ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 4

Выбор защитных мер

СТ РК ИСО/МЭК 13335-4-2008

(ИСО/МЭК 13335-4:2000 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 4. Выбор защитных мер», 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 13335-4:2000 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 4. Выбор защитных мер» («Information technology. Security techniques. Management of information and communication security. Part 4. Selection of safeguards»), 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). Настоящий стандарт не содержит каких-либо готовых решений. Тем специалистам в рамках организации, которые отвечают за обеспечение безопасности ИТ, следует адаптировать материал данного документа применительно 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 содержит руководящие указания для организаций, системы информационных технологий которых подключаются к внешним сетям. Эти указания относятся к выбору и использованию средств защиты, обеспечивающих безопасность внешних соединений и сервисов, предоставляемых по данным соединениям, а также дополнительных средств

защиты, необходимых для систем информационных технологий в связи с указанными соединениями.

Цель настоящего стандарта – предоставление руководства по выбору защитных мер. Это руководство предусматривается для ситуаций, когда принято решения выбрать защитные меры для системы ИТ:

– согласно типу и характеристикам системы ИТ,

– согласно широким оценкам угроз и забот, касающихся обеспечения безопасности,

– в соответствии с результатами подробного анализа степени рисков.

В дополнение к этому руководству предоставлены перекрестные ссылки, показывающие, где выбор защитных мер может быть поддержан за счет применения общедоступных инструкций, содержащих описание мер защиты.

Настоящий стандарт также показывает, как может быть разработана базисная инструкция по обеспечению безопасности в масштабе всей организации (или ее отдельной части). Подробные меры защиты сети указаны в документах, на которые приведены ссылки в приложениях А -И.

Основные задачи настоящего стандарта:

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

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

– дать несколько моделей, которые могут быть использованы для объяснения защиты ИТ;

– предоставить общее руководство по управлению защитой ИТ.

Настоящий стандарт разделен на 11 разделов. Раздел 4 содержит введение к выбору защитных мер и концепции базисного обеспечения безопасности. В разделах 5–8 рассматриваются вопросы базисного обеспечения безопасности систем ИТ. Для того, чтобы выбрать подходящие защитные меры, необходимо сделать базисные оценки вне зависимости от того, будет ли затем проводиться подробный анализ степени рисков. Эти оценки изложены в разделе 5, где рассмотрены следующие вопросы:

– для какого типа системы ИТ предполагается выбор защитных мер (например, автономный ПК и подсоединенный к сети)?

– где находятся системы ИТ, какие условия окружающей среды вокруг мест расположения этих систем?

– какие меры защиты уже приняты и/или планируются?

– насколько сделанные оценки дают достаточную информацию, чтобы выбирать базисные защитные меры для системы ИТ?

В разделе 6 сделан обзор защитных мер, которые предполагается выбирать. Они разделены на организационные и физические (т.е. выборка

сделана в соответствии с потребностями и заботами обеспечения безопасности, а также с учетом ограничений) и на специальные меры защиты систем ИТ. Все защитные меры сгруппированы по категориям. Для каждой категории дано описание наиболее типичных защитных мер, включая краткое пояснение защиты, которую они предназначены обеспечивать. Специальные защитные меры в рамках этих категорий, их подробное описание можно найти в документах по базисной безопасности, на которые есть ссылки в приложениях А – И к настоящему стандарту. Для облегчения пользования этими документами перекрестные ссылки между категориями защитных мер этого стандарта и главами других документов, указанных в приложениях, даны в таблицах для каждой категории.

Если решено, что тип оценки достаточно подробно изложен в разделе 5 для выбора защитных мер, то в разделе 7 приведен список подходящих мер защиты для каждой типичной системы ИТ, описание которых дано в 5.1. Если защитные меры выбираются на основе типа системы ИТ, то отдельные базисы могут потребоваться для автономных рабочих станций, сетевых АРМ (автоматизированное рабочее место) или серверов. Для обеспечения требуемого уровня безопасности необходимо выбрать защитные меры, пригодные в специфических обстоятельствах, сравнить их с уже существующими (или планируемыми) мерами обеспечения безопасности и внедрить все новое, что можно использовать для достижения заданного уровня защиты.

Если решено, что существует необходимость более глубокой оценки для выбора эффективных и подходящих защитных мер, то раздел 8 оказывает поддержку для такого выбора с учетом рассмотрения вопросов безопасности на высоком уровне (в соответствии с важностью информации) и возможных угроз. Однако в данном разделе меры защиты предложены согласно явному беспокойству в части обеспечения безопасности, принимая во внимание соответствующие угрозы и окончательное рассмотрение типа системы ИТ. На Рис. 1 показан общий вид путей выбора защитных мер, описание которых дано в разделах 5, 7 и 8.

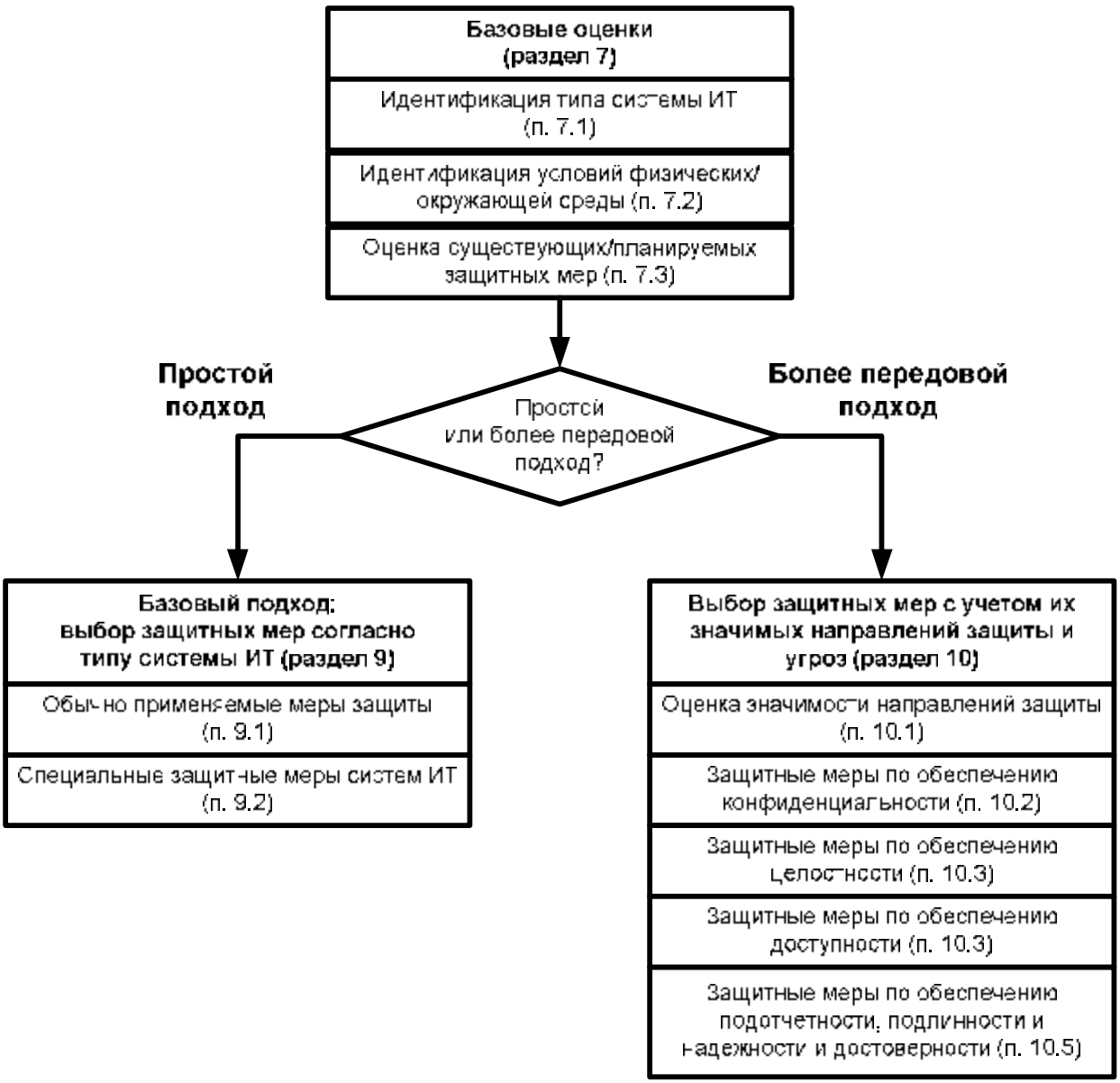

Рисунок 1. Выбор защитных мер согласно типу системы ИТ,
либо согласно значимым направлениям защиты и угрозам

В разделах 7 и 8 дано описание пути выбора защитных мер из документов по базисной безопасности, которые могут быть применены или для системы ИТ, или формирования пакета мер защиты, подходящих для ряда систем ИТ в определенных обстоятельствах. Путем сосредоточения внимания на типе рассматриваемой системы ИТ, подход, предложенный в разделе 7, допускает возможность того, что некоторые риски анализируются неадекватно и выбираются некоторые защитные меры, которые не являются необходимыми или соответствующими. Подход, предложенный в разделе 8, обращает внимание на заботы, связанные с обеспечением безопасности, и соответствующие угрозы, и позволяет разрабатывать оптимальный пакет

защитных мер. Разделы 7 и 8 могут быть использованы для поддержки выбора защитных мер без детальных оценок всех вариантов, которые попадают в область применения базисной защиты. Однако и при более подробной оценке, т.е. при анализе степени рисков, разделы 7 и 8 все еще будут полезными при выборе защитных мер.

В разделе 9 рассматривается ситуация, когда решено, что необходимо сделать подробный анализ рисков в связи с высоким уровнем обеспечения безопасности и потребностями. Руководство по анализу рисков дано в стандарте *СТ РК ИСО/МЭК 13335-3-2008*. В разделе 9 дано описание взаимосвязи между частями 3 и 4 *СТ РК ИСО/МЭК 13335*, а также того, как результаты методов в *СТ РК ИСО/МЭК 13335-3-2008* могут быть применены для поддержки выбора защитных мер. В нем также дается характеристика других факторов, способных влиять на выбор защиты, например, ограничения, подлежащие принятию во внимание, законные или другие требования, которые должны быть выполнены и т.д. Подход, рассмотренный в разделе 9, отличается от подходов в разделах 7 и 8 в том, что он дает руководство для выбора пакета защитных мер, которые оптимизированы для конкретной ситуации. Этот подход не является базисным, но, тем не менее, может быть использован для выбора мер защиты в дополнение к базисной безопасности в некоторых обстоятельствах. Альтернативно этот подход может быть применен без какой-либо связи с базисной защитой.

В разделе 10 рассматриваются вопросы составления инструкции (или каталога) по базисной безопасности для всей организации или ее отдельных частей. При разработке инструкции (или каталога) по базисной безопасности рассматриваются защитные меры, ранее выявленные для систем ИТ или групп систем ИТ, и определяется общий пакет защитных мер. В зависимости от степени секретности, озабоченности и ограничений могут быть выбраны разные уровни базисной безопасности. Рассматриваются преимущества и недостатки, чтобы облегчить принятие подходящего решения для каждой организации.

Краткое резюме настоящего стандарта дано в разделе 11 и библиографии, а в приложениях А-И сделан обзор защитных инструкций, на которые есть ссылки в разделе 6.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ
Часть 4
Выбор защитных мер

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт представляет руководство по выбору защитных мер с учетом потребностей бизнеса и забот, связанных с обеспечением безопасности. В нем дано описание процесса выбора защитных мер в соответствии с рисками и беспокойствами по обеспечению безопасности, а также специфической средой окружения, в которой работает организация. В стандарте показано, как достигать соответствующей защиты и как ее можно поддерживать путем применения базисной безопасности. Здесь также дано разъяснение, как подход, намеченный в настоящем стандарте, поддерживает методы управления защитой информационных технологий, которые сформулированы в *СТ РК ИСО/МЭК 13335-3-2008*.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

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 ИТ.

СТ РК ИСО/МЭК 13335-5-2008 Информационная технология. Управление защитой информационных и коммуникационных технологий. Часть 5. Руководство по управлению защитой сети.

СТ РК ИСО/МЭК 10181-2-2008 Информационная технология. Взаимодействие открытых систем. Основы безопасности открытых систем. Часть 2. Основы аутентификации.

СТ РК ИСО/МЭК 11770-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 1. Основные положения

3 Термины и определения

В настоящем стандарте применяются термины по *СТ РК ИСО/МЭК 13335-1-2008* , а также термин с соответствующим определением:

Идентификация (identification)**:** Процесс установления однозначной идентичности сущности.

4 Введение к выбору защитных мер и концепция базисной безопасности

В настоящем разделе дается краткий обзор темы выбора защитных мер и как и когда может быть применена в этом процессе концепция базисной безопасности. Имеются два главных подхода к выбору защитных мер, т.е. использование базисного подхода и выполнение подробного анализа степени рисков. Существуют несколько путей проведения анализа рисков, один из которых подробно изложен в *СТ РК ИСО/МЭК 13335-3-2008* и называется подробным анализом рисков. В части 3 также рассматриваются преимущества и недостатки разных подходов к оценке рисков и, следовательно, к выбору защитных мер.

Проведение подробного анализа рисков дает то преимущество, что этим достигается всесторонний обзор рисков. Результат может быть применен для выбора защитных мер, которые обоснованы этими рисками и должны быть реализованы. Таким образом, можно избежать крайностей в обеспечении защиты. Так как для анализа рисков требуется много времени, усилий и экспертиз, то он больше подходит для систем ИТ с высоким уровнем степени риска, тогда как более простой подход может считаться достаточным для систем с низкой степенью риска. Использование анализа рисков высокого уровня позволяет выявлять системы с более низкой степенью риска. Этот анализ рисков высокого уровня не обязательно должен быть формализованным или сложным процессом. Защитные меры для систем меньшего риска могут быть выбраны путем применения базисной безопасности. Этот уровень обеспечения безопасности может быть, по меньшей мере, минимальным, как определено организацией для каждого типа системы ИТ. Уровень базисного обеспечения безопасности достигается путем реализации минимального пакета защитных мер, известных как базисные меры защиты.

Вследствие различий процессов выбора защитных мер в данном документе рассматриваются два разных пути применения базисного подхода:

– применение базисного подхода в случае, когда рекомендуются защитные меры в соответствии с типом и характеристиками рассматриваемой системы ИТ;

– применение базисного подхода в случае, когда рекомендуются защитные меры в соответствии с беспокойством по обеспечению безопасности и угрозами, а также принимая во внимание рассматриваемую систему ИТ.

Чтобы иметь общий обзор представленных разных параллельных путей выбора защитных мер, здесь также дана развернутая картина (рисунок 2), показывающая отношение между *СТ РК ИСО/МЭК 13335-3-2008* и настоящим стандартом.

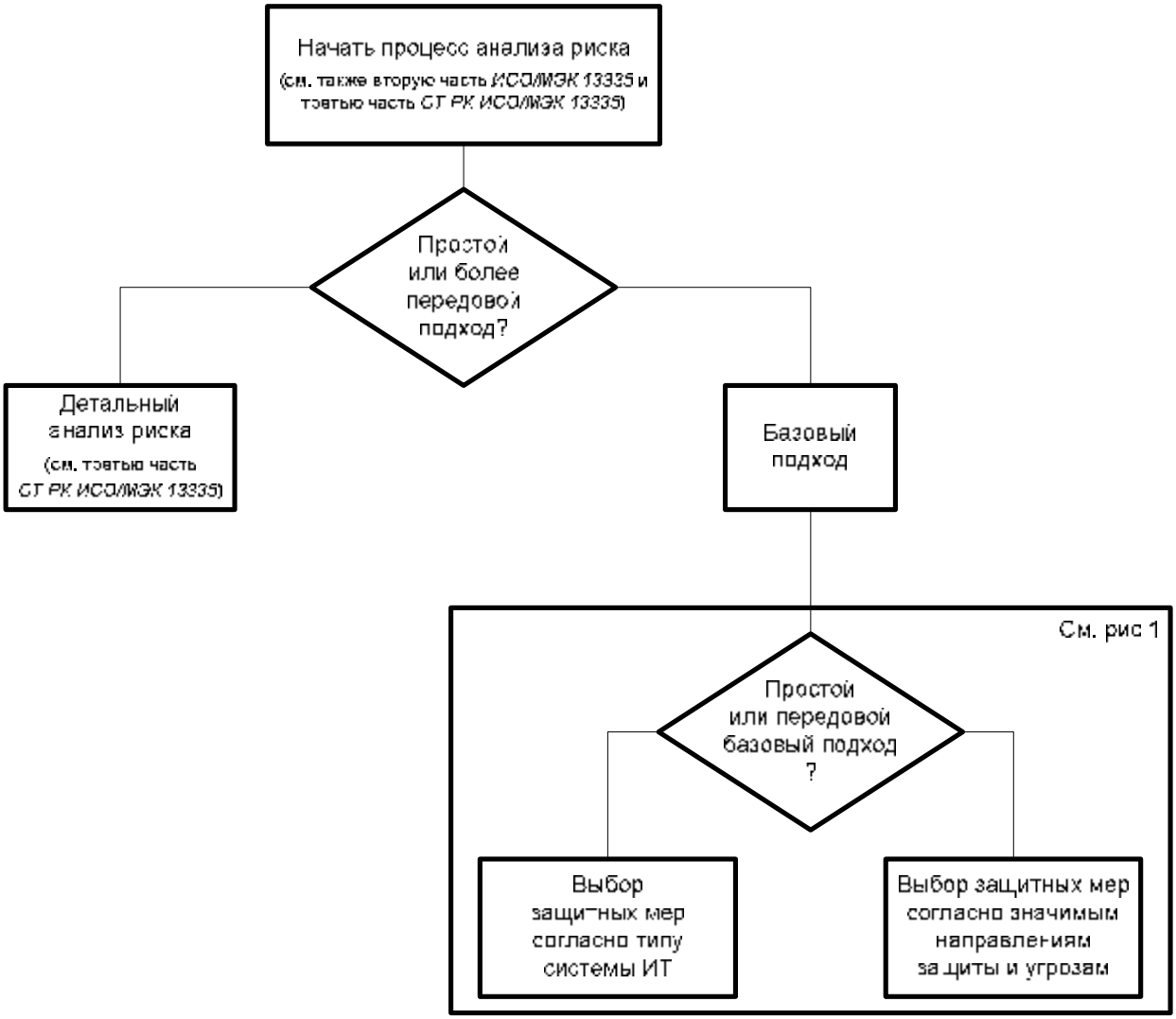

Рисунок 2. Пути выбора защитных мер

Планируемый базисный подход следует выбирать в зависимости от ресурсов, которые могут быть израсходованы на процесс выборки, осознанного беспокойства за обеспечение безопасности, типа и характеристик рассматриваемой системы ИТ. Если организация не желает тратить много времени и усилий на выбор защитных мер (по какой-либо

причине), то подходящим может быть базисный подход, предлагающий защиту без дальнейших оценок. Однако, если операции, связанные с деятельностью организации, зависят от системы ИТ и/или сервиса и обрабатываемая информация является конфиденциальной, то скорее всего потребуются дополнительные защитные меры. В этом случае настоятельно рекомендуется сделать, по меньшей мере, обзор важности информации на высоком уровне безопасности и рассмотреть вероятные угрозы, чтобы лучше обратить внимание на защитные меры, необходимые для обеспечения более эффективной безопасности системы ИТ. Если деловые операции организации в большой степени зависят от системы ИТ и сервиса и/или обрабатываемая информация является строго конфиденциальной, то степень риска может быть высокой, поэтому подробный анализ рисков является наилучшим способом идентификации подходящей защиты.

Специальные защитные меры следует выявлять на основе подробного анализа рисков в случае, когда:

– тип рассматриваемой системы не представлен соответственно типами, рассмотренными в настоящем стандарте;

– есть ощущение, что бизнес или потребности по обеспечению безопасности несоизмеримы с решениями, предложенными в этих разделах;

– более подробная оценка предписана вследствие потенциальных рисков высокой степени или значимости системы ИТ для бизнеса.

Следует заметить, что даже при детальном анализе рисков все еще полезно применять базисные меры защиты к системе ИТ.

Первое решение организации касается вопроса использования собственного базисного подхода или он должен быть частью более всесторонней стратегии анализа рисков (см. *СТ РК ИСО/МЭК 13335-3-2008*). Принимая такое решение, следует заметить, что при использовании собственного базисного подхода конечный процесс выбора защитных мер может дать в результате менее оптимизированную безопасность, чем в случае принятия более широкой стратегии анализа риска. Однако меньшие расходы и меньшая потребность в ресурсах для выбора мер обеспечения безопасности и достижение, по меньшей мере, минимального уровня безопасности для всех систем ИТ могли бы оправдать решение следовать собственному базисному подходу.

Основная защита системы ИТ может быть достигнута через идентификацию и применение пакета уместных защитных мер, которые являются подходящими в разнообразии обстоятельств с низким риском, т.е. они удовлетворяют, по меньшей мере, потребности обеспечения безопасности. Например, подходящие меры обеспечения безопасности могут быть выявлены по каталогам, которые предлагают пакеты защитных мер для типов систем ИТ, чтобы обеспечить их защиту от большинства общих угроз. Эти каталоги защитных мер содержат информацию о категориях защиты или

подробное описание предохранительных устройств или то и другое вместе, но в них обычно нет указаний, какие защитные меры следует применять в конкретных обстоятельствах. Существует возможность, что если системы ИТ организации (или ее подразделения) похожи по своей сущности и предоставляемым сервисам, то защитные меры, выбранные через базисный подход, можно было бы применить ко всем системам ИТ. На рисунке 3 показаны разные пути применения базисного подхода, рассмотренного в настоящем стандарте.

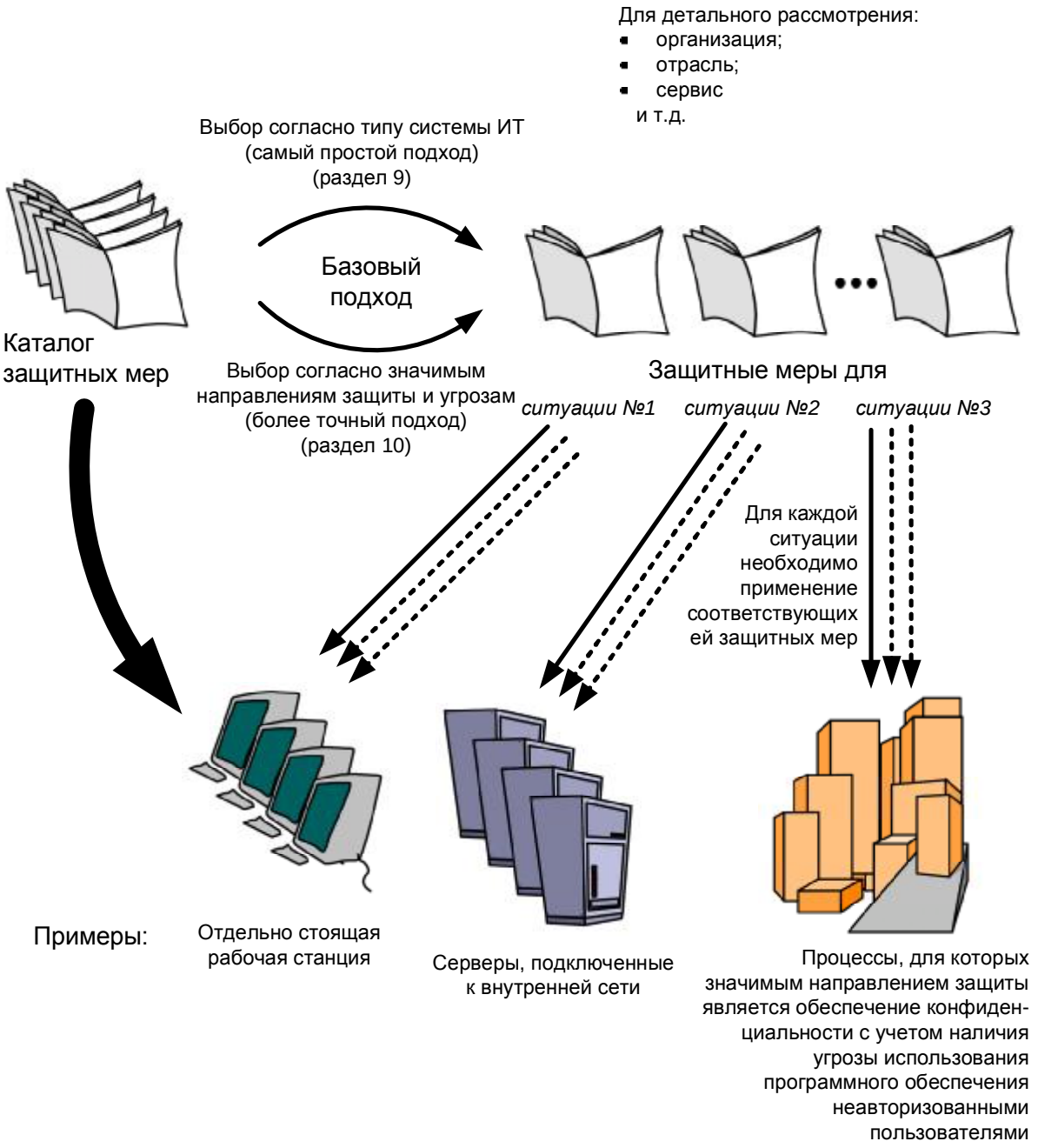

Рисунок 3. Подходы к выбору защитных мер

В случае, когда организация приняла решение по применению базисной защиты ко всей организации или ее части, необходимо выделить части организации, для которых допустим единый базис защиты, и определить, на какой уровень защиты должен быть нацелен данный базис. В большинстве случаев при использовании базисной защиты, выбор заниженного уровня защиты не допускается, пока не будут применены дополнительные защитные меры там, где это оправдано и необходимо для управления рисками средней и высокой степени. В качестве альтернативы возможно приведение базис к среднему уровню защиты, т.е. можно было бы разрешить исключения ниже и выше базиса, если бы они были обоснованы, например, по результатам анализа риска.

Одна из выгод базисной защиты заключается в том, что в случае ее применения к группе систем ИТ можно рассчитывать на определенный уровень защиты в пределах всей этой группы. В этих обстоятельствах очень выгодно разрабатывать и подтверждать документами базисный каталог защитных мер для всей организации или ее подразделения.

5 Базисные оценки

Процесс выбора защитных мер всегда требует некоторого знания типа и характеристики рассматриваемой системы ИТ (например, автономная рабочая станция или автоматизированное рабочее место, подсоединенное к сети), так как эти знания оказывают значимое влияние на выбранные защитные меры, предназначенные предохранять эту систему. Также полезно иметь представление об инфраструктуре в переводе на здания, комнаты и т.д. Другим важным фактором, связанным с выбором защитных мер, является оценка существующей и/или планируемой защиты во избежание ненужной работы, траты времени и денег. Однако настоятельно рекомендуется всегда использовать оценки, характеризуемые в разделе 5, в качестве базиса для выбора защитных мер. При выборе защитных мер следует учитывать требования бизнеса и подход организации к обеспечению безопасности. В заключение должно быть установлено, есть ли необходимость в более подробной оценке (в соответствии с описанием в разделе 8) или подробном анализе рисков (как рассмотрено в разделе 9).

5.1 Идентификация типа системы ИТ

Чтобы оценить существующую или планируемую систему ИТ, рассматриваемую систему ИТ следует сравнить с перечисленными ниже компонентами, при этом следует идентифицировать компоненты, представляющие систему. В разделе 7 предложены защитные меры для каждого из перечисленных компонентов. К ним относятся:

– автономная рабочая станция;

– рабочая станция (клиент без ресурсов коллективного пользования), подсоединенная к сети;

– сервер или рабочая станция с ресурсами коллективного пользования, подсоединенными к сети.

5.2 Идентификация физических условий и окружающей среды

Оценка окружающей среды включает выявление физической инфраструктуры, поддерживающей существующую или планируемую систему ИТ, а также существующие и/или планируемые защитные меры, имеющие отношение к системе ИТ. Так как все защитные меры следует совмещать с физическим окружением, то эти оценки являются важными для успешного выбора. При рассмотрении инфраструктуры определенную помощь могут оказать ответы на следующие вопросы. Следует также обдумать среду окружения организации и любые специальные обстоятельства, которые необходимо принимать во внимание.

– Периметр и здание

– Где расположено здание? В границах своего местоположения с забором по периметру или на улице с интенсивным движением транспорта и т.д.

– Здание арендует одна или много организаций?

– В случае аренды многими организациями, кто они?

– Где находятся уязвимые/критичные зоны?

– Контроль доступа

– Кто имеет доступ в здание?

– Установлена ли в здании система контроля физического доступа?

– Насколько монолитна конструкция здания?

– Насколько прочны двери, окна и т.д., и какая защита им предоставлена?

– Есть ли охрана здания, круглосуточная или только в рабочие часы?

– Оснащено ли здание и/или комната с важным оборудованием ИТ охранной сигнализацией от проникновения внутрь?

– Местная защита

– Как защищена(ы) комната(ы), где размещается система ИТ?

– Какие установлены средства охранной сигнализации и рассеяния и где?

– Какие установлены средства обнаружения воды/утечки жидкости?

– Работают ли коммунальные службы типа бесперебойного электроснабжения, водопровода и кондиционирования (для управления температурой и влажностью)?

Ответив на эти вопросы, можно легко идентифицировать существующие физические и другие защитные меры. Важно понимать, что не следует считать тратой времени процесс рассмотрения местоположения здания, чтобы выявить одновременно проблемы, касающиеся дверей, замков и средств контроля физического доступа, и установленный порядок действий.

5.3 Оценка существующих/планируемых защитных мер

После оценки физических условий окружающей среды и компонентов системы ИТ следует идентифицировать все другие защитные меры, уже принятые на месте или планируемые для реализации. Это необходимо сделать для того, чтобы избежать повторного выбора уже существующих или планируемых защитных мер. Кроме того, знание защитных мер, внедренных или запланированных, помогает выбирать другие защитные меры, действующие в комбинации с уже имеющейся или планируемой защитой. При выборе защитных мер следует принимать во внимание их совместимость с уже существующей защитой. Одна защита может конфликтовать с другой или мешать ее успешной работе и действующей охране.

Для идентификации существующих или планируемых защитных мер могут помочь следующие действия:

– просмотр документов, содержащих информацию о защитных мерах (например, планы защиты информационных технологий компании, концепции обеспечения безопасности ИТ). Если процесс обеспечения безопасности документально подтверждается, то в документах следует перечислить все существующие или планируемые защитные меры и статус их реализации;

– проверка вместе с ответственными сотрудниками (например, офицером по безопасности системы ИТ, управдомом или руководителем операций) и пользователями в отношении того, какие защитные меры действительно реализуются для рассматриваемой системы ИТ;

– осмотр здания с целью обозрения защитных мер, их сравнения с перечнем мер, подлежащих реализации, проверка их правильной работы и эффективности.

Может быть установлено, что существующие защитные меры превышают текущие потребности. В этом случае следует рассмотреть вопрос об исключении лишних мер. При этом следует принять во внимание факторы обеспечения безопасности и стоимости. Так как защитные меры влияют друг на друга, то исключение избыточной защиты может снизить местный общий уровень безопасности. Кроме того, возможно дешевле оставить защиту на месте, чем снимать. Наоборот, когда поддержание и

обслуживание лишней защиты связано с высокими расходами, будет дешевле снять избыточную защиту.

6 Защитные меры

Следующий раздел дает общий обзор возможных защитных мер, подлежащих реализации для повышения уровня безопасности. Некоторые из этих защитных мер связаны с работой механизмов, другие можно считать порядком действий, которые должны соблюдаться на месте. Организационные и физические защитные меры, которые могли бы подходить для систем ИТ, сведены вместе в 6.1. Специальные защитные меры для системы ИТ рассматриваются в 6.2. Следует заметить, что защитные меры характеризуются независимо от способа их выбора, т.е. некоторые защитные меры могут выбираться каким-либо способом, другие могут быть только идентифицированы путем выполнения подробного анализа рисков.

Чтобы упростить характеристику различных типов защиты, введены категории защитных мер. Последующие параграфы содержат краткое описание этих категорий и указание, какие типы защиты ИТ имеют к ним отношение. Также в приложениях А - И (см. библиографию) перечислены ссылки на инструкции и наставления с указанием, где можно найти более подробную информацию о защитных мерах, упомянутых в этом стандарте.

6.1 Организационные и физические меры защиты

Таблицы в конце этого раздела показывают источники дополнительной информации об упомянутых категориях защитных мер.

6.1.1 Управление защитой ИТ и политика

Эта категория защиты содержит все меры, имеющие отношение к управлению безопасностью ИТ, планированию, что следует делать, распределению обязанностей по этим процессам и все другие уместные действия. Эти защитные меры уже представлены в *СТ РК ИСО/МЭК 13335-1-2008 и СТ РК ИСО/МЭК 13335-3-2008*. Целью этих мер является достижение подходящего и согласующегося уровня безопасности в масштабе всей организации. Ниже перечислены защитные меры в этой области.

1 Политика безопасности ИТ

Следует разработать письменный документ, содержащий правила, директивы и установленный порядок действий с описанием, как управлять, охранять и распределять ресурсы в пределах организации. В нем следует указать на необходимость документов и предоставить инструкции по их содержанию, определяющему политику обеспечения безопасности систем ИТ.

2 Политика безопасности системы ИТ

Для каждой системы ИТ следует разработать политику безопасности, в которой должно быть описание защитных мер, подлежащих реализации на месте.

3 Управление безопасностью ИТ

Управление безопасностью ИТ следует сформулировать и скоординировать внутри организации в зависимости от ее размера, например, путем учреждения комитета по безопасности ИТ и назначения лица (часто офицера по безопасности ИТ), ответственного за безопасность каждой системы ИТ.

4 Распределение обязанностей

Обязанности по обеспечению безопасности ИТ в масштабе всей организации следует ясно подтвердить документами и распределить в соответствии с политикой безопасности в рамках компании и для систем ИТ.

5 Организация безопасности информационных технологий

Все процессы бизнеса, которые могут поддерживать безопасность ИТ (например, закупка, сотрудничество с другими организациями), следует организовать для оказания поддержки в области обеспечения безопасности.

6 Идентификация и оценивание имущества

Все имущество в пределах организации и для каждой системы ИТ следует идентифицировать и определить его ценность для осуществления бизнеса.

7 Утверждение систем ИТ

Системы ИТ следует утверждать в соответствии с политикой безопасности ИТ. Процесс утверждения следует нацелить на выяснения того, что внедренные защитные меры гарантируют подходящий уровень защиты. Следует учитывать, что система ИТ может включать сети и основные линии связи.

6.1.2 Проверка безопасности на соответствие

Важно поддерживать соответствие со всеми необходимыми мерами защиты и соответствующими законами, правилами и политиками, так как любая защита, правило или политика могут работать только в случае, если их соблюдают пользователи и им соответствуют сами системы. Защитные меры в этой области перечислены ниже.

1 Соответствие с политикой безопасности ИТ и защитными мерами

Периодические проверки следует проводить для выяснения, что все защитные меры, принятые на месте и перечисленные в политике безопасности ИТ и соответствующих политик безопасности систем(ы) ИТ, а также другие документы, например, методы безопасной работы и чрезвычайные планы, реализуются и используются правильно и эффективно

(включая конечного пользователя). В случае необходимости меры защиты должны проходить испытания.

2 Соответствие с законодательством и нормативными документами

Проверки на соответствие, упомянутое выше, следует осуществлять для гарантии, что соблюдаются все законы и нормативные документы, относящиеся к стране или странам, в которых находится система ИТ. В случае, когда такое законодательство существует, то оно должно включать законы по охране данных и секретности, копированию программного обеспечения, защите документов организаций, неправильному использованию систем ИТ или криптографии.

6.1.3 Действия в случае особой ситуации

Каждый сотрудник организации должен осознавать необходимость оперативного оповещения ответственных специалистов об инцидентах информационной безопасности, включая нарушения в функционировании программного обеспечения и выявленные слабости в защите. Для этого в организации должна быть разработана соответствующая схема оповещения ответственных специалистов. Действия в случае особой ситуации включают следующее:

1 Сообщение о возникновении особой ситуации

Доклад в случае особой ситуации является осознанной обязанностью каждого сотрудника. Непредвиденные отказы и сбои могут быть также выявлены и доложены с помощью инструментальных средств. Для того, чтобы повысить эффективность действий в особых ситуациях, следует иметь схему передачи сообщений и пункты выхода на связь в пределах организации.

2 Сообщение о слабых местах в защите

Если пользователи замечают какие-либо недостатки, относящиеся к обеспечению безопасности, то они обязаны как можно быстрее доложить об этом ответственному лицу.

3 Сообщение о нарушениях в работе программного обеспечения

Если пользователи замечают какие-либо нарушения в работе программного обеспечения, связанного с безопасностью, то они обязаны как можно быстрее доложить об этом ответственному лицу.

4 Управление в случае особой ситуации

Процесс управления должен обеспечивать поддержку защиты от непредвиденных ситуаций, их обнаружение, оповещение и соответствующую реакцию на инцидент. Информацию о непредвиденных ситуациях, если они происходят, следует накапливать и оценивать, чтобы избежать повторения происшествий в будущем и ограничить ущерб.

6.1.4 Управление персоналом

Защитные меры в данной категории призваны снижать риски безопасности в результате ошибок или преднамеренного/непреднамеренного нарушения правил безопасности персоналом (штатным или нанятым по контракту). Ниже перечислены защитные меры в этой области.

1 Защитные меры для постоянного или временного служебного персонала

Все сотрудники должны понимать свою роль и обязанности в том, что касается безопасности. Все процедуры, касающиеся безопасности и необходимые для соблюдения персоналом, следует указать и сформулировать в документах. При наборе персонала они подлежат проверке и, в случае необходимости, должны подписать соглашение о соблюдении правил секретности.

2 Защитные меры для персонала, нанятого по контракту

Следует держать под контролем персонал, работающий по контракту (например, людей, приходящих для уборки или технического обслуживания), а также любого другого посетителя. Персонал, нанятый по контракту на длительное время, должен подписать соглашение о соблюдении правил секретности, прежде чем он может быть допущен (физически или логически) к средствам ИТ организации.

3 Осведомленность о мерах безопасности и обучение

Весь персонал, который использует, разрабатывает, поддерживает и имеет доступ к оборудованию ИТ, следует регулярно инструктировать по вопросам обеспечения безопасности и снабжать соответствующими материалами. Этим гарантируется осведомленность персонала о важности информации, обрабатываемой в интересах бизнеса, сопутствующих угрозах, уязвимости и рисках, и, следовательно, понимание необходимости защитных мер. Пользователей следует обучать правильному использованию средств ИТ в целях избегания ошибок. Для отдельного персонала, например, администраторов корпоративный безопасности и администраторов безопасности ИТ, может потребоваться специальное обучение.

4 Дисциплинарный процесс

Все служащие должны понимать последствия (намеренного или непреднамеренного) нарушения специфической политики безопасности ИТ в рамках всей организации или любого, подтвержденного документально соглашения о соблюдении секретности.

6.1.5 Операционные вопросы

Защитные меры в этой области направлены на проведение действий, поддерживающих безопасное, правильное и надежное функционирование оборудования ИТ и систем, которые связаны и используются с этим оборудованием. Большинство из этих мер могут быть реализованы путем

решения организационных вопросов. Операционные защитные меры необходимо принимать в комбинации с другой, например, физической и технической защитой. Ниже перечислены защитные меры в области операционных вопросов.

1 Управление конфигурацией и изменениями

Управление конфигурацией является процессом отслеживания изменений в системах ИТ. При этом главная задача обеспечения безопасности заключается в том, чтобы изменения в системах ИТ не снижали эффективность защитных мер и достигнутой всеобщей безопасности. Управление в этом случае может способствовать выявлению новых последствий от изменений, происходящих в системах ИТ.

2 Управление емкостью

Управление емкостью следует использовать для предотвращения сбоев вследствие недостаточной емкости. При оценке необходимой емкости для системы ИТ следует учитывать будущие требования к пропускной способности и текущие тенденции.

3 Документация

Все аспекты конфигурации ИТ и операций следует документировать для обеспечения непрерывности и последовательности. Безопасность системы ИТ также нуждается в документальном подтверждении через политику безопасности ИТ, в документах, регламентирующих операционные процедуры безопасности, стратегических отчетах и планах по обеспечению непрерывной работы организации и восстановления после нештатных/аварийных ситуаций. Данная документация должна быть понятной и соответствовать текущей обстановке.

4 Текущее обслуживание

Оборудование ИТ следует правильно обслуживать для обеспечения ее непрерывной надежности, готовности и целостности. Все требования к безопасности, которые должны быть удовлетворены подрядчиками по текущему обслуживанию, следует подтвердить документально в соответствующих контрактах. Текущее обслуживание следует проводить согласно контракту с подрядчиком и с привлечением только квалифицированного персонала.

5 Мониторинг изменений, имеющих отношение к безопасности

Следует осуществлять текущий контроль изменений воздействий, угроз, уязвимости и рисков, а также связанных с ними характеристик. В ходе мониторинга следует отслеживать существующие и новые аспекты. Окружающая среда, в которой расположена система, также подлежит текущему контролю.

6 Следы ревизии и регистрация

Аудиторские и регистрирующие способности серверов (запись следов ревизии и анализ средств), сетей (ревизия аппаратно-программных средств

межсетевой защиты) и применений (аудиторские средства систем передачи сообщений или обработка транзакций) следует использовать для записи подробностей событий, относящихся к обеспечению безопасности. Сюда входят легко опознаваемые несанкционированные или ошибочные события и подробности очевидных нормальных событий, которые могут потребоваться для анализа позднее. Следы ревизии и журналы регистрации следует регулярно просматривать для обнаружения несанкционированной деятельности и принятия соответствующих корректирующих мер. События, зарегистрированные в журналах, следует также анализировать на повторяемость аналогичных происшествий, которые указывают на присутствие слабых мест или угроз, против которых еще не приняты адекватные защитные меры. Такой анализ может также выявлять шаблоны в очевидных несвязанных событиях, которые позволяют идентифицировать людей, занимающихся несанкционированной деятельностью, или определять основные причины проблем безопасности.

Примечание. В этом тексте аудиторские способности систем и применений и "регистрирующие способности" применяются в одном и том же смысле. В то время как такие способности могут быть использованы для поддержки более широких аудитов финансовой сохранности, они удовлетворяют только часть требований для такой деятельности и читателю следует понимать применение этой терминологии.

7 Проведение испытаний по безопасности

Испытания по безопасности следует проводить для проверки, что все оборудование ИТ и связанные с ним компоненты программного обеспечения функционируют безопасным образом. Следует проверить соответствие требованиям, определенным политикой безопасности системы ИТ и соответствующими планами проведения испытаний, а также установить критерии, позволяющие демонстрировать достижение необходимого уровня безопасности.

8 Защита носителей данных

Защита носителей данных охватывает самые разнообразные меры, направленные на обеспечение учета и защиты (на физическом уровне и на уровне среды) магнитных лент, дисков, печатных копий и других носителей. Данными защитными мерами являются: маркировка, регистрация, контроль целостности, защита физического доступа, защита от влияния окружающей среды, регламентация передачи и гарантированное уничтожение носителей данных.

9 Гарантированное стирание памяти

Секретность информации, ранее записанной в запоминающем устройстве, следует сохранять, если эта информация больше не требуется. Следует обеспечить, чтобы файлы, содержащие конфиденциальный материал, стирались или по ним осуществлялась физическая перезапись, или они уничтожались иначе, так как при вызове штатной функции удаления не

всегда обеспечивает невозможность восстановления данных. Средства, одобренные ответственным персоналом (например, офицером по безопасности) следует всегда предоставлять в распоряжение пользователей, чтобы использовать их для полного и безопасного стирания.

10 Разделение обязанностей

Для того чтобы свести к минимуму риски и возможности злоупотребления полномочиями, следует применить распределение обязанностей там, где это требуется и возможно. В частности, обязанности и функции, которые в комбинации могут привести к обходу защитных мер или аудитов или чрезмерному преимуществу для работника, следует держать раздельно.

11 Правильное использование программного обеспечения

Следует гарантировать невозможность повторного копирования печатных материалов, а на лицензионные соглашения должны распространяться права собственника программного обеспечения.

12 Контроль изменений программного обеспечения

Контроль программного обеспечения следует применять для поддержания его сохранности в случае внесения изменений. Контроль изменений программного обеспечения применяют только к программам, в то время как управление конфигурацией и изменениями (см. п.1) применимо целиком к системам ИТ и их окружению. Следует установить методы контроля изменений программного обеспечения, которое управляет всеми изменениями и обеспечивает поддержание безопасности всего процесса. К ним относится санкционированное разрешение на изменения, рассмотрение вопросов безопасности для промежуточных решений и проверка безопасности на конечной стадии.

6.1.6 Планирование обеспечения непрерывной работы и восстановления

Чтобы защитить бизнес, особенно его важные процессы, от воздействий серьезных неисправностей или бедствий и свести к минимуму ущерб, нанесенный такими событиями, следует разработать стратегию и план(ы) обеспечения непрерывной работы организации и восстановления после нештатных/чрезвычайных ситуаций. Сюда входят следующие защитные меры:

1 Стратегия обеспечения непрерывной работы и восстановления

Стратегию обеспечения непрерывной работы организации и восстановления после нештатных и чрезвычайных ситуаций следует сформулировать и подтвердить документально в отношении рассматриваемой системы ИТ на основе потенциальных выявленных вредоносных воздействий на бизнес вследствие неготовности к работе, модификации и разрушения.

2 План обеспечения непрерывной работы и восстановления

На основе стратегии обеспечения непрерывной работы и восстановления следует разработать и подтвердить документально чрезвычайные планы бизнеса, включая планы на случай чрезвычайной обстановки и восстановления после бедствия.

3 Проверка и корректировка плана обеспечения непрерывной работы и восстановления

Прежде чем принять план обеспечения непрерывной работы и восстановления, его следует тщательно проверить, чтобы удостовериться, что он работает в обстоятельствах 'реальной жизни' и с ним ознакомлены все штатные работники, имеющие отношение к его реализации. Так как планы обеспечения непрерывной работы и восстановления могут быстро устаревать, то важно их периодически корректировать. Стратегию обеспечения непрерывной работы и восстановления следует также совершенствовать по мере необходимости.

4 Дублирование

Следует сохранять резервные копии всех важных файлов и другие данные бизнеса, программы и документацию важных систем. Периодичность дублирования следует поддерживать в зависимости от важности информации и в соответствии с планом обеспечения непрерывной работы и восстановления. Резервные копии следует хранить в безопасности и отдельно, а также периодически проверять восстановленные копии на готовность к работе.

6.1.7 Физическая безопасность

Защитные меры в этой области связаны с физической защитой. Их следует рассматривать в комбинации с идентификацией среды окружения, изложенной в 7.2. Несколько последующих пунктов применимы к зданиям, зонам безопасности, местам размещения ЭВМ и офисам. Выбор защитных мер зависит от рассматриваемой части здания. Защитные меры в этой области перечислены ниже.

1 Материальная защита

Физические защитные меры для охраны здания включают заборы, физический контроль доступа, прочные стены, двери и окна. Зоны безопасности в пределах здания следует защищать от несанкционированного проникновения с помощью физического контроля доступа, охраны и т.д. Зоны безопасности могут быть необходимы для оборудования ИТ, например, серверов, связанного с ними программного обеспечения и данных, поддерживающих важные виды деятельности бизнеса. Доступ в такие зоны безопасности следует ограничить до минимального числа необходимого персонала, а все подробности доступа следует регистрировать. Все

диагностическое и контрольное оборудование следует хранить в безопасном месте и его использование следует держать под строгим контролем.

2 Противопожарная защита

Оборудование и окружающие зоны, включая доступ к ним, следует защищать от распространения огня из какого-либо места в здании или соседних строениях. Опасность пожара вблизи комнат/зон, содержащих оборудование, следует свести до минимума. Следует иметь защиту от пожаров, начинающихся в пределах и/или затрагивающих комнаты/зоны, содержащие главное оборудование. Защитные меры должны предусматривать обнаружение огня и дыма, охранную сигнализацию и подавление очага возгорания. Следует позаботиться также о том, чтобы противопожарная защита не вела к повреждению систем ИТ от воды или других средств тушения.

3 Защита от воды/рабочей жидкости

Не следует располагать значимые средства в какой-либо зоне, в которой возможна утечка воды или другой жидкости. Следует обеспечить подходящую защиту в случае, когда существует значимая угроза затопления.

4 Защита от стихийных бедствий

Здания, содержащие важное оборудование, следует защищать от удара молнии. Также самое важное оборудование следует оснастить защитой от грозового разряда. Защита от стихийных бедствий может быть достигнута за счет размещения оборудования в зонах, где стихийные бедствия маловероятны, а также разработки стратегии и плана обеспечения непрерывной работы и восстановления.

5 Защита от воровства

Чтобы обеспечить контроль уровня запасов, все части оборудования следует однозначно идентифицировать и учитывать. Охрану/приемщиков следует нацеливать на проверку оборудования или ресурсов, выносимых из комнаты/зоны или здания без разрешения. Следует соответственно защищать секретную информацию и собственническое программное обеспечение на портативных носителях (например, гибких дисках).

6 Энергоснабжение и кондиционирование

Все оборудование ИТ следует защищать при необходимости в случае отключений электричества. Следует предусмотреть подходящий источник энергоснабжения и бесперебойного питания. Другой целью защиты является обеспечение допустимой температуры и влажности.

7 Прокладка кабелей

Силовые и коммуникационные кабели, по которым осуществляется передача данных или предоставление сервисов ИТ, следует защищать от перехвата, повреждения и перегрузки. Проложенные кабели следует предохранять от случайного или преднамеренного повреждения, для этого их следует выбирать и прокладывать соответствующим образом. При

планировании следует учитывать перспективные разработки во избежание многих проблем. В оправданных случаях кабели следует защищать от возможного подслушивания.

Таблица 6.1.1. Политика и менеджмент безопасности ИТ

	Нормы и правила Для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1])	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Политика безопасности ИТ	3.1	--	1.1, 1.2	5.1	*.3.1.1	3	--	5.1, 5.2
2. Политика безопасности систем(ы) ИТ	--	--	1.1, 1.2	5.2, 5.3	*.3.1.1	3	--	5.2, 5.3
3. Управление безопасностью ИТ	4.1.1, 4.1.2	--	1.1, 1.2	6	*.3.1.1	4	2.1	6
4.Распределение ответственности	4.1.3	--	1.3	2.4, 2.5, 3	*.3.1.1	4	2.1	2.4, 2.5, 3
5. Организация безопасности ИТ	4.1	--	1.2	3.5	--	4	2.2	3.5
6.Идентификация имущества и оценка	5	--	2.2	7.1	--	5.6, 7.1	5.1	7.1
7. Утверждение систем ИТ	4.1.4	--	--	8	5	--	6.7	8, 9

1) * Обозначает любое число между 6 и 11.

Таблица 6.1.2. Проверка соответствия безопасности

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1.Соответствие с политикой безопасности и защитными мерами	12.2	--	1.3	10.2.3	--	10.2	7.1, 7-2	9.4, 10.2.3
2.Соответствие с законами и нормативными документами	12.1	--	3.1, 3.2	6.3, 10.2.3	6.3.11	8.18, 10.2	8.1	1.5, 2.9, 6.3, 10.2.3

Таблица 6.1.3. Действия в особой ситуации

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Оповещение об особой ситуации в обеспечении безопасности	6.3.1	--	М2	12	--	10.4	--	12
2. Сообщение о слабых местах в защите	6.3.2	--	М2	12	--	10.4	--	12
3. Сообщение о сбое в функционировании программного обеспечения.	6.3.3	--	М2	12	--	10.4	--	12
4. Управление в особых ситуациях.	8.1.3	--	М2	12	--	10.4	--	18.1.3

Таблица 6.1.4. Персонал

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Защита постоянного и временного штата	6.1	--	3.2, М3	10.1	*.3.9	9.2	4.1, 2.2	10.1
2. Защита для работников, нанятых по контракту	6.1	--	--	10.3	*.3.9	9.2	4.1, 2.2	10.3
3. Понимание вопросов безопасности и профессиональная подготовка	6.2	--	1.2, М3	13, 10.1.4	*.3.9	9.1	4.2, 2.2	13, 10.1.4
4.Дисциплинарный процесс	6.3.5	--	3.2, М3	--	*.3.9	9.2.6	2.2.1	13.1

1) * Обозначает любое число между 6 и 11.

Таблица 6.1.5. Операционные вопросы

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Управление конфигурацией и изменениями	8.2, 10.5	--	--	14.3, 8.4.1	--	7.4	9	14.3, 8.4.1, 8.4.4
2. Управление емкостью	8.2.1	--	--	--	--	--	--	--
3. Документация	8.1.1, 8.6.3	--	М2	14.6	--	8.4.6, 8.5.7, 8.7	--	14.6
4 Текущее обслуживание	7.2.4	--	М2	14.7	*.3.6	8.1.4, 8.10.5, 10.1	6.5	14.7
5. Текущий контроль изменений, касающихся безопасности	--	--	1.2	7.3.3	--	7.4, 8.1.3, 8.2.5,8.3.7	6.7	7.3.3, 8.4.4
6. Следы аудита и регистрация	8.4	--	М2	18	--	7.3, 8.1.8, 8.2.10, 8.9.5	6.7	(18)
7. Испытание системы безопасности.	--	--	М2	8.4.3	--	8.3.5	6.7, 3	8.4.3

	Нормы и правила для управления безопаснос-тью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информацион ных систем здравоохра-нения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
8. Средства контроля сетевого доступа	8.6	--	8, М2	14.5	*.3.5	8.4 – 8.14	5	14.5
9.Гарантированн ое стирание в ЗУ	--	--	М4	--	---	8.1.9	6.3, 5	14.5.7
10. Разделение обязанностей	8.1.4	--	М2	--	--	--	--	10.1.1
11. Правильное использование ПО	12.1.2	--	М2	--	*.3.8	8.3	6.3	14.2
12 Контроль за изменениями в ПО	10.5.1, 10.5.3	--	М2	--	*.3.8	8.3.7	6.3	8.4.4, 14.2

[1]* Обозначает любое число между 6 и 11.

Таблица 6.1.6. Планирование обеспечения непрерывной работы и восстановления

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Стратегия обеспечения непрерывной работы и восстановления	11.1.1, 11.1.2	--	3.3, М6	11.2, 11.3, 11.4	*.3.3	8.19, 8.1.7, 8.4.5, 8.5.5, 8.6.5, 8.7.5, 8.8.3, 8.19	7.3, 7.4, 7.5	11.2, 11.3, 11.4
2. План обеспечения непрерывной работы и восстановления	11.1.3, 11.1.4	--	3.3, М6	11.5	*.3.3		--	11.5
3. Испытание и корректировка плана обеспечения непрерывной работы и восстановления	11.1.5	--	3.3, М6	11.6	*.3.3		--	11.6
4. Резервные копии	8.4.1	--	3.4	14.4	*.3.2.4	--	7.1, 7.2	14.4

[1]* Обозначает любое число между 6 и 11.

Таблица 6.1.7. Физическое обеспечение безопасности

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Материальная защита	7.1	--	4.1, 4.3, M1	15.1	*.3.1.2	8.1.1, 8.6.2, 8.9.1	3.1, 3.4, 4	15.1
2.Противопожарная защита	7.2.1	--	--	15.2	*.3.1.4	8.1.1, 8.6.2, 8.9.1	3.1, 3.2, 7.5	15.2
3. Предохранение от воды/рабочей жидкости	7.2.1	--	M2	15.5	*.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.5
4. Защита на случай стихийного бедствия	7.2.1	--	M2	15.4	*.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.4
5. Охрана от воровства	7.1	--	1.2	15.1	*.3.1.3	8.1.1, 8.6.2, 8.9.1	3.3, 3.4, 4	15.1
6. Энергоснабжение и кондиционирование	7.2.2	--	M2	15.6	*.3.4	8.1.1, 8.6.2, 8.9.1	3.2, 7.3	15.6
7. Прокладка кабелей	7.2.3	--	4.2, M1	--	--	8.1.1, 8.6.2, 8.9.1	8.2	15, 15.1, 15.7

1) * Обозначает любое число между 6 и 11.

6.2 Специальные защитные меры систем ИТ

Таблицы в конце этого раздела показывают, где искать дополнительную информацию по упомянутым категориям защитных мер.

6.2.1 Идентификация и аутентификация (И&А)

Идентификация является средством, с помощью которого пользователь предоставляет в систему заявленную идентичность. Аутентификация является средством установления действительности этого заявления. Далее следуют примеры достижения И&А (возможны другие механизмы классификации И&А).

1 И&А на основе того, что известно пользователю

Пароли являются наиболее типичным способом И&А на основе известного пользователю нечто, связанного с процессом распознавания. Распределение паролей и их периодическую смену следует держать под контролем. Если пользователи сами выбирают пароли, то они должны быть осведомлены об общих правилах назначения и обращения с паролями. Для поддержки паролей можно применять программное обеспечение, например, путем ограничения использования общих паролей или узоров и символов. В случае пожелания или необходимости иметь копии паролей их следует надежно хранить для разрешения доступа пользователя, не имеющего или забывшего пароль. Идентификация и аутентификация на основе нечто, известного пользователю, может использовать способы криптографии и протоколы распознавания. Этот тип распознавания и подтверждения может также применяться для И&А при удаленном входе в систему.

2 И&А на основе того, чем владеет пользователь

Объектами, которыми владеет пользователь для целей И&А, могут быть карточки (жетоны) с запоминающим устройством (ЗУ) или микропроцессором. Общепринято применять кредитные карточки с магнитным запоминающим устройством на обратной стороне. Аутентификация обеспечивается на основе нечто, имеющегося в распоряжении пользователя (карточка) или известного пользователю (личный идентификационный номер). Типичным примером является карточка с микропроцессором.

3 И&А на основе нечто самого пользователя

Технологии биометрической аутентификации используют единственные в своем роде характеристики и атрибуты индивидуального распознавания личности. Это могут быть отпечатки пальцы, геометрия ладони, сетчатка глаз, а также тембр голоса и подпись личности. Уместные подробности могут надежно храниться в памяти микропроцессора карточки или в системе.

6.2.2 Логический контроль доступа и аудит

Защитные меры в этой области реализуются для того, чтобы:

– ограничивать доступ к информации, компьютерам, сетям, приложениям, ресурсам системы, файлам и программам;

– регистрировать подробности ошибки и действий пользователя при аудите и анализе записей для обнаружения и исправления нарушений безопасности соответствующим образом.

Общепринятым средством усиления контроля доступа является использование тонкостей И&А, включенных в списки контроля доступа, которые определяют, какие файлы, ресурсы и т.д. разрешены для доступа пользователя и какие формы может принимать этот доступ. Ниже перечислены защитные меры в области контроля логического доступа и аудита.

1 Политика контроля доступа

Для каждого пользователя или группы пользователей следует четко определить политику контроля доступа. Эта политика дает права доступа в соответствии с требованиями бизнеса, например, готовность к работе, производительность и принцип 'необходимости знать'. Следует руководствоваться общим принципом: 'даем столько прав, сколько необходимо, и лишь столько, сколько возможно'. Распределение прав доступа следует учитывать в подходе организации к обеспечению безопасности (например, открытый или ограниченный доступ), культуре удовлетворения потребностей бизнеса и признанию со стороны пользователей.

2 Доступ пользователя в ЭВМ

Контроль компьютерного доступа применяется для предотвращения несанкционированного проникновения. Следует обеспечить возможность опознавания и проверки подлинности личности каждого санкционированного пользователя, как при успешной, так и неудачной его попытке осуществить регистрацию. Контроль компьютерного доступа может быть облегчен с помощью паролей или другого метода идентификации и аутентификации.

3 Доступ пользователя к данным, сервисам и приложениям

Контроль доступа следует применять для защиты данных и сервисов в компьютере или пределах сети от несанкционированного проникновения. Это может быть сделано с помощью подходящих механизмов И&А (см. п. 6.2.1), соответствующих интерфейсов между сетевыми сервисами и конфигурации сети, обеспечивающей только санкционированный доступ к сервисам ИТ (ограничительное распределение прав). Чтобы предотвратить несанкционированный доступ к приложениям, следует ввести контроль

доступа на основе роли, которую пользователь играет в выполнении функций бизнеса.

4 Пересмотр и корректировка прав доступа

Все права доступа, предоставленные пользователю, следует периодически пересматривать и корректировать, если изменились требования к обеспечению безопасности и потребности бизнеса для доступа. Права привилегированного доступа следует пересматривать чаще для контроля их правильного использования. Права доступа необходимо изымать сразу, когда пропадает их необходимость.

5 Контрольные журналы

Все работы с поддержкой ИТ следует регистрировать, а контрольные журналы следует периодически просматривать для установления успешных и неудачных попыток войти в систему, получить доступ к данным, функциям используемой системы и т.д. Неисправности также следует регистрировать и периодически анализировать. Полученные данные следует применять в соответствии с законодательством по защите данных и секретности, например, их можно хранить только в течение ограниченного периода времени и использовать только для обнаружения нарушений безопасности.

6.2.3 Защита от вредоносного кода

Вредоносные коды могут поступать в систему по внешним соединениям либо через файлы и программное обеспечение с переносных дисков. Если не были применены соответствующие защитные меры, то вредоносный код может оставаться незамеченным вплоть до оказания ими негативного воздействия. Вредоносный код может компрометировать защитные меры (например, перехватывать и раскрывать пароли), случайно раскрывать или изменять информацию, нарушать целостность системы, уничтожать информацию и использовать без разрешения ресурсы системы.

Вредоносный код бывает следующих видов:

– вирусы;

– черви;

– троянские кони.

Носителями вредоносного кода являются:

– исполняемое программное обеспечение;

– файлы данных (содержащие исполняемые макроопределения, например, текстовые документы и таблицы);

– исполняемые вложения на Веб-страницах.

Вредоносные коды могут распространяться через:

– дискеты;

– другие съемные носители;

– электронную почту;

– компьютерные сети;

– скачиваемые файлы.

Вредоносные коды могут быть внесены в систему путем преднамеренных действий пользователя либо через не видимые для пользователя взаимодействия на системном уровне. Защита от вредоносного кода может быть обеспечена с помощью перечисленных ниже защитных мер:

1 Сканеры

Различные формы вредоносного кода могут быть обнаружены и удалены путем использования специального сканирующего программного обеспечения, а также путем проверки целостности файловых хранилищ. Сканеры могут работать в автономном режиме или под управлением центрального процессора. Работа сканера в режиме онлайн обеспечивает активное предохранение, т.е. обнаружение (и, возможно, удаление) вредоносного кода до распространения заражения и нанесения ущерба системе ИТ. Имеются сканеры для автономных компьютеров и рабочих станций, серверов файлов, серверов электронной почты и средств межсетевой защиты. Однако пользователи и администраторы должны понимать, что нельзя полагаться на сканеры для обнаружения всех возможных вариантов вредоносного кода (даже если они определенного типа), потому что непрерывно возникают новые формы вредоносного кода.

2 Проверки целостности

Типично требуются другие формы защиты, чтобы усиливать предохранение, которое обеспечивают сканеры. Например, можно использовать контрольные суммы для проверки изменений, внесенных в программу. Программное обеспечение целостности должно быть неотъемлемой частью технических мер защиты, обеспечивающей предохранение от вредоносного кода. Этот технический прием может быть использован для файлов данных и программ, которые не имеют статуса информации для дальнейшего применения.

3 Контроль обращения съемных носителей

Неконтролируемое обращение носителей (особенно дискет) может привести к увеличенному риску внедрения вредоносного кода в системы ИТ организации. Контроль обращения в среде передачи может быть достигнут путем использования:

– специального программного обеспечения;

– административных мер защиты (см. ниже).

4 Административные меры защиты

Следует разрабатывать руководящие указания для пользователей и администраторов, определяющие в общих чертах процедуры и практические действия для минимизации возможности внесения вредоносного кода. Такие указания должны охватывать загрузку игр и другого исполняющего

программного обеспечения, использование разных типов сервисов в сети Интернет и импортные файлы разных типов. При необходимости следует делать независимые обзоры источника или исполнительного кода. Следует проводить на месте ознакомительное обучение и дисциплинарные действия, чтобы персонал соблюдал документально подтвержденные процедуры и практики предотвращения поступления вредоносного кода в систему.

6.2.4 Управление сетью

Эта область включает темы планирования, эксплуатации и администрирования сетей. Должная конфигурация и администрирование сетей являются эффективными средствами снижения степени рисков. В настоящее время разрабатываются несколько документов ИСО, содержащих последующую информацию о защитных мерах для обеспечения безопасности сети. Ниже перечислены защитные меры в области управления сетью.

1 Операционные процедуры

Установление операционных процедур и распределение ответственности необходимо для обеспечения правильной и безопасной работы сетей. Сюда входит документация операционных процедур и установление порядка действий для реагирования на соответствующие особые случаи (см. 6.1.3).

2 Системное планирование

Чтобы гарантировать надежное функционирование и адекватную пропускную способность сети, необходимы перспективное планирование и приготовление, а также текущий контроль (включая загрузочные статистики). Следует применять критерии приемки для новых систем, контролировать изменения и реагировать на них (см. также 6.1.5).

3 Конфигурация сети.

Подходящая конфигурация сети является весьма важной для ее надежного функционирования. Сюда входит стандартизованный подход для конфигурации серверов по всей организации и, что очень важно, хорошая сопроводительная документация. Далее следует обеспечить применение серверов только для специальных целей (например, никакие другие задачи не должны решаться средствами межсетевой защиты) и достаточное предохранение от неисправностей.

4 Изоляция сетей

Чтобы свести к минимуму риски и возможности неправильного использования сети в работе, следует изолировать (логически или физически) ресурсы организации, связанные с решением критичных бизнес-задач и/или со строго конфиденциальной информацией. Кроме того, ресурсы, связанные с разработкой, должны быть отделены от ресурсов, находящихся в эксплуатации.

5 Мониторинг сети

Текущий контроль сети следует использовать для выявления слабых мест в конфигурации существующей сети. Это позволяет вносить изменения в конфигурацию, вызванные анализом трафика, и помогает идентифицировать взломщиков сети.

6 Обнаружение вторжения

Попытки получить доступ в систему или системы и успешный несанкционированный вход следует обнаруживать с тем, чтобы организация могла реагировать соответствующим и эффективным образом.

6.2.5 Криптография

Криптография – это способ преобразования данных, нацеленный на обеспечение их защиты. Существует множество различных способов ее применения в процессах защиты информационных технологий, например, криптография может быть использована для обеспечения конфиденциальности и/или целостности данных, для обеспечения неотказуемости от совершенных над информацией действий и для применения передовых методов И&А. При использовании средств криптографической защиты необходимо учитывать требования всех соответствующих законов и норм. Одним из наиболее важных аспектов криптографии является адекватная система управления ключами, которая в деталях рассмотрена в стандарте *СТ РК ИСО/МЭК 11770-1-2008*. Дополнительная информация о классах криптографических приложений приведена в приложении Б стандарта *СТ РК ИСО/МЭК 11770-1-2008*. Использование криптографии в И&А рассматривается в п. 6.2.1. настоящего документа. Для поддержки некоторых приложений, реализующих криптографические защитные меры, могут быть использованы сервисы постановки временных отметок.

1 Обеспечение конфиденциальности данных

В обстоятельствах, когда важно сохранение конфиденциальности, например, в случае особенно секретной информации, необходимо рассматривать защитные меры путем шифрования информации для хранения или передачи по сетям. Решение о применении шифрования следует принимать с учетом:

– соответствующих государственных законов и правил;

– требований управления ключами и трудностей, которые придется преодолевать для обеспечения действительного улучшения безопасности без создания новых уязвимых мест;

– пригодности механизмов шифрования, используемых для ситуации развертывания, и степень необходимой защиты.

2 Обеспечение целостности данных

В обстоятельствах, когда важно сохранение целостности хранимых или обрабатываемых данных, функции молчания, цифровые подписи и/или защитные меры целостности следует рассмотреть для предохранения информации в памяти или предназначенной для передачи. Защитные меры целостности (например, использование так называемых кодов аутентификации сообщений) обеспечивает защиту от случайного или намеренного изменения содержания, добавления или исключения информации. Цифровые подписи могут обеспечивать не только подобное предохранение целостности сообщений, но имеют свойства, позволяющие обеспечивать неотказуемость от совершенных над информацией действий. Решение использовать цифровые подписи и другие меры защиты целостности следует принимать с учетом следующего:

– законов государства и правил, имеющих к этому отношение,

– инфраструктуры общедоступных ключей,

– требований к управлению ключами и трудностей, которые придется преодолевать для обеспечения действительного улучшения безопасности без создания новых уязвимых мест.

3 Обеспечение неотказуемости

Методы криптографии (например, методы электронно-цифровой подписи) могут быть использованы для подтверждения (доказательства) факта отправки, передачи, доставки, подтверждения приема сообщений, взаимодействий и новостей.

4 Подлинность данных

В ситуациях, когда важно обеспечить подлинность, можно использовать цифровую подпись для подтверждения подлинности данных. Эта необходимость особенно возникает при ссылке на данные источников третьей стороны или когда большая группа лиц заинтересована в точности справочных данных. Цифровые подписи могут также применяться для подтверждения, что данные поступают от определенного лица.

5 Управление ключами

Управление ключами включает технические, организационные и процедурные аспекты, которые необходимы для поддержки любого способа криптографии. Задачей управления ключами является надежное администрирование и менеджмент криптографическими ключами и связанной с этим информацией. Управление ключами включает генерирование, регистрацию, сертификацию, распределение, установку, хранение, архивирование, отмену, извлечение и уничтожение ключей. Кроме

того, важно правильно назначать управление ключами, чтобы снизить риск дискредитации ключей и их использование людьми, не имеющими на то полномочий. Процедуры управления ключами зависят от применяемого алгоритма, использования ключа по назначению и политики безопасности ИТ. Более подробно об управлении ключами см. в стандарте *СТ РК ИСО/МЭК 11770-1-2008*.

Таблица 6.2.1. Идентификация и аутентификация (И&А)

	Нормы и правила для управления безопас-ностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопас-ности ЭВМ	Категории безопасности и защита информацион ных систем здравоохране ния[1])	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. И&А на основе чего-то, что пользователь знает	9.2.3, 9.3.1, 9.4., 9.5.1	4.2.1, 5.2.1, приложение А	М4	16.1	*.3.2.1	7.2.1, 7.2.2	6.2	16.1
2. И&А на основе чего-то, чем пользователь владеет			--	16.2	*.3.2.1		6.2	16.2
3. И&А на основе нечто самого пользователя			--	16.3	*.3.2.1		6.2	16.3

[1]* Обозначает любое число между 6 и 11.

Таблица 6.2.2. Контроль логического доступа и аудит

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Политика контроля доступа	9.1	--	М2	17.1, 17.2, 17.3	*.3.2.1	7.2, 8.1.2, 8.2.2, 8.4.1	6.4	17.1, 17.2, 17.3
2. Доступ пользователя к ЭВМ	9.2, 9.3, 9.5	4.2.4, 5.2.4, приложение А	М4		*.3.2.1		6.2, 3.3	
3. Доступ пользователя к данным, сервисам и приложениям	9.4, 9.6		М4		*.3.2.1		6.4	
4. Пересмотр и корректировка прав доступа	9.1, 9.2.4	--	М2	17.4	*.3.2.1		--	17.4
5.Контрольные журналы	9.7	--	М4	18	*.3.2.2	7.3, 8.2.10	6.7	18

[1]* Обозначает любое число между 6 и 11.

Таблица 6.2.3. Защита от вредоносного кода

	Нормы и правила для управле-ния безопас-ностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасност и ЭВМ	Категории безопасности и защита информацион ных систем здравоохране ния[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Сканеры	8.3	--	М4	--	*.3.10	8.3.11, 8.3.16	7.4	4.6, 5.2.1, 6.4, 8.4.4, 11
2. Средства проверки целостности	8.3	--	М4	--	--	8.3.11, 8.3.16	7.4	--
3. Контроль обращения сменных носителей информации	7.3.2	--	--	--	--	--	--	--
4. Процедурные меры защиты	8.3	--	М4	--	*.3.10	8.3.11, 8.3.16	7.4	6.2.2, 9.3, 12, 14.2

[1]* Обозначает любое число между 6 и 11.

Таблица 6.2.4. Управление сетью

	Нормы и правила для управления безопасностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Операционные процедуры	8.5.1	--	М2	--	--	8.2, 8.3	8.2	14.6
2. Планирование системы	8.2	--	М2, М4	8.4	--		6.1	8.4
3. Конфигурация сети	--	--	М4	--	--		9, 6.1	14.3
4 Разделение сети	9.4.6	--	М2	--	--	--	3.1	--
5. Мониторинг сети	9.7	--	М2	18.1.3	--	8.2.7	--	18.1.3
6. Обнаружение вторжения	--	--	--	18.1.3	--	--	6	18.1.3

Таблица 6.2.5. Криптография

	Нормы и правила для управле-ния безопас-ностью	Стандарт ETSI по базисной безопасности. Свойства и механизмы	Руководство по базисной защите ИТ	Справочник NIST по безопасности ЭВМ	Категории безопасности и защита информационных систем здравоохранения[1)]	Руководство ТК68 по защите информации	Рекомендации для рабочих станций	Канадский справочник по безопасности ИТ
1. Предохранение секретности данных	10.3.2	4.2.2, 5.2.2, приложение А	М4	19.5.1	--	8.23	8.1	19.5.1
2. Предохранение целостности данных	10.3.3	4.2.3, 5.2.3, приложение А	М4	19.5.2	--	8.23	8.1	19.5.2
3. Неотказуемость	10.3.4	4.2.6, 5.2.6, приложение А	--	19.2.3	--	8.23	8.1	19.2.3
4. Аутентификация данных	10.3.2	4.2.3, 5.2.3, приложение А	М4	19.5.2	--	8.23	8.1	19.5.2
5. Управление ключами	10.3.5	4.2.5, 5.2.5, приложение А	--	19.3	--	8.23	8.1	19.3

[1]* Обозначает любое число между 6 и 11.

7 Базисный подход: выбор защитных мер согласно типу системы ИТ

Как было рассмотрено в разделе 6, имеются два разных пакета защитных мер, механизмов и/или процедур, которые могут быть применены, чтобы предохранять системы ИТ. С одной стороны, имеется лишь несколько организационных защитных категорий, которые обычно применимы для каждой системы ИТ, если специфические обстоятельства делают их необходимыми (как считается в 6.1), независимо от индивидуальных компонентов. Выбор этих защитных мер рассматривается в 7.1. По причине общей применимости следует всегда рассматривать защитные меры из этих категорий. Более того, большинство защитных мер являются дорогими для реализации, так как они основаны на представлении организационных структур и процедур.

С другой стороны, имеются специфические защитные меры систем ИТ (как считается в 6.2) и тогда выбор этих защитных мер зависит от типа и характеристик рассматриваемой системы ИТ. Выбор этих защитных мер рассматривается в 7.2.

Возможно, что одна или больше из этих категорий или специфических мер защиты не применимы к системе ИТ. Например, шифрование может не потребоваться, если передаваемая или принимаемая информация не нуждается в конфиденциальности, а целостность может быть проверена иначе. Более детальный выбор может быть сделан только путем рассмотрения дополнительной информации (см. разделы 8 и 9).

После того, как все типы защиты, применимые для системы ИТ, идентифицированы, дополнительная информация по ним и специфическим защитным мерам может быть получена путем использования раздела 6 или одного или больше документов, перечисленных в приложениях А - И. Связи с разделом 6 показаны в таблице в конце раздела 7. Перед реализацией выбранных защитных мер их следует внимательно проверить путем сравнения с уже существующей и/или планируемой защитой (см. 5.3).

Следует рассмотреть применение более точного анализа (см. разделы 8 и/или 9) для выбора дополнительных защитных мер. Если защитные меры выбираются по разным критериям (базисные защитные меры и дополнительная защита), то окончательный пакет защитных мер, намеченный для реализации, следует внимательно согласовать вместе. После обзора нескольких систем ИТ, следует рассмотреть возможность развертывания базисной защиты в масштабе всей организации (см. раздел 10).

Другой возможностью выбора защитных мер без подробного рассмотрения этой проблемы является применение прикладной специфической базисной защиты. Например, имеются справочники по базисной защите для электросвязи, здравоохранения, банковской системы

(см. приложения Б, Д и Е) и много других. При использовании этих справочников можно, например, сравнивать существующие или планируемые защитные меры с теми, которые рекомендованы. Однако при выборе защиты, которая должна быть внедрена, все же полезно внимательно рассмотреть потребности и беспокойства, связанные с обеспечением безопасности.

7.1 Обычно применяемые защитные меры

Обычно применяются следующие категории защитных мер:

– управление безопасностью ИТ и политика в этой области (6.1.1);

– проверка на соответствие уровню безопасности (6.1.2);

– действия в особых ситуациях (6.1.3);

– управление персоналом (6.1.4);

– операционные вопросы (6.1.5);

– планирование обеспечения непрерывной работы и восстановления (6.1.6);

– физическая защита (6.1.7).

Защитные меры этих категорий образуют базис для успешного управления безопасностью информационных технологий. В этом смысле их не следует недооценивать. Важно также обеспечить рабочее взаимодействие этих защитных мер с технической защитой, рассмотренной ниже. Как много может сделать организация в этих областях, зависит от потребностей и забот, связанных с обеспечением безопасности (см. раздел 8), и ресурсов, имеющихся в наличии.

Многие другие категории защиты можно применить в большинстве случаев, но способ реализации обычно является специфическим к частным обстоятельствам (например, защитные меры, обеспечивающие контроль доступа к сети, отличаются от защиты, предоставляющей доступ к автономной ЭВМ).

При выборе защитных мер из обычно применяемых защитных категорий полезно принять во внимание размер организации, потребности в обеспечении безопасности, так как все это влияет на степень реализации защитных мер. Например, небольшая организация не будет иметь ни потребности, ни персонал, чтобы учредить комитет по обеспечению безопасности ИТ, тем не менее, кто-то должен быть на месте, чтобы выполнять эти функции. Все защитные меры, перечисленные в 8.1, следует сводить в соответствующую систему всякий раз, когда это необходимо.

7.2 Специальные защитные меры систем ИТ

В дополнение к обычно применяемой защите следует также выбирать специальные защитные меры для каждого уместного типа компонента

системы. В таблице ниже показан пример, как начинать процесс выбора специальных защитных мер системы ИТ. В этом примере "X" относится к защите, которую следует реализовать в нормальных обстоятельствах, а '(X)' отмечает защитные меры, которые могут потребоваться в некоторых случаях. Процесс выбора защиты будет продолжен путем рассмотрения защитных характеристик, представленных в 6.2. Дополнительная информация может быть получена из документов по базисной защите, перечисленных в приложениях А - И.

	Автономная рабочая станция	Подсоединенное к сети АРМ (клиент без разделяемых ресурсов)	Подсоединенные к сети сервер или АРМ с ресурсами коллективного пользования
И & А			
И & А на основе чего-то, что пользователь знает	X	X	X
И & А на основе того, чем пользователь владеет	X	X	X
И & А на основе нечто самого пользователя	(X)	(X)	(X)
Контроль логического доступа и аудит			
Политика контроля доступа			X
Доступ пользователя в ЭВМ	X	X	X
Доступ к данным, сервисам и приложениям.	X	X	X
Обзор и корректировка прав доступа			X
Контрольные журналы	X	X	X
Вредоносный код			
Сканеры	X	X	X
Средства проверки целостности	X	X	X
Контроль обращения съемных носителей	X	X	X
Процедурные защитные меры	X	X	X
Управление сетью			
Операционные процедуры			X
Системное планирование			X
Конфигурация сети			X
Разделение сети			X
Мониторинг сети			X
Обнаружение вторжения			X
Криптография			
Сохранение секретности данных	(X)	(X)	(X)
Защита целостности данных	(X)	(X)	(X)
Неотказуемость		(X)	(X)

Подлинность данных	(X)	(X)	(X)
Управление ключами	(X)	(X)	(X)

8 Выбор защитных мер согласно заботам о защите и угрозам

Выбор защитных мер в соответствии с заботами об обеспечении безопасности и угрозами, изложенный в этом разделе, может быть использован следующим образом:

1. На первом этапе следует идентифицировать и оценить заботы, касающиеся обеспечения безопасности. Следует рассмотреть требования секретности, целостности, готовности, подотчетности, подлинности и надежности. Прочность защиты и количество выбранных защитных мер должны соответствовать оценкам обеспокоенности состоянием безопасности.

2. На втором этапе для каждой заботы, связанной с обеспечением безопасности, перечисляются типовые угрозы, а для каждой угрозы предлагаются защитные меры в соответствии с рассматриваемой системой ИТ. Различные типы систем ИТ перечислены в подразделе 5.1, а возможные защитные меры приведены в подразделах 6-го раздела. Описанный путь предоставляет возможность удовлетворить специфические потребности в обеспечении безопасности и направлять защиту на те места, где это действительно необходимо.

8.1 Оценка забот, касающихся обеспечения безопасности

Чтобы выбрать соответствующую защиту эффективным путем, необходимо понимать те беспокойства, которые касаются обеспечения безопасности деловых операций, поддерживаемых рассматриваемой системой ИТ. После идентификации такой озабоченности и с учетом соответствующих угроз можно выбирать защитные меры согласно описанию в 8.2 - 8.5.

Если оценка согласно этому разделу покажет необходимость высокой степени безопасности, то рекомендуется подробный подход к решению этой проблемы. Дополнительный материал можно найти в разделе 9.

Заботы, касающиеся обеспечения безопасности, включают следующее:

– возможность раскрытия секретности;

– нарушение целостности;

– неготовность к работе;

– потеря подотчетности;

– сомнения в подлинности;

– снижение надежности.

В оценку следует включить и саму систему ИТ, хранимую или обрабатываемую в ней информацию и деловые операции, которые она

выполняет. Этим выявляются задачи защитных мер, которые будут выбираться. Разные части системы ИТ или хранимой и обрабатываемой информации могут вызывать разную озабоченность с точки зрения обеспечения безопасности. Важно соотнести эти озабоченности с ценными свойствами системы, так как это влияет на угрозы, которые могли бы применяться, а, следовательно, и на выбор защиты.

Заботы, связанные с обеспечением безопасности, можно рассматривать с позиции воздействия неисправности или нарушения безопасности, которое могло бы стать причиной серьезного или незначительного сбоя деловых операций, или не причинило бы никакого вреда. Например, если секретная информация компании обрабатывается в системе ИТ, то несанкционированное раскрытие этой информации конкуренту дает ему возможность делать предложения по более низкой цене, нанося тем самым ущерб бизнесу компании. С другой стороны, если общедоступная информация обрабатывается в системе ИТ, то ее раскрытие не принесет никакого вреда. Рассмотрение возможных угроз (см. 8.2 - 8.5) может помочь в прояснении забот об обеспечении безопасности. Оценки, характеризуемые ниже, следует делать отдельно для каждого ресурса системы, так как обеспечение безопасности для каждого ресурса может быть разным. В случае, когда заботы, связанные с обеспечением безопасности, достаточно известны, то ресурсы с одинаковыми или подобными требованиями бизнеса и заботами могут быть сведены в группы.

Если система ИТ обрабатывает больше, чем один тип информации, то разные типы могут нуждаться в отдельном рассмотрении. Предохранение, которое в состоянии предоставить система ИТ, должно быть достаточным для всех типов обрабатываемой информации. Таким образом, если некоторая информация имеет высокую степень обеспечения безопасности, то всю систему следует предохранять соответственно. В случае, когда объем информации с высокой степенью обеспечения безопасности небольшой, то следует рассмотреть возможность перевода этой информации в другую систему, если она совместима с процессами бизнеса.

В случае, когда выявлено, что все возможные утраты секретности, целостности, готовности, подотчетности, подлинности и надежности, способны причинить незначительный ущерб, то подход от пункта 8.2 и далее обеспечит достаточную безопасность для рассматриваемой системы ИТ. В случае, когда любая из выявленных выше утрат способна причинить серьезный ущерб, то следует оценить, есть ли необходимость в выборе защитных мер, предложенных дополнительно в 8.2-8.5. Предложения по более подробным оценкам и выбору защитных мер на основе результатов этих оценок даны в *СТ РК ИСО/МЭК 13335-3-2008* и в разделе 9. Тем не менее, защитные меры, предложенные в 10.2 и далее могут служить базисом для более точного выбора.

8.1.1 Возможность раскрытия секретности

Рассмотрите, какой ущерб мог бы возникнуть при утрате конфиденциальности определенного ресурса(ов) (преднамеренно или случайно). Например, раскрытие секретности может привести к следующему:

– утрате общественного доверия или снижению общественного имиджа;

– ответственности перед законом, включая ответственность за нарушение законодательства в области предохранения данных;

– вредоносному влиянию на политику организации;

– созданию угрозы безопасности персонала;

– финансовым потерям.

В соответствии с ответами на поставленные выше вопросы следует решить, будет ли общий ущерб от раскрытия секретности серьезным, незначительным или вообще не будет никакого ущерба. Это решение следует подтвердить документально.

8.1.2 Нарушение целостности

Рассмотрите, какой ущерб мог бы возникнуть при нарушении целостности определенного ресурса(ов) (преднамеренно или случайно). Например, нарушение целостности может привести к следующему:

– принятию неправильных решений;

– обману;

– прерыванию функций бизнеса;

– утрате общественного доверия или снижению общественного имиджа;

– финансовым потерям;

– ответственности перед законом, включая ответственность за нарушение законодательства в области предохранения данных.

В соответствии с ответами на поставленные выше вопросы следует решить, будет ли общий ущерб от нарушения целостности серьезным, незначительным или вообще не будет никакого ущерба. Это решение следует подтвердить документально.

8.1.3 Нарушение готовности (доступности)

Рассмотрите, какой ущерб мог бы возникнуть при другой, чем кратковременное нарушение готовности применений или доступности информации, т.е. какие функции бизнеса в случае прерывания могли бы иметь результатом неудовлетворенный ответ или время завершения. Следует также рассмотреть чрезмерную форму неготовности к работе, постоянную утерю данных и/или физическое повреждение аппаратных и программных средств. Например, неготовность к работе может привести к следующему:

– принятию неправильных решений;

– неспособности выполнять важные задачи;

– утрате общественного доверия или снижению общественного имиджа;

– финансовым потерям и ответственности перед законом, включая ответственность за нарушение законодательства в области предохранения данных и невыполнения контрактов в предельные сроки;

– значимым расходам на восстановление.

Следует заметить, что ущерб от неготовности к работе может значимо колебаться для разных периодов времени такой неготовности. Желательно рассмотреть все ущербы, которые можно было бы понести в разные периоды времени, и оценить ущерб для каждого периода как серьезный, незначительный или никакой. Эту информацию следует использовать при выборе защитных мер.

В соответствии с ответами на поставленные выше вопросы следует решить, будет ли общий ущерб от неготовности к работе серьезным, незначительным или вообще не будет никакого ущерба. Это решение следует подтвердить документально.

8.1.4 Потеря подотчетности

Рассмотрите, какой ущерб мог бы возникнуть при потере подотчетности пользователей системы или субъектов (например, программного обеспечения), действующих от имени пользователя. В это рассмотрение следует включить автоматически генерируемые сообщения, которые могут быть причиной возникновения действия. Например, потеря подотчетности может привести к следующему:

– манипулированию системой со стороны пользователей;

– обману;

– промышленному шпионажу;

– неконтролируемым действиям;

– ложным обвинениям;

– ответственности перед законом, включая ответственность за нарушение законодательства в области предохранения данных.

В соответствии с ответами на поставленные выше вопросы следует решить, будет ли общий ущерб от потери подотчетности серьезным, незначительным или вообще не будет никакого ущерба. Это решение следует подтвердить документально.

8.1.5 Сомнения в подлинности

Рассмотрите, какой ущерб мог бы возникнуть в случае сомнения в подлинности данных, сообщений, независимо от того, используют ли их люди или системы. Это особенно важно в распределенных системах, где принятые решения распространяются на широкие сообщества или где

используются ссылки на информацию. Сомнения в подлинности могут привести к следующему:

– обману;

– использованию достоверных процессов с недостоверными данными, что ведет к результату, вводящему в заблуждение;

– манипулированию организацией извне;

– промышленному шпионажу;

– ложным обвинениям;

– ответственности перед законом, включая ответственность за нарушение законодательства в области предохранения данных.

В соответствии с ответами на поставленные выше вопросы следует решить, будет ли общий ущерб от сомнения в подлинности серьезным, незначительным или вообще не будет никакого ущерба. Это решение следует подтвердить документально.

8.1.6 Снижение надежности

Рассмотрите, какой ущерб мог бы возникнуть в случае снижения надежности систем. Это также важно в отношении функциональности, которая является вторичной характеристикой надежности. Например, снижение надежности может привести к следующему:

– обману;

– утери доли рынка;

– снижению мотивации в работе персонала;

– ненадежным поставщикам;

– утрате доверия покупателей;

– ответственности перед законом, включая ответственность за нарушение законодательства в области предохранения данных.

В соответствии с ответами на поставленные выше вопросы следует решить, будет ли общий ущерб от снижения надежности серьезным, незначительным или вообще не будет никакого ущерба. Это решение следует подтвердить документально.

8.2 Защитные меры для обеспечения секретности

Типы угроз, которые могли бы подорвать конфиденциальность, перечислены ниже с защитными мерами, чтобы предохранять от предложенных угроз. Даны также ссылки на защитные меры в разделе 6. Если эти меры подходят для выбора защиты, то следует принимать во внимание тип и характеристики системы ИТ.

Следует заметить, что большинство защитных мер, перечисленных в 6.1, обеспечивают более 'общее' предохранение, т.е. направлены на ряд угроз и предоставляют защиту путем поддержки управления общей эффективной

безопасностью информационных технологий. Поэтому нет подробного перечисления защитных мер, но их действие не следует недооценивать, и они должны быть реализованы для общей эффективной защиты. Угрозы следуют в алфавитном порядке.

8.2.1 Подслушивание

Способ получения доступа к секретной информации является подслушиванием, например, путем ответвления линии и прослушивания телефонного разговора. Защитные меры от этой угрозы перечислены ниже.

– **Физическая защита**. Это могут быть комнаты, стены, здания и т.д., которые делают подслушивание невозможным или маловероятным. Другой способ заключается в добавлении шумов. Этот тип предохранения подробно не рассматривается в разделе 8. В случае защиты телефонов соответствующая прокладка кабелей может обеспечивать некоторое предохранение от подслушивания. Здесь этот вопрос не рассматривается, но изложен в *СТ РК ИСО/МЭК 13335-5-2008*.

– **Политика безопасности**. Другой путь избежать подслушивания заключается в установлении строгих правил, определяющих, когда, где и каким образом следует обмениваться секретной информацией.

– **Сохранение конфиденциальности данных**. Еще один путь защиты от подслушивания связан с шифрованием сообщений перед сеансом обмена данными. Более подробно этот вопрос изложен в 6.2.5.

8.2.2 Электромагнитное излучение

Электромагнитное излучение могут использовать взломщики, чтобы получить знание об информации, обрабатываемой в системе ИТ. Защитные меры от электромагнитного излучения перечислены ниже.

– **Физическая защита**. Это может быть наружная обшивка комнат, стен и т.д., которая не позволяет электромагнитному излучению выходить за ее пределы. Этот тип предохранения подробно не рассматривается в 6.1.7 (это не дешевый способ защиты от электромагнитного излучения).

– **Сохранение конфиденциальности данных**. Более подробную информацию см. в 6.2.5. Следует заметить, что эта защита применима к шифрованной информации, но не для информации на этапе обработки, отображения или распечатки.

– **Использование оборудования ИТ с малым уровнем излучения**. Этот вопрос не рассматривается подробно в разделе 6, но можно купить оборудование, имеющее встроенные средства предохранения от электромагнитного излучения.

8.2.3 Вредоносный код

Вредоносный код может привести к утрате конфиденциальности, например, через возможность перехвата и раскрытия паролей. Защитные меры от этой угрозы перечислены ниже.

– **Предохранение от вредоносного кода**. Подробное описание защиты от вредоносного кода см. в 6.2.3.

– **Действия в особых ситуациях**. Своевременный доклад о любой особой ситуации может ограничить ущерб от вредоносных атак. Обнаружение вторжения можно использовать для пресечения попыток проникновения в систему или сеть. Дополнительную информацию по этому вопросу можно найти в 6.1.3.

8.2.4 Сокрытие фактической личности пользователя

Сокрытие фактической личности пользователя может быть использовано для обхода процессов аутентификации и связанных с ним защитных сервисов и функций. В заключение это может привести к проблемам конфиденциальности всякий раз, когда такое сокрытие обеспечивает доступ к секретной информации. Защитные меры от этой угрозы перечислены ниже.

– **И & А.** Сокрытие фактической личности пользователя значительно усложняется, если защитные меры И & А основаны на комбинации того, что известно пользователю, или того, чем он владеет, или присущих только ему характеристиках (см. 6.2.1).

– **Логический контроль доступа и аудит**. Логический контроль доступа не может различать санкционированного пользователя и того, кто проникает под его личностью, но местное применение такого контроля может уменьшить зону несанкционированного доступа (см. 6.2.2). Обзор и анализ контрольных журналов регистрации позволяет обнаруживать несанкционированные действия.

– **Предохранение от вредоносного кода**. Так как один из путей получения паролей связан с внедрением вредоносного кода для перехвата паролей, то следует устанавливать местную защиту от таких программ (см. 6.2.3).

– **Управление сетью**. Другой способ захвата секретного материала является сокрытие фактической личности в трафике, например, в электронной почте. В настоящее время ISO разрабатывает несколько документов, содержащих дополнительную информацию о подробных защитных мерах по обеспечению безопасности сетей.

– **Сохранение конфиденциальности данных**. Если по какой-либо причине упомянутый выше тип защиты невозможен или недостаточен, то

дополнительная защита может быть обеспечена путем хранения секретных данных в зашифрованном виде (см. 6.2.5).

8.2.5 Направление сообщений по ошибочному/измененному маршруту

Ошибочный маршрут – это преднамеренное или случайное направление сообщений по некорректному маршруту, тогда как изменение маршрута может иметь место с хорошей и плохой целью. Изменение маршрута может быть, например, сделано для поддержания непрерывности готовности к работе. Направление сообщений по ошибочному/измененному маршруту может привести к утрате конфиденциальности, если оно допускает несанкционированный доступ к этим сообщениям. Защитные меры от этой угрозы перечислены ниже.

– **Управление сетью.** Защита от направления сообщений по ошибочному/измененному маршруту может быть найдена в других документах ИСО, которые разрабатываются. В них будет содержаться дополнительная информация по обеспечению безопасности сети.

– **Сохранение конфиденциальности данных.** Чтобы не допустить несанкционированный доступ в случае ошибочного или измененного направления сообщений, эти сообщения могут быть зашифрованы. Дополнительную информацию по этому вопросу можно найти в 6.2.5.

8.2.6 Сбой программного обеспечения

Сбои программного обеспечения ставят под угрозу сохранение конфиденциальности, если программное обеспечение обеспечивает, например, контроль доступа или шифрование, или если сбой программного обеспечения создает брешь, например, в операционной системе. Защитные меры для сохранения конфиденциальности в этом случае перечислены ниже.

– **Действия в особых ситуациях**. Каждый, кто замечает неправильное функционирование программного обеспечения, обязан сообщить об этом ответственному лицу с тем, чтобы можно было быстро предпринять соответствующие действия. Дополнительную информацию можно найти в 6.1.3.

– **Операционные вопросы**. Некоторые сбои программного обеспечения можно избежать через его тестирование перед использованием или путем контроля изменений программного обеспечения (см. 6.1.5).

8.2.7 Воровство

Воровство может угрожать сохранению конфиденциальности, если украденный компонент несет секретную информацию, которая может оказаться доступной. Защитные меры против воровства перечислены ниже.

– **Физическая защита**. Это может быть материальное предохранение, затрудняющее доступ в здание, зону или комнату с оборудованием ИТ, или специальные защитные меры от кражи (см. описание в 6.1.7).

– **Управление персоналом**. Защитные меры в части управления персоналом (контролирование постороннего персонала, соглашения о сохранении конфиденциальности и т.д.) следует поддерживать на месте, затрудняя возможность кражи (см. 6.1.4).

– **Сохранение секретности данных**. Такую защиту следует внедрить, если существует вероятность кражи оборудования ИТ, содержащего секретную информацию, например, небольшой портативный компьютер. Подробности см. в 6.2.5.

– **Средства защиты носителей информации**. Любую среду, содержащую секретный материал, следует предохранять от воровства (см. 6.1.5).

8.2.8 Несанкционированный доступ в компьютер, к данным, сервисам и приложениям

Несанкционированный доступ в компьютер, к данным, сервисам и приложениям может быть угрозой, если возможен доступ к любому секретному материалу. Защитные меры для предохранения от несанкционированного доступа включают соответствующее опознавание и проверку регистрации, логический контроль доступа, аудит на уровне системы ИТ и разделение сетей на сетевом уровне.

– **И&А**. Защитные меры путем соответствующего опознавания и проверки регистрации следует использовать в комбинации с контролем логического доступа для предотвращения несанкционированного доступа.

– **Логический контроль доступа и аудит**. Защитные меры, изложенные в 6.2.2, следует использовать для контроля логического доступа через использование механизмов управления доступом. Обзор и анализ контрольных журналов регистрации позволяет обнаруживать несанкционированные виды деятельности людей с правами доступа в систему.

– **Разделение сетей**. Чтобы затруднить несанкционированный доступ, следует применять местное разделение сетей (см. 6.2.4).

– **Физический контроль доступа**. Кроме логического может применяться физический контроль доступа (см. 6.1.7).

– **Средства защиты носителей данных**. Если секретная информация хранится на других носителях (например, дискетах), то следует учредить местный контроль среды для ее защиты от несанкционированного доступа.

– **Сохранение секретности данных**. Если по какой-либо причине защита носителей данных невозможна или недостаточна, то дополнительное

предохранение может быть обеспечено путем хранения секретных данных в зашифрованном виде (см. 6.2.5).

8.2.9 Несанкционированный доступ в среду хранения

Доступ и использование запоминающей среды без соответствующих полномочий угрожают конфиденциальности, если в этой среде хранится секретный материал. Защитные меры сохранения секретности перечислены ниже.

– **Операционные вопросы**. Можно применять средства контроля среды для обеспечения, например, физической защиты и подотчетности за носителями информации, а также гарантированного стирания хранимой информации с тем, чтобы никто не мог воспользоваться секретным материалом из ранее стертой среды (см. 6.1.5). Специальное внимание следует обращать на защиту легко снимаемых носителей информации, например, дискеты, резервные копии на магнитной ленте и бумаге.

– **Физическая безопасность**. Соответствующая защита комнат (прочные стены и окна, а также физический контроль доступа) и безопасная мебель могут предохранять от несанкционированного доступа (см. 6.1.7).

– **Сохранение секретности данных**. Дополнительное предохранение секретного материала в среде хранения может быть достигнуто путем шифрования. Эффективная система управления ключами необходима для безопасного применения криптографии (см. 6.2.5).

8.3 Меры защиты целостности

Типы угроз, которые могут подвергать опасности целостность, перечислены ниже вместе с защитными мерами от этих угроз. Даны также ссылки на меры защиты, изложенные в разделе 6. При выборе защиты следует учитывать тип и характеристики системы ИТ.

Следует заметить, что большинство мер, перечисленных в 6.1, обеспечивают в основном 'общую' защиту, т.е. они направлены против ряда угроз и предохраняют за счет поддержки общего эффективного управления безопасностью ИТ. Здесь эти меры подробно не рассматриваются. Не следует преуменьшать действие таких мер, поэтому они подлежат реализации для общей эффективной защиты. Угрозы целостности рассматриваются в следующем порядке.

8.3.1 Ухудшение среды хранения

Ухудшение среды хранения угрожает целостности того, что в ней хранится. Если целостность является важным свойством среды, то следует применять следующие защитные меры.

– **Средства контроля среды**. Достаточные средства контроля среды включают проверку целостности (см. 6.1.5), которая обнаруживает в запоминающем устройстве испорченные файлы.

– **Резервные копии**. Резервные копии следует делать на все важные файлы, данные бизнеса и т.д. При обнаружении потери целостности, например, через средства контроля среды или во время тестирования резервных копий, следует использовать эти копии или предыдущие записи для восстановления целостности файлов. Подробности о резервных копиях см. в 6.1.6.

– **Предохранение целостности данных**. Криптографические способы могут быть использованы для защиты целостности данных в запоминающем устройстве. Дополнительную информацию см. в 6.2.5.

8.3.2 Ошибка технического обслуживания.

Если техническое обслуживание проводится нерегулярно или с ошибками, то целостность всей затронутой информации находится под угрозой. Меры защиты целостности в этом случае перечислены ниже.

– **Техническое обслуживание**. Правильное техническое обслуживание - это наилучший способ избежать ошибок при осмотре и ремонте (см. 6.1.5). Сюда также входят подтвержденные документально и проверенные методы технического обслуживания и соответствующий надзор за проведением работ.

– **Резервные копии**. Если в процессе технического обслуживания имели место ошибки, то можно использовать резервные копии для восстановления целостности поврежденной информации (см. 6.1.6).

– **Предохранение целостности данных**. Можно использовать средства криптографии для сохранения целостности информации. Дополнительные подробности см. в 6.2.5.

8.3.3 Вредоносный код

Вредоносный код может привести к нарушению целостности, например, в случае, когда в данные или файлы вносит изменения лицо, получившее несанкционированный доступ с помощью вредоносного кода, или такие изменения делает сам код. Защитные меры против вредоносного кода перечислены ниже.

– **Предохранение от вредоносного кода**. Подробное описание защиты от вредоносного кода см. в 6.2.3.

– **Действия в особой ситуации**. Своевременное сообщение о любой необычной ситуации может ограничить ущерб от воздействия вредоносного кода. Средства обнаружения проникновения могут быть использованы, чтобы воспрепятствовать попыткам несанкционированного доступа в систему или сеть. Дополнительную информацию можно найти в 6.1.3.

8.3.4 Сокрытие фактической личности пользователя

Сокрытие фактической личности пользователя может быть использовано, чтобы обойти аутентификацию и все связанные с ней сервисы и функции безопасности, что может привести к нарушению целостности информации, если сокрытие направлено на получение возможности изменения информации. Защитные меры в этой области перечислены ниже.

– **И&А.** Имитация законного пользователя становится более трудной, если защита с помощью И&А основана на комбинациях того, что знает пользователь, чем он владеет, а также на применении характеристик, присущих самому пользователю (см. 6.2.1).

– **Логический контроль доступа и аудит**. Логический контроль доступа не может различать пользователя, имеющего полномочия, и кого-то другого, имитирующего законного пользователя, но местное использование механизмов контроля доступа может уменьшать зону вредоносного воздействия (см. 6.2.2). Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности.

– **Предохранение от вредоносного кода**. Так как одним из путей овладения паролями является внедрение вредоносного кода для перехвата паролей, то на месте должна быть предусмотрена защита от таких вредоносных программ (см. 6.2.3).

– **Управление сетью**. Другой путь несанкционированного доступа связан с сокрытием фактической личности пользователя в трафике, например, электронной почте. В настоящее время ISO разрабатывает несколько документов, содержащих дополнительную информацию по защитным мерам обеспечения безопасности на уровне сети.

– **Сохранение целостности данных**. Если по какой-либо причине упомянутый выше тип защиты невозможен или недостаточен, то дополнительное предохранение данных может быть обеспечено способами криптографии, подобным цифровым подписям (см. 6.2.5).

8.3.5 Направление сообщений по ошибочному/измененному маршруту

Ошибочный маршрут - это преднамеренное или случайное неправильное направление сообщений, тогда как изменение маршрута может иметь место с хорошей и плохой целью. Изменение маршрута может быть, например, сделано для поддержания целостности готовности к работе. Направление сообщений по ошибочному/измененному маршруту может привести к нарушению целостности, например, в случае, когда сообщения изменяются и затем передаются исходному адресату. Защитные меры от этой угрозы перечислены ниже.

– **Управление сетью**. Защита от направления сообщений по ошибочному/измененному маршруту может быть найдена в других документах ISO, которые разрабатываются. В них будет содержаться дополнительная информация по обеспечению безопасности сети.

– **Предохранение целостности данных**. Чтобы не допустить несанкционированных корректировок в случае ошибочного или измененного направления сообщений, можно использовать хэш-функции и цифровые подписи. Дополнительную информацию по этому вопросу можно найти в 6.2.5.

8.3.6 Неотказуемость

Защитные меры по обеспечению неотказуемости следует применять в случае, когда важно иметь доказательство факта отправки и/или получения сообщения, а также факта транспортировки его через сетевую инфраструктуру. Имеются специфические криптографические меры защиты, указанные в 6.2.5, которые служат базисом для обеспечения неотказуемости.

8.3.7 Сбои программного обеспечения

Сбои программного обеспечения могут нарушать целостность данных и информации, которая обрабатывается с помощью этих программ. Защитные меры для предохранения целостности перечислены ниже.

– **Сообщение о сбоях в программном обеспечении**. Быстрое сообщение о сбоях программного обеспечения помогает ограничить возможный ущерб (см. 6.1.3).

– **Операционные вопросы**. Тестирование безопасности может быть использовано для обеспечения правильного функционирования программного обеспечения. Путем контроля изменений программ можно избежать проблем, которые возникают в связи с усовершенствованием или другими корректировками программного обеспечения (см. 6.1.5).

– **Резервные копии**. Резервные копии, например, предыдущего поколения можно использовать для восстановления целостности данных, которые обработаны с помощью программного обеспечения, функционирующего со сбоями (см. 6.1.6).

– **Предохранение целостности данных**. Средства криптографии могут быть использованы для предохранения целостности информации (см. 6.2.5).

8.3.8 Нарушения в снабжении (энергия, кондиционирование)

Нарушения в снабжении могут вызывать проблемы целостности, если эти нарушения являются причиной других неисправностей. Например, перебои в энергоснабжении могут привести к выходу из строя аппаратных средств, техническим неисправностям или проблемам хранения данных. Защитные меры против этих специфических проблем можно найти в

соответствующих подразделах. Меры защиты против нарушений энергоснабжения перечислены ниже.

– Энергия и кондиционирование. При необходимости следует использовать подходящие защитные меры для избежания проблем энергоснабжения и кондиционирования, например, в случае всплеска напряжения (см. 6.1.7).

– Резервные копии. Резервные копии следует использовать для восстановления поврежденной информации (см. 6.1.6).

8.3.9 Техническая неисправность

Технические неисправности, например, в сети могут нарушать целостность любой информации, которая хранится или обрабатывается в сети. Меры защиты в этом случае перечислены ниже.

– **Операционные вопросы**. Управление конфигурацией и изменениями, а также управление пропускной способностью следует использовать, чтобы не допускать неисправностей в системе ИТ или сети (см. 6.1.5).

– **Управление сетью.** Следует использовать операционные процедуры, планирование системы и правильную конфигурацию сети, чтобы свести к минимуму риски от технических неисправностей (см. 6.2.4).

– **Энергия и кондиционирование**. Защитные меры, связанные с подходящим энергоснабжением и кондиционированием, например, защиту от всплесков напряжения, следует использовать в случае, когда необходимо избежать проблем в результате нарушения такого снабжения (см. 6.1.7).

– **Резервные копии**. Резервные копии следует использовать для восстановления поврежденной информации (см. 6.1.6).

8.3.10 Ошибки передачи

Ошибки передачи могут нарушить целостность передаваемой информации. Меры для защиты целостности в этом случае перечислены ниже.

– **Прокладка кабелей**. Планирование и соответствующая прокладка кабелей позволяют исключить ошибки при передаче, если, например, ошибка вызвана перегрузкой (см. 6.1.7).

– **Управление сетью.** Сетевое оборудование следует правильно эксплуатировать и технически обслуживать для избежания ошибок при передаче. В настоящее время ISO разрабатывает несколько документов, содержащих дополнительную информацию о подробностях обеспечения безопасности сети, которая может быть применена для предохранения от ошибок при передаче.

– **Сохранение целостности данных**. Проверочные суммы и циклическое, избыточное кодирование в протоколах связи может быть

использовано для предохранения от случайных ошибок передачи. Средства криптографии можно применять для сохранения целостности передаваемых данных в случае преднамеренного воздействия. Дополнительную информацию см. в 6.2.5.

8.3.11 Несанкционированный доступ в компьютеры, к данным, сервисам и приложениям

Несанкционированный доступ в компьютеры, к данным, сервисам и приложениям может быть угрозой для целостности информации, если возможно несанкционированное изменение. Защитные меры против несанкционированного доступа включают подходящую идентификацию и аутентификацию, логический контроль доступа, аудит на системном уровне ИТ и разделение сетей на сетевом уровне.

– **И & А.** Соответствующие защитные меры с помощью И & А следует использовать в комбинации с логическим контролем доступа для предотвращения несанкционированного проникновения.

– **Логический контроль доступа и аудит.** Меры защиты в 6.2.2 следует использовать для обеспечения логического контроля доступа через соответствующие механизмы. Просмотр и анализ контрольных журналов регистрации позволяет обнаруживать несанкционированную деятельность людей, не имеющих прав доступа в систему.

– **Разделение сетей.** Чтобы затруднить несанкционированный доступ, следует осуществить местное разделение сетей (см. 6.2.4).

– **Физический контроль доступа**. Кроме логического предотвращения незаконного проникновения, эта задача может решаться с помощью физического контроля доступа (см. 6.1.7).

– **Контроль среды**. Если секретные данные хранятся на другом носителе (например, дискете), то следует использовать местные средства контроля среды (6.1.5) для защиты от несанкционированного доступа.

– **Целостность данных**. Средства криптографии можно использовать для предохранения целостности информации в запоминающем устройстве или во время передачи. Дополнительную информацию см. в 6.2.5.

8.3.12 Использование несанкционированных программ и данных

Использование несанкционированных программ и данных создает угрозу информации в запоминающем устройстве и при обработке в системе, где такое случается, если эти программы и данные используются для незаконного изменения информации или содержат вредоносный код (например, игры). Защитные меры в этом случае перечислены ниже.

– **Осведомленность в вопросах безопасности и обучение**. До сознания всех служащих следует довести тот факт, что им запрещается устанавливать и использовать любое программное обеспечение без разрешения

управляющего по вопросам безопасности системы ИТ или лица, отвечающего за безопасность этой системы (см. также 6.1.4).

– **Резервные копии**. Резервные копии следует использовать для восстановления поврежденной информации (см. 6.1.6).

– **И & А.** Соответствующие защитные меры с помощью И & А следует использовать в комбинации с логическим контролем доступа для предотвращения несанкционированного проникновения.

– **Логический контроль доступа и аудит**. Логический контроль доступа, изложенный в 6.2.2, должен гарантировать, что только уполномоченные операторы могут применять программное обеспечение для обработки и изменения информации. Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности.

– **Предохранение от вредоносного кода**. Все программы и данные следует проверять перед использованием на наличие вредоносного кода (см. 6.2.3).

8.3.13 Несанкционированный доступ в среду хранения

Несанкционированный доступ и использование среды хранения информации могут подвергать опасности целостность, так как в этом случае возможно несанкционированное изменение информации, записанной в этой среде. Защитные меры по сохранению целостности перечислены ниже.

– **Операционные вопросы**. Можно применять средства контроля среды, например, для физического предохранения и подотчетности, чтобы не допустить проникновения в эту среду, а также проверку целостности для обнаружения любой компрометации целостности информации, записанной в этой среде (см. 6.1.5). Особое внимание следует уделять защите легко снимаемой среды, например, дискеты, магнитные ленты с записями резервных копий и бумажные носители.

– **Физическая безопасность**. Соответствующая защита комнат (прочные стены и окна, а также физический контроль доступа) и безопасная мебель могут предохранять от несанкционированного доступа (см. 6.1.7).

– **Целостность данных**. Средства криптографии можно использовать для предохранения целостности информации в запоминающем устройстве. Дополнительную информацию см. в 6.2.5.

8.3.14 Ошибка пользователя

Ошибка пользователя может нарушить целостность информации. Защитные меры от этого перечислены ниже.

– **Осведомленность в вопросах безопасности и обучение**. Всех пользователей следует обучать, чтобы они не допускали ошибок при обработке информации (6.1.4). В программу следует включить обучение

определенным методикам для специальных действий, например, порядок действий при операциях или обеспечении безопасности.

– **Резервные копии**. Резервные копии, например, предыдущее поколение, могут быть использованы для восстановления целостности информации, поврежденной в результате ошибок пользователя (см. 6.1.6).

8.4 Меры обеспечения доступности

Типы угроз, направленных на нарушении доступности, перечислены ниже со ссылкой на соответствующие защитные меры из 6 раздела настоящего стандарта. При выборе защитных мер, по необходимости, могут учитываться тип и характеристики системы ИТ.

Большинство мер, перечисленных в п. 6.1, обеспечивают достаточно общий уровень защиты, т.е. они не направлены против конкретных специфических угроз, а обеспечивают защиту от большинства из них путем всеобъемлющего эффективного управления безопасностью ИТ. Эти общие меры защиты в данном разделе подробно не рассматриваются, однако не следует преуменьшать эффективность таких мер - они подлежат реализации для обеспечения общей эффективной защиты.

Требования к доступности могут быть самыми разными: от некритичности к временным задержкам систем ИТ и данных (однако ситуация потери таких данных или недоступности таких систем недопустима), до сильной чувствительности к временным задержкам систем ИТ и данных.

В первом случае доступность может быть обеспечена путем резервирования систем и данных, во втором же не обойтись без системы, устойчивой к внешним воздействиям.

8.4.1 Разрушительное воздействие

Информация может быть уничтожена в результате разрушительного воздействия. Защитные меры от этого перечислены ниже.

– **Дисциплинарный процесс**. Все служащие должны осознавать последствия, если они (преднамеренно или случайно) уничтожат информацию (см. также 6.1.4).

– **Средства контроля среды**. Все носители информации следует соответственно предохранять от несанкционированного доступа, используя физическую защиту и подотчетность для всей сетевой архитектуры (см. 6.1.5).

– **Резервные копии**. Резервные копии следует делать со всех важных файлов, данных бизнеса и т.д. Если файл или любая другая информация недоступны (по какой-либо причине), то для восстановления информации следует использовать резервную копию или предыдущее поколение резервных копий. Дополнительно о резервных копиях см. в 6.1.6.

– **Материальная защита**. Средства контроля физического доступа следует использовать для предотвращения несанкционированного доступа, который мог бы способствовать несанкционированному повреждению оборудования ИТ или информации (см. 6.1.7).

– **И & А.** Соответствующие защитные меры с помощью И & А следует использовать в комбинации с логическим контролем доступа для предотвращения несанкционированного проникновения.

– **Логический контроль доступа и аудит**. Логический контроль доступа, изложенный в 6.2.2, должен гарантировать, что не может иметь место несанкционированный доступ к информации, приводящий к ее уничтожению. Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности.

8.4.2 Ухудшение среды хранения

Ухудшение среды хранения угрожает готовности к функционированию того, что в ней хранится. Если готовность является важным свойством среды, то следует применять следующие защитные меры.

– **Средства контроля среды**. Периодическое тестирование среды хранения позволяет обнаруживать ее ухудшение в лучшем случае до того момента, когда информация действительно является недоступной. Следует обеспечить такие условия хранения среды, чтобы никакое внешнее воздействие не могло бы стать причиной ухудшения ее функционирования (см. 6.1.5).

– **Резервные копии**. Резервные копии следует делать на все важные файлы, данные бизнеса и т.д. Если файл или какая-либо другая информация недоступны (по какой-либо причине), то следует использовать резервную копию или предыдущее поколение резервных копий для восстановления информации. Подробности о резервных копиях см в п. 6.1.6.

8.4.3 Неисправность аппаратуры связи и сбои сервисов

Неисправность аппаратуры и нарушения в работе сервисов связи угрожают готовности информации, передаваемой через эти сервисы. В зависимости от причины неисправности или нарушения сервисов полезно обратить внимание на сбои программного обеспечения (8.4.11), подачи электропитания (10.4.12) или другие технические неисправности (8.4.13). Меры защиты готовности перечислены ниже.

– **Избыточность и резервные копии**. Избыточная реализация компонентов сервисов связи можно применять для снижения вероятности нарушения их работы. В зависимости от максимального допустимого времени вынужденного простоя можно также предусмотреть резервное оборудование, чтобы выполнять требования связи. В любом случае данные конфигурации и расположения следует резервировать для обеспечения

готовности к работе в аварийных условиях. Общую информацию о резервировании можно также найти в 6.1.6.

– **Управление сетью**. В настоящее время ISO разрабатывает несколько документов, содержащих дополнительную информацию о подробностях обеспечения безопасности сети, которая может быть применена для предохранения от сбоев в работе аппаратуры связи и сервисов.

– **Прокладка кабелей**. Тщательное планирование и соответствующая прокладка кабелей позволяют избежать повреждений. В случае подозрения неисправности на линии связи ее следует проверить. (см. также п. 6.1.7).

– **Обеспечение неотказуемости**. Для подтверждения фактов транспортировки сообщения через сетевую инфраструктуру, факта отправки или факта приема сообщения следует использовать сервисы обеспечения неотказуемости (см. 6.2.5). В таком случае могут быть легко обнаружены неисправности связи или пропущенная информация.

8.4.4 Пожар, вода

Огонь и/или вода могут уничтожить информацию и оборудование ИТ. Защитные меры от огня и воды перечислены ниже.

– **Физическая защита**. Все здания и комнаты, содержащие оборудование ИТ или среду хранения важной информации, следует оборудовать соответственно средствами защиты против пожара и проникновения воды (см. 6.1.7).

– **План обеспечения непрерывной работы и восстановления**. Для того, чтобы предохранить бизнес от разрушительного воздействия огня и воды, следует разработать местный план обеспечения непрерывной работы и восстановления, а также обеспечить резервирование всей важной информации (см. 6.1.6).

8.4.5 Ошибка технического обслуживания

Если техническое обслуживание проводится нерегулярно или с ошибками, то готовность всей затронутой информации находится под угрозой. Меры защиты готовности в этом случае перечислены ниже.

– **Техническое обслуживание**. Правильное техническое обслуживание - это наилучший способ избежать ошибок при осмотре и ремонте (см. 6.1.5).

– **Резервные копии**. Если в процессе технического обслуживания имели место ошибки, то можно использовать резервные копии для восстановления готовности утерянной информации (см. 6.1.6).

8.4.6 Вредоносный код

Вредоносный код может быть применен, чтобы обойти аутентификацию и связанные с ней все сервисы и функции безопасности. В результате это может привести к нарушению готовности, например, в случае, когда данные

или файлы уничтожает лицо, получившее несанкционированный доступ с помощью вредоносного кода, или файлы стирает сам код. Защитные меры против вредоносного кода перечислены ниже.

– **Предохранение от вредоносного кода**. Подробное описание защиты от вредоносного кода см. в 6.2.3.

– **Действия в особой ситуации**. Своевременное сообщение о любой необычной ситуации может ограничить ущерб от воздействия вредоносного кода. Средства обнаружения проникновения могут быть использованы, чтобы воспрепятствовать попыткам несанкционированного доступа в систему или сеть. Дополнительную информацию можно найти в 6.1.3.

8.4.7 Сокрытие фактической личности пользователя

Сокрытие фактической личности пользователя может быть использовано для обхода процесса аутентификации и связанных с ним защитных сервисов и функций, что может привести к нарушению доступности информации, если сокрытие направлено на получение возможности удаления или уничтожения информации. Данное направление защиты включает в себя следующие меры:

– **И&А.** Имитация законного пользователя становится более трудной, если защита с помощью И&А основана на комбинациях того, что знает пользователь, чем он владеет, а также на применении характеристик, присущих самому пользователю (см. 6.2.1).

– **Логический контроль доступа и аудит**. Логический контроль доступа не может различать между пользователем, имеющим полномочия, и кем-то другим, имитирующим законного пользователя, но местное использование механизмов контроля доступа может уменьшать зону вредоносного воздействия (см. 6.2.2). Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности.

– **Предохранение от вредоносного кода**. Так как один из путей овладения паролями является внедрение вредоносного кода для перехвата паролей, то на месте должна быть предусмотрена защита от таких вредоносных программ (см. 6.2.3).

– **Управление сетью**. Другой путь несанкционированного доступа связан с сокрытием фактической личности пользователя в трафике, например, электронной почте. В настоящее время ISO разрабатывает несколько документов, содержащих дополнительную информацию по защитным мерам обеспечения безопасности на уровне сети.

– **Резервирование данных.** Копии данных не могут предохранять от подделок под законного пользователя, но снижают воздействие разрушительных событий, связанных с попытками незаконного проникновения (см. 6.1.6).

8.4.8 Направление сообщений по ошибочному/измененному маршруту

Ошибочный маршрут - это преднамеренное или случайное неправильное направление сообщений, тогда как изменение маршрута может иметь место с хорошей и плохой целью. Изменение маршрута может быть, например, сделано для поддержания целостности готовности к работе. Направление сообщений по ошибочному/измененному маршруту ведет к недоступности сообщений. Защитные меры от этой угрозы перечислены ниже.

– **Управление сетью**. Защита от направления сообщений по ошибочному/измененному маршруту может быть найдена в других документах ISO, которые разрабатываются. В них будет содержаться дополнительная информация по обеспечению безопасности сети.

– **Обеспечение неотказуемости**. Для подтверждения фактов транспортировки сообщения через сетевую инфраструктуру, факта отправки или факта приема сообщения следует использовать сервисы обеспечения неотказуемости (см. 6.2.5).

8.4.9 Злоупотребление ресурсами

Злоупотребление ресурсами ведет к недоступности информации или сервисов. Меры защиты против этого перечислены ниже.

– **Управление персоналом**. Все сотрудники компании должны осознавать последствия ненадлежащего использования ресурсов. В случае необходимости следует применять дисциплинарные процессы (6.1.4).

– **Оперативные вопросы**. Следует осуществлять текущий контроль для обнаружения неразрешенных видов деятельности, а также применять разделение обязанностей для сведения к минимуму возможностей злоупотребления привилегиями (см. 6.1.5).

– **И & А.** Соответствующие защитные меры с помощью И & А следует использовать в комбинации с логическим контролем доступа для предотвращения несанкционированного проникновения.

– **Логический контроль доступа и аудит**. Защитные меры, изложенные в 6.2.2, следует использовать для логического контроля доступа к ресурсам через механизмы управления доступом. Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности.

– **Управление сетью.** Подходящую конфигурацию сети и разделение следует применять для уменьшения возможности неправильного использования сетевых ресурсов (см. 6.2.4).

8.4.10 Стихийные бедствия

Для предотвращения потери информации и сервисов по причине стихийных бедствий следует реализовать на месте следующие защитные меры.

– **Предохранение от стихийных бедствий**. Все здания следует предохранять насколько это возможно от стихийных бедствий (см. 6.1.7).

– **План обеспечения непрерывной работы и восстановления**. Следует разработать и испытать местный план обеспечения непрерывной работы и восстановления для каждого здания, а также обеспечить доступность к резервным копиям всей важной информации, сервисам и ресурсам (см. 6.1.6).

8.4.11 Сбои программного обеспечения

Сбои программного обеспечения могут привести к недоступности данных и информации, которая обрабатывается с помощью этих программ. Защитные меры для предохранения доступности перечислены ниже.

– **Сообщение о сбоях в программном обеспечении.** Быстрое сообщение о сбоях программного обеспечения помогает ограничить возможный ущерб (см. 6.1.3).

– **Операционные вопросы**. Тестирование безопасности может быть использовано для обеспечения правильного функционирования программного обеспечения. Путем контроля изменений программ можно избежать проблем, которые возникают в связи с усовершенствованием или другими корректировками программного обеспечения (см. 6.1.5).

– **Резервные копии**. Резервные копии, например, предыдущего поколения можно использовать для восстановления данных, которые обработаны с помощью программного обеспечения, функционирующего со сбоями (см. 6.1.6).

8.4.12 Нарушения в снабжении (энергия, кондиционирование)

Нарушения в снабжении могут вызывать проблемы готовности, если эти нарушения являются причиной других неисправностей. Например, перебои в энергоснабжении могут привести к выходу из строя аппаратных средств, техническим неисправностям или проблемам хранения данных. Защитные меры против этих специфических проблем можно найти в соответствующих подразделах. Меры защиты против нарушений снабжения перечислены ниже.

– **Энергия и кондиционирование**. При необходимости следует использовать подходящие защитные меры для избегания проблем энергоснабжения и кондиционирования, например, в случае всплеска напряжения (см. 8.1.7).

– **Резервные копии**. Следует делать резервные копии всех важных файлов, данных бизнеса и т.д. При потере файла или другой информации по причине сбоев в снабжении следует использовать резервные копии для восстановления информации. Более подробно о резервировании см. 6.1.6.

8.4.13 Технические неисправности

Технические неисправности, например, в сети могут нарушать доступность любой информации, которая хранится или обрабатывается в сети. Меры защиты в этом случае перечислены ниже.

– **Операционные вопросы**. Управление конфигурацией и изменениями, а также управление пропускной способностью следует использовать, чтобы не допускать неисправностей в системе ИТ или сети. Документация и техническое обслуживание применяются для обеспечения безаварийной работы системы (см. 6.1.5).

– **Управление сетью**. Следует использовать операционные процедуры, планирование системы и правильную конфигурацию сети, чтобы свести к минимуму риски от технических неисправностей (см. 6.2.4).

– **План обеспечения непрерывной работы и восстановления**. Чтобы защитить бизнес от губительных воздействий технических неисправностей, следует иметь на месте план обеспечения непрерывной работы и восстановления, а также доступные резервы всей важной информации, сервисов и ресурсов (см. 6.1.6).

8.4.14 Воровство

Воровство может угрожать доступности информации и готовности оборудования ИТ. Защитные меры против воровства перечислены ниже.

– **Физическая защита**. Это может быть материальное предохранение, затрудняющее доступ в здание, зону или комнату с оборудованием ИТ, или специальные защитные меры от кражи (см. описание в 6.1.7).

– **Управление персоналом**. Защитные меры в части управления персоналом (текущий контроль постороннего персонала, соглашения о сохранении конфиденциальности и т.д.) следует поддерживать на месте, затрудняя возможность кражи (см. 6.1.4).

– **Средства контроля носителей информации**. Любую среду, содержащую важный материал, следует предохранять от воровства (см. 6.1.5).

8.4.15 Перегрузка трафика

Перегрузка трафика угрожает доступности информации, передаваемой через предоставляемые сервисы. Меры защиты доступности и готовности перечислены ниже.

– **Избыточность и резервные копии**. Избыточная реализация компонентов сервисов связи можно применять для снижения вероятности перегрузки трафика. В зависимости от максимального допустимого времени вынужденного простоя можно также предусмотреть резервное оборудование, чтобы выполнять требования связи. В любом случае данные конфигурации и расположения следует резервировать для обеспечения готовности в аварийных условиях. Общую информацию о резервировании можно также найти в 6.1.6.

– **Управление сетью.** Следует использовать правильную конфигурацию, менеджмент и администрирование сетей и сервисов связи для избежания перегрузки (см. 6.2.4).

– **Управление сетью**. В настоящее время ISO разрабатывает документы, содержащие дополнительную информацию по защитным мерам обеспечения безопасности на уровне сети, которые могут быть применены для предохранения от перегрузки трафика.

8.4.16 Ошибки передачи

Ошибки передачи могут нарушить готовность передаваемой информации. Меры для защиты готовности перечислены ниже.

– **Прокладка кабелей**. Тщательное планирование и соответствующая прокладка кабелей позволяют исключить ошибки при передаче, если, например, ошибка вызвана перегрузкой (см. 6.1.7).

– **Управление сетью**. Менеджмент сети не может предотвратить ошибки при передаче, но способен распознавать проблемы, возникающие от ошибок передачи и включать тревожную сигнализацию в каждом случае, что позволяет своевременного реагировать на эти проблемы. В настоящее время ISO разрабатывает документы, содержащие дополнительную информацию о подробностях обеспечения безопасности сети, которая может быть применена для предохранения от ошибок при передаче.

8.4.17 Несанкционированный доступ в компьютеры, к данным, сервисам и приложениям

Несанкционированный доступ в компьютеры, к данным, сервисам и приложениям может быть угрозой для готовности информации, если возможно несанкционированное уничтожение этой информации. Защитные меры против несанкционированного доступа включают подходящую идентификацию и аутентификацию, логический контроль доступа, аудит на системном уровне ИТ и разделение сетей на сетевом уровне.

– **И & А.** Соответствующие защитные меры с помощью И & А следует использовать в комбинации с логическим контролем доступа для предотвращения несанкционированного проникновения.

– **Логический контроль доступа и аудит**. Меры защиты в 6.2.2 следует использовать для логического контроля доступа через соответствующие механизмы управления. Просмотр и анализ контрольных журналов регистрации позволяет обнаруживать несанкционированную деятельность людей, не имеющих прав доступа в систему.

– **Разделение сетей.** Чтобы затруднить несанкционированный доступ, следует осуществить местное разделение сетей (см. п. 6.2.4).

– **Физический контроль доступа**. Кроме логического предотвращения незаконного проникновения, эта задача может решаться с помощью физического контроля доступа (см. 6.1.7).

– **Контроль среды**. Если секретные данные хранятся на другом носителе (например, дискете), то следует использовать местные средства контроля среды (6.1.5) для защиты от несанкционированного доступа.

8.4.18 Использование несанкционированных программ и данных

Использование несанкционированных программ и данных создает угрозу готовности и доступности информации в запоминающем устройстве и при обработке в системе, в которой такое случается, если программы и данные используются для уничтожения информации или если они содержат вредосносный код (например, игры). Защитные меры в этом случае перечислены ниже.

– **Осведомленность в вопросах безопасности и обучение.** До сознания всех служащих следует довести тот факт, что им запрещается устанавливать и использовать любое программное обеспечение без разрешения управляющего по вопросам безопасности системы ИТ или лица, отвечающего за безопасность этой системы (см. также 6.1.4).

– **Резервные копии**. Резервные копии следует использовать для восстановления поврежденной информации (см. 6.1.6).

– **И & А.** Соответствующие защитные меры с помощью И & А следует использовать в комбинации с логическим контролем доступа для предотвращения несанкционированного проникновения.

– **Логический контроль доступа и аудит**. Логический контроль доступа, изложенный в 6.2.2, должен гарантировать, что только уполномоченные операторы могут применять программное обеспечение для обработки и удаления информации. Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности.

– **Предохранение от вредоносного кода**. Все программы и данные следует проверять перед использованием на присутствие вредоносного кода (см. 6.2.3).

8.4.19 Несанкционированный доступ в среду хранения

Несанкционированные доступ и использование среды хранения информации могут подвергать опасности ее готовность, так как в этом случае возможно несанкционированное уничтожение информации, записанной в этой среде. Защитные меры по сохранению готовности перечислены ниже.

– **Операционные вопросы**. Можно применять средства контроля носителей информации, например, для физического предохранения и подотчетности среды, чтобы не допустить несанкционированного доступа к информации, записанной в этой среде (см. 6.1.5). Особое внимание следует уделять защите легко снимаемой среды, например, дискеты, магнитные ленты с записями резервных копий и бумажные носители.

– **Физическая безопасность**. Соответствующая защита комнат (прочные стены и окна, а также физический контроль доступа) и безопасная мебель могут предохранять от несанкционированного доступа (см. 6.1.7).

8.4.20 Ошибка пользователя

Ошибка пользователя может нарушить доступность информации. Защитные меры от этого перечислены ниже.

– **Осведомленность в вопросах безопасности и обучение**. Всех пользователей следует обучать, чтобы они не допускали ошибок при обработке информации (6.1.4). В программу следует включить обучение определенным методикам для специальных действий, например, порядок действий при операциях или обеспечении безопасности.

– **Резервные копии**. Резервные копии, например, предыдущее поколение, могут быть использованы для восстановления информации, поврежденной в результате ошибок пользователя (см. 6.1.6).

8.5 Защитные меры для подотчетности, подлинности и надежности

Область применения подотчетности, подлинности и надежности широко различается в разных доменах. Эти различия подразумевают, что может применяться множество разных защитных мер. Поэтому могут быть даны только общие указания.

Защитные меры, перечисленные в 6.1, предоставляют 'общее предохранение', т.е. они направлены на ряд угроз и обеспечивают защиту путем поддержки общего эффективного управления безопасностью ИТ. Здесь они не перечислены, но их влияние не следует преуменьшать, и они подлежат реализации для обеспечения общей эффективной защиты.

8.5.1 Подотчетность

При защите подотчетности следует учитывать любую угрозу, которая может привести к выполнению действий, не свойственных специфической сущности или субъекту. Некоторые примеры таких угроз даны ниже:

– коллективное пользование учетными записями;

– отсутствие возможности оперативного контроля действий;

– имитация под законного пользователя;

– сбой программного обеспечения;

– несанкционированный доступ в компьютер, к данным, сервисам и приложениям;

– недостатки механизма аутентификации сущностей.

Имеются два типа подотчетности, которые следует принимать во внимание. Один тип имеет дело с идентификацией пользователя, подотчетного за определенные действия с информацией и системами ИТ. Контрольные журналы регистрации предоставляют такую подотчетность. Другой тип касается подотчетности между пользователями в системе. Сервисы обеспечения неотказуемости, разделение сведений между пользователями или спаренное управление могут обеспечить второй тип подотчетности.

Многие защитные меры могут быть использованы и способны внести свой вклад в усиление подотчетности. Могут быть применены защитные меры, начиная от политики безопасности, логического контроля доступа и аудита и кончая внедрением одноразовых паролей и средств управления носителями информации. Реализация политики в области владения информацией является предпосылкой для подотчетности. Выбор специальных мер защиты будет зависеть от специфики использования подотчетности в пределах домена.

8.5.2 Подлинность

Доверие к подлинности может быть уменьшено любой угрозой, которая заставляет человека, систему или процесс усомниться в том, что объект является тем, что он представляет. Некоторые примеры возникновения такой ситуации связаны с отсутствием контроля за изменением данных, отсутствием проверки происхождения (источника) данных, отсутствием регистрации источника данных.

Многие защитные меры могут быть использованы и способны внести свой вклад в увеличение гарантий подлинности. Могут быть применены защитные меры, начиная от использования отмеченных справочных данных, логического контроля доступа и аудита и до цифровых подписей. Выбор специальных мер защиты будет зависеть от специфики использования аутентичности в пределах домена.

8.5.3 Надежность

Любая угроза, которая может привести к непоследовательному поведению систем или процессов, будет иметь результатом снижение надежности. Примерами таких угроз являются нелогичное функционирование системы и ненадежные поставщики. Снижение надежности дает в итоге плохое обслуживание покупателей и потерю их доверия.

Многие защитные меры могут быть использованы и способны внести свой вклад в усиление надежности. Могут быть применены защитные меры, начиная от планов обеспечения непрерывной работы и восстановления, внедрения избыточности в физическую архитектуру и техническое обслуживание системы и до идентификации, аутентификации, логического контроля доступа и аудита. Выбор специальных мер защиты будет зависеть от специфики использования надежности в пределах домена.

9 Выбор защитных мер согласно подробным оценкам

Выбор защитных мер согласно подробным оценкам следует тем же принципам, которые применялись в предыдущих разделах. Проведение детального анализа рисков позволяет учесть специальные требования и обстоятельства систем ИТ и их ресурсы. Разница от предыдущих разделов заключается в уровне усилий и подробностей, собранных во время процесса оценивания. Поэтому возможно квалифицированное обоснование выбранных защитных мер. В 9.1 рассматривается, как стандарт *СТ РК ИСО/МЭК 13335-3-2008*, определяющий метод анализа рисков, может быть применен в процессе выбора защитных мер в настоящей части этого стандарта. Принципы выбора рассмотрены в 9.2.

9.1 Взаимосвязь между частями 3 и 4 *СТ РК ИСО/МЭК 13335*

В *СТ РК ИСО/МЭК 13335-3-2008* описаны методы управления безопасностью информационных технологий. Кроме всего прочего, в данной части рассматриваются различные варианты стратегии анализа риска и предлагается рекомендуемый подход к проведению анализа риска. Основными вариантами стратегии являются следующие:

– использование базисного подхода для всех систем ИТ;

– использование детального анализа рисков для всех систем ИТ;

– использование 'рекомендованного подхода'.

После анализа рисков высокого уровня для всех систем ИТ рассматривается базисный подход к системам ИТ при низком уровне риска и детальный анализ рисков для систем ИТ при высоком уровне риска.

Если решено использовать анализ рисков в деталях для всех систем ИТ, чтобы выявить защитные меры, то в п. 9.2 настоящего стандарта дается

информация о том, как выбирать защиту и как эффективно использовать результаты подробного анализа рисков. Тем не менее, все же следует использовать информацию о защитных мерах, в том числе для специальных систем ИТ, и связь между заботами о безопасности, угрозами и защитными мерами в разделах 6 - 8 настоящего стандарта.

9.2 Принципы выбора

В основном имеются четыре аспекта, которые могут касаться защитных мер, т.е. воздействия, угрозы, уязвимость и сами риски. Риск сам по себе рассматривается при решении скорее снизить или избежать, чем принять риски (примером снижения риска является получение страхового полиса, а примером избежания риска - перевод секретной информации в другой компьютер). Компоненты, которые все вместе создают риски, т.е. воздействия, угрозы, уязвимые места, являются главной целью защитных мер. Пути, по которым защитные меры могут бороться против этих аспектов, следующие:

– **угрозы** - защитные меры могут снижать вероятность возникновения угрозы (например, рассмотрение угрозы потери данных вследствие ошибок пользователя, затем курс обучения пользователей могут снизить количество этих ошибок) или в случае спланированного воздействия сдерживать угрозу путем увеличения технической сложности, которую надо преодолеть для достижения успешной атаки;

– **уязвимость** - защитные меры могут снять уязвимость или сделать ее менее серьезной (например, внутренняя сеть, подсоединенная к внешней сети, уязвима для несанкционированного доступа, однако, реализация подходящей межсетевой защиты делает это соединение более надежным, а разъединение снимает эту уязвимость);

– **воздействие** - защитные меры могут снизить воздействие или помочь его избежать. Например, если вредоносное воздействие - это недоступность информации, то она снижается путем создания копий, которые хранятся в безопасном месте, а также разработки плана обеспечения непрерывной работы и восстановления, готового для введения в действие. Если имеются записи аудита, то анализ и средства предупреждения могут обеспечить раннее обнаружение особой ситуации и снизить вредоносное воздействие на бизнес.

От того, как и где используется защитная мера, во многом зависят те выгоды, которые получают от ее реализации. Очень часто, угрозы могут возникать по причине более чем одного слабого места в системе. Поэтому, если применяется защитная мера, которая предотвращает одну угрозу, несколько слабых мест могут потребовать защиту одновременно. Обратное утверждение тоже верно - мера защиты, предохраняющая одно слабое место, может быть принята против нескольких угроз. Эти выгоды следует

учитывать, когда это возможно, при выборе защитных мер. Эти дополнительные выгоды следует всегда подтверждать документально, чтобы иметь полную картину требований безопасности, которым удовлетворяют защитные меры.

В общем, защитные меры могут предоставить один из следующих типов защиты: предохранение, сдерживание, обнаружение, снижение, восстановление, корректировку, мониторинг и осведомление. Какой из этих атрибутов наиболее предпочтителен, зависит от специфики обстоятельств и того, что каждая мера защиты должна обеспечить. Во многих случаях защитные меры могут предоставить несколько типов защиты, что снова дает дополнительные выгоды. По возможности, защитные меры, предоставляющие многочисленные выгоды, следует искать в первую очередь.

Безопасность следует всегда удерживать в разумном равновесии при обращении к воздействиям, упомянутым выше. Если слишком много внимания уделяется одному типу защиты, то маловероятно, что общий уровень безопасности будет эффективным. Например, если используется большинство сдерживающих мер защиты без адекватных мер обнаружения на месте, чтобы определять, когда сдерживание уже не работает, то общая безопасность не будет эффективной.

Предложенные защитные меры необходимо до реализации сравнить с существующим обеспечением безопасности для оценки, какие меры могут быть расширены или усовершенствованы. В любом случае это будет дешевле, чем внедрять новую защиту.

Во время выбора защитных мер важно взвесить расходы по реализации защиты против стоимости того, что будет предохраняться, и оценить возврат вложений в показателях снижения рисков. Расходы на реализацию и техническое обслуживание могут быть выше стоимость самой защиты, следовательно, это следует учитывать при выборе защитных мер.

Технические ограничения, например, требования к функционированию, управляемость (требования к операционной поддержке) и вопросы совместимости могут затруднять использование некоторых защитных мер. В этих случаях управляющие по системам и безопасности должны работать вместе для определения оптимальных решений. Если защитные меры снижают функционирование, то снова управляющие по системам и безопасности должны находить решение, обеспечивающее необходимую работу системы при гарантированном достаточном уровне безопасности.

Такие аспекты, как, например, законодательство по обеспечению секретности и правоведение, могут требовать реализацию некоторых защитных мер не месте, следовательно, определяя неизменные элементы использованного или идентифицированного базиса.

10 Разработка базиса в масштабе всей организации

Когда организация решает применить базисную безопасность ко всей организации или к ее части, то следует рассмотреть следующие вопросы:

– Какие части организации или систем могут предохраняться на одном и том же базисе, какие требуют разного рассмотрения или следует ли применить один и тот же базис в масштабе всей организации?

– На какой уровень обеспечения безопасности следует нацеливать базис (или разные базисы)?

– Как могут быть определены защитные меры, образующие разные (при необходимости) базисы?

На рисунке 4 показаны разные пути применения базисной защиты.

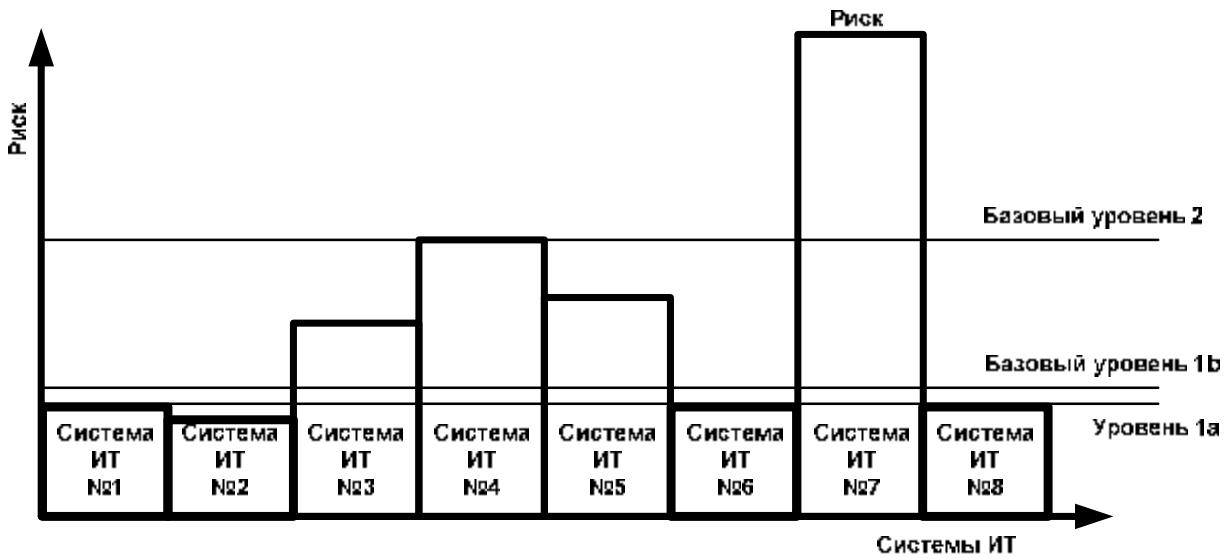

Рисунок 4. Разные базовые уровни

Преимущество применения разных уровней базиса в пределах организации заключается в том, что большинство систем будут соответственно защищены, т.е. им будет обеспечен не слишком низкий и не слишком высокий уровень безопасности. (Как на рисунке 4 для систем ИТ 1, 2, 6 и 8 с уровнем базиса 1 и для систем 3, 4 и 5 с уровнем базиса 2). Если системы ИТ с различными требованиями безопасности являются 'действительно разными' (в том смысле, что большинство требуемых защитных мер для каждой системы ИТ являются разными), тогда применение разных базисов рекомендуется для этой организации. Если имеются принципиально разные требования обеспечения безопасности, то решение о применении базисного подхода следует пересмотреть.

Если с другой стороны единственным различием между разными базовыми уровнями являются необходимость в некоторых дополнительных

защитных мерах, чтобы образовать более высокие базовые уровни, тогда, может быть, не стоит внедрять несколько разных базовых уровней. Если реализуется только один базовый уровень, то непроизводительные издержки организации могут быть значимо снижены, тогда каждый в пределах организации может полагаться на один и тот же имеющийся уровень обеспечения безопасности.

Безопасность на базовом уровне, к которой следует стремиться, соотносится с решением, можно ли логически реализовать один или больше уровней базовой безопасности. Если выбираются разные базовые уровни, то они должны быть точно установлены в соответствии с требованиями безопасности системы ИТ, которую предполагается предохранять. Обычно любой базовый уровень не следует предусматривать для удовлетворения требований систем ИТ к безопасности самого низкого уровня (подобно требованиям системы ИТ №2 на Рисунке 4). Благоразумно стремиться к уровню, который является достаточным для большинства (базовый уровень 1a на Рис. 4) или всех (базовый уровень 1b) систем ИТ, которые предполагается предохранять. Зачастую целесообразно стремиться к наивысшему уровню обеспечения безопасности систем ИТ с помощью базисных защитных мер, так как обычно это не очень дорого, но обеспечивается достаточная безопасность для всех рассматриваемых систем ИТ. Необходим тщательный анализ рассматриваемых систем ИТ, чтобы принять окончательное решение, какие системы ИТ следует предохранять на одном и том же базисном уровне. Некоторые системы ИТ во многом схожи по характеристикам и/или требованиям обеспечения безопасности. В этом случае их следует предохранять на одном и том же базовом уровне. Если с другой стороны несколько систем полностью различаются по своим требованиям к обеспечению безопасности, то довольно часто самым легким способом удовлетворения их требований является раздельное рассмотрение каждой системы.

То же самое справедливо, если решено внедрить базовый уровень обеспечения безопасности в масштабе все организации. Эта базовая безопасность может стремиться к реализации трех разных уровней обеспечения безопасности:

– низкий уровень с добавлением специальных защитных мер, чтобы предохранять все системы ИТ с более высокими требованиями;

– средний уровень с добавлением специальных защитных мер, чтобы предохранять все системы ИТ с более высокими требованиями;

– высокий уровень, достаточный для предохранения всех систем ИТ, подлежащих защите с помощью базисного обеспечения безопасности.

Как уже объяснялось выше, средний или высокий уровень базисного обеспечения безопасности может быть целесообразным для многих организаций, чтобы обеспечить им достаточную защиту, надежную

безопасность по всей организации и снижение непроизводительных расходов. Окончательное решение должно быть принято согласно корпоративной политике безопасности и требованиям к обеспечению безопасности рассматриваемых систем ИТ.

11 Резюме

В настоящем стандарте рассмотрены разные пути выбора защитных мер, которые могут быть использованы для достижения базовой защиты или поддержки технических приемов, изложенных в *СТ РК ИСО/МЭК 13335-3-2008*. Настоящий стандарт содержит также обзор общепринятых защитных мер, которые могут быть выбраны, следуя любому из упомянутых выше подходов. Здесь имеются ссылки на разные руководства по базисной защите, которые содержат более подробное описание защитных мер. В настоящем стандарте дано описание разных путей разработки базисной безопасности в масштабе всей организации, преимущества и недостатки альтернатив. Этот стандарт может использовать любая организация малого и крупного бизнеса, которая желает выбрать защитные меры для предохранения своих систем информационных технологий.

Приложение А
(справочное)
Нормы и правила управления защитой информации

(Тип: общий)

Область применения

Стандарты [1], [2] опубликованы под руководством Совета по стандартам Британского института стандартов. [1] заменяет версию 1995г., которая в настоящее время изъята из пользования. Стандарт BS 7799 предназначается для директоров, менеджеров и служащих, отвечающих за инициирование, реализацию и поддержание информационной безопасности в своих организациях. Его можно рассматривать в качестве базиса для разработки стандартов обеспечения безопасности в организациях.

Стандарты [1], [2] подготовлены под руководством комитета BDD/2 (управление защитой информации) в составе BSI/DISC. Эти новые версии учитывают последние разработки в области применения технологии обработки информации, особенно в сетях и средствах связи. В них также уделено внимание вовлечению и ответственности бизнеса за обеспечение безопасности информации. В процессе ревизии учитывается вклад организаций разных стран мира.

Эти документы предоставляют полный набор средств управления, заключающих в себе наилучший практический опыт в информационной безопасности в полном объеме, насколько это возможно. Они призваны служить в качестве исходной точки для выявления диапазона средств управления, необходимых для большинства ситуаций, когда информационные системы используются в промышленности и торговле, и, следовательно, могут быть применены в больших, средних и малых организациях.

Содержание [1]

8.3 Предохранение от вредоносного кода
8.4 Служебные действия
8.5 Управление сетью
8.6 Обращение с носителями информации и безопасность
8.7 Обмен данными и программным обеспечением
9. Контроль доступа
9.1 Требования бизнеса для систем доступа
9.2 Управление доступом пользователей
9.3 Ответственности пользователей
9.4 Контроль доступа в сеть
9.5 Контроль доступа в компьютер
9.6 Контроль доступа к применению
9.7 Мониторинг доступа к системным ресурсам и их использования
9.8 Мобильная обработка данных и удаленная работа
10. Разработка системы и техническое обслуживание
10.1 Требования системы к обеспечению безопасности
10.2 Безопасность в прикладных системах
10.3 Криптографические средства контроля
10.4 Безопасность в условиях разработки и поддержки
11. Управление непрерывной работой и восстановлением
11.1 Аспекты управления непрерывной работой и восстановлением
12 Соответствие
12.1 Соответствие с законными требованиями
12.2 Обзор политики безопасности и технического соответствия
12.3 Соглашения по аудиту системы

Контактная информация

BSI
389 Chiswick High Road
London, W4 4AL
UK
Тел. +44 181 996 7000
Факс. +44 181 996 7001

BS 7799 опубликован также в Австралии и Новой Зеландии как *AS/NZS 4444*. Контактная информация:

SAA
P.O.Box 1055
AUS Strathfield NSW 2135
Australia
Тел. +61 297 464700
Факс. +61 297 464766

BS 7799 опубликован также в Швеции как *SS 62 77 99*. Контактная информация:

STG
S-11289 Stockholm
SWEDEN
Тел. +46 8136250
Факс. +46 86186128

Приложение Б
(справочное)
Стандарт ETSI по базовой безопасности. Свойства и механизмы

(Тип: специальное применение в информационных технологиях)

Область применения

В [3] перечислены все свойства и механизмы, которые проанализированы и могут применяться в стандартах ETSI. Однако в приложении к документу просто даны руководящие указания по выбору и применению специальных механизмов безопасности. Если нужны специальные рекомендации, то для этого даны соответствующие ссылки на источники информации. Более того, эксперты ETSI STAG готовы помочь в случае вопросов и проблем. Во многих случаях механизмы безопасности не являются официально стандартизованными, но зарегистрированы для использования. Многие механизмы не опубликованы по причине безопасности, но они могут быть использованы в специфических применениях ETSI. В связи со значительной активностью в сферах телекоммуникаций и криптографии, данный документ подлежит регулярному пересмотру и корректировке.

Содержание

Контактная информация

ETSI Secretariat

06921 Sophia Antipolis Cedex

France

Тел. +33 9294 4200

Факс. +33 9365 4716

Приложение В
(справочное)
Руководство по базовой защите ИТ

(Тип: специально для систем ИТ)

Область применения

Цель - базисная защита ИТ через соответствующее применение организационных, инфраструктурных и технических защитных мер, а также защитных мер в части управления персоналом. Базовая защита должна обеспечить стандартную безопасность систем ИТ, которая является адекватной и достаточной для требований защиты среднего уровня и может служить в качестве базиса для применений в ИТ, требующих более высокую степень защиты.

С этой целью [4] рекомендует пакет контрмер для типичных конфигураций ИТ, условий окружения и организационных построений. При подготовке этого руководства орган по безопасности информации Германии принял расчетные оценки рисков на основе известных угроз и слабых мест и разработал пакет мер, подходящих для этой цели. Соответственно, пользователям руководства по базисной защите ИТ не придется снова делать такие анализы, касающиеся базовой защиты ИТ. Они должны только позаботиться о том, чтобы рекомендованные защитные меры были последовательно и полностью реализованы.

В то же время [4] помогает обеспечить безопасность ИТ в том, что касается выполнения требований к защите на среднем уровне экономически выгодным способом, так как политика безопасности индивидуальных систем ИТ может ссылаться на это руководство. Таким образом, базовая защита ИТ становится общепринятой основой соглашения по защитным мерам, чтобы удовлетворять требования к защите на среднем уровне.

Содержание

4.3.4 Комната технической инфраструктуры
5. Системы, не входящие в сеть
5.1 Дисковая операционная система DOS PC (однопользовательская)
5.2 Системы UNIX
5.3 Портативный носимый компьютер
5.4 Дисковая операционная система DOS PC (многопользовательская)
5.5 ПК Windows NT
5.6 ПК Windows 95
5.7 Общая система, не входящая в сеть
6. Сетевые системы
6.1 Сеть ПК на основе серверов
6.2 Сеть UNIX
6.3 Архитектура сети равноправных ЭВМ на базе Windows для рабочих групп
6.4 Сеть на основе Windows NT
6.5 Семейство операционных систем Novel Netware 3.x
6.6 Семейство операционных систем Novel Netware 4.x
6.7 Гетерогенные сети
6.8 Управление сетью и системами
7. Системы передачи данных
7.1 Обмен между средами хранения
7.2 Модем
7.3 Межсетевая защита
7.4 Электронная почта
7.5 Веб-сервер
8. Электросвязь
8.1 Система электросвязи
8.2 Факсимильные аппараты
8.3 Автоответчики
8.4 Аппаратура дистанционного действия
9. Другие компоненты ИТ
9.1 Стандартное программное обеспечение
9.2 Системы управления базами данных.
9.3 Системы удаленной работы.
Каталоги защитных мер
Каталоги угроз
Каталоги таблиц сопоставления угроз и защитных мер

Комитет по стандартам

DIN
Burggrafenstrasse 6
10787 Berlin
Germany
Тел. +49 30 2601 2652
Факс. +49 30 2601 1723

Контактная информация

BSI
Postfach 20 03 63
53133 Bonn
Germany
Тел. +49 228 9582 0, Факс. +49 228 9582 400

Приложение Г
(справочное)
Справочник NIST по компьютерной безопасности

(Тип: общий)

Область применения

Справочник [5] обеспечивает защиту компьютеризованных ресурсов, включая аппаратуру, программное обеспечение и информацию. В нем разъясняются важные концепции, вопросы стоимости и взаимоотношения средств контроля безопасности. Здесь показаны выгоды средств контроля безопасности, основные технологии или подходы для каждого контроля и важные связанные между собой суждения.

Справочник [5] дает широкий обзор компьютерной безопасности, чтобы читатель мог понять свои нужды в этой области и разработать правильный подход к выбору подходящих средств контроля безопасности. В нем нет подробного описания этапов, необходимых для реализации программы обеспечения компьютерной безопасности. Справочник предоставляет подробные методики внедрения средств контроля или дает руководящее указание по аудиту безопасности специальных систем. В конце каждой главы справочника даны общие ссылки. Способы получения книг и статей показаны в конце каждой главы в частях II, III и IV.

Целью справочника [5] не является спецификация требований. В нем скорее рассматриваются выгоды разных средств контроля компьютерной безопасности и ситуации, в которых их применение может быть пригодным. Некоторые требования для федеральных систем отмечены по тексту. Настоящий документ дает советы и руководящие указания, в нем не обусловлены какие-либо меры наказания.

Содержание

Комитет по стандартам
ANSI
11 West 42nd Street
13th floor
USA - New York, N.Y. 10036
USA
Тел. +1 212 642 4900
Факс. +1 212 840 2298
Контактная информация
Лаборатория компьютерных систем
NIST
Gaithersburg
MD 20899-0001

Приложение Д
(справочное)
Медицинская информация: Категории безопасности и защита информационных систем здравоохранения

(Тип: специальное применение ИТ)

Область применения

Настоящий европейский предварительный стандарт [6] задает метод присвоения категорий автоматическим информационным системам здравоохранения. Принятые защитные меры означают предохранение до приемлемого уровня доступности данных, секретности и целостности. Предоставляется категория для каждой системы, заданная соответствующим пакетом защитных требований, которая являются подходящей для уровня рисков, присущих в этой категории.

Настоящий европейский предварительный стандарт [6] применяется ко всем автоматическим информационным системам, которые обрабатывают данные здравоохранения. Сюда входят системы, которые вносят непосредственный вклад в заботу о пациентах, например, результаты анализов лабораторий. Но он также включает статистические и административные системы, которые обеспечивают оперативную поддержку для самого учреждения здравоохранения, например, платежные ведомости штата, персонал, системы планирования и финансовой поддержки. Однако системы, для которых важна конфиденциальность, т.е. информация в общественном домене, не рассматриваются в настоящем европейском предварительном стандарте. Публика, на которую направлен этот стандарт, состоит из потребителей/покупателей надежных информационных систем в здравоохранении или разработчиков/производителей таких систем. Внедрение терминов этого стандарта считается ответственной реакцией менеджмента на обязательства по национальным и европейским законам, а также общественное ожидание высокого стандарта безопасности информации в области здравоохранения.

Содержание

Контактная информация

CEN TC 251,
Rue de Stassart 36,
1050 Brussels,
Belgium

Приложение Е
(справочное)
Банковские и сопутствующие финансовые сервисы. Руководящие указания технического комитета ИСО №68 по защите информации

(Тип: специальное применение ИТ)

Область применения

Финансовые учреждения все больше полагаются на информационные технологии для успешного ведения бизнеса. Управление риском является центральным звеном в секторе финансовых сервисов. Финансовые учреждения управляют риском через расчетливую практику бизнеса, внимательное заключение контрактов, страхование и использование механизмов безопасности.

Есть потребность управления безопасностью информации в пределах финансовых учреждений в полном объеме. Настоящий технический отчет [7] не предназначен давать характерное решение для всех ситуаций. Каждый случай должен быть исследован по своим собственным меркам за и против, чтобы затем выбрать подходящие действия. Настоящий технический отчет [7] предоставляет указания, но не решения.

Задачи настоящего технического отчета [7]:

– представить структуру программы безопасности информации,

– представить руководство по выбору средств контроля безопасности, которые показывают приемлемую практику ведения бизнеса,

– не противоречить существующим стандартам, а также новым разработкам объективных и общепринятых критериев безопасности.

Настоящий технический отчет [7] предназначается для использования финансовыми учреждениями всех размеров и типов, которые желают применить экономную и коммерчески целесообразную программу обеспечения безопасности информации. Он также полезен для тех, кто предоставляет сервисы финансовым учреждениям. Технический отчет [7] может также служить в качестве первоисточника для преподавателей и издателей, обслуживающих финансовую деятельность.

Содержание

Контактная информация
Секретариат ISO/TC68/SC2
Post Office Box 11
Annapolis Junction
MD 20701
USA
Тел. +1 301 688 3586
Факс. +1 301 192 1019

Приложение Ж
(справочное)
Защита секретной информации, не охваченной законами. Рекомендации для АРМ

(Тип: общий)

Область применения

Настоящий документ [8] рекомендует все меры, подлежащие внедрению официальными лицами организации для того, чтобы обеспечить предохранение секретной информации, не охваченной подзаконными актами по секретности, и которая обрабатывается, находится в обращении или хранится с помощью компьютерных средств. Эти рекомендации касаются в частности следующего:

– программного обеспечения, которое является дорогостоящим или воровство, ухудшение или раскрытие которого может поставить организацию в затруднительное положение,

– ограниченного обращения или специфической конфиденциальной информации, которая при условии взятого обязательства профессиональной секретности, не должна разглашаться. Для информации более высокого уровня секретности, т.е. специальной информации, организации должны предусмотреть усиленные меры безопасности, рекомендованные в настоящем документе.

Организации должны составлять свои внутренние инструкции на основе этих рекомендаций.

Содержание

Контактная информация

AFNOR
Tour Europe
92049 Paris La Defense Cedex
France
Тел. : +33 1 4291 5555
Факс.: +33 1 4291 5656

Приложение И
(справочное)
Канадский справочник по безопасности информационных технологий

(Тип: общий)

Область применения

Настоящий справочник [9] помогает обеспечивать безопасность компьютеризованных ресурсов (включая аппаратные и программные средства) путем разъяснения важных концепций, вопросов стоимости и взаимодействия средств контроля. Он иллюстрирует выгоды средств контроля безопасности, основные технологии или подходы для каждого контроля и важные рассуждения.

Справочник [9] дает широкий обзор компьютерной безопасности, чтобы читатели понимали потребности в компьютерной безопасности и разрабатывали правильный подход к выбору подходящих средств контроля. В нем нет описания подробных шагов, необходимых для реализации программ компьютерной безопасности, но предоставлены подробные методики внедрения средств контроля или дано руководящее указание по аудиту безопасности специальных систем. В конце каждой главы приведены общие ссылки, а в конце каждой главы частей II, III и IV даны указания, как получить соответствующие книги и статьи.

Целью настоящего справочника [9] не является спецификация требований. В нем скорее обсуждаются выгоды, предоставляемые разными средствами обеспечения безопасности компьютеров, и ситуации, в которых применение этих средств может быть подходящим. Некоторые требования для федеральных систем отмечены по тексту. Настоящий документ [9] дает советы и указания, в нем не обусловлены какие-либо меры наказания.

Содержание

Комитет по стандартам
SCC
45 O'Connor Street,
Suite 1200,
Ottawa, Ontario K1P 6N7
Canada.
Тел. +1 613 238 3222
Факс: +1 613 995 4564

Контактная информация
Учреждение по обеспечению безопасности связи
P.O. Box 9703, Terminal
Ottawa, Ontario KIG 3Z4
Canada

Приложение
(справочное)
Библиография

[1] BS 7799-1:1999 Нормы и правила для управления защитой информации.

[2] BS 7799-2:1999 Спецификация для систем управления защитой информации.

[3] Стандарт ETSI по базовой безопасности. Свойства и механизмы.

[4] Руководство по базовой защите ИТ.

[5] Справочник NIST по компьютерной безопасности.

[6] Медицинская информация: категории безопасности и защита информационных систем здравоохранения.

[7] Банковские и сопутствующие финансовые сервисы. Руководящие указания технического комитета ИСО №68 по защите информации.

[8] Защита секретной информации, не охваченной законами. Рекомендации для АРМ.

[9] Канадский справочник по безопасности информационных технологий.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, взаимодействие сетей, взаимодействие открытых систем, коммуникационные процедуры, защита информации, технологии безопасности.

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