"ГОСТ Р ИСО/МЭК ТО 13335-5-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети"
(утв. и введен в действие Приказом Ростехрегулирования от 19.12.2006 N 317-ст)

Утвержден и введен в действие
Приказом Федерального агентства
по техническому регулированию
и метрологии
от 19 декабря 2006 г. N 317-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

ЧАСТЬ 5

РУКОВОДСТВО ПО МЕНЕДЖМЕНТУ БЕЗОПАСНОСТИ СЕТИ

**Information technology. Security techniques.
Part 5. Management guidance on network security**

**ISO/IEC TR 13335-5:2001
Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security
(IDT)**

ГОСТ Р ИСО/МЭК ТО 13335-5-2006

Группа Т00

ОКС 13.110
35.020

Дата введения
1 июня 2007 года

Предисловие

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

Сведения о стандарте

1. Подготовлен Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России") на основе собственного аутентичного перевода стандарта, указанного в пункте 4.

2. Внесен Техническим комитетом по стандартизации ТК 10 "Перспективные производственные технологии, менеджмент и оценка рисков".

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2006 г. N 317-ст.

4. Настоящий стандарт идентичен международному отчету ИСО/МЭК ТО 13335-5:2001 "Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 5. Руководство по менеджменту безопасности сети" (ISO/IEC TR 13335-5:2001 "Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security").

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

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

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

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт представляет собой руководство по управлению безопасностью сетями для персонала, ответственного за эту деятельность, и содержит основные положения по выявлению и анализу факторов, имеющих отношение к компонентам безопасности связи. Эти факторы следует учитывать при установлении требований по безопасности сети.

Настоящий стандарт основан на положениях ИСО/МЭК 13335-4 путем описания метода идентификации и анализа выбора контролируемых зон, имеющих отношение к сетевым соединениям, с точки зрения обеспечения безопасности.

Аспекты детального проектирования и технической реализации контролируемых зон не входят в область применения настоящего стандарта. Такие рекомендации планируется включить в разрабатываемые международные документы.

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК ТО 7498-1:1994 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Базовая модель

ИСО/МЭК ТО 7498-2:1998 Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты

ИСО/МЭК ТО 7498-3:1997 Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель: присвоение имен и адресация

ИСО/МЭК ТО 7498-4:1989 Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Структура управления

ИСО/МЭК 13335-1:2004 Информационная технология. Методы обеспечения менеджмента безопасности информационных и телекоммуникационных технологий. Часть 1. Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий

ИСО/МЭК ТО 13335-3:1998 Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 3. Методы управления безопасностью информационных технологий

ИСО/МЭК ТО 13335-4:2000 Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 4. Выбор мер защиты

ИСО/МЭК 13888 (все части) Информационная технология. Методы защиты. Строгое выполнение обязательств

ИСО/МЭК ТО 14516:2002 Информационная технология. Руководящие указания по использованию и управлению услугами доверительной третьей стороны

ИСО/МЭК ТО 15947:2002 Информационная технология. Методы защиты. Основные положения по обнаружению проникновения в информационные технологии

Ссылки на другие документы, имеющие отношение к рассматриваемой теме, приведены в библиографии [1] - [3].

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем стандарте применены термины по ИСО/МЭК 13335-1.

4. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем стандарте применены следующие обозначения и сокращения:

EDI - электронный обмен данными;

IP -протокол Интернет;

ИТ - информационная технология;

ПК - персональный компьютер;

PIN - личный идентификационный номер;

SecOPs - защитные операционные процедуры.

5. СТРУКТУРА

Настоящий стандарт основан на следующем подходе: вначале проводится процесс идентификации и анализа факторов, влияющих на средства связи, в целях установления требований по сетевой безопасности, и затем определяются потенциальные контролируемые зоны. При этом указывается, где можно использовать соответствующие положения других частей ИСО/МЭК 13335.

В настоящем стандарте приведено описание трех основных критериев идентификации потенциальных контролируемых зон в помощь лицам, ответственным за обеспечение безопасности ИТ. Эти критерии распознают:

1) разные типы сетевых соединений;

2) характеристики разной организации сети, соответствующие доверительные отношения и

3) потенциальные виды рисков обеспечения безопасности, связанного с сетевыми соединениями (использованием услуг, предоставляемых через эти соединения).

Результаты комбинирования этих критериев затем используют для индикации потенциальных контролируемых зон. Приводится также краткое описание потенциальных контролируемых зон с указанием источников, где они характеризуются более подробно.

6. ЦЕЛЬ

Цель настоящего стандарта - дать руководство для идентификации и анализа факторов, относящихся к безопасности средств связи. Эти факторы следует учитывать для того, чтобы устанавливать требования по безопасности сети и указывать на потенциальные контролируемые зоны.

7. ОБЩЕЕ ПРЕДСТАВЛЕНИЕ

7.1. Предпосылка

Государственные и коммерческие организации в большой степени полагаются на использование информации при ведении своего бизнеса. Нарушение таких характеристик информации и услуг, как конфиденциальность, целостность, доступность, неотказуемость, подотчетность, аутентичность и достоверность, может иметь неблагоприятное воздействие на деловые операции и бизнес организации. Поэтому существует необходимость в обеспечении безопасности информации и управлении безопасностью систем ИТ в пределах организации.

Необходимость в обеспечении безопасности информации особенно важна в современном информационном пространстве, так как многие системы ИТ организаций объединяются в сети. Сетевые соединения могут находиться в границах самой организации, между разными организациями и иногда между организацией и сетями общего пользования. Государственные и

коммерческие организации ведут свою деятельность универсально. Поэтому организации зависят от всех видов связи - от использующих автоматизированные системы информационного обслуживания до использующих "классические" средства. Их потребности в сетях должны быть удовлетворены, при этом обеспечению безопасности сетей придается все большее значение.

Рекомендации по идентификации и анализу факторов, относящихся к обеспечению безопасности средств связи, приведены в 7.2. Эти факторы следует принимать во внимание для того, чтобы устанавливать требования к безопасности сетей и указывать на потенциальные контролируемые зоны. Эти процессы более подробно рассмотрены в последующих разделах.

7.2. Процесс идентификации

При рассмотрении сетевых соединений всем ответственным специалистам организации следует четко представлять себе требования бизнеса и преимущества конкретных средств связи. Кроме того, специалисты и другие пользователи соединений должны быть осведомлены о рисках обеспечения безопасности и соответствующих контролируемых зонах сетевых соединений. Требования бизнеса и преимущества в обеспечении безопасности оказывают влияние на многие решения и действия, осуществляемые в процессе рассмотрения сетевых соединений, выявления контролируемых зон и последующего выбора, проектирования, внедрения и поддержания безопасности с помощью защитных мер. Следовательно, в течение всего процесса следует помнить об этих требованиях бизнеса и ожидаемых преимуществах. Для того чтобы идентифицировать заданные требования безопасности, имеющие отношение к сети, и контролируемые зоны, необходимо решить следующие задачи:

- анализ общих требований к обеспечению безопасности сетевых соединений, изложенных в политике безопасности ИТ организации (см. раздел 8);

- анализ сетевой структуры и ее применения, который имеет отношение к сетевым соединениям, чтобы иметь необходимую основу для выполнения последующих задач (см. раздел 9);

- идентификация типа или типов рассматриваемого соединения сети (см. раздел 10);

- анализ характеристик предложенного объединения в сеть (используя при необходимости имеющуюся информацию о применении структуры сети) и связанные с этим доверительные отношения (см. раздел 11);

- определение видов рисков безопасности, если это возможно, с помощью анализа рисков и управления результатами проведенного анализа, включая оценки деловых операций и информацию, которую предполагается передавать через соединения, и любую другую информацию, потенциально доступную для несанкционированного получения через эти соединения (см. раздел 12);

- идентификация потенциально контролируемых зон, которые могут быть использованы на основе анализа типа(ов) соединения и характеристик организации сети и связанных с этим доверительных отношений, а также видов установленных рисков безопасности (см. раздел 13);

- разработка документации и анализ вариантов структуры обеспечения безопасности (см. раздел 14);

- распределение задач по детальному выбору защитных мер, проектированию, реализации и их обслуживанию, используя идентифицированные потенциально контролируемые зоны и согласованную структуру обеспечения безопасности (см. раздел 15).

Общие рекомендации по идентификации защитных мер содержатся в ИСО/МЭК ТО 13335-4. Настоящий стандарт дополняет ИСО/МЭК ТО 13335-4 и представляет процесс выбора подходящих контролируемых зон с точки зрения обеспечения безопасности, связанной с подключениями к сетям связи.

Общий процесс идентификации и анализа факторов, относящихся к средствам связи, представлен на рисунке 1. Факторы, относящиеся к средствам связи, следует принимать во внимание для того, чтобы устанавливать требования к обеспечению безопасности сети и указывать на потенциальные контролируемые зоны. Каждый этап этого процесса подробно изложен в последующих разделах настоящего стандарта.

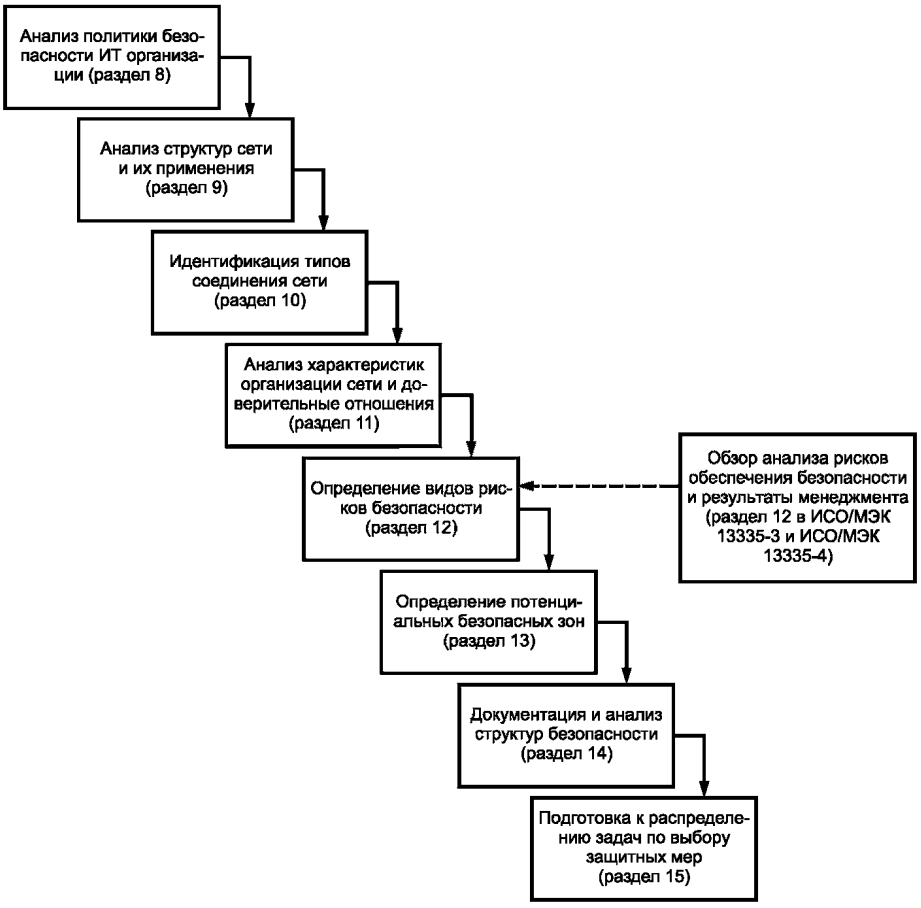

Рисунок 1. Процесс идентификации и анализа факторов, относящихся к средствам связи и ведущих к установлению требований безопасности сети

На рисунке 1 сплошными линиями представлен главный путь процесса. Пунктиром отмечены случаи, когда виды риска обеспечения безопасности могут быть установлены на

основе результатов их анализа и управления результатами этого анализа.

В дополнение к главному пути процесса на некоторых этапах может возникнуть необходимость вернуться к результатам предыдущих этапов для сохранения последовательности, в частности, к этапам "Анализ политики организации по безопасности ИТ" и "Анализ структур сети и их применений". Например, в следующих ситуациях:

- после установления риска обеспечения безопасности может потребоваться анализ политики безопасности ИТ организации, если что-то не учтено на уровне политики;

- если при идентификации потенциальных контролируемых зон необходимо принимать во внимание политику безопасности ИТ организации, потому что в ней может быть задано, что определенная безопасность должна быть реализована по всей организации, независимо от рисков;

- если необходимо обеспечить совместимость при выборе варианта структуры безопасности и проведения анализа структур сети и их применения.

8. АНАЛИЗ ТРЕБОВАНИЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ИТ ОРГАНИЗАЦИИ

Политика организации по безопасности ИТ включает в себя решения о необходимости обеспечения характеристик конфиденциальности, целостности, неотказуемости, подотчетности, аутентичности и достоверности передачи/приема сообщений, а также взгляды на типы угроз и требования безопасности, имеющие непосредственное отношение к сетевым соединениям.

Например, в соответствии с политикой организации по безопасности ИТ следует принять решение о том, что:

- доступность некоторых типов информации или услуг является предметом рассмотрения;

- никакие соединения не разрешаются через коммутируемые линии связи;

- все соединения с Интернетом должны быть через переход межсетевого экрана;

- должен применяться конкретный тип перехода межсетевого экрана;

- никакие платежные инструкции не являются действительными без цифровой подписи.

Такие решения, мнения и требования, приемлемые в масштабе организации, должны быть приняты во внимание при определении видов риска обеспечения безопасности (см. раздел 12) и идентификации потенциальных контролируемых зон для сетевых соединений (см. раздел 13). При наличии каких-либо требований к обеспечению безопасности они могут быть подтверждены документами в виде предварительного перечня потенциальных контролируемых зон и, при необходимости, отражены в вариантах структуры обеспечения безопасности. Место документа по политике безопасности ИТ в рамках подхода организации к безопасности ИТ, его содержание и отношение с другими аналогичными документами приведены в ИСО/МЭК ТО 13335-3.

9. АНАЛИЗ СТРУКТУР СЕТИ И ИХ ПРИМЕНЕНИЯ

9.1. Введение

Выполняют следующие последовательные этапы процесса подтверждения потенциальных контролируемых зон, т.е. идентифицируют:

- типы соединения сети, которые планируется использовать;

- характеристики сети и соответствующих вовлеченных доверительных отношений;

- виды риска обеспечения безопасности.

Список потенциальных контролируемых зон (а позднее - соответствующих проектов безопасности определенного соединения) всегда следует составлять в контексте структуры сети, уже существующей или планируемой к использованию, и ее применения.

Таким образом, следует обстоятельно изучить соответствующую структуру сети и ее применение для того, чтобы обеспечить необходимое понимание и контекст последующих этапов процесса.

При выяснении этих аспектов, по возможности, на ранней стадии процесс идентификации соответствующих критериев определения требований к обеспечению безопасности, выявления потенциальных контролируемых зон и уточнения безопасной структуры становится более эффективным. Результатом этого процесса будет выбор наиболее выполнимого решения по обеспечению безопасности (см. 9.2 и 9.5).

В то же время рассмотрение структурных аспектов сети и их применение на ранней стадии предоставляет возможность для анализа и возможного пересмотра этих структур, если приемлемое решение обеспечения безопасности не может быть реально выполнено в пределах имеющейся структуры сети.

В процессе принятия решения о структурах сети и их применении необходимо рассматривать разные их аспекты, в том числе:

- типы сети;

- протоколы сети;

- применение сети.

Некоторые вопросы для анализа этих аспектов рассмотрены в 9.2 и 9.4, другие - в 9.5.

Общее руководство по структурам сети и их применению - в стандартах серии ИСО/МЭК ТО 7498.

9.2. Типы сети

В зависимости от площади развертывания сети подразделяют на следующие типы:

- локальные (вычислительные), используемые для местного соединения систем;

- региональные (вычислительные), используемые для соединения систем в пределах региона;

- глобальные, используемые для соединения систем в более широких масштабах, чем региональные, вплоть до глобальных.

9.3. Протоколы сети

Разные протоколы имеют свои характеристики обеспечения безопасности и требуют специального рассмотрения, например:

- протоколы коллективного пользования средой используются главным образом в локальных сетях (иногда в масштабе региона) и обеспечивают механизмы регулирования коллективного использования среды между системами. При коллективном использовании среды вся информация физически доступна с помощью всех подсоединенных систем;

- маршрутные протоколы используются для определения пути через узлы, по которым информация распространяется в пределах локальных и региональных сетей. Информация физически доступна для всех систем вдоль маршрута, который может быть случайно или преднамеренно изменен.

Протоколы могут быть применены на разных сетевых топологиях, например, в виде шины, кольца или звезды, с реализацией через беспроводные или другие средства связи, которые могут оказывать дополнительное влияние на обеспечение безопасности.

9.4. Сетевые приложения

Тип приложений, используемых в сети, необходимо рассматривать в контексте обеспечения безопасности, и типы могут включать в себя:

- приложение на основе эмуляции терминала;

- приложение на основе запоминающего устройства (прямого применения или программы планировщика);

- серверные приложения клиента.

9.5. Дополнительное соображение

При анализе структуры сети и ее применения следует рассмотреть существующие сетевые входящие или исходящие соединения в пределах организации, а также сеть, с которой предлагается соединение. Существующие соединения организации могут ограничивать или не допускать новые соединения, например, по условиям соглашений или контрактов. Присутствие других входящих или исходящих соединений сети, к которой требуется соединение, может внести дополнительную уязвимость и, следовательно, создать риски более высокого уровня, потребовав более высокой безопасности и/или дополнительных защитных мер.

10. ИДЕНТИФИКАЦИЯ ТИПОВ СЕТЕВОГО СОЕДИНЕНИЯ

Существует много однородных типов сетевого соединения, которые может использовать организация. Некоторые типы соединений могут быть осуществлены через частные сети (доступ ограничен до известного сообщества), другие - через сеть общего пользования (доступ потенциально разрешен для любой организации или конкретного лица). Далее эти типы сетевого

соединения могут быть использованы для предоставления разнообразных услуг, например, электронной почты или EDI, и для применения средств сетей Интернет, Интранет или Экстранет, каждая из которых может потребовать отдельного рассмотрения безопасности. Каждый из типов соединений может иметь разные уязвимости и, следовательно, соответствующие риски безопасности, которые, в конечном счете, потребуют разного набора защитных мер.

Путь распределения по категориям однородных типов сетевого соединения, которое может потребоваться для бизнеса, с описанием примера, показанного для каждого типа, представлен в таблице 1.

Таблица 1

Типы сетевого соединения

Номер пункта	Тип сетевого соединения	Пример
10.1	Соединение в пределах одной контролируемой территории организации	Взаимная связь между разными частями одной и той же организации в пределах одной и той же контролируемой территории, т.е. одиночное контролируемое здание или помещение
10.2	Соединение между разными территориально удаленными частями одной и той же организации	Взаимная связь между региональными офисами (и/или региональных офисов с местом расположения головного офиса компании). В этом типе соединения большинство пользователей (если не все) имеют возможность подключения к системам ИТ, доступным через сеть. Однако не все пользователи в пределах организации наделены полномочиями для доступа ко всем приложениям или информации (т.е. каждое подключение пользователя осуществляется в соответствии с предоставленными привилегиями). Один доступ из другой части организации может служить для дистанционного технического обслуживания
10.3	Соединения между узлом связи организации и персоналом, работающим в местах, удаленных от организации	Использование работниками мобильных терминалов обмена данными (например, продавцом, проверяющим наличие запаса от покупателя) или установление работниками дистанционных линий связи с вычислительной системой организации из дома или другого удаленного места, не связанного через сеть этой организации. В этом типе сетевого соединения пользователь имеет полномочия использовать свою локальную систему

10.4	Соединения между разными организациями в границах закрытого сообщества, например по причине контрактных или других законных обязывающих ситуаций или интересов бизнеса (банковских операций или страхования)	Связь между двумя или большим числом организаций в случае, если существует потребность бизнеса способствовать электронным транзакциям (например, электронный перевод платежей в банковской сфере деятельности). Этот тип соединения аналогичен типу по пункту 10.2, за исключением того, что соединяемые узлы связи принадлежат двум или более организациям и соединения не предназначены обеспечивать доступ ко всему пакету приложений, используемых каждой участвующей организацией
10.5	Соединения с другими организациями	Следует иметь удаленные базы данных, поддерживаемые другими организациями (например, через предоставляемые услуги). В этом типе сетевого соединения внешняя организация, к информации которой разрешается доступ, заранее наделяет индивидуальными полномочиями всех пользователей, в том числе из соединяющих организаций. Однако хотя все пользователи заранее наделяются такими полномочиями, нет возможности проверки потенциальных пользователей иначе чем через их способность платить за предлагаемые услуги. Следует иметь также доступ к приложениям в системах организации, хранящей или обрабатывающей технологическую информацию, которая может быть предоставлена пользователям из внешних организаций. В таких условиях внешние пользователи были бы известны и уполномочены

10.6	Соединение с однородными областями общего пользования	Пользователи и организации могут инициировать доступ к общим базам данных, веб-сайтам и/или электронной почте (через Интернет) в случае, если это делается с целью получения или передачи информации между абонентами или узлами связи, которые организация специально заранее не наделила полномочиями. В этом типе соединения пользователи организации могли бы использовать упомянутые выше средства для организационных (возможно даже частных) целей, однако организация в таком случае контролирует незначительный объем передаваемой информации. Доступ может быть инициирован внешними пользователями средств организации (через Интернет). В этом типе сетевого соединения организация не может персонально санкционировать доступ для конкретных внешних пользователей заранее

При должном учете сетевых структур и их применения (см. раздел 9) следует выбрать один или более типов, представленных в таблице 1 и подходящих для рассматриваемых сетевых соединений.

Следует заметить, что однородные типы сетевого соединения, изложенные в настоящем стандарте, могут быть организованы и распределены по категориям преимущественно с точки зрения перспектив бизнеса, а не технических средств. Это означает, что два разных типа сетевого соединения могут быть иногда реализованы аналогичными техническими средствами, и в одних случаях защитные меры могут быть как одинаковыми, так и (в других случаях) разными.

11. АНАЛИЗ ХАРАКТЕРИСТИК СЕТИ И СВЯЗАННЫХ С НИМИ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ

11.1. Характеристики сети

Характеристики существующих или планируемых сетей следует регулярно пересматривать. Особенно важно выяснить:

- является ли сеть сетью общего пользования и доступна ли для любого абонента;

- частная ли это сеть, состоящая из собственных или арендованных линий связи и поэтому считающаяся более защищенной по сравнению с сетью общего пользования.

Важно также знать тип данных, транспортируемых сетью, например:

- сеть передачи данных, предназначенная главным образом для обмена данными с использованием соответствующих протоколов;

- сеть для речевых сообщений, предназначенная для телефонной связи, но также используемая для передачи данных;

- сеть, обеспечивающая телефонную связь и передачу данных.

Целесообразна также информация о том, является ли сеть коммутируемой или обеспечивает связь с коммутацией пакетов сообщений.

Следует также определить, является ли соединение постоянным или устанавливается по потребности.

11.2. Доверительные отношения

Поскольку характеристики существующих или предложенных сетей уже идентифицированы и, как минимум, установлено, является ли сеть общей или частной (11.1), то необходимо идентифицировать связанные с ними доверительные отношения.

Во-первых, необходимо идентифицировать доверительную среду(ы), связанную(ые) с сетевым соединением с помощью простой матрицы, представленной в таблице 2.

Таблица 2

Характеристики доверительной среды

Доверительная среда	Характеристика
Низкая	Сеть с неизвестным сообществом пользователей
Средняя	Сеть с известным сообществом пользователей и в пределах замкнутого делового круга (более одной организации)
Высокая	Сеть с неизвестным сообществом пользователей только в пределах организации

Во-вторых, текущая доверительная среда (низкая, средняя, высокая) должна относиться к применимой характеристике сети (общей или частной) и типу используемого соединения сетей (см. 10.1 - 10.6) для установления доверительных отношений. Это может быть сделано с помощью матрицы, представленной в таблице 3.

Таблица 3

Идентификация доверительных отношений

Тип соединения сети (см. раздел 10)	Доверительная среда		
	Низкая	Средняя	Высокая
Сеть общего пользования	10,6	10,4 10,5	10,2 10,3
Частная сеть	10,4 10,5	10,4 10,5	10,1 10,2 10,3

Определение категории для каждого доверительного отношения - по таблице 3. Все возможные категории представлены в таблице 4.

Таблица 4

Категории доверительных отношений

Категория доверительного отношения	Характеристика
Низкая/общая	Низкое доверие и использование общей сети

Средняя/общая	Среднее доверие и использование общей сети
Высокая/общая	Высокое доверие и использование частной сети
Низкая/частная	Низкое доверие и использование частной сети
Средняя/частная	Среднее доверие и использование частной сети
Высокая/частная	Высокое доверие и использование частной сети

Эти обращения будут использованы в разделе 12 настоящего стандарта для подтверждения видов риска безопасности и определения потенциальных контролируемых зон.

Эти задачи можно решить (при необходимости) с помощью информации, имеющейся в сетевых структурах и их применении (см. раздел 9).

12. ОПРЕДЕЛЕНИЕ ВИДОВ РИСКА БЕЗОПАСНОСТИ

Работа большинства организаций в настоящее время зависит от использования систем ИТ и сетей, поддерживающих их деловые операции. Более того, во многих случаях существует конкретное требование бизнеса по использованию сетевых соединений между системами ИТ в месте расположения каждой организации и других местах внутри и за пределами организации. При подсоединении к другой сети большое внимание следует уделять защите соединяющей организации от возникновения дополнительных рисков. Возникновение рисков возможно в результате, например, собственного соединения организации или соединений на другом конце сети.

В то время как сетевые соединения являются важными по деловым соображениям, необходимо признать, что их использование может вносить дополнительные риски безопасности, некоторые из которых, возможно, связаны с необходимостью строгого соблюдения соответствующих законов и постановлений. Виды рисков, указанные в настоящем разделе, отражают озабоченности, связанные с обеспечением безопасности. К ним относят несанкционированный доступ к информации, передачи без разрешения, внедрение злонамеренного кода, отказ подтверждения источника и подключения к услугам. Таким образом, виды риска безопасности, с которыми может встретиться организация, касаются:

- конфиденциальности информации;

- целостности информации;

- доступности информации и услуг;

- отказа от подтверждения обязательств;

- подотчетности транзакций;

- достоверности информации;

- надежности информации.

Не все виды риска безопасности применимы к любому помещению или любой организации. Однако соответствующие виды риска безопасности необходимо выявлять для определения потенциальных контролируемых зон (и, в конечном итоге, для выбора, проектирования, реализации и поддержания защитных мер).

Следует собирать и анализировать информацию по импликациям (вовлечению) в деловые операции, имеющие отношение к указанным выше видам риска безопасности (желательно по результатам анализа рисков и управления результатами проведенного анализа). При этом рассмотрению подлежат конфиденциальность или важность информации (возможное вредное влияние на бизнес) и соответствующие потенциальные угрозы и уязвимости. В случае более значимого вредного влияния на деловые операции организации следует обратиться к матрице видов риска, представленной в таблице 5.

Таблица 5

Матрица видов риска безопасности и ссылок на номера пунктов, описывающих потенциальные защитные зоны

Тип риска	Ссылка на доверительное отношение					
	Низкая/общая	Средняя/общая	Высокая/общая	Низкая/частная	Средняя/частная	Высокая/частная
Раскрытие конфиденциальности	13.2.2	13.2.2	13.2.2	13.2.2	13.2.2	13.2.2
	13.2.3	13.2.3	13.2.3	13.2.3	13.2.3	13.2.3
	13.2.6	13.2.4	13.2.5	13.2.4	13.2.4	13.2.5
	13.4	13.2.6	13.2.6	13.2.6	13.2.6	13.2.6
	13.5	13.3.2	13.3.2	13.3.2	13.3.2	13.3.2
	13.7	13.3.3	13.3.3	13.3.4	13.3.3	13.3.5
	13.8	13.3.4	13.3.4	13.4	13.3.4	13.4
	13.9	13.4	13.3.5	13.5	13.4	13.7
	13.12	13.5	13.4	13.7	13.7	13.9
		13.7	13.5	13.8	13.8	
		13.8	13.7	13.9	13.9	
		13.9	13.8	13.12	13.12	
		13.12	13.9			
			13.12			

Нарушение целостности	13.2.2 13.2.3 13.2.6 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.5 13.4 13.6 13.7 13.10
Потеря готовности (доступности)	13.2.2 13.2.3 13.2.6 13.4 13.5 13.6 13.7 13.8 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.6 13.7	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.6 13.7 13.8 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.5 13.4 13.6 13.7 13.12 13.13

		13.13	13.8 13.13	13.13		
Потеря способности подтверждать передачу/прием в сети	13.2.2 13.2.3 13.2.6 13.4 13.5 13.7 13.11 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.7 13.11 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.7 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.7 13.11 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.7 13.11 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.7 13.13
Потеря подотчетности	13.2.2 13.2.6 13.2.4 13.6 13.7 13.8 13.12	13.2.2 13.2.6 13.2.4 13.3.4 13.4 13.6 13.7 13.8 13.12	13.2.2 13.2.6 13.3.3 13.3.4 13.4 13.6 13.7 13.8 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.3 13.3.4 13.4 13.6 13.7 13.8 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.3 13.4 13.6 13.7 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.3 13.3.4 13.4 13.7
Потеря аутентичности	13.2.2	13.2.2	13.2.2	13.2.2	13.2.2	13.2.2

	13.2.6 13.2.4 13.3.3 13.5 13.6 13.8 13.10 13.12	13.2.6 13.2.4 13.3.3 13.3.4 13.4 13.5 13.6 13.8 13.10 13.12	13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.3 13.2.4 13.2.5 13.2.6 13.4 13.5 13.6 13.8 13.10 13.12	13.2.3 13.2.4 13.2.5 13.2.6 13.3.2 13.4 13.5 13.6 13.10 13.12	13.2.3 13.2.5 13.2.6 13.3.2 13.3.4 13.4 13.5 13.6 13.7 13.10
Ухудшение надежности	13.2.2 13.2.6 13.2.4 13.3.3 13.5 13.6 13.8 13.12 13.13	13.2.2 13.2.6 13.2.4 13.3.3 13.4 13.5 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.4 13.5 13.6 13.8 13.12 13.13	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.2 13.5 13.6 13.7 13.12 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.4 13.5 13.6 13.7 13.12 13.13

Необходимо обратить внимание на то, что при завершении этой задачи следует использовать результаты анализа риска безопасности и управление результатами этого анализа, проведенного в отношении соединения(й) сети. Эти результаты позволят определить уровень детализации анализа проведенного управления и сосредоточить внимание на потенциально вредном влиянии, оказываемом на бизнес в связи с перечисленными выше видами риска, а также с типами угроз, уязвимостями и, следовательно, рисками для деятельности организации.

Ссылки на доверительные отношения по разделу 11 указывают в подзаголовках к таблице 5, а причиняемые воздействия - в левой части таблицы.

В точках пересечения указывают ссылки на потенциальные контролируемые зоны, которые далее рассматриваются в разделе 13.

Следует заметить, что в таблице 5 показано, как с увеличением доверия пользователя увеличивается необходимость в защитных мерах. Для этого существуют две причины.

Первая - имеется ряд защитных мер, описание которых приведено в ИСО/МЭК 13335-4 (и поэтому здесь не повторяется). Эти меры следует выбирать для обеспечения безопасности ведущих средств ИТ, в том числе идентификации и аутентификации и логического контроля доступа. Конфигурация разрешений (привилегий) в ситуациях нижнего уровня доверия должна обеспечивать доступ только к ресурсам, которые согласуются с доверительной моделью и потребностями планируемого доступа. В ситуациях низкого доверия степень идентификации и аутентификации, логический контроль доступа и защитные меры (см. ИСО/МЭК 13335-4) должны быть выше, чем в ситуациях высокого доверия. При невозможности подобных действий должны быть внедрены дополнительные защитные меры.

Вторая - пользующиеся доверием пользователи обычно получают доступ к более важной/критической информации и/или функциональности. Это может означать потребность в дополнительной защите в качестве признания ценности ресурсов доступа, но не в качестве доверия к пользователям.

13. ОПРЕДЕЛЕНИЕ РЕАЛЬНЫХ ПОТЕНЦИАЛЬНЫХ КОНТРОЛИРУЕМЫХ ЗОН

13.1. Введение

Теперь следует на основе использования ссылок по таблице 5 идентифицировать потенциально контролируемые зоны из раздела 13. Потенциально контролируемые зоны, представленные в 13.2 - 13.13, следует выбирать, используя раздел 12. Следует заметить, что частное решение защиты может на самом деле включать в себя ряд потенциально контролируемых зон, представленных в 13.2 - 13.13.

Следует также заметить, что ряд защитных мер относится к соответствующим системам ИТ независимо от того, имеют ли ИТ какие-либо сетевые соединения. Эти защитные меры следует выбирать, используя ИСО/МЭК 13335-4. Необходимо также отметить, что в настоящем стандарте сделано предположение о том, что имеются базовые защитные меры, изложенные в ИСО/МЭК 13335-4 для систем той организации, от которой исходят сетевые соединения.

Перечень потенциально контролируемых зон необходимо тщательно проанализировать в контексте соответствующих структур сети и их применений. Затем перечень можно применять как основу для последующего выбора мер защиты безопасности, их проектирования, реализации и технического обслуживания (см. раздел 15).

13.2. Управление безопасностью услуг

13.2.1. Введение

Ключевое требование обеспечения безопасности для конкретной сети заключается в том, что осуществляются действия по управлению безопасностью услуг, устанавливающие и контролирующие операции по безопасности и реализацию безопасности. Такие действия следует проводить для обеспечения безопасности всех ИТ организации. Деятельность управления сетевыми соединениями включает в себя:

- распределение ответственности и полномочий, связанных с обеспечением безопасности сетевых соединений, и назначение представителя руководства, несущего общую ответственность за их безопасность;

- документальное оформление заявления о политике в области безопасности систем, а также всей необходимой документации по структуре <*> технического обеспечения безопасности;

<*> Следует представить и документировать проект структуры технического обеспечения безопасности (спецификацию защиты) как часть процесса технического проектирования структуры. Этот проект и технический проект архитектуры должны быть согласованы друг с другом.

- разработку документированных процедур по обеспечению безопасности;

- проверку соответствия безопасности с целью убедиться в том, что безопасность поддерживается на требуемом уровне;

- документированное получение подтвержденных условий обеспечения безопасности для планируемого соединения, прежде чем будет получено разрешение на подключение к организации или сообществу;

- документированное получение подтвержденных условий обеспечения безопасности пользователей услуг, предоставляемых сетью;

- разработку схем действий в особой ситуации;

- документированное получение подтвержденных и проверенных планов непрерывности бизнеса/восстановления после стихийного бедствия.

Следует заметить, что настоящий раздел строится на аспектах, изложенных в ИСО/МЭК 13335-4. Только важные темы, касающиеся сетевых соединений, характеризуются далее в настоящем стандарте. Темы, не затронутые далее в настоящем стандарте, - в соответствии с ИСО/МЭК 13335-4.

13.2.2. Организационные процедуры обеспечения безопасности

Для поддержки политики обеспечения безопасности систем следует разработать и соблюдать документацию по организационным процедурам обеспечения безопасности. В них следует подробно изложить повседневные действия, связанные с обеспечением безопасности, и назначить лиц, ответственных за их проведение.

13.2.3. Проверка соответствия требованиям безопасности

Проверку соответствия требованиям безопасности в отношении сетевых соединений следует проводить в соответствии с контрольным перечнем, составленным на основе защитных мер, определенных в:

- политике безопасности систем;

- процедурах, имеющих отношение к безопасности;

- структуре технического обеспечения безопасности;

- политике доступа (безопасности) к услугам через межсетевой экран;

- плане(ах) обеспечения непрерывности бизнеса;

- условиях обеспечения безопасности для соединений по требованию.

Проверку соответствия следует проводить до операционного включения любого сетевого соединения, перед основным новым выпуском (имеющим отношение к значимому бизнесу или изменению в сети) либо ежегодно.

13.2.4. Условия обеспечения безопасности для соединения

Если условия обеспечения безопасности для соединения не согласованы на месте или по контракту, то организация принимает на себя риски, связанные с внешним концом сетевого соединения.

Например, организация A может потребовать от организации B, чтобы до подключения к системам организации A через сетевое соединение организация B поддерживала и демонстрировала заданный уровень безопасности для систем, вовлеченных в это соединение. В этом случае организация A может быть уверена, что организация B справляется со своими рисками должным образом. В таких ситуациях организация A должна определить условия обеспечения безопасности в конце сетевого соединения со стороны организации B, которые должны быть установлены в документации по соединению с подробным указанием необходимых защитных мер. Организация B должна реализовать и поддерживать в рабочем состоянии установленные защитные меры, и направлять организации A отчет об эффективности защитных мер и поддержанию необходимого уровня безопасности. Таким образом, сохраняется право поручать или проводить проверку соответствия требованиям безопасности соединения в конце сетевого соединения со стороны организации B.

Возможны также случаи, когда организации согласуют документ по условиям обеспечения безопасности для соединения, в котором записывают обязательства и ответственность для всех сторон, включая взаимную проверку соответствия требованиям по безопасности.

13.2.5. Условия безопасности, подтвержденные документально, для пользователей услуг, предоставляемых сетью

Для пользователей услуг, желающих работать дистанционно, разрабатывают документ с условиями обеспечения безопасности предоставляемых сетью услуг. В документе определяют ответственность пользователя за безопасную эксплуатацию аппаратных и программных средств, а также за обеспечение защиты данных.

13.2.6. Обработка инцидентов

Нежелательные инциденты с большой вероятностью могут происходить и оказывать серьезное вредное воздействие на бизнес при наличии сетевых соединений (в противоположность ситуации, когда их нет). Более того, при сетевых соединениях с другими организациями могут быть, в частности, нарушены юридические требования, связанные с внештатными ситуациями.

Следовательно, организация с сетевыми соединениями должна предусмотреть документированные и осуществимые схемы действий при обработке инцидентов, обладать соответствующей инфраструктурой, способной быстро реагировать по мере идентификации инцидентов, уменьшать их воздействие, а также извлекать уроки из непредвиденных ситуаций в целях предотвращения их повтора.

13.3. Идентификация и аутентификация

13.3.1. Введение

Организация должна обеспечивать безопасность услуг, предоставляемых сетью, и защиту связанной с ними информации путем ограничения доступа через соединения с авторизованным персоналом (внутри или за пределами организации). Эти требования распространяются не только на использование сетевых соединений. Организация должна подробно определить использование сетевых соединений в соответствии с защитными мерами, установленными в ИСО/МЭК 13335-4.

Четыре контролируемые зоны, целесообразные для использования сетевых соединений, а также системы ИТ, имеющие непосредственное отношение к таким соединениям, представлены в 13.3.2 - 13.3.5.

13.3.2. Дистанционная регистрация при входе в систему

Дистанционная регистрация авторизованного персонала, работающего вдали от организации, специалистов дистанционного технического обслуживания или персонала других организаций осуществляется через кодовые вызовы организации, соединения Интернета, выделенные магистральные линии других организаций или коллективный доступ по Интернету. Существуют соединения, установленные внутренними системами по требованию или с помощью партнеров по контракту, с использованием сети общего пользования. Каждый тип дистанционной регистрации при входе в систему требует дополнительных защитных мер, соответствующих особенностям типа соединения. Примерами таких защитных мер являются:

- отказ разрешения на прямой доступ в систему и программное обеспечение сети на основе учетных записей, используемых для дистанционного доступа, за исключением случаев, когда предоставлена дополнительная аутентификация (см. 13.3.3);

- предохранение от несанкционированного доступа к информации, связанной с программным обеспечением электронной почты и справочной базой данных в памяти ПК и переносных компьютеров, используемых персоналом организации за пределами ее офисов.

13.3.3. Совершенствование аутентификации

Использование пар имя/пароль является простым путем установления подлинности пользователей, но пары имя/пароль могут быть дискредитированы или вскрыты. Существуют другие более безопасные пути аутентификации пользователей, особенно удаленных. Такое совершенствование аутентификации необходимо в случае, если существует высокая вероятность получения услуги лицом без соответствующих полномочий к защищаемым и важным системам. Это возможно, например, в случае, если доступ может быть инициирован по сетям общего пользования или система доступа не находится под непосредственным контролем организации (например, с переносного компьютера).

В случае если необходима усовершенствованная аутентификация по сетевым соединениям (например, по контракту) или она оправдана рисками, то организации следует рассмотреть процесс определения подлинности пользователя с помощью соответствующих защитных мер, таких как:

- использование других средств идентификации для поддержания аутентификации пользователей, таких как дистанционно проверяемые маркеры доступа, карточки с микропроцессором или магнитной полосой (используемые через считывающее устройство-приставку к ПК), ручные устройства генерации ключа одноразового прохода, модемы с набором обратного номера или биометрические средства контроля;

- обеспечение функционирования маркера доступа или карточки только с опознавательным счетом пользователя (предпочтительно с учетной записью ПК и места/точки доступа), а также любого личного идентификационного номера (PIN) или биометрического профиля;

- использование проверки линии вызывающего оператора;

- использование линий связи через модемы, разъединенные в режиме ожидания и соединяемые только после проверки идентичности вызывающего оператора.

13.3.4. Дистанционная идентификация системы

В соответствии с 13.3.3 аутентификацию следует совершенствовать путем проверки системы (и ее местоположения/точки доступа), из которой осуществляется внешний доступ.

Разные сетевые структуры могут предлагать разные виды идентификации. Следовательно, организация может совершенствовать идентификацию путем выбора подходящей структуры сети. При этом следует принимать во внимание все защитные возможности выбранной структуры сети.

13.3.5. Единичный пароль безопасности

В случае вовлечения сетевых соединений пользователи могут столкнуться с многократными проверками идентификации и аутентификации. В этом случае у пользователей может возникнуть желание осуществлять рискованные действия, такие как запись паролей или повторное применение одних и тех же данных аутентификации. Единичное предъявление пароля может уменьшить риски такого поведения путем уменьшения числа паролей, которые пользователи должны помнить. Вместе с уменьшением рисков возможно повышение производительности труда пользователя и снижение нагрузки на пульт, с которого осуществляется повторный ввод паролей.

Следует заметить, что последствия нарушений в системе единичного предъявления пароля могут быть серьезными, так как не одна, а многие системы и приложения поставлены на грань риска и открыты для дискредитации (иногда такой риск называют "ключами в королевство").

Поэтому необходимо задействовать более совершенные механизмы идентификации и аутентификации. В целях обеспечения безопасности организация может исключить из режима единичного предъявления пароля высокопривилегированные функции идентификации и аутентификации (на системном уровне).

13.4. Результаты аудита

Важно обеспечить эффективность безопасности сети через обнаружение, расследование и составление отчетов инцидентов безопасности. Следует записывать подробную информацию по результатам аудита ошибочных и адекватных событий, чтобы иметь возможность составлять тщательный анализ потенциальных и фактических инцидентов безопасности. Однако следует признать, что запись огромных объемов связанной с аудитом информации может затруднить проведение анализа и неблагоприятно повлиять на проведение аудита. Поэтому необходимо определить период времени, в течение которого следует отслеживать действия пользователей в контрольном журнале.

Большинство контрольных мер защиты, касающихся сетевых соединений и связанных с ними систем ИТ, могут быть установлены в соответствии с ИСО/МЭК 13335-4. Что касается сетевых соединений, то важно обеспечить возможность аудита следующих типов событий:

- попытки дистанционной неудачной регистрации при входе в систему с указанием даты и времени;

- события неудачной повторной аутентификации (или применения средства идентификации);

- нарушения трафика через шлюз обеспечения безопасности;

- сигналы опасности в системе управления с вовлечением защиты (например, дублирование IP-адреса, нарушения в схеме однонаправленного канала передачи данных).

Результаты аудита могут содержать конфиденциальную информацию или сведения, которыми могут воспользоваться для вторжения в систему через сетевые соединения. Более того, сведения о результатах аудита могут служить доказательством передачи данных по сети в случае появления разногласий. Поэтому результаты аудита особенно необходимы в контексте обеспечения целостности и подтверждения отправки/приема информации. Следовательно, все результаты аудита следует защищать надлежащим образом.

13.5. Обнаружение вторжения

С увеличением числа соединений в сети облегчается проникновение в нее по следующим причинам:

- увеличивается число путей проникновения в системы ИТ организации и сети;

- появляется возможность вскрытия первоначального места доступа;

- становится возможен доступ через сети и целевые внутренние системы ИТ.

Нарушители становятся более искушенными и применяют более эффективные методы атак, а средства проникновения все более доступны в Интернете или общедоступной литературе. Многие из этих средств автоматизированы, могут быть очень эффективными и простыми для применения, в том числе для лиц с небольшим опытом работы.

Для большинства организаций экономически невозможно предотвратить все потенциальные вторжения. Следовательно, некоторые вторжения возможны. Риски, связанные с большинством вторжений, могут быть снижены путем реализации надежной идентификации и аутентификации, логического контроля доступа, системы учета и аудита защитных мер в дополнение к возможности обнаружения вторжения. Такую возможность обеспечивают те средства, которые позволяют прогнозировать вторжения, выявлять их в реальном масштабе времени и давать соответствующие сигналы тревоги. Появляется также возможность локального сбора информации о вторжениях с последующим ее объединением и анализом, а также изучение схем нормального поведения/использования ИТ организации.

Во многих случаях может быть очевидной возможность некоторого несанкционированного или нежелательного события. На эту возможность может указывать небольшое ухудшение в услугах по совершенно неопределенным причинам или большое число доступов в несвойственное время, или отказ предоставления каких-либо специальных услуг. В большинстве случаев важно как можно быстрее узнать причину, масштабность и последствия вторжения.

Следует заметить, что упомянутая выше возможность вторжения является более сложной, чем инструментарий анализа результатов аудита и методы по 13.4 и соответствующему разделу ИСО/МЭК 13335-4. Более эффективные возможности обнаружения вторжения связаны с применением специального послеоперационного контроля, при котором применяются правила автоматического анализа прошлых действий, зарегистрированных в результатах аудита и в других контрольных журналах для того, чтобы прогнозировать вторжения, а также анализируются результаты ревизий известных примеров злонамеренной деятельности или деятельности, не характерной для сложившейся практики.

Более подробно эти вопросы изложены в ИСО/МЭК 15947.

13.6. Предохранение от злонамеренного кода

Пользователям необходимо знать, что злонамеренный код может быть введен в их сетевое окружение через сетевые соединения. Злонамеренный код не может быть обнаружен до нанесения ущерба, если не применять адекватные защитные меры. Злонамеренный код может подорвать защитные меры обеспечения безопасности (например, путем перехвата и раскрытия паролей), привести к непреднамеренному раскрытию или изменению информации, уничтожению данных и/или несанкционированному использованию системных ресурсов.

Некоторые формы злонамеренного кода могут быть обнаружены и удалены с помощью специального сканирующего программного обеспечения. В аппаратно-программные средства межсетевой защиты, серверы файлов, серверы почты и рабочие станции для защиты от некоторых типов злонамеренного кода могут быть включены сканеры. Для обнаружения нового злонамеренного кода важно поддерживать сканирующее программное обеспечение на должном уровне путем, по меньшей мере, еженедельного обновления. Однако пользователям и

администраторам следует понимать, что нельзя полагаться только на сканеры для обнаружения всех злонамеренных кодов (или конкретного типа), так как постоянно появляются новые типы злонамеренных кодов. Как правило, требуются другие защитные меры для улучшения безопасности, осуществляемые с помощью сканеров (при их наличии).

Пользователям и администраторам систем, использующих сетевые соединения, следует понимать, что риски, связанные со злонамеренным программным обеспечением, увеличиваются, если имеешь дело с внешними сторонами через внешние линии связи. Для пользователей и администраторов следует разработать руководства, в которых в общих чертах намечены процедуры и практические действия, направленные на уменьшение возможности ввода злонамеренного кода.

Пользователям и администраторам следует обращать особое внимание на конфигурацию конкретных системы и приложения, связанных с сетевыми соединениями для отключения функций, которые не нужны в конкретных обстоятельствах (например, приложения ПК следует конфигурировать так, чтобы макросы блокировались по умолчанию или требовалось подтверждение пользователя до их выполнения).

Подробно о злонамеренном коде см. ИСО/МЭК 13335-4.

13.7. Управление безопасностью сети

Управление любой сетью следует осуществлять с учетом обеспечения и поддержания ее безопасности, что может быть выполнено при должном рассмотрении имеющихся в наличии и относящихся к службам обеспечения безопасности сетевых протоколов.

В организации следует предусмотреть ряд защитных мер, рассмотренных в ИСО/МЭК 13335-4. Кроме того, все порты дистанционной диагностики, виртуальные или физические, следует защитить от несанкционированного доступа.

13.8. Межсетевые переходы безопасности

Правильное расположение межсетевых переходов безопасности позволит защищать внутренние системы организации, безопасно управлять и контролировать текущий трафик в соответствии с подтвержденной документами политикой безопасного межсетевого доступа к услугам.

Межсетевые переходы безопасности предназначены для:

- разделения логических сетей;

- обеспечения ограничения и анализа функций по информации, проходящей между логическими сетями;

- обслуживания организации в качестве средства управления доступом в сеть этой организации и выходом из нее;

- проведения в жизнь политики организации в области обеспечения безопасности, касающейся сетевых соединений;

- предоставления одного места для регистрации с целью входа в систему.

Для каждого межсетевого перехода безопасности следует разработать отдельный документ, определяющий политику (безопасности) доступа к услугам, и реализовать его для каждого соединения для того, чтобы гарантировать прохождение через это соединение только разрешенного трафика. Должна быть создана возможность определения допустимых соединений отдельно в соответствии с протоколом связи и другими деталями. Для обеспечения доступа через соединение только законных пользователей и действительного трафика в политике доступа к услугам следует сформулировать и подробно описать ограничения и правила применительно к трафику, проходящему в обе стороны через каждый межсетевой переход обеспечения безопасности, а также определить параметры управления трафиком и его конфигурацию.

Всем межсетевым переходам безопасности следует предоставить возможность для полного использования идентификации и аутентификации, логического контроля доступа и средств аудита. Кроме того, их следует периодически проверять на несанкционированное вторжение в программное обеспечение и/или данные, а при обнаружении таковых составлять отчеты в соответствии со схемой действий организации при обработке инцидентов.

Следует обращать внимание на то, что присоединение к сети должно осуществляться только после проверки соответствия выбранного межсетевого перехода требованиям организации. Все риски в результате такого соединения должны быть под надежным контролем. Следует гарантировать невозможность присоединения, минуя межсетевой переход безопасности.

13.9. Конфиденциальность обмена данными по сетям

Если важно сохранить конфиденциальность, следует рассмотреть криптографические способы защиты для шифрования информации, проходящей через сетевые соединения. Решение о применении криптографических мер защиты следует принимать с учетом:

- законодательства (особенно если сетевое соединение затрагивает несколько областей или органов власти);

- требований управления ключами и трудностями, которые приходится преодолевать для обеспечения заметного улучшения безопасности без создания новых значимых предпосылок уязвимости;

- адекватности используемых механизмов шифрования для задействованного типа сетевого соединения и степени необходимой безопасности.

13.10. Целостность данных, передаваемых по сетям

В случаях если важно сохранить целостность данных, организация должна рассмотреть возможность использования цифровой подписи и других мер защиты целостности сообщения для защиты информации, проходящей через сетевые соединения.

В случае если основным требованием является защита от случайного или преднамеренного изменения, добавления или удаления информации, организация должна предпринять необходимые меры по защите целостности сообщения (например, использование кодов ее аутентификации).

Применение цифровой подписи в качестве меры защиты может заменить аналогичную

защиту, которая осуществляется путем аутентификации сообщений, но дополнительно обладает свойствами, позволяющими разблокировать процедуры подтверждения отправки/приема сообщения (см. 13.11). Решение о применении цифровой подписи или мерах защиты целостности сообщения следует принимать с учетом:

- законодательных и обязательных требований (особенно в случае если сетевое соединение затрагивает сообщение между несколькими регионами или органами власти);

- соответствующих основных общественных инфраструктур;

- основных требований менеджмента и трудностей, которые приходится преодолевать для обеспечения действительного улучшения безопасности без создания новых существенных предпосылок уязвимости;

- пригодности базовых механизмов вовлеченного типа сетевого соединения и степени необходимой безопасности;

- надежной и доверительной регистрации пользователей или объектов, связанных с ключами (сертифицированными в случае необходимости), применяемых в протоколах цифровой подписи.

13.11. Подтверждение отправки/приема информации

В случае если требуется представить существенное доказательство передачи информации по сети, рассматривают следующие защитные меры:

- протоколы связи, подтверждающие передачу документа;

- протоколы приложения, требующие представления исходного адреса или идентификатора и проверки на наличие данной информации;

- межсетевые переходы, в которых проверяются форматы адресов отправителя и получателя на достоверность синтаксиса и непротиворечивость с информацией в соответствующих директориях;

- протоколы, подтверждающие доставку из сетей;

- протоколы, включающие в себя механизмы, разрешающие устанавливать последовательность информации.

В случае если важно иметь доказательство передачи или приема информации, а факт передачи или приема является предметом спора, дальнейшие гарантии следует предоставлять стандартным методом цифровой подписи. Отправителям информации (если требуется доказательство источника) следует скреплять эту информацию цифровой подписью общепринятого образца. Если требуется доказательство доставки, то отправителям следует запрашивать ответ, скрепленный цифровой подписью. Для достижения данной степени гарантии следует принять во внимание:

- использование механизмов подтверждения (цифровая подпись, отметки времени и т.д.), поддержанных доверительной третьей стороной, например, органом по сертификации, и соответствующей инфраструктурой ключей общего пользования;

- сообщения о регистрации с использованием механизмов предотвращения изменений в контрольных журналах;

- механизмы сохранения конфиденциальности и/или личных ключей (подписи) против несанкционированного использования;

- архивирование сертификаций и ключей, необходимых для разрешения споров с тем, чтобы обеспечить их доступность и целостность в течение необходимого периода времени (который может быть длиннее периода использования соответствующих ключей).

Информацию по безопасности информации от искажения ее смысла см. в ИСО/МЭК ТО 14516 и ИСО/МЭК 13888.

13.12. Виртуальные частные сети

Виртуальная частная сеть (VPN) является частной сетью, которая реализуется путем использования инфраструктуры уже существующих сетей. С точки зрения пользователей виртуальная частная сеть функционирует и предлагает частные функциональные возможности и услуги.

В виртуальной частной сети применяются криптографические методы обеспечения защиты функциональных возможностей и услуг, особенно в случае если сеть, на которой построена VPN, является сетью общего пользования (например, Интернет). В большинстве реализаций линии связи между партнерами шифруют для обеспечения конфиденциальности, а протоколы аутентификации используют для проверки идентичности систем, подсоединенных к виртуальной частной сети. Обычно шифрованная информация проходит через безопасный тоннель, подсоединяющий организации к межсетевому переходу с поддержанием конфиденциальности и целостности информации. Межсетевой переход затем идентифицирует дистанционного пользователя и позволяет ему получать доступ только к информации, санкционированной для приема.

Ко всем частным сетям важно применять меры, адекватные мерам обеспечения безопасности всех систем, подсоединенных к VPN, с тем, чтобы гарантировать возможность только санкционированных линий связи с другими сетями.

Виртуальная частная сеть может быть использована, например, для того, чтобы:

- реализовать дистанционный доступ к организации от мобильного абонента или работников, находящихся за пределами системы;

- соединить разные места работы организации, включая избыточные линии связи для реализации резервной инфраструктуры;

- установить соединения с сетью организации для других партнеров организации/бизнеса.

13.13. Непрерывность бизнеса/восстановления после стихийного бедствия

Важно, чтобы защитные меры для продолжения функции бизнеса в случае стихийного бедствия путем обеспечения способности к восстановлению каждой деловой операции были приняты в заданный интервал времени после прерывания деятельности. Руководство для

совместного планирования продолжения бизнеса и восстановления после стихийного бедствия, включая соответствующую стратегию и родственные планы с последующим тестированием, - в соответствии с ИСО/МЭК 13335-4.

Необходимо обратить внимание на требования сохранения основных и применения дополнительных сетевых соединений достаточной пропускной способности, а также на восстановление соединений после нежелательного события. В основе данных требований лежит важность соединений в обеспечении бизнеса в течение продолжительного времени, а также прогнозируемое вредное влияние на бизнес в случае их нарушений. При этом возможности соединений могут предоставить организации много преимуществ в гибкости и способности использовать практические подходы, но они могут стать точками уязвимости и "единичными точками неисправностей", которые способны оказать разрушительные воздействия на организацию.

14. ДОКУМЕНТИРОВАНИЕ И АНАЛИЗ ВАРИАНТОВ СТРУКТУР БЕЗОПАСНОСТИ

Документирование различных вариантов структур безопасности предоставляет возможность для рассмотрения различных вариантов решений и создает базу для анализа с целью выбора компромиссного решения. Это также способствует разрешению проблем, связанных с часто возникающими техническими ограничениями и противоречиями между потребностями бизнеса и обеспечением безопасности.

При составлении документации по разным вариантам структур безопасности необходимо принимать во внимание требования, установленные в политике безопасности систем ИТ организации (см. раздел 8), и перечень потенциальных контролируемых зон (см. разделы 12 и 13). Следует также учитывать существующие в организации структуры безопасности. После документирования и анализа вариантов структур безопасности выбранная схема обеспечения безопасности должна быть согласована. Организация может вносить изменения в структуру сети и ее применение (для обеспечения совместимости с предпочтительной схемой обеспечения безопасности), а также в перечень потенциальных защитных мер (например, при согласовании может быть выявлено, что структура безопасности может быть технически реализована только альтернативным способом, что потребует применения дополнительных защитных мер).

15. ПОДГОТОВКА К РАСПРЕДЕЛЕНИЮ ЗАДАЧ ПО ВЫБОРУ ЗАЩИТНЫХ МЕР, ПРОЕКТИРОВАНИЮ, РЕАЛИЗАЦИИ И ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ

Используя перечень потенциальных контролируемых зон (см. раздел 13) и согласованную структуру безопасности (см. раздел 14), организация может начинать подготовку к планированию и распределению задач для детального выбора защитных мер обеспечения безопасности, а также к их проектированию, реализации и техническому обслуживанию.

16. КРАТКОЕ ИЗЛОЖЕНИЕ

Настоящий стандарт устанавливает руководящие указания по подсоединению системы информационных технологий организации к сетям. Стандарт основан на следующем подходе: вначале проводится процесс идентификации и анализа факторов, влияющих на средства связи в целях установления требований по сетевой безопасности. Затем определяются потенциальные контролируемые зоны (организация может ссылаться на соответствующие положения других

частей ИСО/МЭК 13335). В помощь персоналу организации, отвечающему за безопасность ИТ и выявление потенциальных контролируемых зон, в настоящем стандарте приведена характеристика следующих трех основных критериев идентификации потенциальных контролируемых зон:

1) различные типы сетевых соединений;

2) различные сетевые характеристики и связанные с ними доверительные отношения;

3) потенциальные виды риска в области безопасности, связанные с сетевым соединением и использованием услуг, предоставляемых через эти соединения.

Затем критерии идентификации используются в матрицах, предназначенных для индикации потенциальных контролируемых зон. Приводится также краткое общее описание потенциальных контролируемых зон.

Приложение А
(справочное)

СВЕДЕНИЯ О СООТВЕТСТВИИ НАЦИОНАЛЬНЫХ СТАНДАРТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ ССЫЛОЧНЫМ МЕЖДУНАРОДНЫМ СТАНДАРТАМ

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта Российской Федерации
ИСО/МЭК ТО 13335-1:1996	ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационных и телекоммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационных и телекоммуникационных технологий
ИСО/МЭК ТО 13335-2:1997	<*>
ИСО/МЭК ТО 13335-3:1998	ГОСТ Р ИСО/МЭК 13335-3-2006 Информационная технология. Рекомендации по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий
ИСО/МЭК ТО 13335-4:2000	ГОСТ Р ИСО/МЭК 13335-4-2006 Информационная технология. Руководящие указания по управлению защитой информационных технологий. Часть 4. Выбор защитных мер

ИСО/МЭК 13888-1:2004	<*>
ИСО/МЭК 13888-2:1998	<*>
ИСО/МЭК 13888-3:1997	<*>
ИСО/МЭК ТО 14516:2002	<*>
ИСО/МЭК ТО 15947:2002	<*>
ИСО/МЭК ТО 7498-1:1994	ГОСТ Р ИСО/МЭК 7498-1-1999 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
ИСО/МЭК ТО 7498-2:1998	ГОСТ Р ИСО 7498-2-1999 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
ИСО/МЭК ТО 7498-3:1997	ГОСТ Р ИСО 7498-3-1997 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 3. Присвоение имен и адресация
ИСО/МЭК ТО 7498-4:1989	ГОСТ Р ИСО/МЭК 7498-4-1999 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления
<*> Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного стандарта находится в информационном фонде технических регламентов и стандартов.	

БИБЛИОГРАФИЯ

[1] IETF Site Security Handbook, of September 1997 (RFC 2196)

[2] IETF Site Security Handbook Addendum for ISPs, of 15th August 1999

[3] NIST Special Publication 800-10: Keeping Your Site Comfortably Secure: An Introduction to Firewalls