ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК ТО 13335-4 — 2007

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 4

Выбор защитных мер

ISO/IEC TR 13335-4:2000
Information technology — Guidelines for the management of information technology security — Part 4: Selection of safeguards
(IDT)

Издание официальное

БЗ 2—2006/14

Москва
Стандартинформ
2007

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России), Банком России, обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 июня 2007 г. № 122-ст

4 Настоящий стандарт идентичен международному отчету ИСО/МЭК ТО 13335-4:2000 «Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 4. Руководство по менеджменту безопасности сети» (ISO/IEC TR 13335-4:2000 «Information technology — Guidelines for the management of information technology security — Part 3: Selection of safeguards»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 — 2004 (подраздел 3.5)

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2007

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Цель . . . 2
5 Краткий обзор . . . 2
6 Введение к выбору защитных мер и концепции базовой безопасности . . . 4
7 Базовые оценки . . . 7
7.1 Идентификация типа системы ИТ . . . 7
7.2 Идентификация физических условий и условий окружающей среды . . . 7
7.3 Оценка существующих/планируемых защитных мер . . . 8
8 Защитные меры . . . 8
8.1 Организационные и физические защитные меры . . . 8
8.2 Специальные защитные меры систем ИТ . . . 19
9 Базовый подход: выбор защитных мер согласно типу системы ИТ . . . 25
9.1 Обычно применяемые защитные меры . . . 26
9.2 Специальные защитные меры систем ИТ . . . 27
10 Выбор защитных мер в соответствии с проблемами безопасности и угрозами . . . 27
10.1 Оценка проблем безопасности . . . 27
10.2 Защитные меры для обеспечения конфиденциальности . . . 30
10.3 Защитные меры целостности . . . 33
10.4 Защитные меры доступности . . . 37
10.5 Защитные меры для подотчетности, аутентичности и достоверности . . . 43
11 Выбор защитных мер согласно детальным оценкам . . . 44
11.1 Взаимосвязь ИСО/МЭК ТО 13335-3 с настоящим стандартом . . . 44
11.2 Принципы выбора . . . 44
12 Разработка базовой безопасности организации . . . 46
13 Выводы . . . 47
Приложение А (справочное) Кодекс менеджмента безопасности информационных технологий . . . 48
Приложение В (справочное) Стандарт ETSI «Свойства и механизмы обеспечения базового уровня безопасности» . . . 50
Приложение С (справочное) Руководство по базовой защите информационных технологий . . . 51
Приложение D (справочное) Справочник NIST по компьютерной безопасности . . . 53
Приложение Е (справочное) Медицинские информационные технологии. Категории безопасности и защита информационных систем здравоохранения . . . 54
Приложение F (справочное) ТК 68 Банковские и другие финансовые услуги. Руководящие указания по информационной безопасности . . . 55
Приложение G (справочное) Защита ценной информации, не подпадающей под действие законодательства о государственной тайне. Рекомендации для автоматизированных рабочих мест . . . 57
Приложение Н (справочное) Канадский справочник по безопасности информационных технологий 58
Приложение I (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 59
Библиография . . . 60

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 4
Выбор защиты мер

Information technology. Security techniques. Part 4. Selection of safeguards

Дата введения — 2007—09—01

1 Область применения

Настоящий стандарт является руководством по выбору защитных мер с учетом потребностей и проблем безопасности организации. В настоящем стандарте описан процесс выбора защитных мер в соответствии с риском системы безопасности и с учетом особенностей окружающей среды. Настоящий стандарт устанавливает способы достижения соответствующей защиты на основе базового уровня безопасности. Приведенный в настоящем стандарте подход к выбору защитных мер согласован с методами управления безопасностью информационных технологий, приведенными в ИСО/МЭК ТО 13335-3.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК 9126-1:2001 Программирование. Качество продукта. Часть 1. Модель качества

ИСО/МЭК 10181-2:1996 Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть 2. Основы аутентификации

ИСО/МЭК 11770-1:1996 Информационные технологии. Методы безопасности. Управление ключами. Часть 1. Структура

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

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

ИСО/МЭК ТО 13335-5:2001 Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 5. Руководство по менеджменту безопасности сети

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 13335-1, а также следующие термины с соответствующими определениями:

3.1 **аутентификация** (authentication): Обеспечение однозначного соответствия заявленного идентификатора объекту.

[ИСО/МЭК 10181-2]

3.2 **идентификация** (identification): Процесс присвоения объекту уникального идентификатора.

Издание официальное

4 Цель

Цель настоящего стандарта — обеспечить руководство по выбору защитных мер. Данное руководство предназначено для ситуаций, когда принято решение выбрать защитные меры для системы информационных технологий (ИТ):

- согласно типу и характеристикам системы ИТ;
- согласно общим оценкам проблем и угроз безопасности;
- в соответствии с результатами детального анализа рисков.

В дополнение к настоящему стандарту предоставлены перекрестные ссылки, показывающие, где выбор защитных мер может быть дополнен за счет применения общедоступных руководств, содержащих описание защитных мер.

Настоящий стандарт также содержит указания по разработке базового руководства по обеспечению безопасности организации (или ее отдельного подразделения). Описание детальных защитных мер сети содержится в документах, на которые есть ссылки в приложениях А — Н. В настоящее время техническими комитетами ИСО разрабатываются другие документы по обеспечению безопасности сетей.

5 Краткий обзор

Раздел 6 настоящего стандарта содержит введение к выбору защитных мер и концепции базового обеспечения безопасности. В разделах 7 — 10 рассматриваются вопросы базового обеспечения безопасности систем ИТ. Для того, чтобы выбрать подходящие защитные меры, необходимо определить базовые оценки безопасности систем ИТ вне зависимости от того, будет ли затем проводиться детальный анализ рисков. Эти оценки изложены в разделе 7, где рассмотрены следующие вопросы:

- для какого типа системы ИТ предполагается выбор защитных мер (например, автономный или подсоединенный к сети персональный компьютер);
- где находятся системы ИТ, какие условия окружающей среды в месте расположения этих систем;
- какие защитные меры уже приняты и/или планируются;
- насколько полученные оценки предоставляют достаточную информацию для выбора базовых защитных мер для системы ИТ.

Раздел 8 содержит обзор защитных мер, которые предполагается выбрать. Они разделены на организационные, технические (т. е. выборка проведена в соответствии с потребностями и нарушениями обеспечения безопасности, а также с учетом ограничений) и на специальные защитные меры систем ИТ. Все защитные меры сгруппированы по категориям. Для каждой категории защитных мер приведено описание наиболее типичных защитных мер, включая краткое описание уровня безопасности, которую они должны обеспечивать. Специальные защитные меры в рамках установленных категорий и их подробное описание можно найти в документах по базовой безопасности (см. ссылки в приложениях А — Н). Для облегчения пользования этими документами перекрестные ссылки между категориями защитных мер настоящего стандарта и главами других документов, указанных в приложениях, приведены в таблицах для каждой категории защитных мер.

Если организацией принято решение, что тип оценки, детально описанный в разделе 7 настоящего стандарта, достаточен для выбора защитных мер, то организация может использовать список подходящих защитных мер, приведенных в разделе 9, для каждой типичной системы ИТ, описание которых приведено в 7.1. Если организация выбирает защитные меры на основе типа системы ИТ, то могут применяться базовые уровни безопасности для автономных рабочих станций, сетевых автоматизированных рабочих мест (АРМ) или серверов. Для обеспечения требуемого уровня безопасности необходимо выбрать защитные меры, пригодные в конкретных условиях, сравнить их с уже существующими (или планируемыми) мерами обеспечения безопасности и внедрить все новое, что можно использовать для достижения заданного уровня безопасности.

Если организацией принято решение о необходимости более глубокой оценки для выбора эффективных и подходящих защитных мер, то раздел 10 настоящего стандарта оказывает поддержку такого выбора с учетом рассмотрения проблем безопасности, на высоком уровне (в соответствии с важностью информации) и возможных угроз. В данном разделе защитные меры предложены согласно проблемам безопасности, с учетом соответствующих угроз и выбранного типа системы ИТ. Схема выбора защитных мер, описание которых приведено в разделах 7, 9 и 10, приведена на рисунке 1.

В разделах 9 и 10 приведено описание выбора защитных мер на основе документов по базовой безопасности, которые могут быть применены или для системы ИТ, или для формирования пакета защитных мер для ряда систем ИТ, используемых в определенных условиях. Ориентируясь на тип системы ИТ, организация может использовать подход, предложенный в разделе 9, который допускает возможность того, что некоторые риски анализируются неадекватно и выбираются некоторые защитные меры, которые не являются необходимыми или соответствующими. В разделе 10 предложен подход, направленный на решение проблем безопасности от соответствующих угроз, который позволяет разработать оптимальный пакет защитных мер. Разделы 9 и 10 организация может использовать для выбора защитных мер без детальных оценок всех вариантов, подладающих под область применения базовой безопасности. Однако и при более детальной оценке, т. е. при детальном анализе рисков, при выборе защитных мер разделы 9 и 10 все еще будут полезными.

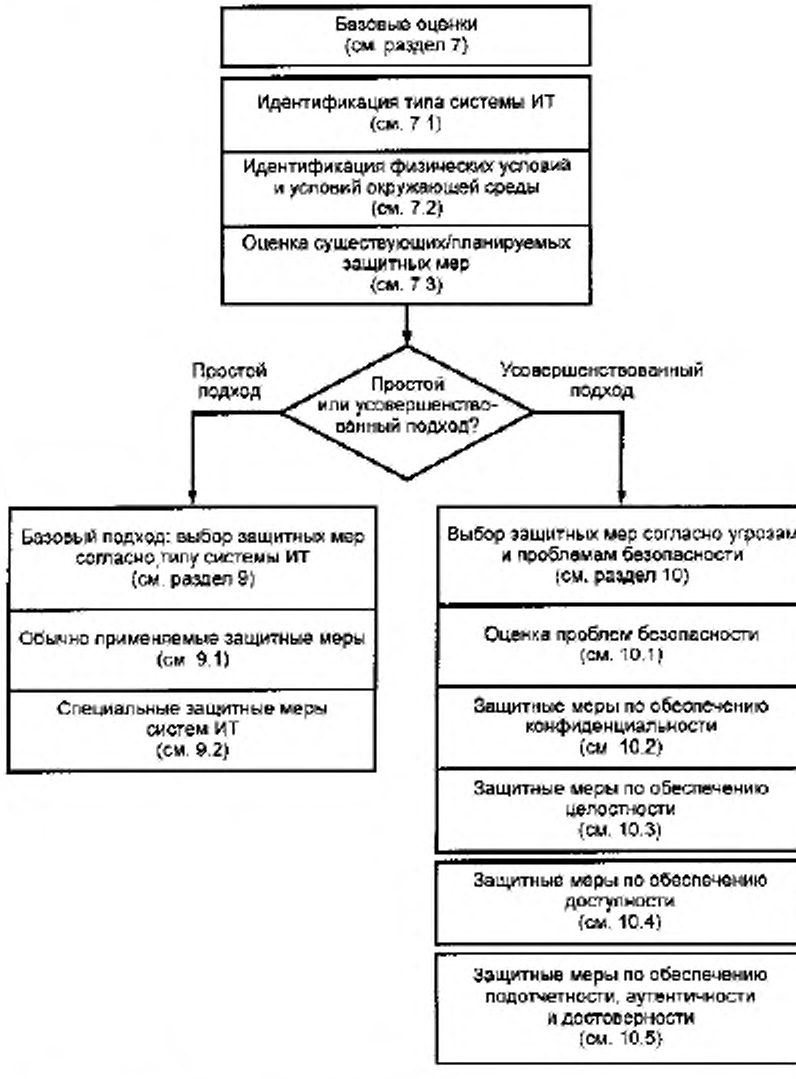

Рисунок 1 — Выбор защитных мер по типу системы информационных технологий, угрозам и проблемам безопасности

В разделе 11 настоящего стандарта рассматривается ситуация, когда организация принимает решение о необходимости проведения детального анализа рисков в связи с высоким уровнем проблем безопасности и потребностями организации. Руководство по анализу рисков приведено в ИСО/МЭК ТО 13335-3. В разделе 11 настоящего стандарта приведено описание взаимосвязи ИСО/МЭК ТО 13335-3 с настоящим стандартом, а также результаты использования методов, изложенных в ИСО/МЭК ТО 13335-3, которые могут учитываться при выборе защитных мер. В разделе 11 также приведено описание других факторов, способных влиять на выбор защитных мер, например, любые ограничения, которые должны быть приняты во внимание, обязательные или иные требования, которые должны быть выполнены и т. д.

Подход, рассмотренный в разделе 11 настоящего стандарта, отличается от подходов в разделах 9 и 10 тем, что он содержит руководство для выбора пакета защитных мер, оптимальных для конкретной ситуации. Этот подход не является базовым, но в некоторых случаях может быть использован для выбора защитных мер в дополнение к мерам базовой безопасности. В качестве альтернативы этот подход может быть применен без какой-либо связи с базовой безопасностью.

В разделе 12 представлено руководство (каталог) по выбору базового уровня безопасности организации в целом или ее отдельных подразделений. Для такого выбора организация должна рассмотреть защитные меры, ранее идентифицированные для систем ИТ или групп систем ИТ, и определить общий пакет защитных мер. В зависимости от степени конфиденциальности, потребности обеспечения безопасности и ограничений могут быть выбраны разные уровни базовой безопасности. В данном разделе рассмотрены преимущества и недостатки различных уровней базовой безопасности, которые могут помочь принятию подходящего решения для каждой организации.

Краткое резюме содержания настоящего стандарта приведено в разделе 13, а в приложениях А — Н краткий обзор инструкций, на которые есть ссылки в разделе 8.

6 Введение к выбору защитных мер и концепции базовой безопасности

В настоящем разделе приведен краткий обзор процесса выбора защитных мер, а также способа и времени применения в этом процессе концепции базовой безопасности. Существуют два главных подхода к выбору защитных мер: использование базового подхода и выполнение детального анализа риска. Выполнение детального анализа риска может проводиться различными подходами, один из которых подробно изложен в ИСО/МЭК ТО 13335-3 и называется детальным анализом риска. В ИСО/МЭК ТО 13335-3 также рассматриваются преимущества и недостатки разных подходов к оценке риска и, следовательно, выбору защитных мер.

Проведение детального анализа риска позволяет всесторонне рассмотреть риск. Результаты детального анализа могут применяться для выбора защитных мер, вызванных этими рисками, и подобные защитные меры должны быть внедрены. Таким образом, можно избежать крайностей в обеспечении безопасности систем ИТ организации. Так как для анализа риска требуется много времени, усилий и проведение многочисленных экспертиз, то он более подходит для систем ИТ с высоким уровнем риска, тогда как более простой подход считается достаточным для систем с низким уровнем риска. Использование анализа риска высокого уровня позволяет выявлять системы с более низким уровнем риска. Анализ риска высокого уровня не должен быть формализованным или сложным. Защитные меры для систем с более низким уровнем риска могут быть выбраны путем применения защитных мер по базовой безопасности. Этот уровень обеспечения безопасности может быть не ниже минимального уровня безопасности, установленного организацией для каждого типа системы ИТ. Уровень базовой безопасности (далее — базовый подход) достигается путем реализации минимального пакета защитных мер, известных как базовые защитные меры.

Вследствие различий в процессах выбора защитных мер в настоящем стандарте рассматриваются два пути применения базового подхода:

- в случае, если рекомендуются защитные меры в соответствии с типом и характеристиками рассматриваемой системы ИТ;
- в случае, если рекомендуются защитные меры в соответствии с угрозами и проблемами безопасности, а также в зависимости от рассматриваемой системы ИТ.

Пути выбора защитных мер приведены на рисунке 2. На рисунке 2 также показаны взаимоотношения между ИСО/МЭК ТО 13335-3 и настоящим стандартом.

Базовый подход следует выбирать в зависимости от ресурсов, которые могут быть потрачены на процесс выбора выявленных проблем безопасности, типа и характеристик рассматриваемой системы ИТ. Если организация не желает тратить (по какой-либо причине) много времени и усилий на выбор защитных

мер, то она может выбрать базовый подход, предлагающий защиту без дальнейших оценок. Однако, если коммерческая деятельность организации хотя бы частично зависит от системы или услуг ИТ и/или обрабатываемая информация является конфиденциальной то, по всей вероятности, могут потребоваться дополнительные защитные меры. В этом случае настоятельно рекомендуется рассмотреть проблемы безопасности информации на более высоком уровне и выявить вероятные угрозы для применения соответствующих защитных мер, необходимых для обеспечения более эффективной безопасности системы ИТ. Если коммерческая деятельность организации в большой степени зависит от системы и услуг ИТ и/или обрабатываемая информация является строго конфиденциальной, то степень риска может быть высокой, поэтому детальный анализ риска является наилучшим способом идентификации защитных мер.

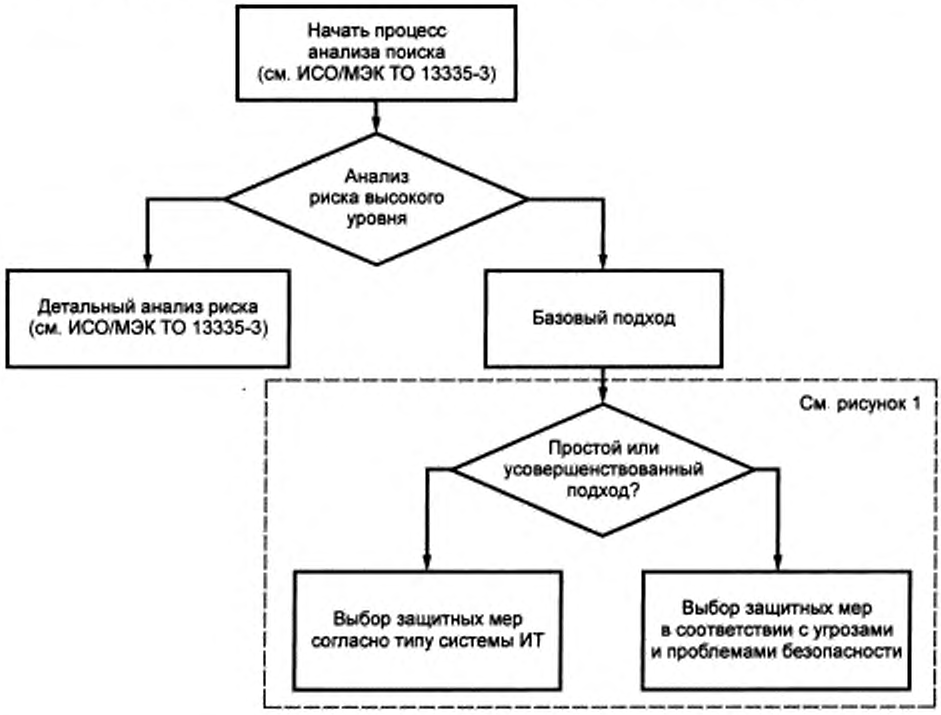

Рисунок 2 — Пути выбора защитных мер

Специальные защитные меры должны быть идентифицированы на основе детального анализа риска в случае если:

- тип рассматриваемой системы ИТ не приведен в настоящем стандарте;
- потребности организации, связанные с коммерческой деятельностью или обеспечением безопасности, несоизмеримы с требованиями настоящего стандарта;
- более детальная оценка необходима вследствие высокого уровня потенциального риска или значимости системы ИТ для бизнеса.

Следует отметить, что даже при детальном анализе риска для организации полезно применять к системе ИТ базовые защитные меры.

Первое решение, которое в этой области должна принять организация, касается вопроса использования базового подхода: его самостоятельного применения или применения в качестве части более всесторонней стратегии анализа риска (см. ИСО/МЭК ТО 13335-3).

Следует заметить, что при принятии решения об использовании базового подхода самостоятельно, процесс выбора защитных мер может в результате привести к менее оптимальному уровню безопасности, чем в случае принятия стратегии более широкого анализа рисков. Однако меньшие расходы и меньшая потребность в ресурсах для выбора защитных мер и достижение минимального уровня безопасности для всех систем ИТ оправдывают решение о применении собственного базового подхода.

Базовая защита системы ИТ может быть достигнута через идентификацию и применение пакета соответствующих защитных мер, которые применимы в условиях с низким уровнем риска, т. е. соответствуют минимальной потребности обеспечения безопасности. Например, соответствующие защитные меры обеспечения безопасности могут быть идентифицированы по каталогам, которые предлагают пакеты защитных мер для различных типов систем ИТ для обеспечения их защиты от большинства общих угроз. Каталоги защитных мер содержат информацию о категориях защитных мер или отдельных защитных мерах, или их совместном применении, но обычно в них отсутствуют указания о типах защитных мер, применяемых в конкретных условиях. Если системы ИТ организации (или ее подразделений) аналогичны, то защитные меры, выбранные путем применения базового подхода, могут быть применены ко всем системам ИТ. Различные пути применения базового подхода выбора защитных мер, рассмотренного в ИСО/МЭК ТО 13335-3, представлены на рисунке 3.

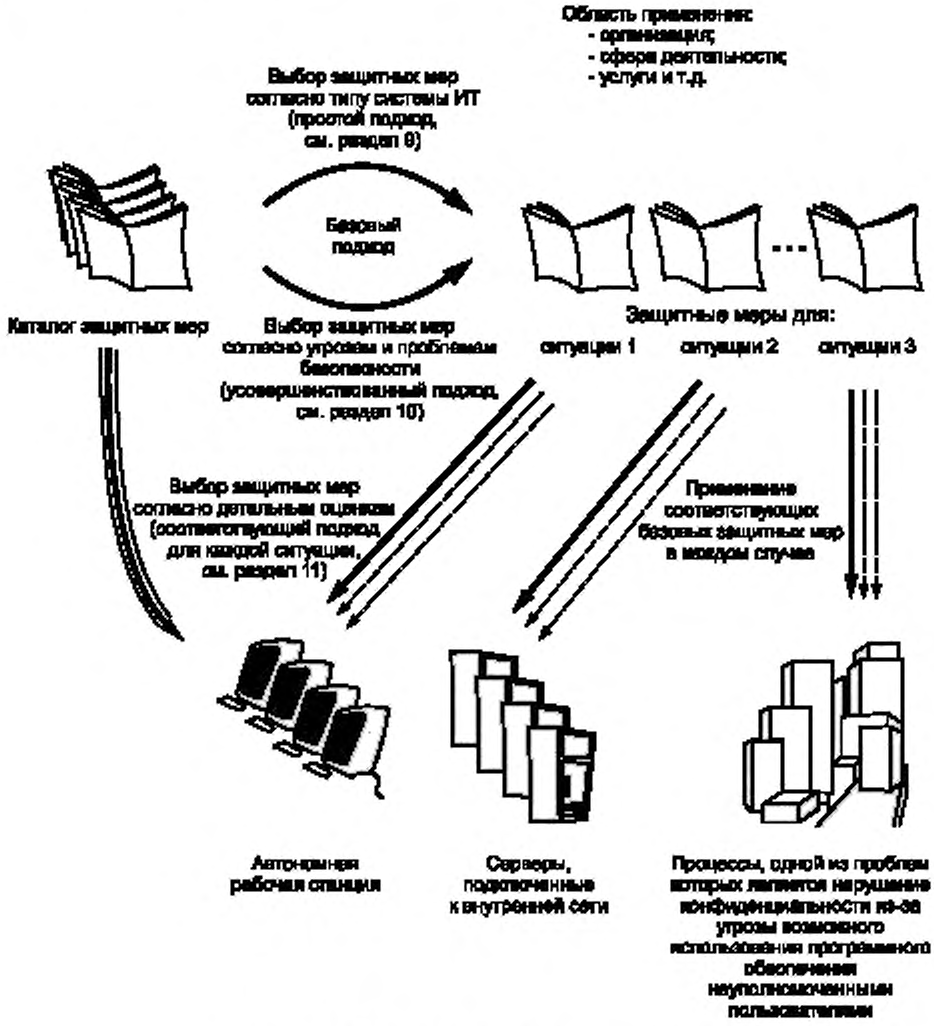

Рисунок 3 — Подходы к выбору защитных мер

Если организация применяет базовый подход ко всей структуре или отдельным своим подразделениям, то необходимо принять решение, какие подразделения организации подходят для применения одного и того же уровня безопасности, а также какой уровень обеспечения безопасности следует выбрать для

данных подразделений организации. В большинстве случаев при использовании базовой безопасности снижение ее уровня недопустимо, в то время как применение дополнительных защитных мер может быть оправдано и необходимо для управления риском среднего и высокого уровня.

В качестве альтернативы базовый подход к безопасности может отражать средний уровень безопасности организации, т. е. в организации допускается обоснованное применение более высокого или более низкого относительно базового уровня безопасности, например по результатам анализа риска. Одним из преимуществ применения базового подхода безопасности к группе систем ИТ является обеспечение определенного уровня безопасности в пределах всей группы систем ИТ. В этих условиях может быть полезным разработка и документирование базового каталога защитных мер для всей организации или ее отдельных подразделений.

7 Базовые оценки

Процесс выбора защитных мер всегда требует знания типа и характеристики рассматриваемой системы ИТ (например автономная или подсоединенная к сети рабочая станция), так как эти знания оказывают влияние на выбранные защитные меры. Таюке полезно иметь представление об инфраструктуре организации (здания, помещения и т. д.). Другим важным фактором, связанным с выбором защитных мер, является оценка существующих и/или планируемых мер защиты во избежание ненужной работы, траты времени и средств. Однако настоятельно рекомендуется всегда использовать оценки, описанные в настоящем разделе, в качестве базовых для выбора защитных мер. При выборе защитных мер следует учитывать требования бизнеса и подход организации к обеспечению безопасности. В заключение необходимо определить, обеспечивают ли эти оценки достаточно информации для выбора базовых мер защиты, или необходима более детальная оценка (см. раздел 10) или детальный анализ риска (см. раздел 11).

7.1 Идентификация типа системы ИТ

Для оценки существующей или планируемой системы ИТ организация должна сравнить рассматриваемую систему ИТ с перечисленными ниже компонентами. Организация должна идентифицировать компоненты, представляющие данную систему. Защитные меры для каждого из перечисленных компонентов представлены в разделе 9. К ним относятся:

- автономная рабочая станция;
- рабочая станция (клиент без ресурсов коллективного пользования), подсоединенная к сети;
- сервер или рабочая станция с ресурсами коллективного пользования, подсоединенные к сети.

7.2 Идентификация физических условий и условий окружающей среды

Оценка окружающей среды включает в себя идентификацию физической инфраструктуры, поддерживающей существующую или планируемую систему ИТ и защитные меры к ней. Защитные меры должны соответствовать окружающей среде, поэтому подобная оценка является важным фактором для успешного выбора защитных мер. При рассмотрении физической инфраструктуры организация должна изучить окружающую среду и специальные обстоятельства, которые необходимо учесть. При этом следует использовать следующие вопросы, относящиеся к:

- территории и зданию:
  - где расположено здание. В границах своей территории с забором по периметру или на улице с интенсивным движением транспорта и т. д.,
  - арендует здание одна или много организаций,
  - область деятельности организаций, арендующих здание (если применимо),
  - где находятся уязвимые/критические области;
- управлению доступом:
  - кто имеет доступ в здание,
  - установлена ли в здании пропускная система,
  - устойчива ли конструкция здания,
  - прочность и уровень защиты дверей, окон и т. д.,
  - охраняются ли здания, охрана круглосуточная или повременная,
  - установлена ли охранная сигнализация на отдельные здания и/или помещения с важным оборудованием ИТ;
- защите на месте:
  - степень защищенности помещений, в которых расположена система ИТ,
  - предусмотрены ли меры пожарной безопасности: сигнал тревоги и блокировка систем,

предусмотрены ли меры по обнаружению утечки воды/ жидкости: сигнал тревоги и пути аварийного стока,

предусмотрены ли вспомогательные коммунальные услуги, например бесперебойное электро- и водоснабжение и вентиляция воздуха (для управления температурой и влажностью)?

Ответив на эти вопросы, можно легко идентифицировать существующие и взаимосвязанные физические и другие защитные меры. Не следует считать тратой времени рассмотрение вопроса о местоположении здания, в том числе дверей, замков и прочих средств контроля физического доступа.

7.3 Оценка существующих/планируемых защитных мер

После оценки физических условий и условий окружающей среды и компонентов системы ИТ должны быть идентифицированы существующие или планируемые защитные меры. Это необходимо сделать во избежание дублирования существующих или планируемых защитных мер. Кроме того, изучение внедренных или запланированных защитных мер помогает при выборе других взаимосвязанных защитных мер. При выборе защитных мер организация должна принимать во внимание их совместимость с существующими защитными мерами. Одни защитные меры могут конфликтовать с другими или мешать их успешной работе и действующей системе безопасности в целом.

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

- просмотр документов, содержащих информацию о мерах безопасности (например, планов или концепций обеспечения безопасности ИТ). Если процесс обеспечения безопасности документирован, то в документации должны быть перечислены все существующие или планируемые защитные меры и статус их реализации;

- проверка вместе с пользователями и ответственными сотрудниками (например специалистом по безопасности системы ИТ, главным инженером или комендантом, ответственным за управление зданием и его эксплуатацию) того, какие защитные меры действительно реализуются для рассматриваемой системы ИТ;

- осмотр здания с целью проверки реализации защитных мер, их сравнения с перечнем установленных защитных мер, оценка их корректности и эффективности.

Может быть установлено, что существующие защитные меры превышают текущие потребности организации. В этом случае следует рассмотреть вопрос об исключении избыточных защитных мер. При этом следует принять во внимание факторы обеспечения безопасности организации и экономической целесообразности применения защитных мер. Защитные меры влияют друг на друга, поэтому исключение избыточных защитных мер может снизить совокупный уровень безопасности. Кроме того, иногда дешевле сохранить избыточные защитные меры, чем их ликвидировать. Наоборот, если поддержание в рабочем состоянии и обслуживание избыточных защитных мер связано с высокими расходами, то дешевле их ликвидировать.

8 Защитные меры

Настоящий раздел содержит краткий обзор возможных защитных мер, подлежащих реализации для повышения уровня безопасности. Защитные меры связаны с работой аппаратных средств и механизмов, а также с процедурами, которые должны соблюдаться персоналом в организации. Организационные и физические защитные меры, применяемые к системам ИТ, рассматриваются в 8.1. Специальные защитные меры для системы ИТ рассматриваются в 8.2. Следует отметить, что защитные меры должны быть описаны вне зависимости от способа их выбора, т. е. некоторые защитные меры могут быть выбраны, другие могут быть идентифицированы путем выполнения детального анализа рисков.

Для того, чтобы упростить описание различных типов защитных мер, организация должна установить категории защитных мер. Настоящий раздел содержит краткое описание этих категорий и указание на то, какие типы безопасности ИТ имеют к ним отношение. В приложениях А — Н приведены ссылки на документы, содержащие более подробную информацию о защитных мерах, приведенных в настоящем стандарте.

8.1 Организационные и физические защитные меры

Источники дополнительной информации о категориях защитных мер приведены в таблицах 8.1.1— 8.1.7.

8.1.1 Политика и управление безопасностью ИТ

Данная категория защитных мер содержит все защитные меры, имеющие отношение к управлению безопасностью ИТ, планированию деятельности, распределению полномочий и ответственности по этим процессам, а также все другие необходимые действия. Эти защитные меры описаны в ИСО/МЭК 13335-1 и

ИСО/МЭК ТО 13335-3. Целью этих защитных мер является достижение необходимого уровня безопасности организации. Ниже перечислены защитные меры в этой области:

1 Политика обеспечения безопасности ИТ организации

Организация должна разработать документированную процедуру, содержащую правила, директивы и установленный порядок действий управления, защиты и распределения активов организации. В документированной процедуре должны быть установлены потребности организации в документах по политике обеспечения безопасности систем ИТ и их содержание и управление.

2 Политика обеспечения безопасности системы ИТ

Для каждой системы ИТ следует разработать политику безопасности системы ИТ, содержащей 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 (уполномоченного по безопасности ИТ), ответственного за безопасность каждой системы ИТ.

4 Распределение ответственности и полномочий

Распределение ответственности и полномочий по обеспечению безопасности ИТ организации должно проводиться и быть задокументировано в соответствии с политикой обеспечения безопасности ИТ и политикой обеспечения безопасности систем ИТ.

5 Организация безопасности ИТ

Для оказания поддержки в области обеспечения безопасности организация должна обеспечить безопасность ИТ всех своих бизнес-процессов (например закупки, взаимодействия с другими организациями).

6 Идентификация и определение стоимости активов

Все активы организации по каждой системе ИТ должны быть идентифицированы, стоимость активов должна быть оценена.

7 Одобрение систем ИТ

Системы ИТ следует одобрять в соответствии с политикой обеспечения безопасности ИТ. Целью процесса одобрения должно быть обеспечение внедрения защитных мер, гарантирующих необходимый уровень безопасности. Следует учитывать то, что система ИТ может включать в себя сети и основные линии связи.

8.1.2 Проверка соответствия безопасности установленным требованиям

Для организации важно обеспечивать соответствие необходимых защитных мер соответствующим законодательным и обязательным требованиям и политике организации в данной области. Это связано с тем, что любая защита, правило и политика работают только в случае, если их соблюдают пользователи и им соответствуют сами системы. К этой категории относятся следующие защитные меры:

1 Соответствие политики обеспечения безопасности ИТ защитным мерам

Организация должна проводить через запланированные интервалы времени проверки всех установленных защитных мер, перечисленных в политике обеспечения безопасности ИТ организации и систем ИТ, а также в другой взаимосвязанной документации организации, например в процедурах обеспечения безопасности работы и планах действий в непредвиденных ситуациях на соответствие корректности и эффективности их использования (включая конечного пользователя). В случае необходимости защитные меры должны проходить испытания.

2 Соответствие законодательным и обязательным требованиям

Организация должна проводить проверку соответствия системы ИТ установленным законодательным и обязательным требованиям стран(ы), в которых (ой) расположена система ИТ. В случае, если такие требования существуют, то они должны включать в себя обязательные требования по охране авторских прав и конфиденциальности информации, защите от копирования программного обеспечения, защите записей организации и защите от неправильного использования систем ИТ и другие (например по применению криптографии).

8.1.3 Обработка инцидента

Персонал организации должен понимать необходимость отчетов об инцидентах безопасности, включая нарушения правильного функционирования программного обеспечения и случаи неустойчивой работы системы. Для этого в организации должна быть разработана соответствующая схема передачи сообщений. Обработка инцидента включает в себя:

1 Отчет об инциденте безопасности

Отчет об инциденте является обязанностью каждого сотрудника. Инциденты и сбои могут быть также идентифицированы и зарегистрированы с помощью инструментальных средств. Для повышения эффектив-

ности деятельности при инциденте должна быть разработана схема передачи отчетов и места их приема в организации.

2 Отчет о слабых местах при обеспечении безопасности

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

3 Отчет 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 возникновения инцидента

Процесс управления должен обеспечивать безопасность от инцидентов, их обнаружение, оповещение и соответствующую реакцию на инцидент. Организация должна проводить сбор и оценку информации об инцидентах во избежание их повторного возникновения, а также для сокращения ущерба.

8.1.4 Персонал

Защитные меры в этой категории должны снижать риски безопасности в результате ошибок или преднамеренного или непреднамеренного нарушения правил безопасности персоналом (штатным или нанятым по контракту). К этой категории относятся следующие защитные меры:

1 Защитные меры для штатного или временного персонала

Все сотрудники должны понимать свою роль и обязанности относительно безопасности. Организация должна определить и документировать процедуры, касающиеся безопасности, которые должны соблюдаться персоналом. При найме персонала на работу он должен подлежать проверке и, в случае необходимости, с персоналом должно быть подписано соглашение о соблюдении правил конфиденциальности.

2 Защитные меры для персонала, нанятого по контракту

Организация должна контролировать персонал, работающий по контракту (например уборщицы или технический персонал), а так же любого другого посетителя. Персонал, нанятый по контракту на длительное время, должен подписать обязательство о соблюдении правил конфиденциальности, прежде чем он получит доступ (физически или логически) к системам ИТ организации.

3 Обучение и осведомленность о мерах безопасности

С персоналом, который использует, разрабатывает, поддерживает в рабочем состоянии и имеет доступ к оборудованию ИТ, должен регулярно проводиться инструктаж по вопросам обеспечения безопасности. Персонал должен обеспечиваться соответствующими материалами. Это позволяет обеспечить осведомленность персонала о важности коммерческой информации, соответствующих угрозах, уязвимостях и риске и, следовательно, понимание необходимости защитных мер. Организация должна обучать пользователей правильному использованию средств ИТ во избежание ошибок. Для ответственного персонала, например специалистов по безопасности ИТ, администраторов, отвечающих за обеспечение безопасности, может потребоваться специальное обучение.

4 Процесс обеспечения исполнительской дисциплины

Персонал организации должен понимать последствия (намеренного или непреднамеренного) нарушения политики обеспечения безопасности ИТ организации или соглашения о соблюдении конфиденциальности.

8.1.5 Эксплуатационные вопросы

Целью защитных мер этой категории является поддержание в рабочем состоянии процедур по обеспечению безопасности, правильного и надежного функционирования оборудования ИТ и связанных с ним систем. Большинство из этих защитных мер могут быть реализованы путем внедрения организационных процедур. Эксплуатационные защитные меры должны быть совмещены с другими видами защиты, например физической и технической. К этой категории относятся следующие защитные меры:

1 Управление конфигурацией и изменениями

Управление конфигурацией является процессом отслеживания изменений в системах ИТ. При этом главная задача обеспечения безопасности организации включает в себя обеспечение эффективности защитных мер и совокупной безопасности при изменениях в системах ИТ. Управление изменениями может способствовать идентификации новых форм применения защитных мер по обеспечению безопасности при изменениях в системах ИТ.

2 Управление резервами

Организация должна управлять резервами для предупреждения возникновения сбоев из-за недостатка ресурсов. При оценке резервов, необходимых для системы ИТ, должны учитываться будущие и текущие требования к резервам.

3 Документация

Все аспекты операций и конфигураций ИТ должны быть задокументированы для обеспечения их непрерывности и последовательности. Безопасность системы ИТ должна быть оформлена документально в политике обеспечения безопасности ИТ, в документации, регламентирующей операционные процедуры безопасности, отчетах и планах по бизнес-стратегии организации. Эта документация должна быть актуализирована и доступна уполномоченному персоналу.

4 Техническое обслуживание

Организация должна проводить техническое обслуживание оборудования ИТ для обеспечения его постоянной надежности, доступности и целостности. Требования по обеспечению безопасности, которые должны соблюдать подрядчики при выполнении технического обслуживания, должны быть документально оформлены и записаны в соответствующих контрактах. Техническое обслуживание должно проводиться в соответствии с контрактом с привлечением квалифицированного персонала.

5 Мониторинг изменений, связанных с безопасностью

Организация должна проводить мониторинг изменений воздействий, угроз, уязвимостей и риска, а также связанных с ними характеристик безопасности. Мониторинг должен включать в себя существующие и новые аспекты. Организация должна проводить мониторинг окружающей среды, в которой расположена система ИТ.

6 Записи аудита и регистрация

Аудиторские и регистрирующие способности серверов (регистрация записей аудита и анализ средств), сетей (аудит аппаратно-программных средств межсетевой защиты и маршрутов) и приложений (аудиторские средства систем передачи сообщений или обработка транзакций) должны использоваться для записи подробностей событий, относящихся к обеспечению безопасности. Эти события включают в себя легко опознаваемые несанкционированные или ошибочные события и подробности очевидных нормальных событий, которые могут потребоваться для дальнейшего анализа. Записи аудита и журналы регистрации должны регулярно анализироваться для обнаружения несанкционированной деятельности и принятия соответствующих корректирующих мер. События, зарегистрированные в журналах, должны также анализироваться на повторяемость аналогичных событий, которые указывают на присутствие уязвимостей или угроз, против которых еще не приняты адекватные защитные меры. Такой анализ может выявлять шаблоны в очевидных несвязанных событиях, которые позволяют идентифицировать лиц, занимающихся несанкционированной деятельностью, или определять основные причины проблем, связанных с безопасностью.

Примечание — В настоящем стандарте термины «аудиторские способности» систем и приложений, и «регистрирующие способности» применяются в одном и том же смысле. В то время подобные способности могут быть использованы для поддержки проведения более широких финансовых аудитов.

7 Тестирование безопасности

Организация должна проводить тестирование безопасности для обеспечения безопасного функционирования всего оборудования ИТ и связанных с ним компонентов программного обеспечения. Должна проводиться проверка соответствия требованиям, установленным в политике обеспечения безопасности системы ИТ и планах проведения тестирования (испытаний), а также установлены критерии, позволяющие демонстрировать достижение необходимого уровня безопасности.

8 Управление носителями информации

Управление носителями информации включает в себя разнообразные защитные меры, обеспечивающие защиту (физическую и в окружающей среде), а также возможность подотчетности дискет, дисков, выводов на печать и в другую среду передачи информации. Управление может включать маркировку, регистрацию, верификацию целостности, защиту физического доступа, защиту от воздействия окружающей среды, процесс передачи и безопасное уничтожение носителей информации.

9 Обеспечение стирания памяти

Конфиденциальность ранее записанной в запоминающем устройстве информации должна быть сохранена, даже если эта информация больше не требуется. Должно быть обеспечено стирание или физичес-

кая перезапись файлов, содержащих конфиденциальный материал, или они должны быть уничтожены другим способом, так как функция стирания не всегда гарантирует полное уничтожение информации. Средства для полного и безопасного стирания, одобренные ответственным персоналом (например, специалистом по безопасности), должны быть предоставлены в распоряжение пользователей.

10 Распределение ответственности и полномочий

Для минимизации риска и возможности для злоупотребления полномочиями, организация должна распределить ответственность и полномочия. В частности должны быть разделены обязанности и функции, которые в комбинации могут привести к обходу защитных мер или аудитов или чрезмерному преимуществу для работника.

11 Корректное использование программного обеспечения

Организация должна обеспечивать невозможность несанкционированного повторного копирования печатных материалов и выполнение лицензионных соглашений в отношении прав собственника программного обеспечения.

12 Управление изменениями программного обеспечения

Организация должна управлять изменениями программного обеспечения для поддержания его целостности в случае внесения изменений (управление изменениями программного обеспечения должно применяться только к программному обеспечению, в то время как управление конфигурацией и изменениями, описанное в соответствующей категории обеспечения безопасности, должно применяться к системам ИТ и их окружению в целом). Должны быть установлены процедуры управления изменениями программного обеспечения, которые предусматривают управление всеми изменениями и обеспечивают поддержание безопасности всего процесса. К ним относится санкционированное разрешение на изменения, рассмотрение вопросов безопасности для принятия промежуточных решений и проверка безопасности на конечной стадии.

8.1.6 Планирование непрерывности бизнеса

Для обеспечения защиты основных бизнес-процессов организации от воздействия серьезных отказов или бедствий и сведения к минимуму ущерба, нанесенного такими событиями, организация должна разработать эффективную стратегию непрерывности бизнеса, включая планы и стратегию действий в чрезвычайной ситуации и восстановления после бедствия. К этой категории относятся следующие защитные меры:

1 Стратегия непрерывности бизнеса

Организация должна разработать и документально оформить стратегию непрерывности бизнеса, включая план действий в чрезвычайной ситуации и восстановление после бедствий, в отношении рассматриваемой системы ИТ на основе потенциальных идентифицированных неблагоприятных воздействий на бизнес вследствие неготовности к работе, модификации или разрушения системы ИТ.

2 План непрерывности бизнеса

На основе стратегии непрерывности бизнеса организация должна разработать и документально оформить планы непрерывности бизнеса в случае возникновения чрезвычайной ситуации и восстановления после бедствия.

3 Проверка и актуализация плана непрерывности бизнеса

Прежде чем принять план непрерывности бизнеса, организация должна тщательно проверить его эффективность в обстоятельствах реальной жизни и довести его до сведения ответственного персонала. Так как планы непрерывности бизнеса могут быстро устаревать, организация должна проводить их периодическую актуализацию. Стратегия непрерывности бизнеса должна совершенствоваться по мере необходимости.

4 Дублирование

Организация должна дублировать все важные файлы и другие информационные данные бизнеса, программы и документацию важных систем. Периодичность дублирования должна быть установлена в зависимости от важности информации и в соответствии с планом непрерывности бизнеса. Резервные копии должны храниться в безопасном месте и отдельно друг от друга, а восстановленные копии — периодически проверяться на достоверность.

8.1.7 Физическая безопасность

Защитные меры в этой области связаны с физической защитой. Их следует рассматривать совместно с идентификацией окружающей среды (см. 7.2). Нижеизложенные защитные меры должны применяться к зданиям, зонам безопасности, местам размещения ЭВМ и офисным помещениям. Выбор защитных мер зависит от рассматриваемой части здания. К этой категории относятся следующие защитные меры:

1 Материальная защита

Физические защитные меры, применяемые для защиты здания, включают в себя заборы, управление физическим доступом (пропускные пункты), прочные стены, двери и окна. Зоны безопасности в пределах здания должны быть защищены от несанкционированного проникновения с помощью управления физическим доступом, охраны и т. д. Зоны безопасности могут быть необходимы для оборудования ИТ, например, серверов, связанного с ними программного обеспечения и данных, поддерживающих важные виды коммерческой деятельности организации. Доступ в такие зоны безопасности должен быть ограничен минимальным числом необходимого персонала, подробное описание доступа должно быть зарегистрировано. Все диагностическое и контрольное оборудование должно храниться в безопасном месте и его использование должно держаться под строгим контролем.

2 Противопожарная защита

Оборудование и прилегающая территория, включая доступ к ним, должны быть защищены от распространения огня из какого-либо места в здании или соседних строений. Опасность возникновения и распространения пожара вблизи помещений и/или зон, содержащих оборудование, должна быть сведена к минимуму. Организация должна обеспечить защиту от пожаров, возникающих в пределах и/или затрагивающих помещения/зоны, содержащие основное оборудование. Защитные меры должны предусматривать обнаружение огня и дыма, охранную сигнализацию и подавление очага возгорания. Следует также учитывать, что противопожарная защита может не вызвать повреждения систем ИТ от воды или других средств тушения.

3 Защита от воды/других жидкостей

Организация не должна размещать основные (значимые) средства в зоне возможного затопления, утечки воды или другой жидкости. Должна быть предусмотрена соответствующая защита в случае возникновения угрозы затопления.

4 Защита от стихийных бедствий

Здания, содержащие важное оборудование, должны быть защищены от удара молнии и оснащено защитой от грозового разряда. Защита от стихийных бедствий может быть достигнута за счет размещения оборудования в зонах, где стихийные бедствия маловероятны, а также применения стратегического и текущего планирования.

5 Защита от хищения

Для обеспечения управления уровнями запасов все части оборудования должны быть однозначно идентифицированы и подлежать инвентарному учету. Персонал охраны и администраторы должны проверять выносимые без разрешения из помещений/зон или здания оборудование или ресурсы. Организация должна обеспечить защиту конфиденциальности информации и прав собственности на программное обеспечение, находящихся на портативных носителях (например, съемных и сменных дисках, флэш-накопителях, оптических дисках, гибких дисках и др.).

6 Энергоснабжение и вентиляция

Все оборудование ИТ должно быть защищено (при необходимости) от внезапного отключения электричества. Должен быть предусмотрен соответствующий альтернативный источник энергоснабжения и бесперебойного питания. Другой целью обеспечения безопасности является поддержание допустимой температуры и влажности.

7 Прокладка кабелей

Силовые и коммуникационные кабели, осуществляющие передачу данных или поддержку служб ИТ, должны быть защищены от перехвата информации, повреждения и перегрузки. Проложенные кабели должны быть защищены от случайного или преднамеренного повреждения.

При планировании кабелей должны учитываться перспективные разработки. В оправданных случаях кабели должны быть защищены от возможного подслушивания.

Таблица 8.1.1 — Политика и управление безопасностью ИТ

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Политика обеспечения безопасности ИТ организации	3.1	—	1.1, 1.2	5.1	6.3.1.1, 7.3.1.1, 8.3.1.1, 9.3.1.1, 10.3.1.1, 11.3.1.1	3	—	5.1, 5.2
2 Политика обеспечения безопасности системы ИТ	—	—	1.1, 1.2	5.2, 5.3	6.3.1.1, 7.3.1.1, 8.3.1.1, 9.3.1.1, 10.3.1.1, 11.3.1.1	3	—	5.2, 5.3
3 Управление безопасностью ИТ	4.1.1, 4.1.2	—	1.1, 1.2	6	6.3.1.1, 7.3.1.1, 8.3.1.1, 9.3.1.1, 10.3.1.1, 11.3.1.1	4	2.1	6
4 Распределение ответственности и полномочий	4.1.3	—	1.3	2.4, 2.5, 3	6.3.1.1, 7.3.1.1, 8.3.1.1, 9.3.1.1, 10.3.1.1, 11.3.1.1	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 и определение стоимости активов	5	—	2.2	7.1	—	5.6, 7.1	5.1	7.1
7 Одобрение систем ИТ	4.1.4	—	—	8	5	—	6.7	8, 9

Таблица 8.1.2 — Проверка соответствия безопасности установленным требованиям

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Соответствие политики обеспечения безопасности ИТ защитным мерам	12.2	—	1.2	10.2.3	—	10.2	7.1, 7.2	9.4, 10.2.3
2 Соответствие законодательным и обязательным требованиям	12.1	—	3.1, 3.2	6.3, 10.2.3	6.3.1	8.18, 10.2	8.1	1.5, 2.9, 6.3, 10.2.3

Таблица 8.1.3 — Обработка инцидента

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Отчет об инциденте безопасности	6.3.1	—	M2	12	—	10.4	—	12
2 Сообщение о слабых местах при обеспечении безопасности	6.3.2	—	M2	12	—	10.4	—	12
3 Сообщение о нарушениях в работе программного обеспечения	6.3.3	—	M2	12	—	10.4	—	12
4 Управление в случае возникновения инцидента	8.1.3	—	M2	12	—	10.4	—	18.1.3

Таблица 8.1.4 — Персонал

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Защитные меры для штатного или временного персонала	6.1	—	3.2, M3	10.1	6.3.9, 7.3.9, 8.3.9, 9.3.9, 10.3.9, 11.3.9	9.2	4.1, 2.2	10.1
2 Защитные меры для персонала, нанятого по контракту	6.1	—	—	10.3	6.3.9, 7.3.9, 8.3.9, 9.3.9, 10.3.9, 11.3.9	9.2	4.1, 2.2	10.3
3 Обучение и осведомленность о мерах безопасности	6.2	—	1.2, M3	13, 10.1.4	6.3.9, 7.3.9, 8.3.9, 9.3.9, 10.3.9, 11.3.9	9.1	4.2, 2.2	13, 10.1.4
4 Процесс обеспечения исполнительской дисциплины	6.3.4	—	3.2, M3	—	6.3.9, 7.3.9, 8.3.9, 9.3.9, 10.3.9, 11.3.9	9.2.6	2.2.1	13.1

Таблица 8.1.5 — Эксплуатационные вопросы

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Управление конфигурацией и изменениями	8.1, 10.5	—	—	14.3, 8.4.1	—	7.4	9	14.3, 8.4.1, 8.4.4
2 Управление резервами	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 Техническое обслуживание	7.2.4	—	М2	14.7	6.3.6, 7.3.6, 8.3.6, 9.3.6, 10.3.6, 11.3.6	8.1.4, 8.10.5, 10.1	6.5	14.7
5 Мониторинг изменений, связанных с безопасностью	—	—	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 Записи аудита и регистрация	8.4	—	М2	18	—	7.3, 8.1.8, 8.2.10, 8.9.5	6.7	(18)
7 Тестирование безопасности	—	—	М2	8.4.3	—	8.3.5	6.7, 3	8.4.3
8 Управление носителями информации	8.6	—	8, М2	14.5	6.3.5, 7.3.5, 8.3.5, 9.3.5, 10 3.5, 11 3 5	8.4—8.14	5	14.5
9 Обеспечение стирания памяти	—	—	М4	—	—	8.1.9	6.3, 5	14.5.7
10 Распределение ответственности и полномочий	8.1.4	—	М2	—	—	—	—	10.1.1
11 Корректное использование программного обеспечения	12.1.2	—	М2	—	6.3.8, 7.3.8, 8.3.8, 9.3.8, 10 3.8, 11 3 8	8.3	6.3	14.2
12 Управление изменениями программного обеспечения	10.5.1, 10.5.3	—	М2	—	6.3.8, 7.3.8, 8.3.8, 9.3.8, 10.3.8, 11.3.8	8.3.7	6.3	8.4.4, 14.2

Таблица 8.1.6 — Планирование непрерывности бизнеса

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Стратегия непрерывности бизнеса	11.1.1, 11.1.2	—	3.3, М6	10.2, 11.3, 11.4	6.3.3, 7.3.3, 8.3.3, 9.3.3, 10 3.3, 11 3 3	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 непрерывности бизнеса	11.1.3, 11.1.4	—	3.3, М6	11.5	6.3.3, 7.3.3, 8.3.3, 9.3.3, 10.3.3, 11.3 3		—	11.5
3 Проверка и актуализация плана непрерывности бизнеса	11.1.5	—	3.3, М6	11.6	6.3.3, 7.3.3, 8.3.3, 9.3.3, 10 3.3, 11.3 3		—	11.6
4 Дублирование	8.4.1	—	3.4	14.4	6.3.2.4, 7.3.2.4, 8.3.2.4, 9.3.2.4, 10 3.2.4, 11 3.2.4	—	7.1, 7.2	14.4

Таблица 8.1.7 — Физическая безопасность

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Материальная защита	7.1	—	4.1, 4.3, M1	15.1	6.3.1.2, 7.3.1.2, 8.3.1.2, 9.3.1.2, 10.3.1.2, 11.3.1.2	8.1.1, 8.6.2, 8.9.1	3.1, 3.4, 4	15.1
2 Противопожарная защита	7.2.1	—	—	15.2	6.3.1.4, 7.3.1.4, 8.3.1.4, 9.3.1.4, 10.3.1.4, 11.3.1.4	8.1.1, 8.6.2, 8.9.1	3.1, 3.2, 7.5	15.2
3 Защита от воды/других жидкостей	7.2.1	—	M2	15.5	6.3.1.4, 7.3.1.4, 8.3.1.4, 9.3.1.4, 10.3.1.4, 11.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.5
4 Защита от стихийных бедствий	7.2.1	—	M2	15.4	6.3.1.4, 7.3.1.4, 8.3.1.4, 9.3.1.4, 10.3.1.4, 11.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.4
5 Защита от хищения	7.1	—	1.2	15.1	6.3.1.3, 7.3.1.3, 8.3.1.3, 9.3.1.3, 10.3.1.3, 11.3.1.3	8.1.1, 8.6.2, 8.9.1	3.3, 3.4, 4	15.1
6 Энергоснабжение и вентиляция	7.2.2	—	M2	15.6	6.3.4, 7.3.4, 8.3.4, 9.3.4, 10.3.4, 11.3.4	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

8.2 Специальные защитные меры систем ИТ

Источники дополнительной информации по упомянутым категориям защитных мер приведены в таблицах 8.2.1—8.2.5.

8.2.1 Идентификация и аутентификация

Идентификация является средством, с помощью которого пользователь представляет заявленный идентификатор в систему. Аутентификация является средством валидации действительности этого заявления. Ниже приведены примеры достижения идентификации и аутентификации (ИА) (существуют также другие классификации ИА):

1 Идентификация и аутентификация на основе некоторой информации, известной пользователю

Наиболее типичным способом идентификации и аутентификации является назначение паролей. Пароль — это отличительная характеристика, связанная с процессом распознавания, и представляющая собой некоторую информацию, которая может быть доступна только пользователю. Организация должна управлять распределением и периодической сменой паролей. 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, организация может ограничить использование обычных паролей или рисунков и символов. При необходимости организация может создавать копии паролей, которые должны надежно сохраняться. Доступ к копиям паролей пользователей, не имеющих или забывших пароль, должен быть регламентирован. Идентификация и аутентификация на основе некоторой информации, известной пользователю, может использовать способы криптографии и протоколы распознавания. Этот тип распознавания и подтверждения может также применяться для дистанционной идентификации и аутентификации.

2 Идентификация и аутентификация на основе того, чем владеет пользователь

Для целей идентификации и аутентификации могут использоваться некоторые объекты, которыми владеет пользователь, например это могут быть карточки (жетоны) с запоминающим устройством (ЗУ) или микропроцессором. Общепринятое применение имеют кредитные карточки с магнитным запоминающим устройством на обратной стороне. Аутентификация обеспечивается на основе комбинации двух факторов: фактора обладания пользователем неким объектом, (например, карточкой, смарт-картой) и фактора знания пользователем некоторой информации (персонального идентификационного номера — PIN кода). Типичным примером является карточка с микропроцессором.

3 Идентификация и аутентификация на основе использования биометрических характеристик пользователя

Технологии биометрической аутентификации используют отличительные характеристики и атрибуты индивидуального распознавания личности. Это могут быть отпечатки пальцев, геометрия ладони, сетчатка глаз, а также тембр голоса и личная подпись. Данные биометрического профиля пользователя должны надежно храниться в защищенной памяти смарт-карты или в системе.

8.2.2 Логическое управление и аудит доступа

Защитные меры в этой категории применяются для:

- ограничения доступа к информации, компьютерам, сетям, приложениям, системным ресурсам, файлам и программам;

- регистрации подробного описания ошибок и действий пользователя в следе аудита и при анализе записей для обнаружения и исправления нарушений при обеспечении безопасности.

Общепринятым средством усиления управления доступом является использование особенностей идентификации и аутентификации, включенных в списки управления доступом, которые определяют, какие файлы, ресурсы и т. д. разрешены для доступа пользователя и какие формы может принимать этот доступ. К этой категории защитных мер относятся:

1 Политика управления доступом

Для каждого пользователя или группы пользователей организация должна установить однозначно определенную политику управления доступом. Эта политика устанавливает права доступа в соответствии с требованиями бизнеса, например принципы доступности, производительности и осведомленности. Организация должна 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 Управление доступом пользователя к ЭВМ

Управление доступом к ЭВМ применяется для предупреждения несанкционированного доступа к компьютеру. Организация должна обеспечивать возможность распознавания и идентификации личности каж-

дого авторизованного пользователя, как при успешной, так и неудачной попытке осуществить регистрацию. Управление компьютерным доступом может быть облегчено с помощью паролей или другого метода идентификации и аутентификации.

3 Управление доступом пользователя к данным, услугам и приложениям

Управление доступом должно применяться для защиты данных и услуг в компьютере или в сети от несанкционированного проникновения. Это может быть достигнуто с помощью соответствующих механизмов идентификации и аутентификации (см. 8.2.1), интерфейсов между сетевыми услугами и конфигурацией сети, обеспечивающей только санкционированный доступ к услугам ИТ (ограниченное распределение прав). Для предупреждения несанкционированного доступа к приложениям, организация должна управлять доступом на основе функциональной роли пользователя в организации.

4 Анализ и актуализация прав доступа

Организация должна проводить периодический анализ и актуализацию всех прав доступа, предоставленных пользователю, если изменились требования к обеспечению безопасности. Права привилегированного доступа для управления их правильным использованием должны чаще анализироваться. Доступ должен быть отменен немедленно, если он больше не нужен.

5 Контрольные журналы

Работы с помощью ИТ должны регистрироваться, а контрольные журналы должны периодически просматриваться для установления успешных и неудачных попыток войти в систему, получить доступ к данным, функциям используемой системы и т. д. Неисправности также должны регистрироваться и периодически анализироваться. Полученные данные должны применяться в соответствии с законодательством по защите данных и конфиденциальности, например, их можно хранить только в течение ограниченного периода времени и использовать только для обнаружения нарушений безопасности.

8.2.3 Защита от злонамеренных кодов

Злонамеренные коды могут проникать в систему через внешние соединения и/или файлы и программное обеспечение, установленные с помощью переносных дисков. Злонамеренные коды могут оставаться необнаруженными до выявления их вредного воздействия, если не реализованы соответствующие защитные меры. Злонамеренные коды могут подрывать защитные меры (например перехватывать и раскрывать пароли), случайно раскрывать или изменять информацию, нарушать целостность системы, уничтожать информацию и использовать без разрешения ресурсы системы. Злонамеренные коды могут быть следующих типов:

- вирусы;
- черви;
- троянские кони.

Носителями злонамеренных кодов являются:

- исполняемое программное обеспечение;
- файлы данных (содержащие исполняемые макроопределения, например, документы по электронной обработке текста или крупноформатные таблицы);
- активное содержание страниц Интернета (WWW).

Злонамеренные коды могут распространяться через:

- гибкие диски;
- другие съемные носители;
- электронную почту;
- сети;
- загрузку.

Злонамеренные коды могут быть внесены в результате преднамеренных действий пользователя или путем взаимодействий на системном уровне, которые пользователь может не видеть. Защита от злонамеренного кода может быть достигнута путем использования ниже перечисленных защитных мер:

1 Сканеры

Различные формы злонамеренного кода могут быть обнаружены и удалены путем специального сканирующего программного обеспечения и проверок на целостность. Сканеры могут работать в автономном режиме или под управлением центрального процессора. Работа сканера в режиме «онлайн» обеспечивает активную защиту, т. е. обнаружение (и возможное удаление) злонамеренного кода до распространения заражения и нанесения ущерба системе ИТ. Рекомендуется использовать сканеры, работающие по принципу фильтрации содержимого сетевых протоколов, для автономных компьютеров и рабочих станций, серверов файлов, серверов электронной почты и средств межсетевой защиты. Однако пользователи и адми-

нистраторы должны понимать, что нельзя полагаться на сканеры для обнаружения всех злонамеренных кодов (даже установленного типа), потому что новые формы злонамеренных кодов возникают непрерывно.

2 Проверки целостности

Обычно для усиления защиты, обеспечиваемой сканерами, требуются другие защитные меры. Например для проверки изменений, внесенных в программу, можно использовать контрольные суммы. Программное обеспечение целостности должно быть неотъемлемой частью технических защитных мер, обеспечивающих защиту от злонамеренного кода. Этот технический прием может быть использован для файлов данных и программ, не имеющих статуса информации для дальнейшего применения.

3 Управление обращением съемных носителей

Неконтролируемое обращение носителей (особенно дискет) может привести к увеличению риска внедрения злонамеренного кода в системы ИТ организации. Управление обращением в среде передач информации может быть достигнуто путем использования:

- специального программного обеспечения;
- процедур организации по защитным мерам (см. ниже).

4 Процедуры организации по защитным мерам

Организация должна разработать руководящие указания для пользователей и администраторов, определяющие процедуры и практические действия для минимизации возможности внесения злонамеренного кода. Такие процедуры должны охватывать загрузку игр и другого исполняемого программного обеспечения, использование разных типов услуг в сети Интернет и импортируемые файлы разных типов. При необходимости должен быть проведен независимый анализ источника или исполнительного кода. Обучение и дисциплинарные действия должны проводиться на рабочем месте для того, чтобы персонал соблюдал документированные процедуры и выполнял необходимые действия для предупреждения злонамеренных кодов.

8.2.4 Управление сетью

Управление сетью включает в себя планирование, эксплуатацию и администрирование сетей. Выбор правильной конфигурации и форм администрирования сетей являются эффективными средствами снижения уровня риска. В настоящее время разрабатываются несколько документов ИСО, содержащих дополнительную информацию о защитных для обеспечения безопасности сети. К этой категории относятся следующие защитные меры:

1 Операционные процедуры

Установление операционных процедур и распределение ответственности необходимо для обеспечения правильной и безопасной работы сетей. К ним относится документация операционных процедур и установление порядка действий для реагирования на значительные инциденты безопасности (см. 8.1.3).

2 Системное планирование

Для обеспечения надежного функционирования и адекватной пропускной способности сети должно проводиться перспективное планирование и подготовка, а также текущий мониторинг (включая загрузочные статистики). Должны применяться критерии приемки новых систем, управлять и реагировать на изменения (см. также 8.1.5).

3 Конфигурация сети

Соответствующая конфигурация сети является важным фактором ее функционирования. Организация должна разработать стандартизованный подход для конфигурации всех своих серверов и обеспечить качественную сопроводительную документацию. Затем должно быть обеспечено применение серверов только для специальных целей (например, никакие другие задачи не должны решаться средствами межсетевой защиты) и достаточная защита от неисправностей.

4 Разделение сетей

Для сведения к минимуму риска и возможностей неправильного использования сети в работе, должны быть логически и физически разделены сети, связанные с различными областями бизнеса. Кроме того, средства разработки должны быть отделены от эксплуатационного оборудования.

5 Мониторинг сети

Мониторинг сети должен использоваться для выявления слабых мест в конфигурации существующей сети, что позволяет вносить изменения в конфигурацию, вызванные анализом трафика, и помогает идентифицировать взломщиков сети.

6 Обнаружение вторжения

Попытки получить доступ в систему или сеть и успешный несанкционированный вход должны быть выявлены для проведения организацией соответствующих корректирующих действий.

8.2.5 Криптография

Криптография, то есть математический способ преобразования данных для обеспечения безопасности, может применяться для многих различных целей обеспечения безопасности ИТ, (например, криптография помогает обеспечивать конфиденциальность и/или целостность данных, неотказуемость, и применяет передовые методы идентификации и аутентификации). В случае применения криптографии следует обращать внимание на соблюдение законодательных и обязательных требований. Одним из наиболее важных аспектов криптографии является адекватная система управления ключами, подробно рассмотренная в ИСО/МЭК 11770-1. Дополнительная информация о классификации криптографических приложений приведена в приложении С ИСО/МЭК 11770-1. Использование криптографии в идентификации и аутентификации рассматривается в 8.2.1. Программные средства обеспечения даты/времени могут быть использованы для поддержки применения криптографических защитных мер. Ниже рассматриваются разные пути использования криптографии:

1 Защита конфиденциальности данных

Если важно сохранение конфиденциальности данных, например в случае особенно конфиденциальной информации, должны применяться защитные меры в виде шифрования информации для хранения и ее передачи по сетям. Решение о применении шифрования должно приниматься с учетом:

- соответствующих законодательных и обязательных требований;
- требований, установленных при управлении ключами и трудностей, которые придется преодолевать для обеспечения действительного улучшения безопасности без создания новых уязвимостей;
- пригодности соответствующих технических средств шифрования, используемых для ситуации развертывания и требуемого уровня защиты.

2 Защита целостности данных

Для защиты информации в памяти или предназначенной для передачи и сохранения целостности хранимых или обрабатываемых данных должны быть применены хэш-функции, цифровые подписи и/или другие защитные меры по обеспечению целостности. Защитные меры по обеспечению целостности данных (например использование так называемых кодов аутентификации сообщений) предоставляют защиту от случайного или намеренного изменения содержания, добавления или исключения информации. Цифровые подписи могут обеспечивать не только подобную защиту целостности сообщений, но имеют свойства, позволяющие делать невозможным изменение смысла передаваемой информации. Решение использовать цифровые подписи и другие защитные меры целостности должны быть приняты с учетом:

- соответствующих законодательных и обязательных требований;
- инфраструктуры открытых ключей;
- требований к управлению ключами и трудностей, которые придется преодолевать для реального усовершенствования безопасности без создания новых уязвимостей.

3 Неотказуемость

Методы криптографии (например на основе использования цифровых подписей) могут быть применены для подтверждения отправки, передачи, доставки, уведомления о приеме, например сообщений или протоколов связи.

4 Аутентичность данных

Для обеспечения аутентичности данных, организация может использовать цифровую подпись для подтверждения подлинности данных. Такая необходимость может возникнуть при ссылке на данные источников третьей стороны или если в точности справочных данных заинтересована большая группа лиц. Для подтверждения того, что данные поступают от определенного лица могут также применяться цифровые подписи.

5 Управление ключами

Управление ключами включает в себя технические, организационные и процедурные аспекты, необходимые для поддержки любого способа криптографии. Задачей управления ключами является надежное администрирование и менеджмент криптографическими ключами и связанной с этим информацией. Управление ключами включает в себя: генерирование, регистрацию, сертификацию, распределение, установку, хранение, архивирование, отмену, извлечение и уничтожение ключей. Кроме того, важно правильно разработать процедуру управления ключами для снижения риска дискредитации ключей и их использование неуполномоченными лицами. Процедуры управления ключами зависят от применяемого алгоритма, использования ключа по назначению и политики обеспечения безопасности. Более подробно управление ключами рассмотрено в ИСО/МЭК 11770-1.

Таблица 8.2.1 — Идентификация и аутентификация

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 ИА на основе некоторой информации, известной пользователю	9.2.3, 9.3.1, 9.4, 9.5.1	4.2.1, 5.2.1, приложение А	М4	16.1	6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1	7.2.1, 7.2.2	6.2	16.1
2 Идентификация и аутентификация на основе того, чем владеет пользователь			—	16.2	6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1		6.2	16.2
3 Идентификация и аутентификация на основе использования биометрических характеристик пользователя			—	16.3	6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1		6.2	16.3

Таблица 8.2.2 — Логическое управление и аудит доступа

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Политика управления доступом	9.1	—	М2	17.1, 17.2, 17.3	6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1	7.2, 8.1.2, 8.2.2, 8.4.1	6.4	17.1, 17.2, 17.3
2 Управление доступом пользователя к ЭВМ	9.2, 9.3, 9.5	4.2.4, 5.2.4, приложение А	М4		6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1		6.2, 3.3	
3 Управление доступом пользователя к данным, услугам и приложениям	9.4, 9.6		М4		6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1		6.4	
4 Анализ и актуализация прав доступа	9.1, 9.2.4	—	М2	17.4	6.3.2.1, 7.3.2.1, 8.3.2.1, 9.3.2.1, 10.3.2.1, 11.3.2.1		—	17.4
5 Контрольные журналы	9.7	—	М4	18	6.3.2.2, 7.3.2.2, 8.3.2.2, 9.3.2.2, 10.3.2.2, 11.3.2.2	7.3, 8.2.10	6.7	18

Таблица 8.2.3 — Защита от злонамеренных кодов

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Сканеры	8.3	—	М4	—	6.3.10, 7.3.10, 8.3.10, 9.3.10, 10.3.10, 11.3.10	8.3.11, 8.3.16	7.4	4.6, 5.2.1, 6.4, 8.4.4, 11
2 Проверки целостности	8.3	—	М4	—	—	8.3.11, 8.3.16	7.4	—
3 Управление обращением съемных носителей	7.3.2	—	—	—	—	—	—	—
4 Процедуры организации по защитным мерам	8.3	—	М4	—	6.3.10, 7.3.10, 8.3.10, 9.3.10, 10.3.10, 11.3.10	8.3.11, 8.3.16	7.4	6.2.2, 9.3, 12, 14.2

Таблица 8.2.4 — Управление сетью

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Операционные процедуры	8.5.1	—	М2	—	—	8.2, 8.3	8.2	14.6
2 Системное планирование	8.2	—	М2, М4	8.4	—		6.1	8.4
3 Конфигурация сети	—	—	М4	—	—		9, 6.1	14.3
4 Разделение сетей	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 8.2.5 — Криптография

Категории защитных мер	Источники дополнительной информации о категориях защитных мер							
	Разделы и пункты [1]	Разделы и пункты [3]	Разделы и пункты [4]	Разделы и пункты [5]	Разделы и пункты [6]	Разделы и пункты [7]	Разделы и пункты [8]	Разделы и пункты [9]
1 Защита конфиденциальности данных	10.3.2	4.2.2, 5.2.2, приложение А	М4	19.5.1	—	8.23	8.1	19.5.1
2 Защита 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	—	19.5.3	—	8.23	8.1	19.2.3
4 Аутентичность 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

9 Базовый подход: выбор защитных мер согласно типу системы ИТ

В соответствии с разделом 8 имеются два разных пакета защитных мер, механизмов и/или процедур, применяемых для защиты системы ИТ. С одной стороны, существуют лишь несколько категорий организационных защитных мер, применяемых для каждой системы ИТ в конкретной ситуации (см. 8.1), независимо от индивидуальных компонентов. Выбор защитных мер рассматривается в 9.1. Так как организация обычно применяет защитные меры из этих категорий, их необходимо рассматривать в первую очередь. Более того, большинство защитных мер являются дорогостоящими, так как они обычно основаны на внедрении организационных структур и процедур.

С другой стороны, имеются специальные защитные меры систем ИТ (см. 8.2), выбор которых зависит от типа и характеристик рассматриваемой системы ИТ. Выбор таких защитных мер рассматривается в 9.2.

Возможно, что одна или более из этих категорий или специальных защитных мер не применимы к системе ИТ. Например, шифрование может не потребоваться, если передаваемая или принимаемая информация не нуждается в конфиденциальности, а целостность данных может быть проверена иначе. Более детальный выбор может быть сделан только после рассмотрения дополнительной информации (см. разделы 10 и 11).

После того как все типы безопасности, применимые для системы ИТ, идентифицированы, дополнительная информация по ним и специальным защитным мерам может быть получена в соответствии с разделом 8 или использованием одного или более документов, перечисленных в приложениях А — Н. Взаимосвязь категорий защитных мер с типом системы ИТ приведена в таблице 9.2. Перед реализацией выбранных защитных мер они должны быть внимательно проверены с существующей и/или планируемой защитой (см. 7.3).

Для выбора дополнительных защитных мер должен быть применен более детальный их анализ (см. разделы 10 и/или 11). Если защитные меры выбирают по разным критериям (базовые защитные меры и дополнительная защита), то окончательный пакет защитных мер должен быть согласован. После анализа нескольких систем ИТ должна быть рассмотрена возможность развертывания базовой безопасности в масштабе всей организации (см. раздел 12).

Другой возможностью выбора защитных мер без детального рассмотрения этой проблемы является применение прикладной специальной базовой безопасности, например с использованием справочников по базовой защите для электросвязи, здравоохранения, банковской системы (см. приложения В, Е и F) и т. д.

При использовании этих справочников можно, например, сравнивать существующие или планируемые защитные меры с рекомендуемыми. Однако при выборе защитных мер, которые должны быть внедрены, полезно внимательно рассмотреть потребности и соображения организации, связанные с обеспечением безопасности.

9.1 Обычно применяемые защитные меры

Обычно применяются следующие категории защитных мер:

- политика и управление безопасностью ИТ (см. 8.1.1);
- проверка соответствия безопасности установленным требованиям (см. 8.1.2);
- обработка инцидента (см. 8.1.3);
- персонал (см. 8.1.4);
- эксплуатационные вопросы (см. 8.1.5);
- планирование непрерывности бизнеса (см. 8.1.6);

Таблица 9.2 — Алгоритм выбора специальных защитных мер системы ИТ

Социальные защитные меры	Автономная рабочая станция	Подсоединенное к сети АРМ (клиент без разделяемых ресурсов)	Подсоединенные к сети сервер или АРМ с ресурсами коллективного пользования
Идентификация и аутентификация			
Идентификация и аутентификация на основе некоторой информации, известной пользователю	·	·	·
Идентификация и аутентификация на основе того, чем владеет пользователь	·	·	·
Идентификация и аутентификация на основе использования биометрических характеристик пользователя	(·)	(·)	(·)
Логическое управление и аудит доступа			
Политика управления доступом			
Управление доступом пользователя к ЭВМ	·	·	·
Управление доступом пользователя к данным, услугам и приложениям	·	·	·
Анализ и актуализация прав доступа			
Контрольные журналы	·	·	·
Злонамеренные коды			
Сканеры	·	·	·
Проверки целостности	·	·	·
Контроль обращения съемных носителей	·	·	·
Административные защитные меры	·	·	·
Управление сетью			
Операционные процедуры			·
Системное планирование			·
Конфигурация сети			·
Разделение сетей			·
Мониторинг сети			·
Обнаружение вторжения			·
Криптография			
Защита конфиденциальности данных	(·)	(·)	(·)
Защита целостности данных	(·)	(·)	(·)
Неотказуемость		(·)	(·)
Аутентичность данных	(·)	(·)	(·)
Управление ключами	(·)	(·)	(·)

Примечание — Знак «·» означает применение защитных мер в нормальных условиях, знак «(·)» — применение защитных мер в особых условиях.

- физическая безопасность (см. 8.1.7).

Защитные меры этих категорий формируют основу для успешного управления безопасностью ИТ. В этом смысле их не следует недооценивать. Важно также обеспечить рабочее взаимодействие этих защитных мер с технической защитой, рассмотренной ниже. Деятельность организации в этой области зависит от ее потребностей обеспечения безопасности (см. раздел 10) и выделенных ресурсов.

Организация может применять и другие категории защитных мер, но способ их реализации зависит от конкретных условий (например защитные меры, обеспечивающие управление доступом к сети, отличаются от управления доступом к автономной рабочей станции).

При выборе защитных мер должны учитываться размер организации и потребности в обеспечении ее безопасности, так как они могут повлиять на степень реализации защитных мер. Например, у небольшой организации не существует ни потребности, ни необходимого персонала для создания группы по обеспечению безопасности ИТ. Тем не менее, в организации должен быть назначен ответственный за выполнение этих функций. Защитные меры, перечисленные в 8.1, должны систематизироваться всякий раз, когда это необходимо.

9.2 Специальные защитные меры систем ИТ

В дополнение к обычно применяемым защитным мерам, должны быть выбраны специальные защитные меры для каждого типа компонента системы. Алгоритм выбора специальных защитных мер системы ИТ приведен в качестве примера в таблице 9.2. В этом примере знак «·» обозначает защитные меры, которые должны быть применены в нормальных условиях, а «(·)» — защитные меры, которые могут потребоваться в особых случаях. Процесс выбора защитных мер должен быть продолжен путем рассмотрения их характеристик, представленных в 8.2. Дополнительная информация может быть получена из документов по базовой защите, перечисленных в приложениях А — Н.

10 Выбор защитных мер в соответствии с проблемами безопасности и угрозами

Выбор защитных мер в соответствии с проблемами и угрозами безопасности, изложенными в настоящем разделе, может быть использован следующим образом:

- на первом этапе должна быть проведена идентификация и оценка проблем безопасности. Организация должна рассмотреть требования по обеспечению конфиденциальности, целостности, доступности, подотчетности, аутентичности и достоверности. Прочность защиты и число выбранных защитных мер должны соответствовать оценкам проблем обеспечения безопасности;
- на втором этапе для каждой из выявленных проблем безопасности должны быть перечислены типичные угрозы и для каждой угрозы в зависимости от рассматриваемой системы ИТ должны быть предложены соответствующие защитные меры. Различные типы систем ИТ приведены в 7.1, краткий перечень защитных мер приведен в подпунктах раздела 8. В некоторых случаях у организации могут возникнуть дополнительные потребности и цели при обеспечении безопасности.

10.1 Оценка проблем безопасности

Для выбора соответствующих эффективных защитных мер организация должна исследовать и оценить проблемы безопасности, связанные с коммерческой деятельностью, которую обслуживает рассматриваемая система ИТ. После идентификации проблем безопасности и с учетом соответствующих угроз можно выбирать защитные меры согласно 10.2—10.5.

Если подобная оценка покажет необходимость высокого уровня безопасности, то рекомендуется детальный подход к решению этой проблемы. Дополнительный материал можно найти в разделе 11.

Проблемы безопасности могут включать в себя потерю:

- конфиденциальности;
- целостности;
- доступности;
- подотчетности;
- аутентичности;
- достоверности.

Оценка должна включать в себя рассматриваемую систему ИТ, хранимую или обрабатываемую в ней информацию и коммерческие операции, которые она обеспечивает. На основе этого идентифицируются задачи выбираемых защитных мер. Различные части системы ИТ или хранимой и обрабатываемой информации могут иметь различные проблемы обеспечения безопасности. Важно напрямую соотнести проблемы

безопасности с активами системы, так как это может повлиять на возможные угрозы и, как следствие, на выбор защитных мер.

Проблемы обеспечения безопасности могут быть оценены с позиции воздействия неисправностей или нарушений безопасности, которое может стать причиной серьезного или незначительного сбоя в коммерческих операциях, или не причинить никакого вреда. Например, если конфиденциальная информация организации обрабатывается в системе ИТ, то несанкционированное раскрытие этой информации конкуренту дает ему возможность сделать предложения по более низкой цене, нанося тем самым ущерб бизнесу организации. С другой стороны, если общедоступная информация обрабатывается в системе ИТ, то ее раскрытие не принесет никакого вреда. Рассмотрение возможных угроз (см. 10.2, 10.3) может помочь в выявлении проблем безопасности. Приведенные ниже оценки, должны быть сделаны отдельно для каждого актива системы, так как проблемы обеспечения безопасности для каждого актива могут быть различными. В случае, если проблемы безопасности достаточно изучены, то активы организации и соответствующие проблемы обеспечения безопасности могут быть сгруппированы.

Если система ИТ обрабатывает информацию более одного типа, то для различных типов информации может быть необходимо отдельное рассмотрение. Защита, которую в состоянии предоставить система ИТ, должна быть достаточной для всех типов обрабатываемой информации. Таким образом, если отдельная информация имеет высокий уровень проблем обеспечения безопасности, то вся система должна быть соответствующим образом защищена. В случае, если объем информации с высоким уровнем проблем безопасности небольшой, то должна быть рассмотрена возможность перевода этой информации в другую систему, если она совместима с бизнес-процессами организации.

В случае, если идентифицированы все возможные варианты потери конфиденциальности, целостности, доступности, подотчетности, аутентичности и достоверности, способные причинить незначительный ущерб, то для рассматриваемой системы ИТ должен быть применен подход начиная от пункта 10.2 и далее по тексту настоящего стандарта. В случае, если любая из идентифицированных выше потерь способна причинить серьезный ущерб организации, должна быть проведена оценка, необходимости выбора защитных мерах, предложенных дополнительно в 10.2—10.5. Предложения по более подробным оценкам и выбору защитных мер на основе результатов этих оценок приведены в ИСО/МЭК ТО 13335-3 и разделе 11 настоящего стандарта. Тем не менее в качестве базовых для более точного выбора защитных мер, должны рассматриваться защитные меры, предложенные в 10.2.

10.1.1 Потеря конфиденциальности

Организация должна рассмотреть возможный ущерб при потере конфиденциальности определенного актива(ов) (преднамеренно или случайно). Например, потеря конфиденциальности может привести к:

- потере общественного доверия или снижению ее имиджа в обществе;
- ответственности перед законом, включая ответственность за нарушение законодательства в области защиты данных;
- отрицательному влиянию на политику организации;
- созданию угрозы безопасности персонала;
- финансовым потерям.

Рассмотрев вышеперечисленные возможные виды потери конфиденциальности, организация должна принять решение о том, будет ли общий ущерб от потери конфиденциальности серьезным, незначительным или не будет никакого ущерба. Принятое решение должно быть документировано.

10.1.2 Потеря целостности

Организация должна рассмотреть возможный ущерб при потере целостности определенного актива(ов) (преднамеренно или случайно). Например, потеря целостности может привести к следующим последствиям:

- принятию неправильных решений;
- обману;
- прерыванию коммерческих операций организации;
- потере общественного доверия или снижению общественного имиджа организации;
- финансовым потерям;
- ответственности перед законом, включая ответственность за нарушение законодательства в области защиты данных.

Рассмотрев вышеперечисленные последствия потери целостности, организация должна принять решение о том, будет ли общий ущерб от потери целостности серьезным, незначительным или не будет никакого ущерба. Принятое решение должно быть задокументировано.

10.1.3 Потеря доступности (готовности)

Организация должна рассмотреть возможный ущерб при кратковременной потере доступности приложения или информации, т. е. рассмотреть прерывание каких коммерческих операций возможно приведет к несоблюдению времени их завершения из-за недоступности приложений или информации. Должны быть также рассмотрены чрезвычайные формы потери доступности, постоянную потерю данных и/или физическое повреждение аппаратных и программных средств. Например, потеря доступности может привести к следующим последствиям:

- принятию неправильных решений;
- неспособности выполнять важные поставленные задачи;
- потере общественного доверия или снижению общественного имиджа организации;
- финансовым потерям;
- ответственности перед законом, включая ответственность за нарушение законодательства в области защиты данных и невыполнения договоров в установленные сроки;
- большим затратам на восстановление.

Ущерб от потери доступности может значительно колебаться для разных периодов подобной потери. Желательно рассмотреть все потери, которые могут возникнуть в разные периоды времени, и оценить ущерб для каждого периода как серьезный, незначительный или как отсутствие ущерба. Эта информация должна быть использована при выборе защитных мер.

Рассмотрев вышеперечисленные последствия потери доступности, организация должна принять решение о том, будет ли общий ущерб от потери доступности серьезным, незначительным или не будет никакого ущерба. Принятое решение должно быть задокументировано.

10.1.4 Потеря подотчетности

Организация должна рассмотреть возможный ущерб при потере подотчетности пользователей системы или субъектов (например, программного обеспечения), действующих от имени пользователя. В этом пункте должны быть рассмотрены автоматически генерируемые сообщения, которые могут стать причиной возникновения инцидента. Например, потеря подотчетности может привести к следующим последствиям:

- манипулированию системой со стороны пользователей;
- обману;
- промышленному шпионажу;
- неконтролируемым действиям;
- ложным обвинениям;
- ответственности перед законом, включая ответственность за нарушение национального законодательства РФ в области защиты данных.

Рассмотрев вышеперечисленные последствия потери подотчетности, организация должна принять решение о том, будет ли общий ущерб от потери подотчетности серьезным, незначительным или не будет никакого ущерба. Принятое решение должно быть задокументировано.

10.1.5 Потеря аутентичности

Организация должна рассмотреть возможный ущерб при потере аутентичности 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. Потеря аутентичности может привести к следующим последствиям:

- обману;
- использованию достоверных процессов с недостоверными данными (что может привести к результату, вводящему в заблуждение);
- манипулированию организацией извне;
- промышленному шпионажу;
- ложным обвинениям;
- ответственности перед законом, включая ответственность за нарушение национального законодательства РФ в области защиты данных.

Рассмотрев вышеперечисленные последствия потери аутентичности, организация должна принять решение о том, будет ли общий ущерб от потери аутентичности серьезным, незначительным или не будет никакого ущерба. Принятое решение должно быть задокументировано.

10.1.6 Потеря достоверности

Организация должна рассмотреть возможный ущерб при потере достоверности систем. Это также важно в отношении функциональности, которая является вторичной характеристикой достоверности (см. ИСО/МЭК 9126). Например, потеря достоверности может привести к следующим последствиям:

- обману;
- потере доли рынка;
- снижению мотивации в работе персонала организации;
- ненадежным поставщикам;
- снижению доверия покупателей;
- ответственности перед законом, включая ответственность за нарушение законодательства в области защиты данных.

Рассмотрев вышеперечисленные последствия потери достоверности, организация должна принять решение о том, будет ли общий ущерб от потери достоверности серьезным, незначительным или не будет никакого ущерба. Принятое решение должно быть задокументировано.

10.2 Защитные меры для обеспечения конфиденциальности

В данном разделе перечислены защитные меры от предполагаемых угроз, связанных с нарушением конфиденциальности. Кроме того, приведены соответствующие ссылки на защитные меры, в соответствии с разделом 8. Если эти защитные меры подходят при выборе защитных мер, то следует принять во внимание тип и характеристики системы ИТ.

Большинство защитных мер, перечисленных в 8.1, обеспечивают более общую защиту, т. е. направлены на ряд угроз, и предоставляют защиту путем поддержки общего эффективного менеджмента безопасности ИТ. Настоящий стандарт не содержит подробного перечисления защитных мер, но их действие не должно быть недооценено и они должны быть реализованы для общей эффективной безопасности.

10.2.1 Подслушивание

Одним из способов получения доступа к конфиденциальной информации является подслушивание, например путем подключения к линии и прослушивания телефонного разговора. Защитные меры от этой угрозы включают в себя:

- физическую защиту.

Защита может включать в себя помещения, стены, здания и т. д., которые делают подслушивание невозможным или маловероятным. Другой способ защиты заключается в добавлении шумов. Этот способ защиты подробно не рассматривается в разделе 8. Для обеспечения безопасности телефонов от подслушивания в качестве защитной меры может использоваться надлежащая прокладка кабелей. Этот вопрос подробно изложен в ИСО/МЭК ТО 13335-5;

- политику обеспечения безопасности.

Другой способ избежать подслушивания заключается в установлении строгих правил, определяющих когда, где и каким образом следует обмениваться конфиденциальной информацией;

- сохранение конфиденциальности данных.

Еще одним способом защиты от подслушивания является шифрование сообщений перед сеансом обмена данными. Более подробно этот способ изложен в 8.2.5.

10.2.2 Электромагнитное излучение

Электромагнитное излучение может использовать взломщик для получения сведений об информации, обрабатываемой в системе ИТ. Защитные меры от электромагнитного излучения включают в себя:

- физическую защиту.

Физическая защита может включать в себя наружную обшивку помещений, стен и т. д., не позволяющую электромагнитному излучению выходить за ее пределы. Этот способ защиты подробно не рассматривается в 8.1.7, так как это не самый дешевый способ защиты от электромагнитного излучения;

- сохранение конфиденциальности данных.

Более подробную информацию см. в 8.2.5. Следует отметить, что сохранение конфиденциальности данных применимо к шифрованной информации, но не к информации на этапе обработки, отображения или распечатки;

- использование оборудования ИТ с малым уровнем излучения.

Использование оборудования ИТ с малым уровнем излучения не рассматривается подробно в разделе 8, однако для защиты организация может приобрести оборудование, имеющее встроенные средства защиты от электромагнитного излучения.

10.2.3 Злонамеренные коды

Злонамеренный код может привести к утрате конфиденциальности, например путем перехвата и/или раскрытия паролей. Защитные меры от этой угрозы включают в себя:

- защиту от злонамеренного кода.

Подробное описание защиты от злонамеренного кода изложено в 8.2.3;

- обработку инцидента.

Своевременный отчет о любых инцидентах может ограничить ущерб от злонамеренных атак. Обнаружение вторжения может использоваться для пресечения попыток проникновения в систему или сеть. Дополнительную информацию см. в 8.1.3.

10.2.4 Подделка под идентификатор законного пользователя

Подделка под идентификатор законного пользователя может быть использована для того, чтобы обойти аутентификацию и связанные с ней услуги и функции обеспечения безопасности. Это может привести к нарушению конфиденциальности всякий раз, когда такая подделка обеспечивает доступ к конфиденциальной информации. Защитные меры от этой угрозы включают в себя:

- идентификацию и аутентификацию.

Подделка под личность законного пользователя затрудняется, если защитные меры идентификации и аутентификации основаны на комбинации того, что известно пользователю, или того, чем он владеет, или присущих только ему характеристиках (см. 8.2.1);

- логическое управление и аудит доступа.

Логическое управление доступом не способно делать различие между санкционированным пользователем и кем-либо, маскирующимся под санкционированного пользователя, но применение механизмов управления доступом на рабочем месте может уменьшить зону воздействия (см. 8.2.2). Рассмотрение и анализ контрольных журналов регистрации позволит обнаружить несанкционированные действия;

- защиту от злонамеренного кода.

Так как один из способов получения паролей связан с внедрением злонамеренного кода для их перехвата, то следует установить местную защиту от таких программ (см. 8.2.3);

- управление сетью.

Другим способом захвата секретного материала является подделка под законного пользователя в трафике, например электронной почте. В настоящее время международная организация по стандартизации (ИСО) разрабатывает несколько документов, содержащих дополнительную информацию о подробных защитных мерах по обеспечению безопасности сетей;

- сохранение конфиденциальности данных.

Если по какой-либо причине упомянутый выше способ обеспечения безопасности невозможен или недостаточен, то дополнительная защита может быть обеспечена путем хранения конфиденциальных данных в зашифрованном виде (см. 8.2.5).

10.2.5 Направление сообщений по ошибочному/другому маршруту

Ошибочный маршрут — это преднамеренное или случайное неправильное направление сообщений, а изменение маршрута может преследовать позитивные и деструктивные цели. Изменение маршрута сообщений может быть, например, сделано для поддержания непрерывности готовности к работе. Направление сообщений по ошибочному/другому маршруту может привести к потере конфиденциальности, если оно допускает несанкционированный доступ к этим сообщениям. Защитные меры от этой угрозы включают в себя:

- управление сетью.

Описание способов защиты от направлений сообщений по ошибочному/другому маршруту будет приведена в других документах ИСО, находящихся на стадии разработки. В них будет содержаться дополнительная информация по обеспечению безопасности сети;

- сохранение конфиденциальности данных.

Для недопущения несанкционированного доступа в случае ошибочного или измененного направления сообщений они могут быть зашифрованы. Дополнительную информацию см. в 8.2.5.

10.2.6 Сбои программного обеспечения

Сбои программного обеспечения ставят под угрозу сохранение конфиденциальности, если программное обеспечение обеспечивает, например управление доступом или шифрование, или если сбой программного обеспечения создает брешь, например в операционной системе. Защитные меры по сохранению конфиденциальности включают в себя:

- обработку инцидента.

Каждый, кто замечает неправильное функционирование программного обеспечения, обязан сообщить об этом ответственному лицу с тем, чтобы можно было как можно быстрее предпринять соответствующие корректирующие и предупреждающие действия. Дополнительную информацию см. в 8.1.3;

- эксплуатационные вопросы.

Некоторых сбоев программного обеспечения можно избежать путем его тестирования перед использованием или управления изменениями программного обеспечения (см. 8.1.5).

10.2.7 Хищение

Хищение может угрожать сохранению конфиденциальности, если украденный компонент содержит конфиденциальную информацию, которая может оказаться доступной. Защитные меры против хищения включают в себя:

- физическую защиту.

Это может быть техническая защита, затрудняющая доступ в здание, зону или помещение с оборудованием ИТ, или специальные защитные меры от хищения (см. 8.1.7);

- персонал.

Защитные меры для персонала (управление доступом персонала и/или посторонних лиц, соглашения о сохранении конфиденциальности и т. д.) должны поддерживаться в рабочем состоянии, затрудняя возможность хищения (см. 8.1.4);

- сохранение конфиденциальности данных.

Такую защиту следует внедрить, если существует вероятность хищения оборудования ИТ, содержащего конфиденциальную информацию, например небольшой портативный компьютер. Подробности см. в 8.2.5;

- средства контроля носителей информации.

Любые носители информации, содержащие секретные материалы, должны охраняться от хищения (см. 8.1.5).

10.2.8 Несанкционированный доступ к компьютерам, данным, услугам и приложениям

Несанкционированный доступ к компьютерам, данным, услугам и приложениям может стать угрозой, если возможен доступ к любому секретному материалу. Защитные меры от несанкционированного доступа включают в себя соответствующее опознавание и проверку регистрации, логическое управление доступом, аудит на уровне системы ИТ и разделение сетей на сетевом уровне:

- идентификацию и аутентификацию.

Защитные меры путем соответствующего опознавания и проверки регистрации следует использовать в комбинации с логическим управлением доступом для предупреждения несанкционированного доступа;

- логическое управление и аудит доступа.

Защитные меры, изложенные в 8.2.2, должны использоваться для логического управления доступом через использование механизмов управления доступом. Рассмотрение и анализ контрольных журналов регистрации позволяет обнаруживать несанкционированные виды деятельности пользователей с правами доступа в систему;

- разделение сетей.

Для затруднения несанкционированного доступа, должно применяться местное разделение сетей (см. 8.2.4);

- физическое управление доступом.

Кроме логического, может применяться физическое управление доступом;

- управление носителями данных.

Если конфиденциальная информация хранится на портативных или иных носителях (например на дискетах), то организация должна установить местное управление носителями данных для их защиты от несанкционированного доступа;

- сохранение конфиденциальности данных.

Если по какой-либо причине управление носителями данных невозможно или недостаточно, то дополнительная защита может обеспечиваться путем хранения конфиденциальных данных в зашифрованном виде (см. 8.2.5).

10.2.9 Несанкционированный доступ к месту хранения носителей информации

Доступ к месту хранения и использование носителей информации без соответствующих полномочий угрожают конфиденциальности, если в этой среде хранятся секретные материалы. Защитные меры сохранения конфиденциальности включают в себя:

- эксплуатационные вопросы.

Можно применять средства управления носителями информации для обеспечения, например физической защиты и подотчетности за носителями информации, а также гарантированного уничтожения хранимой информации для того, чтобы никто не мог воспользоваться секретным материалом из ранее уничтоженной информации (см. 8.1.5). Особое внимание следует обратить на защиту информации на легко снимаемых носителях, например дискетах, резервных копиях на магнитной ленте, а также на защиту бумажных носителей информации;

- физическую безопасность.

Соответствующая защита помещений (прочные стены и окна, а также физическое управление доступом) и офисного оборудования могут предохранить от несанкционированного доступа (см. 8.1.7);

- сохранение конфиденциальности данных.

Дополнительная защита секретного материала в месте хранения носителей информации может быть достигнута путем шифрования информации. Эффективная система управления ключами необходима для безопасного применения криптографии (см. 8.2.5).

10.3 Защитные меры целостности

В данном разделе перечислены защитные меры от предполагаемых угроз, связанных с нарушением целостности. Кроме того, приведены соответствующие ссылки на защитные меры, описанные в разделе 8. При выборе защитных мер следует учитывать тип и характеристики системы ИТ.

Большинство защитных мер, перечисленных в 8.1, обеспечивают более общую защиту, т.е. направлены на ряд угроз, и предоставляют защиту путем поддержки общего эффективного менеджмента безопасности ИТ. В настоящем стандарте эти меры подробно не рассматриваются. Не следует преуменьшать действие таких мер, поэтому они подлежат реализации для общей эффективной безопасности.

10.3.1 Ухудшение места хранения носителей информации

Ухудшение места хранения носителей информации угрожает целостности того, что в ней хранится. Если целостность является важным свойством носителей информации, то должны применяться следующие защитные меры:

- управление носителями информации.

Успешное управление носителями информации включает в себя верификацию целостности (см. 8.1.5), которая может обнаружить в запоминающем устройстве испорченные файлы;

- резервные копии.

Резервные копии должны быть сделаны со всех важных файлов, данных бизнеса и т. д. При обнаружении потери целостности, например через управление носителями информации или во время тестирования резервных копий, должны использоваться эти копии или предыдущие записи для восстановления целостности файлов. Подробное описание резервных копий см. в 8.1.6;

- защита целостности данных.

Криптографические способы могут быть использованы для безопасности целостности данных в запоминающем устройстве. Дополнительную информацию см. в 8.2.5.

10.3.2 Ошибка технического обслуживания

Если техническое обслуживание проводится нерегулярно или с ошибками, то целостность всей затронутой информации находится под угрозой. Защитные меры целостности в этом случае включают в себя:

- техническое обслуживание.

Правильное техническое обслуживание является наилучшим способом избежать ошибок при осмотре и ремонте (см. 8.1.5). Техническое обслуживание включает в себя документированные верифицированные процедуры по техническому обслуживанию, и соответствующий контроль за проведением работ;

- резервные копии.

Если в процессе технического обслуживания имели место ошибки, то организация может использовать резервные копии для восстановления целостности поврежденной информации (см. 8.1.6);

- защиту целостности данных.

Организация может использовать средства криптографии для сохранения целостности информации. Подробнее см. 8.2.5.

10.3.3 Злонамеренный код

Злонамеренный код может привести к нарушению целостности, например в случае, если в данные или файлы вносит изменения лицо, получившее несанкционированный доступ с помощью злонамеренного кода, или такие изменения вносит сам код. Защитные меры против злонамеренного кода включают в себя:

- защиту от злонамеренного кода.

Подробное описание защиты от злонамеренного кода см. 8.2.3;

- обработку инцидента.

Своевременное сообщение о любых необычных инцидентах может ограничить ущерб от воздействия злонамеренного кода. Для того, чтобы воспрепятствовать попыткам несанкционированного доступа в систему или сеть, организация может использовать соответствующие средства обнаружения проникновения. Дополнительную информацию см. в 8.1.3.

10.3.4 Подделка под идентификатор законного пользователя

Подделка под идентификатор законного пользователя может быть использована для того, чтобы обойти аутентификацию и связанные с ней услуги и функции безопасности. В итоге проблемы целостности могут возникать всякий раз, когда под видом законного пользователя осуществляется доступ и модификация информации. Защитные меры в этой области включают в себя:

- идентификацию и аутентификацию.

Имитация законного пользователя затрудняется, если защита с помощью идентификации и аутентификации основана на комбинациях того, что знает пользователь, чем он владеет, а также на применении характеристик, присущих самому пользователю (см. 8.2.1);

- логическое управление и аудит доступа.

Логическое управление доступом не имеет различий между санкционированным пользователем и лицом, маскирующимся под санкционированного пользователя, но применение механизмов управления доступом может уменьшить зону воздействия (см. 8.2.2). Просмотр и анализ журналов регистрации позволяет обнаружить несанкционированные виды деятельности;

- защиту от злонамеренного кода.

Так как одним из путей овладения паролями является внедрение злонамеренного кода для перехвата паролей, то должна быть предусмотрена защита от таких злонамеренных программ (см. 8.2.3);

- управление сетью.

Другой способ несанкционированного доступа связан с подделкой под законного пользователя в трафике, например электронной почте. В настоящее время международная организация по стандартизации (ИСО) разрабатывает несколько документов, содержащих дополнительную информацию о подробных защитных мерах по обеспечению безопасности сетей;

- сохранение целостности данных.

Если по какой-либо причине упомянутый выше способ обеспечения безопасности невозможен или недостаточен, то дополнительная защита может быть обеспечена способами криптографии, подобными цифровым подписям (см. 8.2.5).

10.3.5 Направление сообщений по ошибочному/другому маршруту

Ошибочный маршрут — это преднамеренное или случайное неправильное направление сообщений, а изменение маршрута может преследовать позитивные и деструктивные цели. Изменение маршрута может быть, например, сделано для поддержания непрерывности готовности к работе. Направление сообщений по неправильному или измененному маршруту может привести к нарушению целостности, например в случае, когда сообщения изменяются и затем передаются исходному адресату. Защитные меры от этой угрозы включают в себя:

- управление сетью.

Описание способов защиты от направлений сообщений по ошибочному/другому маршруту будет приведено в других документах ИСО, находящихся на стадии разработки. В них будет содержаться дополнительная информация по обеспечению безопасности сети;

- защиту целостности данных.

Для недопущения несанкционированных корректировок в случае ошибочного или измененного направления сообщений можно использовать хэш-функции и цифровые подписи. Дополнительную информацию см. в 8.2.5.

10.3.6 Неотказуемость

Защитные меры для обеспечения неотказуемости должны применяться в случае, если важно иметь доказательство того, что сообщение послано и/или получено и что сеть обеспечила его передачу. Имеются специальные криптографические защитные меры, указанные в 8.2.5, являющимися базовыми для обеспечения неотказуемости (целостность и неотказуемость данных).

10.3.7 Сбои программного обеспечения

Сбои программного обеспечения могут нарушать целостность данных и информации, которая обрабатывается с помощью такого программного обеспечения. Меры для защиты целостности включают в себя:

- сообщение о сбоях в программном обеспечении.

Быстрое сообщение о сбоях программного обеспечения помогает снизить возможный ущерб (см. 8.1.3);

- эксплуатационные вопросы.

Тестирование безопасности может быть использовано для обеспечения корректного функционирования программного обеспечения. С помощью управления изменениями программного обеспечения можно избежать проблем, которые возникают в связи с усовершенствованием или другими корректировками программного обеспечения (см. 8.1.5);

- резервные копии.

Резервные копии, например программное обеспечение предыдущего поколения, можно использовать для восстановления целостности данных, обработаных с помощью программного обеспечения, функционирующего со сбоями (см. 8.1.6);

- защиту целостности данных.

Средства криптографии могут быть использованы для защиты целостности информации (см. 8.2.5).

10.3.8 Отказы в источниках питания (электроснабжение и вентиляция)

Отказы в источниках питания 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 от этих проблем можно найти в соответствующих подпунктах настоящего стандарта. Защитные меры в этой области включают в себя:

- электроснабжение и вентиляцию.

При необходимости следует использовать подходящие защитные меры для того, чтобы избежать проблем, связанных с электроснабжением и вентиляцией, например, в случае скачка напряжения (см. 8.1.7);

- резервные копии.

Резервные копии должны использоваться для восстановления поврежденной информации (см. 8.1.6).

10.3.9 Техническая неисправность

Технические неисправности, например в сети, могут нарушать целостность любой информации, хранящейся или обрабатываемой в сети. Защитные меры в этой области включают в себя:

- эксплуатационные вопросы.

Организация должна использовать управление конфигурацией и изменениями, а также управление пропускной способностью для того, чтобы не допускать неисправностей в системе ИТ или сети (см. 8.1.5);

- управление сетью.

Организация должна использовать операционные процедуры, планирование системы и правильную конфигурацию сети для того, чтобы свести к минимуму риск от технических неисправностей (см. 8.2.4);

- электроснабжение и вентиляцию.

При необходимости следует использовать подходящие защитные меры для того, чтобы избежать проблем, связанных с электроснабжением и вентиляцией, например, в случае скачка напряжения (см. 8.1.7);

- резервные копии.

Резервные копии должны использоваться для восстановления поврежденной информации (см. 8.1.6).

10.3.10 Ошибки передачи

Ошибки передачи могут нарушить целостность передаваемой информации. Меры по обеспечению целостности в этом случае включают в себя:

- прокладку кабелей.

Планирование и соответствующая прокладка кабелей позволяют исключить ошибки при передаче, если, например, ошибка вызвана перегрузкой (см. 8.1.7);

- управление сетью.

Сетевое оборудование должно правильно эксплуатироваться и технически обслуживаться для того, чтобы избежать ошибок при передаче. В настоящее время международная организация по стандартизации

(ИСО) разрабатывает несколько документов, содержащих дополнительную информацию по обеспечению безопасности сети, которая может быть применена для защиты от ошибок при передаче;

- сохранение целостности данных.

Контрольные суммы и циклическое кодирование в протоколах связи может быть использовано для защиты от случайных ошибок передачи. Средства криптографии можно применять для сохранения целостности передаваемых данных в случае преднамеренного воздействия на данные. Дополнительную информацию см. в 8.2.5.

10.3.11 Несанкционированный доступ к компьютерам, данным, услугам и приложениям

Несанкционированный доступ к компьютерам, данным, услугам и приложениям может стать угрозой для целостности информации, если возможно их несанкционированное изменение. Защитные меры против несанкционированного доступа включают в себя соответствующую идентификацию и аутентификацию, логическое управление и аудит доступа на системном уровне ИТ и разделение сетей на сетевом уровне:

- идентификацию и аутентификацию.

Соответствующие защитные меры с помощью идентификации и аутентификации должны использоваться совместно с логическим управлением доступом для предупреждения несанкционированного проникновения;

- логическое управление и аудит доступа.

Защитные меры, представленные в 8.2.2, должны использоваться для обеспечения логического управления доступом с помощью соответствующих механизмов. Просмотр и анализ контрольных журналов регистрации позволяет обнаружить несанкционированную деятельность лиц, не имеющих прав доступа в систему;

- разделение сетей.

Чтобы затруднить несанкционированный доступ, должно осуществиться местное разделение сетей (8.2.4);

- физический контроль доступа.

Кроме логического предупреждения незаконного проникновения, эта задача может решаться с помощью физического управления доступом (8.1.7);

- управление носителями информации.

Если конфиденциальные данные хранятся на портативном или ином носителе (например на дискете), то должны использоваться местные управления носителями информации (8.1.5) для защиты от несанкционированного доступа;

- целостность данных.

Средства криптографии можно использовать для защиты целостности информации в запоминающем устройстве или во время ее передачи. Дополнительную информацию см. 8.2.5.

10.3.12 Использование несанкционированных программ и данных

Использование несанкционированных программ и данных создает угрозу целостности информации в запоминающем устройстве и при обработке ее в системе, если эти программы и данные используются для незаконного изменения информации или содержат злонамеренный код (например игры). Защитные меры в этой области включают в себя:

- осведомленность и обучение по вопросам безопасности.

До сведения всего персонала должна быть доведена информация о запрете установления и использования любого программного обеспечения без разрешения администратора системы ИТ или ответственного за безопасность этой системы (см. 8.1.4);

- резервные копии.

Резервные копии следует использовать для восстановления поврежденной информации (8.1.6);

- идентификацию и аутентификацию.

Соответствующие защитные меры с помощью идентификации и аутентификации должны использоваться совместно с логическим управлением доступом для предупреждения несанкционированного проникновения;

- логическое управление и аудит доступа.

Логическое управление доступом, описанное в 8.2.2, должно обеспечивать применение программного обеспечения для обработки и изменения информации только уполномоченными пользователями. Просмотр и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности;

- защиту от злонамеренного кода.

Все программы и данные должны проверяться перед использованием на наличие злонамеренного кода (см. 8.2.3).

10.3.13 Несанкционированный доступ к месту хранения носителей информации

Несанкционированный доступ к месту хранения носителей информации может подвергать опасности целостность этой информации, так как в этом случае возможно несанкционированное изменение информации, записанной на этом носителе информации. Защитные меры по сохранению целостности включают в себя:

- эксплуатационные вопросы.

Организация может применять средства управления носителями информации, например для физической защиты и подотчетности для того, чтобы не допустить проникновения в место хранения, а также верификацию целостности для обнаружения любой компрометации целостности информации, записанной на этом носителе информации (см. 8.1.5). Особое внимание должна уделять защите легко снимаемых носителей, например дискеты, магнитные ленты с записями резервных копий и бумажные носители;

- физическую безопасность.

Соответствующая защита помещений (прочные стены и окна, а также физическое управление доступом) и офисное оборудование могут предохранить от несанкционированного доступа (см. 8.1.7);

- целостность данных.

Организация может использовать средства криптографии для защиты целостности информации в запоминающем устройстве. Дополнительную информацию см. в 8.2.5.

10.3.14 Ошибка пользователя

Ошибка пользователя может нарушить целостность информации. Защитные меры для целостности информации включают в себя:

- осведомленность в вопросах безопасности и соответствующее обучение.

Организация должна провести обучение всех пользователей для того, чтобы они не допускали ошибок при обработке информации (см. 8.1.4). В программу обучения должно быть включено изучение определенных методик для специальных действий, например процедуры по эксплуатации и обеспечению безопасности;

- резервные копии.

Резервные копии, например предыдущее поколение программного обеспечения, могут быть использованы для восстановления целостности информации, поврежденной в результате ошибок пользователя (см. 8.1.6).

10.4 Защитные меры доступности

В данном подразделе перечислены защитные меры от предполагаемых угроз, связанных с нарушением доступности. Кроме того, приведены соответствующие ссылки на защитные меры, описанные в разделе 8. При выборе защитных мер должны учитываться тип и характеристики системы ИТ.

Большинство защитных мер, перечисленных в 8.1, обеспечивают более общую защиту, т.е. направлены на ряд угроз, и предоставляют защиту путем поддержки общего эффективного менеджмента безопасности ИТ. В настоящем стандарте эти меры подробно не рассматриваются. Не следует преуменьшать действие таких мер, поэтому они подлежат реализации для общей эффективной безопасности.

Потребности в доступности данных могут охватывать широкий диапазон: от данных, независимых от времени или систем ИТ (потеря таких данных и недоступность таких систем все еще считаются критическими), до данных, сильно зависимых от времени или систем ИТ. Доступность данных или готовность систем ИТ, независимых от времени, можно защищать с помощью резервных копий, тогда как в случае зависимости от времени может потребоваться система, устойчивая к внешним воздействиям.

10.4.1 Разрушительное воздействие (деструктивных атак)

Информация может быть уничтожена в результате разрушительного воздействия (деструктивных атак). Защитные меры в этой области включают в себя:

- дисциплинарный процесс.

Весь персонал организации должен понимать последствия преднамеренного или случайного уничтожения информации (см. 8.1.4);

- средства управления носителями информации.

Все носители информации должны быть соответствующим образом защищены от несанкционированного доступа, используя физическую защиту и подотчетность для всей структуры сети (см. 8.1.5);

- резервные копии.

Резервные копии должны быть сделаны со всех важных файлов, данных бизнеса и т. д. При обнаружении потери файла или любой другой информации (по какой-либо причине) для восстановления этой информации должны использоваться резервные копии и/или предыдущее поколение резервных копий. Дополнительно о резервных копиях см. в 8.1.6;

- материальную защиту.

Средства управления физическим доступом должны использоваться для предупреждения несанкционированного доступа, который мог бы способствовать несанкционированному повреждению оборудования ИТ или информации (см. 8.1.7);

- идентификацию и аутентификацию.

Соответствующие защитные меры с помощью идентификации и аутентификации должны использоваться совместно с логическим управлением доступом для предупреждения несанкционированного проникновения;

- логическое управление и аудит доступа.

Логическое управление доступом, описанное в 8.2.2, должно обеспечивать защиту от несанкционированного доступа к информации, который может привести к ее уничтожению. Рассмотрение и анализ журналов регистрации данных позволяет обнаруживать несанкционированные виды деятельности.

10.4.2 Ухудшение места хранения носителей информации

Ухудшение места хранения носителей информации угрожает готовности к функционированию объектов хранения. Если доступность (готовность к работе) является важным свойством носителей информации, организация должна применять следующие защитные меры:

- управление носителями информации.

Периодические проверки места хранения носителей информации позволяют обнаруживать ухудшение состояния носителей до того момента, когда информация действительно станет недоступной. Организация должна обеспечивать условия хранения носителей информации, исключающее внешнее воздействие, которое может стать причиной ухудшения ее функционирования (см. 8.1.5);

- резервные копии.

Резервные копии должны быть сделаны со всех важных файлов, данных бизнеса и т. д. Если файл или какая-либо другая информация недоступны (по какой-либо причине), организация должна использовать резервную копию или предыдущее поколение резервных копий для восстановления информации. Подробнее о резервных копиях см. в 8.1.6.

10.4.3 Неисправность аппаратуры связи и сбои коммуникационных услуг

Неисправность аппаратуры и нарушения в работе коммуникационных услуг связи угрожают доступности информации, передаваемой через эти коммуникационные услуги. В зависимости от причины неисправности или нарушения коммуникационных услуг полезно обратить внимание на сбои программного обеспечения (см. 10.4.11), подачи электропитания (см. 10.4.12) или другие технические неисправности (см. 10.4.13). Защитные меры доступности включают в себя:

- резервирование и резервные копии.

Внедрение резервирования компонентов коммуникационных услуг может применяться для снижения вероятности нарушения их работы. В зависимости от максимального допустимого времени вынужденного простоя может быть предусмотрено резервное оборудование для выполнения установленных требований. Данные о конфигурации и компоновочном плане должны резервироваться для обеспечения их доступности в аварийных ситуациях. Общую информацию о резервировании см. в 8.1.6;

- управление сетью.

В настоящее время международная организация по стандартизации (ИСО) разрабатывает несколько документов, содержащих дополнительную информацию о подробных защитных мерах по обеспечению безопасности сети, применимую для защиты от сбоев в работе коммуникационных аппаратуры и услуг;

- прокладку кабелей.

Планирование и соответствующая прокладка кабелей позволяют избежать повреждений. В случае подозрения неисправности на линии связи ее следует проверить (см. 8.1.7);

- неотказуемость.

Если требуется подтверждение сетевых передач, отправки или приема сообщений, организация должна обеспечить неотказуемость (см. 8.2.5). В этом случае легко могут быть обнаружены неисправности связи или пропущенная информация.

10.4.4 Защита от пожара и/или затопления

Огонь и/или вода могут уничтожить информацию и оборудование ИТ. Защитные меры от огня и/или воды включают в себя:

- физическую защиту.

Все здания и помещения, содержащие оборудование ИТ или места хранения важной информации, должны быть оборудованы соответствующими средствами защиты от пожара и затопления (см. 8.1.7);

- план непрерывности бизнеса.

Для защиты бизнеса от разрушительного воздействия огня и воды организация должна разработать план непрерывности бизнеса, а также обеспечить резервирование всей важной информации (см. 8.1.6).

10.4.5 Ошибка технического обслуживания

Если техническое обслуживание проводится нерегулярно или с ошибками, то доступность соответствующей информации может находится под угрозой. Защитные меры в этой области включают в себя:

- техническое обслуживание.

Правильное техническое обслуживание является наилучшим способом избежать ошибок при осмотре и ремонте (см. 8.1.5);

- резервные копии.

Если в процессе технического обслуживания имели место ошибки, то можно использовать резервные копии для восстановления доступности утерянной информации (см. 8.1.6).

10.4.6 Злонамеренный код

Злонамеренный код может быть применен для того, чтобы обойти аутентификацию и связанные с ней услуги и функции безопасности. В результате это может привести к потере доступности, например, если данные или файлы уничтожает лицо, получившее несанкционированный доступ с помощью злонамеренного кода, или сам код стирает файлы. Защитные меры против злонамеренного кода включают в себя:

- защиту от злонамеренного кода.

Подробное описание защиты от злонамеренных кодов см. в 8.2.3;

- обработку инцидента.

Своевременное сообщение о любом необычном инциденте может ограничить ущерб от воздействия злонамеренного кода. Средства обнаружения проникновения могут быть использованы для того, чтобы воспрепятствовать попыткам несанкционированного доступа в систему или сеть. Дополнительную информацию см. в 8.1.3.

10.4.7 Подделка под идентификатор законного пользователя

Подделка под идентификатор законного пользователя может быть использована для того, чтобы обойти аутентификацию и все связанные с ней услуги и функции безопасности. В результате могут возникать проблемы доступности всякий раз, когда при подделке под идентификатор законного пользователя создается возможность удаления или уничтожения информации. Защитные меры в этой области включают в себя:

- идентификацию и аутентификацию.

Имитация законного пользователя затрудняется, если защита с помощью идентификации и аутентификации основана на комбинациях того, что знает пользователь, чем он владеет, а также на применении характеристик, присущих самому пользователю (см. 8.2.1);

- логическое управление и аудит доступа.

Логическое управление доступом не может делать различие между санкционированным пользователем и лицом, маскирующимся под санкционированного пользователя, но применение механизмов управления доступом может уменьшить область вредоносного воздействия (см. 8.2.2). Рассмотрение и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности;

- защиту от злонамеренного кода.

Так как одним из способов овладения паролями является внедрение злонамеренного кода для перехвата паролей, то организация должна предусмотреть защиту от таких злонамеренных программ (см. 8.2.3);

- управление сетью.

Другой путь несанкционированного доступа связан с подделкой под законного пользователя в трафике, например электронной почте. В настоящее время международная организация по стандартизации (ИСО) разрабатывает несколько документов, содержащих дополнительную информацию по защитным мерам для обеспечения безопасности на уровне сети;

- резервирование данных.

Копии данных не могут предохранять от подделок под идентификатор законного пользователя, но снижают воздействие разрушительных событий, связанных с попытками незаконного проникновения (см. 8.1.6).

10.4.8 Неправильная маршрутизация или изменение маршрутизации сообщений

Ошибочный маршрут — это преднамеренное или случайное неправильное направление сообщений, а изменение маршрута может преследовать позитивные и деструктивные цели. Изменение маршрута может быть, например, сделано для поддержания непрерывности готовности к работе. Направление сообщений по неправильному или измененному маршруту может привести к нарушению целостности, например в случае, когда сообщения изменяются и затем передаются исходному адресату. Защитные меры от этой угрозы включают в себя:

- управление сетью.

Описание способов защиты от направлений сообщений по ошибочному/другому маршруту будет приведено в других документах ИСО, находящихся на стадии разработки. В них будет содержаться дополнительная информация по обеспечению безопасности сети;

- неотказуемость.

Если требуется подтверждение сетевых передач, отправки или приема сообщений, организация должна обеспечить неотказуемость (см. 8.2.5).

10.4.9 Злоупотребление ресурсами

Злоупотребление ресурсами ведет к недоступности информации или услуг. Защитные меры в этой области включают в себя:

- персонал.

Весь персонал должен понимать последствия неправильного использования ресурсов. В случае необходимости должны применяться дисциплинарные процессы (см. 8.1.4);

- эксплуатационные вопросы.

Организация должна проводить мониторинг для обнаружения неразрешенных видов деятельности, а также применять распределение обязанностей для сведения к минимуму возможностей злоупотребления привилегиями (см. 8.1.5);

- идентификацию и аутентификацию.

Соответствующие защитные меры с помощью идентификации и аутентификации должны использоваться совместно с логическим управлением доступом для предупреждения несанкционированного проникновения;

- логическое управление и аудит доступа.

Защитные меры, описанные в 8.2.2, должны использоваться для логического управления доступом к ресурсам через механизмы управления доступом. Рассмотрение и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности;

- управление сетью.

Организация должна применять соответствующую конфигурацию и разделение сети для уменьшения возможности неправильного использования сетевых ресурсов (см. 8.2.4).

10.4.10 Стихийные бедствия

Для предупреждения потери информации и услуг по причине стихийных бедствий организация должна внедрить следующие защитные меры:

- защиту от стихийных бедствий.

Все здания должны предохраняться насколько это возможно от стихийных бедствий (см. 8.1.7);

- план непрерывности бизнеса.

Организация должна разработать и испытать план непрерывности бизнеса для каждого здания, а также обеспечить доступность резервных копий всей важной информации, услуг и ресурсов (см. 8.1.6).

10.4.11 Сбои программного обеспечения

Сбои программного обеспечения могут привести к недоступности данных и информации, которая обрабатывается с помощью этих программ. Защитные меры в этой области включают в себя:

- сообщение о сбоях в программном обеспечении.

Быстрое сообщение о сбоях программного обеспечения помогает ограничить возможный ущерб (см. 8.1.3);

- эксплуатационные вопросы.

Тестирование безопасности может быть использовано для обеспечения правильного функционирования программного обеспечения. Организация может применять управление изменениями программ для

того, чтобы избежать проблем, которые возникают в связи с усовершенствованием или другими корректировками программного обеспечения (см. 8.1.5);

- резервные копии.

Резервные копии, например программное обеспечение предыдущего поколения, могут использоваться для восстановления данных, обработанных с помощью программного обеспечения, функционирующего со сбоями (см. 8.1.6).

10.4.12 Нарушения в снабжении (электроснабжение и вентиляция)

Нарушения в снабжении могут вызывать проблемы доступности, если эти нарушения являются причиной других неисправностей. Например, перебои в энергоснабжении могут привести к выходу из строя аппаратных средств, техническим неисправностям или проблемам с хранением данных. Защитные меры против этих специфических проблем можно найти в соответствующих подпунктах. Защитные меры в этой области включают в себя:

- электроснабжение и вентиляцию.

При необходимости организация должна использовать соответствующие защитные меры во избежание проблем с энергоснабжением и вентиляцией, например в случае скачка напряжения (см. 8.1.7);

- резервные копии.

Организация должна сделать резервные копии всех важных файлов, данных бизнеса и т. д. При потере файла или другой информации по причине сбоев в снабжении резервные копии должны использоваться для восстановления информации. Более подробно о резервировании см. в 8.1.6.

10.4.13 Технические неисправности

Технические неисправности, например в сети, могут нарушать доступность любой информации, хранящейся или обрабатываемой в сети. Защитные меры этой области включают в себя:

- эксплуатационные вопросы.

Управление конфигурацией и изменениями, а также управление пропускной способностью должны использоваться для того, чтобы не допускать неисправностей в системе ИТ или сети. Документация и техническое обслуживание применяются для обеспечения безаварийной работы системы (см. 8.1.5);

- управление сетью.

Организация должна использовать операционные процедуры, планирование системы и правильную конфигурацию сети для того, чтобы свести к минимуму риск от технических неисправностей (см. 8.2.4);

- план непрерывности бизнеса.

Для защиты бизнеса от губительных воздействий технических неисправностей, организация должна разработать и внедрить план непрерывности бизнеса, а также создать доступные резервы всей важной информации, услуг и ресурсов (см. 8.1.6).

10.4.14 Хищение

Хищение может угрожать доступности информации и готовности оборудования ИТ. Защитные меры в этой области включают в себя:

- физическую защиту.

Это может быть техническая защита, затрудняющая доступ в здание, зону или помещение с оборудованием ИТ, или специальные защитные меры от хищения (см. 8.1.7);

- персонал.

Защитные меры для персонала (управление доступом персонала и/или посторонних лиц, соглашения о сохранении конфиденциальности и т. д.) должны поддерживаться в рабочем состоянии, затрудняя возможность хищения (см. 8.1.4);

- средства управления носителями информации.

Любые носители информации, содержащие важный материал, должны предохраняться от хищения (см. 8.1.5).

10.4.15 Перегрузка трафика

Перегрузка трафика угрожает доступности информации, передаваемой через предоставляемые услуги. Защитные меры в этой области включают в себя:

- резервирование и резервные копии.

Внедрение резервирования компонентов коммуникационных услуг может применяться для снижения вероятности перегрузки трафика. В зависимости от максимального допустимого времени вынужденного простоя может быть предусмотрено резервное оборудование для выполнения установленных требований. Данные о конфигурации и компоновочном плане должны резервироваться для обеспечения их доступности в аварийных ситуациях. Общую информацию о резервировании см. в 8.1.6;

- управление сетью.

Организация должна использовать правильную конфигурацию, менеджмент и администрирование сетей и услуг связи для того, чтобы избежать перегрузки (см. 8.2.4);

- управление сетью.

В настоящее время международная организация по стандартизации (ИСО) разрабатывает несколько документов, содержащих дополнительную информацию о подробных защитных мерах по обеспечению безопасности сети, применимую для защиты от перегрузки трафика.

10.4.16 Ошибки передачи

Ошибки передачи могут нарушить доступность передаваемой информации. Меры в этой области включают в себя:

- прокладку кабелей.

Планирование и соответствующая прокладка кабелей позволяют избежать ошибки при передаче, если, например, ошибка вызвана перегрузкой (см. 8.1.7);

- управление сетью.

Управление сетью не может предотвратить ошибки при передаче, но способно распознавать проблемы, возникающие от ошибок передачи и в каждом случае включать тревожную сигнализацию, что позволяет своевременного реагировать на эти проблемы. В настоящее время международная организация по стандартизации (ИСО) разрабатывает несколько документов, содержащих дополнительную информацию о защитных мерах по обеспечению безопасности сети, применяемых для защиты от ошибок при передаче.

10.4.17 Несанкционированный доступ к компьютерам, данным, услугам и приложениям

Несанкционированный доступ к компьютерам, данным, услугам и приложениям может стать угрозой для доступности информации, если возможно несанкционированное уничтожение этой информации. Защитные меры против несанкционированного доступа включают в себя на сетевом уровне:

- идентификацию и аутентификацию.

Соответствующие защитные меры с помощью идентификации и аутентификации должны использоваться совместно с логическим управлением доступом для предупреждения несанкционированного проникновения;

- логическое управление и аудит доступа.

Защитные меры, описанные в 8.2.2, должны использоваться для логического управления доступом через соответствующие механизмы управления. Рассмотрение и анализ контрольных журналов регистрации позволяет обнаружить несанкционированную деятельность лиц, не имеющих прав доступа в систему;

- разделение сетей.

Для того чтобы затруднить несанкционированный доступ, организация должна осуществлять разделение сетей (см. 8.2.4);

- физическое управление доступом.

Кроме логического предупреждения незаконного проникновения, эта задача может решаться с помощью физического управление доступом (см. 8.1.7);

- управление носителями информации.

Если конфиденциальные данные хранятся на портативных или иных носителях (например на дискете), то организация должна использовать средства управления носителями информации (см. 8.1.5) для защиты от несанкционированного доступа.

10.4.18 Использование несанкционированных программ и данных

Использование несанкционированных программ и данных создает угрозу доступности информации в запоминающем устройстве и при обработке в системе, если программы и данные используются для уничтожения информации или если они содержат злонамеренный код (например компьютерные игры). Защитные меры в этой области включают в себя:

- осведомленность в вопросах безопасности и обучение.

Организация должна довести до сведения всего персонала информацию о запрете установления и использования любого программного обеспечения без разрешения администратора сети или лица, ответственного за обеспечение безопасности этой системы (см. 8.1.4);

- резервные копии.

Резервные копии должны использоваться для восстановления поврежденной информации (см. 8.1.6);

- идентификацию и аутентификацию.

Соответствующие защитные меры с помощью идентификации и аутентификации должны использоваться совместно с логическим управлением доступом для предупреждения несанкционированного проникновения;

- логическое управление и аудит доступа.

Логическое управление доступом, описанное в 8.2.2, должно обеспечивать применение программного обеспечения для обработки и удаления информации только санкционированными пользователями. Рассмотрение и анализ журналов регистрации позволяет обнаруживать несанкционированные виды деятельности;

- защиту от злонамеренного кода.

Все программы и данные должны проверяться перед использованием на присутствие злонамеренного кода (вирусы) (см. 8.2.3).

10.4.19 Несанкционированный доступ в места хранения носителей информации

Несанкционированный доступ к местам хранения носителей информации может подвергать опасности доступность информации, так как в этом случае возможно несанкционированное уничтожение информации, записанной на этих носителях. Защитные меры в этой области включают в себя:

- эксплуатационные вопросы.

Организация может управлять носителями информации, например для физической защиты и подотчетности носителей информации для того, чтобы не допустить несанкционированный доступ к информации, записанной на этих носителях (см. 8.1.5). Особое внимание должно уделяться защите легко снимаемых носителей информации, например дискет, магнитных лент с записями резервных копий и бумажных носителей;

- физическую безопасность.

Соответствующая защита помещений (прочные стены и окна, а также физическое управление доступом) и офисное оборудование могут защитить от несанкционированного доступа (см. 8.1.7).

10.4.20 Ошибка пользователя

Ошибка пользователя может нарушить доступность информации. Защитные меры в этой области включают в себя:

- осведомленность в вопросах безопасности и обучение.

Организация должна провести соответствующее обучение всех пользователей для того, чтобы они не допускали ошибок при обработке информации (см. 8.1.4). В программу обучения должно быть включено обучение определенным методикам для специальных действий, например процедурам по эксплуатации или обеспечению безопасности;

- резервные копии.

Резервные копии, например предыдущее поколение программного обеспечения, могут быть использованы для восстановления информации, поврежденной в результате ошибок пользователя (см. 8.1.6).

10.5 Защитные меры для подотчетности, аутентичности и достоверности

Область применения подотчетности, аутентичности и достоверности широко различается в разных доменах. Эти различия подразумевают возможное применение множества разных защитных мер. Поэтому для них могут быть приведены только общие рекомендации.

Защитные меры, перечисленные в 8.1, предоставляют общую защиту, т.е. они направлены на ряд угроз и обеспечивают защиту путем поддержки общего эффективного управления безопасностью ИТ. Настоящий подраздел их не содержит, но влияние этих мер не следует приуменьшать и они также подлежат реализации для обеспечения общей эффективной безопасности.

10.5.1 Подотчетность

При защите подотчетности должна учитываться любая угроза, которая может привести к выполнению действий, не свойственных рассматриваемому объекту или субъекту. Ниже приведены примеры некоторых подобных угроз:

- коллективное пользование учетными записями;
- отсутствие возможности оперативного контроля действий;
- имитация законного пользователя;
- сбой программного обеспечения;
- несанкционированный доступ к компьютеру, данным, услугам и приложениям;
- неудовлетворительная аутентификация.

Существуют два типа подотчетности, которые должны быть приняты во внимание. Первый тип связан с идентификацией пользователя, подотчетного за определенные действия с информацией и системами ИТ. Контрольные журналы регистрации предоставляют такую подотчетность. Второй — касается подотчетности между пользователями в системе. Это может быть достигнуто путем применения услуг по обнаружению неотказуемости, дробления знаний или двойного контроля.

Многие защитные меры могут внести вклад в улучшение подотчетности, начиная от политики обеспечения безопасности, логического управления и аудита доступа и до внедрения одноразовых паролей и средств управления носителями информации. Реализация политики в области владения информацией является предпосылкой для обеспечения подотчетности. Выбор специальных защитных мер будет зависеть от специфики использования подотчетности в пределах домена.

10.5.2 Аутентичность

Доверие к аутентичности может быть снижено любой угрозой, которая заставляет человека, систему или процесс усомниться в том, что объект является тем, что он представляет из себя. Примерами возникновения такой ситуации является изменение данных без надлежащего контроля, происхождение непроверенных или неподдерживаемых данных.

Многие защитные меры могут внести свой вклад в улучшение аутентичности, начиная от использования утвержденных справочных данных, логического управления и аудита доступа и до цифровых подписей. Выбор специальных защитных мер зависит от специфики использования аутентичности в пределах данной области.

10.5.3 Достоверность

Любая угроза, которая может привести к непоследовательному поведению систем или процессов, приводит к снижению достоверности. Примерами таких угроз являются нелогичное функционирование системы и ненадежные поставщики. Снижение достоверности приводит к плохому обслуживанию потребителей и потере их доверия.

Многие защитные меры могут внести свой вклад в усиление достоверности, начиная от планов непрерывности бизнеса, внедрения резервирования в физическую структуру и техническое обслуживание системы и до идентификации, аутентификации, логического управления и аудита доступа. Выбор специальных защитных мер будет зависеть от специфики выбора показателей достоверности в пределах данной области.

11 Выбор защитных мер согласно детальным оценкам

Выбор защитных мер согласно детальным оценкам основывается на тех же принципах, которые применялись в предыдущих разделах. Проведение детального анализа риска позволяет учесть специальные требования и обстоятельства систем ИТ и их активы. Отличие от предыдущих разделов заключается в уровне усилий и детализации процесса оценивания. Поэтому, возможно квалифицированное обоснование выбранных защитных мер. Подраздел 11.1 настоящего стандарта направлен на то, чтобы использовать положения о методах анализа риска, установленные в ИСО/МЭК ТО 13335-3, для процесса выбора защитных мер, установленных в настоящем стандарте. Принципы выбора защитных мер рассмотрены в 11.2.

11.1 Взаимосвязь ИСО/МЭК ТО 13335-3 с настоящим стандартом

В ИСО/МЭК ТО 13335-3 представлены технические приемы управления безопасностью ИТ. В нем также рассматриваются варианты стратегии анализа возможных рисков организации и рекомендованный подход для анализа риска. Основными вариантами стратегии для применения в пределах организации является использование:

- базового подхода для всех систем ИТ;
- детального анализа риска для всех систем ИТ;
- рекомендованного подхода, т. е. после детального анализа риска всех систем ИТ используется базовый подход к системам ИТ с низким уровнем риска и детальный анализ риска для систем ИТ с высоким уровнем риска.

Если принято решение использовать детальный анализ риска для всех систем ИТ для идентификации защитных мер, то организация должна использовать информацию о выборе защитных мер и эффективном использовании результатов детального анализа риска, приведенную в 11.2. Кроме того, организация должна использовать информацию о защитных мерах, в том числе для специальных систем ИТ, и связь между проблемами безопасности и угрозами, приведенными в разделах 8—10.

11.2 Принципы выбора

Базовыми принято считать четыре аспекта, связанные с защитными мерами, т. е. воздействия, угрозы, уязвимость и риск. Риск сам по себе рассматривается, когда организация принимает решение о снижении или избежании риска до момента его принятия (примером снижения риска является получение страхового полиса, а примером избегания риска — перевод конфиденциальной информации в другой компьютер).

Аспекты, формирующие риск (воздействия, угрозы, уязвимости), являются главной целью защитных мер. Существуют следующие пути борьбы защитных мер против этих аспектов:

- угрозы — защитные меры могут снижать вероятность возникновения угрозы (например рассмотрение угрозы потери данных вследствие ошибок пользователя, курс обучения пользователей, направленный на снижение числа ошибок) или в случае запланированной вредоносной атаки (воздействия) сдерживать угрозу путем увеличения технической сложности, которую надо преодолеть для достижения успешности атаки;

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

- воздействие — защитные меры могут снизить воздействие или помочь его избежать (например, если вредное воздействие заключается в недоступности информации, то оно может быть снижено путем создания копий, хранящихся в безопасном месте, а также разработки и внедрения плана непрерывности бизнеса). Если существуют записи аудита, то анализ и средства предупреждения могут обеспечить раннее обнаружение инцидента и снизить вредное воздействие на бизнес.

От того, как и где используется конкретная защитная мера, во многом зависят те выгоды, которые получает организация от ее реализации. Очень часто угрозы могут относиться к нескольким уязвимостям. Поэтому, если применяется защитная мера, предотвращающая одну угрозу, то одновременно она может защищать несколько уязвимостей системы. Обратное утверждение тоже верно — мера безопасности, предохраняющая одну уязвимость, может быть принята против нескольких угроз. Эти выгоды следует учитывать при выборе защитных мер. Дополнительные выгоды должны быть подтверждены документально для того, чтобы иметь полную картину требований безопасности, которым удовлетворяют защитные меры.

Обычно, защитные меры могут обеспечить один или более типов защиты: предупреждение, сдерживание, обнаружение, снижение, восстановление, корректировку, мониторинг и осведомленность. Выбор защитных мер в данном случае зависит от особенностей ситуации и предназначении защитных мер. Во многих случаях защитные меры направлены на обеспечение нескольких типов защиты, что приносит дополнительные выгоды. Подобные защитные меры, предоставляющие многочисленные выгоды, должны быть выбраны в первую очередь.

Организация должна поддерживать в разумных пределах баланс безопасности и воздействий. Если слишком много внимания уделяется одному типу защиты, то маловероятно, что общий уровень безопасности будет эффективен. Например, если большинство сдерживающих защитных мер используется без адекватных мер обнаружения для определения того, когда сдерживание уже не работает, то общая безопасность не будет эффективной.

Предложенные защитные меры необходимо до их реализации сравнить с существующими мерами по обеспечению безопасности, чтобы оценить, какие меры могут быть усилены или усовершенствованы. В любом случае это будет дешевле, чем внедрять новую защиту.

Во время выбора защитных мер важно сравнить расходы по реализации защиты со стоимостью активов и оценить возврат вложений с точки зрения снижения рисков. Расходы на реализацию и техническое обслуживание могут быть выше стоимости самой защиты, и это следует учитывать при выборе защитных мер.

Технические ограничения, например требования к функционированию, управляемости (требования к операционной поддержке) и вопросам совместимости могут затруднять использование некоторых защитных мер. В этих случаях специалисты по системам ИТ и обеспечению безопасности должны работать совместно для выработки оптимальных решений. Если защитные меры снижают эффективность функционирования систем, то эти специалисты по системам ИТ и обеспечению безопасности должны находить решение, обеспечивающее эффективную работу системы ИТ при гарантированном достаточном уровне безопасности.

Для таких аспектов, как охрана неприкосновенности и юридическая защита личной информации, может потребоваться наличие специальных защитных мер. Таким образом, организация должна исследовать и идентифицировать базовые защищаемые элементы.

12 Разработка базовой безопасности организации

В случае, если организация принимает решение о применении базовой безопасности ко всей организации или к ее части, то должны быть рассмотрены следующие вопросы:

- какие части организации или систем могут быть защищены на одном и том же базовом уровне, а какие требуют разного уровня безопасности, или должен ли применяться один и тот же базовый уровень для всей организации;
- на какой уровень обеспечения безопасности должна быть нацелена базовая безопасность (или ее варианты);
- как могут быть определены защитные меры, образующие различную (при необходимости) базовую безопасность.

Схема различных базовых уровней обеспечения безопасности представлена на рисунке 4.

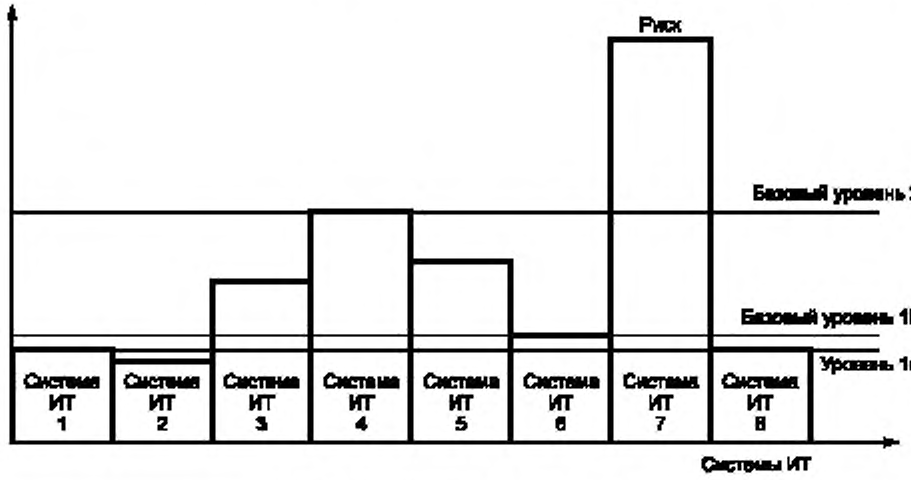

Рисунок 4 — Различные базовые уровни

Преимущество применения различных уровней базовой безопасности в организации заключается в том, что большинство систем будут соответствующим образом защищены, т. е. им будет обеспечен не слишком низкий и не слишком высокий уровень безопасности (например для систем ИТ 1, 2, 6 и 8 с уровнем базовой безопасности 1 и для систем ИТ 3, 4 и 5 с уровнем базовой безопасности 2 на рисунке 4). Если системы ИТ с различными требованиями безопасности действительно отличаются (большинство требуемых защитных мер различны для каждой системы ИТ), тогда для данной организации рекомендуется применять различные базовые уровни безопасности. Если имеются принципиально разные требования обеспечения безопасности, то решение о применении базового уровня безопасности должно быть пересмотрено.

Если, с другой стороны, единственным различием между различными базовыми уровнями безопасности является потребность в некоторых дополнительных защитных мерах для повышения базового уровня безопасности, то возможно отсутствует необходимость во внедрении нескольких различных базовых уровней. Если реализуется только один базовый уровень безопасности, то непроизводительные издержки организации могут быть значительно снижены, и персонал организации может ориентироваться на один и тот же существующий уровень обеспечения безопасности.

Использование базового уровня обеспечения безопасности должно соотноситься с возможностью логически реализовать один или более уровней базовой безопасности. Если выбраны различные базовые уровни обеспечения безопасности, то они должны быть точно установлены в соответствии с требованиями обеспечения безопасности защищаемой системы ИТ. Обычно базовый уровень обеспечения безопасности не должен быть нацелен на удовлетворение требований систем ИТ к безопасности самого низкого уровня (см. требования системы ИТ 2 на рисунке 4). Следует стремиться к уровню, достаточному для большинства

(см. базовый уровень 1a на рисунке 4) или всех (см. базовый уровень 1b на рисунке 4) систем ИТ. Целесообразно стремиться к наивысшему уровню обеспечения безопасности систем ИТ с помощью базовых защитных мер, так как они обеспечивают достаточный уровень безопасности для всех рассматриваемых систем ИТ при небольших затратах. Для принятия окончательного решения о том, какие системы ИТ должны быть защищены на одном и том же базовом уровне, организация должна провести детальное рассмотрение систем ИТ. Некоторые системы ИТ во многом схожи по характеристикам и/или требованиям обеспечения безопасности. В этом случае они должны быть защищены на одном и том же базовом уровне. Если, с другой стороны, несколько систем полностью отличаются по своим требованиям к обеспечению безопасности, то часто самым легким способом удовлетворения требований безопасности является рассмотрение каждой системы в отдельности.

Это справедливо и для случая, если принято решение о внедрении базового уровня обеспечения безопасности для всей организации. Принятый базовый уровень безопасности может стремиться к реализации трех разных уровней обеспечения безопасности:

- низкого уровня с добавлением специальных защитных мер для защиты всей системы ИТ с более высокими требованиями,
- среднего уровня с добавлением специальных защитных мер для защиты всей системы ИТ с более высокими требованиями;
- высокого уровня, достаточного для обеспечения безопасности всех систем ИТ, подлежащих защите с помощью базовой безопасности.

Как было указано выше, средний или высокий уровень обеспечения базовой безопасности целесообразно использовать для многих организаций для обеспечения достаточной защиты безопасности организации и снижения накладных расходов. Окончательное решение должно быть принято в соответствии с политикой безопасности организации и требований к обеспечению безопасности рассматриваемых систем ИТ.

13 Выводы

В настоящем стандарте рассмотрены различные пути выбора защитных мер, которые могут быть использованы для достижения базового уровня обеспечения безопасности и в качестве дополнительной информации к методам, описанным в ИСО/МЭК ТО 13335-3. Настоящий стандарт содержит обзор общепринятых защитных мер, которые могут быть выбраны, исходя из упомянутых выше подходов. Настоящий стандарт содержит ссылки на разные руководства по базовой безопасности с более подробным описанием защитных мер. В нем также приведено описание различных путей разработки базовой безопасности организации, преимущества и недостатки различных подходов по обеспечению безопасности. Настоящий стандарт может применяться любыми организациями малого и крупного бизнеса, выбирающих защитные меры для своих систем информационных технологий.

Приложение А
(справочное)

Кодекс менеджмента безопасности информационных технологий

В настоящем приложении приведено краткое описание национальных стандартов Великобритании [1] и [2] серии BS 7799.

Область применения

Серия стандартов BS 7799 включает в себя две части:

BS 7799-1:1999 Кодекс менеджмента безопасности информационных технологий;

BS 7799-2:1999 Технические условия по системам менеджмента безопасности информационных технологий.

Данные стандарты опубликованы Британским институтом стандартов. Стандарт BS 7799-1:1999 ([1]) заменяет версию 1995 г. Обе части стандарта BS 7799 предназначены для высшего руководства и персонала, ответственного за инициирование, реализацию и поддержание в рабочем состоянии информационной безопасности организации, и могут использоваться в качестве основы для разработки стандартов по обеспечению безопасности организации.

Стандарты [1] и [2] подготовлены комитетом Британского института стандартов по управлению защитой информации. Данные стандарты учитывают последние разработки в области применения технологии обработки информации, особенно в сетях и средствах связи. В них также уделено внимание вовлечению и ответственности высшего руководства организации за обеспечение безопасности информации. В процессе их пересмотра был учтен опыт организаций разных стран мира.

Содержание данных стандартов включают в себя полный набор средств управления и наилучший практический опыт в области информационной безопасности. Данные стандарты также предназначены для применения в качестве основы для выявления диапазона средств управления, необходимых для большинства ситуаций, связанных с использованием информационных систем в промышленности и торговле и, следовательно, могут быть применены в больших, средних и малых организациях.

Содержание [1]:

1 Область применения
2 Термины и определения
3 Политика обеспечения безопасности
  3.1 Политика обеспечения информационной безопасности
4 Организация безопасности
  4.1 Инфраструктура обеспечения безопасности информации
  4.2 Безопасность доступа третьей стороны
  4.3 Аутсорсинг
5 Классификация и управление активами
  5.1 Подотчетность активов
  5.2 Классификация информации
6 Обеспечение безопасности персонала
  6.1 Безопасность в определении видов работ и выделенных ресурсов
  6.2 Обучение пользователей
  6.3 Реагирование на инциденты
7 Безопасность физической и окружающей среды
  7.1 Области безопасности
  7.2 Безопасность оборудования
  7.3 Общие средства управления
8 Управление систем связи и операционный менеджмент
  8.1 Операционные процедуры и распределение ответственности
  8.2 Планирование и приемка систем
  8.3 Защита от злонамеренных кодов
  8.4 Действия по обслуживанию
  8.5 Управление сетью
  8.6 Обращение и безопасность носителей информации
  8.7 Обмен данными и программным обеспечением
9 Управление доступом
  9.1 Требования к системам доступа в организации
  9.2 Управление доступом пользователей
  9.3 Ответственность пользователей

9.4 Управление доступом в сеть
9.5 Управление доступом в компьютер
9.6 Управление доступом к приложениям
9.7 Мониторинг систем доступа и пользователей
9.8 Мобильная обработка данных и дистанционная работа
10 Разработка и техническое обслуживание системы
10.1 Требования к системам обеспечения безопасности
10.2 Безопасность в прикладных системах
10.3 Криптографические средства управления
10.4 Безопасность файлов прикладных систем
10.5 Безопасность при разработке и поддержки окружающей среды
11 Управление непрерывностью бизнеса
11.1 Аспекты управления непрерывностью бизнеса
12 Соответствие
12.1 Соответствие законодательным и обязательным требованиям
12.2 Анализ политики безопасности и технического соответствия
12.3 Вопросы, связанные с аудитом системы

Приложение В
(справочное)

Стандарт ETSI[1] «Свойства и механизмы обеспечения базового уровня безопасности»

В настоящем приложении приведено краткое описание стандарта ETSI [3].

Область применения

В стандарте ETSI перечислены все свойства и механизмы обеспечения базового уровня безопасности, которые подверглись оценке и могут применяться в других стандартах ETSI. Однако в приложении к данному стандарту приведены руководящие указания по выбору и применению специальных механизмов обеспечения безопасности. Для специальных рекомендаций приведены соответствующие ссылки на источники информации. Более того, эксперты соответствующих комитетов ETSI могут помочь в случае возникновения вопросов. В большинстве случаев официальные стандарты по применению механизмов обеспечения безопасности отсутствуют, однако сами механизмы обеспечения безопасности используются в организациях. Многие механизмы не опубликованы по причине обеспечения безопасности, так как они используются в специальных приложениях ETSI. Так как наблюдается значительная активность в областях телекоммуникации и криптографии, то данный стандарт периодически пересматривается и корректируется.

Содержание

1 Область применения
2 Нормативные ссылки
- 2.1 Общие свойства и механизмы
- 2.2 Свойства и механизмы, имеющие отношение к прикладным системам

3 Определения, символы и сокращения
- 3.1 Определения
- 3.2 Сокращения

4 Свойства безопасности
- 4.1 Введение
- 4.2 Обзор свойств безопасности
- 4.2.1 Аутентификация
- 4.2.2 Конфиденциальность
- 4.2.3 Целостность
- 4.2.4 Управление доступом
- 4.2.5 Управление ключами
- 4.2.6 Неотказуемость
- 4.2.7 Аудит безопасности

5 Механизмы обеспечения безопасности
- 5.1 Введение
- 5.2 Краткий обзор
- 5.2.1 Механизмы аутентификации/идентификации
- 5.2.2 Механизмы конфиденциальности
- 5.2.3 Механизмы целостности
- 5.2.4 Механизмы управления доступом
- 5.2.5 Механизмы управления ключами
- 5.2.6 Механизмы неотказуемости
- 5.3 Формат описания

Приложение А (справочное) Описание механизмов:
- Механизмы обеспечения безопасности/аутентификация/идентификация
- Механизмы обеспечения безопасности/аутентификация/идентификация/методы на основе практических знаний
- Механизмы обеспечения безопасности/конфиденциальность/шифрование
- Механизмы обеспечения безопасности/целостность
- Механизмы обеспечения безопасности/управление доступом
- Механизмы обеспечения безопасности/управления ключами/распределения открытых ключей

Приложение В (справочное) Связь между услугами и механизмами безопасности

[1] Европейский институт телекоммуникационных стандартов.

Приложение С
(справочное)

Руководство по базовой защите информационных технологий

В настоящем приложении приведено краткое описание стандарта [4].

Область применения

Целью базовой защиты ИТ путем соответствующего применения стандартизованных организационных, персональных, инфраструктурных и технических защитных мер является достижение стандарта безопасности систем ИТ, который является адекватным и достаточным для удовлетворения требований защиты среднего уровня и может служить в качестве основы для применения в ИТ, требующих более высокого уровня защиты.

С этой целью руководство по базисной защите ИТ рекомендует пакет контрмер для типичных конфигураций, окружающей среды и организационных структур ИТ. При подготовке этого руководства орган по обеспечению безопасности информации Германии принял расчетные оценки риска на основе известных угроз и уязвимостей и разработал для этой цели пакет мер. Таким образом, пользователям руководства по базисной защите ИТ не придется снова проводить подобный анализ базовой защиты ИТ. Пользователи должны только обеспечить последовательную и полную реализацию рекомендованных защитных мер.

В то же время руководство по базовой защите ИТ помогает обеспечить безопасность ИТ в том, что касается экономически эффективного выполнения требований к защите на среднем уровне, так как политика безопасности индивидуальных систем может ссылаться на это руководство. Таким образом, базовая защита ИТ становится общепринятой основой соглашения по защитным мерам для соответствия требованиям защиты среднего уровня.

Содержание

1 Менеджмент безопасности ИТ
2 Применение руководства по базовой защите ИТ
- 2.1 Применение руководства по базовой защите ИТ
- 2.2 Установление требований к защите
- 2.3 Использование руководства по базовой защите ИТ
- 2.4 Практические советы и операционные вспомогательные средства

3 Базовая защита ИТ основных компонентов
- 3.1 Организация
- 3.2 Персонал
- 3.3 Планирование действий в нештатных ситуациях
- 3.4 Резервирование
- 3.5 Защита данных
- 3.6 Защита от компьютерного вируса
- 3.7 Общее представление о криптографии

4 Инфраструктура
- 4.1 Здания
- 4.2 Прокладка кабелей
- 4.3 Помещения
- 4.3.1 Офис
- 4.3.2 Помещение для сервера
- 4.3.3 Архивы запоминающих устройств
- 4.3.4 Помещение технической инфраструктуры

5 Системы, не входящие в сеть
- 5.1 Дисковая операционная система DOS PC (одиночный пользователь)
- 5.2 Системы UNIX
- 5.3 Портативный переносной компьютер
- 5.4 Дисковая операционная система DOS PC (несколько пользователей)
- 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 сервера
- 6.2 Сеть UNIX
- 6.3 Структура 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 Интернет сервер
8 Дистанционная передача данных (телекоммуникация)
8.1 Телекоммуникационные системы
8.2 Факсимильные аппараты
8.3 Автоответчики
8.4 Аппаратура дистанционного действия
9 Другие компоненты ИТ
9.1 Стандартное программное обеспечение
9.2 Базы данных
9.3 Средства передачи данных
Каталоги защитных мер
Каталоги угроз
Каталоги угроз с таблицами защитных мер

Приложение D
(справочное)

Справочник NIST[1)] по компьютерной безопасности

В настоящем приложении приведено краткое описание справочника NIST [5].

Область применения

Справочник NIST обеспечивает защиту компьютеризованных ресурсов, включая аппаратуру, программное обеспечение и информацию. В нем разъясняются важные концепции, вопросы стоимости и взаимоотношения средств управления безопасностью. В нем приведены преимущества внедрения средств управления безопасностью, основные технологии или подходы для каждого вида контроля.

Справочник NIST дает широкий обзор компьютерной безопасности с тем, чтобы пользователь мог понять свои нужды в этой области и разработать правильный подход к выбору подходящих средств управления безопасностью. Справочник NIST не содержит описания этапов, необходимых для реализации программы обеспечения компьютерной безопасности. Справочник NIST предоставляет подробные методики внедрения средств управления безопасностью или предлагает руководящие указания по аудиту безопасности специальных систем. В конце каждой главы справочника NIST приведены ссылочные данные.

Целью справочника NIST не является описание требований. В нем рассматриваются преимущества использования различных средств управления компьютерной безопасностью и ситуации, в которых их применение может быть необходимым. Особые требования для национальных систем выделены в тексте. Справочник NIST содержит рекомендации и руководящие указания, в нем не предусмотрены какие-либо меры наказания.

Содержание

I Введение и общий обзор
- 1 Введение
- 2 Элементы компьютерной безопасности
- 3 Распределение ответственности и полномочий
- 4 Общие угрозы: краткий обзор

II Средства менеджмента
- 5 Политика обеспечения компьютерной безопасности
- 6 Менеджмент программы компьютерной безопасности
- 7 Менеджмент риска компьютерной безопасности
- 8 Безопасность и планирование в жизненном цикле компьютерной системы
- 9 Гарантии

III Средства операционного управления
- 10 Управление персоналом/пользователями
- 11 Подготовка к внештатным ситуациям и стихийным бедствиям
- 12 Обработка инцидента в компьютерной безопасности
- 13 Осведомленность, обучение и образование
- 14 Вопросы безопасности при эксплуатации и технической поддержки компьютера
- 15 Безопасность физической и окружающей среды

IV Технические средства управления
- 16 Идентификация и аутентификация
- 17 Логическое управление доступом
- 18 Следы аудита
- 19 Криптография

V Пример
- 20 Оценка и снижение риска для гипотетической компьютерной системы

[1)] Национальный институт стандартов и технологий США.

Приложение Е
(справочное)

Медицинские информационные технологии. Категории безопасности и защита информационных систем здравоохранения

В настоящем приложении приведено краткое описание европейского стандарта ENV [6].

Область применения

Настоящий европейский стандарт устанавливает методы классификации автоматизированных информационных систем здравоохранения с точки зрения безопасности. Принятые защитные меры обеспечивают предохранение доступности, конфиденциальности и целостности данных до приемлемого уровня. Приведено соответствие пакета защитных требований и требуемого уровня риска для каждой категории.

Настоящий европейский стандарт применяется ко всем автоматическим информационным системам здравоохранения. Сюда относятся системы, непосредственно связанные с лечением пациентов, например системы обработки результатов анализов лабораторий. Он также включает в себя статистические и административные системы, обеспечивающие оперативную поддержку самого учреждения здравоохранения, например платежные ведомости персонала, системы планирования и финансового учета. Однако системы, для которых важным требованием является конфиденциальность, в настоящем европейском стандарте не рассматривается. Данный стандарт предназначен для потребителей надежных информационных систем в здравоохранении и/или разработчиков/производителей таких систем. Внедрение терминов и положений, установленных в данном стандарте, способствует выполнению обязательств по национальному и европейскому законодательству в области здравоохранения, а также отвечает ожиданиям общества в соответствии со стандартами безопасности информации высокого уровня.

Содержание

1 Область применения
2 Нормативные ссылки
3 Термины и определения
4 Сокращения
5 Классификация информационных систем здравоохранения
6 Защитный профиль I (требования базового уровня)
7 Защитный профиль II
Требования базового уровня
Требования повышенного уровня
8 Защитный профиль III
Требования базового уровня
Требования повышенного уровня
9 Защитный профиль IV
Требования базового уровня
Требования повышенного уровня
10 Защитный профиль V
Требования базового уровня
Требования повышенного уровня
11 Защитный профиль VI
Требования базового уровня
Требования повышенного уровня
Приложение А (справочное) Подход к классификации системы
Приложение В (справочное) Рекомендации по использованию европейского стандарта
Приложение С (справочное) Примеры категорий информационных систем
Приложение D (справочное) Классификация информационных систем
Приложение Е (справочное) Источники угроз
Приложение F (справочное) Библиография

Приложение F
(справочное)

ТК 68 Банковские и другие финансовые услуги. Руководящие указания по информационной безопасности

В настоящем приложении приведено краткое описание документа [7].

Область применения

Финансовые учреждения все чаще используют информационные технологии для успешного ведения бизнеса. Менеджмент риска является основным компонентом обеспечения качественных финансовых услуг. Финансовые учреждения управляют риском через эффективную практику бизнеса, внимательное заключение договоров, страхование и использование механизмов безопасности.

Финансовые учреждения испытывают потребность управления безопасностью информации в любых ситуациях. Настоящий документ не предлагает решений для всех ситуаций. Каждая ситуация должна быть исследована индивидуально. Настоящий документ содержит общие рекомендации.

Основными задачами настоящего документа являются:

- представление структуры программы информационной безопасности;
- представление руководства по выбору средств управления безопасностью, устанавливающего приемлемую практику ведения бизнеса,
- соответствие существующим стандартам, а также новым разработкам объективных и общепринятых критериев безопасности.

Настоящий документ предназначается для использования финансовыми учреждениями всех типов, которые желают применить экономную и коммерчески целесообразную программу обеспечения информационной безопасности. Он также полезен для тех, кто предоставляет услуги финансовым учреждениям. Настоящий документ может также служить в качестве первоисточника для преподавателей и издателей, обслуживающих финансовую деятельность.

Содержание

1 Введение
2 Управление безопасностью ИТ
3 Политика безопасности ИТ организации
4 Организация безопасности ИТ
    4.1 Обязательства
    4.2 Ответственность и полномочия
5 Анализ риска
    5.1 Введение
    5.2 Иллюстрированный процесс оценки риска
    5.3 Угрозы
    5.4 Уязвимости
    5.5 Категории рисков
    5.6 Идентификация и анализ функций организации
    5.7 Процесс оценки риска
6 Рекомендации по обеспечению безопасности ИТ
    6.1 Принятие риска
7 Выбор защитных мер по обеспечению безопасности
    7.1 Классификация информации
    7.2 Логическое управление доступом
    7.3 След ревизии
    7.4 Управление изменениями
8 Внедрение защитных мер
    8.1 Компьютеры
    8.2 Сети
    8.3 Программное обеспечение
    8.4 Голосовая, телефонная и другая взаимосвязанная аппаратура
    8.5 Факсы и изображения
    8.6 Электронная почта
    8.7 Документы на бумажном носителе
    8.8 Микроформы и другие способы хранение носителей информации
    8.9 Карты финансовой транзакции
    8.10 Автоматические ответчики

8.11 Электронные фонды и трансферты
8.12 Чеки
8.13 Электронная коммерция
8.14 Электронные деньги
8.15 Внесистемные средства
8.16 Страхование
8.17 Аудит
8.18 Обязательное соответствие
8.19 Планирование восстановления после стихийного бедствия
8.20 Внешние поставщики услуг
8.21 Криптографические операции
8.22 Секретность (защита частной информации)
8.23 Внедрение криптографических средств управления
9 Осведомленность о безопасности
9.1 Осведомленность об информационной безопасности
9.2 Человеческие факторы
10 Дальнейшее обеспечение безопасности
10.1 Техническое обслуживание
10.2 Соответствие безопасности
10.3 Мониторинг
10.4 Обработка инцидента
11 Ссылки
Приложение А (справочное) Образцы документации
Приложение В (справочное) Примеры базового уровня и обеспечение безопасности

Приложение G
(справочное)

Защита ценной информации, не подпадающей под действие законодательства о государственной тайне. Рекомендации для автоматизированных рабочих мест

В настоящем приложении приведено краткое описание документа [8].

Область применения

Настоящий документ рекомендует специалистам организации меры по внедрению обеспечения защиты ценной информации, не подпадающей под действие законодательства о государственной тайне, которая обрабатывается, обращается и хранится с помощью компьютерных средств. Настоящие рекомендации в частности касаются:

- дорогостоящего программного обеспечения или хищений, ухудшения состояния или раскрытия информации, которые могут поставить организацию в затруднительное положение;
- ограниченного обращения или специфической конфиденциальной информации, которая при условии принятых обязательств сохранения профессиональной конфиденциальности, не должна разглашаться. Для информации более высокого уровня конфиденциальности, т.е. особо секретной информации, организация должна предусмотреть усиленные меры обеспечения безопасности, рекомендованные в настоящем документе.

Организация должна составлять свои внутренние инструкции на основе этих рекомендаций.

Содержание

Введение
1 Область применения
2 Административное управление и организация обеспечения безопасности
  2.1 Партнеры по безопасности и их роль
  2.2 Процедуры
3 Физическая безопасность
  3.1 Местоположение
  3.2 Инсталляция аппаратных средств ЭВМ
  3.3 Управление доступом персонала к аппаратным средствам
  3.4 Управление доступом персонала в здания
4 Безопасность, касающаяся персонала
  4.1 Ответственность и процедуры
  4.2 Обучение и осведомленность — повышенная осведомленность
5 Безопасность документов
  5.1 Обращение и защита информации
  5.2 Обращение и защита носителей информации
6 Безопасность компьютеров
  6.1 Компьютерное оборудование
  6.2 Управление доступом
  6.3 Программное обеспечение
  6.4 Файлы
  6.5 Техническое обслуживание
  6.6 Временный ремонт
  6.7 Надзор и верификация
7 Процедура сохранения (резервирования) и порядка действий в непредвиденной ситуации
  7.1 Процедура сохранения (резервирования) файлов данных
  7.2 Процедура сохранения программного обеспечения
  7.3 Процедура действий в непредвиденной ситуации: случай обычных неисправностей
  7.4 Порядок действий в непредвиденной ситуации: случай логического воздействия (атаки)
  7.5 Порядок действий в непредвиденной ситуации: случай «катастрофический»
8 Безопасный обмен информацией по средствам связи
  8.1 Криптографическое обеспечение безопасности
  8.2 Безопасность каналов и доступов передачи
9 Управление конфигурацией
Приложение А (справочное) Принятые обязательства

Приложение Н
(справочное)

Канадский справочник по безопасности информационных технологий

В настоящем приложении приведено краткое описание справочника [9].

Область применения

Настоящий справочник помогает обеспечивать безопасность компьютеризованных ресурсов (включая аппаратные и программные средства) путем разъяснения важных концепций, вопросов стоимости и взаимодействия средств управления безопасностью. Справочник показывает преимущества внедрения средств управления безопасностью, основные технологии или подходы для каждого вида средства обеспечения безопасности.

Настоящий справочник дает широкий обзор компьютерной безопасности с тем, чтобы пользователь мог понять свои нужды в этой области и разработать правильный подход к выбору подходящих средств управления безопасностью. Справочник NIST не содержит описания этапов, необходимых для реализации программы обеспечения компьютерной безопасности. Настоящий справочник NIST предоставляет подробные методики внедрения средств управления безопасностью или предлагает руководящие указания по аудиту безопасности специальных систем. В конце каждой главы справочника NIST приведены ссылочные данные.

Настоящий справочник не содержит требований. В нем рассматриваются преимущества использования различных средств управления компьютерной безопасностью и ситуации, в которых их применение может быть необходимым. Особые требования для национальных систем выделены в тексте. Справочник содержит рекомендации и руководящие указания и не предусматривает каких-либо мер наказания.

Содержание

I Введение и общий обзор
- 1 Введение
- 2 Элементы компьютерной безопасности
- 3 Распределение ответственности и полномочий
- 4 Общие угрозы: краткий обзор

II Средства менеджмента
- 5 Политика обеспечения компьютерной безопасности
- 6 Менеджмент программы компьютерной безопасности
- 7 Менеджмент риска компьютерной безопасности
- 8 Безопасность и планирование в жизненном цикле компьютерной системы
- 9 Гарантии

III Средства операционного управления
- 10 Управление персоналом/пользователями
- 11 Подготовка к внештатным ситуациям и стихийным бедствиям
- 12 Обработка инцидента в компьютерной безопасности
- 13 Осведомленность, обучение и образование
- 14 Вопросы безопасности при эксплуатации и технической поддержки компьютера
- 15 Безопасность физической и окружающей среды

IV Технические средства управления
- 16 Идентификация и аутентификация
- 17 Логическое управление доступом
- 18 Следы аудита
- 19 Криптография

V Пример
- 20 Оценка и снижение риска для гипотетической компьютерной системы

Приложение I
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 13335-1:2004	ГОСТ Р ИСО/МЭК 13335-1—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
ИСО/МЭК ТО 13335-3:1998	ГОСТ Р ИСО/МЭК ТО 13335-3—2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
ИСО/МЭК ТО 13335-5:2001	ГОСТ Р ИСО/МЭК ТО 13335-5—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
ИСО/МЭК 10181-2:1996	*
ИСО/МЭК 11770-1:1996	*
ИСО/МЭК 9126-1:2001	*
BS 7799-1:1999	*

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

Библиография

[1] BS 7799-1:1999 Code of Practice for Information Security Management
[2] BS 7799-2:1999 Specification for Information Security Management Systems
[3] ETR 237:1996 Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms
[4] IT Baseline Protection Manual, Германия
[5] NIST Computer Security Handbook
[6] ENV 12924:1997 Medical Informatics — Security Categorisation and Protection for Healthcare Information Systems
[7] ISO/TR 13569:2005 Financial services — Information security guidelines
[8] Protection of sensitive information not covered by the Official Secrets Act — Recommendations for computer workstations
[9] Canadian Handbook on Information Technology Security

УДК 004.056:006.354 ОКС 13.110
35.020 Т59

Ключевые слова: информационная технология, информационная безопасность, риск, угроза, уязвимость

Редактор *В. Н. Копысов*
Технический редактор *Н. С. Гришанова*
Корректор *С. В. Смирнова*
Компьютерная верстка *А. П. Финогеновой*

Сдано в набор 26.06.2007. Подписано в печать 19.09.2007. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 7,44. Уч.-изд. л. 6,80. Тираж 351 экз. Зак. 1774.

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

gost.e-ecolog.ru