ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 5

Руководство по управлению защитой сети

СТ РК ИСО/МЭК 13335-5-2008

(ИСО/МЭК 13335-5:2001 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 5. Руководство по управлению защитой сети», IDT)

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 13335-5:2001 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 5. Руководство по управлению защитой сети» («Information technology. Security techniques. Management of information and communication security. Part 5. Management guidance on network security»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Стандарт *СТ РК ИСО/МЭК 13335* под общим названием «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий» состоит из следующих частей:

– Часть 1. Общие понятия и модели управления защитой информационных и коммуникационных технологий.

– Часть 3. Методические указания по управлению защитой ИТ.

– Часть 4. Выбор защитных мер.

– Часть 5. Руководство по управлению защитой сети.

Готовится к публикации следующая часть международного стандарта ИСО/МЭК 13335:

– Часть 2. Управление рисками при защите информационных и коммуникационных систем.

Целью стандарта *СТ РК ИСО/МЭК 13335* является предоставление руководства по аспектам управления защитой информационных технологий (ИТ). Настоящая часть стандарта не содержит каких-либо готовых решений. Тем специалистам в рамках организации, которые отвечают за обеспечение безопасности ИТ, следует адаптировать материал данной части стандарта *СТ РК ИСО/МЭК 13335* к своим специфическим потребностям.

Стандарт *СТ РК ИСО/МЭК 13335* состоит из четырех частей.

В Части 1 сделан общий обзор основных концепций и моделей, применяемых для характеристики управления защитой ИТ. Данный документ ориентирован на специалистов, ответственных за программу общей безопасности организации и/или ее систем ИТ.

В Части 3 дана характеристика методов, важная для тех, кто связан с управленческой деятельностью в течение жизненного цикла проекта, например, планирование, разработка, внедрение, проведение испытаний, приобретение или операции.

В Части 4 даны руководящие указания по выбору защитных мер, их поддержка за счет использования основных моделей и средств управления. Здесь также дано описание того, как выбранные защитные меры дополняют методы обеспечения безопасности, изложенные в Части 3, и как можно использовать дополнительные оценочные модели для выбора защитных мер.

Часть 5 дает руководство, касающееся сетей и средств связи для управленческого персонала, отвечающего за обеспечение безопасности ИТ. Это руководство поддерживает идентификацию и анализ факторов, связанных со средствами связи и передачи данных. Эти факторы следует учитывать при установлении требований к сетевой защите. В настоящей части содержится краткое введение к возможным зонам защиты.

Цель настоящего стандарта – предоставить руководство для идентификации и анализа факторов, относящихся к средствам связи. Данные факторы должны учитываться при формировании требований по обеспечению безопасности сети и указывать на потенциальные защитные зоны.

Основные задачи настоящего стандарта:

– определить и дать описание концепций, связанных с управлением защитой ИТ;

– выявить отношения между управлением защитой ИТ и менеджментом ИТ вообще;

– предоставить ряд моделей, которые могут быть использованы для разъяснения порядка защиты ИТ;

– предоставить общее руководство по управлению защитой ИТ.

Подход, используемый в настоящем стандарте, заключается в том, чтобы сначала дать характеристику общему процессу идентификации и произвести анализ относящихся к средствам связи факторов, которые следует принимать во внимание, чтобы устанавливать требования к сетевой защите, а затем предоставить индикацию потенциальных защитных зон. При этом указывается, где можно использовать соответствующее содержание других частей стандарта *СТ РК ИСО/МЭК 13335*.

В настоящем документе для специалистов, ответственных за обеспечение безопасности ИТ, предоставлено описание трех простых критериев идентификации потенциальных защитных зон. По этим критериям распознают:

1) разные типы сетевых соединений;

2) характеристики разной организации сети и соответствующие доверительные отношения;

3) потенциальные типы риска обеспечения безопасности, связанного с сетевыми соединениями (использованием сервисов, предоставляемых через эти соединения).

Результаты комбинирования этих критериев затем используются для индикации потенциальных защитных зон. Затем дано краткое вступительное описание потенциальных защитных зон с указанием источников, где они характеризуются более подробно.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ
Часть 5
Руководство по управлению защитой сети

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт предоставляет руководство по сетям и средствам связи для специалистов, ответственных за управление защитой информационных технологий (ИТ), и поддерживает выявление и анализ факторов, имеющих отношение к средствам связи. Эти факторы следует учитывать при установлении требований к обеспечению безопасности сетей.

Настоящий стандарт основан на четвертой части *СТ РК ИСО/МЭК 13335* путем представления метода идентификации подходящих защитных зон с точки зрения обеспечения безопасности, имеющей отношение к сетевым соединениям.

В рамки настоящего стандарта не входит задача дать рекомендации по детальному проектированию и аспектам реализации технических защитных зон. Такие рекомендации планируется включить в другие документы ИСО.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК 1.9-2003 Государственная система стандартизации Республики Казахстан. Порядок применения международных, региональных и национальных стандартов и нормативных документов по стандартизации, метрологии, сертификации и аккредитации.

СТ РК ГОСТ Р ИСО/МЭК 7498-1-2006 Информационная технология. Взаимодействие открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

СТ РК ГОСТ Р ИСО 7498-2-2006 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

СТ РК ИСО/МЭК 13335-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 1. Общие понятия и модели для управления защитой информационных и коммуникационных технологий.

СТ РК ИСО/МЭК 13335-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 3. Методические указания по управлению защитой информационных технологий.

СТ РК ИСО/МЭК 13335-4-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 4. Выбор защитных мер.

СТ РК ИСО/МЭК 13888-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость. Часть 2. Механизмы, использующие симметричные методы.

ИСО/МЭК 7498-3:1997* Информационные технологии. Взаимодействие открытых систем. Базовая эталонная модель: присвоение имен и адресация.

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

ИСО/МЭК 13888-1:2004* Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость. Часть 1. Общие положения.

ИСО/МЭК 13888-3:1998* Информационная технология. Методы безопасности. Неотказуемость. Часть 2. Механизмы, использующие ассиметричные методы.

3 Термины и определения

В настоящем стандарте применяются термины по *СТ РК ИСО/МЭК 13335-1-2008*.

4 Сокращения

В настоящем стандарте установлены следующие сокращения:

4.1 IP; протокол сетевого уровня из семейства протоколов TCP/IP (Internet Protocol).

4.2 ИТ; информационные технологии.

4.3 ПК; персональный компьютер.

4.4 PIN; персональный идентификационный номер (Personal Identification Number).

---

* Применяется в соответствии *СТ РК 1.9*

5 Общее представление

5.1 Предпосылка

Государственные и коммерческие организации в большой степени полагаются на использование информации при ведении своего бизнеса. Утрата конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентификации и надежности информации и сервисов может оказать вредоносное воздействие на деловые операции организации. Поэтому существует большая потребность в предохранении информации и управлении безопасностью систем ИТ в пределах организаций.

Эта большая потребность в предохранении информации особенно важна в современном окружающем мире, потому что многие системы ИТ организаций объединяются в сети. Сетевые соединения могут быть организованы в пределах одной организации, между разными организациями и иногда между организацией и сетями общего пользования. Государственные и коммерческие организации ведут дела во всем мире. Поэтому они зависят от всех видов связи: от автоматизированных систем информационного обслуживания до других 'классических' средств. Их потребности в сетях должны быть удовлетворены, при этом обеспечению безопасности сетей придается все большее значение.

В 5.2 даны рекомендованные процессы для идентификации и анализа факторов, относящихся к средствам связи. Эти факторы следует принимать во внимание, чтобы устанавливать требования к обеспечению безопасности сети и указывать на потенциальные защитные зоны. Данные процессы более подробно раскрываются в последующих разделах.

5.2 Процесс идентификации

При рассмотрении сетевых соединений всем ответственным специалистам организации следует четко представлять требования бизнеса и преимущества связи. Кроме того, они и другие пользователи соединений должны быть осведомлены о рисках обеспечения безопасности и соответствующих защитных зонах данных сетевых соединений. Требования бизнеса и выгоды оказывают влияние на многие решения и действия, принимаемые в процессе рассмотрения сетевых соединений, выявления защитных зон и последующего выбора, проектирования, внедрения и поддержания средств обеспечения безопасности. Следовательно, в течение всего процесса следует помнить о требованиях бизнеса и ожидаемой выгоде. Чтобы идентифицировать подходящие требования безопасности, имеющие отношение к сети, и защитные зоны, необходимо выполнить следующие задачи:

– сделать критический обзор общих требований к обеспечению безопасности сетевых соединений, которые изложены в политике безопасности ИТ (см. раздел 6);

– пересмотреть сетевые архитектуры и приложения, которые имеют отношение к сетевым соединениям, чтобы иметь необходимую предпосылку для выполнения последующих задач (см. раздел 7);

– идентифицировать тип или типы рассматриваемого соединения сети (см. раздел 8);

– проверить характеристики предложенного объединения в сеть (используя при необходимости имеющуюся информацию о сети и архитектуре применений) и связанные с этим доверительные отношения (см. раздел 9);

– установить родственные типы риска безопасности, где это возможно, с помощью анализа рисков и рассмотрения его результатов на уровне менеджмента, включая оценки деловых операций и информации, которую предполагается передавать через соединения, и любой другой информации, потенциально доступной законным образом через эти соединения (см. раздел 10);

– определить указатели на потенциально безопасные зоны, которые могут быть подходящими, на основе типа(ов) соединения и характеристик организации сети и связанных с этим доверительных отношений, а также типов установленных рисков безопасности (см. раздел 11);

– произвести и оформить документально критический обзор вариантов архитектуры обеспечения безопасности (см. раздел 12);

– приготовить распределение задач для выбора подробных защитных мер, проектирования, реализации и обслуживания, используя выявленные указатели на потенциально безопасные зоны и согласованную архитектуру обеспечения безопасности (см. раздел 13).

Настоящий стандарт дополняет *СТ РК ИСО/МЭК 13335-4-2008* и представляет процесс выявления подходящих защитных зон с точки зрения обеспечения безопасности, связанной с подключениями к сетям коммуникаций.

На рисунке 1 дано разъяснение общего процесса идентификации и анализа факторов, относящихся к средствам связи. Данные факторы следует принимать во внимание, чтобы устанавливать требования к обеспечению безопасности сети и указывать потенциальные защитные зоны. Каждый этап процесса подробно изложен в последующих разделах.

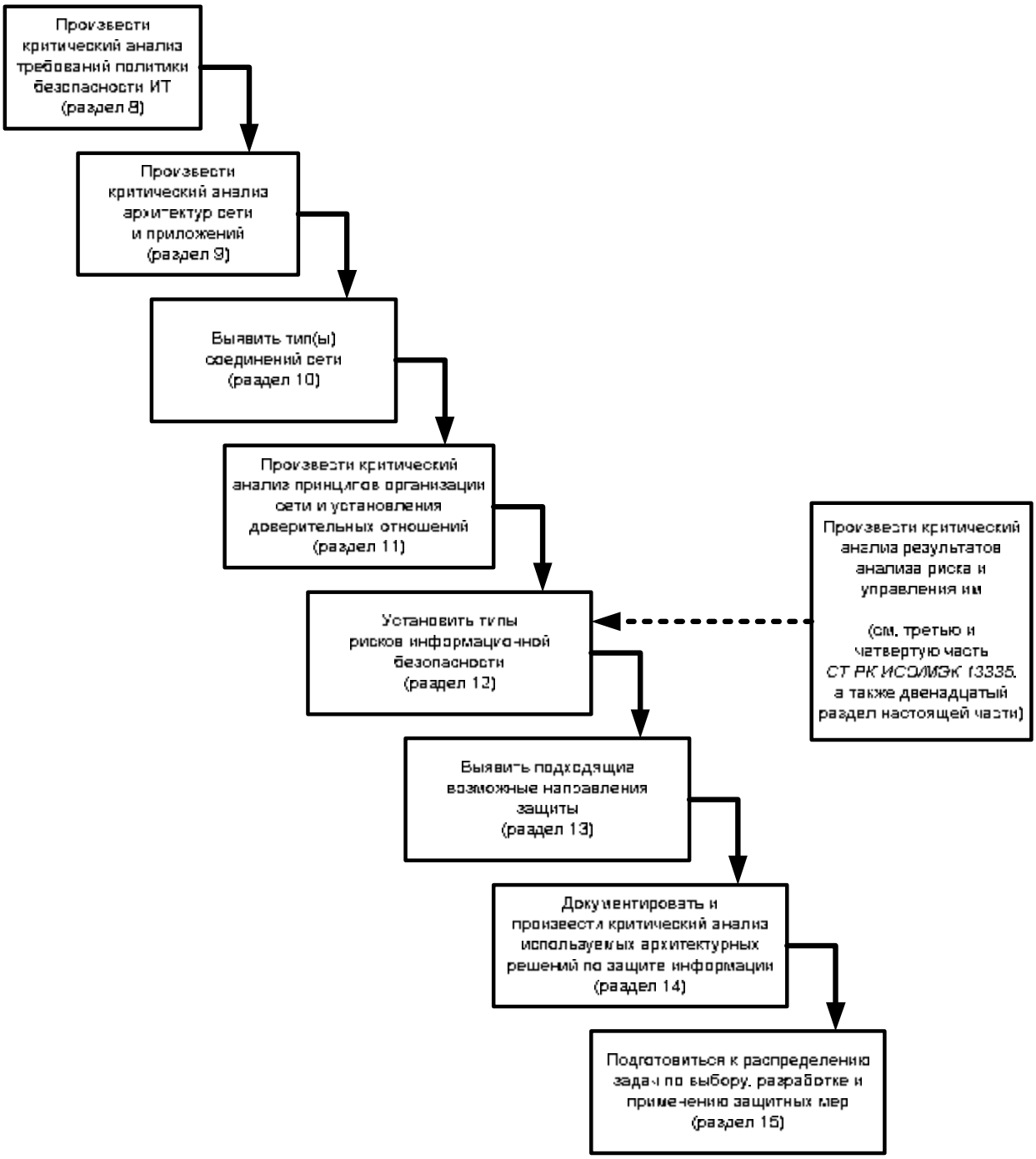

Рисунок 1. Процесс для идентификации и анализа факторов, относящихся к средствам связи и ведущих к установлению требований защиты сетей

Следует заметить, что на рисунке 1 сплошные линии представляют главный путь процесса. Пунктирная линия показывает случаи, когда типы риска обеспечения безопасности могут быть установлены на основе результатов их анализа и критического обзора со стороны менеджмента.

В дополнение к главному пути процесса на некоторых этапах может возникнуть необходимость вернуться к результатам предыдущих этапов для сохранения последовательности, в частности, к этапам "Критический анализ требований политики безопасности ИТ" и "Критический анализ архитектур сети и приложений". Например:

– после установления риска обеспечения безопасности может потребоваться критический анализ требований политики безопасности ИТ вследствие возникновения чего-то такого, что на самом деле не охвачено на уровне этой политики;

– при идентификации потенциальных защитных зон следует принимать во внимание политику безопасности ИТ, потому что в ней может быть, например, задано, что определенная защита должна быть реализована по всей организации независимо от рисков;

– чтобы обеспечить совместимость при выборе варианта архитектуры обеспечения безопасности, может потребоваться рассмотрение сетевых архитектур и приложений.

6 Обзор требований политики безопасности информационных технологий

Политика безопасности ИТ включает заявления о необходимости обеспечения конфиденциальности, целостности, неотказуемости, подотчетности, аутентификации и надежности, а также взгляды на типы угрозы и требования защиты, которые непосредственно имеют отношение к сетевым соединениям.

Например, в соответствии с такой политикой следует заявить, что:

– доступность некоторых типов информации или сервисов является предметом главной озабоченности;

– никакие соединения не разрешаются через коммутируемые линии связи;

– все соединения с сетью Интернет должны производиться через межсетевые экраны;

– должен применяться определенный тип межсетевого экрана;

– никакие платежные инструкции не являются действительными без цифровой подписи.

Такие заявления, взгляды и требования, приемлемые в масштабе организации, должны быть приняты во внимание при определении типов риска обеспечения безопасности (см. раздел 10) и идентификации потенциальных защитных зон для сетевых соединений (см. раздел 11). Если имеются какие-либо такие требования к обеспечению безопасности, то они могут быть подтверждены документами в черновом перечне потенциальных защитных зон и при необходимости отражены в вариантах архитектуры

обеспечения безопасности. Позиционирование документа по политике ИТ в пределах подхода организации к защите ИТ, его содержание и отношения с другими аналогичными документами даны в *СТ РК ИСО/МЭК 13335-3-2008*.

7 Обзор архитектур сети и приложений

7.1 Введение

Последующие шаги к подтверждению сделанного выбора потенциальных защитных зон, а именно определение:

– типа(ов) соединения сети, планируемых к использованию;

– характеристики используемых принципов организации сети и связанных с ними доверительных отношений;

– типов рисков информационной безопасности,

и составление перечня потенциальных защитных зон (а позднее соответствующих проектов защиты определенного соединения), следует всегда делать в контексте архитектуры сети и приложений, которые уже используются или планируются к использованию.

Таким образом, следует обстоятельно изучить уместную архитектуру сети и приложения, чтобы обеспечить необходимое понимание и контекст последующих этапов процесса.

Следовательно, выясняя эти аспекты, по возможности на самой ранней стадии, процесс идентификации уместных критериев для определения требований к обеспечению безопасности, выявления потенциальных защитных зон и уточнения безопасной архитектуры становится более эффективным. В конечном итоге результатом этого процесса будет наиболее выполнимое решение по обеспечению безопасности (см. 7.2 и 7.5).

Одновременно рассмотрение архитектурных аспектов сети и приложений на ранней стадии предоставляет возможность для критического обзора и возможной переработки этих архитектур, если приемлемое решение обеспечения безопасности не может быть реально выполнено в пределах имеющейся структуры.

В процессе принятия решения об архитектурах сети и приложениях необходимо рассматривать разные аспекты, в том числе:

– типы сети;

– протоколы сети;

– приложения сети.

Некоторые вопросы для критического обзора этих аспектов рассмотрены в 7.2 и 7.4, другие представлены в 7.5.

(Общее руководство по архитектурам сети и применениям можно найти в *СТ РК ГОСТ Р ИСО/МЭК 7498-1*, *СТ РК ГОСТ Р ИСО 7498-2*, ИСО/МЭК 7498-3, ИСО/МЭК 7498-4 .)

7.2 Типы сети

В зависимости от площади развертывания, сети могут быть разделены на следующие категории:

– локальные (вычислительные) сети, которые используются для местного соединения систем;

– региональные (вычислительные) сети, которые используются для соединения систем в пределах метрополии;

– глобальные сети, которые используются для соединения систем в более широких регионах вплоть до всемирного охвата.

7.3 Протоколы сети

Разные протоколы имеют различные 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;

– протоколы маршрутизации используются для определения пути через разные узлы, по которым информация распространяется в пределах локальных и региональных сетей. Информация физически доступна для всех систем, через которые проходит маршрут, который в свою очередь может быть изменен случайно или преднамеренно.

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

7.4 Сетевые приложения

Тип приложений, используемых в сети, необходимо рассматривать в контексте обеспечения безопасности. Типы могут включать:

– приложения на основе эмуляции терминала;

– приложения на основе запоминающего устройства, прямого применения или программы-планировщика;

– приложения сервера клиента.

7.5 Другие рассуждения

При критическом обзоре архитектуры или приложений следует обсудить 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, потребовать более высокую гарантию и/или дополнительные защитные меры.

8 Идентификация типов сетевого соединения

Существует много родовых типов сетевых соединений, которые могут быть использованы организацией. Часть типовых соединений может быть реализована через частные сети (доступ ограничен до известного сообщества), другие – через сети общего пользования (доступ потенциально разрешен для любой организации или человека). Далее эти типы сетевого соединения могут быть использованы для предоставления разнообразных сервисов, например, электронной почты или электронного обмена данными, и могут вовлекать использование средств сетей Интернет, интранет или экстранет, каждая из которых может потребовать разного рассмотрения безопасности. Каждый из типов соединения может иметь свои слабые места и, соответственно, свои риски безопасности и, в конечном счете, потребует разный набор защитных мер.

В таблице 1 показан один путь распределения по категориям родовых типов сетевого соединения, которое может потребоваться для бизнеса, с описанием примера, показанного для каждого типа.

При должном учете сетевых архитектур и приложений (см. раздел 7), следует выбрать один или более типов, показанных в таблице 1 и подходящих для рассматриваемых сетевых соединений.

Следует заметить, что родовые типы сетевого соединения, рассматриваемого в настоящем документе, организуются и распределяются по категориям с точки зрения перспективных потребностей бизнеса, чем с технической точки зрения. Это означает, что два разных типа сетевого соединения могут быть иногда реализованы аналогичными техническими средствами и в некоторых случаях защитные меры могут быть одинаковыми, но бывают и другие случаи, кода они могут быть разными.

Таблица 1. Типы сетевых соединений

Подраздел	Тип сетевого соединения	Характерный пример
8.1	Соединение в пределах одного управляемого местоположения организации	Взаимная связь между разными частями одной и той же организации в границах одного и того же управляемого местоположения, т.е. одиночное контролируемое здание или рабочая площадка

8.2	Соединение между географически разделенными частями одной и той же организации	Взаимная связь между региональными офисами (и/или региональных офисов с местом расположения головного офиса компании). В данном типе соединений 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 осуществлялось бы в соответствии с предоставленными привилегиями). Один доступ из другой части организации мог бы служить для целей удаленного технического обслуживания.
8.3	Соединения между узлом связи организации и персоналом, работающим в местах, удаленных от организации	Использование работниками мобильных терминалов обмены данными (например, продавцом, проверяющим наличие запаса от покупателя) или установление работниками удаленных 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.
8.4	Соединения между разными организациями в границах закрытого сообщества, например, по причине контрактных или других законных обязывающих ситуаций, или подобных интересов бизнеса, скажем банковских операций или страхования.	Взаимная связь между двумя или большим числом организаций в случае, когда имеется потребность бизнеса способствовать электронным транзакциям (например, электронного перевода платежей в банковской сфере деятельности). Этот тип соединения аналогичен п. 10.2 за исключением, что соединяемые узлы связи принадлежат двум или более организациям и соединения не обязаны обеспечивать доступ ко всему пакету приложений, используемых каждой участвующей организацией
8.5	Соединения с другими организациями	Возможно наличие доступа к удаленным базам данным, принадлежащим сторонним организациям (например, через поставщиков сервисов).

		При данном типе соединения сетей все пользователи, включая пользователей из подключаемой организации, предварительно авторизованы сторонней компанией на доступ к ее информации. Однако, несмотря на то, что все пользователи заранее наделяются полномочиями, может не существовать способа доступа к удаленному ресурсу без проведения соответствующей оплаты.
		Возможно наличие внешнего доступа к приложениям систем ИТ компании, которые хранят и/или обрабатывают информацию предоставляемую пользователям из сторонних организаций. В таком случае внешние пользователи должны быть известны и авторизованы компанией, к которой они осуществляют подключение.
		Возможно наличие доступа к ресурсам компании из сторонней организации в целях удаленного обслуживания систем ИТ. Для таких типов пользователей и сетевых подключений могут установлены расширенные привилегии доступа.
8.6	Соединение с родственным доменом общего пользования	Пользователи организации могли бы инициировать доступ к общим базам данных, средствами Веб-узлов и/или электронной почты (через сеть Интернет) в случае, когда это делается с целью извлечения информации или ее передачи между абонентами или узлами связи, которые организация специально заранее не наделила полномочиями. В данном типе соединений пользователи организации могли бы использовать упомянутые выше средства для организационных (возможно даже частных целей), однако, организация может слабо контролировать передаваемую информацию.
		Доступ может быть инициирован внешними пользователями средств организации (через сеть Интернет). В этом типе сетевого соединения доступ индивидуальным внешним пользователям организация разрешает специально и заранее.

9 Критический обзор характеристик организации сети и связанных с ними доверительных отношений

9.1 Характеристики сети

Характеристики существующих или предложенных сетей следует пересматривать. Особенно важно получить и проанализировать следующую информацию о сети:

– является ли она сетью общего пользования и доступна для любого абонента;

– это частная сеть, состоящая из собственнических 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 телефонию и передачу данных.

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

Более того, следует определить, является ли соединение постоянным или устанавливается по потребности.

9.2 Доверительные отношения

Доверительные отношения следует идентифицировать после определения характеристик существующей сети или в случае создания предложенной сети и установления ее принадлежности к частному сектору или для общего пользования (см. 9.1).

Во-первых, следует идентифицировать подходящую доверительную среду окружения, связанную с сетевым соединением(ями), используя простую матрицу, показанную в таблице 2.

Таблица 2. Характеристика доверительной среды окружения

Доверительное окружение	Характеристика
Низкое	Сеть с неизвестным сообществом пользователей
Среднее	Сеть с известным сообществом пользователей и в пределах замкнутого делового круга (более чем одной организации)

Высокое	Сеть с неизвестным сообществом пользователей только в пределах организации

Во вторых, уместное доверительное окружение (малое, среднее или высокое) следует соотнести с приемлемой характеристикой сети (общей или частной) и типом(ми) вовлеченного сетевого соединения (см. 8.1 – 8.6), чтобы установить доверительные отношения. Это может быть сделано с помощью матрицы, показанной в таблице 3.

Таблица 3. Идентификация доверительных отношений

		ДОВЕРИТЕЛЬНОЕ ОКРУЖЕНИЕ		
		НИЗКОЕ	СРЕДНЕЕ	ВЫСОКОЕ
ТИПЫ СОЕДИНЕНИЯ СЕТИ (см. раздел 8)	СЕТЬ ОБЩЕГО ПОЛЬЗОВАНИЯ	8.6	8.4 8.5	8.2 8.3
	ЧАСТНАЯ СЕТЬ	8.4 8.5	8.4 8.5	8.1 8.2 8.3

Категория обращения может быть установлена для каждого уместного доверительного отношения. Все возможные категории показаны в таблице 4.

Таблица 4. Обращение к доверительным отношениям

Категория доверительного отношения	Характеристика
НИЗКОЕ/ОБЩАЯ	Низкое доверие и использование общей сети
СРЕДНЕЕ/ОБЩАЯ	Среднее доверие и использование общей сети
ВЫСОКОЕ/ОБЩАЯ	Высокое доверие и использование частной сети
НИЗКОЕ/ЧАСТНАЯ	Низкое доверие и использование частной сети
СРЕДНЕЕ/ЧАСТНАЯ	Среднее доверие и использование частной сети
ВЫСОКОЕ/ЧАСТНАЯ	Высокое доверие и использование частной сети

Данные обращения будут использованы в разделе 10 для подтверждения типов риска безопасности, а также выявления потенциальных защитных зон.

Решению данной задачи может помочь информация, доступная по архитектурам и приложениям (см. раздел 7).

10 Определение типов риска безопасности

Как было отмечено ранее, работа большинства организаций в настоящее время зависит от использования систем ИТ и сетей, поддерживающих их деловые операции. Более того, во многих случаях имеется определенное требование бизнеса по использованию сетевых соединений между системами ИТ в месте расположения каждой организации и в других местах внутри и за пределами организации. При подсоединении к другой сети большое внимание следует уделять предохранению соединяющей организации от возникновения дополнительных рисков. Эти риски возможны в результате, например, собственного соединения организации или сетевых соединений на другом конце.

В то время как сетевые соединения являются важными по деловым соображениям, необходимо признать, что использование данных соединений может вносить дополнительные риски безопасности, ряд которых, возможно, связан с необходимостью строгого соблюдения соответствующего законодательства и нормативных документов. Типы рисков, указанные в настоящем разделе, отражают озабоченности, связанные с обеспечением безопасности. К ним относятся несанкционированный доступ к информации, неавторизованная передача информации, внедрение вредоносного кода, отказ от факта отправки/получения информации и отказы в обслуживании. Таким образом, типы риска безопасности, с которыми может встретиться организация, касаются следующего:

– конфиденциальности информации;
– целостности информации;
– доступности информации и сервисов;
– невозможности отказа от факта совершенных действий;
– подотчетности транзакций;
– достоверности информации;
– надежности информации.

Не все возможные типы риска безопасности применимы в каждом месте или для каждой организации. Однако уместные типы риска безопасности необходимо выявлять с тем, чтобы можно было определить потенциальные защитные зоны (и в конечном итоге выбрать, спроектировать, реализовать и поддерживать защитные меры).

Следует собирать информацию по импликациям (вовлечению) в деловые операции, имеющие отношение к указанным выше типам риска безопасности (желательно по результатам анализа рисков и обзору

менеджмента[1]). При этом подлежат рассмотрению секретность или значимость вовлеченной информации (выраженной в виде возможного вредоносного воздействия на бизнес) и соответствующие потенциальные угрозы и уязвимости. В случае более значимого вредоносного воздействия на деловые операции организации следует обратиться к матрице, приведенной в таблице 5.

При сборе информации по импликациям необходимо использовать результаты анализа риска безопасности и критического обзора менеджмента, проведенного в отношении соединения(ий) сети. Эти результаты позволят определить уровень детализации проведенного критического обзора и сосредоточить внимание на потенциально вредоносном влиянии, которое оказывается на бизнес в связи с перечисленными выше типами риска, а также типами угроз, уязвимости и другими заботами.

Соответствующие ссылки на доверительные отношения, установленные в разделе 9, следует показать сверху матрицы в таблице 5, а влияния, вызывающие озабоченность, с левой стороны матрицы. Ссылки на подходящих пересечениях следует отметить, так как они указывают на потенциальные защитные зоны, представленные в разделе 11.

Таблица 5. Типы риска ИБ и ссылки на подходящие меры защиты

		Ссылки на доверительное отношение					
		НИЗКОЕ/ ОБЩАЯ	СРЕДНЕЕ/ ОБЩАЯ	ВЫСОКОЕ/ ОБЩАЯ	НИЗКОЕ/ ЧАСТНАЯ	СРЕДНЕЕ/ ЧАСТНАЯ	ВЫСОКОЕ/ ЧАСТНАЯ
	Потеря способности обеспечения конфиденциальности	11.2.2 11.2.3 11.2.6 11.4 11.5 11.7 11.8 11.9 11.12	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.5 11.7 11.8 11.9 11.12	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.3 11.3.4 11.3.5 11.4 11.5 11.7 11.8 11.9 11.12	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.4 11.4 11.5 11.7 11.8 11.9 11.12	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.7 11.8 11.9 11.12	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.5 11.4 11.7 11.9

[1] Руководство по анализу риска безопасности и подходы менеджмента даются в СТ РК ИСО/МЭК 13335-3-2008 и СТ РК ИСО/МЭК 13335-4-2008.

		Ссылки на доверительное отношение					
		НИЗКОЕ/ ОБЩАЯ	СРЕДНЕЕ/ ОБЩАЯ	ВЫСОКОЕ/ ОБЩАЯ	НИЗКОЕ/ ЧАСТНАЯ	СРЕДНЕЕ/ ЧАСТНАЯ	ВЫСОКОЕ/ ЧАСТНАЯ
	Нарушение целостности	11.2.2 11.2.3 11.2.6 11.4 11.5 11.6 11.7 11.8 11.10 11.12	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.5 11.6 11.7 11.8 11.10 11.12	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.3 11.3.4 11.3.5 11.4 11.5 11.6 11.7 11.8 11.10 11.12	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.4 11.4 11.5 11.6 11.7 11.8 11.10 11.12	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.6 11.7 11.8 11.10 11.12	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.5 11.4 11.6 11.7 11.10
	Потеря доступности	11.2.2 11.2.3 11.2.6 11.4 11.5 11.6 11.7 11.8 11.13	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.5 11.6 11.7 11.8 11.13	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.3 11.3.4 11.3.5 11.4 11.5 11.6 11.7 11.8 11.13	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.4 11.4 11.5 11.6 11.7 11.8 11.12 11.13	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.4 11.4 11.6 11.7 11.8 11.12 11.13	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.5 11.4 11.6 11.7 11.12 11.13
	Потеря способности обеспечения неотказуемости	11.2.2 11.2.3 11.2.6 11.4 11.5 11.7 11.11 11.13	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.5 11.7 11.11 11.13	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.3 11.3.4 11.3.5 11.4 11.5 11.7 11.13	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.4 11.4 11.5 11.7 11.11 11.13	11.2.2 11.2.3 11.2.4 11.2.6 11.3.2 11.3.4 11.4 11.7 11.11 11.13	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.3 11.3.4 11.3.5 11.4 11.7 11.13
	Потеря подотчетности	11.2.2 11.2.6 11.2.4 11.6 11.7 11.8 11.12	11.2.2 11.2.6 11.2.4 11.3.4 11.4 11.6 11.7 11.8 11.12	11.2.2 11.2.6 11.3.3 11.3.4 11.4 11.6 11.7 11.8 11.12	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.3.3 11.3.4 11.4 11.6 11.7 11.8 11.12	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.3.3 11.4 11.6 11.7 11.12	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.3.3 11.3.4 11.4 11.7

		Ссылки на доверительное отношение					
		НИЗКОЕ/ ОБЩАЯ	СРЕДНЕЕ/ ОБЩАЯ	ВЫСОКОЕ/ ОБЩАЯ	НИЗКОЕ/ ЧАСТНАЯ	СРЕДНЕЕ/ ЧАСТНАЯ	ВЫСОКОЕ/ ЧАСТНАЯ
	Потеря способности обеспечения подлинности	11.2.2 11.2.6 11.2.4 11.3.3 11.5 11.6 11.8 11.10 11.12	11.2.2 11.2.6 11.2.4 11.3.3 11.3.4 11.4 11.5 11.6 11.8 11.10 11.12	11.2.2 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.5 11.6 11.7 11.8 11.10 11.12	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.4 11.5 11.6 11.8 11.10 11.12	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.3.2 11.4 11.5 11.6 11.10 11.12	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.4 11.4 11.5 11.6 11.7 11.10
	Ухудшение надежности	11.2.2 11.2.6 11.2.4 11.3.3 11.5 11.6 11.8 11.12 11.13	11.2.2 11.2.6 11.2.4 11.3.3 11.4 11.5 11.6 11.7 11.8 11.12 11.13	11.2.2 11.2.6 11.3.2 11.3.3 11.3.4 11.4 11.5 11.6 11.7 11.8 11.12 11.13	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.4 11.5 11.6 11.8 11.12 11.13	11.2.2 11.2.3 11.2.4 11.2.5 11.2.6 11.3.2 11.5 11.6 11.7 11.12 11.13	11.2.2 11.2.3 11.2.5 11.2.6 11.3.2 11.3.4 11.5 11.6 11.7 11.12 11.13

Следует заметить, что таблица показывает, как с увеличением доверия пользователя увеличивается необходимость в защитных мерах. Для этого существуют две причины:

Во-первых, имеется ряд защитных мер, описание которых дано в *СТ РК ИСО/МЭК 13335-4-2008*. Эти меры следует выбирать для защиты ведущих средств ИТ, в том числе для 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 (согласно описанию в *СТ РК ИСО/МЭК 13335-4-2008*) должны быть выше, чем в ситуациях высокого доверия. Если это нельзя обеспечить, тогда потребуется реализация уместных защитных мер.

Во-вторых, пользующиеся доверием пользователи обычно получают доступ к более важной/критичной информации и/или функциональности. Это может означать потребность в дополнительной защите как отражении ценности ресурсов доступа, но не доверия к пользователям.

11 Выявление подходящих потенциальных защитных зон

11.1 Введение

Теперь следует на основе использования ссылок из раздела 10 идентифицировать потенциально защитные зоны из раздела 13. Потенциально защитные зоны представлены в 11.2 – 11.13, которые следует выбирать в подходящих случаях после использования положений раздела 10. Следует заметить, что частное решение защиты может на самом деле включать ряд потенциально защитных зон, представленных в 11.2 – 11.13.

Следует заметить, что ряд защитных мер имеют отношение к уместным системам ИТ независимо от того, имеют ли ИТ какие-либо сетевые соединения. Данные защитные меры следует выбирать с использованием *СТ РК ИСО/МЭК 13335-4-2008*. Следует также заметить, что в настоящем стандарте сделано предположение о том, что базовые защитные меры, описанные в *СТ РК ИСО/МЭК 13335-4-2008,* применены для рассматриваемых систем организации, от которой исходят сетевые соединения.

Перечень потенциально защитных зон необходимо тщательно пересмотреть в контексте уместных сетевых архитектур и приложений. Затем его можно применять в качестве базиса для последующего выбора подробных мер обеспечения безопасности, проектирования, реализации и технического обслуживания (см. раздел 13).

11.2 Менеджмент безопасности сервисов

11.2.1 Введение

Ключевое требование обеспечения безопасности для какой-либо сети заключается в деятельности менеджмента по предоставлению безопасных сервисов. В результате этой деятельности инициируется и управляется реализация и операция безопасности. Такие действия следует проводить для обеспечения безопасности всех ИТ организации. Что касается сетевых соединений, то деятельность менеджмента включает следующее:

– определение всех обязанностей, связанных с обеспечением безопасности сетевых соединений и назначение управляющего, отвечающего за общую безопасность;

– политику безопасности систем(ы) ИТ, подтвержденную документами, и сопроводительную документацию по архитектуре[2] технического обеспечения безопасности;

[2] Как часть процесса технического проектирования архитектуры, следует представить и подтвердить документами проект архитектуры технического обеспечения безопасности (спецификацию защиты). Этот проект должен быть совместимый с техническим проектом архитектуры и наоборот.

– рабочие процедуры обеспечения безопасности, подтвержденные документами;

– проведение проверки соответствия безопасности с целью убедиться, что безопасность поддерживается на требуемом уровне;

– документально подтвержденные условия обеспечения безопасности для планируемого соединения прежде, чем будет получено разрешение на подключение к организации или сообществу;

– документально подтвержденные условия обеспечения безопасности пользователей сервисов, предоставляемых сетью;

– схему действий в особой ситуации;

– документально подтвержденные и проверенные планы обеспечения непрерывной работы и восстановления.

Следует заметить, что этот раздел строится на аспектах, изложенных в *СТ РК ИСО/МЭК 13335-4-2008*. Только важные темы, касающиеся сетевых соединений, характеризуются далее в этом документе. Темы, которые далее не упоминаются по тексту, следует искать в *СТ РК ИСО/МЭК 13335-4-2008*.

11.2.2 Операционные процедуры обеспечения безопасности

В поддержку политики безопасности систем(ы) ИТ следует разработать и соблюдать документы по операционным процедурам обеспечения безопасности. В них следует подробно изложить повседневные действия, связанные с обеспечением безопасности, и назначить ответственных за их проведение.

11.2.3 Проверка соответствия требованиям безопасности

Проверку соответствия требованиям безопасности в отношении сетевых соединений следует проводить по контрольному перечню, составленному на основе защитных мер, специфицированных в следующих документах:

– политика безопасности систем(ы) ИТ;

– рабочие процедуры, имеющие отношение к безопасности;

– архитектура технического обеспечения безопасности;

– политика доступа (безопасности) к сервисам через защитный межсетевой интерфейс;

– план(ы) обеспечения непрерывной работы и восстановления;

– условия 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) и в противном случае ежегодно.

11.2.4 Условия обеспечения безопасности для соединения

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

Как пример, организация А может потребовать от организации В, что до подключения к системам А через сетевое соединение организация В должна поддерживать и демонстрировать заданный уровень безопасности для систем, вовлеченных в это соединение. В этом случае организация А может быть уверена, что организация В справляется со своими рисками допустимым образом. В таких ситуациях организация А разрабатывает условия обеспечения безопасности для документа на соединение, в котором должны быть подробно указаны защитные меры, необходимые на конце В. Эти меры реализует организация В после подписания обязательного заявления по этим мерам и поддержанию безопасности. Таким образом, сохраняется право поручить или провести проверку соответствия требованиям безопасности соединения на конце В.

Возможны также случаи, когда организации взаимно согласуют документ по «условиям обеспечения безопасности для соединения», в котором следует записать обязательства и ответственности для всех сторон, включая обоюдную проверку соответствия.

11.2.5 Условия безопасности, подтвержденные документально для пользователей сервисов, предоставляемых сетью

Для пользователей, уполномоченных работать удаленно, следует издать документ с условиями обеспечения безопасности предоставляемых сетью сервисов. В нем следует определить ответственность пользователя за безопасную эксплуатацию аппаратных и программных средств, а также защиту данных.

11.2.6 Действия в непредвиденных ситуациях

Нежелательные инциденты более вероятно могут происходить и оказывать серьезное вредоносное воздействие на бизнес при наличии сетевых соединений (в противоположность ситуации, когда их нет). Более того, при сетевых соединениях с другими организациями, в частности, могут быть значимые нарушения закона, связанные с внештатными ситуациями.

Следовательно, организация с сетевыми соединениями должна предусмотреть хорошо документированные и выполнимые схемы действий в непредвиденных ситуациях, иметь на месте соответствующую инфраструктуру, способную быстро реагировать по мере идентификации инцидентов, уменьшать их воздействие, а также извлекать уроки в целях предотвращения их повтора.

11.3 Идентификация и аутентификация

11.3.1 Введение

Важно обеспечить безопасность сервисов, предоставляемых сетью и предохранение соответствующих данных путем ограничения доступа через соединения к уполномоченному персоналу (внутри или за пределами организации). Эти требования не распространяются исключительно на использование соединений сети и, следовательно, подробное использование сетевого соединения следует определять на основе защитных мер, изложенных в *СТ РК ИСО/МЭК 13335-4-2008*.

Четыре защитные зоны, которые следует считать уместными для использования сетевых соединений, и системы ИТ, имеющие непосредственное отношение к таким соединениям, представлены в 11.3.2 – 11.3.5.

11.3.2 Регистрация пользователя при удаленном входе в систему

Регистрация уполномоченного персонала, работающего за пределами организации, специалистов удаленного технического обслуживания или персонала из других организаций при удаленном подключении к сети осуществляется через кодовые вызовы организации, соединения через сеть Интернет, выделенные магистральные линии от других организаций или коллективный доступ через сеть Интернет. Имеются соединения, установленные по требованию внутренними системами или с помощью партнеров по контракту, используя сети общего пользования. Каждый тип регистрации пользователя при удаленном входе в систему требует дополнительных защитных мер, соответствующих характерному типу соединения. Примером защитных мер является следующее:

– отказ разрешения на прямой доступ в систему и к программному обеспечению сети на основе учетных записей, используемых для удаленного доступа за исключением, когда предоставлена дополнительная аутентификация (см. 11.3.3),

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

11.3.3 Совершенствование аутентификации

Использование пар имени/пароля является простым путем для установления подлинности пользователей, однако данные атрибуты могут быть дискредитированы или отгаданы. Имеются другие более безопасные пути аутентификации пользователей (в первую очередь, удаленных пользователей). Совершенствование аутентификации необходимо в случае,

когда существует высокая вероятность того, что лицо без соответствующих полномочий может получить доступ к защищаемым важным системам. Это возможно, например, в случае, когда доступ может быть инициирован по сетям общего пользования или система доступа не находится под непосредственным контролем самой организации (например, с переносного компьютера).

В случае, когда необходима усовершенствованная аутентификация по сетевым соединениям (например, согласно договору), или она оправдана рисками, то организации следует рассмотреть процесс опознания лица с помощью применения уместных защитных мер. Например:

– использование других средств идентификации, чтобы поддерживать аутентификацию пользователей. К ним относятся удаленно 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 совместно 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, которые разъединены в режиме ожидания и соединяются только после проверки идентичности вызывающего оператора.

11.3.4 Удаленная идентификация системы

Как предполагалось в 11.3.3, соответствующую аутентификацию следует совершенствовать путем проверки системы (и ее местоположения/точки доступа), из которой осуществляется внешний доступ.

Следует признать, что разные сетевые архитектуры могут предлагать разные способности идентификации. Следовательно, организация может совершенствовать идентификацию путем выбора подходящей архитектуры сети. При этом следует принимать во внимание все защитные возможности выбранной архитектуры сети.

11.3.5 Засекреченное единичное предъявление пароля

В случае, когда вовлечены сетевые соединения, пользователи могут столкнуться с многократными проверками идентификации и аутентификации. В таких обстоятельствах у пользователей может возникнуть желание пользоваться незащищенными практическими способами, например, записью паролей и повторным применением 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 может быть повышена производительность пользователя и снижена нагрузка на пульт, связанный с новой установкой паролей.

Однако следует заметить, что последствия нарушений в системе единичного предъявления пароля могут быть серьезными, так как не одна, а много систем и приложений будут поставлены на грань риска и открыты для дискредитации (иногда такой риск называют "ключами в королевство").

Поэтому необходимы более совершенные, чем нормальные механизмы идентификации и аутентификации. Желательно исключить высоко привилегированные функции идентификации и аутентификации (на системном уровне) из режима единичного предъявления пароля в целях обеспечения безопасности.

11.4 Следы аудита

Важно обеспечить эффективность безопасности сети путем обнаружения, расследования и составления отчетов о происшествиях, связанных с безопасностью. Достаточную информацию по следам аудита сбойных ситуаций и действительных событий следует фиксировать, чтобы иметь возможность тщательного критического обзора подозреваемых и действительных происшествий. Однако следует признать, что регистрация огромных объемов информации, связанной с аудитом, может затруднить проведение анализов и неблагоприятно влиять на функционирование ревизии. Поэтому необходимо определить период времени, в течение которого действительно следует отслеживать действия пользователей в контрольном журнале.

Большинство требуемых контрольных мер защиты, касающихся сетевых соединений и связанных с ними систем ИТ, могут быть установлены путем использования *СТ РК ИСО/МЭК 13335-4-2008*. Что касается сетевых соединений, то важно обеспечить возможность аудита следующих типов событий:

– неудачные попытки удаленной регистрации при входе в систему с регистрацией указанием даты и времени;

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

– нарушения трафика через шлюз обеспечения безопасности;

– удаленные попытки доступа к протоколам регистрации событий;

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

Следы аудита могут содержать секретную информацию или сведения, которыми могут воспользоваться для вторжения в систему с использованием сетевых соединений. Более того, сведения о следах аудита могут служить доказательством передачи данных по сети в случае разногласия. Поэтому они особенно необходимы в контексте обеспечения целостности и неотказуемости. Следовательно, все следы аудита следует предохранять соответствующим образом.

11.5 Обнаружение вторжения

С увеличением соединений в сети становится легче в нее проникать по следующим причинам:

– можно найти многочисленные пути проникновения в системы ИТ организации и сети;

– появляется возможность утаивания первоначального места доступа;

– возможен доступ через сети и целевые внутренние системы ИТ.

Хакеры становятся все более изощренными и применяют более продвинутые методы атак, а средства проникновения легко доступны в сети Интернет или открытой литературе. Многие из этих средств автоматизированы, могут быть очень эффективными и простыми для применения, в том числе для людей с небольшим опытом.

Для большинства организаций экономически невозможно предотвратить все потенциальные проникновения. Следовательно, некоторые проникновения вполне возможны. Риски, связанные с большинством вторжений, могут быть рассмотрены через реализацию надежной идентификации и аутентификации, логический контроль доступа, систему учета и защитные меры аудита вместе с возможностью их обнаружения. Такую возможность обеспечивают средства, позволяющие прогнозировать вторжения, выявлять их в реальном масштабе времени и поднимать соответствующую тревогу. Появляется также возможность местного сбора информации о вторжениях с последующим объединением и анализом, а также изучением схем нормального поведения/использования ИТ организации.

Во многих ситуациях может быть очевидной возможность некоторого несанкционированного или нежелательного события. На это может указывать небольшое ухудшение в предоставлении сервисов по явно неизвестным причинам или неожиданное число доступов в необычное время, или это может быть отказ предоставления каких-либо специальных сервисов. В большинстве ситуаций важно знать как можно быстрее причину, серьезность и рамки вторжения.

Следует заметить, что упомянутая выше возможность является более сложной, чем инструментарий анализа следов аудита и методы, которые подразумеваются в 11.4 и соответствующем разделе *СТ РК ИСО/МЭК*

13335-4-2008. Более эффективные возможности обнаружения вторжения связаны с применением специального послеоперационного контроля. В нем применяются правила автоматического анализа прошлых действий, зарегистрированных в следах аудита и других контрольных журналах, чтобы прогнозировать вторжения, а также анализируются результаты ревизий на предмет известного вредоносного поведения или операций, которые являются нетипичными для нормального использования.

Более подробно эти вопросы изложены в [1].

11.6 Предохранение от вредоносного кода

Пользователям необходимо знать, что вредоносный код может быть введен в их окружение через сетевые соединения. Вредоносный код не может быть обнаружен до нанесения им ущерба, если не применять подходящие защитные меры. Вредоносный код может скомпрометировать защитные меры (например, путем перехвата и раскрытия паролей), привести к непреднамеренному раскрытию или изменению информации, уничтожению данных и/или несанкционированному использованию системных ресурсов.

Некоторые формы вредоносного кода могут быть обнаружены и удалены с помощью специального сканирующего программного обеспечения (сканеров). Сканеры могут быть включены в аппаратно-программные средства межсетевой защиты, серверы файлов, серверы почты и рабочие станции против некоторых типов вредоносного кода. Чтобы иметь возможность обнаружения нового вредоносного кода, важно поддерживать сканирующее программное обеспечение на современном уровне путем, по меньшей мере, еженедельного обновления версий. Однако пользователям и администраторам следует понимать, что нельзя полагаться только на сканеры для обнаружения всех возможных вариантов вредоносного кода (или даже определенного типа), потому что постоянно появляются новые формы вредоносного кода. Соответственно, требуются другие защитные меры для усиления предохранения, осуществляемого с помощью сканеров (при наличии).

Пользователям и администраторам систем, использующих сетевые соединения, следует понимать, что риски, связанные с вредоносным программным обеспечением, увеличиваются, если имеешь дело с внешними партнерами через внешние линии связи. Для пользователей и администраторов следует разработать руководящие указания, регламентирующие в общих чертах процедуры и практические действия, направленные на уменьшение возможности поступления вредоносного кода в систему.

Пользователям и администраторам следует обращать специальное внимание на конфигурацию системы и приложения, связанные с сетевыми

соединениями, чтобы отключать функции, которые не требуются в данных обстоятельствах (например, приложения ПК следует конфигурировать таким образом, что макроопределения блокируются по умолчанию или для их возбуждения требуется подтверждение пользователя).

Детальная информация по вопросам связанным с вредоносным кодом приведена в *СТ РК ИСО/МЭК 13335-4-2008*.

11.7 Управление защитой сети

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

В организации следует рассмотреть ряд защитных мер, большинство которых можно определить путем применения *СТ РК ИСО/МЭК 13335-4-2008*. Кроме того, все порты дистанционной диагностики, виртуальные или физические, следует предохранять от несанкционированного доступа.

11.8 Межсетевые экраны

Подходящее расположение межсетевых экранов позволит защищать внутренние системы организации, справляться и контролировать текущий трафик в соответствии с подтвержденной документами политикой защиты межсетевых взаимодействий.

Межсетевые экраны предназначены для того, чтобы:

– разделять логические сети;

– обеспечивать ограничение и анализ функций по информации, которая проходит между логическими сетями;

– обслуживать организацию в качестве средства управления доступом в сеть этой организации и выходом из нее;

– предоставлять единую управляемую и контролируемую точку входа в сеть;

– проводить в жизнь политику организации в области обеспечения безопасности, касающейся сетевых соединений;

– предоставлять одно место для регистрации с целью входа в систему.

Для каждого межсетевого экрана следует разработать отдельный документ, определяющий политику (безопасность) доступа к сервисам, и реализовать его для каждого соединения, чтобы гарантировать прохождение через это соединение только разрешенного трафика. Должна быть возможность определять допустимые соединения отдельно в соответствии с протоколом связи и другими тонкостями. Чтобы обеспечить через соединение доступ только истинных пользователей и действительного трафика, в политике следует учредить и подробно записать ограничения и

правила применительно для трафика, проходящего в обе стороны через каждый межсетевой экран, а также определить параметры управления трафиком и его конфигурацию.

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

Обращается внимание на то, что соединение к сети должно иметь место только после проверки соответствия выбранного межсетевого экрана требованиям организации и что все риски в результате такого соединения могут быть под надежным контролем. Следует гарантировать, что обход межсетевого экрана является невозможным.

11.9 Конфиденциальность обмена данными по сетям

В обстоятельствах, когда важно сохранить конфиденциальность, следует рассмотреть криптографические меры защиты, чтобы шифровать информацию, проходящую через сетевые соединения. Решение о применении криптографических мер защиты следует принимать с учетом следующего:

– действующих государственных законов и правил (особенно в случае, когда сетевое соединение вовлекает несколько стран или судебные органы),

– требований управления ключами и трудностей, которые приходится преодолевать для обеспечения действительного улучшения безопасности без создания новых значимых предпосылок уязвимости,

– пригодности используемых механизмов шифрования для типа вовлеченного сетевого соединения и степени необходимой защиты.

11.10 Целостность данных, передаваемых по сетям

В обстоятельствах, когда важно сохранить целостность данных, следует рассмотреть цифровую подпись и меры защиты целостности сообщения, чтобы предохранять информацию, проходящую через сетевые соединения.

Меры защиты целостности сообщения (например, путем использования кодов ее аутентификации) являются подходящими в случаях, когда предохранение от случайного или преднамеренного изменения, добавления или удаления информации является главным требованием.

Защита с помощью цифровой подписи может обеспечивать аналогичное предохранение аутентификации сообщений, но также имеет приоритеты, которые позволяют разблокировать процедуры обеспечения неотказуемости

(см. 11.11). Решение о применении цифровой подписи или мерах защиты целостности сообщения следует принимать с учетом следующего:

– уместных государственных законов и правил (особенно в случае, когда сетевое соединение связывает несколько стран или вовлекает разные судебные органы),

– уместных инфраструктур ключей общего пользования,

– требований управления ключами и трудностей, которые приходится преодолевать для обеспечения действительного улучшения безопасности без создания новых значимых предпосылок уязвимости,

– пригодности базовых механизмов, используемых для вовлеченного типа сетевого соединения и степени необходимой защиты и

– надежной и доверенной регистрации пользователей или объектов, связанных с ключами (сертифицированными в случае необходимости), которые применяются в протоколах цифровой подписи.

11.11 Неотказуемость от совершенных действий по обмену информацией

В случае, когда требуется представить свидетельство передачи информации по сети, следует использовать следующие защитные меры:

– протоколы связи, которые дают подтверждение факта отправки документа;

– протоколы приложения, которые требуют представления исходного адреса или идентификатора и проверки на присутствие данной информации;

– межсетевые экраны, где проверяются форматы адресов отправителя и получателя на достоверность синтаксиса и согласованность с информацией в соответствующих директориях;

– протоколы, которые подтверждают факты доставки информации в рамках межсетевых взаимодействий;

– протоколы, которые включают механизмы, разрешающие устанавливать последовательность информации.

В случае, когда важно иметь доказательство передачи или приема информации, если этот факт является предметом спора, дальнейшие гарантии следует предоставлять через использование стандартного метода цифровой подписи. Отправителям информации, если требуется подтверждение источника сообщения, следует скреплять эту информацию цифровой подписью общепринятого стандарта. Если требуется доказательство факта доставки, то отправителям следует запрашивать ответ, скрепленный цифровой подписью. Для достижения этого уровня гарантии следует принять во внимание следующее:

– использование механизмов обеспечения неотказуемости (цифровая подпись, отметки времени и т.д.), поддержанные доверенной третьей

стороной, например, удостоверяющим центром, и соответствующей инфраструктурой ключей общего пользования,

– сообщения о регистрации, используя механизмы предотвращения изменений в контрольных журналах,

– введение механизмов защиты технологических секретов и/или секретных (ЭЦП) ключей от несанкционированного использования;

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

Детальная информация по обеспечению неотказуемости приведена в *СТ РК ИСО/МЭК 13888-2*, ИСО/МЭК 13888-1, ИСО/МЭК 13888-3.

11.12 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 сервисы.

В виртуальной частной сети применяются криптографические методы для обеспечения защиты функциональных возможностей и сервисов, особенно в случае, если сеть, на которой построена VPN, является сетью общего пользования (например, сеть Интернет). В большинстве реализаций линии связи между партнерами шифруются для обеспечения конфиденциальности, а протоколы аутентификации используются для проверки идентичности систем, подсоединенных к виртуальной частной сети. Обычно шифрованная информация проходит через безопасный 'тоннель', который подсоединяет к межсетевому экрану организации с поддержанием конфиденциальности и целостности информации. Межсетевой экран затем идентифицирует удаленного пользователя и позволяет пользователю получать доступ только к информации, которая санкционирована для приема.

Что касается всех частных сетей, то важно применять адекватные меры обеспечения безопасности всех систем, подсоединенных к VPN, например, для гарантии того, что с другими сетями возможны только санкционированные линии связи.

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

– реализовать удаленный доступ к ресурсам организации для мобильного абонента или работников, находящихся за пределами системы,

– соединять вместе разные места работы организации, включая избыточные линии связи для реализации резервной инфраструктуры,

– устанавливать соединения с сетью организации для других партнеров организации/бизнеса.

11.13 Обеспечение непрерывной работы и восстановления

Важно, чтобы защитные меры были приняты для продолжения функции бизнеса в случае стихийного бедствия путем обеспечения способности к восстановлению каждой деловой операции в подходящий интервал времени после прерывания. Руководство для совместного планирования обеспечения непрерывности работы и восстановления, включая соответствующую стратегию и родственные планы с последующим тестированием, можно взять из *СТ РК ИСО/МЭК 13335-4-2008*.

С точки зрения сетевых соединений необходимо обратить внимание на сохранение основных и применение дополнительных соединений достаточной пропускной способности, а также восстановление соединений после нежелательного события. В основу этих аспектов и требований следует положить важность соединений в обеспечении бизнеса в течение продолжительного времени, а также прогнозируемое вредоносное влияние на бизнес в случае нарушений. При этом возможности соединений могут предоставить организации много преимуществ в том, что касается гибкости и способности использовать созидательные подходы, но они могут также представлять уязвимые места и 'единичные точки неисправностей", которые могли бы оказывать разрушительные воздействия на организацию.

12 Документация и критический обзор вариантов архитектур безопасности

Документация возможных вариантов архитектур безопасности предоставляет средство для исследования разных решений и базис для анализа с целью выбора компромиссного решения. Это также способствует разрешению проблем, связанных с техническими ограничениями и противоречиями между потребностями бизнеса и обеспечением безопасности, которые часто возникают.

При составлении документов по разным вариантам необходимо принимать во внимание потребности политики безопасности систем(ы) ИТ (см. раздел 6), соответствующую сетевую архитектуру и приложения (см. раздел 7) и перечень потенциальных защитных зон, полученных согласно разделам 10 и 11. Следует также учесть существующие архитектуры безопасности. После документирования и критического обзора вариантов следует согласовать предпочтительную архитектуру обеспечения безопасности. Затем возможны изменения в архитектурах сети и

приложениях (для обеспечения совместимости с предпочтительной архитектурой обеспечения безопасности) и в перечне потенциальных защитных мер (например, вследствие согласования, что архитектура безопасности может быть технически реализована только особым способом, требуя альтернативу выявленной защите).

13 Приготовления для распределения задач по выбору защитных мер, проектированию, реализации и техническому обслуживанию

Используя перечень потенциальных защитных зон (раздел 11) и согласованную архитектуру безопасности (раздел 12) организация может начинать приготовления по планированию и распределению задач для детального выбора защитных мер обеспечения безопасности, проектирования, реализации и технического обслуживания.

14 Краткое изложение

СТ РК ИСО/МЭК 13335-5-2008 дает руководство организации, подсоединяющей свои системы информационных технологий к сетям. Принятый подход предусматривает сначала подвести итог всему процессу идентификации и анализа факторов, связанных с обменом данных по линиям связи, которые следует учитывать при установлении требований к обеспечению безопасности сети. Затем дано указание на потенциальные защитные зоны (со ссылками на возможное использование других частей *СТ РК ИСО/МЭК 13335*). В настоящем стандарте дана характеристика трех простых критериев в помощь людям, отвечающим за безопасность ИТ, и для выявления потенциальных защитных зон. К ним относится следующее:

– разные типы сетевых соединений;

– разные характеристики образования сети и родственные доверительные отношения;

– потенциальные типы риска безопасности, связанного с сетевым соединением и использованием сервисов, предоставляемых через эти соединения.

Затем критерии выбора отражены в матрицах, которые используются для индикации потенциальных защитных зон. В последующем предоставлено краткое вводное описание этих потенциальных защитных зон.

Приложение
(справочное)
Библиография

[1] ИСО/МЭК 15947 «Информационная технология. Методы защиты. Основные положения по обнаружения проникновения в информационные технологии».

[2] RFC 2196:1997, Справочник проблемной группы по проектированию сети Интернет по обеспечению безопасности узла сети.- Сентябрь 1997 .

Добавление к справочнику IETF по обеспечению безопасности узла сети.- 15 августа 1999. Добавление предназначено для поставщиков сервисов сети Интернет.

[3] NIST 800-10, Обеспечение защиты вычислительного центра сети (сайта). Введение в межсетевое экранирование.- Декабрь 1994.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, межсетевое взаимодействие, коммуникационные процедуры, методы защиты, управление, правила (инструкции).

Для заметок

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074