ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК ТО 13335-3— 2007

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 3

Методы менеджмента безопасности информационных технологий

ISO/IEC TR 13335-3:1998
Information technology — Guidelines for the management of information technology security — Part 3: Techniques for the management of information technology security (IDT)

Издание официальное

БЗ 2—2006/13

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 13335-3:1998 «Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 3. Методы менеджмента безопасности информационных технологий» (ISO/IEC TR 13335-3:1998 «Information technology — Guidelines for the management of information technology security — Part 3: Techniques for the management of information technology security»).

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

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 Структура . . . 1
5 Цель . . . 1
6 Способы управления безопасностью информационных технологий . . . 2
7 Цели, стратегия и политика безопасности информационных технологий . . . 3
7.1 Цели и стратегия безопасности информационных технологий . . . 4
7.2 Политика безопасности информационных технологий . . . 5
8 Основные варианты стратегии анализа риска организации . . . 7
8.1 Базовый подход . . . 7
8.2 Неформальный подход . . . 8
8.3 Детальный анализ риска . . . 9
8.4 Комбинированный подход . . . 9
9 Комбинированный подход . . . 10
9.1 Анализ высокого уровня риска . . . 10
9.2 Базовый подход . . . 10
9.3 Детальный анализ риска . . . 11
9.4 Выбор защитных мер . . . 17
9.5 Приемлемость рисков . . . 21
9.6 Политика безопасности систем информационных технологий . . . 21
9.7 План безопасности информационных технологий . . . 22
10 Выполнение плана информационной безопасности . . . 23
10.1 Осуществление мер защиты . . . 23
10.2 Компетентность по вопросам безопасности . . . 24
10.3 Обучение персонала информационной безопасности . . . 26
10.4 Процесс одобрения информационных систем . . . 27
11 Последующее сопровождение системы . . . 28
11.1 Обслуживание . . . 28
11.2 Проверка соответствия безопасности . . . 28
11.3 Управление изменениями . . . 30
11.4 Мониторинг . . . 30
11.5 Обработка инцидентов . . . 31
12 Резюме . . . 33
Приложение A (справочное) Примерный перечень вопросов, входящих в состав политики безопасности информационных технологий организации . . . 34
Приложение B (справочное) Оценка активов . . . 36
Приложение C (справочное) Перечень типичных видов угроз . . . 38
Приложение D (справочное) Примеры общих уязвимостей . . . 39
Приложение E (справочное) Типология методов анализа риска . . . 41
Приложение F (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 45

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 3

Методы менеджмента безопасности информационных технологий

Information technology. Security techniques. Part 3. Techniques for the management of information technology security

Дата введения — 2007—09—01

1 Область применения

Настоящий стандарт устанавливает методы менеджмента безопасности информационных технологий. В основе этих методов лежат общие принципы, установленные в ИСО/МЭК 13335-1. Стандарт будет полезен при внедрении мероприятий по обеспечению безопасности информационных технологий. Для полного понимания настоящего стандарта необходимо знание концепций и моделей, менеджмента и планирования безопасности информационных технологий, установленных в ИСО/МЭК 13335-1.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

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 13335-4:2004 Информационная технология. Рекомендации по менеджменту безопасности информационных технологий. Часть 4. Выбор мер защиты.

3 Термины и определения

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

4 Структура

Настоящий стандарт содержит 12 разделов. Раздел 5 содержит информацию о цели настоящего стандарта. В разделе 6 приведен общий обзор способов управления безопасностью информационных технологий. В разделе 7 приведены цели, стратегия и политика обеспечения безопасности информационных технологий. Раздел 8 содержит описание вариантов стратегии анализа риска. В разделе 9 приведено детальное описание комбинированного подхода анализа риска. Раздел 10 посвящен вопросам применения защитных мер, а также подробному обсуждению программ ознакомления персонала с мерами обеспечения безопасности и процесса их одобрения. Раздел 11 содержит описание работ по последующему наблюдению за системой, необходимых для обеспечения эффективного действия средств защиты. И наконец, в разделе 12 приведено краткое описание настоящего стандарта.

5 Цель

Цель настоящего стандарта — дать необходимые описания и рекомендации по способам эффективного управления безопасностью информационных технологий. Эти способы могут быть использованы для оценки требований по безопасности и рисков. Кроме того, они должны помочь устанавливать и поддержи-

Издание официальное

вать необходимые средства обеспечения безопасности, то есть правильный уровень обеспечения безопасности информационных технологий. Может возникнуть необходимость в том, чтобы результаты, полученные таким образом, были усилены за счет применения дополнительных средств защиты применительно к данной организации и данной среде. Настоящий стандарт предназначен для сотрудников организации, ответственных за управление безопасностью информационных технологий и/или за внедрение мер обеспечения их безопасности.

6 Способы управления безопасностью информационных технологий

Процесс управления безопасностью информационных технологий основывается на принципах, изложенных в ИСО/МЭК 13335-1, и может быть реализован как в масштабе всей организации, так и в конкретной ее части. На схеме (см. рисунок 1) приведены основные этапы этого процесса, а также показана обратная связь между результатами процесса и его отдельными частями. Такая обратная связь должна устанавли-

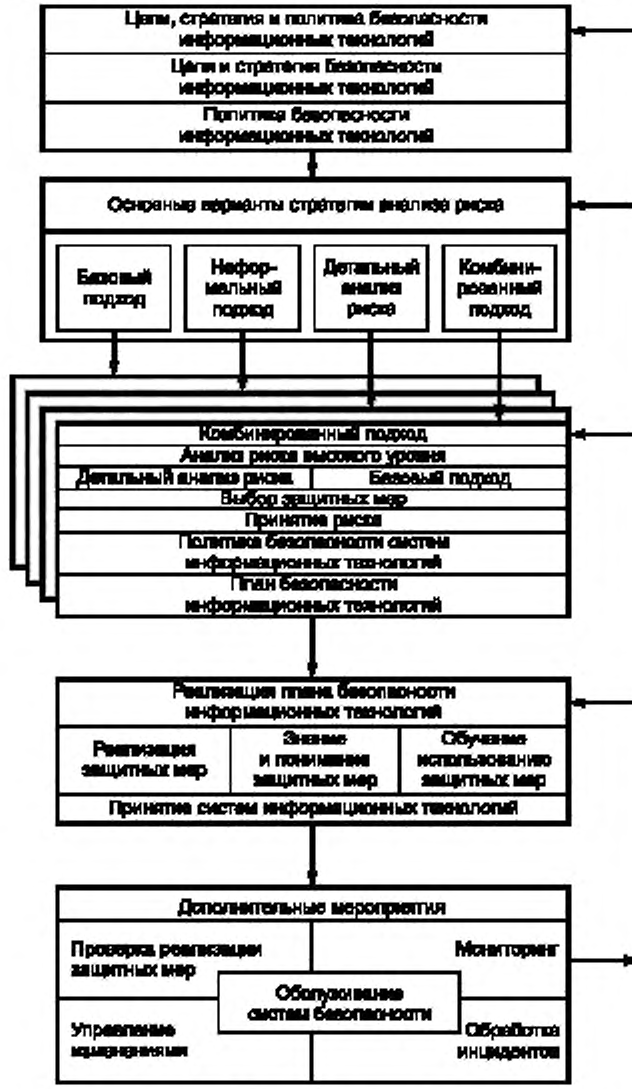


Рисунок 1 — Схема управления безопасностью информационных технологий

ваться по мере необходимости как в пределах продолжительности одного из этапов, так и после завершения одного или нескольких этапов. Данная схема демонстрирует основные направления, рассматриваемые в настоящем стандарте.

Управление безопасностью информационных технологий включает в себя анализ требований по обеспечению безопасности, разработку плана выполнения этих требований, реализацию положений этого плана, а также управление и административный контроль над реализуемой системой безопасности. Этот процесс начинается с определения целей и стратегии, которые устанавливает для себя организация в целях обеспечения безопасности и разработки политики безопасности информационных технологий.

Важной частью процесса управления безопасностью информационных технологий является оценка уровня риска и методов снижения его до приемлемого уровня. Необходимо при этом учитывать направленность деловой деятельности организации, ее организационную структуру и условия эксплуатации системы ИТ, а также специфические вопросы и виды рисков, присущие каждой системе обеспечения безопасности информационных технологий.

После проведения оценки требований безопасности, предъявляемых к системам информационных технологий и отдельным видам услуг, следует выбрать стратегию анализа риска. Основные варианты такой стратегии подробно рассматриваются в разделе 8. Для выделения системы с высоким уровнем риска необходимо провести анализ уровня риска и выбрать варианты стратегии обеспечения безопасности информационных технологий. Затем выделенные системы рассматриваются с использованием метода детального анализа риска, а для остальных систем может применяться базовый подход (с принятием базового уровня риска). Применительно к системам с высоким уровнем риска подробно рассматриваются активы, возможные угрозы и уязвимости системы в целях проведения детального анализа риска, что позволит облегчить выбор эффективных защитных мер, которые будут соответствовать оценкам уровня риска. Использование данного варианта базового подхода позволит сосредоточить процесс управления риском на областях, отличающихся наивысшим уровнем риска или требующих наибольшего внимания. Таким образом может быть разработана программа, характеризующаяся наименьшими затратами времени и средств.

После оценки уровня риска для каждой системы информационных технологий определяют соответствующие меры защиты, направленные на снижение уровня риска до приемлемого уровня. Эти меры реализуются в соответствии с планом безопасности информационных технологий. Реализация плана должна сопровождаться выполнением программ знания и понимания мер безопасности и обучения использованию этих мер, что является важным результатом эффективности принятых защитных мер.

Кроме того, управление безопасностью информационных технологий включает в себя решение текущих задач, связанных с проведением различных последующих действий, что может привести к корректировке полученных ранее результатов и принятых решений. Последующие действия включают в себя обслуживание и проверку соответствия безопасности, управление изменениями, мониторинг и обработку инцидентов.

7 Цели, стратегия и политика безопасности информационных технологий

После того как организация сформулировала цели безопасности информационных технологий, должна быть выбрана стратегия безопасности с тем, чтобы сформировать основу для разработки политики безопасности информационных технологий. Разработка политики безопасности ИТ чрезвычайно важна для обеспечения приемлемости результатов процесса менеджмента риска и должного эффекта от снижения уровня риска. Для разработки и эффективной реализации политики безопасности ИТ требуется организационное решение в рамках организации. Важно, чтобы разработанная политика безопасности информационных технологий учитывала цели и конкретные особенности деятельности организации. Она должна соответствовать политике безопасности и деловой направленности организации. При наличии такого соответствия реализация политики безопасности информационных технологий будет способствовать наиболее эффективному использованию ресурсов и обеспечит последовательный подход к проблемам безопасности для широкого диапазона условий функционирования системы.

Может возникнуть необходимость в разработке отдельной и специфической политики безопасности для каждой из систем информационных технологий. Подобная политика должна быть основана на результатах анализа риска (или результатах базового подхода) и соответствовать политике безопасности систем информационных технологий, при этом политика безопасности должна учитывать рекомендации по обеспечению безопасности, выработанные для соответствующей системы.

7.1 Цели и стратегия безопасности информационных технологий

В качестве первого шага в процессе управления безопасностью информационных технологий необходимо рассмотреть вопрос о том, какой общий уровень риска является приемлемым для данной организации. Правильно выбранный уровень приемлемого риска и, соответственно, допустимый уровень безопасности являются ключевыми моментами успешного управления безопасностью. Допустимый общий уровень безопасности определяется целями, которые ставит перед собой организация при создании системы обеспечения безопасности информационных технологий. Для того чтобы оценить и сформулировать такие цели, необходимо изучить имеющиеся активы и определить, насколько ценными они являются для данной организации. Критерием в этом случае является то, насколько важную роль играют информационные технологии в процессе проведения организацией своей деловой деятельности, при этом стоимость самих информационных технологий составляет лишь малую часть общих затрат. При рассмотрении вопроса о том, насколько важны для функционирования организации информационные технологии, необходимо ответить на следующие вопросы:

- какие важные (очень важные) элементы деловой практики предприятия не могут осуществляться без привлечения информационных технологий;
- какие вопросы могут решаться исключительно с помощью использования информационных технологий;
- принятие каких важных решений зависит от достоверности, целостности или доступности информации, обрабатываемой с использованием информационных технологий, или от своевременного получения такой информации;
- какие виды конфиденциальной информации, обрабатываемой с использованием информационных технологий, подлежат защите;
- какие последствия могут наступить для организации после появления нежелательного инцидента нарушения системы обеспечения безопасности?

Ответы на поставленные вопросы могут помочь сформулировать цели создания системы безопасности в организации. Если, например какие-то важные или очень важные элементы деятельности предприятия зависят от достоверности или своевременности полученной информации, то одной из целей создания системы безопасности может стать необходимость обеспечения целостности и оперативности информации в процессе обработки последней системами информационных технологий. Кроме того, при рассмотрении целей создания системы безопасности необходимо учитывать степень важности целей проводимых деловых операций, а также их связь с вопросами безопасности.

В зависимости от поставленных организацией целей создания системы безопасности необходимо выработать стратегию достижения этих целей. Стратегия должна соответствовать ценности защищаемых активов. Если, например ответ на один или несколько приведенных выше вопросов является положительным, то весьма вероятно, что данная организация должна предъявлять повышенные требования к обеспечению безопасности и ей необходимо выбрать стратегию, предусматривающую приложение значительных усилий для выполнения этих требований.

Любая стратегия, направленная на обеспечение информационной безопасности, должна содержать общие положения о том, как организация собирается обеспечить достижение своих целей в этой области. Основное содержание этих положений стратегии будет зависеть от числа, содержания и важности поставленных целей, при этом обычно организация считает необходимым распространить поставленные требования на все свои подразделения. По своему содержанию основные положения стратегий могут иметь как специфический, так и общий характер.

В качестве положений стратегии специфического характера можно привести следующий пример, когда первичной целью системы обеспечения безопасности информационных технологий является, исходя из деловых соображений, необходимость обеспечения высокого уровня доступности. В этом случае одно из направлений стратегии должно заключаться в сведении к минимуму опасности заражения системы информационных технологий вирусами путем повсеместного размещения антивирусных программных средств (или выделения отдельных сайтов, через которые должна проходить вся получаемая информация для ее проверки на наличие вирусов).

В качестве положений общего характера, имеющих общий характер, можно привести следующий пример, когда основная работа организации заключается в оказании информационных услуг, в связи с чем возможные потребители должны быть уверены в защищенности ее систем информационных технологий. В этом случае основным положением стратегии может быть проведение аттестации систем информационных технологий на безопасность с привлечением третьей стороны, обладающей соответствующим опытом.

В качестве других возможных основных положений стратегии безопасности информационных технологий можно, в зависимости от конкретных целей и их комбинаций, привести следующие положения:

- стратегия и методы анализа риска, используемые в масштабе всей организации;
- оценка необходимости разработки политики безопасности информационных технологий для каждой системы;
- оценка необходимости создания рабочих процедур безопасности для каждой системы;
- разработка схемы классификации систем по уровню чувствительности информации в масштабах всей организации;
- оценка необходимости учета и проверка условий безопасности соединений до места подключения к ним других организаций;
- разработка схем обработки инцидентов, связанных с нарушением системы безопасности для универсального использования.

После разработки стратегии безопасности эта стратегия и ее составные элементы должны быть включены в состав политики безопасности информационных технологий организации.

7.2 Политика безопасности информационных технологий

Политика безопасности информационных технологий должна вырабатываться на основе содержания стратегии и целей создания системы обеспечения безопасности. Важно сформировать политику безопасности и затем проводить ее в соответствии с направленностью деятельности организации, состоянием обеспечения безопасности, содержанием политики в области информационных технологий, а также с учетом положений законодательства и нормативных документов в области обеспечения безопасности.

Как было показано в разделе 7.1, важным фактором, влияющим на содержание политики в области обеспечения безопасности информационных технологий, является то, как в организации используются эти технологии. Чем большей является необходимость их использования и чем шире организации приходится их применять, тем более практичной является потребность в обеспечении безопасности информационных технологий для достижения организацией своих деловых целей. При формировании в организации политики безопасности информационных технологий необходимо учитывать сложившуюся практику деловой деятельности, организацию и культуру ведения производства, поскольку они могут повлиять как на подход к обеспечению безопасности, так и на отдельные защитные меры, которые легко встраиваются в одни условия производственной деятельности и могут оказаться неприемлемыми в других.

Перечисленные в политике безопасности информационных технологий мероприятия, касающиеся проблем обеспечения безопасности информационных технологий, могут основываться на целях и стратегии организации, результатах проведенного ранее анализа риска систем безопасности и принципов управления, результатах проведения дополнительных мероприятий, таких как проверка действенности состояния реализованных защитных мер, результатах мониторинга и изучения процесса повседневного использования систем безопасности, а также на содержании отчетов об экстренных ситуациях, связанных с вопросами обеспечения безопасности.

Необходимо рассматривать любые случаи обнаружения серьезных угроз или уязвимостей в системе безопасности, а политика безопасности информационных технологий должна содержать описание общих методов подхода организации к решению указанных проблем обеспечения безопасности. Более подробно методы и действия по обеспечению безопасности систем информационных технологий описываются в политиках безопасности различных систем информационных технологий либо в других подобных документах, например в инструкциях по обеспечению безопасности.

В разработке политики безопасности информационных технологий должны принимать участие:

- персонал служб аудита;
- персонал финансовых служб;
- персонал подразделений, обслуживающих информационные системы, и их пользователей;
- персонал служб, обеспечивающих функционирование вычислительной техники и инфраструктур (т. е. лиц, ответственных за состояние помещений и вспомогательного оборудования, электрооборудования и кондиционеров);
- личный состав;
- персонал служб безопасности;
- руководство организации.

В соответствии с целями безопасности и стратегией, принятой организацией для достижения этих целей, выбирается соответствующий уровень детализации политики обеспечения безопасности информа-

ционных технологий. Описание этой политики должно включать в себя, по меньшей мере, следующую информацию:

- сведения о целях и области ее применения;
- цели системы обеспечения безопасности и их соотношение с правовыми и нормативными обязательствами и деловыми целями организации;
- требования, предъявляемые к системе обеспечения безопасности информационных технологий с точки зрения обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации;
- сведения об управлении безопасностью, включающие в себя данные об ответственности и полномочиях как организации, так и отдельных лиц;
- вариант подхода к управлению риском, принятый организацией;
- пути и способы определения приоритетов при реализации защитных мер;
- сведения об общем уровне безопасности и остаточном риске, необходимых для осуществления управления;
- сведения о наличии общих правил контроля доступа (логический контроль доступа при одновременном контроле физического доступа лиц в здания, рабочие помещения, а также к системам и информации);
- сведения о доведении до персонала мер безопасности и обучении лиц, осуществляемом организацией;
- сведения об общих процедурах контроля и поддержания безопасности;
- общие проблемы обеспечения безопасности, касающиеся обслуживающего персонала;
- средства и способы доведения сути политики безопасности информационных технологий до всех заинтересованных лиц;
- обстоятельства, при которых может быть проведен пересмотр политики безопасности ИТ;
- методы контроля изменений, вносимых в политику безопасности информационных технологий организации.

При разработке политики безопасности информационных технологий с более высокой степенью детализации должны быть дополнительно рассмотрены следующие вопросы:

- модели и процедуры обеспечения безопасности, распространяющиеся на все подразделения организации;
- использование стандартов;
- процедуры внедрения защитных мер;
- особенности подхода к дополнительно проводящимся мероприятиям, таким как:
  - проверка действенности систем обеспечения безопасности,
  - мониторинг использования средств обеспечения безопасности,
  - обработка инцидентов, связанных с нарушением безопасности,
  - мониторинг функционирования системы информационных технологий,
  - обстоятельства, при которых требуется приглашение сторонних экспертов по проблемам обеспечения безопасности.

Примерный перечень вопросов, входящих в состав политики безопасности информационных технологий, приведен в приложении А.

Как уже говорилось в настоящем стандарте, результаты проведенного ранее анализа риска и принципов управления, проверки действующей системы безопасности и инцидентов, связанных с нарушением безопасности, могут отразиться на содержании политики обеспечения безопасности информационных технологий, что, в свою очередь, может привести к пересмотру или доработке ранее сформулированной стратегии (или политики) безопасности ИТ.

Для обеспечения поддержки проведении мероприятий, связанных с вопросами безопасности, необходимо, чтобы политика безопасности информационных систем была одобрена высшим руководством предприятия.

На основе содержания политики безопасности информационных технологий необходимо сформулировать директиву, обязательную для всех руководящих работников и служащих. При этом может потребоваться получение подписи каждого служащего на документе, содержащем положения о его ответственности за поддержание безопасности в пределах организации. Кроме того, должна быть разработана и реализована программа по обеспечению знания и понимания мер безопасности и проведено обучение использованию этих мер.

Должно быть назначено лицо, ответственное за реализацию политики безопасности информационных технологий и обеспечение соответствия политики требованиям и реальному состоянию дел в организации.

Обычно таким ответственным лицом в организации является сотрудник службы безопасности информационных технологий, помимо своих должностных обязанностей отвечающий и за проведение дополнительных мероприятий, которые должны включать в себя контрольный анализ действующих защитных мер, обработку инцидентов, связанных с нарушением системы безопасности и обнаружением уязвимостей в системе, а также внесением изменений в содержание политики безопасности, если в результате проведенных мероприятий возникнет такая необходимость.

8 Основные варианты стратегии анализа риска организации

Прежде чем приступить к любым действиям, связанным с анализом риска, организация должна иметь стратегию проведения такого анализа, причем составные части этой стратегии (методы, способы и т.д.) должны быть отражены в содержании политики обеспечения безопасности информационных технологий. Эти методы и критерии выбора вариантов стратегии анализа риска должны отвечать потребностям организации. Стратегия анализа риска должна обеспечивать соответствие выбранного варианта стратегии условиям осуществления деловых операций и приложения усилий по обеспечению безопасности в тех областях, где это действительно необходимо. Рассматриваемые ниже варианты стратегии представляют собой четыре разных подхода к анализу риска. Основное различие между ними состоит в степени глубины проводимого анализа. Поскольку обычно проведение детального анализа риска для всех систем информационных технологий сопряжено со слишком большими затратами, тогда как поверхностное рассмотрение проблем, связанных с серьезным риском, не дает нужного эффекта, необходимо найти баланс между рассматриваемыми ниже вариантами.

Если не рассматривать вариант стратегии анализа риска, заключающийся в отсутствии принятия каких-либо защитных мер, и допустить, что реально появление различных видов риска неизвестного уровня и интенсивности, то существуют четыре основных варианта стратегии анализа риска организации:

- использование базового подхода (с низкой степенью риска) для всех систем информационных технологий, независимо от уровня риска, которому подвергаются системы, принятие того, что уровень обеспечения безопасности не всегда может оказаться достаточным;
- использование неформального подхода к проведению анализа риска, обращая особое внимание на системы информационных технологий, которые, как представляется, подвергаются наибольшему риску;
- проведение детального анализа риска с использованием формального подхода ко всем системам информационных технологий или
- проведение сначала анализа риска «высокого уровня» с тем, чтобы определить, какие из систем информационных технологий подвержены высокому уровню риска и какие имеют критическое значение для ведения деловых операций, с последующим проведением детального анализа риска для выделенных систем, а для всех остальных — ограничиваются применением базового подхода к проблемам обеспечения безопасности.

Ниже рассматриваются возможные варианты подхода к обеспечению безопасности и приводятся рекомендации по выбору предпочтительных вариантов.

Если организация решит не уделять внимания вопросам безопасности или отложить на потом внедрение защитных мер, то ее руководство должно ясно представлять себе возможные последствия такого решения. Хотя в этом случае отпадает необходимость затрат времени, средств, рабочих или других ресурсов, такое решение имеет ряд недостатков. Если организация не уверена в том, что функционирование ее систем информационных технологий абсолютно не критично к внешним угрозам, она может впоследствии встретиться с серьезными проблемами. Так, организация может нарушить положения каких-либо законодательных и нормативных актов или репутация организации может пострадать в случае несанкционированных доступов к информации и непринятия действий по их предупреждению. Если организацию не очень заботят проблемы обеспечения безопасности информационных технологий или она не имеет систем, безопасность которых важна для ведения деловых операций, она может следовать подобной стратегии. Однако при этом не будет иметь представления о том, насколько хорошо или плохо реальное состояние ее дел, так что для большинства организаций следование такой стратегии вряд ли является правильным.

8.1 Базовый подход

В случае использования первого варианта подхода к анализу риска организация может применить базовый уровень обеспечения безопасности ко всем системам информационных технологий путем выбора стандартных защитных мер безопасности. Перечень рекомендуемых стандартных защитных мер приведен

в документах по базовой безопасности (см. ИСО/МЭК ТО 13335-4); более подробное описание этого варианта подхода см. в 9.2.

Существует ряд преимуществ использования этого варианта подхода, в том числе:

- возможность обойтись минимальным количеством ресурсов при проведении анализа и контроля риска для каждого случая принятия защитных мер и, соответственно, потратить меньше времени и усилий на выбор этих мер;

- при применении базовых защитных мер безопасности можно принять экономически эффективное решение, поскольку те же или схожие базовые защитные меры безопасности могут быть без особых проблем применены во многих системах, если большое число систем в рамках организации функционирует в одних и тех же условиях и предъявляемые к обеспечению безопасности требования соизмеримы.

В то же время этот вариант подхода имеет следующие недостатки:

- если принимается слишком высокий базовый уровень, то для ряда систем информационных технологий уровень обеспечения безопасности будет завышен;

- если базовый уровень будет принят слишком низким, то для ряда систем информационных технологий уровень обеспечения безопасности будет недостаточен, что увеличит риск ее нарушения и

- могут возникнуть трудности при внесении изменений, затрагивающих вопросы обеспечения безопасности. Так, если была проведена модернизация системы, то могут возникнуть сложности при оценке способностей первоначально примененных базовых защитных мер безопасности и далее оставаться достаточно эффективными.

Если все используемые в организации системы информационных технологий характеризуются низким уровнем требований к обеспечению безопасности, то первый вариант стратегии анализа риска может оказаться экономически эффективным. В этом случае базовый уровень безопасности должен выбираться так, чтобы он соответствовал уровню защиты, необходимому для большинства систем информационных технологий. Для большинства организаций всегда существует необходимость использовать некоторые минимальные стандартные уровни для обеспечения защиты важнейшей информации с целью отвечать требованиям правовых и нормативных актов — например требованиям закона о безопасности информации. Однако в случаях, если отдельные системы организации характеризуются различной степенью чувствительности, разными объемами и сложностью деловой информации, использование общих стандартов применительно ко всем системам будет логически неверным, экономически неоправданным.

8.2 Неформальный подход

Второй вариант подхода предусматривает проведение неформального анализа риска, основанного на практическом опыте конкретного эксперта. Неформальный подход предполагает использование знаний и практического опыта специалистов, а не структурных методов.

Этот подход обладает следующими достоинствами:

- не требует использования значительных средств или времени. При его использовании эксперт не должен приобретать дополнительные знания по своей специальности, а затраты времени на анализ риска при этом меньше, чем при проведении детального анализа риска.

Однако данный подход имеет и свои недостатки:

- при отсутствии хотя бы одного элемента базового подхода (первый вариант стратегии анализа риска) или комплексного перечня контрольных операций увеличивается вероятность пропуска ряда важных деталей у всех систем информационных технологий, действующих в организации;

- могут возникнуть трудности при обосновании необходимости реализации защитных мер, определенных по результатам анализа риска, проведенного подобным подходом;

- для экспертов, не обладающих значительным опытом работы в области анализа риска, не существует готовых рекомендаций, которые могли бы облегчить их работу;

- подходы организации к анализу риска в прошлом были продиктованы исключительно оценкой уязвимости систем, т. е. потребность в мерах обеспечения безопасности основывалась на наличии у этих систем уязвимостей без анализа того, существуют ли угрозы, способные реализовать наличие этих уязвимостей (без обоснования реальной необходимости в использовании защитных мер);

- результаты проведения анализа могут в какой-то мере зависеть от субъективного подхода, личных предубеждений эксперта и, кроме того, могут возникнуть проблемы в случае, если специалист, который проводил неформальный анализ, покидает организацию.

С учетом приведенных выше недостатков второй вариант подхода к анализу риска для многих организаций будет неэффективным.

8.3 Детальный анализ риска

Третий вариант подхода предполагает проведение детального анализа риска с получением результатов для всех систем информационных технологий, действующих в организации. Детальный анализ риска включает в себя подробную идентификацию и оценку активов, оценку возможных угроз, которым могут подвергнуться эти активы, а также оценку уровня их уязвимости. Результаты этих операций затем используют для оценки рисков и последующей идентификации обоснованных защитных мер. Третий вариант подхода подробно представлен в 9.3.

Этот вариант подхода имеет следующие преимущества:

- весьма вероятно, что в результате этого подхода для каждой из систем будут определены соответствующие ей защитные меры обеспечения безопасности;

- результаты проведения детального анализа могут быть использованы при управлении изменениями в системе обеспечения безопасности.

В то же время такой вариант подхода характеризуется следующими недостатками:

- для его реализации и получения нужного результата требуется затратить значительное количество средств, времени и квалифицированного труда;

- существует вероятность того, что определение необходимых защитных мер для какой-либо критической системы произойдет слишком поздно, поскольку анализ будет проводиться одинаково тщательно для систем информационных технологий и для проведения анализа всех систем потребуется значительное время.

Таким образом, использование детального анализа риска применительно ко всем системам информационных технологий не рекомендуется. Если принято решение прибегнуть к такому варианту подхода, то возможны следующие дополнительные разновидности его использования:

- стандартный подход, отвечающий критериям настоящего стандарта (например подход по 9.3);

- стандартный подход в разных вариантах, отвечающий потребностям организации; для ряда организаций предпочтительным может быть использование «детального анализа риска» (см. 9.3).

8.4 Комбинированный подход

В соответствии с четвертым вариантом подхода предполагается проводить предварительный анализ высокого уровня риска для всех систем информационных технологий, обращая особое внимание на деловую значимость системы и уровень риска, которому она подвергается. Для систем информационных технологий, которые имеют важное значение для деловой деятельности организации и/или подвержены высокому уровню риска, в первую очередь проводят детальный анализ риска. Для остальных систем информационных технологий следует ограничиться базовым вариантом подхода. Таким образом, комбинированный вариант, сочетающий лучшие свойства подходов, описанных в 8.1 и 8.3, позволяет при сведении к минимуму времени и усилий, затраченных на идентификацию должных защитных мер, обеспечить необходимую защиту систем с высоким уровнем риска.

Кроме того, комбинированный вариант подхода имеет следующие преимущества:

- использование быстрого и простого предварительного анализа риска позволит обеспечить принятие программы анализа риска;

- существует возможность быстро оценить оперативное состояние программы обеспечения безопасности организации, т. е. использование такого подхода будет в значительной мере способствовать успешному планированию;

- ресурсы и средства могут быть вложены туда, где они принесут максимальный эффект, так как они в первую очередь будут направлены в системы, в наибольшей степени нуждающиеся в обеспечении безопасности;

- проведение последующих мероприятий будет более успешным.

Единственный потенциальный недостаток данного варианта подхода состоит в следующем: поскольку предварительный анализ риска проводят исходя из предположения о его возможном высоком уровне, отдельные системы могут быть ошибочно отнесены к системам, не требующим проведения детального анализа риска. К этим системам в дальнейшем будут применены базовые методы обеспечения безопасности. При необходимости можно будет вернуться к рассмотрению этих систем с тем, чтобы удостовериться, не требуют ли они более тщательного по сравнению с базовым подходом рассмотрения.

Использование данного варианта подхода с анализом высокого уровня риска в сочетании с базовым подходом и (если необходимо) детальным анализом риска обеспечивает большинству организаций наиболее эффективное решение проблем. Таким образом, подобный подход является наиболее предпочтительным и будет более подробно рассмотрен в разделе 9.

9 Комбинированный подход

Настоящий раздел содержит указания для реализации рекомендованной выше стратегии комбинированного подхода.

9.1 Анализ высокого уровня риска

Прежде всего проводят предварительный анализ высокого уровня риска с тем, чтобы установить, какой из вариантов подхода (базовый или детальный) лучше подходит для конкретной системы информационных технологий. В ходе проведения такого предварительного анализа рассматривают деловую значимость систем информационных технологий и обрабатываемой с их помощью информации, а также уровня риска с учетом вида деловой деятельности организации. Исходные данные для принятия решения о том, какой вариант подхода является наиболее подходящим для каждой системы информационных технологий, могут быть получены на основе рассмотрения следующих условий:

- деловых целей, для достижения которых организация использует данную систему информационных технологий;
- в какой степени деловая активность предприятия зависит от конкретной системы информационных технологий, т. е. насколько функции, которые организация считает критическими для своего существования или эффективной реализации деловой деятельности, зависят от функционирования этой системы или обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации, обрабатываемой этой системой;
- вложения денежных средств в эту систему информационных технологий, в том числе в ее разработку, обслуживание или замену;
- активов данной системы ИТ, в которые организация вкладывает средства.

После того как эти условия проанализированы, принятие решения обычно не вызывает затруднений. Если целевое назначение системы важно для проведения организацией своей деловой деятельности, если стоимость замены системы высока или средства, вложенные в активы, подвержены высокому уровню риска, то для данной системы необходимо проведение детального анализа риска. Наличие одного из перечисленных выше условий может служить основанием для проведения детального анализа риска.

Придерживаются следующего общего правила: если прекращение функционирования данной системы информационных технологий может причинить ущерб или принести убытки организации, отрицательно повлиять на ее деловую деятельность или активы, то для оценки потенциального риска проводят детальный анализ риска (см. 9.3). Во всех других случаях достаточная безопасность системы может быть обеспечена применением базового подхода (см. 9.2).

9.2 Базовый подход

Цель обеспечения безопасности с помощью базового подхода состоит в том, чтобы подобрать для организации минимальный набор защитных мер для защиты всех или отдельных систем информационных технологий. Используя базовый подход, можно применять соответствующий ему базовый уровень безопасности в организации и, кроме того (см. 9.1), дополнительно использовать результаты детального анализа риска для обеспечения безопасности систем информационных технологий с высоким уровнем риска или систем, играющих важную роль в деловой деятельности организации. Использование базового подхода позволяет снизить инвестиции организации на исследование результатов анализа риска (см. 8.1).

Удовлетворительная защита с помощью базового подхода может быть обеспечена путем использования справочных материалов (каталогов) по защитным мерам безопасности, где можно подобрать набор средств для защиты системы информационных технологий от наиболее часто встречающихся угроз. Базовый уровень безопасности может быть установлен в соответствии с потребностями организации, при этом в проведении детальной оценки угроз, рисков и уязвимости систем не будет необходимости. Все, что нужно сделать, применяя базовый подход к обеспечению безопасности, — выбрать из справочных материалов (каталогов) по защитным мерам безопасности соответствующие пункты которые подходят для рассматриваемой системы информационных технологий. При наличии в системе установленных защитных мер их необходимо сравнить с рекомендуемыми в каталогах. Защитные меры, которые отсутствуют в системе, но могут быть в ней использованы, должны быть реализованы.

Справочные материалы (каталоги) по защитным мерам безопасности могут содержать во-первых, подробное описание рекомендуемых защитных мер, во-вторых, рекомендации с набором требований по обеспечению безопасности, которыми можно воспользоваться при выборе рекомендуемых мер для данной системы. Оба варианта имеют свои преимущества. Сведения о справочных материалах обоих вариантов можно найти в приложениях А — Н, приведенных в ИСО/МЭК ТО 13335-4. Одной из целей базового

подхода является согласование защитных мер в масштабе всей организации, что может быть достигнуто при использовании каждого из указанных выше вариантов.

В настоящее время существует несколько справочников, содержащих перечни базовых защитных мер. Кроме того, в ряде случаев среди компаний, занятых в одной отрасли производства, можно найти компании со схожими условиями ведения деловой деятельности. После изучения их основных потребностей может оказаться, что справочники с перечнем базовых мер безопасности могут быть использованы несколькими различными организациями. Такие справочники можно найти, например, в:

- международных организациях по стандартизации и национальных научно- технических центрах по стандартизации и метрологии;
- научно-технических центрах отраслевых стандартов (или нормативов);
- организациях, имеющих аналогичную деловую деятельность или сопоставимых по масштабам работ.

Любая организация может выработать свой базовый уровень безопасности в соответствии с собственными условиями деловой деятельности и деловыми целями.

9.3 Детальный анализ риска

Как было показано в 8.3, детальный анализ риска для систем информационных технологий предполагает идентификацию всех возможных рисков и оценку их уровня. Необходимость проведения детального анализа риска может быть определена без ненужных затрат времени и средств после анализа высокого уровня риска для всех систем и последующего изучения результатов детального анализа риска, проведенного только для критических систем (см. 8.3) или систем с высоким уровнем риска, в соответствии с 8.4.

Анализ риска проводится путем идентификации нежелательных событий, создающих неблагоприятные деловые ситуации, и определения вероятности их появления. Нежелательные события также могут негативно влиять на деловой процесс, сотрудников организации или любой элемент делового процесса. Такое неблагоприятное воздействие нежелательных событий является сложным сочетанием возможных видов ущерба, наносимого стоимости активов, подвергающихся риску. Вероятность такого события зависит от того, насколько привлекательным является данный актив для потенциального нарушителя, вероятности реализации угроз и легкости, с какой нарушитель может воспользоваться уязвимыми местами системы. Результаты анализа риска позволяют идентифицировать системы информационных технологий с высоким уровнем риска и выбрать меры обеспечения безопасности, которые могут быть использованы для снижения уровня идентифицированного риска до приемлемого уровня.

Менеджмент риска, детальный анализ риска приведены на рисунке 2. Результаты детального анализа риска позволяют проводить выбор обоснованных защитных мер как части процесса управления риском. Требования, предъявляемые к выбранным мерам защиты, должны быть зафиксированы в политике безопасности систем информационных технологий и соответствующем ей плане безопасности. Множество инцидентов, связанных с нарушением системы безопасности, и внешние угрозы могут оказать влияние на требования к обеспечению безопасности системы и вызвать необходимость в пересмотре части анализа риска (или анализа в целом). К таким внешним угрозам могут относиться: недавние существенные изменения в системе, запланированные изменения, а также последствия инцидентов нарушений безопасности, по которым необходимо принимать соответствующие меры.

Существует несколько методов проведения анализа риска, начиная с подходов, основывающихся на перечне контрольных операций, и кончая методами, основанными на структурном анализе системы. При этом могут использоваться как автоматизированные (компьютерные) программы, так и расчет вручную. Любые метод или программа, используемые организацией, должны, по меньшей мере, содержать операции, перечисленные в пунктах 9.3.1—9.3.7. Важно также, чтобы используемые методы не противоречили практике ведения дел, сложившейся в организации.

После завершения первого этапа рассмотрения результатов детального анализа рисков для системы результаты рассмотрения — сведения о активах и их ценностях, угрозах, уязвимостях и уровнях риска, определенных мерах обеспечения безопасности — должны быть сохранены (например в базе данных системы). Применение методов, использующих вспомогательные программные средства, сильно облегчает эту работу.

Представляемая информация, иногда рассматриваемая в качестве модели, может быть затем довольно эффективно использована после того как со временем с ней происходят изменения, не зависящие от конфигурации, типа обрабатываемой информации, сценариев угроз и т. д. При этом в качестве входных данных приводят только сведения об этих изменениях, что позволяет определить влияние изменений на

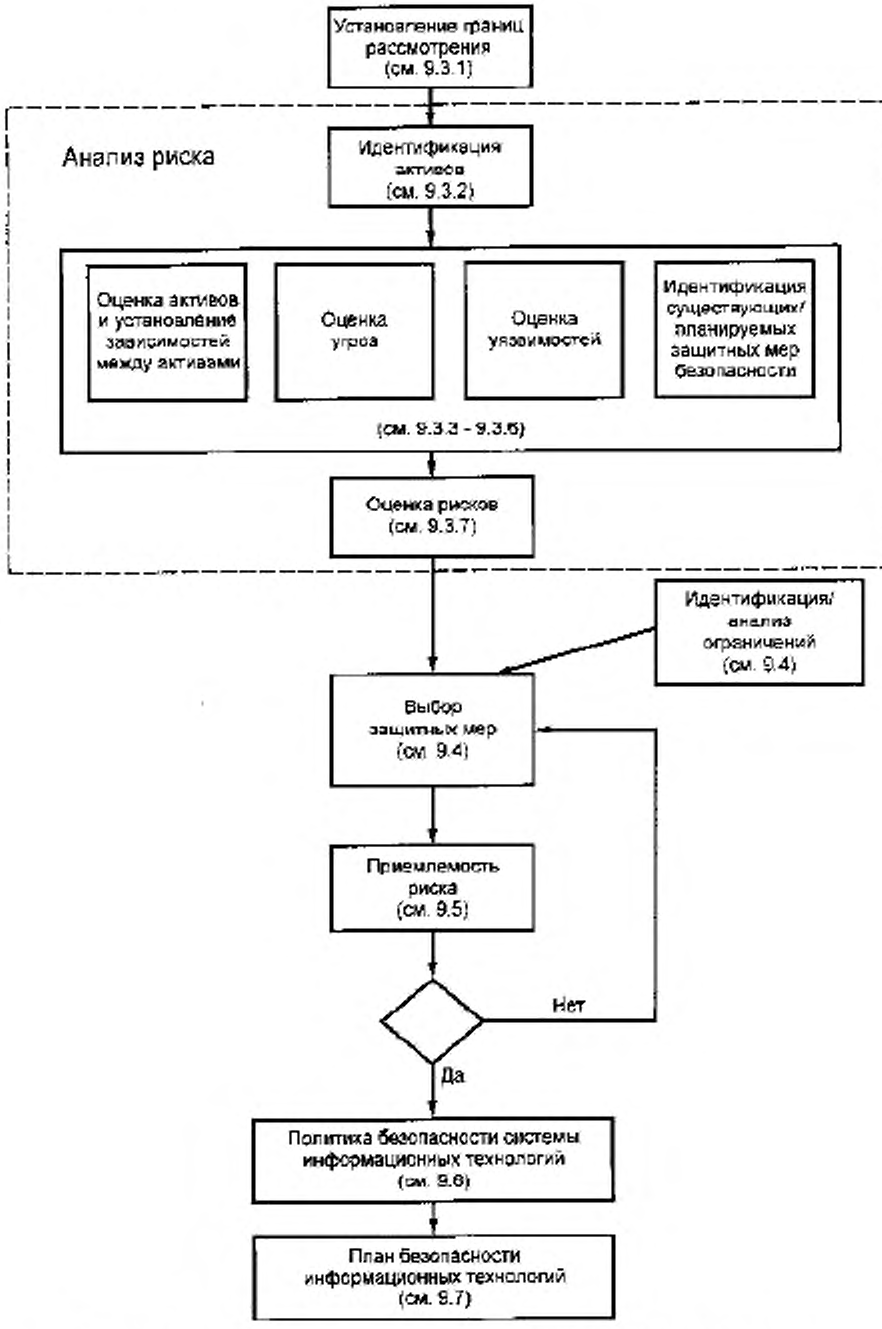


Рисунок 2 — Менеджмент риска с использованием детального анализа риска

необходимые меры обеспечения безопасности. Более того, такие модели могут быть использованы для быстрого изучения различных вариантов, например при разработке новой системы информационных технологий или применительно к другим системам со схожими принципами построения.

9.3.1 Установление границ рассмотрения

Прежде чем получить исходные данные для идентификации и оценки активов, необходимо определить границы рассмотрения (см. рисунок 2). Тщательное определение границ на этой стадии анализа риска позволяет избежать ненужных операций и повысить качество анализа риска. Установление границ рассмотрения должно четко определить, какие из перечисленных ниже ресурсов должны быть учтены при рассмотрении результатов анализа риска. Для конкретной системы информационных технологий учитывают:

- активы информационных технологий (например аппаратные средства, информационное обеспечение, информация);
- служащих (например персонал организации, субподрядчики, персонал сторонних организаций);
- условия осуществления производственной деятельности (например здания, оборудование);
- деловую деятельность (операции).

9.3.2 Идентификация активов

Актив системы информационных технологий является компонентом или частью общей системы, в которую организация напрямую вкладывает средства, и который, соответственно, требует защиты со стороны организации. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства и программное обеспечение. Могут существовать следующие типы активов:

- информация/данные (например файлы, содержащие информацию о платежах или продукте);
- аппаратные средства (например компьютеры, принтеры);
- программное обеспечение, включая прикладные программы (например программы обработки текстов, программы целевого назначения);
- оборудование для обеспечения связи (например телефоны, медные и оптоволоконные кабели);
- программно-аппаратные средства (например гибкие магнитные диски, CD-ROM, программируемые ROM);
- документы (например контракты);
- фонды (например в банковских автоматах);
- продукция организации;
- услуги (например информационные, вычислительные услуги);
- конфиденциальность и доверие при оказании услуг (например услуг по совершению платежей);
- оборудование, обеспечивающее необходимые условия работы;
- персонал организации;
- престиж (имидж) организации.

Активы, включенные в установленные (см. 9.3.1) границы рассмотрения, должны быть обнаружены, и наоборот, — любые активы, выведенные за границы рассмотрения (независимо от того, по каким соображениям это было сделано), должны быть рассмотрены еще раз с тем, чтобы убедиться, что они не были забыты или упущены.

9.3.3 Оценка активов и установление зависимости между активами

После того как все цели процесса идентификации активов были достигнуты и составлен перечень всех активов рассматриваемой системы информационных технологий, должна быть определена ценность этих активов. Ценность актива определяется его важностью для деловой деятельности организации, при этом уровень оценки деловой деятельности может исходить из соображений обеспечения безопасности, т. е. насколько может пострадать деловая деятельность организации и другие активы системы информационных технологий от утечки, искажения, недоступности и/или разрушения информации. Таким образом, идентификация и оценка активов, проведенные на основе учета деловых интересов организации, являются основным фактором в определении риска.

Исходные данные для оценки должны быть получены от владельцев и пользователей активов. Специалист(ы), проводящий(ие) анализ риска, должен(должны) составить перечень активов; при этом следует запросить содействие лиц, непосредственно занимающихся планированием деловой деятельности, финансами, информационными системами и другими соответствующими направлениями деловой активности для определения ценности каждого из активов. Полученные данные соотносят со стоимостью создания и обслуживания актива, а также с возможностью негативного воздействия на деловую деятельность, связанного с нарушением конфиденциальности, целостности, доступности, достоверности и надежности информации. Идентифицированные активы являются ценностью для организации. Однако невозможно непосредственно определить финансовую стоимость каждого из них. Необходимо также определить ценность или степень важности актива для организации в некоммерческой деятельности. В противном случае будет

трудно определить уровень необходимой защиты и объем средств, которые организации следует израсходовать на принятие мер защиты. Примером шкалы оценок может быть определение уровня ценности как «низкий», «средний» или «высокий» или, с большей степенью детализации, «пренебрежимо малый», «низкий», «средний», «высокий», «очень высокий».

Более подробно о возможных уровнях и шкалах оценки, которые могут быть использованы при оценке ценности активов, основываясь на оценке возможного ущерба, см. приложение В. Независимо от используемой шкалы оценок, в ходе проведения оценки необходимо рассмотреть проблемы, связанные с уровнем возможного ущерба, причиной которого может быть:

- нарушение законодательства и/или технических норм;
- снижение уровня деловой активности;
- потеря/ухудшение репутации;
- нарушение конфиденциальности личной информации;
- возникновение угрозы личной безопасности;
- неблагоприятные последствия деятельности правоохранительных органов;
- нарушение конфиденциальности в коммерческих вопросах;
- нарушение общественного порядка;
- финансовые потери;
- перебои в выполнении деловых операций;
- угроза экологического ущерба.

Каждая организация может выдвинуть также собственные критерии оценки, исходя из важности конкретных проблем для своей деловой деятельности; эти критерии следует дополнить критериями, приведенными в приложении В. Кроме того, организация должна установить собственные границы для ущербов, определяемых как «низкие» и «высокие». Так например, финансовый ущерб, катастрофически высокий для небольшой компании, может быть низким или пренебрежимо малым для крупной компании.

На этой стадии процесса оценки следует подчеркнуть, что метод оценки должен обеспечивать получение не только количественных, но и качественных оценок — там, где получение количественных оценок невозможно (например возможность оценки стоимости потери жизни или деловой репутации). Используемая шкала оценок должна быть снабжена соответствующими пояснениями.

Следует также выявить виды зависимости одних активов от других, поскольку наличие таких видов зависимостей может оказать влияние на оценку активов. Например конфиденциальность данных должна быть обеспечена на протяжении всего процесса их обработки, т. е. необходимость обеспечения безопасности программ обработки данных следует напрямую соотнести с уровнем ценности конфиденциальности обрабатываемых данных. Кроме того, если деловая деятельность зависит от целостности вырабатываемых программой данных, то входные данные для этой программы должны иметь соответствующую степень надежности. Более того, целостность информации будет определяться качеством аппаратных средств и программного обеспечения, используемых для ее хранения и обработки. Функционирование аппаратных средств будет также зависеть от качества энергоснабжения и, возможно, от работы систем кондиционирования воздуха. Таким образом, данные о зависимостях, существующих между отдельными активами, будут способствовать идентификации некоторых видов угроз и определению конкретных уязвимостей, а использование данных о зависимостях даст уверенность в том, что активы оценены в соответствии с их реальной ценностью (с учетом существующих взаимозависимостей) и уровень безопасности выбран обоснованно.

Уровни ценности активов, от которых зависят другие активы, могут быть изменены в следующих случаях:

- если уровни ценности зависимых активов (например данных) ниже или равны уровню ценности рассматриваемого актива (например программного обеспечения), то этот уровень останется прежним;
- если уровни ценности зависимых активов (например данных) выше, то уровень ценности рассматриваемого актива (например программного обеспечения) необходимо повысить с учетом:

уровня соответствующей зависимости,

уровней ценности других активов.

Организация может иметь в своем распоряжении некоторые многократно используемые активы, например копии программ систем программного обеспечения или персональные компьютеры, подобные использующимся в большинстве учреждений. Это необходимо учитывать при проведении оценки активов. С одной стороны, копии программ и т. д. в ходе оценки легко упустить из виду, и поэтому следует позаботиться о том, чтобы учесть их все; с другой стороны, их наличие может снизить остроту проблемы доступности информации.

Конечным результатом данного этапа является составление перечня активов и их оценка с учетом таких показателей, как раскрытие информации (сохранение конфиденциальности), изменение данных (сохранение целостности), невозможность доступа и разрушение информации (сокращение доступности) и стоимость замены.

9.3.4 Оценка угроз

Угроза (потенциальная возможность неблагоприятного воздействия) обладает способностью наносить ущерб системе информационных технологий и ее активам. Если эта угроза реализуется, она может взаимодействовать с системой и вызвать нежелательные инциденты, оказывающие неблагоприятное воздействие на систему. В основе угроз может лежать как природный, так и человеческий фактор; они могут реализовываться случайно или преднамеренно. Источники как случайных, так и преднамеренных угроз должны быть идентифицированы, а вероятность их реализации — оценена. Важно не упустить из виду ни одной возможной угрозы, так как в результате возможно нарушение функционирования или появление уязвимостей системы обеспечения безопасности информационных технологий.

Исходные данные для оценки угроз следует получать от владельцев или пользователей активов, служащих отделов кадров, специалистов по разработке оборудования и информационным технологиям, а также лиц, отвечающих за реализацию защитных мер в организации. Другие организации, например федеральное правительство и местные органы власти, также могут оказать помощь при проведении оценки угроз, например предоставить необходимые статистические данные. Полезным может быть использование перечня наиболее часто встречающихся угроз (примеры типичных видов угроз приведены в приложении С). Также полезно использование каталогов угроз (наиболее соответствующих нуждам конкретной организации или виду ее деловой деятельности), так как ни один перечень не может быть достаточно полным. Ниже приведены некоторые наиболее часто встречающиеся варианты угроз:

- ошибки и упущения;
- мошенничество и кража;
- случаи вредительства со стороны персонала;
- ухудшение состояния материальной части и инфраструктуры;
- программное обеспечение хакеров, например имитация действий законного пользователя;
- программное обеспечение, нарушающее нормальную работу системы;
- промышленный шпионаж.

При использовании материалов каталогов угроз или результатов ранее проводившихся оценок угроз следует иметь в виду, что угрозы постоянно меняются, особенно в случае смены организацией деловой направленности или информационных технологий. Например, компьютерные вирусы 90-х годов представляют гораздо более серьезную угрозу, чем компьютерные вирусы 80-х. Нужно также отметить, что следствием внедрения таких мер защиты, как антивирусные программы, вероятно, является постоянное появление новых вирусов, не поддающихся воздействию действующих антивирусных программ.

После идентификации источника угроз (кто и что является причиной угрозы) и объекта угрозы (какой из элементов системы может подвергнуться воздействию угрозы) необходимо оценить вероятность реализации угрозы. При этом следует учитывать:

- частоту появления угрозы (как часто она может возникать согласно статистическим, опытным и другим данным), если имеются соответствующие статистические и другие материалы;

- мотивацию, возможности и ресурсы, необходимые потенциальному нарушителю и, возможно, имеющиеся в его распоряжении; степень привлекательности и уязвимости активов системы информационных технологий с точки зрения возможного нарушителя и источника умышленной угрозы;

- географические факторы — такие как наличие поблизости химических или нефтеперерабатывающих предприятий, возможность возникновения экстремальных погодных условий, а также факторов, которые могут вызвать ошибки у персонала, выход из строя оборудования и послужить причиной реализации случайной угрозы.

В зависимости от требуемой точности анализа может возникнуть необходимость разделить активы на отдельные компоненты и рассматривать угрозы относительно этих компонентов. Например, одним из таких активов можно считать актив, обозначенный как «центральные серверы обслуживания данных», но если эти серверы расположены в различных географических точках, то этот актив необходимо разделить на «центральный сервер 1» и «центральный сервер 2», поскольку для серверов одни угрозы могут различаться по характеру опасности, а другие — по степени опасности. Таким образом актив, включающий в себя программное обеспечение под объединенным названием «прикладное программное обеспечение», затем можно разбить на два или более элемента «прикладного программного обеспечения». Например, содержа-

щий данные актив, вначале обозначенный как «досье на преступников», разбивают на два: «текст досье на преступников» и «изобразительная информация к досье на преступников».

После завершения оценки угроз составляют перечень идентифицированных угроз, активов или групп активов, подверженных этим угрозам, а также определяют степень вероятности реализации угроз с разбивкой на группы высокой, средней и низкой вероятности.

9.3.5 Оценка уязвимости

Этот вид оценки предполагает идентификацию уязвимостей окружающей среды, организации, процедур, персонала, менеджмента, администрации, аппаратных средств, программного обеспечения или аппаратура связи, которые могли бы быть использованы источником угроз для нанесения ущерба активам и деловой деятельности организации, осуществляемой с их использованием. Само по себе наличие уязвимостей не наносит ущерба, поскольку для этого необходимо наличие соответствующей угрозы. Наличие уязвимости при отсутствии такой угрозы не требует применения защитных мер, но уязвимость должна быть зафиксирована и в дальнейшем проверена на случай изменения ситуации. Следует отметить, что некорректно использующиеся, а также неправильно функционирующие защитные меры безопасности могут сами по себе стать источниками появления уязвимостей.

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива, которые могут использоваться иным образом или для иных целей, чем те, для которых приобретался или изготавливался данный актив. Например, одним из свойств электрически стираемого перепрограммируемого постоянного устройства (ЭСППЗУ) является то, что хранящаяся в нем информация может быть стерта или заменена (одно из свойств конструкции ЭСППЗУ). Однако наличие такого свойства означает также возможность несанкционированного уничтожения информации, хранящейся на ЭСППЗУ, т. е. мы имеем дело с возможной уязвимостью.

В процессе оценки уязвимости происходит идентификация уязвимостей, в которых могут быть реализованы возможные угрозы, а также оценка вероятного уровня слабости, т. е. легкости реализации угрозы. Например, отдельные виды активов можно легко продать, скрыть или переместить — эти их свойства могут быть связаны с наличием уязвимости. Исходные данные для оценки уязвимости должны быть получены от владельцев или пользователей актива, специалистов по обслуживающим устройствам, экспертов по программным и аппаратным средствам систем информационных технологий. Примерами уязвимостей могут быть:

- незащищенные подсоединения (например к Интернету);
- неквалифицированные пользователи;
- неправильный выбор и использование пароля доступа;
- отсутствие должного контроля доступа (логического и/или физического);
- отсутствие резервных копий информационных данных или программного обеспечения;
- расположение ресурсов в районах, подверженных затоплению.

Примеры других общих уязвимостей приведены в приложении D.

Важно оценить, насколько велика степень уязвимости или насколько легко ее можно использовать. Степень уязвимости следует оценивать по отношению к каждой угрозе, которая может использовать эту уязвимость в конкретной ситуации. Например, система может оказаться уязвимой к угрозе нелегального проникновения при идентификации пользователя и несанкционированного использования ресурсов. С одной стороны, степень уязвимости по отношению к нелегальному проникновению при идентификации пользователя может быть высокой в связи с отсутствием аутентификации пользователей. С другой стороны степень уязвимости по отношению к несанкционированному использованию ресурсов может быть низкой, поскольку даже при отсутствии аутентификации пользователей способы несанкционированного использования ресурсов ограничены.

После завершения оценки уязвимостей должен быть составлен перечень уязвимостей и проведена оценка степени вероятности возможной реализации отмеченных уязвимостей, например «высокая», «средняя» или «низкая».

9.3.6 Идентификация существующих/планируемых защитных мер

Использование идентифицированных после рассмотрения результатов анализа риска защитных мер должно проводиться с учетом уже существующих или планируемых защитных мер. Действующие или планируемые защитные меры должны быть частью общего процесса, во избежание не вызываемых необходимостью затрат труда и средств, т. е. дублирования защитных мер. Кроме того, использование действующих или планируемых защитных мер может происходить без должного обоснования. В этом случае необходимо проверить, следует ли заменить меры обеспечения безопасности новыми, более обоснованными, или сохранить прежние (например по экономическим соображениям).

Кроме того, необходимо провести дополнительную проверку с тем, чтобы определить, являются ли защитные меры безопасности, выбранные после проведения анализа риска (см. 9.4), совместимыми с действующими и планируемыми мерами безопасности (т. е. выбранные и действующие меры безопасности не должны противоречить друг другу).

В процессе идентификации уже действующих защитных мер безопасности необходимо проверить, правильно ли они функционируют. Если предполагается, что какое-то средство защитной меры безопасности функционирует правильно, однако это не подтверждается в процессе осуществления деловых операций, то функционирование его может стать источником возможной уязвимости.

По результатам проведения идентификации защитных мер составляют перечень действующих и планируемых защитных мер безопасности с указанием статуса их реализации и использования.

9.3.7 Оценка рисков

Целью данного этапа является идентификация и оценка рисков, которым подвергаются рассматриваемая система информационных технологий и ее активы с тем, чтобы идентифицировать и выбрать подходящие и обоснованные защитные меры безопасности. Величина риска определяется ценностью подвергающихся риску активов, вероятностью реализации угроз, способных оказать негативное воздействие на деловую активность, возможностью использования уязвимостей идентифицированными угрозами, а также наличием действующих или планируемых защитных мер, использование которых могло бы снизить уровень риска.

Существуют различные способы учета таких факторов (активы, угрозы, уязвимости), например, можно объединить оценки риска, связанные с активами, уязвимостями и угрозами, для того, чтобы получить оценки измерения общего уровня риска. Различные варианты подхода к анализу риска, основанные на использовании оценок, полученных для активов, уязвимостей и угроз, см. приложение Е.

Вне зависимости от использованного способа оценки измерения риска результатом оценки прежде всего должно стать составление перечня оцененных рисков для каждого возможного случая раскрытия, изменения, ограничения доступности и разрушения информации в рассматриваемой системе информационных технологий. Составленный перечень оцененных рисков затем используют при идентификации рисков, на которые следует обращать внимание в первую очередь при выборе защитных мер. Метод оценки рисков должен быть повторяемым и прослеживаемым.

Как уже говорилось выше (см. 9.3), для ускорения всех или отдельных элементов процесса анализа риска могут использоваться различные автоматизированные программные средства. Если организация решит использовать такие средства, необходимо проследить, чтобы выбранный подход соответствовал принятым в организации стратегии и политике безопасности информационных технологий. Кроме того, следует обратить особое внимание на правильность используемых входных данных, поскольку качество работы программных средств определяется качеством входных данных.

9.4 Выбор защитных мер

Для снижения оцененных уровней риска до приемлемых необходимо отобрать и идентифицировать подходящие и обоснованные меры безопасности. Для правильности выбора необходимо принять во внимание наличие действующих или запланированных мер безопасности, структуру обеспечения безопасности информационных технологий и наличие ограничений различного типа (см. 9.3.6, 9.4.2 и 9.4.3). Дополнительные рекомендации по выбору защитных мер — в соответствии с ИСО/МЭК ТО 13335-4.

9.4.1 Определение защитных мер

Результаты оценки уровня риска, проведенной на предыдущем этапе (см. 9.3), должны использоваться в качестве основы для идентификации защитных мер, необходимых для должного обеспечения безопасности системы.

Для выбора защитных мер, обеспечивающих эффективную защиту при некоторых уровнях риска, необходимо рассмотреть результаты анализа риска. Наличие уязвимости к определенным видам угроз позволяет определить, где и в какой форме необходимо использование дополнительных мер защиты.

Возможны также альтернативные варианты использования защитных мер, выбор которых производится исходя из стоимости рассмотренных защитных мер. Область использования защитных мер включает в себя:

- физическую окружающую среду;
- обслуживающий персонал;
- администрацию;
- аппаратные средства/программное обеспечение;
- средства обеспечения связи (коммуникации).

Действующие и запланированные меры защиты безопасности следует рассмотреть повторно с точки зрения их сравнительной стоимости (с учетом стоимости обслуживания) и принять решение об их невключении (или отказе от их реализации) или доработке, если они недостаточно эффективны. Следует отметить, что иногда удаление недостаточно эффективных действующих защитных мер обходится дороже, чем их использование и принятие дополнительных защитных мер (в случае необходимости). Возможны также случаи, когда действие защитных мер может быть распространено на активы, находящиеся вне установленных границ рассмотрения (см. 9.3.1).

Для идентификации защитных мер полезно рассмотреть уязвимости системы, требующие защиты, и виды угроз, которые могут реализоваться при наличии этих уязвимостей. Существуют следующие возможности снижения уровня риска:

- избегать риска;
- уступить риск (например, путем страховки);
- снизить уровень угроз;
- снизить степень уязвимости системы ИТ;
- снизить возможность воздействия нежелательных событий;
- отслеживать появление нежелательных событий, реагировать на их появление и устранять их последствия.

Какая из этих возможностей (или их сочетание) окажется наиболее приемлемой для конкретной организации, зависит от конкретных обстоятельств. Существенную помощь может оказать также использование справочных материалов (каталогов) по защитным мерам безопасности. Однако при использовании защитных мер, выбранных по каталогу, необходимо их доработать с тем, чтобы они соответствовали специфическим требованиям организации.

Другим важным аспектом выбора защитных мер являются экономические соображения. Не следует рекомендовать использование защитных мер, стоимость реализации и эксплуатации которых превышала бы стоимость защищаемых активов. Также нерационально рекомендовать использование защитных мер, стоимость которых превышает бюджет той организации, где предполагается их использование. Однако следует с большой осторожностью подходить к случаям, когда из-за ограниченности бюджета приходится уменьшать число или снижать качество реализуемых защитных мер, поскольку это подразумевает возможность более высокого, чем планировалось, уровня риска. Принятый бюджет организации на защитные меры должен с осторожностью использоваться в качестве ограничивающего затраты фактора.

В случае, если для обеспечения безопасности системы информационных технологий используется базовый подход, выбор защитных мер сравнительно прост. Справочные материалы (каталоги) по защитным мерам безопасности предлагают набор защитных мер, способных защитить систему информационных технологий от наиболее часто встречающихся видов угроз. В этом случае рекомендуемые каталогом меры обеспечения безопасности следует сравнить с уже действующими или запланированными, а упомянутые в каталоге меры (отсутствующие или применение которых не планируется) должны составить перечень защитных мер, которые необходимо реализовать для обеспечения базового уровня безопасности.

Выбор защитных мер должен всегда включать в себя комбинацию организационных (не технических) и технических мер защиты. В качестве организационных рассматриваются меры, обеспечивающие физическую, персональную и административную безопасность.

Защитные меры для физической безопасности включают в себя обеспечение прочности внутренних стен зданий, использование кодовых дверных замков, систем пожаротушения и охранных служб. Обеспечение безопасности персонала включает в себя проверку лиц при приеме на работу (особенно лиц, нанимающихся на важные с точки зрения обеспечения безопасности должности), контроль за работой персонала и реализацию программ знания и понимания мер защиты.

Административная безопасность включает в себя безопасные способы ведения документации, наличие методов разработки и принятия прикладных программ, а также процедур обработки инцидентов в случаях нарушения систем безопасности. При таком способе обеспечения безопасности очень важно, чтобы для каждой системы была разработана система ведения деловой деятельности организации, предусматривающая в том числе возможность появления непредвиденных обстоятельств (ликвидацию последствий нарушения систем безопасности) и включающая в себя соответствующую стратегию и план (планы). План должен содержать подробные сведения о важнейших функциях и приоритетах, подлежащих восстановлению, необходимых условиях обработки информации и способах организации, которые необходимо осуществлять в случае аварии или временного прекращения работы системы. План должен содержать перечень шагов, которые следует предпринять для обеспечения безопасности важнейшей информации, подлежащей обработке, не прекращая при этом ведения организацией деловых операций.

Технические меры защиты предусматривают защиту аппаратных средств и программного обеспечения, а также систем связи. При этом выбор защитных мер проводят в соответствии с их степенью риска для обеспечения функциональной пригодности и надежной системы безопасности. Функциональная пригодность системы должна включать в себя, например проведение идентификации и аутентификации пользователя, выполнение требований логического контроля допуска, обеспечение ведения контрольного журнала и регистрацию происходящих в системе безопасности событий, обеспечение безопасности путем обратного вызова запрашивающего, определение подлинности сообщений, шифрование информации и т. д. Требования к надежности систем безопасности определяют уровень доверия, необходимый при осуществлении функций безопасности, и тем самым определяют виды проверок, тестирования безопасности и т. д., обеспечивающих подтверждение этого уровня. При принятии решения об использовании дополнительного набора организационных и технических защитных мер могут быть выбраны разные варианты выполнения требований к обеспечению технической безопасности. Следует определить структуру технической безопасности для каждого из данных вариантов, с помощью которой можно получить дополнительное подтверждение правильности построения системы безопасности и возможности ее реализации на заданном технологическом уровне.

Организация может выбрать применение продукции и систем, прошедших оценку, в качестве одного из способов решения задачи окончательного построения системы безопасности. Продукцией и системой, прошедшими оценку, считаются те, испытания которых проводились третьей стороной. Этой третьей стороной может быть другое подразделение той же организации или независимая организация, специализирующаяся на оценке продукции и/или систем. Испытания могут проводиться на соответствие набору заранее установленных критериев оценки, которые формулируются, исходя из особенностей создаваемой системы; в то же время может существовать обобщенный набор критериев оценки, соответствующих различным ситуациям. Критерии оценки продукции могут определять требования к функциональности и/или надежности продукции и систем. Существует несколько схем оценки качества продукции, многие из них формируются по заказу правительственных служб и международных организаций по стандартизации. Организация может принять решение об использовании продукции и/или систем, прошедших оценку, если ей требуется уверенность в том, что продукция отвечает требованиям к функциональности, и необходимы гарантии точности и полноты реализации элементов функциональности продукции и систем. В качестве альтернативы использованию оцененной продукции проводят целевые практические испытания продукции на безопасность, положительные результаты которых могут дать уверенность в качестве и безопасности поставляемой продукции.

В процессе выбора защитных мер, предлагаемых для реализации, необходимо учитывать ряд факторов, таких как:

- доступность использования защитных мер;
- прозрачность защитных мер для пользователя;
- в какой мере использование защитных мер помогает пользователю решать свои задачи;
- относительная надежность (стойкость) системы безопасности;
- виды выполняемых функций — предупреждение, сдерживание, обнаружение, восстановление, исправление, мониторинг и обмен информацией.

Обычно защитные меры предназначены для выполнения только некоторых из числа перечисленных выше функций (чем больше, тем лучше). При рассмотрении системы безопасности в целом или набора используемых защитных мер следует установить (если возможно) необходимые пропорции между видами функций, что позволит обеспечить большую эффективность и действенность системы обеспечения безопасности в целом. Может потребоваться проведение анализа рентабельности или анализа компромиссного решения (метод сравнения возможных альтернативных вариантов с использованием набора критериев, каждому из которых придается свое значение весового коэффициента в зависимости от его относительной важности применительно к определенной ситуации).

9.4.2 Структура безопасности информационных технологий

Структура безопасности информационных технологий отражает процесс обеспечения требований безопасности для отдельной системы информационных технологий как части общей структуры системы. Поэтому так важно рассмотрение структуры обеспечения безопасности информационных технологий в процессе выбора защитных мер.

Структура безопасности информационных технологий может использоваться при разработке новых систем, а также при внесении существенных изменений в существующие системы. Данная структура основывается на результатах анализа риска или базового подхода, должна учитывать требования к обеспече-

нию безопасности и на их основе разработать набор технических мер защиты по обеспечению безопасности систем. В ряде случаев, если изменения вносят в существующие системы, некоторые требования могут быть в форме специфических защитных мер, которые должны быть использованы.

В структуре безопасности информационных технологий особое внимание уделяют техническим защитным мерам по обеспечению безопасности и достижению с их помощью целей безопасности; при этом следует принимать во внимание также соответствующие нетехнические средства обеспечения безопасности. Хотя структура безопасности может быть построена на основе использования ряда различных подходов и перспектив, следует всегда учитывать следующий фундаментальный принцип ее построения: нельзя допускать неблагоприятное воздействие проблемы обеспечения безопасности в пределах уникальной зоны безопасности (зоны с одинаковыми или схожими требованиями к обеспечению безопасности и средствам ее защиты) на обеспечение безопасности в другой отдельной зоне безопасности. Структура безопасности информационных технологий обычно включает в себя одну или более зон безопасности. Зоны безопасности должны соответствовать областям деловой деятельности организации. Эти области деловой деятельности могут соответствовать функциональным секторам отдельных видов деловой деятельности организации, таким как выплата заработной платы, производство продукции или обслуживание покупателей, или они могут соответствовать функциональным секторам таких видов деятельности, как обслуживание электронной почты или выполнение конторских операций.

В зависимости от наличия одного или нескольких признаков существуют различные типы зон безопасности. Примерами признаков могут быть:

- уровни, категории или виды информации, доступные в пределах зоны безопасности;
- операции, которые могут проходить в пределах зоны безопасности;
- объединения по интересам, ассоциируемые с зоной безопасности;
- отношения к другим зонам безопасности и окружающим их средам;
- виды функций или доступ к информации, которые могут запрашивать объединения по интересам внутри зоны безопасности.

При построении структуры обеспечения безопасности информационных технологий необходимо также учитывать следующие проблемы:

- взаимоотношения и взаимозависимости между отдельными зонами безопасности;
- роль (или участие) взаимоотношений и взаимозависимостей в снижении качества услуг по обеспечению безопасности;
- необходимость организации дополнительных услуг или принятия дополнительных мер защиты для исправления, контроля или недопущения случаев снижения качества услуг.

Структура безопасности информационных технологий не существует сама по себе, но опирается на содержание других документов по информационным технологиям и согласовывается с ними. Наиболее важными из этих документов являются структура системы информационных технологий и структуры других соответствующих систем (аппаратные средства, средства связи и прикладные программы). Структура безопасности информационных технологий не должна содержать полного описания системы ИТ, а только описание технических вопросов и элементов, касающихся обеспечения безопасности. Назначение этой структуры состоит в том, чтобы свести к минимуму случаи неблагоприятного воздействия на пользователей, обеспечивая при этом оптимальную внутреннюю защиту инфраструктуры систем ИТ.

К структуре безопасности информационных технологий имеет отношение множество других документов или она может находиться в подчиненном положении по отношению к ним. К числу таких документов относятся:

- проект безопасности информационных технологий;
- рабочая концепция безопасности информационных технологий;
- план безопасности информационных технологий;
- политика безопасности системы информационных технологий;
- документы по сертификации и аккредитации системы информационных технологий (в случае необходимости).

9.4.3 Идентификация и анализ ограничений

На выбор мер защиты влияют многие ограничения. Эти ограничения необходимо принимать во внимание при разработке и реализации рекомендаций. К типичным ограничениям относят:

- ограничения по времени.

Может существовать множество видов ограничений по времени. Например, первый вид — защитная мера безопасности — должен быть реализован в пределах периода времени, приемлемого для руковод-

ства организации. Второй вид ограничения по времени — реализация конкретной защитной меры безопасности в пределах жизненного срока соответствующей системы. Третьим видом ограничения по времени может быть длительность периода времени, необходимого руководству организации для принятия решения о том, стоит ли и дальше подвергать систему угрозам наличия конкретного риска;

- финансовые ограничения.

Стоимость реализации рекомендуемых мер защиты не должна превышать ценности активов, для безопасности которых они предназначены. Необходимо сделать все возможное, чтобы не выйти за пределы выделенных на эти цели ассигнований. Однако в ряде случаев достижение необходимого уровня безопасности и приемлемого уровня риска может оказаться невозможным в пределах подобных финансовых ограничений. В этом случае выход из сложившейся ситуации предоставляется на усмотрение руководства организации;

- технические ограничения.

Технические проблемы, например совместимость программ или аппаратных средств, легко разрешаются, если уделить им серьезное внимание в процессе выбора средств защиты. Кроме того, при реализации разработанных ранее защитных мер применительно к существующим системам часто возникают затруднения, связанные с техническими ограничениями. Наличие подобных затруднений могут переместить направленность (пересмотр выбора) защитных мер в сторону организационных и физических способов защиты;

- социологические ограничения.

Особенности социологических ограничений при выборе защитных мер могут зависеть от того, о какой стране, отрасли, организации или даже отделе организации идет речь. Этими ограничениями нельзя пренебрегать, поскольку эффективность использования многих технических защитных мер зависит от активной поддержки их сотрудниками организации. Если сотрудники не понимают необходимости таких мер или не считают их приемлемыми по моральным соображениям, то существует большая вероятность того, что со временем эффективность защитных мер будет снижаться;

- ограничения окружающей среды.

На выбор защитных мер могут влиять также и экологические факторы, например прилегающие территории, экстремальные природные условия, состояние окружающей среды и прилегающих городских территорий и т. д.;

- правовые ограничения.

Правовые ограничения, например установленные законодательством требования о защите личной информации или статьи уголовного кодекса, касающиеся обработки информации, могут повлиять на выбор мер защиты. Законы и нормативы, не имеющие прямого отношения к защите информационных технологий, например требования противопожарной безопасности и статьи трудового законодательства, могут также повлиять на выбор мер защиты.

9.5 Приемлемость рисков

После выбора защитных мер и идентификации снижения уровня риска в результате применения защитных мер всегда будут иметь место остаточные риски, поскольку система не может быть абсолютно безопасной. Эти остаточные риски должны оцениваться организацией как приемлемые или неприемлемые. Такая оценка может быть осуществлена путем рассмотрения потенциальных неблагоприятных воздействий на сферу деловой деятельности, которые могут быть вызваны остаточными рисками. Очевидно, что существование неприемлемых рисков нельзя допускать без дальнейшего их обсуждения. Необходимо управленческое решение о допустимости таких рисков в связи с имеющимися ограничениями (например по затратам средств или невозможности предупреждения рисков — падение самолетов на здания или землетрясения; тем не менее планы восстановительных работ на случай подобных катастроф могут быть подготовлены) либо необходимо предусмотреть дополнительные и, возможно, дорогостоящие меры защиты для снижения уровня неприемлемых рисков.

9.6 Политика безопасности систем информационных технологий

В документе, отражающем политику безопасности системы информационных технологий, должно содержаться подробное описание применяемых защитных мер с обоснованием их необходимости. Использование применяемых защитных мер должно быть описано в плане безопасности информационных технологий.

Многие системы информационных технологий нуждаются в собственной политике безопасности, построенной на основе рассмотрения результатов анализа рисков. Обычно это справедливо по отношению к крупным и сложным системам. Политика безопасности системы информационных технологий должна быть

совместимой с политикой безопасности информационных технологий — между ними не следует допускать расхождений. Политика безопасности системы информационных технологий должна быть направлена на вопросы более низкого уровня, чем политика безопасности информационных технологий. Политика безопасности системы информационных технологий базируется на результатах анализа рисков и определении защитных мер для конкретной системы и поддерживается мерами защиты, выбранными в соответствии с оцененными рисками. Защитные меры должны обеспечивать достижение требуемого уровня безопасности защищаемой системы.

Политика безопасности системы информационных технологий не должна зависеть от применяемой стратегии анализа риска, а также должна определять меры защиты (в том числе методы защиты), необходимые для достижения необходимого уровня безопасности рассматриваемой системы. Политика безопасности системы информационных технологий и относящиеся к ней вспомогательные документы должны освещать следующие проблемы:

- определение системы информационных технологий, описание ее компонентов и границ (описание должно охватывать все аппаратное, программное обеспечение, персонал, окружающую среду, а также все виды деятельности — т. е. все, что в совокупности образует данную систему);
- определение целей бизнеса, которые должны быть достигнуты с помощью данной системы информационных технологий, — это может оказать воздействие на политику безопасности информационных технологий применительно к данной системе, выбранный подход к анализу рисков, а также на выбор и приоритетность осуществления защитных мер;
- определение целей безопасности системы;
- определение степени общей зависимости от системы информационных технологий, т. е. насколько деловая деятельность организации может пострадать от потери или раскрытия системы информационных технологий, задач, которые должна выполнять данная система информационных технологий, и характера обрабатываемой информации;
- определение уровня капиталовложений в информационные технологии: стоимости разработки, поддержания в рабочем состоянии и замены конкретной системы информационных технологий, включая расходы на приобретение, эксплуатацию и смену помещения;
- определение подхода к анализу рисков, выбранного для конкретной системы информационных технологий;
- определение активов системы информационных технологий, защиту которых должна обеспечить организация;
- оценку указанных активов, определяющую, что произошло бы с организацией в случае, если эти активы были бы поставлены под угрозу (стоимость хранящейся информации должна быть описана на основе возможного негативного воздействия на деловую деятельность данной организации в случае раскрытия, изменения, исчезновения или уничтожения этой информации);
- оценку угроз для системы информационных технологий и хранящейся информации, включая зависимость между характеристиками активов, угрозами и вероятностью реализации этих угроз;
- оценки уязвимости системы информационных технологий, включая описание слабых сторон системы, в которых могут реализоваться существующие угрозы;
- наличие рисков по безопасности конкретной системы информационных технологий, возникающие вследствие:

возможных негативных воздействий на деловую деятельность организации,

наличия вероятности реализации угроз,

легкости реализации угроз уязвимостей;

- перечень средств безопасности, выбранных для обеспечения безопасности данной системы информационных технологий;
- оценки стоимости защитных мер информационных технологий.

Если доказано, что система требует лишь базовой защиты, можно привести сведения по вышеперечисленным проблемам, даже если в некоторых случаях они будут менее подробными, чем для систем, по которым был проведен детальный анализ рисков.

9.7 План безопасности информационных технологий

План безопасности информационных технологий представляет собой документ по координации мер, определяющих действия для обеспечения необходимой безопасности системы информационных технологий. В плане безопасности должны быть отражены результаты рассмотрения проблем (см. 9.6) и перечислены краткосрочные, среднесрочные и долгосрочные мероприятия, направленные на достижение и поддер-

жание необходимого уровня безопасности с указанием стоимости этих мероприятий и графика их проведения. План безопасности по каждой системе информационных технологий должен включать в себя:

- цели безопасности информационных технологий с точки зрения обеспечения конфиденциальности, целостности, доступности, подотчетности, аутентичности и надежности;
- вариант анализа рисков, выбранный для конкретной системы информационных технологий (см. раздел 8);
- оценку ожидаемых остаточных и приемлемых рисков, которые будут существовать после осуществления намеченных защитных мер (см. 9.5);
- перечень выбранных для применения защитных мер (см. 9.4), а также перечень существующих и планируемых защитных мер, включая определение их эффективности и указание потребности в их совершенствовании (см. 9.3.6 и 9.4); этот второй перечень должен включать в себя:

последовательность осуществления выбранных и совершенствования существующих мер защиты,
описание практического применения выбранных и существующих мер защиты,
оценку стоимости установки и эксплуатации выбранных мер защиты,
оценку потребности в персонале для эксплуатации и контроля при осуществлении необходимых мер защиты;

- подробный рабочий план реализации выбранных мер защиты, содержащий:

последовательность выполнения конкретных операций,
график работ, соответствующий установленной последовательности выполнения операций,
суммы необходимых денежных средств,
распределение обязанностей,
процедуры ознакомления и обучения персонала, имеющего дело с информационными технологиями и конечных пользователей с применяемыми мерами защиты в целях повышения эффективности их действия,
график процессов одобрения (если необходимо);

- график процедур контроля сроков исполнения.

План безопасности информационных технологий должен содержать описание средств обслуживания для управления процессом правильного внедрения необходимых защитных мер, например методов:

- представления сообщений о состоянии работ;
- выявления возможных трудностей;
- оценки по каждой из вышеперечисленных проблем, включая методы, связанные с возможными изменениями отдельных частей плана (если необходимо).

Результатом данного этапа (см. 9.7) должен стать план безопасности информационных технологий для каждой системы, основанный на политике обеспечения безопасности систем информационных технологий с учетом результатов анализа высокого уровня риска, описанного в разделе 9. План безопасности должен обеспечить своевременное введение указанных защитных мер в соответствии с приоритетами, определенными на основе анализа рисков для системы информационных технологий, а также в соответствии с описанием методов осуществления указанных мер защиты и обеспечения необходимого уровня безопасности. Данный план безопасности, кроме того, должен содержать график последующих процедур, поддерживающих этот уровень безопасности. Подробное описание этих процедур приведено в разделе 11.

10 Выполнение плана информационной безопасности

Правильная реализация мер защиты основывается, главным образом, на хорошо составленном и документированном плане обеспечения информационной безопасности. Понимание безопасности и обучение новым информационным технологиям должны идти параллельно. Меры защиты должны быть одобрены до начала эксплуатации системы или после того как реализация плана информационной безопасности завершена.

10.1 Осуществление мер защиты

Для осуществления мер защиты необходимо выполнить все пункты плана обеспечения информационной безопасности. Лицо, ответственное за этот план (обычно служащий из руководящего состава организации, ответственный за безопасность), должно обеспечить отслеживание приоритетных и основных пунктов плана обеспечения информационной безопасности.

Документация по защитным мерам является важной частью документации по информационной безопасности, обеспечивающей непрерывность и последовательность действий. Поддержание непрерывности

и последовательности действий может быть выполнено различными способами. Документация по защитным мерам должна быть составной частью документации по безопасности организации, например плана обеспечения информационной безопасности, бизнес-плана, документации по анализу рисков, политики и процедур по обеспечению безопасности. Документация должна быть разработана с учетом потребностей руководства организации, пользователей, системных администраторов, обслуживающего персонала и лиц, вовлеченных в управление изменениями и конфигурации систем. Документация должна постоянно актуализироваться и быть достаточно подробной для исключения ошибок при обеспечении безопасности систем и в то же время предоставлять информацию, обеспечивающую правильность и эффективность деятельности по защите их систем безопасности. Часть документов, особенно касающихся угроз, уязвимостей и рисков, может содержать конфиденциальные данные и должна быть защищена от несанкционированного раскрытия. Организация должна обращаться с подобными документами очень аккуратно и дополнительно может использовать доверительные распределенные процедуры.

Распределенные процедуры должны определять способы хранения, использования и обеспечения доступа конфиденциальной информации по мерам защиты. Кроме того, эти процедуры должны определять лиц, отвечающих за хранение информации по мерам защиты, имеющих право доступа и использования информации. При разработке процедур распространения информации и определении доступа к ней необходимо учитывать ряд специфических факторов, таких как необходимость обеспечения бесперебойной работы систем информационных технологий, наличие плана аварийного восстановления производственной деятельности, стратегию и план действий в случае бедствия или другого непредвиденного события, для которых время является критическим фактором. Наконец, необходим строгий контроль за документацией по мерам защиты с тем, чтобы не допустить несанкционированных изменений, способных снизить эффективность мер защиты.

Как только план информационной безопасности будет закончен и расписан по ответственным функциям, должны быть внедрены меры защиты, проверена и испытана их сочетаемость с безопасностью. Анализ проверки сочетаемости с безопасностью проводят для подтверждения того, что меры защиты внедрены корректно, соответственно испытаны и эффективно применяются. Допускается проведение оценки безопасности как части этого анализа. Тестирование является важным способом обеспечения корректности внедренных мер защиты. Оценку безопасности проводят в соответствии с планом проверки обеспечения безопасности, описывающим подход к тестированию, график проверки обеспечения безопасности и окружающую среду. В зависимости от результатов оценки рисков может использоваться тестирование по преодолению защиты. Необходимо иметь детальные методы тестирования защиты с использованием стандартной формы отчета. Цель тестирования — внедрение и проверка мер защиты методом, обеспечивающим выполнение плана обеспечения информационной безопасности с учетом снижения риска до требуемого уровня.

10.2 Компетентность в вопросах безопасности

Цель программы обеспечения компетентности в вопросах безопасности состоит в том, чтобы повысить знания сотрудников организации до необходимого уровня, когда процессы обеспечения безопасности становятся регулярными и все сотрудники их выполняют. Программа должна обеспечить персоналу и конечным пользователям достаточное знание систем ИТ (в аппаратных средствах и программном обеспечении) с тем, чтобы они понимали необходимость мер защиты и могли их правильно использовать. Эффективными можно считать только те меры защиты, которые хорошо усвоены персоналом организации и конечными пользователями.

Данные для программы обеспечения компетентности в вопросах безопасности должны поступать от всех подразделений организации. Данные должны включать в себя вопросы общей стратегии организации по информационной безопасности и охватывать все задачи плана обеспечения информационной безопасности организации. Группе, занимающейся программой обеспечения компетентности в вопросах безопасности, должна быть обеспечена административная поддержка всех отделов. Программа обеспечения компетентности в вопросах безопасности должна затрагивать следующие темы при проведении обучающих курсов, обсуждений или других видов обучения в целях повышения эффективности этих мер:

- значение информационной безопасности для организации и сотрудников;
- цели и задачи системы обеспечения информационной безопасности в части сохранения ее конфиденциальности, целостности, доступности, подлинности и надежности;
- последствия инцидентов нарушения информационной безопасности как для организации, так и для ее сотрудников;
- важность корректного использования информационных систем, включая аппаратные средства и программное обеспечение;

- разъяснение стратегии и задач организации по обеспечению информационной безопасности, директив и рекомендаций, объяснение стратегии управления рисками, ведущей к пониманию рисков и мер защиты;

- необходимую защиту информационных систем от рисков;

- ограничение доступа в информационную среду (уполномоченный персонал, блокировка дверей, знаки идентификации, регистрация посещений) и к информации (логическое управление доступом, права чтения/модификации данных) и причины необходимых ограничений;

- необходимость в сообщениях о нарушениях защиты или попытках нарушения;

- процедуры, обязанности и рабочие задания по обеспечению безопасности;

- ограничения деятельности персонала и конечных пользователей, вызванные факторами обеспечения безопасности;

- ответственность персонала за нарушение информационной безопасности;

- значение плана обеспечения информационной безопасности системы для осуществления и контроля мер защиты;

- необходимые меры защиты и их правильное применение;

- методы, связанные с проверкой согласованности мер контроля;

- управление изменениями и конфигурацией системы.

Разработка программы обеспечения компетентности в вопросах безопасности начинается с процесса анализа стратегии безопасности, целей и политики обеспечения безопасности. Этот процесс должен проводиться рабочей группой, идентифицирующей критические аспекты в работе организации и имеющей полную поддержку главного руководства организации.

Рабочая группа, проводящая такой анализ, должна установить требования к вопросам безопасности в соответствии с общей стратегией информационной безопасности организации. Эти требования должны учитывать деятельность организации по обеспечению безопасности в целом (не только информационной безопасности) и доведены до сведения персонала в форме плакатов, листовок, информационных бюллетеней, при помощи внутренней почты и т. д.

Затем рабочая группа должна провести специальные совещания по вопросам безопасности. Необходим глубокий анализ требований к подготовке материалов совещаний. Совещания должны проводиться регулярно (например один раз в шесть месяцев), чтобы обеспечить осведомленность всего персонала с рисками, свойственными современным информационным технологиям.

Ответственность за определение целей и содержания программы обеспечения компетентности в вопросах безопасности должна быть распределена на уровне главных администраторов на конференции по вопросам информационной безопасности. Ответственность за разработку и выполнение этой программы должна быть возложена на лицо, отвечающее в организации за безопасность, и на рабочую группу разработки программы. Возложение ответственности должно быть одновременным с деятельностью в организации по вопросам обучения и профессиональной подготовки. Однако, поскольку каждый сотрудник организации несет ответственность за безопасность и должен быть ознакомлен со стратегией ее обеспечения, программа обеспечения компетентности в вопросах безопасности должна быть внедрена на всех уровнях организации.

10.2.1 Анализ потребности в знаниях

Для определения уровня понимания проблем безопасности (уже существующего у разных категорий групп сотрудников — руководство, менеджеры и исполнители) и выяснения наиболее приемлемых методов передачи им новой информации необходимо провести анализ потребности в знаниях в этой области. Анализ потребностей в знаниях исследует стратегию, методы, знание проблем безопасности и необходимость их повышения по сравнению с имеющимся в организации уровнем.

10.2.2 Представление программы

Всесторонняя программа обеспечения компетентности в вопросах безопасности должна включать в себя методы взаимодействия и содействия. Внимание в этой части программы должно быть сосредоточено на недостатках, идентифицированных на этапе анализа потребностей в знаниях по безопасности ИТ. Сотрудники должны понимать, что информационные активы имеют ценность и угрозы для активов являются вполне реальными.

Положительным моментом программы обеспечения компетентности в вопросах безопасности является возможность участия сотрудников в программе обеспечения безопасности. Методы взаимодействия (собрания персонала, обучающие курсы и т. д.) обеспечивают двухстороннее обсуждение, в котором сотрудники и персонал, обеспечивающий безопасность, обсуждают правильность концепций и требова-

ний, вытекающих из анализа потребностей в знаниях. Методы обучения (видеоматериалы, обучающие материалы, содержащие сведения по безопасности в электронной почте, плакаты, печатные издания и т. д.) принадлежат к числу односторонних методов, позволяющих осуществлять управление широковещательными процессами, распространением информации и влиять на обучение персонала.

10.2.3 Контроль программы обеспечения компетентности в вопросах безопасности

Существуют два компонента, обеспечивающих эффективный контроль за программой обеспечения компетентности в вопросах безопасности:

- периодическая оценка, определяющая эффективность программы при помощи контроля за поведением персонала в ситуациях, связанных с безопасностью, и идентификация мест, требующих изменения форм представления программы;

- контроль за изменениями в программе, при котором производятся изменения в общей программе обеспечения безопасности (изменяются стратегия или политика обеспечения безопасности, характер угроз для информации, появляются новые активы или технологии и т. п.), появляется необходимость изменить программу обеспечения компетентности в вопросах безопасности в целом с тем, чтобы обновить знания и квалификацию персонала и отразить эти изменения в программе.

10.3 Обучение персонала информационной безопасности

Помимо общей программы обеспечения компетентности в вопросах безопасности, предназначенной для каждого сотрудника организации, необходимо специальное обучение персонала, связанное с задачами и обязанностями по обеспечению информационной безопасности. Степень этого обучения зависит от уровня важности информационной безопасности для организации и должна варьироваться согласно требованиям безопасности с учетом выполняемой работы. В случае необходимости не исключено более углубленное образование (университетские лекции, специальные курсы и т. д.). Программа обучения персонала информационной безопасности должна быть разработана так, чтобы охватить все потребности обеспечения безопасности конкретной организации.

В список лиц, которым необходимо специальное обучение по информационной безопасности, следует включать:

- сотрудников, занимающих ключевые посты в разработке информационной системы;
- сотрудников, занимающих ключевые посты в эксплуатации информационной системы;
- должностных лиц организации, руководящих разработкой проекта информационной системы и программы обеспечения ее безопасности;
- сотрудников, несущих административную ответственность за безопасность, например контролирующих доступ или управляющих директориями.

Проверка необходимости специального обучения информационной безопасности должна быть проведена для текущих и запланированных задач, проектов и т. д. Каждый новый проект со специальными требованиями безопасности должен сопровождаться соответствующей программой обучения, разработанной до начала проекта и своевременно выполняемой.

Темы курсов обучения информационной безопасности должны соответствовать функциям и должностным обязанностям обучаемых сотрудников. Рекомендуется включать в список следующие темы:

- определение понятия «безопасность»;
- предупреждение нарушений конфиденциальности, целостности и доступности;
- потенциальные угрозы, которые могут оказать неблагоприятное воздействие на производственную деятельность организации и сотрудников;
- классификация чувствительности информации;
- процесс обеспечения общей безопасности;
- описание процесса обеспечения общей безопасности;
- компоненты анализа риска;
- меры защиты и обучение приемам их применения;
- роли и обязанности сотрудников;
- политика информационной безопасности.

Правильное выполнение и использование мер защиты является одним из наиболее важных аспектов программы обучения информационной безопасности. Каждая организация должна разработать собственную программу обучения информационной безопасности согласно ее потребностям и существующим или запланированным мерам защиты. Ниже приведены примеры тем, связанных с применением мер защиты, в которых сбалансированы технические и организационные аспекты безопасности:

- инфраструктура системы безопасности:
  роли и обязанности,

стратегия безопасности,
регулярная проверка согласованности мер защиты,
обработка инцидентов, связанных с нарушением безопасности;
- физическая безопасность:
здания,
офисные и компьютерные помещения и комнаты,
оборудование;
- безопасность персонала;
- безопасность носителей;
- безопасность аппаратных средств/программного обеспечения:
идентификация и аутентификация,
логический контроль доступа,
учет и аудит безопасности,
очистка носителей данных;
- телекоммуникационная безопасность:
сетевая инфраструктура,
каналы, маршрутизаторы, шлюзы, межсетевые экраны,
Интернет и другие внешние связи,
непрерывность бизнеса, включая планирование действий в чрезвычайных ситуациях (восстановление после аварий), стратегия и план(планы).

10.4 Процесс одобрения информационных систем

Организации должны обеспечить одобрение всех или предпочтительных информационных систем на предмет их соответствия установленным требованиям политики информационной безопасности и плану ее обеспечения. Процесс одобрения должен быть проведен такими методами, как проверка согласованности мер защиты, тестирование мер защиты и/или оценка системы. Процедуры одобрения могут проводиться согласно стандартам организации или национальным стандартам, а орган, выполняющий процедуру одобрения, может быть внутренним или внешним по отношению к организации.

Процесс одобрения должен быть направлен на обеспечение внедренными мерами защиты необходимого уровня безопасности информации. Одобрение должно иметь силу для конкретной операционной среды в течение конкретного периода времени, оговоренного в стратегии или плане обеспечения информационной безопасности организации. Любые значительные изменения в мерах защиты или изменения в инструкциях, влияющие на безопасность, могут потребовать нового их одобрения. Критерии, на основании которых делается новое одобрение, должны быть включены в стратегию информационной безопасности организации.

Процесс одобрения систем ИТ состоит, главным образом, из анализа документов, технических осмотров и оценок (например проверки согласованности мер защиты). Для выполнения этого процесса необходимо руководствоваться следующими положениями:

- процесс одобрения должен быть спланирован и приспособлен к конкретным информационным системам; этот первый шаг помогает также определить график осуществления плана информационной безопасности, необходимые ресурсы и ответственность;

- должны быть собраны документы, используемые в процессе;

- каждый документ должен проверяться на полноту и согласованность с другими документами;

- должен быть закончен анализ и тестирование по критериям, описанным в плане информационной безопасности;

- итоги процесса одобрения должны быть изложены в отчете с указанием уровня соответствия системы требованиям безопасности (полная, частичная, ограниченная или несоответствие), наличия отклонений или ограничений в рабочем процессе;

- новое одобрение необходимо, если информационная система или ее среда претерпели изменения, а также в конце срока действия предыдущего одобрения.

Сразу после окончания процесса одобрения начинают процедуры сопровождения информационной системы. Сопровождение помогает обнаружить и проанализировать изменения в системе, ее защите и среде. При обнаружении изменений в системе необходимо ее обновление с последующим новым одобрением.

Необходимость одобрения систем коммерческого партнера определяется базовым уровнем безопасности и нормами, действующими в организации, которая:

- желает установить собственную версию базового уровня безопасности или свои нормы и передать их партнерам/поставщикам для одобрения до подключения к своим ресурсам;
- ведет торговлю с другими компаниями и желает поддерживать с ними информационную связь, для чего ей необходимо продемонстрировать свой уровень безопасности с позиций базового уровня и общих норм безопасности;
- желает установить уровни рисков нарушений информационной безопасности для других информационно подсоединенных компаний, которые эти компании должны соблюдать. Это даст возможность организации заставить партнеров провести процесс одобрения безопасности своих систем на основании проверки согласованности мер защиты, которые будут указывать на степень соответствия этих мер частям базового уровня и норм безопасности, совместимым с принятыми в организации требованиями безопасности.

11 Последующее сопровождение системы

Последующее сопровождение системы ИТ (хотя ими часто пренебрегают) является одним из наиболее важных аспектов обеспечения информационной безопасности. Внедренные меры защиты могут быть эффективны, если они проверены в реальном производственном процессе. Необходима уверенность в том, что защитные меры используются правильно и любые инциденты и изменения безопасности будут обнаружены при сопровождении. Главная цель последующего сопровождения состоит в обеспечении продолжения функционирования мер защиты системы, как было назначено при их планировании. Со временем качество работы каждого механизма или службы снижается. Последующее сопровождение должно обнаружить это ухудшение и определить корректирующие действия. Этот способ является единственным для поддержания необходимого для защиты системы уровня безопасности. Процедуры, описанные в настоящем разделе, составляют основу эффективной программы последующего сопровождения. Управление информационной безопасностью является непрерывным процессом, который не завершается после выполнения плана обеспечения безопасности.

11.1 Обслуживание

Большинство мер защиты требуют обслуживания и административной поддержки для обеспечения их правильного и соответствующего функционирования в течение срока службы. Эти действия (обслуживание и администрирование) должны планироваться и выполняться регулярно, что должно свести к минимуму связанные с ними накладные расходы и сохранить эффективность мер защиты.

Для обнаружения сбоев в системах ИТ необходим периодический контроль. Бесконтрольная мера защиты не представляет ценности, так как нельзя определить, в какой степени можно на нее положиться.

Обслуживание включает в себя:

- проверку системных журналов;
- корректировку параметров, отражающих изменения и добавления в систему;
- переоценку рыночных цен или схем пересчета;
- обновление системы новыми версиями.

Затраты на обслуживание и администрирование должны всегда рассматриваться отдельно при оценке и выборе мер защиты, так как стоимость обслуживания и администрирования могут значительно отличаться для различных мер защиты. Поэтому затраты могут быть определяющим фактором при выборе мер защиты. В общем случае желательно везде, где возможно, свести к минимуму затраты на обслуживание и администрирование, поскольку они представляют собой периодические издержки, а не одноразовые затраты.

11.2 Проверка соответствия безопасности

Проверка соответствия безопасности включает в себя обзор и анализ осуществленных мер защиты. Она используется для контроля соответствия информационной системы или услуги требованиям, указанным в политике безопасности, принятой организацией, и плане информационной безопасности. Проверки уровня безопасности могут использоваться для контроля в ситуациях:

- внедрения новых информационных систем и услуг;
- наступления времени периодической (например годовой) проверки существующих систем или услуг;
- внесения изменений в стратегию информационной безопасности существующих систем и услуг с целью определения поправок, необходимых для сохранения заданного уровня безопасности.

Проверки безопасности могут проводиться с использованием собственного или привлеченного персонала и, по существу, основаны на использовании контрольных проверок, касающихся стратегии безопасности.

Меры защиты информационной системы могут быть проверены:

- периодическим контролем и тестированием;
- отслеживанием инцидентов в процессе эксплуатации системы;
- проведением выборочных проверок с оценкой уровня безопасности в специфических чувствительных областях деятельности организации или в местах, вызывающих беспокойство.

При проведении любой проверки уровня безопасности ценная информация о работе информационной системы может быть получена от использования:

- пакетов программ, регистрирующих события;
- контрольных журналов с полной записью событий.

Проверка уровня безопасности, проводимая в процессе одобрения и при дальнейших регулярных проверках, должна базироваться на согласованных перечнях мер защиты, составленных по результатам последнего анализа рисков, на стратегии информационной безопасности, принятой в организации, а таюке инструкциях по информационной безопасности, принятых руководством организации, включая регистрацию инцидентов. Цель проверок — убедиться, что меры защиты внедрены корректно, используются правильно и (при необходимости) тестированы.

Контролер/инспектор по проверке уровня безопасности должен в течение рабочего дня проходить по помещениям и наблюдать за выполнением мер защиты. Результаты наблюдений должны быть, по возможности, перепроверены. Люди обычно говорят то, чему верят, а не то, что есть на самом деле, поэтому необходимы перепроверки при участии других людей, работающих вместе.

Большое значение при проверке уровня безопасности имеют подробная таблица контрольных проверок и согласованная форма отчета по результатам проверки. Таблица контрольных проверок должна охватывать общую идентифицирующую информацию, например детали конфигурации системы, обязанности персонала по обеспечению информационной безопасности, документы, определяющие стратегию, окружающую обстановку. Физическая безопасность должна касаться как внешних (например окружающей обстановки вокруг здания, возможности проникновения через крышки люков), так и внутренних (например прочности конструкции здания, замков, системы пожарной сигнализации и защиты, системы сигнализации при затоплении водой/жидкостью, отказов в энергоснабжении и т. д.) аспектов.

Существует ряд критических для безопасности слабых мест, требующих контроля:

- области, доступные для физического проникновения или охраняемые по периметру (например заклиненные двери, которые открываются карточками или наборным шифром);
- неправильно работающие или установленные механизмы (например их отсутствие, неполное распределение по контролируемой зоне или неправильный выбор типа детекторных устройств).

Достаточно ли детекторов дыма/температуры для данной области, установлены ли они на правильной высоте. Срабатывает ли система сигнализации. Подается ли ее сигнал на контрольный пункт. Не появились ли новые источники угроз, например, не используется ли помещение для хранения легковоспламеняющихся веществ. Имеется ли адекватный запасной источник электропитания и предусмотрены ли процедуры его включения. Правильно ли выбраны типы кабелей, не проходят ли они около острых кромок.

При поиске слабых мест может быть полезно ответить на следующие вопросы:

- безопасность персонала (необходимость следить за процедурами приема на службу):

действенны ли рекомендации. Проверены ли перерывы в трудовой деятельности. Имеет ли персонал представление о безопасности. Существует ли зависимость ключевых функций от одного человека;

- организационная безопасность:

как распределяются документы. Являются ли документы общего пользования обновленными. Правильно ли используются процедуры по анализу риска, проверке состояния и регистрации инцидентов. Является ли план обеспечения непрерывности бизнеса корректным и действующим;

- безопасность аппаратных средств/программного обеспечения:

находится ли резервное копирование на достаточном уровне. Насколько хороши процедуры выбора идентификатора/пароля пользователей. Содержат ли журналы контроля регистрацию ошибок и их прослеживание с достаточной степенью детализации и выбором. Соответствует ли проверенная программа согласованным требованиям;

- безопасность коммуникаций:

обеспечена ли требуемая степень дублирования; имеется ли необходимое оборудование и программное обеспечение и правильно ли оно используется при наборе телефонного номера с клавиатуры ЭВМ. На-

сколько эффективна система управления ключами и связанные с этим операции, если требуется шифрование и/или аутентификация сообщения?

Проверка уровня безопасности — важная задача, требующая для успешного ее выполнения достаточного опыта и знаний. Этот отдельный вид деятельности отличается от внутреннего аудита в организации.

11.3 Управление изменениями

Информационные системы и окружающая среда, в которой они функционируют, постоянно изменяются. Изменения информационных систем есть результат появления новых защитных мер и услуг или обнаружения новых угроз и уязвимостей. Данные изменения могут также привести к новым угрозам и образованию новых уязвимостей. Изменения информационной системы включают в себя:

- новые процедуры;
- новые защитные меры;
- обновление программного обеспечения;
- пересмотр аппаратной среды;
- появление новых потребителей, в том числе внешних организаций или анонимных пользователей;
- дополнительную организацию сети и внутреннюю связь.

Когда планируются или происходят изменения в информационной системе, важно определить, как это повлияет (если повлияет) на информационную безопасность системы в целом. Если система имеет службу управления конфигурацией или другую организационную структуру, управляющую техническими системными изменениями, то в состав этой службы должно быть включено ответственное лицо по безопасности или его представитель с полномочиями определять воздействие любого изменения на информационную безопасность. При больших изменениях, включающих в себя покупку новых аппаратных средств, программного обеспечения, служба проводит повторный анализ требований безопасности. При незначительных изменениях в системе всесторонний анализ не требуется, но все-таки некоторый анализ необходим. В обоих случаях следует оценить преимущества и расходы, связанные с изменениями. Для незначительных изменений этот анализ может быть проведен неофициально, но результаты анализа и связанные с ними решения должны быть зарегистрированы.

11.4 Мониторинг

Мониторинг — это продолжение действий, направленных на проверку соответствия системы, ее пользователей и среды уровню безопасности, предусмотренному планом информационной безопасности, принятым в организации. Необходимы также повседневные планы контроля с дополнительными рекомендациями и процедурами для обеспечения безопасной работы системы, периодические консультации с пользователями, рабочим персоналом и разработчиками систем для обеспечения полной отслеживаемости всех аспектов безопасности и соответствия плана информационной безопасности текущему состоянию дел.

Одна из причин, определяющих важность контроля информационной безопасности, заключается в том, что он позволяет выявить изменения, влияющие на безопасность. Некоторые аспекты обеспечения безопасности ИТ, которые должны находиться под контролем, включают в себя активы и их стоимость, угрозы активам и их уязвимость, меры защиты активов.

Активы контролируют для определения изменений их ценности и обнаружения изменений в требованиях информационной безопасности систем. Возможными причинами этих изменений могут быть изменения:

- производственных целей организации;
- программных приложений, работающих в информационной системе;
- информации, обрабатываемой информационной системой;
- аппаратного обеспечения информационной системы.

Угрозы и уязвимости контролируют с целью определения изменений в уровне их опасности (например, вызванных изменениями среды, инфраструктуры или техническими возможностями) и обнаружения на ранней стадии других видов угроз или уязвимостей. Изменения угроз и уязвимостей могут быть вызваны также в результате изменений в активах.

Меры защиты контролируют на предмет их соответствия результативности и эффективности в течение всего времени применения. Необходимо, чтобы защитные меры были адекватными и защищали информационную систему на требуемом уровне. Не исключено, что изменения, связанные с активами, угрозами и уязвимыми местами, могут повлиять на эффективность и адекватность мер защиты.

Кроме того, если внедряется новая информационная система или изменяется существующая, то появляется необходимость убедиться в том, что такие изменения не повлияют на состояние существующих мер защиты и новые системы будут введены с адекватными мерами защиты.

При обнаружении отклонений в безопасности информационной системы необходимо их исследовать и результаты доложить руководству организации для возможного пересмотра мер защиты или, в серьезных случаях, пересмотра стратегии информационной безопасности и проведения нового анализа рисков.

В целях обеспечения требований политики информационной безопасности должны быть привлечены соответствующие ресурсы для поддержания необходимого уровня повседневного контроля следующих элементов:

- существующих мер защиты;
- ввода новых систем или услуг;
- планирования изменений в существующих системах или услугах.

Выходные данные защитных мер фиксируют в формах записи файлов регистрации данных при появлении событий. Эти файлы регистрации данных должны быть проанализированы с использованием статистических методов для раннего обнаружения тенденций к изменениям и обнаружения повторяемости инцидентов. Организация должна назначить лиц, ответственных за анализ этих файлов регистрации данных.

В дистрибутивных средах файлы регистрации данных могут записывать информацию, относящуюся к одной среде. Для верного понимания природы сложного события необходимо объединить информацию различных файлов регистрации данных и свести ее в одну запись о событии. Объединение записей событий представляет сложную задачу, важным аспектом которой является идентификация параметра (или параметров) объединения записи различных файлов регистрации данных с параметром конфиденциальности.

Метод управления контролем ежедневного мониторинга заключается в подготовке документации, описывающей необходимые действия при выполнении производственных процедур обеспечения безопасности. Эта документация описывает действия, необходимые для поддержания требуемого уровня безопасности всех систем и услуг и обеспечения его подтверждения в течение длительного времени.

Процедуры актуализации конфигурации системы безопасности должны быть задокументированы. Процедуры должны включать в себя корректирующие параметры безопасности и актуализации любой информации по управлению безопасностью. Эти изменения должны быть зарегистрированы и одобрены в рамках процессов управления конфигурацией системы. Организация должна установить процедуры выполнения регулярного обслуживания для обеспечения защиты от угроз безопасности информации. Организация должна установить порядок выполнения доверительных распределенных процедур для каждого компонента безопасности (если это применимо).

Необходимо описание процедуры контроля мер защиты. Должны быть установлены способы и частота проведения проверки уровня защищенности. Необходимо описание применения методов и инструментов статистического анализа. Должно быть разработано руководство по корректировке критериев контрольных проверок для различных производственных условий.

11.5 Обработка инцидентов

Как уже отмечалось, для идентификации рисков и уровня их опасности необходим анализ рисков. Информация по инцидентам, связанным с нарушением безопасности, необходима для поддержки процесса анализа рисков и расширения применения его результатов. Эта информация должна быть собрана и проанализирована безопасным способом (с пользой для дела). Поэтому важно, чтобы каждая организация имела схему анализа инцидентов (IAS*) для поддержания процесса анализа рисков и управления другими аспектами деятельности организации, связанными с безопасностью.

Процедура обработки инцидентов должна быть основана на требованиях пользователей с тем, чтобы быть полезной и принятой действующими и потенциальными пользователями. Процедура обработки инцидентов должна быть включена в программу обеспечения компетентности в вопросах безопасности с тем, чтобы персонал имел представление о ее характере, полезности и способах использования результатов для:

- совершенствования анализа риска и управления пересмотром;
- предотвращения инцидентов;
- повышения уровня компетентности в вопросах информационной безопасности;
- получения «сигнала тревоги» для использования группой обеспечения компьютерной безопасности в аварийных ситуациях.

Любая процедура обработки инцидентов должна содержать следующие ключевые аспекты, связанные с приведенными выше перечислениями:

- заранее составленные схемы действий по обработке нежелательных инцидентов в момент их проявления, независимо от того, вызваны ли они внешней или внутренней логической и физической атакой или произошли случайно в результате сбоя оборудования или ошибки персонала;

---

* Incident analysis scheme (англ.).

- обучение назначенных сотрудников методам расследования инцидентов, например организация группы аварийного компьютерного обеспечения.

Группа обеспечения компьютерной безопасности в аварийных ситуациях — это сотрудники, расследующие причины инцидента, связанного с нарушением информационной безопасности, определяющие потенциальную возможность его повторения или проводящие периодический анализ данных за длительный период времени. Заключения, сделанные группой обеспечения компьютерной безопасности, могут служить основанием для предупреждающих действий. Группа обеспечения компьютерной безопасности в аварийных ситуациях может быть создана внутри организации или работать по контракту со стороны.

При наличии схемы действий и обученного персонала в случае возникновения инцидента не следует принимать поспешных решений. Необходимо сохранить данные, которые позволят проследить и идентифицировать источник инцидента, привести в действие меры защиты наиболее ценных активов, что позволит снизить расходы на инцидент и устранение его последствий. Таким образом, организация в будущем сможет свести к минимуму любые известные отрицательные инциденты.

Каждая организация должна иметь эффективную процедуру обработки инцидентов, охватывающую:

- подготовку — предупреждающие меры со стороны руководства организации, рекомендации и процедуры по обработке инцидентов (включая сохранение доказательных данных, обслуживание файлов регистрации данных по событиям и связь с общественностью), необходимые документы, планы обеспечения бесперебойной работы информационной системы;

- уведомление — процедуры, средства и обязанности по регистрации информации об инцидентах;

- оценку — процедуры и обязанности по расследованию инцидентов и определению уровня их опасности;

- управление — процедуры и обязанности по обработке инцидентов, снижению ущерба от них и уведомлению вышестоящего руководства;

- восстановление — процедуры и обязанности по восстановлению нормальной работы;

- анализ — процедуры и обязанности при выполнении действий после инцидента, включая расследование юридических аспектов инцидента и анализ тенденций.

Следует отметить, что если одни организации видят выгоду от использования процедуры обработки инцидентов, то другие — считают, что еще бóльшую выгоду можно получить, объединяя эту информацию и создавая общую базу данных по инцидентам, что позволит гораздо быстрее получать предупреждения, идентифицировать тенденции и принимать меры защиты. Объединенная база данных по инцидентам должна быть достаточно гибкой для того, чтобы учитывать требования общих (все секторы, типы угроз и их возможные воздействия) и частных (отдельные секторы, угрозы и их воздействия) интересов. Каждая процедура обработки инцидентов, внутри или вне организации, должна использовать одинаковую типологию, метрологию и структуру программного обеспечения для регистрации информации по инцидентам. Это облегчает сравнение и анализ. Использование общей структуры является ключевым моментом для получения всеобъемлющих результатов и в особенности более достоверной базы данных для быстрой идентификации «предупреждения», которое невозможно получить от одиночной процедуры обработки инцидентов.

Взаимосвязь между процедурой обработки инцидентов, процессом анализа рисков и методами управления может существенно повысить качество оценки рисков, угроз и уязвимостей и увеличить выгоду от использования процедуры обработки инцидентов.

Информация по случаям возникновения угроз способна значительно улучшить качество оценки угрозы и, следовательно, качество оценки рисков. В процессе расследования инцидента (ов) вполне вероятно, что будет собрана новая дополнительная информация об уязвимостях систем и способах их устранения. Применение процедуры обработки инцидентов дает возможность пользователю идентифицировать и оценить уязвимости системы и предоставить полезные входные данные для оценки рисков. Эти данные частично основаны на информации об угрозах и частично — на результатах расследования инцидентов, проведенного группой обеспечения компьютерной безопасности в аварийных ситуациях.

Например, угроза логического проникновения (присутствие «взломщика» и привлекательность обрабатываемой информации) может сочетаться (чем и создается риск) с уязвимостью к логическому проникновению (неадекватность или отсутствие соответствующих контрольных механизмов логического доступа в систему). Поэтому использование процедуры обработки инцидентов для идентификации и оценки уязвимостей может использоваться через информацию об угрозах, которая введена в базу данных о случившихся инцидентах, вместе с информацией от других источников, особенно группой обеспечения компьютерной безопасности в аварийных ситуациях, которые могут обнаружить ранее неидентифицированные уязвимости.

Следует отметить, что процедура обработки инцидентов касается инцидентов уже произошедших. Поэтому эта процедура не дает непосредственно доступа к информации о тех уязвимостях, которые могут присутствовать, но не проявились в инцидентах. Кроме того, данные по обработке инцидентов в статистическом анализе и анализе тенденций следует использовать осторожно, поскольку входные данные по результатам проведения работ могут быть неполными или ошибочными. Тем не менее, результаты работы группы обеспечения компьютерной безопасности в аварийных ситуациях могут указать на наличие ранее незамеченных уязвимостей. В целом, регулярный ввод данных по расследованию инцидентов в процессе анализа рисков и управление проверками могут существенно улучшить качество оценки рисков, угроз и уязвимостей.

12 Резюме

В настоящем стандарте рассмотрено несколько методов, важных для управления информационной безопасностью. Эти методы основаны на концепциях и моделях, представленных в ИСО/МЭК 13335-1. В настоящем стандарте рассмотрены преимущества и недостатки четырех возможных стратегий анализа риска. Подробно описаны объединенный подход и несколько методов, полезных для практического внедрения. Некоторые организации, особенно небольшие, не могут применить все методы, приведенные в настоящем стандарте. Важно подчеркнуть, что каждый из этих методов должен быть проанализирован и применен в подходящей для организации форме.

Приложение А
(справочное)

Примерный перечень вопросов, входящих в состав политики безопасности информационных технологий организации

Содержание

1 Введение
1.1 Общий обзор
1.2 Область применения и цель политики обеспечения безопасности информационных технологий
2 Цели и принципы обеспечения безопасности
2.1 Цели
2.2 Принципы
3 Организация и инфраструктура безопасности
3.1 Ответственность
3.2 Основные направления политики обеспечения безопасности
3.3 Регистрация инцидентов нарушения безопасности
4 Анализ риска и стратегия менеджмента в области обеспечения безопасности ИТ
4.1 Введение
4.2 Менеджмент и анализ риска
4.3 Проверка соответствия мер обеспечения безопасности предъявляемым требованиям
5 Чувствительность информации и риски
5.1 Введение
5.2 Схема маркировки информации
5.3 Общий обзор информации в организации
5.4 Уровни ценности и чувствительности информации в организации
5.5 Общий обзор угроз, уязвимых мест и рисков
6 Безопасность аппаратно-программного обеспечения
6.1 Идентификация и аутентификация
6.2 Контроль доступа
6.3 Журнал учета использования ресурсов и аудит
6.4 Полное стирание
6.5 Программное обеспечение, нарушающее нормальную работу системы
6.6 Безопасность ПК
6.7 Безопасность компактных портативных компьютеров
7 Безопасность связи
7.1 Введение
7.2 Инфраструктура сетей
7.3 Интернет
7.4 Криптографическая аутентификация и аутентификация сообщений
8 Физическая безопасность
8.1 Введение
8.2 Размещение оборудования
8.3 Безопасность и защита зданий
8.4 Защита коммуникаций и систем обеспечения энергоносителями в зданиях
8.5 Защита вспомогательных служб
8.6 Несанкционированное проникновение в помещения
8.7 Доступность ПК и рабочих станций
8.8 Доступ к магнитным носителям информации
8.9 Защита персонала
8.10 Противопожарная защита
8.11 Защита от воды (жидкой среды)
8.12 Обнаружение опасностей и сообщение о них
8.13 Защита системы освещения
8.14 Защита оборудования от кражи
8.15 Защита окружающей среды
8.16 Управление услугами и техническим обслуживанием
9 Безопасность персонала
9.1 Введение
9.2 Условия найма персонала

9.3 Осведомленность и обучение персонала в области безопасности
9.4 Служащие
9.5 Контракты с лицами, проводящими самостоятельную работу
9.6 Привлечение третьих сторон
10 Безопасность документов и носителей информации
10.1 Введение
10.2 Безопасность документов
10.3 Хранение носителей информации
10.4 Ликвидация носителей информации
11 Обеспечение непрерывности деловой деятельности, включая планирование действий при чрезвычайных ситуациях и восстановлении после аварий, стратегии и план (планы)
11.1 Введение
11.2 Запасные варианты
11.3 Стратегия обеспечения бесперебойной работы организации
11.4 План (планы) обеспечения бесперебойной работы организации
12 Надомная работа
13 Политика аутсортинга
13.1 Введение
13.2 Требования безопасности
14 Управление изменениями
14.1 Обратная связь
14.2 Изменения в политике обеспечения безопасности
14.3 Статус документа
Приложение А Список руководств (рекомендаций) по обеспечению безопасности
Прилжение В Обязательные требования (законы и подзаконные акты)
Приложение С Вопросы, относящиеся к компетенции должностного лица из числа руководящего состава в области безопасности ИТ организации
Приложение D Вопросы, относящиеся к компетенции международных форумов с комитетов по обеспечению безопасности информационных технологий
Приложение Е Содержание политики обеспечения безопасности систем информационных технологий

Приложение В
(справочное)

Оценка активов

Оценка активов организации является важным этапом в общем процессе анализа риска. Ценность, определенная для каждого актива, должна выражаться способом, наилучшим образом соответствующим данному активу и юридическому лицу, ведущему деловую деятельность. Чтобы выполнить оценку активов, организация сначала должна провести инвентаризацию своих активов. Для обеспечения полного учета активов часто полезно сгруппировать их по типам, например информационные активы, активы программного обеспечения, физические активы и услуги. Целесообразно также назначить «владельцев» активов, которые будут нести ответственность за определение их ценности.

Следующий этап — согласование масштабов оценки, которая должна быть произведена, и критериев определения конкретной стоимости активов. Из-за разнообразия активов большинства организаций весьма вероятно, что некоторые активы из тех, что могут быть оценены в денежных единицах, будут оцениваться в местной валюте, в то время как другие активы могут оцениваться по качественной шкале в диапазоне от «очень низкой» до «очень высокой» цены. Решение использовать количественную или качественную оценку принимает конкретная организация, но при этом выбранный тип оценки должен соответствовать подлежащим оценке активам. Для одного и того же актива могут быть использованы также оба типа оценки.

Типичными терминами, используемыми для качественной оценки ценности активов, являются: «пренебрежимо малая», «очень малая», «малая», «средняя», «высокая», «очень высокая», «имеющая критическое значение». Выбор и диапазон терминов, являющихся подходящими для данной организации, в значительной степени зависят от потребностей организации в безопасности, величины этой организации, а также других, специфичных для данной организации факторов.

Критерии, используемые в качестве основы для оценки ценности каждого актива, должны выражаться в однозначных (недвусмысленных) терминах. С этим часто бывают связаны наиболее сложные аспекты оценки активов, поскольку ценность некоторых из них приходится определять субъективно. Поэтому для определения ценности активов целесообразно привлекать достаточно большое число разных людей. Возможны следующие критерии определения ценности активов: первоначальная стоимость актива, стоимость его обновления или воссоздания. Ценность актива может также носить нематериальный характер, например цена доброго имени или репутации компании.

Другой подход к оценке активов основывается на затратах, понесенных по причине утраты конфиденциальности, целостности или доступности вследствие происшедшего инцидента. Применение подобных оценок предоставляет три важных фактора ценности актива в дополнение к стоимости воссоздания актива, основанной на оценках потенциального ущерба или неблагоприятного воздействия на деловую деятельность в результате происшедшего инцидента нарушения безопасности с предполагаемым набором обстоятельств. Следует подчеркнуть, что этот подход учитывает ущерб и другие затраты, связанные с воздействием, которые являются необходимыми для введения соответствующих факторов при оценке риска.

Многие активы могут в процессе оценки иметь несколько присвоенных им ценностей. Например бизнес-план может быть оценен на основе трудозатрат на его разработку или на введение данных, или ценности для конкурента. Весьма велика вероятность того, что значения этих ценностей будут значительно отличаться друг от друга. Присвоенная ценность актива может быть максимальной из всех возможных ценностей или суммой некоторых или всех возможных ценностей. При окончательном анализе необходимо тщательно определить итоговую ценность актива, поскольку от нее зависит объем ресурсов, необходимых для обеспечения защиты данного актива.

В конечном счете все оценки активов должны проводиться на основе общего подхода. Это может быть сделано при помощи следующих критериев, которые могут использоваться для оценки возможного ущерба от потери конфиденциальности, целостности или доступности активов:

- нарушение законов и/или подзаконных актов;
- снижение эффективности бизнеса;
- потеря престижа/негативное воздействие на репутацию;
- нарушение конфиденциальности личных данных;
- необеспеченность личной безопасности;
- негативный эффект с точки зрения обеспечения правопорядка;
- нарушение конфиденциальности коммерческой информации;
- нарушение общественного порядка;
- финансовые потери;
- нарушение деловых операций;
- угроза охране окружающей среды.

Перечисленные выше примеры критериев оценки могут быть использованы для оценки активов. Для выполнения оценок организация должна выбирать критерии, соответствующие типу ее деловой деятельности и установленным требованиям по обеспечению безопасности. Поэтому некоторые из вышеперечисленных критериев оценки могут оказаться неприменимыми, тогда как другие могут быть добавлены к данным критериям оценки.

После выбора подходящих критериев организация должна договориться о шкале оценки, которая будет использоваться во всей организации. Первым шагом должно быть установление числа используемых уровней. Правил для установления наиболее подходящего числа уровней не существует. Большее число уровней обеспечивает более высокую степень детализации, но иногда слишком тонкое дифференцирование затрудняет оценку активов организации. Обычно число уровней оценки находится в диапазоне от трех (например «малая», «средняя» и «высокая» ценность) до десяти при условии, что это совместимо с подходом организации к общему процессу оценки риска.

Кроме того, организация может устанавливать собственные пределы ценности активов (например «малая», «средняя» и «высокая»). Эти пределы должны быть оценены по выбранным критериям, например, возможные финансовые потери следует оценивать в денежных единицах, тогда как при оценке по критерию угрозы для личной безопасности оценка в денежных единицах окажется непригодной. В конечном счете организация сама должна решить, какой ущерб считать малым, а какой — большим. Ущерб, который может стать бедственным для маленькой организации, для очень крупной организации может быть сочтен малым или даже пренебрежимо малым.

Приложение С
(справочное)

Перечень типичных видов угроз

В настоящем приложении приведен перечень типичных видов угроз. Этот перечень можно использовать в процессе оценки угроз, вызванных одним или несколькими преднамеренными или случайными событиями, или событиями, связанными с окружающей средой и имеющими естественное происхождение. Угрозы, обусловленные преднамеренными действиями, обозначены в перечне буквой D, угрозы, обусловленные случайными действиями, — A и угрозы, обусловленные естественными причинами, — E. Таким образом, буквой D обозначают все преднамеренные действия, объектами которых являются активы информационных технологий, буквой A — все совершаемые людьми действия, которые могут случайно нанести вред активам информационных технологий, буквой E — инциденты, не основанные на действиях, совершаемых людьми.

Землетрясение	E
Затопление	D, A, E
Ураган	E
Попадание молнии	E
Забастовка	D, A
Бомбовая атака	D, A
Применение оружия	D, A
Пожар	D, A
Намеренное повреждение	D
Неисправности в системе электроснабжения	A
Неисправности в системе водоснабжения	A
Неисправности в системе кондиционирования воздуха	D, A
Аппаратные отказы	A
Колебания напряжения	A, E
Экстремальные величины температуры и влажности	D, A, E
Воздействие пыли	E
Электромагнитное излучение	D, A, E
Статическое электричество	E
Кража	D
Несанкционированное использование носителей данных	D
Ухудшение состояния носителей данных	E
Ошибка обслуживающего персонала	D, A
Ошибка при обслуживании	D, A
Программные сбои	D, A
Использование программного обеспечения несанкционированными пользователями	D, A
Использование программного обеспечения несанкционированным способом	D, A
Нелегальное проникновение злоумышленников под видом санкционированных пользователей	D
Незаконное использование программного обеспечения	D, A
Вредоносное программное обеспечение	D, A
Незаконный импорт/экспорт программного обеспечения	D
Ошибка операторов	D, A
Ошибка при обслуживании	D, A
Доступ несанкционированных пользователей к сети	D
Использование сетевых средств несанкционированным способом	D
Технические неисправности сетевых компонентов	A
Ошибки передачи	A
Повреждение линий	D, A
Перегруженный трафик	D, A
Перехват информации	D
Несанкционированное проникновение к средствам связи	D
Анализ трафика	D
Направление сообщений по ошибочному адресу	A
Изменение маршрута направления сообщений	D
Изменение смысла переданной информации	D
Сбои в функционировании услуг связи (например сетевых услуг)	D, A
Недостаточная численность персонала	A
Ошибки пользователей	D, A
Ненадлежащее использование ресурсов	D, A

Приложение D
(справочное)

Примеры общих уязвимостей

В настоящем приложении приведены примеры уязвимых мест применительно к различным объектам, требующим обеспечения безопасности, а также примеры угроз, которые могут возникнуть на конкретных объектах. Данные примеры могут оказаться полезными при оценке уязвимых мест. Следует отметить, что в некоторых случаях упомянутым выше уязвимым местам могут угрожать другие угрозы.

1 Среда и инфраструктура

Отсутствие физической защиты зданий, дверей и окон (возможна, например, угроза кражи).

Неправильное или халатное использование физических средств управления доступом в здания, помещения (возможна, например, угроза намеренного повреждения).

Нестабильная работа электросети (возможна, например, угроза колебаний напряжения).

Размещение в зонах возможного затопления (возможна, например, угроза затопления).

2 Аппаратное обеспечение

Отсутствие схем периодической замены (возможна, например, угроза ухудшения состояния запоминающей среды).

Подверженность колебаниям напряжения (возможна, например, угроза возникновения колебаний напряжения).

Подверженность температурным колебаниям (возможна, например, угроза возникновения экстремальных значений температуры).

Подверженность воздействию влаги, пыли, загрязнения (возможна, например, угроза запыления).

Чувствительность к воздействию электромагнитного излучения (возможна, например, угроза воздействия электромагнитного излучения).

Недостаточное обслуживание/неправильная инсталляция запоминающих сред (возможна, например, угроза возникновения ошибки при обслуживании).

Отсутствие контроля за эффективным изменением конфигурации (возможна, например, угроза ошибки операторов).

3 Программное обеспечение

Неясные или неполные технические требования к разработке средств программного обеспечения (возможна, например, угроза программных сбоев).

Отсутствие тестирования или недостаточное тестирование программного обеспечения (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

Сложный пользовательский интерфейс (возможна, например, угроза ошибки операторов).

Отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей).

Отсутствие аудиторской проверки (возможна, например, угроза использования программного обеспечения несанкционированным способом).

Хорошо известные дефекты программного обеспечения (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

Незащищенные таблицы паролей (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей).

Плохое управление паролями (легко определяемые пароли, хранение в незашифрованном виде, недостаточно частая замена паролей).

Неправильное присвоение прав доступа (возможна, например, угроза использования программного обеспечения несанкционированным способом).

Неконтролируемая загрузка и использование программного обеспечения (возможна, например, угроза столкновения с вредоносным программным обеспечением).

Отсутствие регистрации конца сеанса при выходе с рабочей станции (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

Отсутствие эффективного контроля внесения изменений (возможна, например, угроза программных сбоев).

Отсутствие документации (возможна, например, угроза ошибки операторов).

Отсутствие резервных копий (возможна, например, угроза воздействия вредоносного программного обеспечения или пожара).

Списание или повторное использование запоминающих сред без надлежащего стирания записей (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

4 Коммуникации

Незащищенные линии связи (возможна, например, угроза перехвата информации).

Неудовлетворительная стыковка кабелей (возможна, например, угроза несанкционированного проникновения к средствам связи).

Отсутствие идентификации и аутентификации отправителя и получателя (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей).

Пересылка паролей открытым текстом (возможна, например, угроза доступа несанкционированных пользователей к сети).

Отсутствие подтверждений посылки или получения сообщения (возможна, например, угроза изменения смысла переданной информации).

Коммутируемые линии (возможна, например, угроза доступа несанкционированных пользователей к сети).

Незащищенные потоки конфиденциальной информации (возможна, например, угроза перехвата информации).

Неадекватное управление сетью (недостаточная гибкость маршрутизации) (возможна, например, угроза перегрузки трафика).

Незащищенные подключения к сетям общего пользования (возможна, например, угроза использования программного обеспечения несанкционированными пользователями).

5 Документы

Хранение в незащищенных местах (возможна, например, угроза хищения).

Недостаточная внимательность при уничтожении (возможна, например, угроза хищения).

Бесконтрольное копирование (возможна, например, угроза хищения).

6 Персонал

Отсутствие персонала (возможна, например, угроза недостаточного числа работников).

Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц (возможна, например, угроза хищения).

Недостаточная подготовка персонала по вопросам обеспечения безопасности (возможна, например, угроза ошибки операторов).

Отсутствие необходимых знаний по вопросам безопасности (возможна, например, угроза ошибок пользователей).

Неправильное использование программно-аппаратного обеспечения (возможна, например, угроза ошибки операторов).

Отсутствие механизмов отслеживания (возможна, например, угроза использования программного обеспечения несанкционированным способом).

Отсутствие политики правильного пользования телекоммуникационными системами для обмена сообщениями (возможна, например, угроза использования сетевых средств несанкционированным способом).

Несоответствующие процедуры набора кадров (возможна, например, угроза намеренного повреждения).

7 Общие уязвимые места

Отказ системы вследствие отказа одного из элементов (возможна, например, угроза сбоев в функционировании услуг связи).

Неадекватные результаты проведения технического обслуживания (возможна, например, угроза аппаратных отказов).

Приложение Е
(справочное)

Типология методов анализа риска

Анализ риска состоит из следующих этапов, приведенных в настоящем приложении, а также в ИСО/МЭК ТО 13335-4:

- идентификация и оценка активов (оценка возможного негативного воздействия на деловую деятельность);
- оценка угроз;
- оценка уязвимых мест;
- оценка существующих и планируемых средств защиты;
- оценка риска.

На заключительном этапе анализа риска должна быть проведена суммарная оценка риска. Как было установлено ранее (см. приложение В), активы, имеющие ценность и характеризующиеся определенной степенью уязвимости, всякий раз подвергаются риску в присутствии угроз. Оценка риска представляет собой оценку соотношения потенциальных негативных воздействий на деловую деятельность в случае нежелательных инцидентов и уровня оцененных угроз и уязвимых мест. Риск фактически является мерой незащищенности системы и связанной с ней организации. Величина риска зависит от:

- ценности активов;
- угроз и связанной с ними вероятности возникновения опасного для активов события;
- легкости реализации угроз в уязвимых местах с оказанием нежелательного воздействия;
- существующих или планируемых средств защиты, снижающих степень уязвимости, угроз и нежелательных воздействий.

Задача анализа риска состоит в определении и оценке рисков, которым подвергается система информационных технологий и ее активы, с целью определения и выбора целесообразных и обоснованных средств обеспечения безопасности. При оценке рисков рассматривают несколько различных его аспектов, включая воздействие опасного события и его вероятность.

Воздействие может быть оценено несколькими способами, в том числе количественно (в денежных единицах) и качественно (оценка может быть основана на использовании для сравнения прилагательных типа умеренное или серьезное), или их комбинацией. Для оценки воздействия необходимо рассчитать вероятность появления угрозы, время ее существования, время сохранения ценности актива и целесообразность защиты актива. На вероятность появления угрозы оказывают влияние следующие факторы:

- привлекательность актива — применяют при рассмотрении угрозы намеренного воздействия людей;
- доступность актива для получения материального вознаграждения — применяют при рассмотрении угрозы намеренного воздействия людей;
- технические возможности создателя угрозы — применяют при рассмотрении угрозы намеренного воздействия людей;
- вероятность возникновения угрозы;
- возможность использования уязвимых мест — применяют к уязвимым местам как технического, так и нетехнического характера.

Многие методы предлагают использование таблиц и различных комбинаций субъективных и эмпирических мер. В настоящее время нельзя говорить о правильном или неправильном методе анализа риска. Важно, чтобы организация пользовалась наиболее удобным и внушающим доверие методом, приносящим воспроизводимые результаты. Ниже приведены несколько примеров методов, основанных на применении таблиц:

Примеры

1 Матрица с заранее определенными значениями

В методах анализа риска такого типа фактические или предполагаемые физические активы оценивают на основе стоимости их замены или восстановления (то есть количественно). Затем эти количественные оценки преобразуют в шкалу качественных оценок, которая используется применительно к активам данных (см. ниже). Фактические или предполагаемые программные активы оценивают так же, как и физические активы с определением стоимости их покупки или восстановления, а затем эти количественные оценки преобразуют в шкалу качественных оценок, которая используется применительно к активам данных. Кроме того, если выяснится, что к конкретному прикладному программному обеспечению существуют свои внутренние требования по конфиденциальности или целостности (например, если исходный код сам является коммерческой тайной), то его оценивают тем же способом, что и активы данных.

Значения ценности активов данных определяют интервьюированием избранных сотрудников, занятых в сфере деловой деятельности («владельцев данных»), которые могут высказывать компе-

тентные суждения относительно данных, определять ценность и чувствительность данных, находящихся в использовании или подлежащих хранению или обработке с обеспечением доступа к ним. Такие интервью облегчают оценку ценности и чувствительности активов данных с учетом самых неблагоприятных вариантов развития событий, которые можно ожидать, руководствуясь разумными основаниями, и которые могут оказать негативное воздействие на деловую деятельность вследствие несанкционированных раскрытия информации, модификации, изменения смысла переданной информации, недоступности информации в различные периоды времени и уничтожения информации.

Оценку проводят на основе рекомендаций по оценке активов данных, которые охватывают:

- личную безопасность;
- персональные данные;
- обязанности соблюдать требования законов и подзаконных актов;
- правовое принуждение;
- коммерческие и экономические интересы;
- финансовые потери / нарушение нормального хода работ;
- общественный порядок;
- политику ведения бизнеса и деловых операций;
- потерю репутации.

Рекомендации облегчают определение значений на числовой шкале (например от 1 до 4), которая предусмотрена для матрицы, используемой в качестве примера (см. таблицу 1), позволяя, таким образом, использовать там, где возможно, количественные, а там, где невозможно, — логические и качественные оценки, например при оценивании степени угрозы для жизни людей.

Важным является также составление пар вопросников по каждому типу угрозы для каждой группы активов, к которым относится данный тип угрозы, что обеспечит возможность оценки уровней угроз (вероятности возникновения угроз) и уровней уязвимости (легкости реализации угроз в уязвимых местах с оказанием нежелательного воздействия). За ответ на каждый вопрос начисляют очки. Очки накапливают с использованием базы знаний и сравнивают с рангами, что позволяет определить уровни угроз (например по шкале с диапазоном уровней от «высокого» до «низкого») и соответственно уровни уязвимости (см. приведенную ниже матрицу), применительно к различным уровням воздействия. Ответы на вопросы, содержащиеся в вопросниках, получают в результате интервьюирования технических специалистов, персонала организации и специалистов по эксплуатации помещений, а также на основе физического обследования мест размещения аппаратуры и проверки состояния документации.

Типы учитываемых угроз распределяют по следующим группам: намеренные несанкционированные действия людей, действия сил природы, ошибки людей и сбои в оборудовании, программном обеспечении или линии связи.

Ценности активов, а также уровни угроз и уязвимости, соответствующие каждому типу воздействия вводят в матрицу для определения каждого сочетания соответствующих мер риска по шкале от 1 до 8. Значения величин размещают в матрице в структурированной форме в соответствии с таблицей 1.

Таблица 1

Ценность актива	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
Обозначение: Н — низкий, С — средний, В — высокий.									

Для каждого актива рассматривают уязвимые места и соответствующие им угрозы. Если имеются уязвимые места без соответствующей угрозы или угрозы без соответствующего уязвимого места, то считают, что в данное время риск отсутствует (необходимо проявлять осторожность на случай возможного изменения ситуации!). Затем идентифицируют соответствующий ряд матрицы по ценности актива, а соответствующую колонку — по степени угрозы и уязвимости. Например, если ценность актива равна 3, угрозу характеризуют как «высокую», а уязвимость — как «низкую», мера

риска равна 5. Предположим, что ценность актива равна 2; при оценке, например угрозы модификации актива, угрозу характеризуют как «низкую», а уязвимость — как «высокую». В этом случае мера риска будет равна 4. Размер матрицы с точки зрения числа категорий, характеризующих степень угрозы, степень уязвимости и ценность актива выбирают в зависимости от потребностей организации. Дополнительные колонки и ряды дают дополнительное число мер риска. Ценность настоящего метода состоит в ранжировании соответствующих рисков.

2 Ранжирование угроз по мерам риска

Для установления пошаговой взаимозависимости между факторами воздействия (ценность актива) и вероятностью возникновения угрозы (с учетом аспектов уязвимости) может использоваться матрица или таблица (см. таблицу 2). Первый шаг — оценка воздействия (ценности актива) по заранее определенной шкале, например от 1 до 5, для каждого подвергаемого угрозе актива (колонка b в таблице 2). Второй шаг — оценка вероятности возникновения угрозы по заранее определенной шкале, например от 1 до 5, для каждой угрозы (колонка с в таблице 2). Третий шаг — расчет мер риска умножением результатов первых двух шагов (b — с). Теперь можно проранжировать опасности по значению коэффициента «подверженности воздействиям». В таблице 2 цифрой 1 обозначены самое малое воздействие и самая низкая вероятность возникновения угрозы.

Таблица 2

Дескриптор угроз a	Оценка воздействия (ценности актива) b	Вероятность возникновения угрозы c	Мера риска d	Ранг угрозы e
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Как показано выше, такой метод позволяет сравнивать и ранжировать по приоритетности разные угрозы с различными воздействиями и вероятности возникновения угрозы. В некоторых случаях необходимо соотнести используемые в этой процедуре эмпирические шкалы с денежными единицами.

3 Оценка частоты появления и возможного ущерба, связанного с рисками

В настоящем примере основное внимание уделяется воздействию нежелательных инцидентов и определению систем, которым следует предоставить приоритет. Для этого оценивают по два значения для каждого актива и риска, которые в разных комбинациях определяют оценку каждого актива. Вычисляют сумму оценок всех активов данной системы и определяют меру риска для данной системы информационных технологий.

Прежде всего определяют ценность каждого актива. Ценность актива связана с возможным повреждением актива, которому угрожают, и назначается для каждой угрозы, которой может подвергнуться данный актив.

Затем определяют значение частоты. Частоту оценивают по сочетанию вероятности возникновения угрозы и легкости возникновения угроз в уязвимых местах (см. таблицу 3).

Таблица 3

Частота	Уровень угрозы								
	«Низкий»			«Средний»			«Высокий»		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
	0	1	2	1	2	3	2	3	4

Затем по таблице 4 определяют оценки по активам/угрозам, находя пересечение колонки ценности актива и строки частоты. Оценки по активам/угрозам суммируют и определяют общую оценку актива. Эта оценка может быть использована для определения различий между активами, образующими часть системы.

Таблица 4

Частота	Ценность актива				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Последний шаг состоит в вычислении суммы оценок всех активов системы для определения оценки системы. Эта оценка может быть использована для определения различий между системами, а также для определения средств защиты системы, которые следует использовать в первую очередь.

В приведенных ниже примерах все значения величин выбраны случайным образом.

Предположим, что в системе S имеется три актива: A1, A2 и A3. Предположим также, что данная система может подвергаться двум угрозам: T1 и T2. Пусть ценность актива A1 будет равна 3, ценность актива A2 — 2 и ценность актива A3 — 4.

Если для сочетания актива A1 и угрозы T1 вероятность возникновения угрозы мала, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 1 (см. таблицу 3).

Оценка сочетания актива A1 и угрозы T1 может быть взята по таблице 4 на пересечении колонки «ценность актива», равной 3, и строки «частота», равной 1. В данном случае эта оценка будет равна 4. Аналогично принимают для оценки сочетания актива A1 и угрозы T2 среднюю вероятность возникновения угрозы и высокую легкость возникновения угрозы в уязвимых местах. Тогда оценка сочетания актива A1 и угрозы T2 будет равна 6.

Затем вычисляют значение общей оценки A1T, которая будет равна 10. Общую оценку активов рассчитывают для каждого актива и применимой угрозы. Общую оценку системы ST определяют по сумме A1T + A2T + A3T.

Теперь можно сопоставить различные системы и различные активы внутри одной системы и установить приоритеты.

4 Разграничение между допустимыми и недопустимыми рисками

Другой способ измерения рисков состоит только в разграничении допустимых и недопустимых рисков. Предпосылка заключается в том, что меры рисков используют лишь для ранжирования областей по срочности принятия необходимых мер, что может быть достигнуто с затратой меньших усилий.

В соответствии с таким подходом применяемая матрица уже не содержит числовых значений, а только буквы T (для допустимых рисков) и N (для недопустимых рисков). Так, например, матрица, используемая для метода 3, может быть преобразована в матрицу по таблице 5.

Таблица 5

Частота	Ценность актива				
	0	1	2	3	4
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Эта матрица, как и предыдущие, приведена только в качестве примера. Обозначение границы между допустимыми и недопустимыми рисками — на усмотрение пользователя.

Приложение F
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК ТО 13335-1:1996	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 13335-4:2000	ГОСТ Р ИСО/МЭК ТО 13335-4 — 2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

УДК 004.056:006.354 ОКС 13.110 35.020 Т59

Ключевые слова: информационная технология, информационная безопасность, базовый подход, меры защиты, мониторинг, обработка инцидентов

Редактор *В. Н. Колысов*
Технический редактор *Л. А. Гусева*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *А. П. Финогеновой*

Сдано в набор 26.06.2007. Подписано в печать 31.07.2007. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 5,58. Уч.-изд. л. 5,30. Тираж 351 экз. Зак. 1773.

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