземная транкинговая радиостанция
TKIP — Протокол целостности временного ключа
UDP — Пакетный протокол передачи данных транспортного уровня
UMTS — Универсальная система мобильной связи
USB — Универсальная последовательная шина
VoIP — Передача голоса по IP
VPN — Виртуальная частная сеть
WAP — Протокол приложений для беспроводной связи
WEP — Протокол шифрования для беспроводной связи
WLAN — Беспроводная локальная сеть
WORM — С однократной записью и многократным считыванием
ГВС — Глобальная сеть
ДМЗ — Демилитаризованная зона
ИБП — Источник бесперебойного питания
ИТ — Информационная технология
КПК — Носимый (карманный) персональный компьютер, «наладонник»
ЛВС — Локальная сеть
ОВЧ — Очень высокая частота
ПК — Персональный компьютер

5 Структура

Использованный в настоящем стандарте подход состоит в том, чтобы:

- сначала рассмотреть в целом весь процесс идентификации и анализа связанных с системами связи факторов, которые следует принимать в расчет для установления требований сетевой безопасности;

- затем обозначить потенциальные области контроля в отношении безопасности связанных с соединениями сетей связи и соединениями между ними. В процессе этого определяют, где могут быть использованы соответствующие требования из ИСО/МЭК 13335-1 и ИСО/МЭК 17799, и идентифицируют области технического проектирования и реализации со ссылками на последующие части настоящего стандарта — ИСО/МЭК 18028-2 — ИСО/МЭК 18028-5.

Далее необходимо описать три простых критерия, которые могут помочь лицам, отвечающим за информационную безопасность, идентифицировать потенциальные области контроля. С помощью этих критериев идентифицируют:

- различные виды сетевых соединений;
- различные сетевые характеристики и взаимосвязанные доверительные отношения;
- потенциальные виды риска безопасности, связанного с сетевыми соединениями (и использованием услуг, предоставляемых через эти соединения).

Результаты комбинирования этих критериев затем используют для идентификации потенциальных областей контроля. Далее по тексту настоящего стандарта следуют краткие описания потенциальных областей контроля с указанием источников, содержащих дополнительную информацию.

В настоящем стандарте рассмотрены следующие области:

- архитектура сетевой безопасности, охватывающая:
  - организацию локальной сети;
  - организацию глобальной сети;
  - беспроводные сети;
  - радиосети;
  - организацию широкополосной сети;
  - шлюзы безопасности (см. также ИСО/МЭК 18028-3);
  - сервисы удаленного доступа (см. также ИСО/МЭК 18028-4);
  - VPN (см. также ИСО/МЭК 18028-5);
  - IP-конвергенцию (данные, голос, видео);
  - разрешение доступа к услугам, предоставляемым сторонними (по отношению к организации) сетями;
  - архитектуру веб-хостинга;
- безопасная структура управления услугами;
- менеджмент сетевой безопасности;
- управление техническими уязвимостями;
- идентификация и аутентификация;
- протоколирование данных аудита и мониторинг сети;
- обнаружение вторжений;
- защита от вредоносного кода;
- общая инфраструктура криптографических услуг;
- управление непрерывностью бизнеса;
- реализация и функционирование средств безопасности, мониторинг и анализ реализации.

6 Цель

Цель настоящего стандарта заключается в том, чтобы предоставить:

- руководство для идентификации и анализа связанных с системами связи факторов, которые следует принимать в расчет при установлении требований сетевой безопасности;
- обозначение потенциальных областей контроля, включая те, которые детально рассмотрены в ИСО/МЭК 18028-2 — ИСО/МЭК 18028-5.

7 Обзор

7.1 Общие положения

Информационные системы большинства государственных и коммерческих организаций связаны сетями, причем масштабы ведения электронного бизнеса на глобальной основе все время увеличиваются. Эти сетевые соединения могут быть организованы в рамках организации, между разными организациями и между организацией и широкой общественностью.

Действительно, бурное развитие технологии общедоступных сетей, в особенности Интернета, предоставляет огромные возможности для ведения бизнеса и оказания электронных государственных услуг. Эти возможности простираются от предоставления более дешевой информационной связи с использованием Интернета в качестве глобального средства связи до более сложных услуг Интернет-провайдеров. Это означает использование относительно дешевых локальных точек подключения на каждом конце ли-

нии связи до полномасштабных систем электронной торговли и предоставление услуг, использующих сервисы и приложения, основанные на Интернет-технологии. Кроме того, новые технологии, включающие объединение данных и голоса, расширяют возможности для использования бизнес-моделей, предусматривающих мобильную и/или удаленную работу сотрудников. Это позволяет служащим работать вдали от базы значительную часть времени, поддерживая контакт путем использования средств удаленного доступа, таких, как модемные подключения, или все чаще встречающихся беспроводных соединений для установления связи с корпоративной сетью и получения доступа к информации и услугам поддержки бизнеса.

Таким образом, одновременно с деловыми преимуществами эта среда также создает новые риски безопасности, требующие осуществления менеджмента. В связи с тем что организации в значительной степени зависят от информации для ведения своей деловой деятельности, утрата конфиденциальности, целостности, доступности, неотказуемости, подотчетности, подлинности и достоверности информации и услуг может оказывать неблагоприятное воздействие на бизнес-операции. Следовательно, существует важнейшее требование обеспечения защиты информации и осуществления менеджмента безопасности информационных систем внутри организации.

Пример типового построения сети, которое используют в настоящее время во многих организациях, представлен на рисунке 1.

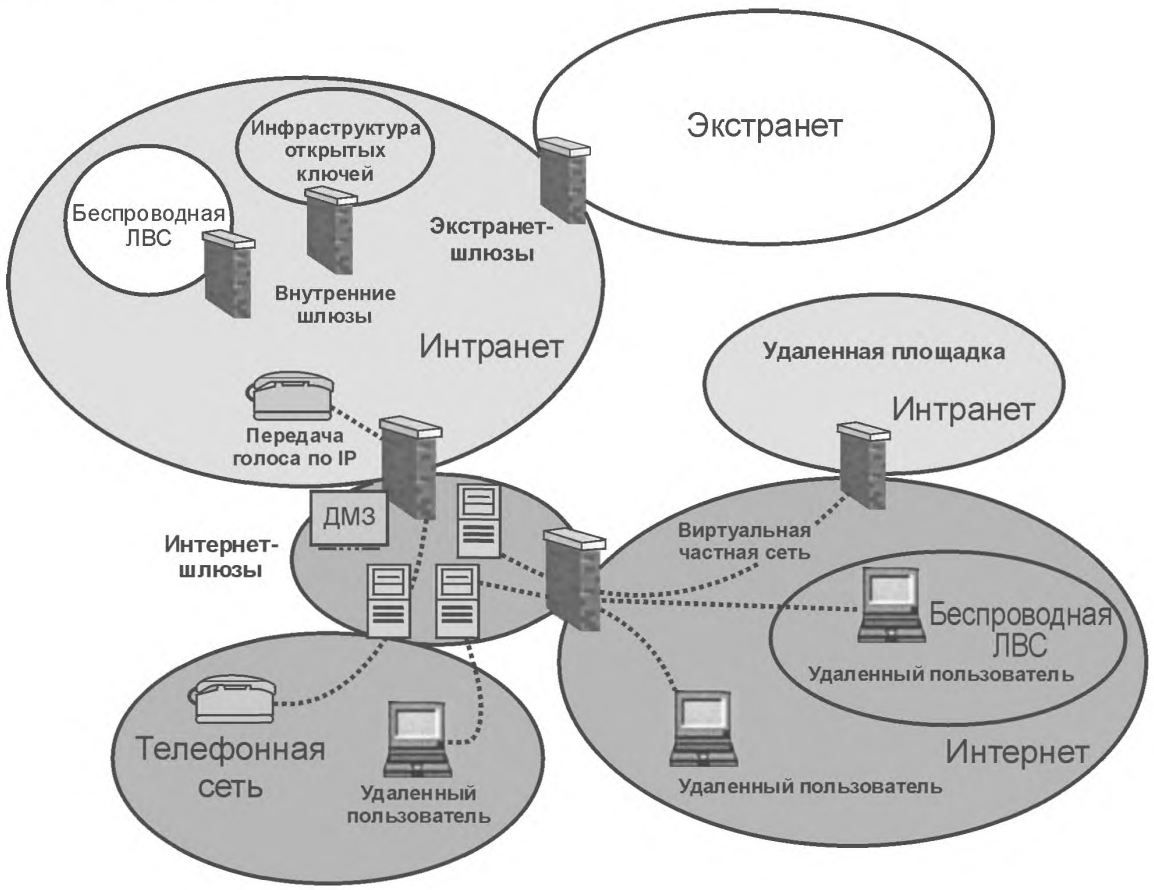

Рисунок 1 — Типовое построение сетевой среды

Интранет — внутренняя сеть, используемая и поддерживаемая организацией. Обычно только работающие в организации лица имеют прямой физический доступ к этой сети, а поскольку сеть расположена в пределах помещений, находящихся во владении организации, можно легко достичь определенного уровня физической защиты. В большинстве случаев интранет неоднороден в плане использованных технологий и требований безопасности; он может включать инфраструктуры, требующие более высокого уровня

защиты, чем предоставляемый интранетом. Управление такими инфраструктурами, например важнейшими частями среды инфраструктуры открытых ключей, может осуществляться в выделенном сегменте интранета. С другой стороны, определенные технологии могут требовать некоторого изолирования, потому что они вносят дополнительные риски, например инфраструктуры беспроводной ЛВС. В обеих ситуациях для реализации этого сегментирования можно использовать внутренние шлюзы безопасности.

В наше время потребности бизнеса большинства организаций делают необходимыми связь и обмен данными с внешними партнерами и другими организациями. Часто связь с большинством важнейших партнеров по бизнесу осуществляют способом, прямо расширяющим интранет в сторону сети организации-партнера; для таких расширений обычно используют термин «экстранет». Поскольку доверие к подключенным организациям-партнерам в большинстве случаев ниже, чем в пределах самой организации, для устранения рисков, вносимых этими соединениями, используют шлюзы безопасности сети экстранет.

Кроме того, общедоступные сети, в основном Интернет, используют сегодня для обеспечения средств связи и обмена данными с партнерами и клиентами (включая общественность) по оптимизированной стоимости 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 специфические компоненты для учета требований различных форм расширения сети интранет, а также для связи с партнерами и клиентами.

Удаленные пользователи могут быть подсоединены посредством технологии VPN, кроме того, они могут использовать беспроводные средства связи, такие, как общественные 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 использовать телефонную сеть.

Если организация решает использовать технологии VoIP для реализации внутренней телефонной сети, то обычно также присутствуют соответствующие шлюзы безопасности для телефонной сети.

Хотя технологии, используемые в таком типичном сценарии организации сети, во многих отношениях предоставляют расширенные возможности и преимущества для бизнеса, например путем снижения или оптимизации расходов, они также приводят к довольно сложным видам среды и обычно вносят новые риски информационной безопасности. Следовательно, должна осуществляться надлежащая оценка рисков, вносимых этими видами среды, а оцененные риски должны уменьшаться путем реализации соответствующих средств контроля безопасности.

Другими словами, благоприятные возможности бизнеса, предлагаемые этими новыми видами среды, необходимо сопоставлять с рисками, возникающими при использовании новых технологий. Например, Интернет имеет ряд технических свойств, которые могут вызывать беспокойство с точки зрения безопасности. Он первоначально проектировался в расчете на установление соединения, а не исходя из соображений безопасности, и многие из обычно используемых основных протоколов не являются в своей основе безопасными. Преимущество Интернета состоит в том, что это очень открытая система, первоначально разработанная научно-исследовательским сообществом во исполнение требований проектов правительства США, с широкой публикацией результатов и свободным распространением программных средств и спецификаций. Это способствовало популярности и быстрому росту Интернета. Однако именно эти популярность и открытость создают значительную уязвимость в плане безопасности. В глобальной среде есть большое количество людей, имеющих способности, знания и склонность к получению доступа к лежащим в ее основе механизмам и протоколам и созданию проблем безопасности, простирающихся от несанкционированного доступа до крупномасштабного отказа в обслуживании.

Подводя итог, можно сказать, что успешное использование коммерческими и государственными организациями возможностей, предлагаемых современными сетями, зависит от того, в какой степени возможно контролировать риски функционирования в открытой среде и осуществлять их менеджмент.

В 7.2 кратко изложены рекомендуемый процесс идентификации и анализа связанных с системами связи факторов, которые следует учитывать при установлении требований сетевой безопасности, и указания потенциальных контролируемых областей (сфер). Подробное изложение этого процесса предоставлено в последующих разделах.

7.2 Процесс идентификации

При рассмотрении вопроса сетевых соединений все лица в организации, чьи обязанности связаны с соединениями, должны отчетливо сознавать требования и интересы бизнеса. Кроме того, они должны

осознавать риски безопасности для таких сетевых соединений и соответствующие сферы контроля. Требования и интересы бизнеса, вероятно, будут влиять на многие решения и действия, предпринимаемые в процессе рассмотрения вопроса сетевых соединений, идентификации потенциальных сфер контроля и в конечном счете выбора, проектирования, реализации и поддержки защитных мер безопасности. Поэтому об этих требованиях и интересах бизнеса следует помнить на протяжении всего процесса. Для идентификации соответствующих требований безопасности, связанных с сетью, и сфер контроля необходимо решить следующие задачи (см. также ИСО/МЭК 17799):

- пересмотреть общие требования безопасности для сетевых соединений, сформулированные в корпоративной политике информационной безопасности организации[1] (см. раздел 8);
- проверить сетевые архитектуры и приложения, связанные с сетевыми соединениями, для обеспечения необходимой подготовки решения последующих задач (см. раздел 9);
- идентифицировать вид (виды) сетевых соединений, подлежащих рассмотрению (см. раздел 10);
- проверить предложенные сетевые характеристики (чему при необходимости будет способствовать имеющаяся информация о сетевых архитектурах и приложениях) и соответствующие доверительные отношения (см. раздел 11);
- где возможно, определить взаимосвязанные виды рисков безопасности с помощью результатов оценки рисков и проводимой руководством проверки, включая рассмотрение ценности для бизнес-операций информации, которая будет передаваться через соединения, и любой другой информации, потенциально доступной несанкционированным образом через эти соединения, а также рассмотрение других предоставляемых услуг[2] (см. раздел 12);
- идентифицировать сферы контроля, соответствующие виду (видам) сетевых соединений, сетевым характеристикам и взаимосвязанным доверительным отношениям, а также видам определенных рисков безопасности, и параллельно документировать и проверять варианты технической архитектуры безопасности, и согласовать предпочтительный вариант[3] (см. раздел 13);
- реализовать и ввести в действие меры безопасности (см. раздел 14);
- осуществлять постоянный мониторинг и проверку реализации мер безопасности[4] (см. раздел 15).

Следует отметить, что общие рекомендации по определению мер безопасности содержатся в ИСО/МЭК 17799. Настоящий стандарт является дополнением к этому стандарту в части определения соответствующих сфер контроля безопасности, связанных с сетевыми соединениями, и к стандартам ИСО/МЭК 18028-2 — ИСО/МЭК 18028-5.

На приведенном ниже рисунке 2 представлен общий процесс идентификации и анализа связанных с системами связи факторов, которые следует учитывать для установления требований сетевой безопасности, и обозначения потенциальных сфер контроля. Каждый этап процесса описан более подробно в разделах, следующих за рисунком 2.

---

[1] Это будет включать позицию этой политики в отношении: 1) регулятивных и законодательных требований безопасности, связанных с сетевыми соединениями, которые определены соответствующими регулятивными или законодательными органами (включая национальные правительственные органы); 2) классификации данных, которые будут храниться или передаваться в сети.

[2] Это будет включать: 1) оценку рисков, связанных с потенциальными нарушениями необходимых предписаний и законов, относящихся к сетевым соединениям, которые определены соответствующими регулятивными или законодательными органами (включая национальные правительственные органы); 2) использование установленных потенциальных неблагоприятных воздействий на бизнес, подтверждающих классификацию данных, которые будут храниться или передаваться в сети.

[3] Этот раздел будет включать средства контроля, необходимые для соблюдения предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулятивными или законодательными органами (включая национальные правительственные органы).

[4] Этот раздел будет включать мониторинг и проверку средств контроля, необходимых для соблюдения предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулятивными или законодательными органами (включая национальные правительственные органы).

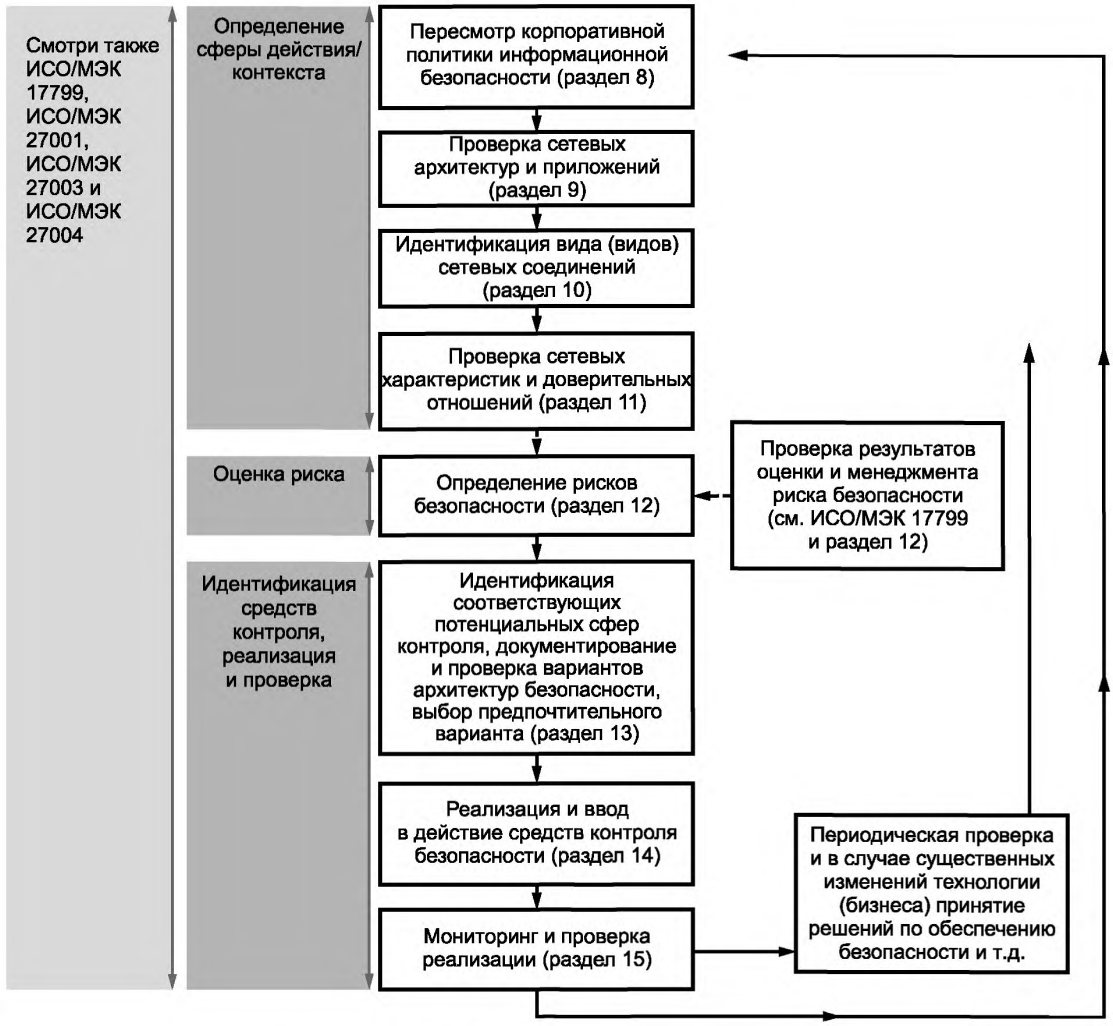

Рисунок 2 — Процесс менеджмента в контексте сетевой безопасности

На рисунке 2 сплошные черные линии представляют основное направление процесса, а пунктирная черная линия — место, где могут быть определены виды рисков безопасности с помощью результатов оценки рисков безопасности и проводимой руководством проверки.

Кроме основного направления процесса на некоторых этапах возникает потребность повторного возвращения к результатам более ранних этапов для обеспечения согласованности, в частности, к этапам «Пересмотр корпоративной политики информационной безопасности» и «Проверка сетевых архитектур и приложений».

- после определения видов рисков безопасности может возникнуть потребность пересмотра корпоративной политики информационной безопасности вследствие возникновения некоторых фактов, которые не охвачены на этом уровне политики;

- при определении потенциальных сфер контроля должна быть учтена корпоративная политика информационной безопасности, потому что она может, например, определять, что конкретная защитная мера должна быть реализована во всей организации независимо от рисков;

- при проверке вариантов архитектуры безопасности необходимо рассматривать сетевые архитектуры и приложения для обеспечения их совместимости.

8 Рассмотрение требований корпоративной политики информационной безопасности

Корпоративная политика информационной безопасности организации может включать формулировки необходимости обеспечения конфиденциальности, целостности, доступности, неотказуемости, подотчетности, подлинности и достоверности, а также определения видов угроз и требования контроля, которые непосредственно связаны с сетевыми соединениями.

Например, такая политика может утверждать, что:

- главная задача — доступность определенных видов информации или услуг;
- все соединения через коммутируемые линии запрещены;
- все соединения с Интернетом следует осуществлять через шлюз безопасности;
- следует использовать определенный вид шлюза безопасности;
- любое платежное поручение (предписание) недействительно без цифровой подписи.

Такие формулировки, определения и требования, будучи применимыми в масштабах организации или сообщества, следует учитывать при определении видов рисков безопасности (см. раздел 12) и определении потенциальных сфер контроля для сетевых соединений (см. раздел 13). Если существуют любые подобные требования безопасности, они должны быть изложены в предварительном (черновом) списке потенциальных сфер контроля и при необходимости отражены в вариантах архитектуры безопасности. Рекомендации по статусу документации корпоративной политики информационной безопасности в части подхода организации к обеспечению информационной безопасности и по ее содержанию и взаимосвязи с другой документацией по безопасности установлены в стандартах ИСО/МЭК 13335-1 и ИСО/МЭК 17799.

9 Проверка сетевых архитектур и приложений

9.1 Общие положения

Как упоминалось в настоящем стандарте, существуют этапы утверждения потенциальных мер безопасности, требующихся для сети:

- определение вида (видов) используемых сетевых соединений;
- определение сетевых характеристик и взаимосвязанных доверительных отношений;
- определение рисков безопасности;
- разработка списка необходимых сфер контроля[1)] и соответствующих проектов.

Следовать этим этапам всегда необходимо в контексте сетевой архитектуры и приложений, которые уже существуют или только планируются.

Соответственно должны быть получены подробности о соответствующей сетевой архитектуре и приложениях, которые должны быть проверены в целях обеспечения необходимого понимания последующих этапов процесса.

В результате уяснения этих аспектов на самой ранней стадии в процессе установления соответствующих критериев определения требований безопасности, определения сфер контроля, проверки вариантов архитектуры технической безопасности и принятия решения о целесообразности одного из них с точки зрения эффективности будут созданы условия для принятия более рационального решения по обеспечению безопасности.

Рассмотрение архитектурных аспектов безопасности сети и приложений на самой ранней стадии даст время для проверки этих архитектур и возможной модификации, если приемлемое решение по обеспечению безопасности не может быть практически достигнуто в текущей архитектуре.

Области, требующие рассмотрения, включают:

- виды сетей;
- сетевые протоколы;
- сетевые приложения;
- технологии, использованные для реализации сетей.

Некоторые вопросы для рассмотрения в каждой из этих сфер обсуждены в 9.2—9.6. В разделе 10 представлены рекомендации по идентификации видов сетевых соединений, а в разделе 11 — рекомендации по определению сетевых характеристик и взаимосвязанных доверительных отношений. В разделе 12

[1)] Подразумеваются сферы контроля, связанные с использованием криптографии, для обеспечения конфиденциальности, целостности и аутентификации.

представлены рекомендации по идентификации рисков безопасности. (Общее руководство по сетевым архитектурам и приложениям можно найти в ИСО/МЭК 7498.)

9.2 Виды сетей

В зависимости от охватываемой ими области сети можно классифицировать как:

- ЛВС, которые используют для локального соединения систем;
- ГВС, которые используют для соединения систем с охватом вплоть до мирового.

(Некоторые источники также используют термин «региональная вычислительная сеть» для локально ограниченной глобальной сети, например в пределах города. Однако в настоящее время для таких сетей используют те же технологии, что и для глобальных сетей, поэтому существенных различий между региональной и глобальной сетью больше не существует. Кроме того, для целей настоящего стандарта персональные сети будут отнесены к ЛВС.)

9.3 Сетевые протоколы

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

- протоколы разделяемой среды в основном используют в ЛВС, и они обеспечивают механизмы регулирования использования разделяемой среды между соединенными системами. При использовании разделяемой среды вся информация в сети физически доступна всем подсоединенным системам;
- протоколы маршрутизации используют для определения маршрутов через различные узлы, по которым передают информацию в ГВС. Информация физически доступна для всех систем вдоль маршрута, и маршрутизация может быть изменена случайно или намеренно;
- протоколы MPLS (многопротокольной коммутации меток-признаков), на которых основаны разные виды сетей, предоставляющих услуги связи, позволяют многим частным сетям делить базовую сеть, предоставляющую услуги связи, причем ни один из членов какой-либо частной сети не знает о существовании других частных сетей, совместно использующих эту базовую сеть. Протоколы MPLS в основном применяют в VPN, где для идентификации и разделения трафика, принадлежащего разным VPN, используют метки-признаки (VPN, основанная на MPLS, не основана на механизмах шифрования данных). Это 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 соединения сетевых услуг, таких, как передача речи и данных в сети, с использованием механизмов качества обслуживания для обеспечения функционирования в режиме реального времени.

Многие протоколы, используемые в сетях, не обеспечивают безопасность. Например, для извлечения паролей из сетевого трафика злоумышленники обычно используют инструментальные средства. Это делает приложения, посылающие незашифрованные пароли через общедоступные сети, крайне уязвимыми.

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

9.4 Сетевые приложения

Виды приложений, используемых в сети, должны быть рассмотрены в контексте безопасности. Эти виды могут включать:

- приложения «тонкого» клиента;
- настольные приложения;
- приложения на основе эмуляции терминала;
- инфраструктуры и приложения обмена сообщениями;
- приложения «хранить и направить» или основанные на буферизации;
- приложения «клиент-сервер».

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

- приложения обмена сообщениями (такие, как шифрование и электронные цифровые подписи для сообщений) могут обеспечивать адекватный уровень безопасности без реализации специальных мер безопасности в сети;
- для реализации соответствующих функциональных возможностей приложения «тонкого» клиента могут требовать загрузки мобильного кода. Так как конфиденциальность может быть менее важной проблемой в этом контексте, чем целостность, для обеспечения вышеуказанного сеть должна предоставлять соответствующие механизмы. В качестве альтернативы при условии выполнения более строгих требова-

ний электронная цифровая подпись мобильного кода обеспечит целостность и дополнительную аутентификацию. Часто это осуществляется в самой структуре приложения, поэтому необходимости предоставления этих услуг в сети может не возникнуть;

- приложения типа «хранить и направить» или основанные на буферизации приложения обычно временно хранят важные данные для дальнейшей обработки в промежуточных узлах. Требования целостности и конфиденциальности для обеспечения защиты данных во время транзита в сети потребуют соответствующих мер безопасности. Однако из-за временного хранения данных на промежуточных хостах этих мер безопасности может быть недостаточно. Таким образом, могут быть востребованы дополнительные меры безопасности для защиты данных, хранящихся на промежуточных хостах.

9.5 Технологии, используемые для реализации сетей

Сети могут быть организованы различными средствами. Общую структуру этих средств определяют географические пространства, охватываемые сетью.

9.5.1 Локальные сети

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 коллективное использование таких ресурсов, как принтер, и совместное использование файлов и приложений. Также ЛВС обычно обеспечивают централизованные услуги типа обмена сообщениями или электронного календаря. В некоторых случаях ЛВС также используют для замены традиционной функции других сетей, например, когда протоколы и сервисы VoIP предоставляются в качестве замены телефонной сети на основе офисной АТС. Небольшие ЛВС чаще всего реализуют с использованием технологии с разделяемой пропускной способностью. Ethernet-протокол представляет собой стандартную технологию, которая была расширена для обеспечения более высокой пропускной способности, а также для поддержки беспроводной среды. Поскольку технологии с разделяемой пропускной способностью, и в частности Ethernet, имеют ограничения в сетях большего размера, в среде ЛВС также используют типичные технологии ГВС, например маршрутизируемые протоколы. ЛВС могут иметь проводную или беспроводную основу.

9.5.1.1 Проводная ЛВС

Проводная ЛВС обычно состоит из узлов, соединенных в сеть через сетевой коммутатор или концентратор посредством сетевых кабелей, которые могут обеспечивать возможности высокоскоростной передачи данных. Широко известные технологии ЛВС включают Ethernet (IEEE 802.3) и Token Ring (IEEE 802.5).

9.5.1.2 Беспроводная ЛВС

Беспроводная локальная сеть (БВС) использует радиоволны высокой частоты для передачи сетевых пакетов по воздуху. Ее уникальность заключается в быстроте организации ЛВС без необходимости прокладки проводов. Широко известные технологии БВС включают реализации IEEE 802.11 и Bluetooth.

9.5.2 Глобальные вычислительные сети

Глобальные вычислительные сети (ГВС) используют для соединения удаленных пунктов и их ЛВС. ГВС может быть создана с использованием кабелей и каналов связи провайдера услуг или, что происходит более часто, путем аренды услуги у провайдера сетей связи. Технологии ГВС делают возможным передачу и маршрутизацию сетевого трафика на большие расстояния и обычно обеспечивают широкие возможности маршрутизации для направления сетевых пакетов в ЛВС нужного пункта назначения. Обычно для связи между собой ЛВС используют физическую общедоступную сетевую инфраструктуру, например выделенные линии, спутниковую связь или волоконно-оптические кабели. ГВС может быть проводной или беспроводной.

9.5.2.1 Проводная ГВС

Проводная ГВС обычно состоит из устройств маршрутизации (например, маршрутизаторов), соединенных с общедоступной или частной сетью телекоммуникационными кабелями. Широко известные технологии проводной глобальной сети включают АТМ, ретрансляцию кадров и протоколы X.25.

9.5.2.2 Беспроводная ГВС

Беспроводная ГВС обычно использует радиоволны для передачи сетевых пакетов по воздуху на большие расстояния, которые могут составлять до десяти километров или более. Широко известные технологии беспроводной глобальной сети включают TDMA, CDMA, GSM и протокол IEEE 802.16.

9.6 Другие соображения

При рассмотрении сетевой архитектуры и приложений следует также обратить внимание на существующие внутри организации сетевые соединения, исходящие из организации или входящие в нее, а

также на сеть, с которой предполагается осуществить соединение. Существующие соединения организации могут ограничивать или не допускать создание новых соединений, например, из-за заключенных соглашений или контрактов. Существование других соединений у сети, к которой требуется подсоединение, может привести к появлению дополнительных уязвимостей и, следовательно, более высоких рисков, что оправдывает применение более строгих и/или дополнительных мер безопасности.

10 Идентификация видов сетевых соединений

Существует много общих видов сетевых соединений, которые могут быть востребованы организацией или сообществом. Некоторые из этих видов соединений можно осуществлять через частные сети (доступ к которым ограничен определенным сообществом), а некоторые — через общедоступные сети (доступ к которым потенциально возможен любой организации или лицу). Кроме того, эти виды сетевых соединений можно использовать для различных услуг, например электронной почты или электронного обмена данными. Также можно использовать средства Интернета, интранета или экстранета, каждому из которых присущи различные подходы, связанные с обеспечением безопасности. Каждый вид соединений может иметь различную степень уязвимости и, следовательно, связанные с ней риски безопасности, поэтому в конечном итоге для каждого вида может потребоваться различный набор мер безопасности (см. ИСО/МЭК 17799).

Приведенная ниже таблица 1 показывает один из способов классификации общих видов сетевых соединений, которые могут потребоваться для ведения бизнеса, с описательным примером для каждого вида.

Обращая должное внимание на соответствующие сетевые архитектуры и приложения (см. раздел 9), следует выбрать один или несколько видов из представленных в таблице 1 в качестве видов, отвечающих требованиям рассматриваемого сетевого соединения (соединений).

Следует отметить, что описанные в настоящем стандарте общие виды сетевых соединений структурированы и классифицированы скорее с точки зрения бизнеса, чем с технической точки зрения. Это означает, что два различных вида сетевых соединений иногда могут быть реализованы с использованием сходных технических средств и что в некоторых случаях меры безопасности могут быть сходными, но есть и другие случаи, в которых они будут различными.

Таблица 1 — Виды сетевых соединений

Обозначение	Вид сетевого соединения	Пример описания
A	Соединение в пределах единственного контролируемого местоположения организации	Соединение между различными частями одной и той же организации в пределах одного и того же контролируемого местоположения, то есть единственного контролируемого строения или площадки
B	Соединение между разными географически разделенными частями одной и той же организации	Соединение между региональными офисами (и/или региональными офисами с центральной площадкой) в рамках единой организации через ГВС. При этом виде сетевого соединения большинство, если не все пользователи, имеют возможность получить доступ к информационным системам через сеть, но не у всех пользователей в пределах организации будет санкционирование для доступа ко всем приложениям или информации (то есть доступ каждого пользователя будет осуществляться только в соответствии с предоставленными привилегиями). Одним из видов доступа из другой части организации может быть доступ для целей удаленного технического обслуживания. Этому виду пользователей и соединений может присваиваться больше привилегий доступа
C	Соединения между площадкой организации и персоналом, работающим вдали от организации	Использование мобильных терминалов данных служащими (например, продавцом, проверяющим доступность товара с площадки клиента) или установление удаленной связи с вычислительными системами организации служащими, работающими дома или на других удаленных площадках, не связанных сетью, поддерживаемой организацией. При этом виде сетевого соединения пользователь авторизуется как системный пользователь в своей ЛВС

Окончание таблицы 1

Обозначение	Вид сетевого соединения	Пример описания
D	Соединения между разными организациями в пределах замкнутого сообщества, например, из-за договорных или других юридически обязательных ситуаций или из-за сходных интересов бизнеса, например банковских услуг или страхования	Соединение между двумя или более организациями, где существует потребность бизнеса в облегчении электронных транзакций между организациями (например, электронный перевод платежей в банковской индустрии). Этот вид сетевого соединения сходен с описанным выше видом B, за исключением того, что связанные между собой площадки принадлежат двум или более организациям и что соединение не предназначено для предоставления доступа к полному спектру приложений, используемых каждой из организаций-участниц
E	Соединения с другими организациями	Это может быть доступ к удаленным базам данных, поддерживаемым другими организациями (например, через провайдеров услуг). При таком виде сетевого соединения всех пользователей, включая пользователей подключаемой организации, индивидуально заранее авторизует внешняя организация, к чьей информации предоставляется доступ. Однако, хотя все пользователи заранее авторизуются, здесь может не быть иной проверки потенциальных пользователей, кроме проверки, связанной с их способностью платить за предлагаемые услуги. Это может быть также доступ к приложениям в системах организации, хранящим или обрабатывающим информацию организации, который может быть предоставлен пользователям из внешних организаций. В этих обстоятельствах внешние пользователи будут известными и авторизованными. Одним из видов доступа из другой организации может быть доступ для целей удаленного технического обслуживания. Этому виду пользователей и соединений может быть присвоено больше привилегий доступа
F	Соединения с общедоступным доменом	Пользователи организации могут инициировать доступ к общедоступным базам данных, веб-сайтам и/или службам электронной почты (например, через Интернет), при этом доступ инициируют для таких целей, как поиск информации или передача информации от/к лицам и/или площадкам, которые не были специально заранее авторизованы организацией. При этом виде соединения пользователи организации могут использовать это средство для целей организации (возможно, даже частных); однако контроль организации над передаваемой информацией может быть лишь незначительным, если вообще он будет иметься. Внешними пользователями может быть инициирован доступ к средствам организации (например, через Интернет). При этом виде сетевого соединения доступ индивидуальных внешних пользователей заранее не был специально санкционирован организацией
G	Соединения с телефонной сетью общего пользования из IP-среды	Может быть инициирован доступ к коммутируемой сети общего пользования с телефона в IP-сети. Такие соединения являются неконтролируемыми, так как звонки могут приниматься из любой точки мира

11 Проверка сетевых характеристик и взаимосвязанных доверительных отношений

11.1 Сетевые характеристики

Сетевые характеристики существующей или предлагаемой сети необходимо проверять. Особенно важно идентифицировать, является ли сеть:

- общедоступной сетью — сетью, которая доступна каждому; или

- частной сетью, например сетью, состоящей из находящихся в собственности или выделенных линий и поэтому считающейся более безопасной, чем общедоступная сеть.

Также важно знать вид передаваемых сетью данных, например:

- сеть передачи данных — сеть, передающая главным образом данные и использующая протоколы передачи данных;

- сеть передачи голоса — сеть, предназначенная для телефона, но также пригодная для передачи данных;

- сеть, объединяющая передачу данных, передачу голоса и (возможно) передачу видеосигналов.

Также значима следующая информация:

- является ли сеть пакетной сетью или коммутируемой сетью;

- поддерживает ли она качество обслуживания, например, в сети, работающей на основе MPLS.

Примечание — Качество обслуживания означает поддержание стабильности характеристик. Сетевые услуги пригодны при обеспечении минимального уровня характеристик (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 необходимости.

11.2 Доверительные отношения

Когда характеристики существующей или предлагаемой сети идентифицированы и, как минимум, установлено, является ли сеть общедоступной или частной (см. 11.1), должны быть идентифицированы взаимосвязанные доверительные отношения.

Во-первых, необходимо определить степень доверия применимой среды (вида среды), связанной с сетевым соединением (соединениями), путем выбора из представленного ниже списка:

- среда с низкой степенью доверия, такая, как сеть с неизвестным кругом пользователей;

- среда со средней степенью доверия, такая, как сеть с известным кругом пользователей и в пределах замкнутого бизнес-сообщества (из нескольких организаций);

- среда с высокой степенью доверия, такая, как сеть с известным кругом пользователей только в пределах организации.

Во-вторых, чтобы установить доверительные отношения, соответствующая степень доверия среды (низкая, средняя и высокая) должна быть связана с применимой сетевой характеристикой (общедоступная или частная сеть) и видом (видами) задействованного сетевого соединения (от A до G). Это может быть выполнено с использованием матрицы, подобной таблице 2.

Таблица 2 — Идентификация доверительных отношений

Виды сетевых соединений (см. раздел 10)		Степень доверия среды		
		Низкая	Средняя	Высокая
Сетевые характеристики	Общедоступная	F G	D E	B C
	Частная	E	D E	A B C

На основе таблицы 2 должна быть определена справочная информация по описаниям характеристик для соответствующих категорий доверительных отношений. Описания всех возможных категорий доверительных отношений представлены в таблице 3.

Таблица 3 — Характеристика доверительных отношений

Категория доверительных отношений	Описание
Низкая/общедоступная	Низкая степень доверия и использование общедоступной сети
Средняя/общедоступная	Средняя степень доверия и использование общедоступной сети
Высокая/общедоступная	Высокая степень доверия и использование общедоступной сети
Низкая/частная	Низкая степень доверия и использование частной сети
Средняя/частная	Средняя степень доверия и использование частной сети
Высокая/частная	Высокая степень доверия и использование частной сети

Эта справочная информация должна быть использована при работе с разделом 12 для подтверждения видов рисков безопасности и идентификации потенциальных сфер контроля.

Выполнение этой задачи может при необходимости быть поддержано доступной информацией, имеющейся в сетевых архитектурах и приложениях (полученной при использовании раздела 9).

12 Идентификация рисков информационной безопасности

Как было отмечено выше, в настоящее время большинство организаций зависят от использования информационных систем и сетей для поддержки своих бизнес-операций. Кроме того, во многих случаях существует четко выраженное требование бизнеса в отношении использования сетевых соединений между информационными системами на каждой площадке организации, а также с другими местоположениями как внутри организации, так и за ее пределами, включая соединения с общедоступной сетью. При установлении соединения с другой сетью следует проявлять значительную осторожность для обеспечения того, чтобы организация, которая подключается, не подвергалась дополнительным рискам (вследствие потенциальных угроз, исходящих от уязвимостей). Эти риски могут исходить, например, от самого соединения или от сетевых соединений на другом конце сети.

Некоторые из этих рисков могут быть связаны с обеспечением соблюдения соответствующего законодательства и положений. Особое внимание следует уделять законам о неприкосновенности частной жизни и защите данных. В некоторых странах приняты законы, устанавливающие защитные меры для сбора, обработки и передачи персональных данных, то есть данных, которые могут быть связаны с конкретным лицом или лицами. В зависимости от соответствующего национального законодательства такие меры безопасности могут налагать специфические обязанности на лиц, собирающих, обрабатывающих и распространяющих персональную информацию через сети, а также могут ограничить возможность передачи этих данных в определенные страны, создавая дополнительные проблемы, связанные с безопасностью. К менее очевидным примерам передачи данных, поднадзорных такому законодательству, относят некоторые аппаратные средства и IP-адреса.

Отраженные в настоящем разделе виды риска связаны с проблемами несанкционированного доступа к информации, несанкционированной передачи информации, внесения вредоносного программного обеспечения, отказа от приема или источника информации, отказа в обслуживании и недоступности информации или услуг. Таким образом, виды рисков безопасности, с которыми может сталкиваться организация, связаны с утратой:

- конфиденциальности информации и кода (в сетях и системах, соединенных с сетями);
- целостности информации и кода (в сетях и системах, соединенных с сетями);
- доступности информации и сетевых услуг (и систем, соединенных с сетями);
- неотказуемости сетевых транзакций (обязательств);
- подотчетности сетевых транзакций;
- аутентичности информации (а также сетевых пользователей и администраторов);
- достоверности информации и кода (в сетях и системах, соединенных с сетями);
- способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов, включая осуществление этого в контексте политики безопасности организации (например, продажа полосы пропускания или использование полосы пропускания для собственной выгоды) и обязанностей в отношении законодательства (например, хранение детской порнографии).

Не все виды рисков безопасности относят к каждому местоположению или к каждой организации. Однако должны быть идентифицированы соответствующие виды рисков безопасности, с тем чтобы могли быть установлены потенциальные сферы контроля (и в конечном счете выбраны, спроектированы, реализованы и поддержаны меры безопасности).

Концептуальная модель сетевой безопасности, показывающая, где могут возникать разные виды рисков безопасности, представлена на рисунке 3.

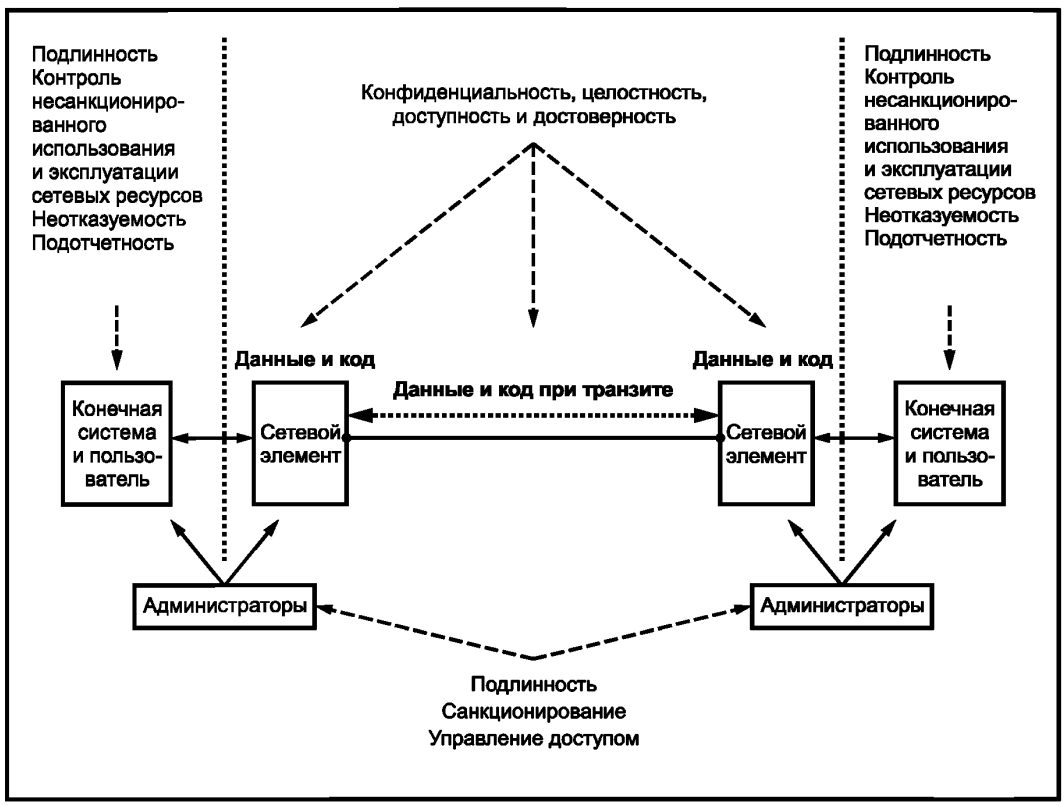

Рисунок 3 — Концептуальная модель сфер риска сетевой безопасности

Должна быть собрана информация о последствиях для бизнес-операций, связанных с упомянутыми видами рисков безопасности, при этом необходимо учитывать конфиденциальность или значимость используемой информации (выраженная как потенциальное неблагоприятное воздействие на бизнес) и связанные с ними потенциальные угрозы и уязвимости. В связи с этим, если существует вероятность более чем незначительного неблагоприятного воздействия на бизнес-операции организации, следует обратиться к таблице 3.

Нужно подчеркнуть, что при выполнении этой задачи следует использовать результаты оценки риска безопасности и проверки (проверок)[1)], проведенных высшим руководством в отношении сетевого соединения (соединений). Эти результаты дадут возможность сосредоточиться до той степени подробностей, с какой была проведена проверка (проверки), на потенциальных неблагоприятных воздействиях на бизнес, связанных с перечисленными выше видами рисков безопасности, а также на видах угроз, уязвимостей и, следовательно, представляющих проблему рисков.

При рассмотрении сетевых уязвимостей во время оценки риска безопасности и проводимой руководством проверки может возникнуть необходимость отдельного рассмотрения ряда сетевых аспектов. В приведенной ниже таблице 4 перечислены виды уязвимостей, которые могут быть использованы для каждого сетевого аспекта.

[1)] Руководство по подходам к оценке и менеджменту риска безопасности приведено в ИСО/МЭК 17799.

Таблица 4 — Виды потенциальных уязвимостей

Сетевой аспект	Виды потенциальных уязвимостей сетевой безопасности				
	Прерывание	Перехват	Модификация	Вторжение	Обман
Сетевые пользователи	Пользователи могут страдать от утраты или прерывания услуг	Транзакции пользователей и/или сетевая деятельность могут быть под контролем	Подробности о пользователях и данные пользователей могут быть модифицированы или разрушены	Пользователи могут быть имитированы для получения несанкционированного доступа к средствам	Пользователи могут быть имитированы для проведения мошеннических транзакций
Сетевые конечные системы	Конечные системы могут стать временно или надолго недоступными	Неуполномоченные лица могут прочесть данные или код на конечных системах	Данные или код могут быть модифицированы или разрушены	Конечные системы могут быть имитированы для получения несанкционированного доступа к средствам. Неуполномоченные лица могут получить доступ к учетным записям системы и использовать их в целях начала дальнейших атак	Конечные системы могут быть имитированы для проведения мошеннических транзакций или начала дальнейших атак
Сетевые приложения	Приложения могут стать временно или надолго недоступными	Данные или код могут быть перехвачены во время передачи или прочитаны на серверах неуполномоченными лицами	Данные или код могут быть модифицированы или разрушены	Неуполномоченные лица могут получить доступ к учетным записям системы и использовать их в целях начала дальнейших атак	Неуполномоченные лица могут получить доступ к учетным записям системы и использовать их в целях начала дальнейших атак
Сетевые сервисы	Сервисы могут стать временно или надолго недоступными	Данные или код могут быть перехвачены во время передачи или прочитаны на серверах неуполномоченными лицами	Данные или код могут быть модифицированы или разрушены	Неуполномоченные лица могут получить доступ к учетным записям системы и использовать их в целях начала дальнейших атак	Сетевые серверы и устройства могут быть имитированы для получения несанкционированного доступа, перехвата сетевого трафика или нарушения сетевых сервисов
Сетевая инфраструктура	Средства могут стать временно или надолго недоступными			Неуполномоченные лица могут совершить проникновение в физические средства	

Используя в качестве основного ориентира результаты оценки риска и проводимой высшим руководством проверки, на основе раздела 11 следует определить соответствующие характеристики доверительных отношений и представить в верхней строке таблицы 5, где создающие проблему воздействия указаны в левой графе таблицы. Затем необходимо отметить ссылки на соответствующие пересечения. Это ссылки на потенциальные сферы контроля, которые представлены в разделе 13.

Таблица 5 — Виды рисков безопасности и ссылки на потенциальные сферы контроля

Виды рисков	Ссылки на доверительные отношения					
	Низкая/ общедоступная	Средняя/ общедоступная	Высокая/ общедоступная	Низкая/ частная	Средняя/ частная	Высокая/ частная
Потеря конфиденциальности	13.2.1[1)] 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.2 13.10.5 —
Потеря целостности	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.3 13.10.5 —

[1)] Применение 13.2.1 зависит от конкретного сетевого сценария.

Окончание таблицы 5

Виды рисков	Ссылки на доверительные отношения					
	Низкая/ общедоступная	Средняя/ общедоступная	Высокая/ общедоступная	Низкая/ частная	Средняя/ частная	Высокая/ частная
Потеря доступности	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.11 —
Потеря неотказуемости	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.8 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.4 13.10.5 13.11 —

Следует отметить, что таблица 5 явно указывает на то, что чем более доверенным является пользователь, тем более необходимыми становятся меры безопасности. Для этого существуют две причины.

Во-первых, существует комплекс мер безопасности, описанных в ИСО/МЭК 17799 и поэтому не повторяющихся в данном документе, которые должны быть выбраны для обеспечения защиты хостов, включая меры безопасности для идентификации и аутентификации и логического управления доступом. В ситуациях с низкой степенью доверия надежность мер безопасности для идентификации и аутентификации и логического управления доступом должна быть выше, чем в ситуациях с высокой степенью доверия. Если это нельзя обеспечить, должны быть реализованы соответствующие дополнительные меры безопасности. Конфигурация разрешений (привилегий) в ситуациях с низкой степенью доверия должна помочь обеспечить предоставление доступа только к тем ресурсам, которые согласованы с моделью доверия и требованиями предполагаемого доступа.

Во-вторых, доверенным пользователям обычно предоставляют доступ к более важной/критичной информации и/или функциональным возможностям. Потребность в дополнительных мерах безопасности в данном случае — показатель значимости ресурсов, к которым получен доступ, а не степень доверия к пользователям.

13 Идентификация соответствующих потенциальных сфер контроля

13.1 Общие положения

На основе результатов оценки риска и проводимой высшим руководством проверки, а также с помощью ссылок, идентифицированных в результате использования раздела 12, должны быть идентифицированы и выбраны из раздела 13 (а также из ИСО/МЭК 17799) потенциальные сферы контроля. В 13.2 рассмотрены различные аспекты архитектуры сетевой безопасности и взаимосвязанные потенциальные сферы контроля, а 13.3—13.11 знакомят с другими взаимосвязанными потенциальными сферами контроля. Конкретное решение по обеспечению безопасности может в действительности охватывать ряд потенциальных сфер контроля, представленных в 13.2—13.11.

Следует подчеркнуть, что существует базовый комплекс мер безопасности, имеющих отношение к информационным системам независимо от наличия любых сетевых соединений, которые будут выбраны путем использования ИСО/МЭК 17799.

Список идентифицированных потенциальных мер безопасности должен быть тщательно проверен в контексте соответствующих сетевых архитектур и приложений. Список должен быть скорректирован по мере необходимости и в последующем использован в качестве основы для реализации необходимых мер безопасности (см. раздел 14), а затем мониторинга и проверки реализации (раздел 15).

13.2 Архитектура сетевой безопасности

13.2.1 Общие положения

Документирование возможных вариантов архитектуры безопасности представляет собой средство для изучения различных решений и основу для анализа компромиссов. Оно также облегчает разрешение проблем, связанных с техническими ограничениями и часто возникающим конфликтом между потребностями бизнеса и потребностями безопасности.

При документировании вариантов должное внимание следует уделять любым требованиям корпоративной политики информационной безопасности (см. раздел 8), релевантной сетевой архитектуре и сетевым приложениям (см. раздел 9), а также перечню потенциальных сфер контроля, идентифицированных путем использования разделов 12 и 13. При выполнении этого следует принимать в расчет любые существующие варианты архитектуры безопасности. Когда варианты будут документально оформлены и проверены как часть процесса проектирования технической архитектуры, предпочтительная архитектура безопасности должна быть согласована и представлена в документе «Спецификации контроля проектирования технической архитектуры безопасности» (который совместим с проектом технической архитектуры и наоборот). Затем могут быть произведены изменения сетевой архитектуры безопасности и приложений (для обеспечения совместимости с предпочтительной архитектурой безопасности) и/или перечня потенциальных мер безопасности (например, потому что достигнута договоренность, что архитектура безопасности может быть технически реализована только определенным способом, неизбежно влекущим за собой альтернативу определенной мере безопасности).

Следует отметить, что в ИСО/МЭК 18028-2 описано «Указание по архитектуре безопасности[1)]», которое очень полезно в качестве базисной точки:

[1)] В контексте ИСО/МЭК 18028-2 «Указание» взято для обозначения одного из примеров того, как представлять техническую архитектуру безопасности на очень высоком уровне. Возможны другие примеры.

- для описания последовательной структуры поддержки планирования, проектирования и реализации сетевой безопасности;

- определения общих связанных с безопасностью элементов архитектуры, которые в случае надлежащего применения могут обеспечить комплексную сетевую безопасность.

На основе «Указания по архитектуре безопасности» в настоящем стандарте представлены описания различных архитектур технической безопасности, необходимых для учета сегодняшних требований и требований ближайшего будущего, которые далее развиваются в ИСО/МЭК 18028-3 — ИСО/МЭК 18028-5.

Принципы, описанные в «Указании по архитектуре безопасности», применимы к любому виду современной сети, будь это сеть передачи данных, речевых сообщений или конвергентная сеть, беспроводная сеть или радиосеть, и могут быть использованы независимо от технологии сети или местоположения в стеке протоколов. В нем рассмотрены вопросы безопасности, связанные с управлением, контролем и использованием сетевой инфраструктуры, сервисов и приложений, и предоставляется всесторонняя нисходящая комплексная перспектива сетевой безопасности. «Указание по архитектуре безопасности» имеет три архитектурных компонента:

- объемы (размеры) безопасности (которые могут быть также определены как «группы мер безопасности»);

- уровни безопасности (которые могут быть также определены как «элементы сетевой безопасности»);

- области (сферы) безопасности (которые могут быть также определены как «домены безопасности»).

Методы (направления) безопасности — это совокупности защитных мер безопасности, предназначенные для рассмотрения конкретного аспекта сетевой безопасности. В «Указании по архитектуре безопасности» определены восемь таких совокупностей, которые распространяются на приложения и информацию конечных пользователей, в том числе:

- неотказуемость;

- конфиденциальность данных;

- целостность данных;

- доступность.

Для комплексного решения по обеспечению безопасности методы (направления) безопасности нужно применить к иерархии групп сетевого оборудования и аппаратуры, которые называют уровнями безопасности:

- уровень безопасности инфраструктуры;

- уровень безопасности сервисов (услуг);

- уровень безопасности приложений.

Уровни безопасности выстраивают один над другим для обеспечения сетевых решений, то есть уровень безопасности инфраструктуры инициирует уровень безопасности сервисов, а уровень безопасности сервисов инициирует уровень безопасности приложений, и определяют, где путем предоставления последовательной перспективы сетевой безопасности необходимо реализовать безопасность как при принятии решений, так и продуктов непосредственно.

Уровень безопасности инфраструктуры представлен сетевыми средствами передачи данных, а также отдельными частями сети, защищенными механизмами, которые реализованы для объемов безопасности. Примеры компонентов, принадлежащих к уровню безопасности инфраструктуры, — отдельные маршрутизаторы, коммутаторы и серверы, а также линии связи между отдельными маршрутизаторами, коммутаторами и серверами.

Безопасность услуг, предоставляемых провайдерами своим клиентам, рассматривают на уровне безопасности сервисов (услуг). Эти услуги варьируются от базового транспортирования и связности до средств поддержки сервисов, подобных тем, которые необходимы для предоставления доступа к Интернету (например, сервисы аутентификации, авторизации и учета, динамической конфигурации хостов, имен доменов и т. д.), сервисов с дополнительными возможностями, таких, как услуга бесплатной передачи голоса, качество обслуживания, VPN и т. д.

Уровень безопасности приложений сосредоточен на безопасности сетевых приложений, к которым имеют доступ клиенты провайдера услуг. Эти приложения, запускаемые в работу сетевыми сервисами, включают базовые приложения передачи файлов (например, протоколы FTP) и просмотра веб-страниц, основные приложения, такие, как справочная служба, сетевые голосовые сообщения и электронная почта, а также приложения высокого уровня, такие, как управление взаимоотношениями с клиентами, электронная/мобильная торговля, онлайновое обучение, сотрудничество с использованием видеотехники, и т. д.

Плоскости безопасности — это определенные виды сетевой деятельности, защищаемые механизмами, которые реализованы для объемов безопасности. «Указание по архитектуре безопасности» определяет три плоскости безопасности, представляющие виды защищаемой деятельности, которая осуществляется в сети:

- плоскость сетевого менеджмента;
- плоскость сетевого контроля и сигнализации;
- плоскость конечных пользователей.

В этих плоскостях рассматриваются конкретные потребности безопасности, связанные соответственно с мероприятиями сетевого менеджмента, мероприятиями сетевого контроля и сигнализации и деятельностью конечных пользователей. Сети должны быть спроектированы таким образом, чтобы события в одной плоскости безопасности оставались, насколько это допустимо, изолированными от других плоскостей безопасности.

Последующие разделы знакомят с различными аспектами реальных технических архитектур безопасности, относящимися к различным сферам организации сети.

Необходимо подчеркнуть, что архитектура технической безопасности для любого проекта должна быть полностью документально описана и согласована, прежде чем будет окончательно сформирован список мер безопасности для реализации.

13.2.2 Организация локальной сети

13.2.2.1 Общие положения

При использовании ЛВС в пределах физически защищенных областей (участков), например только в пределах собственных помещений организации, риски, вероятно, будут таковы, что потребуются только базовые технические защитные меры. Однако в случае их использования в более широкой среде, а также при использовании беспроводных технологий (см. 13.2.4) одна только физическая защита вряд ли будет гарантировать приемлемый уровень безопасности. Кроме того, технологии с разделяемой пропускной способностью, наиболее часто используемые в ЛВС, делают возможным доступ ко всему сетевому трафику с любой системы, использующей разделяемую пропускную способность.

ПК представляет собой уязвимую область, так как является пользовательским интерфейсом. Если ПК не блокируется, существует вероятность установки пользователем в ЛВС несанкционированного программного обеспечения. Серверы, используемые в корпоративной сети, как те, которые предназначены для Интернета, так и внутренние серверы, не имеющие непосредственного соединения с Интернетом, служат источником потенциального риска безопасности. Хотя большинство служб ИТ утверждают, что они внимательно относятся к применению патчей по мере их доступности, к этому риску нужно относиться очень серьезно, так как даже крупным организациям не удавалось своевременно установить патчи на все серверы, что приводило к разрушению «червями» внутреннего сетевого трафика.

13.2.2.2 Риски безопасности

В проводных ЛВС риски безопасности создаются узлами, физически соединенными с сетью. Основные риски безопасности, связанные с локальными сетями, вызываются:

- несанкционированным доступом и изменениями, вносимыми в ПК, серверы и другие соединенные с ЛВС устройства;
- серверами, на которых не установлены патчи;
- низким качеством паролей;
- хищением аппаратных средств;
- нарушениями энергоснабжения;
- импортом вредоносного программного обеспечения посредством электронной почты и доступом к веб-страницам;
- неудачей резервного копирования локальных жестких дисков;
- отказом аппаратных средств, таких, как жесткие диски;
- несанкционированными соединениями с ЛВС (лэптопы);
- несанкционированным доступом к концентраторам или коммутационным стойкам;
- паролями по умолчанию на портах управления концентраторов и коммутаторов;
- недостаточной физической защитой.

13.2.2.3 Меры безопасности

Поддержание безопасности пространства ЛВС требует обеспечения защиты компонентов ЛВС и подсоединенных устройств. Таким образом, мерами безопасности для защиты среды ЛВС могут быть:

- физические меры безопасности и меры безопасности, связанные с влиянием окружающей 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 камер слежения (наблюдения) для предотвращения несанкционированного выноса оборудования с площадки (из помещения);

- обеспечение хранения концентраторов и маршрутизаторов ЛВС в физически защищенных шкафах в безопасных помещениях связи;

- использование ИБП с автоматическим отключением для критических устройств и пользователей ПК, если они не хотят потерять находящуюся в процессе выполнения работу;

- аппаратные и программные меры безопасности:

- конфигурирование устройств с частными IP-адресами;

- строгая политика паролей;

- требование протоколирования на каждой рабочей станции с использованием по крайней мере пары «идентификатор пользователя/пароль»;

- установка антивирусного программного обеспечения и его регулярное автоматическое обновление;

- реализация безопасных установок протоколирования;

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

- зеркальное копирование накопителей сервера (или реализация RAID) для обеспечения избыточности;

- удаление ненужного программного обеспечения;

- организационные меры безопасности:

- документирование установок программного обеспечения и безопасности для использования в будущем при конфигурировании новых рабочих станций;

- планирование периодического скачивания и установки патчей для операционной системы;

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

- реализация протокола для фиксирования проблем технического обслуживания и неправильного использования рабочих станций;

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

- обеспечение режима резервного копирования;

- обеспечение изменения паролей по умолчанию на всех концентраторах и коммутаторах;

- установка соответствующих имен сообщества/паролей в протоколе сетевого управления;

- надлежащее формирование протоколов в случае доступности и реализация процедур их контроля;

- планирование периодической установки обновленных версий программно-аппаратных средств;

- 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 сети устройств на предмет наличия уязвимости.

13.2.3 Организация глобальной сети

13.2.3.1 Общие положения

Традиционная ГВС была первоначально создана с использованием фиксированных линий связи между помещениями (узлами), арендуемыми у провайдеров услуг, причем провайдер услуг выполняет минимальную управленческую деятельность, связанную с этими линиями связи, помимо обеспечения их функционирования. Однако развитие технологии ГВС привело к перекладыванию ответственности за управление на провайдера услуг с выгодой для организации, заключающейся в отсутствии необходимости развертывать собственную сеть и управлять ею. Это означает, что ответственность по обеспечению безопасности менеджмента сети возлагается на провайдера услуг. Кроме того, поскольку ГВС главным образом используется для направления сетевого трафика на большие расстояния, функция маршрутизации должна быть

хорошо защищена, чтобы исключить вероятность направления сетевого трафика в представляющую неверный пункт назначения ЛВС. Таким образом, проходящий через локальную сеть трафик подвержен перехвату лицами, имеющими доступ к инфраструктуре ГВС. Поскольку инфраструктура ГВС более доступна, чем инфраструктура ЛВС, следует соблюдать осторожность, обеспечивая шифрование передаваемой через среду ГВС значимой информации. С провайдером услуг должен быть заключен контракт, в котором должно быть обговорено условие демонстрации уровня безопасности, необходимого организации.

13.2.3.2 Риски безопасности

Хотя проводная ГВС разделяет основные риски безопасности с проводной ЛВС (см. 13.2.2), ее использование подразумевает большее число рисков безопасности вследствие более значительной подверженности воздействию сетевого трафика в ГВС, что означает необходимость наличия средств контроля, включая средства контроля доступа, для обеспечения того, чтобы проводную ГВС было нелегко скомпрометировать, вызывая тем самым широко распространяющееся нарушение. Аналогичным образом, хотя беспроводная ГВС разделяет основные риски безопасности с беспроводной ЛВС (см. 13.2.2), она более подвержена разрушению из-за возможностей преднамеренных помех в системе, используемой для передачи сетевых пакетов. Основные риски безопасности, связанные с ГВС, включают:

- вторжение, когда происходит раскрытие информации или целостность данных не может быть гарантирована;
- атаки отказа в обслуживании, когда ресурсы становятся недоступными для уполномоченных пользователей;
- учетные записи для коммутируемого доступа в Интернет и соединений с внешней стороной для личного использования дома, которые легко могут обходить любые защитные меры, реализованные на сетевом и серверном уровнях, подвергая корпоративную сеть воздействию имеющихся в электронной почте «червей», «троянских коней» и других вирусов;
- запаздывание, которое будет оказывать влияние на голосовую передачу через IP-сервисы;
- флуктуацию фазы в сети, которая будет оказывать влияние на качество голосовой передачи (вызываемую главным образом в результате использования медных кабелей для поставки услуг);
- сбой устройств;
- повреждение кабеля;
- устройства с неустановленными патчами;
- потерю электроснабжения на транзитной площадке, затрагивающую многие другие площадки;
- средства сетевого управления провайдера услуг.

13.2.3.3 Средства контроля безопасности

Основные средства контроля безопасности, необходимые для обеспечения защиты ГВС, включают:

- замену небезопасных по своей природе протоколов, таких, как Telnet и FTP, на безопасные протоколы, такие, как SSH и SCP;
- шифрование каналов управления;
- реализацию безопасной аутентификации для получения доступа к устройствам ГВС с соответствующей подачей сигнализации для устройств с использованием отчетности SNMP;
- обеспечение безопасности физического оборудования ГВС на каждой площадке, такое, как использование запираемых шкафов с сигнализацией;
- использование ИБП для обеспечения защиты от нарушения энергоснабжения;
- двойное соединение площадок с использованием разных маршрутов;
- активный последовательный опрос устройств ГВС;
- составление схемы сетевых устройств для идентификации несанкционированных устройств;
- средство управления патчами;
- шифрованные оверлеи для значимых данных;
- получение гарантий сервиса от провайдера услуг по таким вопросам, как задержка и флуктуация фазы;
- реализацию аудита и подотчетности для доступа к устройствам ГВС;
- использование межсетевых экранов, отвергающих любой неожиданный входящий трафик;
- обеспечение того, чтобы структура MPLS и адреса были скрытыми;
- присвоение IP-адресов, которые не могут быть маршрутизированы через Интернет;
- использование трансляции сетевых адресов, которая скрывает внутренние IP-адреса, но позволяет устройствам с немаршрутизируемыми адресами делать запросы из Интернета;

- использование антивирусного программного обеспечения, чтобы помешать вредоносному программному обеспечению, такому, как «троянские кони», «черви» и другие вирусы, открывать лазейки в безопасности изнутри сети;
- использование систем обнаружения вторжений для идентификации подозрительного трафика;
- обеспечение логической безопасности систем сетевого управления;
- обеспечение физической безопасности мест сетевого управления;
- обеспечение резервного копирования устройств;
- проведение проверок надежности персонала, занимающегося сетевым менеджментом.

13.2.4 Беспроводные сети

13.2.4.1 Общие положения

Беспроводные сети определены 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 беспроводными локальными сетями. Основные используемые технологии стандартизированы в документах на основе IEEE 802.11. Следует подчеркнуть, что беспроводные сети составляют категорию сетей, отличную от радиосетей, таких, как GSM, 3G и ОВЧ, так как те используют антенные мачты для передачи (см. 13.2.5).

БВС страдают от всех уязвимостей проводных локальных сетей и вдобавок от некоторых особых уязвимостей, связанных с характеристиками беспроводной связи. Для рассмотрения вопроса этих дополнительных уязвимостей были разработаны особые технологии (главным образом основанные на шифровании), хотя у более ранних версий этих технологий (например, протокол шифрования в беспроводной связи WEP) имелись слабые места архитектуры, и поэтому они не соответствовали требованиям конфиденциальности.

13.2.4.2 Риски безопасности

Основные сферы рисков безопасности, связанные с использованием беспроводных локальных сетей, включают:

- подслушивание;
- несанкционированный доступ;
- взаимные и преднамеренные помехи;
- неправильную конфигурацию;
- отключение по умолчанию безопасного режима доступа;
- некорректные протоколы WEP или TKIP;
- некорректный SNMP, используемый для управления БВС;
- возможные затруднения с идентификацией конкретного пользователя БВС.

13.2.4.3 Средства контроля безопасности

Средства контроля безопасности, необходимые для БВС, включают:

- организацию межсетевой защиты БВС от корпоративной инфраструктуры;
- реализацию VPN на основе IPsec через БВС между клиентом и периметровым межсетевым экраном;
- рассмотрение вопроса улучшения безопасности каждого устройства БВС путем конфигурирования персональных межсетевых экранов, программных средств обнаружения вторжений и антивирусного программного обеспечения на клиентском устройстве;
- контроль уровня передаваемого сигнала для исключения распространения за пределы физической сферы организации;
- конфигурирование SNMP на доступ только для чтения;
- управление сетью по дополнительному шифрованному каналу, например используя SSH;
- поддержку физической безопасности точек беспроводного доступа;
- повышение прочности любых серверных компонентов;
- тестирование системы;
- рассмотрение вопроса использования системы обнаружения вторжений между корпоративной сетью и БВС.

13.2.5 Радиосети

13.2.5.1 Общие положения

Радиосети определены как сети, использующие радиоволны в качестве средства связи для охвата географически обширных областей. Типичными примерами радиосетей являются сети сотовой связи, ис-

пользующие такие технологии, как GSM или UMTS, и предоставляющие общедоступные сервисы голосовой связи и передачи данных.

Следует подчеркнуть, что сети, использующие радиоволны для охвата небольших областей, рассматриваются как другая категория (см. 13.2.4).

Примеры радиосетей включают:

- TETRA (наземная транкинговая радиосеть);
- GSM (глобальная система мобильной связи);
- 3G (включая UMTS — универсальная система мобильной связи);
- GPRS (пакетная радиосвязь общего назначения);
- CDPD (сотовая система передачи пакетов цифровых данных);
- CDMA (многостанционный доступ с кодовым разделением каналов).

13.2.5.2 Риски безопасности

Существует ряд общих сценариев угроз безопасности, связанных с рисками, применимыми к радиосетям, включая:

- подслушивание;
- перехват сеанса связи;
- выдачу себя за другое лицо (персонация);
- угрозы прикладного уровня, например мошенничество;
- отказ в обслуживании.

Примеры рисков в контексте некоторых видов радиосетей представлены ниже.

Риски безопасности, связанные с GSM:

- алгоритмы A5/x и Comp128-1 не являются стойкими;
- GSM-шифрование обычно отключено;
- возможно клонирование SIM-карт.

Риски безопасности, связанные с 3G:

- телефоны уязвимы для электронных атак, включая внесение вредоносного программного обеспечения, например вирусов;
- возможности атак высоки, потому что телефоны обычно включены;
- услуги могут подвергаться подслушиванию;
- в радиосетях могут быть преднамеренные помехи;
- возможно введение ложных базовых станций;
- возможен несанкционированный доступ к шлюзам;
- возможны атаки услуг и несанкционированный доступ к услугам через Интернет;
- возможно внесение спама;
- системы управления подвержены несанкционированному доступу через RAS;
- услуги подвержены атакам посредством потерянного или похищенного оборудования инженерно-технической помощи, включая КПК.

UMTS является основным представителем глобального семейства технологий 3G и предоставляет существенные возможности широкополосной передачи и пропускной способности для поддержки большего числа клиентов голосовой связи и передачи данных. Она использует полосу частот шириной 5 МГц на одну несущую 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 простирающимися от 2·10 до 2·20 МГц, для снижения расходов на развертывание 3G-сетей.

GPRS — существенный шаг вперед к сетям 3G, так как возросли 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 или 13,4 Кбит TDMA таймслотов общей пропускной способностью 72,4 или 107,2 Кбит. GPRS поддерживает 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, что может стать проблемой безопасности. GPRS-провайдер обычно старается повысить безопасность связи, обеспечивая межсетевой экран между GPRS-сетью и Интернетом, но это должно быть сконфигурировано так, чтобы дать возможность правомерным сервисам работать, и следовательно, не может быть использовано третьей стороной.

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 RC4 поточный шифр с 40-битовыми ключами для шифрования. CDPD определена в стандарте IS-732. Алгоритм не является стойким и может быть дешифрован методом полного перебора.

CDMA — форма расширенного спектра — является семейством методов цифровой связи, которые использовались в течение многих лет. Основной принцип расширенного спектра — использование шумоподобных несущих, имеющих большую ширину полосы пропускания, чем требуется для простой прямой связи при одной и той же скорости передачи данных. Технология цифрового кодирования позволяет CDMA предупреждать подслушивание, намеренное или случайное. Технология CDMA разбивает звук на фрагменты, проходящие по расширенному спектру частот. Каждый фрагмент 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. Поскольку существуют миллионы кодовых комбинаций, доступных для любого звонка, это обеспечивает защиту от подслушивания.

13.2.5.3 Средства контроля безопасности

Существует ряд технических средств контроля безопасности для осуществления менеджмента рисков радиосетей от идентифицированных угроз:

- надежная аутентификация;
- шифрование с эффективными алгоритмами;
- защищенные базовые станции;
- межсетевые экраны;
- защита от вредоносного программного обеспечения (вирусы, «троянский конь» и т. д.);
- антиспам.

13.2.6 Организация широкополосной сети

13.2.6.1 Общие положения

Широкополосные сети — это группа технологий, позволяющая индивидуальным абонентам осуществлять высокоскоростной доступ к точке присутствия сети Интернет. В настоящее время существует четыре основные технологии:

- 3G;
- кабельная;
- спутниковая;
- DSL.

Что касается DSL, существуют два основных вида: асимметричная (ADSL), где скорость потока от пользователя ниже (от четверти до половины скорости потока к пользователю), и симметричная (SDSL), где скорости потоков 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 эта технология постоянного подключения высокоскоростная и стоит дешевле традиционных систем связи. Все технологии делают возможным доступ в Интернет и, следовательно, простираются только от Интернета до помещений абонента. Использование Интернета в качестве универсальной службы связи позволяет быстро и дешево организовывать линии связи с другими площадками, возможно, с развертыванием VPN для безопасных линий связи.

13.2.6.2 Риски безопасности

Широкополосная связь — это просто высокоскоростная линия связи постоянного подключения между абонентом и Интернетом. Эти свойства делают подрывную деятельность против подключенной к широкополосной связи системы легкой задачей для хакеров и непосредственно ведут к следующим рискам:

- раскрытие, модификация или удаление информации в результате несанкционированного удаленного доступа;
- распространение вредоносного программного обеспечения;
- прием/передача и выполнение несанкционированных программ;
- кража личных данных;
- неправильное конфигурирование систем клиента;
- внесение программных уязвимостей;
- сетевой затор;
- отказ в обслуживании.

13.2.6.3 Средства контроля безопасности

Существует ряд технических средств контроля безопасности для осуществления менеджмента рисков широкополосной связи от идентифицированных угроз, включая:

- межсетевые экраны для малого домашнего офиса;
- программные средства защиты от вредоносного программного обеспечения (включая вирусы);
- системы обнаружения вторжений, включая системы предупреждения вторжений;
- VPN;
- исправленные версии программ/патчи.

13.2.7 Шлюзы безопасности

13.2.7.1 Общие положения

Соответствующий механизм шлюза безопасности должен обеспечивать защиту внутренних систем организации и осуществлять безопасные управление и контроль проходящего через него трафика в соответствии с принятой политикой доступа к сервису шлюза безопасности (см. 13.2.7.3).

13.2.7.2 Риски безопасности

Хакеры предпринимают все более изощренные попытки взлома сетей, обслуживающих бизнес, и в центре внимания находятся шлюзы. Попытки несанкционированного доступа могут быть злонамеренными, ведущими, например, в результате атаки к отказу в обслуживании, они могут быть направлены на злоупотребление ресурсами или на получение ценной информации. Шлюзы должны защищать организацию от таких вторжений извне, например из Интернета или сетей третьей стороны. Неконтролируемое исходящее из организации информационное наполнение приводит к правовым проблемам и потенциальной потере интеллектуальной собственности. По мере того как все больше организаций устанавливают связь с Интернетом для удовлетворения своих организационных потребностей, они сталкиваются с необходимостью контроля доступа к ненадлежащим или нежелательным веб-сайтам. Без такого контроля организации рискуют потерять производительность, подвергнуться неприятностям и неправильно распределять пропускную способность из-за непродуктивного «блуждания» по веб-сайтам. Если не рассматривать эти угрозы, возрастает риск того, что соединения с внешним миром могут стать недоступными, данные могут быть испорчены или ценные активы организации могут подвергнуться несанкционированному раскрытию. Данные, размещенные на веб-сайтах или иным образом переданные без надлежащих полномочий, тоже могут повлечь за собой правовые неприятности, например инсайдерскую торговлю.

13.2.7.3 Меры безопасности

Шлюз безопасности должен:

- разделять логические сети;
- выполнять функции ограничения и анализа информации, проходящей между логическими сетями;
- быть средством контроля доступа к информации, поступающей в сеть организации и выходящей из нее;
- обеспечивать единственную контролируемую и управляемую точку входа в сеть;
- проводить политику безопасности организации относительно сетевых соединений;
- обеспечивать одну точку для протоколирования.

Для каждого шлюза безопасности должен быть разработан отдельный документ политики безопасности доступа к услугам, и его содержание должно выполняться для гарантии прохождения только санкционированного трафика. Этот документ должен содержать набор правил, которым шлюз должен подчиняться, и конфигурацию шлюза. Необходимо сделать возможным определение разрешенных соединений в отдельности согласно протоколу связи и другим деталям. Таким образом, для гарантирования получения доступа от соединений систем связи только разрешенным пользователям и трафику в политике должны быть определены и подробно зафиксированы ограничения и правила, применяемые к трафику, проходящему через шлюз безопасности в обоих направлениях, и параметры его управления и конфигурации.

Необходимо полностью использовать доступные средства идентификации и аутентификации логического контроля доступа и аудита шлюзов безопасности. Кроме того, их необходимо регулярно проверять на наличие несанкционированных ПО и/или данных; при их обнаружении должны быть составлены отчеты об инцидентах в соответствии со схемой менеджмента инцидентов ИБ организации и/или организаций (см. ИСО/МЭК ТО 18044).

Необходимо, чтобы подключение к сети осуществлялось только после проверки соответствия выбранного шлюза безопасности требованиям организации и/или сообщества и возможности безопасного менеджмента всех рисков, проистекающих из подобного соединения. Должна быть гарантирована невозможность обхода шлюза безопасности.

Хорошим примером шлюза безопасности является межсетевой экран. Межсетевые экраны обычно должны обладать соответствующей степенью гарантии, соизмеримой с оцененным риском, когда стандартный набор правил межсетевого экрана обычно начинается с запрещения всего доступа между внутренними и внешними сетями и добавления отдельных правил для обеспечения соответствия только необходимым каналам связи.

Более подробная информация о шлюзах безопасности представлена в ИСО/МЭК 18028-3 (а также в ИСО/МЭК 17799).

Следует отметить, что, несмотря на отсутствие обсуждения аспектов сетевой безопасности персональных межсетевых экранов (специального типа межсетевых экранов) в ИСО/МЭК 18028-3, они также должны быть рассмотрены. В отличие от большинства центральных узлов, защищенных специальными межсетевыми экранами, удаленные системы не могут быть обеспечены экономически и практически. Взамен можно использовать персональный межсетевой экран, контролирующий поток информации в удаленный компьютер (и иногда из него). Персонал может осуществлять выполнение правил (политик) межсетевого экрана дистанционно в центральном пункте, освобождая удаленного пользователя системы от необходимости изучения технической стороны процесса. Однако, если это невозможно, следует позаботиться об обеспечении эффективной конфигурации, особенно если персонал на удаленном узле не знаком с ИТ. Некоторые персональные межсетевые экраны, ограничивая распространение вредоносных программ, также могут ограничивать возможности передачи по сети санкционированных программ (даже библиотек).

13.2.8 Сервисы удаленного доступа

13.2.8.1 Общие положения

Целью сервисов удаленного доступа (СУД) является осуществление обмена данными между удаленным узлом и центральным сервисом. Для этого существует ряд решений, включающий:

- передачу информации через Интернет;
- службу IP автоматической телефонной связи.

Системы связи через Интернет все в большей степени используют предоставленные Интернет-провайдером каналы связи ADSL для обеспечения высокой пропускной способности из центрального узла и более низкую пропускную способность из удаленного узла к центральному. Для обеспечения безопасности потоков обменных данных (кроме наименее засекреченных) необходимо использовать VPN (см. 13.2.9).

Службы IP автоматической телефонной связи позволяют удаленному узлу (обычно одиночному пользователю) набирать номер блока модемов на центральной станции. После аутентификации устанавливается связь между удаленным узлом и центральным сервисом. Если только в приложении не используется протокол безопасности, в этом режиме связи шифрование обычно не применяют. Доступ к СУД реализуют посредством сети ISDN или аналоговых линий. Так или иначе пользователь звонит в центральный узел, где имеется определенный уровень аутентификации. Доступ к СУД обеспечивает передачу только незашифрованных данных.

13.2.8.2 Риски безопасности

Существует ряд рисков безопасности, которые могут быть связаны с СУД:

- несанкционированный доступ к системам, сервисам и информации организации (включая прослушивание), приводящий к раскрытию, несанкционированным изменениям или разрушению информации и/или сервисов;
- введение вредоносного кода в системы, сервисы и информацию организации с их последующей модификацией, недоступностью и разрушением;
- атака DoS на сервисы организации.

13.2.8.3 Меры безопасности

Удаленный доступ подразумевает наличие самозащиты центральных сервисов от несанкционированного доступа. Считается, что сами удаленные системы имеют защиту от ряда угроз безопасности. Меры безопасности, которые могут потребоваться, включают:

- межсетевые экраны (включая персональные межсетевые экраны);
- ACL маршрутизатора;
- шифрование каналов доступа к Интернету;
- определитель линии вызова;
- строгую аутентификацию;
- антивирусное ПО;
- управление аудитом.

Более подробная информация о безопасности СУД содержится в ИСО/МЭК 18028-4.

13.2.9 Виртуальные частные сети

13.2.9.1 Общие положения

VPN является частной сетью, которая реализуется с помощью инфраструктуры существующих сетей. С точки зрения пользователя, VPN функционирует как частная сеть и предлагает аналогичные функциональные возможности и услуги. VPN может быть использована в различных ситуациях:

- реализация удаленного доступа к организации для мобильных или находящихся за пределами организации сотрудников;
- связь между различными местоположениями организации, включая избыточные связи для внедрения инфраструктуры восстановления;
- установление подсоединений к сети организации для других организаций/партнеров по бизнесу.

Другими словами, VPN позволяет двум компьютерам или сетям обмениваться информацией безопасным образом в незащищенной передающей среде (например, в Интернете). Этот обмен ранее осуществляли с большими затратами посредством использования арендуемых линий с шифраторами в канале связи. Однако с появлением высокоскоростных каналов связи Интернета и подходящего оконечного оборудования на каждом конце сети появилась возможность установления безопасных связей между узлами сети с помощью VPN.

13.2.9.2 Риски безопасности

Ключевой риск безопасности для систем связи в незащищенной сети заключается в том, что секретная информация может быть доступна для несанкционированного доступа, что приводит к ее раскрытию и/или изменению. В дополнение к рискам, обычно связанным с локальными и глобальными сетями (см. 13.2.2.2 и 13.2.3.2 соответственно), обычные риски, связанные с VPN, включают:

- незащищенную реализацию из-за:
  - нетестированного или дефектного набора шифров;
  - коллективной тайны, которая может быть легко раскрыта;
  - плохой топологической схемы сети;
  - неуверенности в безопасности удаленного клиента;
  - неуверенности в аутентификации пользователей;
- неуверенность в безопасности основного провайдера услуг;
- плохие функционирование или доступность сервиса;
- несоответствие нормативным и законодательным требованиям к применению шифрования в некоторых странах.

13.2.9.3 Меры безопасности

В VPN в сетевых протоколах и/или протоколах приложений для реализации функциональных возможностей и услуг в области безопасности обычно используют криптографические технологии, особенно если сеть, на которой построена VPN, является общедоступной сетью (например, Интернет). В большинстве случаев для обеспечения конфиденциальности при реализации каналы связи между участниками зашифровывают, а для подтверждения идентичности систем, подключенных к VPN, используют протоколы аутентификации. Обычно зашифрованная информация проходит по безопасному туннелю, который соединяется со шлюзом организации, сохраняя конфиденциальность и целостность информации. Затем шлюз идентифицирует удаленного пользователя и разрешает ему доступ только к той информации, на получение которой он имеет санкцию.

Таким образом, VPN представляет собой механизм, основывающийся на туннелировании протокола, — обработка одного полного протокола (клиентский протокол) как простого потока битов и заключение его в другой протокол (главный протокол). Обычно протокол носителя VPN обеспечивает безопасность (конфиденциальность и целостность) клиентского протокола(ов). При рассмотрении использования VPN следует определить следующие аспекты архитектуры:

- безопасность конечной точки;
- безопасность завершения;
- защита от вредоносного ПО;
- аутентификация;
- обнаружение вторжений;
- шлюзы безопасности (включая межсетевые экраны);
- проектирование сети;
- возможность другого соединения;
- раздельное туннелирование;

- протоколирование данных аудита и мониторинг сети;
- техническое управление уязвимостями.

Более подробная информация о VPN, включая каждый из аспектов архитектуры, представлена в ИСО/МЭК 18028-5.

13.2.10 IP-Конвергенция (данные, голос, видео)

13.2.10.1 Общие положения

По мере завоевания популярности конвергенцией голоса и данных необходимо выявлять и учитывать связанные с ней проблемы безопасности. Хотя действующие практические приемы передачи голоса нуждаются в мерах безопасности для предотвращения мошенничества, связанного с международными разговорами, голосовой почтой, и других угроз безопасности, эти системы не объединены в корпоративную сеть данных и не подвержены тем же рискам, что и сети данных IP. При конвергенции голоса и данных для уменьшения риска атак необходимо внедрение мер безопасности.

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

13.2.10.2 Риски безопасности

Основные области риска могут быть связаны с атаками, основанными на IP, на специфические для поставщика уязвимости ПО и аппаратные средства или платформу операционной системы, на которой размещено приложение VoIP. Риски, связанные с компонентами приложения VoIP, включают атаки на сетевые устройства и приложения, и им могут содействовать уязвимости в проектировании или реализации решения, связанные с VoIP. Существуют следующие области риска:

- качество обслуживания (без контроля качества обслуживания в целом может возникнуть вероятность потери качества или прерывания вызовов из-за потери пакета и задержки распространения сигнала в сети);
- недоступность услуги из-за атак DoS или изменений в таблицах маршрутизации;
- на целостность и доступность могут повлиять вирусы, которые могут проникнуть в сеть через незащищенные системы VoIP и ухудшить или даже вызвать потерю сервиса, а также могут распространиться на серверы в сети, что приведет к их повреждению;
- программофоны на персональных компьютерах клиента являются источником значительного риска, так как они могут стать точками проникновения вирусов и вторжения;
- серверы VoIP и системы управления VoIP являются источником риска, если они не защищены межсетевыми экранами;
- безопасность сети данных может оказаться под угрозой из-за большого количества портов, открытых на межсетевых экранах для поддержки. 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;
- мошенничество является ключевой проблемой VoIP, и отсутствие внимания к проблемам безопасности только добавляет риски. Хакеры могут получить несанкционированный доступ к услуге VoIP посредством имитации атак воспроизведения или нападения на соединения. К значительным расходам может привести мошенничество, связанное с международными разговорами или несанкционированными вызовами;
- нарушения конфиденциальности могут возникать вследствие перехвата информации в сети сотрудниками и другим персоналом, имеющим доступ к сети;
- прослушивание речевых вызовов;
- так как для работы IP-телефоны нуждаются в питании, телефонная сеть не может функционировать в случае отключения электричества;
- существует еще больший риск сбоя у сервисов, связанных с голосом и передачей данных, из-за использования общих компонентов, например ЛВС.

13.2.10.3 Меры безопасности

Существует ряд технических мер безопасности для менеджмента рисков от идентифицированных угроз конвергированным IP-сетям, включающий следующие положения:

- в объединенную сеть должны внедряться средства контроля качества обслуживания, иначе существует вероятность ухудшения качества голоса. Оказание сетевых услуг и, где возможно, предоставление IP-каналов связи следует осуществлять по волоконно-оптическому кабелю для минимизации дрожания фазы (которое влияет на качество голоса);

- все серверы VoIP должны конфигурироваться с защитой от вредоносного ПО;
- поддерживающие ПК программофоны должны быть снабжены персональными межсетевыми экранами, а ПО проверки наличия вирусов должно регулярно обновляться;
- для защиты от атак серверы передачи голоса по IP и системы управления VoIP должны быть защищены межсетевыми экранами;
- проектировщики должны гарантировать открытие минимального количества портов межсетевых экранов для поддержки услуг по VoIP;
- для борьбы с мошенничеством, связанным с международными разговорами, должны внедряться меры безопасности, направленные против повторного воспроизведения и на борьбу с имитацией (спуфингом), для предотвращения нападения на соединения;
- следует аутентифицировать весь доступ к серверам управления;
- по возможности услуги, связанные с передачей голоса и данных, должны быть разделены;
- необходимо рассмотреть возможность использования системы обнаружения атак для серверов, поддерживающих услуги по VoIP;
- необходимо рассмотреть возможность шифрования канала прохождения данных, когда в сети VoIP должна обсуждаться секретная информация;
- IP должны питаться через концентраторы сети Ethernet, поддерживаемые ИБП;
- может потребоваться обыкновенный речевой сервис, который имеет автономный источник питания для использования в аварийных ситуациях.

13.2.11 Разрешение доступа к услугам, предоставляемым внешними (по отношению к организациям) сетями

13.2.11.1 Общие положения

Предоставление услуг электронной почты и Интернета организации в целях удовлетворения законных бизнес-требований приводит к возникновению разнообразных угроз, которые могут использовать уязвимые системы, и если эти услуги не спроектированы и не эксплуатируются правильно, то они представляют значительный риск для организации. Например, несмотря на барьеры, стоящие перед спаммерами, распространяющими свою деятельность на работающий персонал, спам является большой проблемой для предприятий и их персонала. Так как спаммеры пытаются узнать имена сотрудников, большинству предприятий понадобится использовать технологии антиспама и обучить пользователей защищать свои адреса электронной почты. Кроме того, пользователям потребуется защита от доступа к Интернету и внедрения в организацию вредоносного ПО, такого, как «троянские кони», что может причинить значительный ущерб информационным системам и репутации организации. Важно учитывать, что Интернету нельзя доверять полностью.

13.2.11.2 Риски безопасности

Основными областями риска при осуществлении доступа к услугам, предоставляемым внешними по отношению к организации сетями, в условиях эксплуатации уязвимостей в сервисах Интернета и электронной почты являются:

- потенциальное введение вредоносного ПО, такого, как «троянские кони»;
- получение огромного объема спама;
- потеря информации организации;
- нанесение ущерба целостности информации или ее потеря;
- атаки DoS;
- несанкционированное использование услуг Интернета и электронной почты, включая неподчинение политике безопасности организации (например, использование услуг в личных целях) и законодательству (например, посылка угрожающих электронных писем).

13.2.11.3 Меры безопасности

Технические мероприятия по обеспечению безопасности менеджмента рисков, исходящих от идентифицированных угроз, для Интернета/электронной почты включают:

- использование межсетевых экранов с уровнями гарантии, соответствующими оцененным рискам, и наборов правил межсетевых экранов, которые относятся к следующему:
  - политике «отказ от всего» по умолчанию;
  - только исходящим сообщениям (например, http/https);
  - электронной почте в обоих направлениях;
- использование ACL и протоколов NAT на маршрутизаторах для ограничения и сокрытия структуры IP-адресации;

- активизация антиспуфинга для предотвращения внешних атак. Меры безопасности антиспуфинга принимают форму непринятия сообщения со стороны (например, из Интернета), если в нем утверждается, что оно исходит изнутри организации, и наоборот;

- активизация веб-модулей и модулей электронной почты в качестве посредника между пользователем рабочей станции и Интернетом так, чтобы предприятие могло обеспечивать безопасность, административный контроль и службу кэширования. Безопасность укрепляется путем сравнения запрошенного унифицированного указателя информационного ресурса с «белым» и «черным» списками (для доступа в Интернет), сканирования данных по известным образцам, перемещения между внутренними и внешними адресами, создания протокола аудита запросов и запрашивающих сторон и наличия антивирусных средств, основанных на модулях доступа;

- антивирусные средства безопасности на веб-модулях доступа и модулях доступа электронной почты. Обычные меры безопасности включают средства, изолирующие подозрительные файлы (например, по типу содержимого) и отсеивающие запрошенные унифицированные указатели информационного ресурса или адреса электронной почты по «черному» списку. (Следует отметить, что «черные» списки не могут считаться защитой от неумелого обращения, особенно, когда подобные списки получают со стороны. В таком случае может появиться опасность получения ложных положительных выводов.) Более подробная информация по антивирусным мерам безопасности представлена в 13.9;

- антиретранслятор на серверах электронной почты и обратные просмотры DNS. Меры безопасности антиретрансляторов определяют, поступает ли входящее электронное письмо от нужной отправляющей организации; в противном случае электронное письмо протоколируется (или изолируется), и сервер электронной почты не предпринимает дальнейших действий;

- разблокирование сигналов тревоги и ловушек протокола SNMP. Протокол SNMP может быть использован для дистанционного управления сетевым устройством и для посылки сообщений (или «ловушек») в целях уведомления станции мониторинга о состоянии этого устройства;

- мониторинг и протоколирование данных аудита сети (см. 13.7);

- установление внеполосного управления, связанного с практикой использования разных сетей для передачи данных и управления, чтобы сделать невозможным подключение злоумышленника к их устройству;

- обеспечение должной связи уязвимостей в клиентском ПО, используемом для доступа к услугам Интернета (например, веб-браузер), с соответствующими процессами управления уязвимостями и применением патчей.

13.2.12 Архитектура размещения информации на веб-узлах

13.2.12.1 Общие положения

Услуги по размещению информации на узлах сети предлагают многие провайдеры сетевых услуг в форме стандартизированной услуги, часто включающей средства базы данных для обработки длительно хранимых данных, а также основную среду времени прогона приложения. Хотя большинство компонентов, необходимых для реализации и предложения услуг по размещению информации на узлах сети, находятся вне области применения настоящего стандарта (такие, как веб-сервер или ПО базы данных), здесь зафиксированы некоторые положения по самой услуге в целом, так как многие считают размещение информации на узлах сети составной частью сетевого ассортимента.

Узлы размещения информации подвержены риску со стороны разнообразных угроз, особенно там, где они подключены к Интернету, например, где известные организации могут быть атакованы периферийными группами. Таким образом, необходимы идентификация всех потенциальных угроз, а затем блокирование всех уязвимостей, которые могли бы эксплуатироваться этими угрозами. Это наилучшим образом достигается исключением уязвимостей из архитектуры при ее проектировании. Рассмотрение этих проблем в соответствии с представленной рекомендацией должно сделать возможным проектирование безопасного, надежного веб-узла с низкой степенью риска уничтожения.

13.2.12.2 Риски безопасности

Основными областями риска являются:

- доступ злоумышленника к прикладной системе и данным через единственную брешь в защите периметра;

- незащищенность компонента инфраструктуры для уязвимостей;

- многочисленные отдельные критические точки (сбоя);

- потеря обслуживания из-за сбоя аппаратных средств;

- неспособность вывода из строя для обслуживания;

- непреднамеренный доступ общественных пользователей к участкам хранения данных;
- загрузка в систему вредоносного ПО;
- компрометация веб-узла с использованием функциональной возможности коммутации;
- неспособность снятия резервных копий без воздействия на работу веб-узла;
- несанкционированное раскрытие плана IP-адресации, облегчающее атаку на веб-узел;
- использование соединений между станциями управления и веб-узлом;
- необнаруженная атака;
- трудность в отслеживании вторжений между устройствами;
- неспособность восстанавливать данные;
- неспособность удовлетворять требованиям соглашения об уровне сервиса;
- неспособность поддерживать непрерывность услуги;
- несанкционированное использование веб-услуг, включая нарушение политики организации (например, использование серверов в личных целях) и несоответствие законодательству (например, хранение материала, который нарушает авторские права, или детской порнографии).

13.2.12.3 Меры безопасности

Существуют следующие технические меры безопасности для менеджмента рисков от идентифицированных угроз для веб-узлов:

- обеспечение тщательного зонирования безопасности для ограничения воздействия успешной атаки;
- спецификация различных типов межсетевых экранов для противодействия возможным уязвимостям межсетевых экранов (более подробная информация о межсетевых экранах представлена в 13.2.7 и ИСО/МЭК 18028-3);
- устойчивость к внешним воздействиям: проект должен быть проверен на наличие потенциально критических точек, которые должны быть устранены;
- преодоление отказа/разделения нагрузки для защиты от сбоя в работе оборудования;
- кластеризация (создание кластеров), где требованием является высокий уровень готовности в среде порядка 24×7;
- предоставление посреднических услуг для ограничения доступа к веб-узлу и обеспечение высокой степени протоколирования;
- антивирусные меры безопасности на загрузках для предотвращения импорта вредоносного ПО (более подробная информация о мерах безопасности для обнаружения и предотвращения вредоносного кода представлена в 13.9);
- коммутация уровня 2, обычно используемая в проекте веб-узла. Коммутация уровня 3 не должна быть использована, если это не является бизнес-требованием (например, как для распределения нагрузки). Кроме того, один и тот же физический коммутатор не должен быть использован обеими сторонами межсетевого экрана. В проект коммутатора следует включать контрольные точки WLAN, разделенные функцией для упрощения настройки системы обнаружения вторжений, так как существует сокращенный протокол, настроенный на любую ЛВС. Кроме того, внедрение резервной ЛВС позволяет эксплуатировать резервные копии в любое время суток, не подвергая опасности работу сайта;
- план IP-адресации для ограничения количества общедоступных адресов до минимума, хранящийся под строжайшим секретом, знание которого может быть использовано для инициирования атаки на веб-узел;
- места подсоединения каналов управления к общедоступным сетям должны шифроваться (более подробную информацию об удаленном доступе см. в ИСО/МЭК 18028-4). Это включает по меньшей мере наличие предупреждений /ловушек протокола SNMP на соединениях портов пульта управления;
- все протоколы аудита событий и транзакций каждого устройства, скопированные на сервер аудита и затем на носители резервных копий, такие, как компакт-диски (более подробная информация о протоколировании данных аудита и мониторинге сети представлена в пункте 13.7);
- реализованная услуга временной синхронизации, поскольку она является основой анализа несанкционированного доступа и возможности отслеживания по протоколам аудита. Для этого требуется синхронизация всех протоколов аудита и, следовательно, серверов до плюс/минус 1 С (здесь уместен протокол NTP; более подробную информацию см. в ИСО/МЭК 17799, подраздел 10.6);
- предпочтительна услуга централизованного резервного копирования, так как существует наибольшая вероятность ее выполнения должным образом;

- необходимость круглосуточного функционирования веб-узлов требует высококачественных аппаратных средств, которые могут выдержать условия этой среды. Для поддержки функционирования в режиме 24×7 в веб-узле должна быть определена инфраструктура сервера. Вспомогательные операционные системы должны быть укреплены, затем все серверы и другие устройства необходимо тестировать на предмет безопасности для обеспечения полной защищенности всех устройств;

- внедренное надежное прикладное ПО, где был проверен код для структуры, которая является логически корректной и использует утвержденное ПО аутентификации.

Также следует отметить, что при проектировании веб-узла вопросы управления непрерывностью бизнеса часто рассматриваются не полностью. В отношении веб-узлов действия по управлению непрерывностью бизнеса должны проводиться полностью (более полно информация об управлении непрерывностью бизнеса изложена в 13.11).

13.3 Основа безопасного управления услугами

13.3.1 Управление услугами

Ключевое требование безопасности к любой организации сети — это ее поддержание действиями безопасного управления услугами, которые инициируют и контролируют внедрение и функционирование мер безопасности. Эти действия служат обеспечению безопасности всех информационных систем организации или сообщества. Менеджмент сетевых соединений должен включать:

- определение всех обязанностей, связанных с безопасностью организации сети, и назначение менеджера по безопасности с общей ответственностью;

- документированную политику безопасности организации сети и сопроводительную документированную архитектуру технической безопасности;

- документированные вспомогательные операции;

- проведение проверки соответствия требованиям безопасности, включая тестирование на безопасность для обеспечения поддержания безопасности на требуемом уровне;

- документированные условия безопасности для соединения, которые надо выполнять до получения разрешения на соединения от сторонних организаций или людей;

- документированные условия безопасности для пользователей сетевых услуг;

- схему менеджмента инцидентов безопасности;

- задокументированные и проверенные планы по поддержанию непрерывности бизнеса/восстановления в аварийных ситуациях.

Следует отметить, что этот пункт касается аспектов, описанных в ИСО/МЭК 17799. В стандарте подробно описаны только особо важные вышеуказанные темы, касающиеся использования сетей. Следовательно, за более подробной информацией, например, о содержании политики безопасности сети и операционных процедурах безопасности и о темах, не указанных здесь, читателю следует обратиться к ИСО/МЭК 17799.

13.3.2 Политика безопасности сетей

Обязанностью руководства является принятие и поддержка политики сетевой безопасности организации (как указано в ИСО/МЭК 17799). Эта политика сетевой безопасности должна вытекать из политики информационной безопасности организации и согласовываться с ней. Политика должна быть реализуемой, легкодоступной для санкционированных членов организации и содержать четкие формулировки:

- позиции организации в отношении приемлемого использования сети;

- дополнительных правил безопасного использования специальных сетевых ресурсов, сервисов и приложений;

- последствий сбоя для выполнения правил безопасности;

- отношения организации к неправильной эксплуатации сети;

- логического обоснования(й) политики и специальных правил безопасности.

В некоторых обстоятельствах эти четкие формулировки могут быть включены в политику информационной безопасности, если это более удобно для организации и/или это делает политику более понятной для персонала.

Политика безопасности сети обычно должна содержать краткое изложение результатов оценки риска безопасности и административного анализа (что служит обоснованием расходов на меры безопасности), включая подробности о всех выбранных мерах безопасности, соразмерных оцененным рискам (см. раздел 12).

13.3.3 Рабочие процедуры обеспечения безопасности

В поддержку политики сетевой безопасности необходимо разработать и сохранять документацию по вспомогательным операциям, охватывающую каждое сетевое соединение при необходимости. В ней долж-

ны содержаться детали повседневных рабочих процедур, связанных с обеспечением безопасности, а также сведения о лицах, ответственных за их использование и менеджмент.

13.3.4 Проверка соответствия требованиям безопасности

Все сетевые соединения необходимо проверять на соответствие требованиям безопасности по сводному контрольному списку, составленному из мер безопасности, определенных в:

- политике безопасности организации сети;
- родственных вспомогательных операциях;
- архитектуре технической безопасности;
- политике (безопасности) доступа к услуге шлюза безопасности;
- плане(ах) обеспечения непрерывности бизнеса;
- условиях безопасности для соединения (если необходимо).

Проверка должна проводиться до введения в действие любого сетевого соединения, до новой основной версии (связанной со значительным изменением, связанным с бизнесом или сетью), во всем остальном — ежегодно.

Проверка должна включать проведение испытания безопасности по общепризнанным стандартам в соответствии со стратегией испытания безопасности и связанными с ней планами, разработанными заранее, точно определяющими, какие, с чем, где и когда должны проводиться испытания. Обычно она должна сочетать поиск уязвимостей и испытания на проникновение. Перед началом любого такого испытания план испытания необходимо проверить, чтобы гарантировать проведение испытания в полном соответствии с действующим законодательством. При проведении этой проверки не следует забывать о том, что сеть может не ограничиваться одной страной — она может распространяться на другие страны с различным законодательством. При проведении испытания в отчетах должны быть указаны особенности обнаруженных уязвимостей, необходимые меры по их устранению и приоритет их принятия.

13.3.5 Условия обеспечения безопасности соединения

При отсутствии согласованных по контракту условий безопасности соединений организация фактически принимает риски, связанные с другим концом сетевого соединения вне ее домена. Подобные риски могут включать риски, связанные с защитой персональной информации/данных, когда соединение можно использовать для обмена персональными данными, который подчиняется национальному законодательству, на одном или обоих концах и когда другой конец сетевого соединения (вне области действия организации) находится в другой стране и законодательство может быть другим.

Например, организация А может потребовать, чтобы перед подключением организации В к ее системам через сетевое соединение организация В поддержала и продемонстрировала определенный уровень безопасности для своей системы, участвующей в этом соединении. Таким образом организацию А можно убедить в том, что организация В управляет своими рисками приемлемым способом. В подобных случаях организация А должна представить условия безопасности для документа по соединению, который уточняет меры безопасности, которые должны быть приняты организацией В. Они должны быть реализованы организацией В, после чего организация А подписывает обязательное соглашение о поддержании безопасности. Организация А сохраняет за собой право на проведение проверки принятых мер обеспечения безопасности в организации В.

Также бывают случаи, когда организации в сообществе обоюдно согласуют документ «Условия безопасности для соединения», в котором записаны обязательства и обязанности всех сторон, включая взаимную проверку соответствия.

13.3.6 Документированные условия безопасности для пользователей сетевых услуг

Пользователям, санкционированным для удаленной работы, необходимо выдавать документ «Условия безопасности для пользователей сетевых услуг». В нем должна быть изложена ответственность пользователя за программное обеспечение, аппаратуру и данные относительно сети и их безопасность.

13.3.7 Менеджмент инцидентов

Инциденты ИБ чаще всего происходят (и их последствия оказывают более серьезное отрицательное воздействие на бизнес) в местах сетевых соединений, в особенности в случае сетевого соединения с другими организациями. Таким образом, могут возникнуть значительные юридические последствия, связанные с инцидентами.

Организация с сетевыми соединениями должна иметь документированную и реализованную схему менеджмента инцидентов ИБ и связанную с ней инфраструктуру, способную быстро реагировать на идентифицированные инциденты, сводить к минимуму их воздействие и делать выводы для предотвращения их повторного появления. Эта схема должна быть способна обрабатывать как события ИБ (идентифици-

рованные возникновения состояния системы, услуги или сети, указывающие на возможное нарушение политики информационной безопасности или отказ средств защиты или прежде неизвестной ситуации, которая может иметь значение для безопасности), так и инциденты ИБ (единичное событие или серии нежелательных или неожиданных событий ИБ, которые со значительной вероятностью могут подвергнуть риску проведение бизнес-операций и угрожать ИБ).

Более подробная информация о менеджменте инцидентов ИБ изложена в ИСО/МЭК 18044.

13.4 Менеджмент сетевой безопасности

13.4.1 Общие положения

Управление любой сетью необходимо осуществлять безопасным способом и, безусловно, обеспечивать поддержку менеджмента сетевой безопасности с оказанием должного внимания различным доступным сетевым протоколам и связанным с ними службам безопасности.

В поддержку вышеуказанного организация должна рассмотреть ряд мер безопасности, большая часть которых может быть определена с помощью ИСО/МЭК 17799. Кроме того, дистанционные диагностические порты, как виртуальные, так и физические, должны быть защищены от несанкционированного доступа.

13.4.2 Аспекты организации сети

Различные аспекты организации сети могут подразделяться на следующие категории.

Пользователи сети — это персонал, являющийся пользователями и/или сетевыми администраторами. Разнообразие пользователей включает отдельных лиц, имеющих доступ к удаленным ресурсам через Интернет, соединения телефонной линии или беспроводные соединения, и лиц, использующих рабочие станции или персональные компьютеры, подключенные к локальной сети. Пользователи, подключенные к локальным сетям, также могут подсоединяться к удаленным ресурсам через межсетевые соединения, которые могут находиться между их локальной сетью и другими сетями. Такие базовые соединения могут быть прозрачными для пользователя.

Оконечными системами являются компьютеры, рабочие станции и мобильные устройства (например, смартфоны и КПК), подключенные к сетям. Они включают устройства, используемые для доступа к сетевым средствам (например, клиентские системы), и устройства, используемые для предоставления услуг (например, серверы, системы главного компьютера). Эта категория включает аппаратуру, программное обеспечение операционных систем и любое программное обеспечение локальных приложений, включая программное обеспечение, которое используют для доступа к сети.

Объединенные в сеть приложения — программное обеспечение прикладных программ, работающее на объединенных в сеть серверах и базисных системах и доступное через компьютерные сетевые соединения для предоставления:

- услуг по осуществлению финансовых операций;
- услуг ПО предприятия (например, CRM, управленческая информационная система, стандарт MRP и т. д.);
- веб-услуг;
- услуг интерактивных баз данных;
- средств оперативной памяти.

Сетевыми услугами являются услуги, предоставляемые сетью, которые обычно реализуют ПО в конечных базисных или серверных системах, образующих часть инфраструктуры сети, например:

- соединяемость;
- электронная почта;
- передача файлов;
- службы каталогов.

Сетевые услуги могут:

- принадлежать организации и быть эксплуатируемыми ею;
- принадлежать организации, но быть эксплуатируемыми внешними организациями по контракту;
- быть арендованы у сторонних организаций;
- быть специально приобретены у сторонних провайдеров;
- быть комбинацией вышеизложенных пунктов.

Инфраструктурой сети являются базовое оборудование для аппаратуры и ПО, например:

- помещения;
- монтаж кабельной проводки;
- беспроводные средства;
- сетевые устройства (например, маршрутизаторы, коммутаторы, модемы и т. д.).

Как указано в разделе 12, эти аспекты сетевой безопасности должны моделироваться как аспекты сети. Эти аспекты строятся один на основе другого в целях создания схемы менеджмента сетевой безопасности, как показано на рисунке 4.

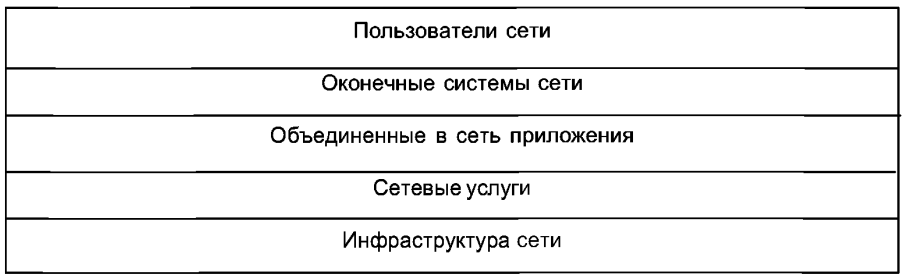

Рисунок 4 — Аспекты схемы менеджмента сетевой безопасности

Существует определенное неизбежное совпадение с некоторыми системами, исполняющими множественные роли в любом реалистичном сценарии сети. Однако эти концептуальные аспекты функциональных возможностей должны содействовать необходимому систематическому процессу оценки, требуемому для определения рисков безопасности, присутствующих в любом отдельном сценарии сети. Каждый аспект в этой концептуальной схеме безопасности должен управляться индивидуально, а все аспекты должны управляться коллективно для обеспечения соответствия общих целей понятию безопасной сети.

13.4.3 Роли и обязанности

Роли и обязанности, которые должны выполняться совместно с менеджментом сетевой безопасности, являются следующими (следует отметить, что в зависимости от масштаба организации эти роли могут объединяться):

1 Для высшего руководства:

- определять цели безопасности организации;
- инициировать, утверждать, опубликовывать и предписывать политику, процедуры и правила безопасности организации;
- инициировать, утверждать, выпускать и предписывать политику использования информационных технологий в организации;
- обеспечивать и приводить в исполнение политики безопасности приемлемого использования.

2 Для сетевого менеджмента:

- разрабатывать детальную политику сетевой безопасности;
- реализовывать политику сетевой безопасности;
- вводить в действие приемлемую политику использования;
- управлять взаимодействием со сторонними заинтересованными организациями/сторонними провайдерами услуг для обеспечения соответствия внешней и внутренней политикам сетевой безопасности.

3 Для группы обеспечения сетевой безопасности:

- приобретать, разрабатывать, испытывать, контролировать и обслуживать компоненты и средства безопасности;
- поддерживать средства и компоненты безопасности для тщательного слежения за эволюцией угроз (например обновляя файлы сигнатуры вируса);
- обновлять значимые конфигурации безопасности (например, списки контроля доступа) согласно изменяющимся потребностям бизнеса.

4 Для администраторов сети:

- устанавливать, обновлять и защищать сервисы и компоненты сетевой безопасности;
- выполнять необходимые ежедневные задачи по применению спецификаций, правил и параметров безопасности, требуемых для действующих политик безопасности;
- предпринимать соответствующие меры для обеспечения защиты компонентов сетевой безопасности (например, резервное копирование, мониторинг сетевой деятельности, реагирование на инциденты безопасности или аварийные сигналы и т. д.).

5 Для пользователей сети:

- сообщать о своих требованиях безопасности;
- подчиняться корпоративной политике безопасности;

- подчиняться корпоративным политикам приемлемого использования сетевых ресурсов;
- сообщать об инцидентах сетевой безопасности;
- обеспечивать обратную связь по вопросам эффективности сетевой безопасности.

6 Для аудиторов (внутренних и/или внешних):

- анализировать и проводить аудит (например, периодически проверять эффективность сетевой безопасности);
- проверять соответствие систем политике сетевой безопасности;
- проверять и испытывать совместимость действующих правил безопасности с текущими бизнес-требованиями и правовыми ограничениями (например, списки на получение доступа к сети).

13.4.4 Мониторинг сети

Мониторинг сети является очень важной частью менеджмента сетевой безопасности. Он рассмотрен в 13.7.

13.4.5 Оценка сетевой безопасности

Сетевая безопасность является динамичным понятием. Персонал обеспечения безопасности должен быть в курсе современных разработок в этой области и обеспечивать непрерывность работы любой сети с самыми современными патчами безопасности и доработками, имеющимися у поставщиков. Необходимо периодически предпринимать шаги по проверке имеющихся мер безопасности по отношению к установленным контрольным точкам, включая тестирование безопасности — поиск уязвимостей и т. д. Безопасность должна быть основным фактором при оценке новой технологии сети.

13.5 Управление техническими уязвимостями

Сетевые среды, как и другие сложные системы, не свободны от погрешностей. В компонентах, часто используемых в сетях, присутствуют и воспроизводятся технические уязвимости. Эксплуатация этих технических уязвимостей может сильно повлиять на безопасность сети, что наиболее часто происходит в областях доступности и конфиденциальности. Следовательно, должно быть управление техническими уязвимостями, охватывающее все компоненты сети, которое должно включать:

- своевременное получение информации о технических уязвимостях;
- оценку подверженности сети подобным уязвимостям;
- определение соответствующих мер безопасности для работы со связанными с этими уязвимостями рисками;
- введение и проверку определенных мер безопасности.

Предпосылкой для управления техническими уязвимостями должно быть наличие современного и полного списка всех компонентов сети, обеспечивающего необходимую техническую информацию, например, о типе устройства, поставщике, номере версии аппаратуры, программно-аппаратных средств или ПО, а также информацию об организации, например об ответственных административных лицах.

Если организация уже разработала общую программу управления техническими уязвимостями, предпочтительным решением проблемы должна быть интеграция управления техническими уязвимостями компонентов сети в общую задачу. (Более подробную информацию об управлении техническими уязвимостями, включая рекомендацию по внедрению, можно найти в ИСО/МЭК 17799.)

13.6 Идентификация и аутентификация

13.6.1 Общие положения

Важно обеспечить сохранение безопасности сетевого сервиса и связанной с ним информации посредством ограничения доступа через соединения санкционированного персонала (являющегося для организации внешним или внутренним). Требования для них не могут быть эксклюзивными для использования сетевых соединений, и поэтому подробные разъяснения, относящиеся к использованию какого-либо сетевого соединения, должны быть получены с помощью ИСО/МЭК 17799.

Четыре контролируемые области, которые могли бы иметь значение для использования сетевых соединений и информационных систем, непосредственно связанных с подобными соединениями, приведены в 13.6.2—13.6.5.

13.6.2 Удаленный вход в систему

Удаленные входы в систему санкционированного персонала, работающего далеко от организации, удаленного обслуживающего персонала или персонала других организаций осуществляются либо через кодовый вызов в организацию, Интернет-соединения, специальные каналы связи из других организаций, либо посредством коллективного доступа через Интернет. Эти соединения созданы по необходимости либо внутренними системами, либо партнерами по контракту с помощью общедоступных сетей. Каждый тип удаленного входа в систему должен иметь дополнительные меры безопасности, соответствующие характеру типа соединения.

Примеры мер безопасности:

- недопущение прямого доступа к системному и сетевому ресурсам, использующимся для удаленного доступа, за исключением случаев предоставления дополнительной аутентификации (см. 13.6.3) и, возможно, шифрования по всей сети;

- защита от несанкционированного доступа к информации, связанной с ПО электронной почты и данными каталога, хранящимися в персональных и дорожных компьютерах, использующихся ее персоналом за пределами офисов организации.

13.6.3 Усложнение аутентификации

Использование идентификатора пользователя/пар паролей — простой способ аутентификации пользователей, но их (идентификаторы и пары паролей) можно скомпрометировать или разгадать. Существуют другие, более безопасные способы аутентификации пользователей, особенно удаленных пользователей. Усложнение аутентификации необходимо при наличии высокой вероятности получения доступа неуполномоченного лица к защищенным и важным системам. Это может быть, например, следствием возможности инициирования доступа через общедоступные сети, или доступ к системе (например, через дорожный компьютер) может находиться за пределами прямого контроля организации.

В случаях требования (например, по контракту) усложнения аутентификации по сетевым соединениям или его обоснования рисками организации следует рассмотреть возможность усиления процесса аутентификации личности посредством внедрения соответствующих мер безопасности.

Простые примеры мер безопасности используют:

- CLID, который можно считать исходящим телефонным номером, принимаемым приемной аппаратурой. Хотя CLID имеет определенную значимость как утвержденный идентификатор вызывающей стороны, он открыт для спуфинга и не должен использоваться в качестве подтвержденного ID без дальнейшей аутентификации. CLID часто используют как быстрый идентификатор установления резервных связей (особенно в цифровых сетях с интегрированным обслуживанием) между сайтами;

- связи через модемы, которые отключаются, когда не используются, и инициируются только после подтверждения идентичности вызывающего оператора.

Более сложными, но очень важными примерами, особенно в контексте удаленного доступа, являются:

- использование других средств идентификации для поддержки аутентификации пользователей, таких, как дистанционно проверенные маркеры и смарт-карты (например, через считывающие устройства, подключенные к ПК), ручные устройства создания одноразового ключа доступа и основанные на применении биометрии средства;

- обеспечение функционирования маркера или смарт-карты только совместно с аутентифицированным абонентом пользователя (и предпочтительно — ПК и месторасположение/точка доступа этого пользователя) и, например, любым соответствующим PIN-кодом или биометрическим профилем.

В общем, это называется строгой аутентификацией, состоящей из двух факторов. При использовании маркеров пользователю необходимо знать PIN, который вместе с маркером делает возможным осуществление аутентификации с единственным значением. Что касается смарт-карт, они могут рассматриваться как автоматизация использования доступа через маркер. Чтобы «открыться», пользователь должен добавить PIN-код к карте после ее вставления в считывающее устройство смарт-карт. Затем каждый раз, когда аутентификация требуется для центральных или удаленных систем, смарт-карта может быть вызвана непосредственно для «подписания» данных (подтверждая аутентификацию) посредством ключа, содержащегося в смарт-карте.

13.6.4 Идентификация удаленной системы

Как предполагалось в 13.6.3, значимая аутентификация должна усовершенствоваться путем проверки полномочий системы (и ее места расположения/точки доступа), из которой осуществляется внешний доступ.

Следует признать, что различные сетевые архитектуры могут предлагать отличающиеся друг от друга потенциальные возможности идентификации. Таким образом, организация может получить улучшение идентификации, выбрав соответствующую архитектуру сети. Необходимо рассматривать все возможности управления безопасностью выбранной архитектуры сети.

13.6.5 Безопасное одноразовое предъявление пароля

Там, где задействуют сетевые соединения, пользователи могут сталкиваться с многочисленными проверками идентификации и аутентификации. В подобных обстоятельствах у пользователей может возникнуть соблазн использовать небезопасные методы, такие, как запись паролей или повторное использо-

вание одних и тех же данных аутентификации. Безопасное одноразовое предъявление пароля может уменьшить риски подобных действий путем сокращения количества паролей, которые пользователь должен запомнить. Наряду с уменьшением рисков можно повысить продуктивность работы пользователя, а рабочие нагрузки «справочного стола», связанные с повторной установкой паролей, могут быть уменьшены.

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.

Следовательно, могут потребоваться механизмы идентификации и аутентификации мощнее обычных, и они могут быть востребованы для исключения идентификации и аутентификации функций с высокой степенью привилегированности (системный уровень) из режима безопасного одноразового предъявления пароля.

13.7 Протоколирование данных аудита и мониторинг сети

Очень важно обеспечить эффективность сетевой безопасности посредством протоколирования данных аудита и его текущего мониторинга с быстрым обнаружением и исследованием событий безопасности, сообщением о них и реагированием на них, а затем на инциденты. Без этой деятельности нельзя быть уверенным в постоянной эффективности мер безопасности и в том, что не будут происходить инциденты безопасности с неблагоприятными воздействиями на бизнес-операции.

В протоколе аудита необходимо регистрировать достаточный объем информации о состояниях ошибки и действительных событиях для осуществления тщательного анализа предполагаемых и фактических инцидентов. Однако, признавая то, что протоколирование огромного объема информации, связанной с аудитом, может затруднить управление анализом и повлиять на его продуктивность, со временем надо будет соблюдать осторожность в отношении протоколируемой информации. Для сетевых соединений необходимо протоколировать данные аудита, включающие следующие типы событий:

- дистанционные неудавшиеся попытки входа в систему с датой и временем;
- события неудачной повторной аутентификации (или использования маркера);
- нарушения трафика через шлюзы безопасности;
- дистанционные попытки получения доступа к протоколам аудита;
- предупреждения/аварийные сигналы для управления системой с последствиями для безопасности (например, дублирование IP-адреса, нарушения физической цепи).

В контексте сетей информация для протоколов аудита должна получаться от различных источников, таких, как маршрутизаторы, межсетевые экраны, системы обнаружения атак, и должна передаваться на центральный сервер аудита для объединения и тщательного анализа. Все протоколы аудита следует проверять как в режиме реального времени, так и в автономном режиме. В режиме реального времени протоколы аудита могут отображаться на экране прокрутки и быть использованными для предупреждения о потенциальных атаках. Автономный анализ имеет большое значение, так как он позволяет определять большую картину с помощью анализа тенденции. Первыми указаниями на атаку могут быть значительные «следы» в протоколах межсетевых экранов, указывающие на зондирующую деятельность по отношению к потенциальной цели. Система обнаружения атак также может это обнаружить в режиме реального времени по отношению к сигнатуре атаки. Таким образом, подчеркивается, что для получения быстрых, специализированных и понятных результатов надо быть очень осторожным при выборе правильного инструментария анализа протокола аудита.

Контрольные записи необходимо сохранять в оперативном режиме на определенный период в соответствии с потребностями организации и все контрольные записи необходимо дублировать и архивировать способом, гарантирующим их целостность и доступность, например с помощью носителей с однократной записью и многократным считыванием, таких, как компакт-диск. Кроме того, протоколы аудита содержат секретную информацию или информацию по использованию для тех, кто может захотеть атаковать систему через сетевые соединения, и обладание протоколами аудита может предоставить доказательство перемещения по сети в случае возникновения спора, в силу чего эти протоколы являются особенно необходимыми в контексте обеспечения целостности и неотказуемости. Следовательно, все протоколы аудита должны быть соответствующим образом защищены, включая случаи уничтожения архивированных компакт-дисков в назначенный срок. Контрольные записи должны храниться безопасным образом в течение периода времени, соответствующего требованиям организации и национальному законодательству. Также важно, чтобы для всех контрольных записей и связанных с ними серверов надлежащим образом учитывалась временная синхронизация, например при использовании протоколов NTP, особенно в ходе судебной экспертизы и при возможном судебном преследовании.

Текущий мониторинг должен охватывать:

- протоколы аудита межсетевых экранов, маршрутизаторов, серверов и т. д.;
- предупреждения/аварийные сигналы из протоколов аудита, предварительно конфигурированных для уведомления об определенных типах событий, от межсетевых экранов, маршрутизаторов, серверов и т. д.;
- выходные данные систем обнаружения атак;
- результаты деятельности сканирования сетевой безопасности;
- информацию о событиях и инцидентах, о которых сообщили пользователи и вспомогательный персонал;
- результаты анализа соответствия безопасности.

События могли оказаться инцидентом безопасности, но были предотвращены, например «ненадлежащий» вход в систему, или фактически вызвали инцидент, но были обнаружены, например распознавание пользователя, который совершил несанкционированное изменение базы данных.

Подчеркивается, что мониторинг сети должен проводиться способом, полностью согласующимся с соответствующими национальным и международным законодательством и положениями. Это подразумевает законодательство по защите данных и для регламентирования действий следственных органов (где по закону все пользователи должны быть проинформированы о мониторинге до его проведения). В общих чертах мониторинг следует проводить ответственно и не использовать, например, для анализа поведения сотрудников в странах с очень ограниченными нормами права, охраняющими неприкосновенность личной жизни. Очевидно, что проводимые действия необходимо согласовывать с политиками безопасности и неприкосновенности частной жизни организации и соответствующими процедурами. Протоколирование данных аудита и мониторинг сети также должны проводиться безопасным в правовом смысле образом, если свидетельство из протокола аудита необходимо использовать при уголовном или гражданском преследовании.

Большую часть мер безопасности по протоколированию данных аудита и мониторингу сети, востребованных в отношении сетевых соединений и информационных систем, связанных с ними, можно определить с помощью ИСО/МЭК 17799.

13.8 Обнаружение вторжений

По мере увеличения количества сетевых соединений злоумышленникам стало проще:

- находить многочисленные способы проникновения в информационные системы и сети организации или сообщества;
- маскировать свои исходные точки доступа;
- получать доступ через сети и внутренние информационные системы.

Кроме того, злоумышленники становятся более изощренными, а более усовершенствованные методы и средства атак — легкодоступными в Интернете или в открытой печати. Действительно, многие из этих средств являются автоматизированными, могут быть очень эффективными и простыми в использовании, в том числе для лиц с ограниченным опытом.

Для большинства организаций экономически невозможно предотвратить все потенциальные проникновения. Следовательно, велика вероятность осуществления каких-либо вторжений. Риски, связанные с большинством этих вторжений, надлежит рассматривать через призму внедрения качественных идентификации и аутентификации, логического контроля доступа, ведения учета и средства контроля аудита и, если это оправдано, вместе со способностью обнаружения вторжения. Подобный подход обеспечивает средства прогнозирования и идентификации вторжений в режиме реального времени и подачи соответствующих тревожных сигналов. Он также дает возможность локального сбора информации по вторжениям и последующего ее обобщения и анализа, а также анализа обычных моделей поведения/использования информационных систем организации.

Во многих ситуациях сразу становится ясно, что происходит несанкционированное или нежелательное событие. Это может быть незначительное ухудшение услуг по якобы неизвестным причинам, или неожиданное количество доступов в необычное время, или отказ в конкретных услугах. В большинстве ситуаций важно как можно скорее узнать причину, масштаб и область действия вторжения.

Следует отметить, что эта система обнаружения вторичных атак является более совершенной мерой обеспечения безопасности, чем средства и методы анализа протоколов аудита, изложенные в 13.7 и родственных пунктах ИСО/МЭК 17799. Более эффективные потенциальные возможности обнаружения вторжения используют специальные постпроцессоры, которые предназначены для использования правил автоматического анализа прошедших действий, зарегистрированных в контрольных записях и других про-

токолах для прогнозирования вторжений и для анализа контрольных записей известных моделей вредоносного поведения или поведения, которое не является типичным при обычном использовании.

Следовательно, система обнаружения атак (СОА) является системой обнаружения вторжений в сеть. Есть два типа СОА:

- сетевая система обнаружения сетевых атак (ССОСА);
- система обнаружения атак на хосты (СОАХ).

ССОСА осуществляет текущий контроль пакетов в сети и пытается обнаружить злоумышленника посредством сопоставления модели атаки с базой данных известных моделей атаки. Типичным примером является поиск большого количества запросов соединений протоколов TCP по многим различным портам на целевой машине, таким образом обнаруживая, что кто-то пытается сканировать порт протокола TCP. Система обнаружения вторжений сети наблюдает за сетевым трафиком посредством сплошного слежения за всем сетевым трафиком.

СОАХ осуществляет текущий контроль деятельности на хостах (серверах). Она осуществляет это путем мониторинга протоколов событий безопасности или проверки изменений в системе, таких, как изменения в критических файлах системы или реестре систем. Существует два типа СОАХ:

- программы контроля целостности системы, которые осуществляют текущий контроль системных файлов и реестра систем для выявления изменений, внесенных злоумышленниками;
- мониторинг протоколов (осуществление текущего контроля протоколов). Операционные системы порождают события безопасности, связанные с критически важными вопросами безопасности, например, пользователь получает привилегии на уровне администратора/корневого каталога.

В некоторых случаях реакции на обнаруженные вторжения могут быть автоматизированными в IDS.

Более подробная информация об обнаружении вторжений представлена в ИСО/МЭК 18043.

13.9 Защита от вредоносного кода

Пользователи должны знать, что через сетевые соединения в их среду может быть введен вредоносный код (вирус). Вредоносный код может заставить компьютер выполнять несанкционированные функции (например, бомбардировать данную цель сообщениями в данное число и время) или фактически уничтожить важные ресурсы (например, стереть файлы), как только он был продублирован, чтобы попытаться найти другие уязвимые хосты. Вредоносный код не может быть обнаружен до нанесения им ущерба, если только не применять соответствующие меры безопасности. Вредоносный код может привести к компрометации мер безопасности (например, захвату и раскрытию паролей), непреднамеренному раскрытию информации, непреднамеренным ее изменениям, уничтожению информации и /или несанкционированному использованию ресурсов системы.

Некоторые формы вредоносного кода могут быть обнаружены и удалены специальным сканирующим ПО. Сетевые экраны, файловые серверы и рабочие станции имеют сканеры для некоторых типов вредоносного кода. В дальнейшем для создания возможности обнаружения нового вредоносного кода очень важно обеспечить постоянное соответствие сканирующего ПО уровню современных требований, желательно посредством ежедневных обновлений. Однако пользователи и администраторы должны знать, что на сканеры нельзя полагаться для обнаружения всех вредоносных кодов (даже если это вредоносные коды определенного типа), так как постоянно появляются все новые формы вредоносного кода. Обычно для усиления защиты, предоставляемой сканерами (где они имеются), требуются другие формы безопасности.

Главной задачей ПО, предназначенного для борьбы с вредоносным кодом, стало сканирование информации и программ для идентификации подозрительных моделей, связанных с вирусами, «червями» и «троянскими конями» (которые иногда называют «вредоносное программное обеспечение»). Библиотека сканируемых моделей, известная как сигнатуры, должна обновляться через определенные промежутки времени или каждый раз, когда становятся доступными новые сигнатуры для предупреждений о вредоносном ПО с высокой степенью риска. В контексте удаленного доступа антивирусное ПО должно прогоняться на удаленных системах, а также на серверах центральной системы, особенно на серверах Windows и электронной почты.

Пользователи и администраторы систем с сетевыми соединениями должны знать, что существуют большие, чем обычно, риски, связанные с вредоносным программным обеспечением при взаимодействии со сторонними организациями по внешним каналам связи. Должны быть разработаны рекомендации для пользователей и администраторов, определяющие процедуры и практические приемы для сведения к минимуму возможности внедрения вредоносного кода.

Пользователи и администраторы должны особо позаботиться о конфигурировании систем и приложений, связанных с сетевыми соединениями, чтобы блокировать функции, которые не являются необходимыми в данных обстоятельствах. (Например, приложения ПК могут конфигурироваться таким образом, что макроячейки блокируются по умолчанию или требуют подтверждения пользователя перед выполнением макрокоманд.)

Более подробная информация о защите от вредоносного кода представлена в ИСО/МЭК 17799.

13.10 Криптографические услуги в общей инфраструктуре

13.10.1 Общие положения

Потребность в безопасности и повышении неприкосновенности частной жизни растет по мере вытеснения электронными формами своих бумажных эквивалентов. Появление сети Интернет и расширение корпоративных сетей для осуществления доступа клиентов и поставщиков, находящихся за пределами организации, усилили потребность в решениях, основанных на криптографии, для поддержки аутентификации и VPN, а также для обеспечения конфиденциальности.

13.10.2 Конфиденциальность данных в сетях

В условиях, когда сохранение конфиденциальности имеет большое значение, для шифрования информации, проходящей по сетевым соединениям, необходимо рассмотреть меры безопасности шифрования. При принятии решения об использовании мер безопасности шифрования необходимо принимать во внимание соответствующие правительственные законы и положения, требования к распределению ключей, пригодность использующихся механизмов шифрования для задействованного типа сетевого соединения и необходимую степень защиты. Механизмы шифрования стандартизованы в ИСО/МЭК 18033. Один широко применяемый метод шифрования известен как блочный шрифт, а способы использования блочных шрифтов для защиты шифрования (режимы работы) стандартизованы в ИСО/МЭК 10116.

13.10.3 Целостность данных в сетях

В условиях, когда сохранение целостности имеет большое значение, необходимо рассмотреть меры безопасности цифровой подписи и/или целостности сообщения для защиты информации, проходящей по сетевым соединениям. Меры безопасности цифровой подписи могут обеспечить подобную защиту мерам безопасности аутентификации сообщений, также они обладают свойствами, которые позволяют им выполнять процедуры неотказуемости (см. 13.10.4). При принятии решения об использовании мер безопасности цифровой подписи или целостности сообщений следует учитывать соответствующие правительственные законы и положения, соответствующие инфраструктуры открытого ключа, требования к распределению ключей и пригодность используемых базовых механизмов для задействованного типа сетевого соединения и необходимую степень защиты, а также надежное и доверительное протоколирование пользователей или объектов, связанных с ключами (при необходимости сертифицированными), используемыми в протоколах цифровой подписи.

Меры безопасности целостности сообщений, известные как коды аутентификации сообщений (КАС), стандартизованы в ИСО/МЭК 9797. Технологии цифровой подписи стандартизованы в ИСО/МЭК 9796 и ИСО/МЭК 14888.

13.10.4 Неотказуемость

При наличии требования предоставления убедительного доказательства прохождения информации по сети необходимо рассмотреть следующие меры безопасности:

- коммуникационные протоколы, предоставляющие подтверждение передачи;
- протоколы приложений, которые требуют предоставления адреса инициатора или идентификатора и проверяют наличие этой информации;
- шлюзы, которые проверяют форматы адреса отправителя и получателя на точность синтаксиса и соответствие информации в соответствующих каталогах;
- протоколы, которые подтверждают доставку из сетей и позволяют определять порядок следования информации.

Когда требуется подтверждение передачи или получения информации в случае возникновения спорной ситуации, необходимо предоставить гарантию, используя стандартный метод цифровой подписи. Когда требуется подтверждение источника, отправители информации должны опечатывать информацию, используя цифровую подпись по общему стандарту. При требовании подтверждения доставки отправители должны запросить ответ, снабженный цифровой подписью. Более подробная информация о неотказуемости представлена в ИСО/МЭК 14516 и ИСО/МЭК 13888.

13.10.5 Распределение ключей

13.10.5.1 Общие положения

Распределение ключей обеспечивает в качестве основной услуги среди всех других криптографических услуг управление всеми необходимыми ключами шифрования во время их полного жизненного цикла и их использование безопасным способом.

В то время как в очень маленьких средах лишь с несколькими соединениями это может быть достигнуто ручными организационными процедурами (например, посредством ручного коммутатора ключей симметричного шифрования), в более крупных средах необходимы предварительно определенные и автоматизированные процедуры, и в большинстве случаев использование технологий шифрования с помощью открытых/секретных ключей будет выгодным.

Технологии шифрования с помощью открытых/секретных ключей решают одну главную проблему технологий симметричного шифрования. Симметричные технологии требуют наличия одинакового ключа на обеих сторонах канала связи (их также называют совместно используемыми секретными технологиями) и, следовательно, предполагают передачу ключа симметричного шифрования. Так как сам ключ симметричного шифрования необходимо хранить в тайне, необходим заранее созданный защищенный канал передачи данных для обмена ключами. Технологии шифрования с помощью открытого/секретного ключа решают эту проблему путем предоставления двух ключей и необходимости передачи только одного из них другому объекту коммуникации. Поскольку этот ключ не является секретным (он называется открытым ключом), он может передаваться по открытым каналам связи. С другим ключом, не предназначенным для передачи, надо обращаться конфиденциально (он называется секретным ключом).

Однако еще остаются проблемы:

- аутентичная передача открытого ключа, или как аутентично получить открытый ключ другого объекта коммуникации;

- адекватная защита секретного ключа.

Передача открытого ключа должна гарантировать получение принимающим объектом открытого ключа, посылаемого передающим объектом. Другими словами, передача должна быть аутентичной, иначе возможный злоумышленник, наблюдающий за передачей открытого ключа, может обменять неузнанный ключ на другой.

Существует несколько методов проверки аутентичности переданного открытого ключа. Самый очевидный метод — проверка на тождественность посланного и полученного открытого ключа. Обычно это делается путем сравнения значений хеш-функции (в данном контексте часто называется «отпечаток пальцев») посланного ключа и полученного ключа интерактивным способом. Отправляющий и принимающий ключ объекты таким образом могут использовать отдельный канал (например, телефонную линию), и важно, чтобы этот канал позволял осуществлять должную аутентификацию отправляющего и принимающего объектов (например, если принимающий объект может установить подлинность отправляющего объекта посредством опознания его/ее голоса).

Поскольку этот двусторонний способ обмена открытым ключом работает при условии участия только небольшого количества общающихся объектов, он не является широко распространенным. Эту проблему можно решить путем введения инфраструктур, обеспечивающих открытым ключом каждый объект и сертифицирующих аутентичность предоставленных открытых ключей. Подобные инфраструктуры, обычно называемые инфраструктурами открытых ключей (ИОК), состоят из различных компонентов. Новые присоединяющиеся объекты протоколируются протоколирующим органом, основной задачей которого является проверка идентичности объекта. Основываясь на протоколировании, сертификационный орган может сертифицировать открытый ключ объекта, а службы каталогов обычно делают сертифицированные открытые ключи (обычно называемые просто «сертификаты») доступными всем объектам, предназначенным для использования системы. Технически сертификат состоит из определенного набора атрибутов объекта (примером является название и электронный адрес пользовательских объектов) и открытого ключа объектов, а аутентичность этой информации гарантирована цифровой подписью этой информации сертификационным органом.

Так как безопасность всех криптографических услуг, основанных на использовании открытых ключей, обеспечивается и управляется ИОК, основывается на аутентичности этих ключей, ИОК имеют очень высокие требования безопасности. Например, если злоумышленник получит доступ к инфраструктуре сертификационного органа, он/она сможет выпустить сертификаты, которые дадут им возможность выдавать себя за другие объекты.

По причинам, связанным с функциональными возможностями, большинство ИОК должно придаваться сети, следовательно, особое внимание должно быть уделено соответствующим мерам сетевой безопасности, чтобы было возможно выполнить все требования безопасности ИОК. Во многих случаях эти меры безопасности включают создание специальной сети для ключевых компонентов ИОК и для защиты этой сети соответствующими шлюзами безопасности или сетевыми экранами.

Что касается соответствующей защиты секретных ключей, эта защита также является критически важной для безопасности, так как, если злоумышленник имеет доступ к секретному ключу объекта, он/она может иметь возможность выдать себя за этот объект. Обычно в зависимости от требований безопасности конкретных организаций, среды или приложений есть несколько решений этой проблемы.

Самое простое решение — защита секретного ключа путем хранения его в симметрично зашифрованной форме в системах организации или, что немногим лучше, на съемных носителях. Тогда ключ объекта обычно находится в пароле (который составляет ключ симметричного шифрования) для разблокирования секретного ключа и чтобы сделать его доступным для сервисов и приложений в целях дальнейшего использования. Основываясь полностью на программном обеспечении, это решение дает значительное преимущество и, следовательно, может относительно легко быть реализовано в различных условиях. Однако с точки зрения безопасности у него имеются крупные недостатки, так как защита:

- зависит от качества выбранного пароля;

- полагается на целостность системы, используемой объектом. Если злоумышленник получает контроль над этой системой, он/она может скопировать секретный ключ, хранящийся в памяти в незашифрованном виде, во время обработки криптографических функций, или он/она может достичь этого же результата, получая пароль и открытый ключ объекта в зашифрованном виде.

Для преодоления этих недостатков есть решения, основанные на применении смарт-карт, базирующиеся на двух факторах: аутентификации для получения доступа к секретному ключу (обычно это обладание смарт-картой) и знании пароля или PIN-кода для его открытия. Их архитектура гарантирует, что секретный ключ никогда не покинет смарт-карту, что подразумевает обработку всех криптографических вычислений, требующих применения секретного ключа, на самой смарт-карте. Значительным преимуществом является то, что это решение защищает секретный ключ даже в ситуациях, когда компрометируется целостность системы, использующейся объектом. Основной недостаток решений, основанных на применении смарт-карт, заключается в необходимости распределять и интегрировать конкретную аппаратуру, связанную со смарт-картами, по объектам и их системам. Хотя в этой области существуют технические стандарты, сам процесс обычно является довольно сложным и дорогостоящим.

Важно отметить, что в этом пункте представлен только краткий обзор процесса распределения ключей. Более подробная информация по этой теме и родственным темам, таким, как ИОК, или более всеобъемлющим темам, таким, как управление тождественностью, содержится в документах и стандартах:

- ИСО/МЭК 9594-8 Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 8. Система понятий аутентификации;

- ИСО/МЭК 11770 (все части) Информационная технология. Методы и средства обеспечения безопасности. Управление ключами;

- ИСО 11166-2 Банковское дело. Управление ключами с помощью ассиметричных алгоритмов. Часть 2. Утвержденные алгоритмы с использованием криптосистемы RSA;

- ИСО 11568 (все части) Банковское дело. Управление ключами. Розничная торговля;

- ИСО 11649 Финансовые услуги. Банковское дело. Структурированная кредиторская ссылка на информацию о пересылаемой сумме;

- ИСО 13492 Банковское дело. Элемент данных, связанный с управлением ключами. Применение и использование элементов данных 53 и 96 по ISO 8583;

- ИСО 21118 Информация, включаемая в спецификационные листы. Проекторы данных.

13.10.5.2 Вопросы безопасности

Существует ряд вопросов безопасности, которые должны быть рассмотрены в контексте распределения ключей, в особенности при использовании или реализации услуг ИОК.

Эти вопросы охватывают следующие темы:

- область действия и использование — использование ИОК по назначению оказывает значительное влияние на состояние безопасности. Например, использование выданных сертификатов влияет главным образом на требования безопасности ИОК;

- политики — предоставляемые услуги ИОК и их назначение, уровень реализованной защиты в ИОК и процессы взаимодействия должны соответствующим образом документироваться в сертификационной политике и положении о сертификационной практике;

- вопросы реализации — организация может выбрать реализацию ИОК на месте («ИОК для внутреннего пользования»), или может принять решение просто закупить услуги ИОК («приобретенные на стороне ИОК»), или может выбрать комбинацию того и другого (например, закупать только ключевые сертификационные услуги, а реализовывать другие услуги, такие, как каталог роуминга, локально);

- конкретные функциональные требования, например для пользователей роуминга, — многие функциональные требования нуждаются в конкретных мерах безопасности. Например, как обеспечить защиту секретных ключей и доступ к сертификатам для пользователей роуминга; одним из решений является использование смарт-карт (см. ниже);

- использование смарт-карт — смарт-карты могут быть использованы для выполнения более строгих требований безопасности (например, как упоминается в 13.10.5.1) или решения проблем в контексте пользователей роуминга. Однако использование смарт-карт требует более тщательного рассмотрения таких вопросов, как процесс жизненного цикла смарт-карт, физическое распространение смарт-карт и манипулирование ими, процесс восстановления после отказа (например, когда пользователь забывает свою смарт-карту), вопросов безопасности, связанных с использованием аппаратуры считывающего устройства и соответствующим интеграционным программным обеспечением в системе клиента;

- оперативные вопросы, например функционирование в оперативном /автономном режиме корневого сертификационного органа, — для выполнения установленных требований безопасности могут использоваться специфические эксплуатационные меры. Например, использование в автономном режиме сертификационного органа корневого каталога, когда его услуги не востребованы, в сочетании с адекватной физической защитой может обеспечить более высокий уровень защиты самых секретных частей системы.

13.11 Управление непрерывностью бизнеса

Важно наличие мер безопасности для гарантирования непрерывности функционирования бизнеса в случае аварийной ситуации путем обеспечения способности восстановления каждой части бизнес-процесса после нарушения его хода за соответствующий интервал времени. Таким образом, у организации должна быть программа управления непрерывностью бизнеса с процессами, охватывающая все стороны обеспечения непрерывности бизнеса и включающая:

- установление приоритетов восстановления бизнеса;

- временные интервалы и требования (поддерживается проверкой анализа влияния на бизнес);

- формулирование стратегии обеспечения непрерывности бизнеса;

- разработку планов непрерывности бизнеса, тестирование планов непрерывности бизнеса, что обеспечивает осведомленность всего персонала о непрерывности бизнеса;

- поддержание плана непрерывности бизнеса и снижение риска.

Только следование этим стадиям может гарантировать, что:

- необходимые приоритеты бизнеса и временные интервалы согласуются с потребностями бизнеса;

- идентифицированные предпочтительные версии стратегий непрерывности бизнеса соответствуют этим приоритетам и временным интервалам;

- существуют и протестированы корректные и необходимые планы и средства, охватывающие информацию, бизнес-процессы, информационные системы и услуги, речевую связь и передачу данных, людей и физическое оборудование.

Руководство по управлению непрерывностью бизнеса в целом, включая разработку соответствующей стратегии непрерывности бизнеса и связанных с ней планов и их последующее тестирование, можно получить в ИСО/МЭК 17799.

В перспективе при организации сети следует учитывать поддержание сетевых соединений, внедрение альтернативных соединений с достаточной пропускной способностью и восстановление соединений после нежелательного события. Эти аспекты и требования должны быть основаны на важности соединений для функционирования бизнеса по прошествии времени и прогнозируемых неблагоприятных воздействий на бизнес в случае нарушения бизнес-процесса. В то время как способность к подключению может давать много преимуществ организации в отношении гибкости и способности использовать креативные подходы в случае нарушения бизнес-процесса, они также могут иметь точки уязвимости и отдельные точки сбоя, которые могут оказать сильное разрушающее воздействие на организацию.

14 Реализация и функционирование мер безопасности

После определения, документирования и согласования архитектуры технической безопасности и мер безопасности должны внедряться меры сетевой безопасности. Перед тем как разрешить начало операций по организации сети, должны быть проверены, обсуждены и протестированы любые выявленные недостатки безопасности (см. раздел 15). Затем после оценки состояния безопасности должны начинаться рабочие операции. По прошествии времени и в случае возникновения значительных изменений следует проводить дальнейшие проверки внедрения (см. раздел 15).

15 Мониторинг и анализ ввода в эксплуатацию

Как указано в разделе 14, первый ввод в эксплуатацию должен быть проверен на соответствие документированной архитектуре технической безопасности и требуемым мерам безопасности, определенным в следующих документах:

- архитектура технической безопасности;
- политика безопасности организации сети;
- родственные вспомогательные операции;
- политика (безопасности) доступа к услугам шлюза безопасности;
- план(ы) непрерывности бизнеса;
- условия безопасности для соединения (при необходимости).

Проверка на соответствие должна быть завершена до оперативной эксплуатации. Проверка считается полной, когда все недостатки выявлены и устранены, что утверждено высшим руководством. В процессе оперативной эксплуатации также необходимо проводить текущий мониторинг и проверочные действия, особенно перед выпуском значительной новой версии, связанной с большими изменениями в бизнес-потребностях, технологии и решениях по безопасности и т. д., в остальных случаях — ежегодно.

Важно, что мониторинг и проверка должны включать проведение тестирования безопасности по признанным стандартам с предварительно разработанными стратегией тестирования безопасности и связанными с ней планами, точно устанавливая, какие тесты, с чем, где и когда следует проводить. Обычно при этом должна быть использована комбинация сканирования уязвимости и тестирования на проникновение. Перед началом подобного тестирования необходимо проверить план тестирования, чтобы гарантировать, что оно будет проведено способом, полностью совместимым с соответствующим законодательством. При проведении этой проверки не следует забывать, что сеть может не быть ограничена только одной страной, она может быть распространена в различных странах с разным законодательством. После тестирования в отчетах должны быть указаны особенности обнаруженных уязвимостей, требуемые пути и очередность их устранения с приложением, подтверждающим, что были применены все согласованные решения проблем. Такие отчеты должно утверждать высшее руководство.

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 наименование соответствующего национального стандарта
ИСО/МЭК 18028-2:2005	—	*
ИСО/МЭК 18028-3:2005	—	*
ИСО/МЭК 18028-4:2005	—	*
ИСО/МЭК 18028-5	—	*
ИСО/МЭК 13335-1:2004	IDT	ГОСТ Р ИСО/МЭК 13335-1—2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»
ИСО/МЭК 17799:2005	IDT	ГОСТ Р ИСО/МЭК 17799—2005 «Информационная технология. Практические правила управления информационной безопасностью»
ИСО/МЭК 18044:2004	IDT	ГОСТ Р ИСО/МЭК ТО 18044—2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
ИСО/МЭК 18043	—	*
ИСО/МЭК ТО 14516:2002	—	*
ИСО/МЭК 13888:2004	—	*
ИСО/МЭК 7498-1:1994	IDT	ГОСТ Р ИСО/МЭК 7498-1—1999 «Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»
ИСО 7498-2:1989	IDT	ГОСТ Р ИСО 7498-2—1999 «Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»
ИСО 7498-3:1997	IDT	ГОСТ Р ИСО 7498-3—1997 «Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 3. Присвоение имен и адресация»
ИСО/МЭК 7498-4:1989	IDT	ГОСТ Р ИСО/МЭК 7498-4—1999 «Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления»
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 10181:1996	—	*

* 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.

Библиография

ИСО/МЭК ТО 14516:2002	Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по применению и управлению услугами доверенной третьей стороны
ISO/IEC TR 14516:2002	(Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services)
ИСО/МЭК 13888 (все части)	Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость
ISO/IEC 13888 (all pats)	(Information technology — IT security techniques — Non-repudiation)
ИСО/МЭК 7498-1:1994	Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
ISO/IEC 7498-1:1994	(Information technology — Open Systems Interconnection. Basic Reference Model. Part 1: The Basic Model)
ИСО 7498-2:1989	Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2. Архитектура безопасности
ISO 7498-2:1989	(Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture)
ИСО 7498-3:1997	Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 3. Присвоение имен и адресация
ISO 7498-3:1997	(Information technology — Open Systems Interconnection — Basic Reference Model — Part 3: Naming and addressing)
ИСО/МЭК 7498-4:1989	Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 4. Схема управления
ISO/IEC 7498-4:1989	(Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework)
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 10181-1:1996	Информационная технология. Взаимодействие открытых систем. Схемы безопасности для открытых систем. Часть 1. Общие положения
ISO/IEC 10181-1:1996	(Information technology — Open Systems Interconnection —Security frameworks for open systems — Part 1:Overview)

Комитет IETF Справочник по безопасности узлов (RFC 2196), сентябрь 1997 г.
(Site Security Handbook (RFC 2196))
Комитет IETF Протокол IP Дорожная карта документации по безопасности
(IP Security Document Roadmap (RFC 2411))
Комитет IETF Архитектура безопасности протокола IP (RFC 2401), ноябрь 1998 г.
(Security Architecture for the Internet Protocol (RFC 2401))
Комитет IETF Распределение адресов для частных Интернет-сетей (RFC 1918), февраль 1996 г.
(Address Allocation for Private Internets (RFC 1918))
Комитет IETF Протокол SNMP Протоколы безопасности (RFC 1352), июль 1992 г.
(SNMP Security Protocols (RFC 1352))
Комитет IETF Глоссарий по компьютерной безопасности (RFC 2828), май 2000 г.
(Internet Security Glossary (RFC 2828))
NIST Специальная публикация серия 800 по компьютерной безопасности, включая: Специальная публикация 800-10 NIST: Поддержание безопасности вашего компьютера: Вводная часть по сетевым экранам
(NIST Special Publications 800 series on Computer Security, including:
NIST Special Publication 800-10: Keeping Your Site Comfortably Secure: An Introduction to Firewalls)

УДК 351.864.1:004:006.354 ОКС 35.040 Т00

Ключевые слова: информационная технология, сетевая безопасность, менеджмент сетевой безопасности

Редактор *П. М. Смирнов*
Технический редактор *В. Н. Прусакова*
Корректор *Е. Ю. Митрофанова*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 03.05.2011. Подписано в печать 04.07.2011. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. 6,51. Уч.-изд. л. 5,80. Тираж 114 экз. Зак. 451

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru