ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 3

Методические указания по управлению защитой информационных технологий

СТ РК ИСО/МЭК 13335-3-2008

(ИСО/МЭК 13335-3:1998 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 3. Методические указания по управлению защитой информационных технологий», IDT)

Издание официальное

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

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

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

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 13335-3:1998 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 3. Методические указания по управлению защитой информационных технологий» («Information technology. Security techniques. Management of information and communication security. Part 3. Techniques for the management of IT Security»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

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

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

– Часть 3. Методические указания по управлению защитой ИТ.

– Часть 4. Выбор защитных мер.

– Часть 5. Руководство по управлению защитой сети.

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

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

Целью стандарта СТ РК ИСО/МЭК 13335 является предоставление руководства по основным аспектам управления обеспечением безопасности информационных технологий. Сотрудники организации, ответственные за обеспечение безопасности информационных технологий, должны быть способны адаптировать материал, содержащийся в настоящем стандарте, к своим конкретным потребностям. Данный документ преследует следующие цели:

– определить и описать концепции, связанные с управлением безопасностью информационных технологий;

– определить взаимосвязи между управлением безопасностью информационных технологий и управлением информационными технологиями в целом;

– представить несколько моделей, которые могут быть использованы для разъяснения понятия безопасности информационных технологий;

– дать общие руководящие указания по управлению обеспечением безопасности информационных технологий.

Стандарт СТ РК ИСО/МЭК 13335 состоит из следующих частей:

Часть 1 дает общий обзор фундаментальных концепций и моделей, используемых для описания управления безопасностью информационных технологий. Данный документ ориентирован на специалистов, ответственных за программу общей безопасности организации и/или ее систем ИТ.

Часть 3 дает описание способов обеспечения безопасности и предназначается для лиц, участвующих в управлении проектом на протяжении всего срока его действия: в части планирования, проектирования, внедрения, тестирования, приобретения или эксплуатации.

Часть 4 содержит указания по выбору средств защиты и их поддержке в виде базовых моделей и мер контроля. В ней также описывается, как эти средства защиты дополняют способы обеспечения безопасности, о которых идет речь в Части 3. Кроме того, в Части 4 говорится о том, как можно использовать методы дополнительной оценки для выбора средств защиты.

Часть 5 содержит руководящие указания для организаций, системы информационных технологий которых подключаются к внешним сетям. Эти указания относятся к выбору и использованию средств защиты, обеспечивающих безопасность внешних соединений и сервисов, поддерживаемых этими соединениями, а также дополнительных средств защиты, необходимых для систем информационных технологий в связи с указанными соединениями.

Цель настоящего стандарта предоставление необходимых описании и рекомендации по способам эффективного управления безопасностью информационных технологий. Эти способы могут быть использованы для оценки требований по безопасности и рисков. Кроме того, они помогут установить и поддерживать необходимые средства обеспечения безопасности, то есть правильный уровень обеспечения безопасности информационных технологий. Может возникнуть необходимость в том, чтобы результаты, полученные таким образом, были увеличены за счет применения дополнительных средств защиты, требуемых применительно к данной организации и данной среде.

Настоящий стандарт, предназначается для любых сотрудников организации, ответственных за управление безопасностью информационных технологий и/или за внедрение мер обеспечения их безопасности.

Настоящий стандарт разделен на 10 разделов. Раздел 4 дает общий обзор по способам управления безопасностью информационных технологий. В разделе 5 подчеркивается важность политики безопасности информационных технологий и описывается ее состав. Раздел 6 содержит описание четырех различных подходов к определению потребностей в защите. Раздел 7 дает детальное описание рекомендуемого подхода. Раздел 8 описывает порядок применения защитных мер, программы обеспечения осведомленности сотрудников в области защиты информации и затрагивает процесс санкционирования эксплуатации систем ИТ. В разделе 9 рассматривается описание работ, следующих за применением защитных мер и необходимых для подтверждения эффективности функционирования защитных мер. В разделе 10 приводится краткое резюме по данной части настоящего стандарта.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ Часть 3 Методические указания по управлению защитой информационных технологий

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт предназначен методам управления обеспечением безопасности информационных технологий. В основе этих методов лежат общие рекомендации, которые изложены в *СТ РК ИСО/МЭК 13335-1-2008*. Эти рекомендации предназначены для сотрудников организации при оказании помощи в осуществлении мероприятий по обеспечению безопасности информационных технологий. Для полного понимания материала, приведенного в настоящем стандарте необходимо ознакомление с концепциями и моделями, которые содержатся в *СТ РК ИСО/МЭК 13335-1-2008*.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на стандарт:

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

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

3 Термины и определения

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

4 Способы управления безопасностью информационных технологий

Процесс управления безопасностью информационных технологий основывается на принципах, изложенных в [1].

Он может быть реализован как в масштабе всей организации, так и в определенной ее части. На рисунке 1 приведены основные этапы этого про-

цесса, а также показана обратная связь между результатами процесса и его отдельными частями. Такая обратная связь должна устанавливаться по мере необходимости как в пределах продолжительности одного из этапов, так и после завершения одного или нескольких этапов. Эта схема демонстрирует основные направления, рассматриваемые в настоящем стандарте.

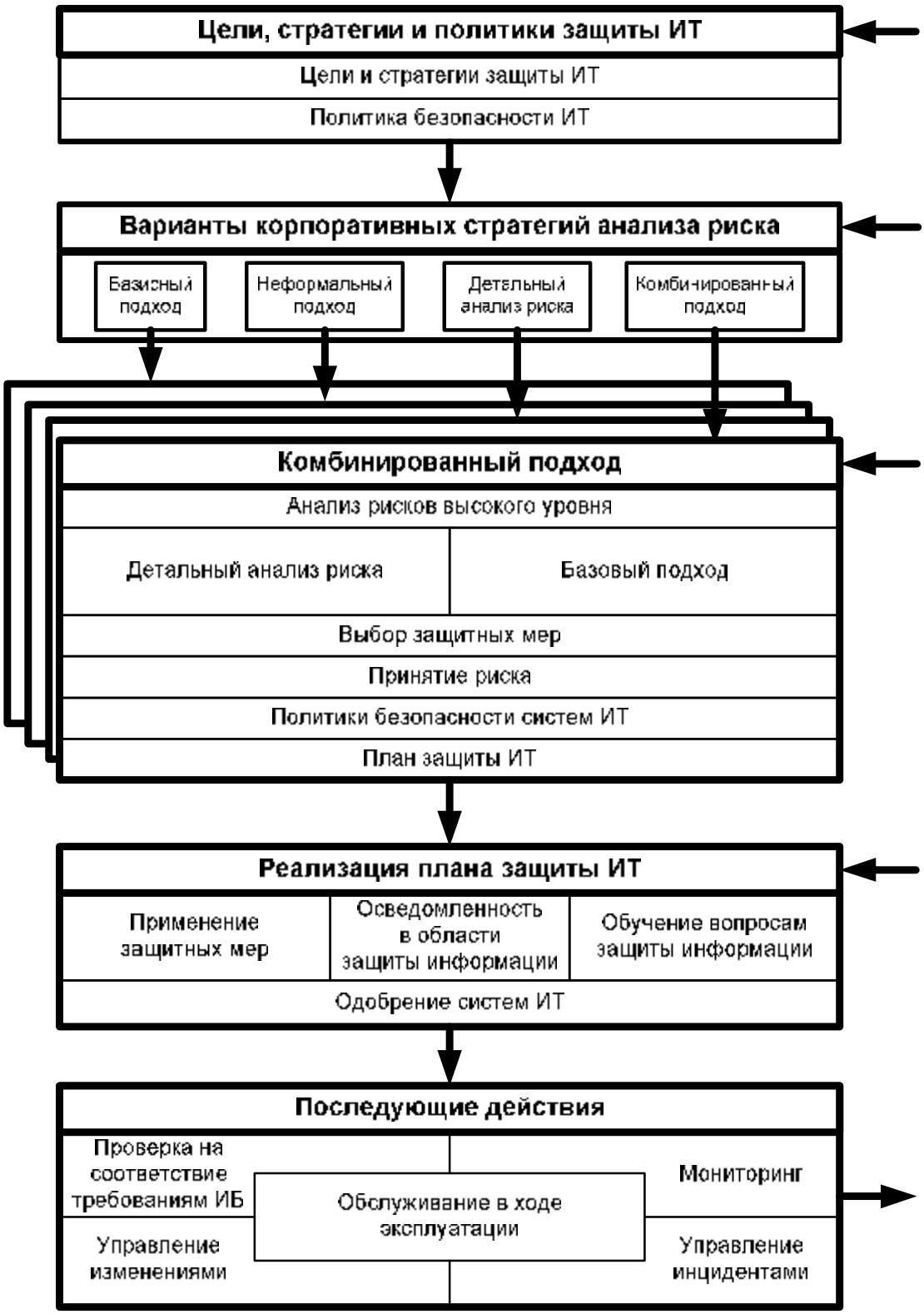

Рисунок 1 – Управление безопасностью информационных технологий

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

Важной частью процесса управления безопасности 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 по защите систем и сервисов ИТ рекомендуется осуществить выбор корпоративной стратегии анализа риска. Основные варианты стратегии подробно рассматриваются в разделе 6. Рекомендуемый вариант стратегии предполагает выделение систем с высоким уровнем риска, проведение для них детального анализа риска, а для систем с низким уровнем риска – использование базисного подхода к анализу риска. Применительно к системам с высоким уровнем риска подробно рассматриваются ресурсы, возможные опасности и уязвимости системы в целях проведения детального анализа риска, что позволит облегчить выбор эффективных защитных мер, которые будут соответствовать оценки уровня риска. Использование данного варианта 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 определяются соответствующие меры защиты, направленные на снижение уровня риска до приемлемого уровня. Эти меры реализуются в соответствии с планом защиты ИТ. Реализация плана должна сопровождаться выполнением программ знания и понимания мер безопасности и обучения использованию этих мер, что является важным решением эффективности принятых защитных мер.

Кроме того, управление безопасностью информационных технологий включает решение текущих задач, связанных с проведением различных дополнительных мероприятий, что может привести к корректировке полученных ранее результатов и принятых решений. Дополнительные мероприятия включают: обслуживание и проверку соответствия систем безопасности тре-

бованиям, управление изменениями, мониторинг и принятие дополнительных мер в случае нарушения и снижения эффективности систем безопасности.

5 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 чрезвычайно важна для того, чтобы гарантировать, что результаты процесса управления риском будут приемлемы и принесут должный эффект от снижения уровня риска. Для разработки и эффективной реализации политики безопасности требуется организационное решение в рамках организации. Важно, чтобы разработанная политика безопасности информационных технологий учитывала корпоративные цели и конкретные особенности деятельности организации. Она должна соответствовать корпоративной политике безопасности и политике компании в области бизнеса. 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 базисного подхода) и соответствовать политике безопасности систем информационных технологий, при этом она должна учитывать рекомендации по обеспечению безопасности, выработанные для соответствующей системы.

5.1 Цели и стратегия безопасности информационных технологий

В качестве первого шага в процессе управления безопасности 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 ресурсы и определить, насколько ценными они являются для данной организации. Критерием в этом случае является то, насколько важную роль играют ин-

формационные технологии в процессе проведения организацией своей деловой деятельности, при этом стоимость самих информационных технологий составляет лишь малую часть общей оценки. При рассмотрении вопроса о том, насколько важны для функционирования организации информационные технологии, необходимо учитывать следующее:

– 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 же от своевременного получения такой информации;

– какие виды конфиденциальной информации, обрабатываемой с использованием информационных технологий, подлежат защите;

– каковы могут быть для организации последствия нежелательного нарушения системы обеспечения безопасности.

Ответы на поставленные вопросы могут помочь сформулировать цели создания системы безопасности в организации. Если, к примеру, 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 определенных целей создания системы безопасности необходимо выработать стратегию достижения этих целей. Эта стратегия должна соответствовать важности защищаемых ресурсов. 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 количества, содержания и важности поставленных целей, при этом обычно организация считает необходимым распространить поставленные требования на все свои подразде-

ления. По своему содержанию, основные положения могут носить как весьма специфический, так и общий характер.

В качестве примера положений первого типа можно привести случай, 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 вирусами путем повсеместного размещения антивирусных программных средств (или выделения отдельных сайтов, через которые должна проходить вся получаемая информация, для проверки на наличие вирусов).

В качестве примера положений второго типа, имеющих общий характер, можно привести случай, когда основная работа организации заключается в предоставлении информационных сервисов, в связи с чем возможные потребители должны быть уверены в защищенности ее систем. В этом случае основным положением стратегии может быть проведение аттестации систем 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:

– 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 категорирования систем по уровням важности защиты информации в масштабах всей организации;

– оценка необходимости учета и проверка условий безопасности соединений до места подключения к ним других организаций;

– определение практических схем принятия защитных мер в случае нарушения системы безопасности.

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

5.2 Политика безопасности информационных технологий

Политика безопасности информационных технологий должна вырабатываться на основе содержания корпоративной стратегии и целей создания системы обеспечения безопасности. Важно сформировать политику и затем

проводить ее в соответствии с направленностью корпоративной 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 5.1, важным фактором, влияющим на содержание политики безопасности информационных технологий, является то, как в организации используются эти технологии. Чем более важной является необходимость их использования, и чем больше 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 одних условиях производственной деятельности и могут оказаться неприемлемыми в других.

Перечисленные в политике безопасности мероприятия, касающиеся проблем обеспечения безопасности информационных технологий, могут основываться на целях и стратегии организации, на результатах проведенного ранее анализа риска систем безопасности и принципов управления, на результатах проведения дополнительных мероприятий, таких как проверка действенности состояния реализованных защитных мер, результаты 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 этих проблем безопасности. Более подробно эти методы и действия описываются в политиках безопасности различных систем информационных технологий, либо в других вспомогательных документах, например, в инструкциях обеспечения безопасности.

В разработке политики безопасности информационных технологий должны принимать участие представители:

– служб аудита;

– финансовых служб;

– подразделений, обслуживающих информационные системы, и их пользователей;

– служб, обеспечивающих функционирование вычислительной техники и инфраструктур (т.е. лиц, ответственных за состояние помещений и вспомогательного оборудования, электрооборудования и кондиционеров);

– служащие;

– служб безопасности;

– руководства организации.

В соответствии с целями безопасности и стратегией, принятой организацией для достижения этих целей, выбирается соответствующий уровень детализации политики безопасности информационных технологий. Описание данной политики должно включать, 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 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, необходимые 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 к информации);

– сведения о вопросах понимания мер безопасности и обучения лиц, осуществляемых организацией;

– сведения об общих процедурах контроля и поддержания безопасности;

– общие проблемы обеспечения безопасности, касающиеся обслуживающего персонала;

– средства и способы доведения сути политики до всех заинтересованных лиц;

– обстоятельства, при которых может быть проведен пересмотр политики;

– методы контроля изменений, вносимых в политику безопасности.

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;

– меры, принимаемые в случаях, связанных с нарушением безопасности;

– мониторинг функционирования системы информационных технологий;

– обстоятельства, при которых требуется приглашение сторонних экспертов по проблемам обеспечения безопасности.

Пример основного содержания политики безопасности информационных технологий приведен в приложении А.

Как уже говорилось в этом разделе, результаты проведенного ранее анализа риска и принципов управления, проверки действующей системы безопасности и случаев нарушения безопасности могут отразиться на содержании политики безопасности информационных технологий. А это, в свою очередь, может привести к возникновению ситуации, когда необходим пересмотр или доработка ранее сформулированной стратегии (или политики).

Для того чтобы гарантировать поддержку в проведении всех мероприятий, связанных с вопросами безопасности, необходимо, чтобы политика безопасности информационных технологий была одобрена высшим руководством предприятия.

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

Один из служащих должен быть назначен ответственным за реализацию политики безопасности информационных технологий и за обеспечение того, чтобы эта политика отражала требования и реальное состояние дел в организации. Обычно таким человеком в организации является сотрудник службы безопасности информационных технологий, который, помимо всего прочего, должен отвечать и за проведение дополнительных мероприятий. Данные мероприятия должны включать проверки соответствия требованиям информационной безопасности, управление инцидентами и слабыми местами в защи-

те, а также внесение изменений в содержание политики безопасности, если в результате проведенных мероприятий возникнет такая необходимость.

6 Основные варианты стратегии анализа корпоративного риска

Прежде чем приступить к любым действиям, связанным с анализом риска, организация должна иметь стратегию для проведения такого анализа, причем составные части этой стратегии (методы, способы и т.д.) должны быть отражены в содержании политики безопасности информационных технологий. Эти методы и критерии выбора вариантов стратегии анализа риска должны отвечать потребностям организации. Стратегия анализа риска должна обеспечивать соответствие выбранного варианта подхода условиям осуществления деловых операций и приложений усилий по обеспечению безопасности в тех областях, где это действительно необходимо. Рассматриваемые ниже варианта представляют четыре различных подхода к анализу риска. Основное различие между ними состоит в уровнях 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 требуемого эффекта, необходимо найти баланс между указанными вариантами.

Если не рассматривать вариант, заключающийся в непринятии каких-либо защитных мер и допустить, что заранее неизвестного появление различных видов риска заданного уровня и интенсивности, то существуют четыре основных варианта стратегии анализа корпоративного риска:

– использовать один и тот же базисный подход (с низкой степенью риска) для всех систем информационных технологий, независимо от уровня риска, которому подвергаются системы, принимая при этом, что уровень обеспечения безопасности не всегда может оказаться достаточным;

– использовать неформальный подход к проведению анализа риска, обращая особое внимание на системы информационных технологий, которые, как представляется, подвергаются наибольшему риску;

– проводить детальный анализ риска с использованием формального подхода ко всем системам информационных технологий, или же:

– провести сначала анализ рисков высокого уровня с тем, чтобы определить, какие системы информационных технологий подвержены высокому уровню риска и какие имеют критичное значение для ведения деловых операций, с последующим проведением детального анализа риска для выделенных систем, а для всех остальных ограничиться применением базисного подхода к проблемам обеспечения безопасности.

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

Если организация решит не уделять внимания вопросам безопасности или отложить на потом внедрение защитных мер, ее руководство должно ясно представлять возможные последствия такого решения. Несмотря на то, что в этом случае и отпадает необходимость затрат времени, средств, рабочих или других ресурсов, такое положение имеет ряд недостатков. Если только организация не уверена в том, что функционирование ее систем информационных технологий абсолютно не критично к внешним угрозам, она может потом встретиться с серьезными ситуациями. Так, организация может нарушить положения законодательных и нормативных актов, или ее репутация может пострадать в случаях, если будут иметь место несанкционированные доступы к информации и окажется, что не было предпринято никаких действий по их предупреждению. Если организацию не очень заботят проблемы обеспечения безопасности информационных технологий или же она не имеет систем, безопасность которых важна для ведения деловых операций, она имеет право следовать подобной стратегии. Однако при этом она остается в положении, когда не имеет представления о том, насколько хорошо или плохо реальное состояние дел, так что для большинства организаций следование такой стратегии вряд ли является правильным.

6.1 Базисный подход

В случае использования первого варианта подхода организация может применить базисный уровень обеспечения безопасности ко всем системам информационных технологий путем выбора стандартных защитных мер безопасности. Перечень рекомендуемых стандартных защитных мер приведен в основных документах и обычно применяемых кодах; более подробное описание этого варианта подхода можно также найти в 7.2.

Существует ряд преимуществ использования этого варианта подхода, а именно:

– 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 использовании базисной защиты можно получить экономически эффективное решение, поскольку одни и те же или схожие базисные защитные меры могут без особых проблем быть применены во многих системах, если их количество в рамках организации функционирует в одних и тех же условиях, и если предъявляемые к обеспечению безопасности требования соизмеримы.

В то же время, этот вариант подхода имеет и свои недостатки, а именно:

– если устанавливается слишком высокий базисный уровень, то для ряда систем информационных технологий будет иметь место завышенный уровень обеспечения безопасности;

– если базисный уровень будет принят слишком низким, то для ряда систем информационных технологий уровень обеспечения безопасности будет недостаточным, что увеличит риск ее нарушения, а кроме того:

– могут возникнуть трудности при внесении изменений, затрагивающих вопросы обеспечения безопасности. Так, если была проведена модернизация системы, то могут возникнуть сложности при оценке того, могут ли первоначально использовавшиеся базисные защитные меры и далее быть 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 базисный уровень безопасности должен выбираться таким образом, чтобы он соответствовал уровню защиты, требующемуся для большинства систем информационных технологий. Для большинства организаций всегда существует необходимость использования некоторых минимальных стандартных уровней для того, чтобы обеспечить защиту важнейшей информации и отвечать требованиям правовых и нормативных актов – например, требованиям закона о безопасности информации. Однако в тех случаях, когда отдельные системы организации характеризуются различной степенью важности, объемами и сложностью деловой информации, использование общих стандартов применительно ко всем системам не будет ни логическим, ни экономически оправданным.

6.2 Неформальный подход

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

Этот метод имеет следующие достоинства:

– он обычно не требует использования значительных средств или времени. При использовании неформального метода 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 метод имеет и свои недостатки:

– отсутствие формального подхода и полного перечня проверок увеличивает вероятность пропуска важных деталей;

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

– эксперты, не обладающие значительным опытом собственной работы в области анализа риска, вряд ли смогут найти для себя готовые рекомендации, которые могли бы облегчить их работу;

– отдельные подходы в прошлом были продиктованы исключительно оценкой уязвимости систем, то есть потребность в мерах обеспечения безопасности основывалась на наличие у этих систем уязвимостей без анализа того, существуют ли угрозы, способные реализовать наличие этих уязвимостей; то есть без обоснования реальной необходимости в использовании защитных мер;

– результаты анализа могут в какой-то мере зависеть от субъективного подхода, от личных предубеждений эксперта;

– могут возникнуть проблемы в случае, если специалист, который проводил неформальный анализ, покидает организацию.

С учетом приведенных выше недостатков этот вариант подхода к анализу риска для многих организаций не будет эффективным.

6.3 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 подробную идентификацию и определение ценности ресурсов, оценку возможных угроз, которым могут подвергнуться эти ресурсы, а также оценку уровня их уязвимости. Результаты этих операций затем используются для оценки рисков и последующего выявления обоснованных защитных мер. Этот вариант подхода подробно описан в 7.3.

Он имеет следующие преимущества:

– весьма вероятно, что в результате такого подхода для каждой из систем будут определены соответствующие ей защитные меры (средства) обеспечения безопасности;

– результаты 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 требуется затратить значительное количество средств, времени и квалифицированного труда, чтобы получить требуемый результат;

– существует вероятность того, что определение необходимых защитных мер для некоторой критичной системы произойдет слишком поздно, по-

скольку анализ будет проводиться одинаково тщательно для систем информационных технологий и в целях завершения анализа всех систем потребуется значительное время.

Таким образом, использование детального анализа риска применительно ко всем системам информационных технологий не рекомендуется. Если же решено прибегнуть к такому подходу, то возможен ряд дополнительных разновидностей его использования:

– использовать стандартный подход, отвечающий критериям, упоминающимся в данном стандарте (например, использовать подход, описанный в 7.3);

– использовать стандартный подход в его различных вариантах, отвечающих потребностям организации; для ряда организаций предпочтительным может быть использование "метода моделирования риска" (описанного в 7.3).

6.4 Комбинированный подход

В соответствии с этим четвертым вариантом подхода предполагается провести предварительный анализ высокого уровня риска для всех систем информационных технологий, обращая каждый раз особое внимание на деловую значимость системы и на степень риска, которому она подвергается. Для систем информационных технологий, которые, как выяснилось, имеют важное значение для деловой деятельности организации и/или подвержены высокой уровня риска, следует провести детальный анализ риска в первую очередь. Для всех остальных систем информационных технологий следует ограничиться базисным вариантом подхода. Таким образом, комбинированный вариант, сочетающий, по сути, лучшие качества подходов, описанных в 6.1 и 6.3, позволяет при сведении к минимуму времени и усилий, затраченных на выявление должных защитных мер, все же обеспечить необходимую защиту систем с высокой степенью риска.

Кроме того, этот вариант подхода имеет следующие преимущества:

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

– имеется возможность быстро оценить оперативное состояние организационной программы обеспечения безопасности, то есть использование такого подхода будет в значительной мере способствовать успешному планированию;

– ресурсы и средства могут быть вложены там, где они принесут максимальный эффект, так как в первую очередь они будут направлены в те системы, которые в наибольшей уровня нуждаются в обеспечении безопасности и проведение последующих мероприятий будет более успешным.

Единственный потенциальный недостаток данного варианта подхода состоит в следующем:

– поскольку предварительные анализы риска проводятся, исходя из предположения о его высоком уровне, хотя, возможно, они и не обладают им, в связи с чем отдельные системы могут быть ошибочно отнесены к системам, не требующим проведения детального анализа риска. С другой стороны, к этим системам в дальнейшем будут применены базовые методы обеспечения безопасности. К тому же, в случае необходимости можно будет еще раз вернуться к рассмотрению этих систем с тем, чтобы удостовериться, не требуют ли они более тщательного по сравнению с базисным подходом рассмотрения.

Использование подхода с анализом высокого уровня риска в сочетании с базисным подходом и (там, где это необходимо) с детальным анализом риска обеспечивает большинству организаций наиболее эффективное решение проблем. В связи с этим, подобный подход является наиболее предпочтительным и будет более подробно рассмотрен в разделе 9.

7 Комбинированный подход

Этот раздел содержит указания для реализации рекомендованной выше стратегии комбинированного анализа риска.

7.1 Анализ высокого уровня риска

Прежде всего, необходимо провести предварительный анализ для высокого уровня риска с тем, чтобы установить, какой вариант подхода (базисным или детальный анализ риска) является наиболее подходящим для той или иной системы информационных технологий. В ходе проведения такого предварительного анализа рассматривается деловая значимость систем информационных технологий и обрабатываемой с их помощью информации, а также уровни рисков 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 обстоятельств:

– деловых целей, для достижения которых организация использует данную систему информационных технологий;

– до какой степени деловая активность предприятия зависит от данной системы информационных технологий, т.е. насколько функции, которые организация считает критичными для своего существования или для эффективной реализации деловой деятельности, зависят от функционирования этой системы, или же от обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации, обрабатываемой этой системой;

– вложения денежных средств в эту систему информационных технологий, в том числе на ее разработку, обслуживание или на замену;

– ресурсов данной системы, в которые организация непосредственно вкладывает средства.

После того как эти обстоятельства проанализированы, принятие решения обычно не вызывает затруднений. Если целевое назначение системы важно для проведения организацией своей деловой деятельности, если стоимость замены системы высока или же если средства, вложенные в ресурсы, подвержены высокому уровню риска, то для данной системы необходимо проведение детального анализа риска. Наличия одного из перечисленных выше условий может быть достаточно для обоснования необходимости проведения детального анализа риска.

Следует придерживаться одного общего правила: если прекращение функционирования данной системы информационных технологий может причинить ущерб или принести убытки организации, отрицательно повлиять на ее деловую деятельность или на ее ресурсы, то для оценки потенциального риска требуется проведение детального анализа риска (см. 7.3). Во всех других случаях достаточная безопасность системы может быть обеспечена при применении базисного подхода (см. 7.2).

7.2 Базисный подход

Цель обеспечения безопасности на базисном уровне состоит в том, чтобы подобрать для организации минимальный набор защитных мер для защиты всех или отдельных систем информационных технологий. Используя такой подход, можно применять базисный уровень безопасности в масштабах всей организации, а кроме того (как указывалось выше), 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 базисного подхода позволяет уменьшить размер ассигнований, которые организация вынуждена тратить на рассмотрение результатов анализа риска (см. 6.1).

Удовлетворительная защита на базисном уровне может быть обеспечена путем использования каталогов по защитным мерам безопасности, в которых можно подобрать набор средств для защиты системы информационных технологий от наиболее часто встречающихся угроз. Уровень базисной защиты может быть установлен в соответствии с потребностями организации, при этом в проведении детальной оценки угроз, рисков и уязвимости систем нет необходимости. Все, что требуется сделать для установки базисного уровня защиты – это выбрать те пункты каталога мер защиты, которые подходят для рассматриваемой системы информационных технологий. При наличии в системе установленных средств защиты необходимо сравнить их с рекомендуемыми в каталогах. Меры защиты, которые отсутствуют в системе, но могут быть использованы в ней, следует реализовать.

Каталоги по защитным мерам безопасности могут содержать подробное описание рекомендуемых мер (средств) защиты, либо же содержать рекомендации с набором требований по обеспечению безопасности, которыми можно воспользоваться при выборе таких мер для рассматриваемой системы. Оба варианта имеют свои преимущества. Сведения о каталогах обоих типов можно найти в приложениях, приведенных в СТ РК ИСО/МЭК 13335-4-2008. Одной из целей базисного подхода является согласование защитных мер в масштабах всей организации, что может быть достигнуто при использовании каждого из указанных выше вариантов.

В настоящее время уже существует несколько документов, с помощью которых можно получить наборы базисных 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 каталоги с перечнем базисных мер безопасности могут быть использованы несколькими различными организациями. Такие каталоги можно получить, например:

– в службах международных и национальных стандартов;

– в службах отраслевых стандартов (или нормативов);

– в других компаниях, скорее всего в компаниях, имеющих ту же деловую направленность или сопоставимых по масштабам работ.

Любая организация может, конечно, выработать свой собственный базисный уровень безопасности, проанализировав его с собственными условиями производственной деятельности и деловыми целями.

7.3 Детальный анализ риска

Как было показано в 6.3, детальный анализ риска для систем информационных технологий предполагает выявление соответствующих рисков и оценку их уровня. Необходимость в проведении детального анализа риска может быть определена без ненужных затрат времени и средств после рассмотрения высокого уровня риска для всех систем и последующего изучения результатов детального анализа риска, проведенного только для критичных систем или систем с высоким уровнем риска, как это было рекомендовано в 6.4.

Анализ риска проводится путем выявления инцидентов, создающих неблагоприятные деловые ситуации, и определения вероятности их появления. Нежелательные события также могут негативно влиять на деловой процесс, на сотрудников или на любую другую значимую для организации сущность. Такое неблагоприятное воздействие инцидентов является сложным сочетанием возможных видов ущерба, наносимого стоимости ресурсов, подвергающихся риску. Вероятность совершения такого события зависит от того, насколько привлекательным является данный ресурс для потенциального нарушителя, от вероятности реализации опасности и от легкости, с какой на-

рушитель может воспользоваться уязвимыми местами системы. Результаты анализа риска позволяют выявить и выбрать меры обеспечения безопасности, которые могут быть использованы для снижения уровня выявленного риска до приемлемого уровня.

Детальный анализ риска предполагает тщательное рассмотрение каждого из шагов, показанных на рисунке 2. Его результаты позволяют проводить выбор обоснованных защитных мер как часть процесса управления риском. Требования, которые предъявляются к этим мерам защиты, зафиксированы в политике безопасности системы ИТ и в соответствующем ей плане защиты. Появление случаев нарушения системы безопасности и внешних угроз может оказать влияние на требования к обеспечению безопасности системы и вызвать необходимость в пересмотре части методов анализа риска (или всего анализа). К таким внешним угрозам могут относиться: недавние существенные изменения в системе, запланированные изменения, а также последствия нарушений безопасности, по которым необходимо принимать соответствующие меры.

Существует несколько методов проведения анализа риска, начиная от подходов, основывающихся на перечне контрольных операций, и кончая методами, основанными на структурном анализе. При этом могут использоваться как автоматизированные (компьютерные), так и ручные программы. Какой бы метод или программа не использовались организацией, они должны, по меньшей мере, содержать операции, перечисленные в следующих разделах. 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 ресурсах и их ценностях, об угрозах, об уязвимостях и уровнях риска, об определенных мерах обеспечения безопасности они должны быть сохранены (например, в базе данных). Очевидно, применение методов, задействующих вспомогательные программные средства, сильно облегчает этот процесс. Эта представляемая информация, которая иногда рассматривается в качестве модели, может затем быть использована довольно эффективно после того, как со временем происходят изменения, независимо от того, касаются ли они конфигурации, типа обрабатываемой информации, сценариев угроз и т.д. При этом в качестве входных данных вводятся лишь сведения об этих изменениях, что позволяет определить влияние изменений на необходимые меры обеспечения безопасности. Более того, такие модели могут быть использованы для быстрого изучения различных вариантов, скажем, при разработке новой системы информационных технологий или же применительно к другим системам, схожим по принципам построения.

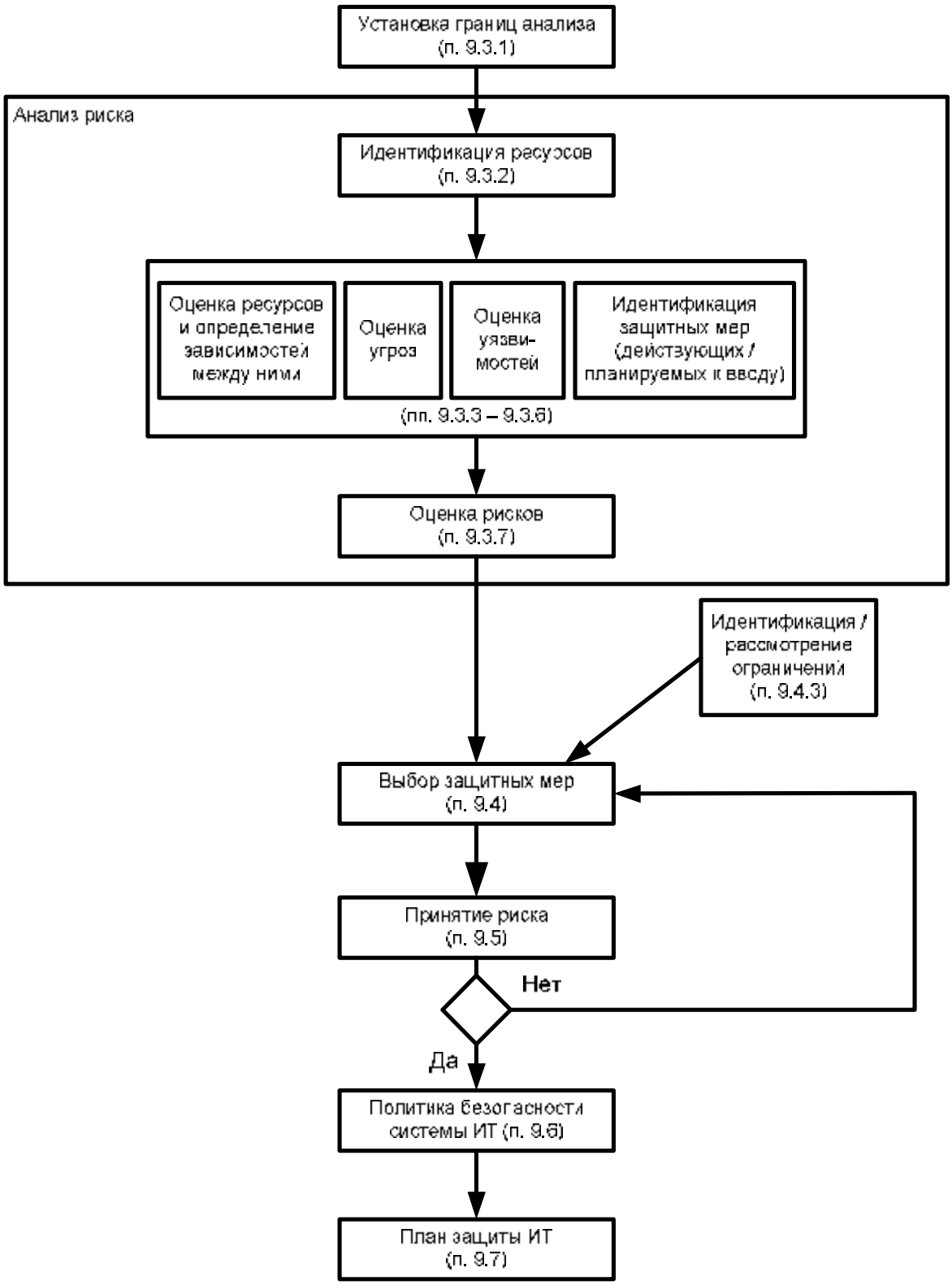

Рисунок 2 – Детальный анализ риска в составе процесса управления риском

7.3.1 Установление границ рассмотрения

Как видно из рисунка 2, прежде чем получить исходные данные для идентификации и оценки ресурсов, необходимо определить границы рассмотрения. Тщательное определение границ на этой стадии позволяет избежать ненужных операций и повысить качество анализа риска. Описание границ рассмотрения должно четко определить, какие из перечисленных ниже факторов должны быть учтены при рассмотрении результатов анализа риска для определенной системы информационных технологий:

– ресурсы информационных технологий (например, аппаратные средства, информационное обеспечение, информация);

– служащие (например, персонал организации, субподрядчики, персонал сторонних организаций);

– условия осуществления производственной деятельности (например, имеющиеся здания, оборудование);

– деловая деятельность (операции).

7.3.2 Выявление ресурсов

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

– информация/данные (например, файлы, содержащие информацию о платежах или о продукте);

– аппаратные средства (например, компьютеры, принтеры);

– программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения);

– оборудование средств 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);

– изготовленные товары;

– сервисы (например, информационные и вычислительные сервисы);

– конфиденциальность и доверие при предоставлении сервисов (например, платежных сервисов);

– оборудование, обеспечивающее необходимые условия работы;

– личный состав;

– престиж (имидж) организации.

Все ресурсы, включенные в установленные границы рассмотрения (см. 7.3.1), должны быть обнаружены и наоборот, – любые ресурсы, выведенные за границы рассмотрения (независимо от того, по каким соображениям), должны быть рассмотрены еще раз с тем, чтобы убедиться, что они не были забыты или упущены.

7.3.3 Оценка ресурсов и установление зависимости между ресурсами

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

Исходные данные для оценки ресурсов должны быть получены от владельцев и пользователей ресурсов. Специалист (специалисты), проводящий анализ риска, должен составить перечень ресурсов; при этом необходимо запросить содействие у лиц, непосредственно занимающихся планированием деловой деятельности, финансами, информационными системами и другими соответствующими направлениями деловой активности с тем, чтобы определить ценность каждого из ресурсов. Полученные данные необходимо соотнести со стоимостью создания и обслуживания ресурса, а также с возможностью негативного воздействия на деловую деятельность, связанного с нарушением конфиденциальности, целостности, доступности, достоверности и надежности информации. Каждый из выявленных ресурсов должен представлять ценность для организации. Однако вряд ли будет возможно прямо и просто определить финансовую стоимость каждого из них. Необходимо также определить ценность или степень важности ресурса для организации в некоммерческой деятельности. В противном случае будет трудно выявить уровень необходимой защиты и объем средств, которые организации следует израсходовать на принятие мер защиты. Примером такой шкалы оценок может быть определение уровня ценности как низкой, средней или высокой, или же, с большей степенью детализации:

– пренебрежимо малая – низкая – средняя – высокая – очень высокая.

В приложении Б описываются более подробно возможные уровни и градации оценки, которые могут быть использованы при определении ценности ресурсов, основываясь на оценке возможного ущерба. Независимо от используемой шкалы оценок, в ходе их проведения необходимо рассмотреть

проблемы, связанные с уровнем возможного ущерба, причиной которого может быть:

– нарушение правовых и/или нормативных положений;
– снижение уровня деловой активности;
– потеря/ухудшение репутации;
– нарушение конфиденциальности личной информации;
– возникновение угрозы личной безопасности;
– негативные последствия введения закона в силу;
– нарушение конфиденциальности в коммерческих вопросах;
– случаи нарушения общественного порядка;
– финансовые потери;
– перебои в выполнении деловых операций;
– опасность экологического ущерба.

Каждая организация может выдвинуть и собственные критерии оценки, исходя из важности отдельных проблем для своего бизнеса; эти критерии следует включить в число критериев, приведенных в приложении Б. Кроме того, организация должна установить свои собственные пределы для ущербов, определяемых как "низкие" и "высокие". Так, например, финансовый ущерб, который может быть катастрофически высоким для небольшой компании, может оказаться низким или пренебрежимо малым для очень крупной компании.

На этой стадии процесса оценки следует подчеркнуть, что метод оценки должен обеспечивать получение не только количественных оценок, но и качественных – там, где получение количественных оценок невозможно или нелогично (например, возможность оценки стоимости потери жизни или деловой репутации). К используемой шкале оценок должны быть даны соответствующие пояснения.

Следует также выявить виды зависимости одних ресурсов от других, поскольку наличие таких зависимостей может оказать влияние на оценку ресурсов. 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 обрабатываемых конфиденциальности данных. Кроме того, если деловой процесс зависит от целостности отдельных данных, вырабатываемых программой, 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. К тому же, функционирование аппаратных средств будет зависеть от качества энергоснабжения и, возможно, от работы систем кондиционирования. Таким образом, данные о зависимостях, существующих между отдельными ресур-

сами, будут способствовать идентификации соответствующих видов угроз и определению конкретных уязвимостей; их использование также будет придавать уверенность в том, что ресурсы оценены в соответствии с их реальной ценностью (с учетом существующих взаимозависимостей) и что уровень безопасности выбран обоснованно.

Уровни ценности ресурсов, от которых зависят другие ресурсы, могут быть изменены в следующих случаях:

– если уровни ценности зависимых ресурсов (например, данных) ниже или равны уровню ценности рассматриваемого ресурса (например, программного обеспечения), то этот уровень останется прежним;

– если уровни ценности зависимых ресурсов (например, данных) выше, то уровень ценности рассматриваемого ресурса (например, программного обеспечения) необходимо повысить с учетом:

– уровня соответствующей зависимости;

– уровней ценности других ресурсов.

Организация может иметь в своем распоряжении отдельные ресурсы, доступ к которым происходит неоднократно, например, копии программ систем программного обеспечения или однотипные персональные компьютеры, которые используются в большинстве учреждений. Этот факт необходимо учитывать при проведении оценки ресурсов. С одной стороны, эти копии и т.д. в ходе оценки легко упустить из виду, 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 ресурсов и их ценности с учетом таких показателей, как раскрытие информации (сохранение конфиденциальности), изменение данных (сохранение целостности), невозможность доступа и разрушение информации (сокращение доступности) и стоимость замены.

7.3.4 Оценка угроз

Угроза (потенциальная возможность неблагоприятного воздействия) обладает способностью наносить ущерб рассматриваемой системе информационных технологий и ее ресурсам. Если эта угроза реализуется, она может как-то взаимодействовать с системой и вызвать нежелательные инциденты, оказывающие неблагоприятное воздействие на систему. В основе угрозы может лежать как природный, так и человеческий фактор, они могут реализовываться случайно или преднамеренно. Источники как случайных, так и преднамеренных угроз должны быть выявлены, а вероятность их реализации должна быть оценена. Важно не упустить из виду ни одной возможной угрозы, так как результатом этого может стать нарушение функционирования и появление слабых мест в защите информационных технологий.

Исходные данные для оценки угроз следует получать от владельцев или пользователей ресурсов, от служащих отделов кадров, от специалистов по разработке оборудования и по информационным технологиям, а также от лиц, отвечающих за реализацию мер защиты в организации. Другие организации, например, правовые учреждения и органы государственной власти, также могут оказать помощь при проведении оценки угроз, например, предоставить соответствующие статистические данные. Полезным может оказаться использование перечня наиболее часто встречающихся возможных угроз -примеры приведены в приложении В. И тем не менее, небесполезно обратиться к помощи, а также к каталогам возможных угроз (которые, возможно, являются более соответствующими 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 проявления угроз:

– ошибки и упущения;

– мошенничество и кража;

– случаи вредительства со стороны персонала;

– ухудшение состояния материальной части и инфраструктуры;

– злонамеренные действия хакеров, например, имитация действий законного пользователя;

– вредоносный код;

– промышленный шпионаж.

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

После выявления 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 ресурсов 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 и выходу из строя оборудования и послужить причиной реализации случайной угрозы.

В зависимости от требуемой точности анализа, может возникнуть необходимость разбить ресурсы на отдельные компоненты и рассматривать угрозы относительно этих компонентов. Например, одним из материальных ресурсов могут быть "центральные серверы обслуживания данных", но когда выясняется, что эти серверы расположены в различных географических точках, то этот ресурс необходимо разделить на "центральный сервер 1" и "центральный сервер 2", поскольку для них одни угрозы могут различаться по характеру, а другие - по степени опасности. Таким же образом ресурс, включающий программное обеспечение, может носить название "прикладное программное обеспечение", но затем его можно разбить на 2 или более элементов "прикладного программного обеспечения". Для ресурса, содержащего данные, можно привести случай, когда он первоначально именовался "досье на преступников", а затем его пришлось разбить на два: "текст досье на преступников" и "изобразительная информация к досье на преступников".

По завершении оценки угроз составляется перечень выявленных угроз, ресурсов или групп ресурсов, подверженных этим опасностям, а также определяется степень вероятности реализации угроз с разбивкой на группы высокой, средней и низкой вероятности.

7.3.5 Оценка уязвимости

Этот вид оценки предполагает выявление слабых мест в физической среде, организационных процессах, процедурах, аппаратном и программном обеспечении, средствах связи, а также у сотрудников, руководителей и администраторов. В первую очередь выявлению подлежат те слабые места, которые могли бы быть использованы источником угрозы для нанесения ущерба ресурсам и деловой деятельности, осуществляемой с их использованием. Само по себе наличие уязвимостей не приносит ущерба, поскольку для этого необходимо присутствие соответствующей угрозы. Существование уязвимого места при отсутствии такой угрозы не требует применения мер защиты, но подобный факт должен быть зафиксирован и в дальнейшем отслеживаться на случай изменения ситуации. Следует отметить, что некорректно выбранные, неправильно функционирующие и некорректно используемые защитные меры безопасности могут сами по себе стать источниками появления уязвимостей.

Понятие уязвимости можно отнести к свойствам или атрибутам ресурса, которые могут использоваться иным образом или для иных целей, чем те,

для которых приобретался или изготавливался данный ресурс. Например, одним из свойств ЭСППЗУ (электронно-стираемое программируемое ПЗУ) является то, что хранящаяся в нем информация может быть стерта или заменена, это одна из конструктивных характеристик ЭСППЗУ. Однако наличие такого свойства означает также, что возможно несанкционированное уничтожение информации, хранящейся на ЭСППЗУ, т.е. здесь мы имеем дело со случаем возможной уязвимости.

В процессе оценки происходит выявление уязвимостей, в которых могут быть реализованы возможные угрозы, а также оценка вероятного уровня уязвимости, то есть легкости реализации угрозы. Например, отдельные виды ресурсов можно легко продать, скрыть или переместить – все эти свойства могут быть связаны с наличием уязвимости. Исходные данные для оценки уязвимости должны быть получены от владельцев или пользователей ресурса, от специалистов по обслуживающим устройствам, от экспертов по программным и аппаратным средствам систем информационных технологий. В качестве примеров уязвимостей можно привести:

– 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.

Другие примеры возможных уязвимостей можно найти в Приложении Г.

Важно оценить, насколько велика степень уязвимости, другими словами насколько легко ее можно будет использовать. Степень уязвимости следует оценивать по отношению к каждой угрозе, которая может использовать эту уязвимость в определенной ситуации. Например, какая-то система может оказаться уязвимой к угрозе имитации идентичности пользователя и к несанкционированному использованию ресурсов. Степень уязвимости по отношению к имитации идентичности 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 все же ограничены.

В результате завершения данного этапа должен быть составлен перечень уязвимости и проведена оценка вероятности возможной реализации отмеченной уязвимости, например - высокая, средняя или низкая.

7.3.6 Выявление существующих/планируемых защитных мер

Использование защитных мер, выявленных вследствие рассмотрения результатов анализа риска, должно проводиться с учетом уже существующих или планируемых защитных мер. Важно, чтобы выявление таких действующих защитных мер было частью общего процесса с тем, чтобы избежать не вызываемых необходимостью затрат труда и средств, то есть фактического дублирования защитных мер. Кроме того, при рассмотрении может оказаться, что использование действующих или планируемых защитных мер на самом деле происходит без должного обоснования. В этом случае необходимо проверить, следует ли заменить эти меры обеспечения безопасности новыми, более подходящими, или же оставить их на месте (например, по экономическим соображениям).

Кроме того, необходимо провести дополнительную проверку с тем, чтобы определить, являются ли защитные меры безопасности, выбранные после рассмотрения результатов анализа риска (см. 7.4), совместимыми с действующими и планируемыми мерами безопасности, то есть выбранные и действующие меры безопасности не должны противоречить друг другу.

В процессе выявления уже действующих защитных мер безопасности необходимо проверить, правильно ли они функционируют. Если предполагалось, что какое-то средство защитной меры безопасности функционирует правильно, однако это не подтверждается в процессе осуществления деловых операций, то его наличие может стать потенциально уязвимым местом системы.

По результатам проведения этого этапа составляется перечень всех действующих и планируемых защитных мер безопасности с указанием статуса их реализации и использования.

7.3.7 Оценка рисков

Целью данного этапа является выявление и оценка рисков, которым подвергаются рассматриваемая система информационных технологий и ее ресурсы с тем, чтобы идентифицировать и выбрать подходящие и обоснованные защитные меры безопасности. Характер риска определяется ценностью подвергающихся риску ресурсов, вероятностью реализации угроз, способных оказать негативное воздействие на деловую активность, возможностью использования уязвимостей выявленными угрозами, а также наличием каких-либо действующих или планируемых мер защиты, использование которых могло бы снизить уровень риска.

Существуют различные способы учета таких факторов, например, можно объединить оценки риска, связанные с ресурсами, уязвимостями и угрозами, чтобы получить оценки определения общего уровня риска. Подробное рассмотрение различных вариантов подхода к анализу риска, основанных на

использовании оценок, полученных для ресурсов, уязвимостей и угроз, можно найти в приложении Д.

Вне зависимости от использованного способа оценки уровня 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. Полученные оценки уровня риска затем используются при выявлении рисков, на которые следует обращать внимание в первую очередь при выборе защитных мер. Метод оценки рисков должен допускать многократность его применения и отслеживаемость получаемых результатов.

Как говорилось выше, 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.

7.4 Выбор мер защиты

Для снижения оцененных уровней риска до приемлемых необходимо выявить и выбрать подходящие и обоснованные меры безопасности. Для того чтобы этот выбор был правильным, необходимо принимать во внимание наличие действующих или запланированных мер безопасности, архитектуру обеспечения безопасности информационных технологий и наличие ограничений различного типа. Дополнительные рекомендации по выбору защитных мер можно найти в СТ РК ИСО/МЭК 13335-4-2008.

7.4.1 Определение мер защиты

Результаты оценки уровня риска, проведенной на предыдущем этапе, должны использоваться в качестве основы для идентификации всех мер защиты, необходимых для должного обеспечения безопасности системы.

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

Возможны и альтернативные варианты используемых мер защиты, выбор которых производится, исходя из стоимости рассмотренных мер защиты. Область использования мер защиты включает:

– физическую окружающую среду;

– обслуживающий персонал;

– организационное управление;

– аппаратные средства/программное обеспечение;

– средства связи и передачи данных.

Действующие и запланированные меры защиты безопасности следует рассмотреть повторно с точки зрения их сравнительной стоимости (с учетом стоимости обслуживания) и принять решение об их не включении (или отказе от их реализации) или доработке – если они недостаточно эффективны. Здесь следует отметить, что иногда исполнение недостаточно эффективных действующих мер защиты обходится дороже, чем их использование при применении условии реализации дополнительного включения защитных мер (в случае необходимости). Возможны также случаи, когда действие защитных мер может быть распространено на ресурсы, находящиеся за установленными границами рассмотрения.

Для выявления защитных мер полезно рассмотреть уязвимости системы, требующие защиты, и виды угроз, которые могут реализоваться при наличии этих уязвимостей. Существует ряд наиболее реальных возможностей уменьшения уровня риска:

– избегать риска;

– перераспределить риск (например, путем страхования);

– снизить уровень угроз;

– снизить степень уязвимости;

– минимизировать последствия возможной реализации угроз;

– отслеживать появление нежелательных событий, реагировать на их появление и устранять их последствия.

Какая из этих возможностей (или сочетание их) окажется наиболее приемлемой, зависит от обстоятельств. Значительную помощь может оказать также использование каталогов. Однако при использовании защитных мер, выбранных по каталогу, необходимо их доработать с тем, чтобы они удовлетворяли специфическим требованиям организации.

Другим важным аспектом выбора мер защиты являются экономические соображения. Неоправданно было бы рекомендовать использование таких защитных мер, стоимость реализации и эксплуатации которых превышала бы стоимость защищаемых ресурсов. Также нерационально было бы рекомендовать использование таких мер защиты, стоимость которых превышала бы бюджет организации, где предполагается их использование. Однако следует с большой осторожностью подходить к случаям, когда из-за ограниченности бюджета приходится уменьшать количество или снижать качество реализуемых мер защиты, поскольку это подразумевает возможность более высокой уровня риска, чем планировалось. При использовании предельных

значений ассигнуемых сумм в качестве лимитирующего фактора при выборе защитных мер следует быть особенно осторожным.

В тех случаях, когда для обеспечения безопасности системы информационных технологий используется базисный подход, выбор мер защиты сравнительно прост. Каталог мер обеспечения безопасности предлагает 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 те упомянутые в каталоге меры, которые отсутствуют или применение которых не планируется, составляют перечень защитных мер, которые необходимо реализовать для обеспечения базисного уровня защиты.

Выбор мер защиты должен всегда включать сочетание организационных (не технических) и технических мер защиты. Организационные меры включают в себя обеспечение безопасности на физическом уровне, на уровне управления персоналом и организацией.

Меры защиты на физическом уровне включают обеспечение прочности внутренних стен здания, использование кодовых дверных замков, систем пожаротушения и охранных служб. Обеспечение безопасности на уровне управления персоналом включает проверку сотрудников при приеме на работу (особенно лиц, занимающих важные с точки зрения обеспечения безопасности должности), контроль за работой сотрудников и реализацию программ знания и понимания мер защиты.

Организационное обеспечение безопасности включает безопасные способы ведения документации, наличие методов разработки и принятия прикладных программ, а также процедур обработки инцидентов безопасности. При таком способе обеспечения безопасности очень важно, чтобы для каждой системы была разработана целостная система ведения деловой деятельности, предусматривающая, в том числе, возможность появления непредвиденных обстоятельств (ликвидацию последствий нарушения систем безопасности), и включающая соответствующую стратегию и план (планы). Такой план должен содержать подробные сведения о важнейших функциях и приоритетах, подлежащих восстановлению, о необходимых условиях обработки информации и об организационных способах, которые необходимо осуществлять в случае аварии или временного прекращения работы системы. Эти планы должны 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 средств связи. При этом выбор мер защиты проводится в соответствии со степенью риска, чтобы обеспечить функциональную пригодность и надежную систему безопасности. Функцио-

нальная пригодность системы должна включать, например, проведение идентификации и аутентификации, 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 устанавливают уровень доверия, необходимый при осуществлении функций безопасности, и определяют тем самым виды проверок, тестирования безопасности и т.д., обеспечивающих подтверждение этого уровня. При принятии решения об использовании дополнительного набора оперативных и технических защитных мер могут существовать различные варианты выполнения требований к обеспечению технической безопасности. Должна быть определена архитектура технической безопасности для каждого из вариантов, с помощью которой можно получить дополнительное подтверждение того, что система безопасности построена правильно и может быть реализована на заданном технологическом уровне.

Организация может сделать выбор в пользу применения сертифицированных продуктов и систем в качестве одного из способов решения задачи окончательного построения системы. Сертифицированными считаются продукты, испытания которых проводились третьей стороной. Этой третьей стороной может быть другое подразделение той же организации или независимая организация, специализирующаяся на сертификации продуктов и систем. Испытания могут проводиться на соответствие набору заранее установленных критериев, которые формулируются исходя из особенностей создаваемой системы; в то же время, может существовать обобщенный набор критериев, которые могут соответствовать различным ситуациям. Критерии оценки продукта могут исходить из требований к функциональности и/или надежности. Существует несколько схем оценки качества, многие из них формируются по заказам правительственных организаций и служб международных стандартов. Организация может принять решение об использовании сертифицированных продуктов и систем, когда ей требуется уверенность в том, что продукт отвечает набору требований к функциональности, и когда ей необходимо иметь гарантии точности и полноты реализации элементов функциональности. В качестве альтернативы использованию сертифицированных продуктов можно привести проведение целевых практических испытаний продукта на безопасность, положительные результаты которых могут дать уверенность в качестве безопасности обеспечиваемой продуктом.

В процессе выбора мер защиты, предлагаемых для реализации, необходимо учитывать ряд факторов, среди них:

– доступность использования мер защиты;

– их прозрачность для пользователя;

– в какой мере их использование помогает пользователю решать свои задачи;

– относительная надежность (стойкость) системы безопасности;

– виды выполняемых функций – предотвращение, сдерживание, обнаружение, восстановление, исправление, мониторинг и информирование.

Обычно средство обеспечения безопасности предназначено для выполнения нескольких из числа перечисленных функций – чем больше, тем лучше. При рассмотрении системы безопасности в целом или набора используемых средств обеспечения безопасности следует установить, если возможно, необходимые пропорции между видами функций, что позволит обеспечить большую эффективность и действенность общей системы обеспечения безопасности в целом. Может потребоваться проведение анализа рентабельности или анализа на основе компромисса (метод сравнения возможных альтернативных вариантов с использованием набора критериев, каждому из которых придается свое весовое значение в зависимости от его относительной важности применительно к определенной ситуации).

7.4.2 Архитектура безопасности информационных технологий

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

Архитектура безопасности информационных технологий может использоваться при разработке новых систем, а также в случаях внесения существенных изменений в существующие системы. Она основывается на результатах анализа риска или базисного подхода, учитывает требования к обеспечению безопасности и перестраивает их в набор технических мер защиты по обеспечению безопасности для систем, которые будут удовлетворять этим требованиям. В ряде случаев, особенно когда изменения вносятся в существующие системы, некоторые требования могут выдвигаться в форме специфических средств обеспечения безопасности, которые должны быть использованы.

В архитектуре безопасности информационных технологий делается особый упор на технические меры защиты по обеспечению безопасности и на то, как с их помощью будут решаться задачи по достижению целей безопасности; при этом следует принимать во внимание и соответствующие нетехнические средства обеспечения безопасности. Несмотря на то, что данная архитектура может быть построена на основе использования ряда различных подходов и перспектив, следует всегда учитывать один фундаментальный принцип ее построения. Нельзя допускать, чтобы проблема обеспечения безопасности в пределах одной области безопасности (зоны с одинаковыми

или схожими требованиями к обеспечению безопасности и к средствам ее защиты) оказывала неблагоприятное воздействие на обеспечение безопасности в другой отдельной области безопасности. Архитектура безопасности информационных технологий обычно включает одну или более областей безопасности. Области безопасности должны следовать за областями деловой деятельности, установленными и используемыми организациями, настолько близко, насколько это практически целесообразно. Эти области деловой деятельности могут следовать за функциональными секторами отдельных видов деловой деятельности, таких как выплата заработной платы, производство продукции или обслуживание покупателей, или же они могут следовать за функциональными секторами таких видов деятельности, как обслуживание электронной почты или выполнение конторских операций.

Области безопасности могут подразделяться в зависимости от наличия одного или нескольких признаков, к числу которых относятся:

– уровни, категории или виды информации, доступные в пределах области;

– операции, которые могут проходить в области;

– объединения по интересам, ассоциируемые с областью;

– отношения к другим областям и средам;

– виды функций или доступ к информации, которые могут запрашивать объединения по интересам внутри области.

При построении архитектуры обеспечения безопасности информационных технологий необходимо учитывать следующие проблемы:

– взаимоотношения и взаимозависимости между отдельными областями безопасности;

– воздействие данных взаимоотношений и взаимосвязей на ослабление защитных механизмов;

– необходимость в дополнительных сервисах и мерах предосторожности для корректировки, управления или противодействия любым послаблениям в защите.

Архитектура безопасности информационных технологий не существует сама по себе, скорее, она опирается на содержание других документов и согласовывается с ними. Наиболее важными из этих документов являются архитектура системы и архитектуры других соответствующих систем, таких как аппаратные средства, средства связи и прикладные программы. Архитектура безопасности информационных технологий не должна содержать полного описания системы, она имеет дело только с техническими вопросами и элементами, касающимися обеспечения безопасности. Назначение этой структуры состоит в том, чтобы свести к минимуму случаи неблагоприятного воздействия на пользователей, обеспечивая при этом оптимальную внутреннюю защиту инфраструктуры.

Ряд других документов имеет отношение к архитектуре безопасности информационных технологий или может находиться в подчиненном положении по отношению к ним. К их числу относятся:

– проект безопасности информационных технологий;

– рабочая концепция безопасности информационных технологий;

– план защиты информационных технологий;

– политика безопасности системы ИТ;

– документация по сертификации и аккредитации системы информационных технологий (в случае необходимости).

7.4.3 Выявление/рассмотрение ограничений

Существует много ограничений, которые могут влиять на выбор мер защиты. Эти ограничения необходимо принимать во внимание при составлении рекомендаций и в ходе их реализации. К типичным ограничениям относятся:

Временные ограничения:

Может существовать множество видов ограничений по времени. Например, мера защиты безопасности должна быть реализована в пределах периода времени, приемлемого для руководства. Другой вид временного ограничения формулируется так: может ли реализация какой-то меры защиты безопасности быть осуществлена в пределах жизненного срока соответствующей системы. Третьим видом временного ограничения может быть длительность периода времени, необходимого руководству для принятия решения о том, стоит ли и дальше подвергать систему угроз из-за наличия конкретного риска.

Финансовые ограничения:

Стоимость реализации рекомендуемых мер защиты не должна превышать ценности ресурсов, для безопасности которых они предназначены. Необходимо сделать все возможное, чтобы не выйти за пределы выделенных ассигнований. Однако в ряде случаев достижение необходимого уровня безопасности и приемлемого уровня риска может оказаться невозможным в пределах подобных финансовых ограничений. В таком случае поиски выхода из сложившейся ситуации предоставляются на усмотрение руководства.

Технические ограничения:

Технические проблемы, такие как совместимость программ или аппаратных средств, могут быть легко разрешимы, 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 может привести к сдвигу направленности защитных мер в сторону организационных и физических способов защиты.

Социологические ограничения:

Социологические ограничения при выборе защитных мер могут иметь свои особенности в зависимости 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 персоналом организации. Если сотрудники не понимают необходимости таких мер или же не считают их приемлемыми по моральным соображениям, то существует большая вероятность того, что со временем эффективность защитных мер будет падать.

Ограничения окружающей среды:

На выбор защитных мер могут влиять и экологические факторы, такие как величина рабочих площадей, экстремальные природные условия, состояние окружающей природы и прилегающих городских территорий и т.д.

Правовые ограничения:

Правовые ограничения – такие как положения закона о защите личной информации или уголовного кодекса, касающиеся обработки информации, - также могут влиять на выбор мер защиты. Законы и нормативы, не имеющие прямого отношения к защите информационных технологий, такие как требования противопожарной безопасности и трудового законодательства, могут также влиять на выбор мер защиты.

7.5 Приемлемость рисков

После выбора мер защиты и определения величины снижения уровня рисков, которое даст применение указанных мер, всегда будут иметь место остаточные риски, поскольку никакую систему нельзя сделать абсолютно безопасной. Эти остаточные риски должны расцениваться организацией как приемлемые или неприемлемые. Такая классификация может быть осуществлена путем рассмотрения потенциальных неблагоприятных угроз на сферу бизнеса, которые могут быть вызваны данными рисками. Очевидно, что существование неприемлемых рисков нельзя допускать без дальнейшего обсуждения. Необходимо управленческое решение о том, можно ли допустить эти риска в связи с имеющимися ограничениями (например, по затратам средств или просто из-за невозможности их предотвращения – речь идет, например, о падении самолетов на здания или о землетрясениях; тем не менее, планы восстановительных работ на случай подобных катастроф могут быть подготовлены) или необходимо предусмотреть дополнительные и, возможно, дорогостоящие меры защиты для снижения уровня неприемлемых рисков.

7.6 Политика безопасности систем(ы) ИТ

В документе, отражающем политику безопасности систем(ы) информационных технологий, должно содержаться подробное описание применяемых мер защиты с обоснованием их необходимости. Использование указанных мер защиты должно быть расписано в плане защиты ИТ.

Многие системы нуждаются в собственной политике безопасности на основе рассмотрения результатов анализа рисков. Обычно это справедливо по отношению к крупным и сложным системам. Политика безопасности систем(ы) ИТ должна быть совместимой с политикой безопасности информационных технологий – не следует допускать никаких разногласий между ними. Она должна быть направлена на вопросы более низкого уровня, чем политика безопасности информационных технологий. Политика безопасности систем ИТ базируется на результатах анализа рисков и определении мер защиты для данной системы и поддерживается рядом мер защиты, выбранных в соответствии с оцененными рисками. Указанные меры защиты должны обеспечивать достижение требуемого уровня безопасности защищаемой системы.

Политика безопасности систем ИТ должна основываться на нижеследующих данных, независимо от применяемой стратегии анализа корпоративного риска, а также должна определять меры защиты (в том числе и методы), необходимые для достижения потребного уровня безопасности рассматриваемой системы. Политика безопасности систем ИТ и вся относящаяся к ней вспомогательная документация должны освещать следующие вопросы:

– определение системы информационных технологий, описание ее компонентов и границ (это описание должно охватывать все аппаратное, программное обеспечение, весь персонал, окружающую среду, а также все виды деятельности, то есть все то, что в своей совокупности образует данную систему);

– определение целей бизнеса, которые должны быть достигнуты с помощью данной системы информационных технологий - это может оказать влияние на политику безопасности информационных технологий применительно к данной системе, на выбранный подход к анализу рисков, а также на выбор и приоритетность осуществления мер защиты;

– определение целей по безопасности системы;

– определение степени общей зависимости от системы информационных технологий, то есть, насколько бизнес организации может пострадать вследствие потери или раскрытия системы информационных технологий, задачи, которые должна выполнять данная система информационных технологий и характер обрабатываемой информации;

– определение уровня капиталовложений в информационные технологии, как стоимости разработки, поддержания в рабочем состоянии и замены данной системы информационных технологий, включая сюда расходы на приобретение, эксплуатацию и замену помещения;

– определение подхода к анализу рисков, выбранных для данной системы информационных технологий;

– определение ресурсов системы информационных технологий, защиту которых желает обеспечить данная организация;

– оценка указанных ресурсов, определяющая, что произошло бы с организацией в том случае, если бы эти ресурсы были раскрыты (стоимость хранящейся информации должна быть описана на основе возможного негативного воздействия на бизнес организации в случае раскрытия, изменения, исчезновения или уничтожения этой информации);

– оценка угроз для системы информационных технологий и хранящейся информации, включая зависимость между характеристиками ресурсов, угрозами и вероятностью реализации этих угроз;

– оценки уязвимости системы информационных технологий, включая описание ее характерных слабых мест в защите, которые могут быть использованы при реализации угроз;

– риски для безопасности данной системы информационных технологий, возникающие в следствие:

– возможных негативных воздействий на бизнес организации;

– наличия вероятности реализации этих угроз;

– легкости реализации угроз уязвимостей;

– перечень средств безопасности, выбранных для обеспечения безопасности данной системы информационных технологий;

– оценка стоимости защитных мер информационных технологий.

Если доказано, что система требует лишь базисной защиты, все равно можно дать сведения по вышеперечисленным позициям, даже если в некоторых случаях они будут менее подробными, чем для систем, по которым был проведен детальный анализ рисков.

7.7 План защиты информационных технологий

План защиты информационных технологий представляет собой координационный документ, определяющий меры, которые необходимо принять для того, чтобы обеспечить потребную безопасность системы информационных технологий. В этом плане должны быть отражены результаты вышеописанного рассмотрения и перечислены краткосрочные, среднесрочные и долгосрочные мероприятия, направленные на достижение и поддержание необходимого уровня безопасности, с указанием стоимости этих мероприятий и графика их осуществления. План по каждой системе должен включать:

– цели по безопасности с точки зрения обеспечения конфиденциальности, целостности, доступности, подотчетности, подлинности и надежности;

– вариант анализа рисков, выбранный для данной системы информационных технологий (см. раздел 6);

– оценку ожидаемых и приемлемых остаточных рисков, которые будут существовать после осуществления намеченных мер защиты (см. 7.5);

– перечень выбранных для применения мер защиты (см. 7.4), а также перечень существующих и планируемых мер защиты, включая определение их эффективности и указание потребностей в их совершенствовании (см. 7.3.6 и 7.4); данный перечень должен включать:

– установленную последовательность осуществления выбранных мер защиты и совершенствования существующих мер защиты;

– описание практического применения этих мер защиты;

– оценку стоимости установки и эксплуатации, указанных мер защиты;

– оценку потребностей в персонале, необходимом для эксплуатации и контроля при их осуществлении указанных мер защиты;

– подробный рабочий план реализации указанных мер защиты, содержащий:

– последовательность выполнения конкретных операций;

– график работ, соответствующий установленной последовательности выполнения операций;

– указание суммы потребных 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 действия этих мер;

– график процессов рассмотрения для тех случаев, когда это необходимо;

– график процедур по контролю сроков исполнения.

Кроме того, план защиты информационных технологий должен содержать описание средств контроля правильности процесса осуществления указанных мер защиты, например:

– методов представления сообщений о состоянии работ;

– методов выявления возможных трудностей;

– методов оценки по каждой из вышеперечисленных позиций, включая методы, связанные с возможными изменениями отдельных частей плана, если в этом возникнет необходимость.

Результатом данного этапа должен стать план защиты информационных технологий для каждой системы, основанный на политике безопасности систем(ы) ИТ с учетом результатов анализа, описанного в разделе 7. Он должен обеспечить своевременное введение указанных мер защиты в соответствие

с приоритетами, определенными на основе рисков для системы информационных технологий, а также в соответствии с описанием методов осуществления указанных мер защиты и обеспечения необходимого уровня безопасности. Данный план, кроме того, должен содержать график методов контроля поддерживаемого уровня безопасности. Подробное описание этих процедур приводится в разделе 9

8 Выполнение плана защиты информационных технологий

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

8.1 Осуществление мер защиты

Для осуществления мер защиты необходимо выполнить все пункты плана защиты ИТ. Лицо, ответственное за этот план (обычно это служащий из руководящего состава, ответственный за безопасность), должно обеспечить, чтобы приоритетные и основные пункты плана защиты ИТ были отслежены.

Документация по мерам защиты является важной частью документации по информационной безопасности, гарантирующей непрерывность и последовательность действий. Поддержание непрерывности и последовательности может быть выполнено различными способами. Документация по мерам защиты может быть составной частью ряда документов по безопасности, например, плана защиты ИТ, плана обеспечения непрерывной работы и восстановления, документов с анализом рисков, документов с описанием стратегии и методов обеспечения безопасности. Она должна быть разработана с учетом потребностей менеджеров, пользователей, администраторов систем, обслуживающего персонала и всех тех, кто участвует в контроле изменений и конфигурации систем. Документация должна быть обновленной и достаточно подробной, чтобы исключить погрешности и оплошности в обеспечении безопасности систем и в то же время предоставлять информацию, которая будет гарантировать правильность и эффективность действий по безопасности. Часть документов, особенно тех, которые касаются угроз, уязвимостей и рисков, может иметь конфиденциальные данные и должна быть защищена от несанкционированного раскрытия. В результате, большинство организаций будет обращаться с этой документацией очень осторожно и может использовать "доверительные" методы распределения.

Если подобные методы используются, они должны быть составлены так, чтобы в них описывалось, как конфиденциальная информация по мерам

защиты будет храниться, использоваться, и каким образом будет обеспечиваться доступ к ней. Кроме того, эти методы должны определять, кто отвечает за хранение информации по мерам защиты, кто будет иметь к ней доступ и использовать её. При разработке методов распределения информации и назначении доступа к ней необходимо учитывать ряд специальных факторов, таких как необходимость обеспечения непрерывной работы организации и восстановления производственной деятельности после нештатных/аварийных ситуаций, стратегию и план действий в случае бедствия или другого непредвиденного события, для которых время является критичным фактором. Наконец, необходим строгий контроль за системой документации по мерам защиты, чтобы не допустить несанкционированных изменений, способных неумышленно уменьшить эффективность мер защиты.

Как только план защиты ИТ закончен и расписан по ответственным лицам, должны быть внедрены меры защиты, проверена и испытана их сочетаемость с безопасностью. Проверка сочетаемости с безопасностью проводится с целью подтверждения, что меры защиты внедрены корректно, соответственно испытаны и эффективно используются. Может быть проведена оценка безопасности как часть этой проверки. Тестирование является важным способом гарантии корректности внедренных мер по защите. Оценка безопасности должна проводиться в соответствии с планом проверки обеспечения безопасности, который описывает подход к тестированию, график 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 состоит в том, чтобы внедрить и проверить меры защиты таким методом, который бы гарантировал выполнение плана защиты ИТ с учетом уменьшения риска до требуемого уровня.

8.2 Компетентность по вопросам безопасности

Цель программы обеспечения компетентности по вопросам безопасности состоит в том, чтобы повысить знания сотрудников до уровня, когда безопасность становится "вторым я", процессы её обеспечения становятся регулярными и все сотрудники их легко выполняют. Программа должна гарантировать, чтобы персонал и конечные пользователи имели достаточно знаний об информационной системе (аппаратных средствах и программном обеспечении) и чтобы они понимали, почему необходимы меры защиты и как ими правильно пользоваться. Эффективно работать могут только те меры защиты, которые хорошо освоены персоналом и конечными пользователями.

Данные для программы обеспечения компетентности по вопросам безопасности должны поступать от всех подразделений организации. Они должны включать вопросы общей стратегии организации по информационной

безопасности и охватывать все задачи плана защиты ИТ организации. Группе, занимающейся программой обеспечения компетентности по вопросам безопасности, необходима административная поддержка от всех отделов. Программа обеспечения компетентности по вопросам безопасности должна затрагивать следующие темы в форме курсов, обсуждений или других видов общения в целях повышения эффективности действия этих мер:

– объяснение значения информационной безопасности для организации и сотрудников;

– цели и задачи системы обеспечения информационной безопасности в смысле сохранения её конфиденциальности, целостности, доступности, подлинности, и надежности;

– последствия от случаев нарушения информационной безопасности как для организации, так и для сотрудников;

– важность корректного использования информационных систем, включая аппаратные средства и программное обеспечение;

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

– необходимая защита информационных систем от рисков;

– ограничение доступа в информационную среду (авторизованный персонал, блокировка дверей, знаки идентификации, регистрация посещений) и к информации (логическое управление доступом, права чтения/модификации данных), и почему эти ограничения необходимы;

– необходимость в сообщениях о нарушениях защиты или попытках нарушения;

– методы, обязанности и рабочие задания;

– ограничения в деятельности персонала и конечных пользователей, накладываемые факторами обеспечения безопасности;

– ответственность персонала за нарушение информационной безопасности;

– значение плана защиты ИТ для реализации 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 по вопросам безопасности начинается с анализа стратегии безопасности, целей и политики. Этот процесс должен проводиться группой лиц, которые понимают критичные стороны работы организации и имеют полную поддержку главного руководства.

Группа, проводящая такой анализ, должна определить распределение требований в соответствии с общей стратегией информационной безопасно-

сти организации. Эти требования должны учитывать деятельность по обеспечению безопасности в целом (а не только информационной безопасности) и публиковаться в различных формах, в виде плакатов, периодических листков, информационных бюллетеней организации и внутренней почты.

После этого группа должна провести специальные совещания по вопросам безопасности. Необходим глубокий анализ требований для подготовки материалов к совещаниям. Они должны проводиться регулярно (например, каждые шесть месяцев), чтобы обеспечить осведомленность всего персонала с рисками, свойственными современным информационным технологиям.

Ответственность за определение целей и содержания программы обеспечения компетентности по вопросам 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 за безопасность в организации и на группу разработки программы. Это должно быть сделано одновременно с общей деятельностью в организации по вопросам обучения и профессиональной подготовки. Однако, поскольку каждый сотрудник несет ответственность за безопасность и должен быть ознакомлен со стратегией её обеспечения, программа обеспечения компетентности в вопросах безопасности должна быть внедрена на всех уровнях организации.

Комплекс перечисленных далее мероприятий необходим к применению для успешной разработки программы обеспечения компетентности по вопросам безопасности.

8.2.1 Анализ потребности в знаниях

Для определения уровня понимания проблем безопасности уже существующего у разных категорий групп служащих (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 текущим уровнем.

8.2.2 Представление программы

Всесторонняя программа обеспечения компетентности по вопросам безопасности должна включать методы взаимодействия и содействия. Внимание в этой части программы должно быть сосредоточено на недостатках, которые были выявлены на этапе определения потребностей в знаниях. Служащие должны понимать, что информационные ресурсы имеют свою ценность, и угрозы для них являются вполне реальными.

Положительным моментом программы обеспечения компетентности по вопросам безопасности является тот факт, что служащие получают возмож-

ность участвовать в программе обеспечения безопасности. Интерактивные методы (собрания коллектива, курсы обучения и т.д.) позволяют организовать двустороннее взаимодействие между сотрудниками и администраторами безопасности, что позволяет удостовериться в правильности принципов и требований, полученных из анализа потребностей в знаниях. Пропагандистские методы (видеоматериалы, специальные вставки, содержащие сведения по безопасности в электронной почте, плакаты, издания и т.д.) принадлежат к числу односторонних методов, позволяющих экономично осуществлять управление широковещательными процессами, распространением информации и влиять на мнение людей.

8.2.3 Контроль программы обеспечения компетентности в вопросах безопасности

Имеются два компонента, которые обеспечивают эффективный контроль программы обеспечения компетентности по вопросам безопасности:

– периодическая оценка её эффективности, которая определяет эффективность программы, контролируя поведение персонала в ситуациях, связанных с безопасностью, и выявляя места, где требуются изменения в формах представления программы;

– контроль за изменениями в программе, когда производятся изменения в общей программе обеспечения безопасности (изменяется стратегия или политика безопасности, появляются новые ресурсы или технологии, изменяется характер угроз для информации и т.п.), появляется необходимость изменить и программу обеспечения компетентности по вопросам безопасности, чтобы обновить знания и квалификацию персонала и отразить эти изменения.

8.3 Обучение персонала информационной безопасности

Помимо общей программы обеспечения компетентности по вопросам безопасности, которая относится к каждому служащему организации, для работающего персонала необходимо специальное обучение, связанное с задачами и обязанностями, по обеспечению информационной безопасности. Глубина этого обучения зависит от уровня важности информационной безопасности для организации и должна варьироваться согласно требованиям безопасности к выполняемой работе. В случае необходимости, не исключено серьезное обучение на уровне университетских лекций, специальных курсов и т.д. Программа обучения персонала информационной безопасности должна быть разработана так, чтобы охватить все потребности в мерах защиты, относящихся к организации.

В список сотрудников, для которых необходимо специальное обучение информационной безопасности, следует включить:

– сотрудников, играющих ключевые роли в разработке информационной системы;

– сотрудников, играющих ключевые роли в эксплуатации информационной системы;

– должностных лиц организации, руководящих разработкой проекта информационной системы и программы обеспечения её безопасности;

– сотрудников, несущих административную ответственность за безопасность, например, контролирующих доступ или управляющих директориями.

Проверка необходимости специального обучения информационной безопасности должна быть сделана 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.

Тематика курсов обучения информационной безопасности должна соответствовать функциям и квалификационным обязанностям обучаемых сотрудников. Общие темы могли бы включать следующее:

– определение понятия "безопасность";

– предотвращение нарушений конфиденциальности, целостности и доступности;

– потенциальные угрозы, которые могут оказать неблагоприятное воздействие на производственную деятельность организации и сотрудников;

– схема классификации информации, требующей обеспечение безопасности;

– процесс обеспечения общей безопасности;

– описание процесса обеспечения общей безопасности;

– компоненты анализа риска;

– меры защиты, и обучение приемам их применения;

– роли и обязанности сотрудников;

– политика безопасности систем(ы) ИТ.

Правильное выполнение и использование мер защиты является одним из наиболее важных аспектов, который должен быть охвачен программой обучения информационной безопасности. Каждая организация должна разработать собственную программу обучения информационной безопасности согласно её потребностям и существующим или запланированным мерам защиты. Ниже приведены примеры тематики, связанной с применением мер защиты, в которых сбалансированы технические и организационные аспекты безопасности:

– инфраструктура системы безопасности:

– роли и обязанности;

– корпоративная политика безопасности;

– регулярная проверка согласованности мер защиты;
– обработка случаев нарушения безопасности;
– безопасность на физическом уровне:
– здания;
– офисные и компьютерные помещения и комнаты;
– оборудование;
– безопасность на уровне управления персоналом;
– безопасность носителей;
– безопасность аппаратных средств / программного обеспечения:
– идентификация и аутентификация;
– логический контроль доступа;
– учет и аудит безопасности;
– очистка носителей данных;
– безопасность средств связи и передачи данных:
– сетевая инфраструктура;
– каналы, маршрутизаторы, шлюзы, межсетевые экраны;
– Интернет и другие внешние связи;
– обеспечение непрерывности работы организация и восстановления после нештатных/аварийных ситуаций, включая соответствующие стратегии и план(ы).

8.4 Процесс рассмотрения информационных систем

Организации должны обеспечить рассмотрение всех или предпочтительных информационных систем на предмет их соответствия требованиям политики безопасности систем(ы) ИТ и плану ее обеспечения. Процесс рассмотрения должен быть основан на таких методах, как проверка согласованности мер защиты, тестирование мер защиты и/или оценка системы. Процедуры рассмотрения могут производиться согласно внутренним или внешним стандартам, а орган, выполняющий утверждение, может быть внутри или вне организации.

Процесс рассмотрения должен быть направлен на то, чтобы внедренные меры защиты обеспечивали необходимый уровень безопасности информации. Утверждение должно иметь силу для определенной операционной среды и в течение определенного периода времени, оговоренных в политике безопасности систем(ы) ИТ, либо в соответствующем ей плане защиты. Любые значительные изменения в мерах защиты или изменения в инструкциях, влияющие на безопасность, могут потребовать нового рассмотрения. Критерии, на основании которых делается новое утверждение, должны быть включены в политику безопасности системы ИТ.

Процесс рассмотрения состоит, главным образом, из анализа документов, технических осмотров и оценок (например, проверка согласованности

мер защиты). Для выполнения этого необходимо руководствоваться следующими положениями:

– процесс рассмотрения должен планироваться и приспосабливаться к конкретным информационным системам; этот первый шаг помогает также определить график, необходимые ресурсы и обязанности;

– должны быть собраны документы, используемые в этом процессе;

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

– должен быть закончен анализ и тестирование по критериям, описанным в плане защиты ИТ;

– итоги процесса рассмотрения 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 утверждение необходимо, если информационная система или ее среда претерпели изменения; а также в конце срока действия предыдущего рассмотрения.

После окончания процесса рассмотрения, сразу начинаются процедуры сопровождения за информационной системой. Сопровождение помогает обнаружить и проанализировать изменения в системе, ее защите и среде. При обнаружении изменений в системе необходимо её обновление с последующим новым рассмотрением и утверждением.

Необходимость рассмотрения систем коммерческого партнера определяется базисным уровнем безопасности и нормами, действующими в организации, которая:

– желает устанавливать собственную версию базисного уровня защиты или свои нормы и передать их партнерам/поставщикам для согласования и рассмотрения до подключения к своим ресурсам;

– ведет торговлю с рядом других компаний и желает быть связанной с ними информационно, и, чтобы сделать это, ей необходимо продемонстрировать свой уровень безопасности с позиций базисного уровня и общих норм по безопасности;

– желает установить уровни рисков нарушений информационной безопасности для других информационно подсоединенных компаний, которые эти компании должны соблюдать. Это даст возможность организации заставить партнеров проводить рассмотрения своих систем на основании проверки согласованности мер защиты, которые будут указывать на степень соответствия этих мер тем частям базисного уровня и норм безопасности, которые совместимы с принятыми требованиями по безопасности в организации.

9 Последующее наблюдение за системой

Последующее наблюдение за системой, несмотря на то, что им часто пренебрегают, является одним из наиболее важных аспектов обеспечения информационной безопасности. Внедренные меры защиты могут быть эффективны, когда они проверяются в реальном производственном процессе. Необходима уверенность, что они используются правильно, что любые изменения и нарушения безопасности обнаруживаются с принятием мер. Главная цель последующего наблюдения состоит в том, чтобы гарантировать, что меры защиты системы продолжают функционировать, как было назначено при их планировании. С течением времени каждый механизм или сервис имеют тенденцию к ухудшению в работе. Последующее наблюдение должно обнаружить это ухудшение и определять корректирующие действия. Это единственный способ поддержать уровень безопасности, необходимый для защиты системы. Процедуры, описанные в этом разделе, представляют собой основу эффективной программы последующего наблюдения. Управление информационной безопасностью является непрерывным процессом, который не останавливается после выполнения плана её обеспечения.

9.1 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. Это сведет к минимуму накладные расходы, связанные с ними, и сохранит эффективность мер защиты.

Для обнаружения сбоев необходим периодический осмотр. Бесконтрольная мера защиты не представляет ценности, так как нельзя определить, на каком уровне можно на нее положиться.

Обслуживание включает:

– проверку журналов регистрации событий;

– корректировку параметров, отражающих изменения и добавления в систему;

– периодическую инициализацию значений начальных чисел и счетчиков;

– обновление версий.

Затраты на обслуживание и администрирование должны всегда разделяться при оценке и выборе различных мер защиты. Так как стоимость обслуживания и администрирования могут значительно отличиться для различных мер защиты. Поэтому этот критерий может быть определяющим фактором при выборе мер защиты. В общем случае, желательно сводить к минимуму расходы на обслуживание и администрирование везде, где воз-

можно, поскольку они представляют периодические издержки, а не одноразовые затраты.

9.2 Проверка соответствия безопасности

Проверка соответствия безопасности представляет собой обзор и анализ осуществленных мер защиты. Она используется для того, чтобы контролировать соответствие информационной системы или сервиса требованиям, указанным в политике безопасности систем(ы) ИТ принятой организацией, и в соответствующем плане защиты систем(ы) ИТ. Проверки уровня безопасности могут использоваться для контроля в следующих ситуациях:

– внедрены новые информационные системы и сервисы;

– наступило время периодической (например, годовой) проверки существующих систем или сервисов;

– внесены изменения в политику безопасности систем(ы) ИТ, 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 политики безопасности систем(ы) ИТ.

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 закрытых областях деятельности организации или в местах, вызывающих беспокойство.

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

– использования пакетов программ, регистрирующих события;

– использования контрольных журналов с полной записью событий.

Проверка уровня безопасности, проводимая в процессе рассмотрения и при дальнейших регулярных проверках, должна базироваться на согласованных перечнях мер защиты по результатам последнего анализа рисков, на политике безопасности систем(ы) ИТ, принятой в организации, а также в инструкциях по информационной безопасности, принятых руководством, включая правила сообщения об инцидентах. Цели проверок состоят в том, чтобы убедиться, что меры защиты внедрены, внедрены корректно, используются правильно и, где необходимо, тестированы.

Контролер/инспектор по проверке уровня безопасности должен проходить по помещениям в обычный рабочий день и смотреть, как выполняются меры защиты. Интервью, конечно, важны, но результаты разговоров должны

быть, по возможности, перепроверены. Люди обычно говорят то, чему верят, а не то, что есть на самом деле, поэтому необходимы перепроверки с другими людьми, работающими вместе.

Большое значение 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 по обеспечению информационной безопасности, документы, определяющие политику организации, окружающую обстановку. Физическая безопасность должна касаться как внешних аспектов, например, окружающей обстановки вокруг здания, возможности проникновения через крышки люков, так и внутренних аспектов, например, прочности конструкции здания, замков, системы пожарной сигнализации и защиты, системы сигнализации при затоплении водой/жидкостью, отказов в энергоснабжении и т.д.

Существует множество мест, требующих своевременного выявления:

– места, доступные для физического проникновения или охраняемые по периметру; например, заклиненные двери, которые открываются карточками или наборным шифром;

– неправильно работающие механизмы или неправильно установленные механизмы, например, отсутствие, неполное распределение по контролируемой зоне или неправильный выбор типа детекторных устройств. Достаточно ли детекторов дыма/температуры для данной площади, 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 использует ли кто-то помещение для хранения легковоспламеняющихся веществ? Имеются ли адекватный запасной источник электропитания, и предусмотрены ли процедуры его включения? Правильно ли выбраны типы кабелей, не проходят ли они около острых кромок?

Ответы на следующие вопросы могут быть использованы для определения слабых мест в защите по остальным направлениям:

– **для безопасности на уровне управления персоналом**: необходимо следить за процедурами приема на службу. Действительны ли рекомендации? Проверены ли перерывы в трудовой деятельности? Имеет ли персонал представление о безопасности? Имеется ли зависимость ключевых функций от одного человека?

– **для безопасности на организационном уровне:** как распределяются документы? Является ли документация общего пользования обновленной? Правильно ли используются процедуры по анализу риска, проверке состояния и регистрации инцидентов? Является ли план обеспечения непрерывности работы и восстановления корректным и действующим ?

– **для безопасности аппаратных средств/программного обеспечения**: находится ли резервное копирование на достаточном уровне? Насколько хо-

роши процедуры выбора идентификатора/пароля пользователей? Содержат ли контрольные журналы регистрацию ошибок и их прослеживание с достаточной детальностью и отбором? Соответствует ли проверенная программа согласованным требованиям?

– **для безопасности средств связи и передачи данных***:* обеспечена ли требуемая степень дублирования? При наборе телефонного номера с клавиатуры ЭВМ, имеется ли необходимое оборудование и программное обеспечение и правильно ли оно используется? Если требуется шифрование и/или аутентификация сообщения, насколько эффективна система управления ключами и связанные с этим операции?

Итак, проверка уровня безопасности – важная задача и требует достаточного опыта и знаний для успешного выполнения. Это отдельный вид деятельности и отличается от внутреннего аудита в организации.

9.3 Управление изменениями

Информационные системы и окружающая среда, в которой они функционируют, постоянно изменяются. Эти изменения есть результат появления новых качеств и сервисов или обнаружения новых угроз и уязвимостей. Эти изменения могут также приводить к новым угрозам и образованию новых уязвимостей. Изменения информационной системы включают:

– новые процедуры;

– новые качества;

– обновленные программы;

– пересмотр аппаратной среды;

– новые потребители, включая внешние организации или анонимных пользователей;

– дополнительные сети и взаимосвязь.

Когда происходят или планируются изменения в информационной системе, важно определить, как это повлияет (если повлияет вообще) на информационную безопасность системы. Если система имеет службу управления конфигурацией или другую организационную структуру, управляющую техническими системными изменениями, то в этот орган должны быть включены ответственное лицо по безопасности или его представитель с полномочиями определять влияние любого изменения на информационную безопасность. При больших изменениях, включающих покупку новых аппаратных средств, программного обеспечения или в составе сервиса, необходимо провести повторный анализ требований безопасности. С другой стороны, при незначительных изменениях в системе всесторонний анализ не требуется, но все-таки какой-то пересмотр необходим. В обоих случаях следует оценить преимущества и расходы, связанные с изменениями. Для незначительных

изменений это может быть выполнено неофициально на совещании, но результат и решения должны быть документированы.

9.4 Мониторинг

Мониторинг – это продолжение действий, направленных на проверку соответствия системы, ее пользователей и среды уровню безопасности, предусмотренному планом защиты ИТ, принятым в организации. Необходимы также повседневные планы контроля с дополнительными рекомендациями и процедурами для обеспечения безопасной работы системы. Необходимы периодические консультации с пользователями, рабочим персоналом и разработчиками систем, чтобы гарантировать, что все аспекты безопасности полностью отслежены и план защиты ИТ соответствует текущему состоянию дел.

Одна из причин, определяющих важность контроля для информационной безопасности, заключается в том, что он позволяет выявить изменения, влияющие на безопасность. Некоторые аспекты, которые должны находиться под контролем включают ресурсы и их стоимость, угрозы ресурсам и их уязвимость, меры защиты ресурсов.

Ресурсы контролируются для определения изменений в их ценности и для обнаружения изменений в требованиях информационной безопасности систем. Возможными причинами этих изменений могут быть отклонения в:

– производственных целях организации;

– программных приложениях, работающих в информационной системе;

– информации, обрабатываемой информационной системой;

– аппаратном обеспечении информационной системы.

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

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

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

При обнаружении отклонений в безопасности необходимо их исследовать и результаты доложить руководству для возможного пересмотра мер

защиты или в серьезных случаях пересмотра политики безопасности систем(ы) ИТ и проведения нового анализа рисков.

Для обеспечения требований политики безопасности систем(ы) ИТ, должны быть привлечены соответствующие ресурсы для поддержания необходимого уровня повседневного контроля следующих элементов:

– существующих мер защиты;

– ввода новых систем или сервисов;

– планирования изменений в существующих системах или сервисах.

Выходные данные защитных мер фиксируются в журналах регистрации событий. Эти журналы должны быть проанализированы с использованием статистических методов, для раннего обнаружения тенденций к изменениям и определения повторных случаев. Должны быть назначены лица, отвечающие за анализ этих журналов.

В распределенных физических средах журналы регистрации могут фиксировать информацию, относящуюся к одной среде. Чтобы верно понимать природу сложного события, необходимо объединить информацию различных журналов и свести её в одну запись события. Объединение записей журналов представляет сложную задачу и её наиболее важный аспект заключается в идентификации параметра (или параметров), который позволяет (которые позволяют) уверенно объединять записи журналов.

Методы управления повседневным контролем заключаются в подготовке документа, описывающего необходимые действия при выполнении производственных процедур для обеспечения безопасности. Этот документ описывает все действия, необходимые для поддержания требуемого уровня безопасности для всех систем и сервисов и для подтверждения его сохранения с течением времени.

Процедуры для обновления конфигурации системы безопасности должны быть документированы. Они должны включать корректируемые параметры безопасности и обновления любой информации по управлению безопасностью. Эти изменения должны быть зарегистрированы и подтверждены процессом управления конфигурацией системы. Необходимо установить процедуры выполнения регулярного обслуживания, чтобы гарантировать, что безопасность информации не поставлена под угрозу. Процедуры доверия поставки должны быть описаны для каждого компонента безопасности, где это применимо.

Необходимо иметь описание процедуры для 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, описывающее порядок корректировки критериев контрольных проверок для различных производственных условий.

9.5 Обработка инцидентов

Как уже подчеркивалось, 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), связанных с нарушением информационной безопасности, для поддержания процесса анализа рисков и управления другими аспектами деятельности организации, связанными с безопасностью.

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

– улучшения анализа риска и управления пересмотром;

– предотвращения инцидентов;

– повышения уровня компетентности по вопросам информационной безопасности;

– получения "предупреждения" для использования командой реагирования на непредвиденные случаи с компьютерами.

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

– заранее составленный план 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;

– обучение выделенных сотрудников методам расследования инцидентов, например, организация группы аварийного компьютерного обеспечения.

Группа аварийного компьютерного обеспечения – это формально выделенная часть сотрудников, которая занимается расследованием причины инцидента, связанного с нарушением информационной безопасности, определяет потенциальную возможность его повторения или проводит периодический анализ данных за длительный период времени. Заключения, сделанные группой, могут служить основанием для превентивных действий. Команда реагирования на непредвиденные случаи с компьютерами может быть создана внутри организации или нанята по контракту со стороны.

При наличии планов 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 более ценных ресурсов, что позволит уменьшить расходы на сам инцидент и на устранение его последствий. Также не желательны любые отрицательные публикации.

Каждая организация должна иметь эффективную процедуру обработки инцидентов, охватывающую:

– подготовку – заранее разработанные превентивные меры, руководства и процедуры по обработке инцидентов (включая сохранение доказательных данных, журналы регистрации событий и связь с общественностью), необходимую документацию, планы обеспечения непрерывной работы и восстановления;

– уведомление – процедуры, средства и обязанности по передаче информации об инцидентах;

– оценка – 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;

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

Следует подчеркнуть, что, если одни организации видят выгоду от использования процедуры обработки инцидентов, другие организации считают, что ещё большую выгоду можно получить, объединяя эту информацию и создавая общую базу данных по инцидентам, что позволит получать предупреждения, идентифицировать тенденции и принимать меры защиты гораздо быстрее. Объединенная база данных по инцидентам должна быть достаточно гибкой, чтобы учитывать требования общих (все секторы, все типы угроз и их возможные последствия) и частных (отдельные секторы, опасности и их последствия) интересов. Каждая процедура обработки инцидентов, внутри или вне организации, должна использовать одинаковую типологию, метрику и структуру программного обеспечения для регистрации информации по инцидентам. Это облегчило бы сравнение и анализ. Использование общей структуры является ключевым моментом для получения всеобъемлющих результатов и особенно более достоверной базы данных для быстрой идентификации такого "предупреждения", которое невозможно получить от одиночной процедуры обработки инцидентов.

Как указывалось выше, достижение взаимосвязи между процедурой обработки инцидентов, процессом анализа рисков и методами управления может существенно улучшать результаты и увеличить выгоду от использования процедуры обработки инцидентов.

Информация по случаям возникновения угроз значительно поможет улучшению мер борьбы с ними, и, таким образом, улучшит качество оценки рисков. В процессе расследования инцидента или инцидентов вполне вероятно, что будет собрана новая и дополнительная информация в отношении уязвимостей систем и способов, которыми их можно устранить. Применение процедуры обработки инцидентов дает возможность пользователю определить и оценить уязвимости системы, и таким образом, дать ценные начальные данные для оценки рисков. Эти данные будут частично основаны на информации об опасностях и частично на результатах расследования инцидентов, проведенного командой реагирования на непредвиденные случаи с компьютерами. Например, опасность логического проникновения (присутствие "взломщика" и привлекательность обрабатываемой информации) может сочетаться с уязвимостью к логическому проникновению (неадекватность или отсутствие соответствующих контрольных механизмов логического доступа в систему), чем создается риск. Поэтому использование процедуры обработки инцидентов для идентификации и оценки уязвимостей может происходить через информацию об опасностях, которая введена в базу данных о случившихся инцидентах, совместно с информацией от других источников, особенно командой реагирования на непредвиденные случаи с компьютерами, которые могут обнаружить ранее неидентифицированные уязвимости.

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

10 Резюме

В настоящем стандарте рассмотрено несколько методов, которые являются важными для управления информационной безопасностью. Эти методы основаны на концепциях и моделях, представленных в СТ РК ИСО/МЭК 13335-1-2008 и процессе управления с сопутствующими обязательствами. Обсуждения в настоящем стандарте показывают преимущества и недостатки четырех возможных стратегий анализа риска. Подробно описаны объединенный подход и несколько методов, которые являются полезными для вне-

дрения на практике. Некоторые организации, особенно небольшие, не могут применить все методы, приведенные в настоящем стандарте так, как они описаны. Важно подчеркнуть, что каждый из этих методов должен быть проанализирован и применен в подходящей для организации форме.

Приложение А
(справочное)
Пример перечня вопросов, входящих в состав политики безопасности информационных технологий

Содержание

Приложение Б
(справочное)
Оценка ресурсов

Оценка ресурсов организации является важным шагом в общем процессе анализа риска. Ценность, определенная для каждого ресурса, должна выражаться таким способом, который наилучшим образом соответствует данному ресурсу и данной компании. Чтобы выполнить оценку ресурсов, организация сначала должна инвентаризовать все свои ресурсы. Для обеспечения полного учета ресурсов часто полезно группировать их по типам, например, информационные ресурсы, программное обеспечение, физические ресурсы и услуги. Целесообразно также назначать «владельцев» ресурсов, которые и будут нести ответственность за определение ценности ресурсов.

Следующий шаг - согласование масштабов оценки, которая должна быть произведена, и критериев определения конкретной стоимости ресурсов. Из-за имеющегося в большинстве организаций разнообразия ресурсов, весьма вероятно, что некоторые ресурсы, которые могут быть измерены в денежных единицах, будут оцениваться в местной валюте в то время, как ценность других ресурсов, имеющая, в основном, качественный характер, может оцениваться по качественной шкале в диапазоне от "очень низкой" до "очень высокой". Решение использовать количественную или качественную оценку – это вопрос предпочтения для организации, но при этом выбранный тип оценки должен соответствовать подлежащим оценке ресурсам. Для одного и того же ресурса могут быть использованы также оба типа оценки.

Типичными терминами, используемыми для качественной оценки ценности ресурсов, являются следующие: пренебрежимо малая, очень малая, малая, средняя, высокая, очень высокая и имеющая критичное значение. Выбор и диапазон терминов, которые являются подходящими для данной организации, в значительной степени зависит от потребностей организации в безопасности, крупности этой организации, а также от других факторов, специфичных для данной организации.

Критерии, используемые в качестве основы для назначения ценности каждого ресурса, должны выражаться в однозначных терминах. С этим часто бывают связаны наиболее трудные аспекты оценки ресурсов, поскольку ценность некоторых ресурсов приходится определять субъективно, и поэтому для определения ценности ресурсов целесообразно привлекать достаточно большое количество разных людей. Возможны следующие критерии определения ценности ресурсов: первоначальная стоимость ресурса, стоимость его обновления или воссоздания. Ценность ресурса может также иметь нематериальный характер, например, ценность доброго имени или репутации компании.

Другой подход к оценке ресурсов основывается на затратах, понесенных по причине утраты конфиденциальности, целостности или доступности вследствие происшедшего инцидента. Такая оценка дала бы три важных меры ценности ресурса, в дополнение к стоимости обновления ресурса, основанной на оценках потенциального ущерба или неблагоприятного воздействия на бизнес в результате происшедшего случая 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 в уравнение оценки риска.

Многие ресурсы 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 же он может быть оценен на основе его ценности для конкурента. Вероятность того, что величины этих ценностей будут значительно отличаться

друг от друга, весьма велика. Присвоенная ценность ресурса может быть максимальной из всех возможных ценностей или может являться суммой некоторых или всех возможных ценностей. При окончательном анализе необходимо тщательно определять итоговую величину ценности ресурса, поскольку от нее зависит объем ресурсов, необходимых для обеспечения защиты ресурса.

В конечном счете, все оценки ресурсов должны проводиться на основе общего подхода. Это может быть сделано при помощи таких критериев, которые приведены ниже. Это следующие критерии, которые могут использоваться для того, чтобы оценить возможный ущерб от потери конфиденциальности, целостности или доступности ресурсов:

– 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 возможные примеры критериев могут быть использованы для оценки ресурсов. Для выполнения оценок организация должна выбирать критерии, соответствующие типу ее бизнеса и установленным требованиям по обеспечению безопасности. Поэтому некоторые из вышеперечисленных критериев могут оказаться неприменимыми, тогда как другие критерии могли бы быть добавлены к данному списку.

После выбора подходящих критериев организация должна договориться о шкале оценки, которая будет использоваться во всей организации. Первым шагом здесь должно являться установление числа используемых уровней. Никаких правил для установления наиболее подходящего числа уровней не существует. Большее количество уровней обеспечивает более высокую степень детализации, но иногда слишком тонкое дифференцирование затрудняет оценку ресурсов организации. Обычно число уровней оценки лежит в диапазоне от 3 (например, малая, средняя и высокая ценность) до 10, при условии, что это совместимо с подходом организации к общему процессу оценки риска.

Кроме того, организация может устанавливать свои собственные пределы ценности ресурсов (например, малая, средняя и высокая ценность). 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, денежные единицы окажутся непригодными. В конечном счете, организация сама должна решить, какой ущерб будет считаться 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 В
(справочное)
Перечень возможных типов опасностей

В нижеследующем списке приводятся типичные виды опасностей. Этот список можно использовать в процессе оценки указанных опасностей, которые могут быть вызваны одним или несколькими преднамеренными или случайными событиями, или же событиями, связанными с окружающей средой и имеющими естественное происхождение. В нижеприводимом списке опасности, обусловленные преднамеренными действиями, отмечены буквой D (deliberate, умышленные); опасности, обусловленные случайными действиями, – буквой A (accidental, случайные); и опасности, обусловленные естественными причинами – буквой E (environmental, связанные с окружающей средой). Таким образом, буква D используется для обозначения всех преднамеренных действий, объектами которых являются ресурсы информационных технологий; буква A используется для обозначения всех совершаемых людьми действий, которые могут случайно нанести вред ресурсам информационных технологий; буква E используется для обозначения всех инцидентов, не основанных 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	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
Маскировка злоумышленников под законных 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 маршруту	A
Изменение маршрута передачи сообщений	D
Отказ от совершенных действий	D
Сбои в функционировании сервисов связи и передачи данных (например, сетевых сервисов)	D, A
Недостаточная численность персонала	A
Ошибки пользователей	D, A
Ненадлежащее использование ресурсов	D, A

Приложение Г
(справочное)
Примеры общих уязвимостей

В нижеприведенных списках содержатся примеры уязвимых мест применительно к различным объектам, требующим обеспечения безопасности, а также примеры опасностей, которые могут возникать в данных объектах. Данные списки могут оказаться полезными при оценке уязвимых мест. Следует отметить, что в некоторых случаях данным уязвимым местам могут угрожать другие опасности.

Г.1 Среда и инфраструктура

Отсутствие физической защиты зданий, дверей и окон

– (возможна, например, опасность кражи);

Неправильное или халатное использование физических средств управления доступом в здания, помещения

– (возможна, например, опасность намеренного повреждения) ;

Нестабильная работа электросети

– (возможна, например, опасность колебаний напряжения) ;

Размещение в зонах возможного затопления

– (возможна, например, опасность затопления).

Г.2 Аппаратное обеспечение

Отсутствие схем периодической замены

– (возможна, например, опасность ухудшения состояния запоминающей среды) ;

Подверженность колебаниям напряжения

– (возможна, например, опасность возникновения колебаний напряжения) ;

Подверженность температурным колебаниям

– (возможна, например, опасность возникновения экстремальных величин температуры) ;

Подверженность воздействию влаги, пыли, загрязнения

– (возможна, например, опасность запыления) ;

Чувствительность к воздействию электромагнитного излучения

– (возможна, например, опасность воздействия электромагнитного излучения) ;

Недостаточное обслуживание/неправильная инсталляция запоминающих сред

– (возможна, например, опасность возникновения ошибки при обслуживании) ;

Отсутствие контроля за эффективным изменением конфигурации

– (возможна, например, опасность ошибки операторов) .

Г.3 Программное обеспечение

Неясные или неполные технические требования на разработку средств программного обеспечения

– (возможна, например, опасность программных сбоев) ;

Отсутствие тестирования или недостаточное тестирование программного обеспечения

– (возможна, например, опасность использования программного обеспечения несанкционированными пользователями) ;

Сложный пользовательский интерфейс

– (возможна, например, опасность ошибки операторов) ;

Отсутствие механизмов идентификации и аутентификации, например, аутентификации пользователей

– (возможна, например, опасность маскировки злоумышленников под законных пользователей) ;

Отсутствие аудиторского следа

– (возможна, например, опасность использования программного обеспечения несанкционированным способом) ;

Хорошо известные дефекты программного обеспечения

– (возможна, например, опасность использования программного обеспечения несанкционированными пользователями) ;

Незащищенные таблицы паролей

– (возможна, например, опасность маскировки злоумышленников под законных пользователей) ;

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

– (возможна, например, опасность маскировки злоумышленников под законных пользователей) ;

Неправильное присвоение прав доступа

– (возможна, например, опасность использования программного обеспечения несанкционированным способом) ;

Неконтролируемая загрузка и использование программного обеспечения

– (возможна, например, опасность столкновения с вредоносным программным обеспечением) ;

Отсутствие регистрации конца сеанса при выходе с рабочей станции

– (возможна, например, опасность использования программного обеспечения несанкционированными пользователями) ;

Отсутствие эффективного контроля внесения изменений

– (возможна, например, опасность программных сбоев) ;

Отсутствие документации

– (возможна, например, опасность ошибки операторов) ;

Отсутствие резервных копий

– (возможна, например, опасность воздействия вредоносного программного обеспечения или пожара) ;

Списание или повторное использование запоминающих сред без надлежащего стирания записей

– (возможна, например, опасность использования программного обеспечения несанкционированными пользователями).

Г.4 Средства связи

Незащищенные линии связи

– (возможна, например, опасность перехвата информации) ;

Неудовлетворительная стыковка кабелей

– (возможна, например, опасность несанкционированного подключения к средствам связи) ;

Отсутствие идентификации и аутентификации отправителя и получателя

– (возможна, например, опасность маскировки злоумышленников под законных пользователей) ;

Пересылка паролей открытым текстом

– (возможна, например, опасность доступа несанкционированных пользователей к сети) ;

Отсутствие подтверждений отправки или получения сообщения

– (возможна, например, угроза отказа от совершенных действий) ;

Коммутируемые линии

– (возможна, например, опасность доступа несанкционированных пользователей к сети) ;

Незащищенные потоки конфиденциальной информации

– (возможна, например, опасность перехвата информации) ;

Неадекватное управление сетью (недостаточная гибкость системы маршрутизации)

– (возможна, например, опасность перегрузки трафика) ;

Незащищенные подключения к сетям общего пользования

– (возможна, например, опасность использования программного обеспечения несанкционированными пользователями).

Г.5 Документы

Хранение в незащищенных местах

– (возможна, например, опасность похищения) ;

Недостаточная внимательность при уничтожении

– (возможна, например, опасность похищения) ;

Бесконтрольное копирование

– (возможна, например, опасность похищения).

Г.6 Персонал

Отсутствие персонала

– (возможна, например, опасность недостаточного количества работников) ;

Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц

– (возможна, например, опасность похищения) ;

Недостаточная подготовка персонала по вопросам обеспечения безопасности

– (возможна, например, опасность ошибки операторов) ;

Отсутствие необходимых знаний по вопросам безопасности

– (возможна, например, опасность ошибок пользователей) ;

Неправильное использование программно-аппаратного обеспечения

– (возможна, например, опасность ошибки операторов) ;

Отсутствие механизмов отслеживания

– (возможна, например, опасность использования программного обеспечения несанкционированным способом) ;

Отсутствие политики, регламентирующей правила корректного использования телекоммуникационной среды и средств обмена сообщениями

– (возможна, например, опасность неавторизованного использования возможностей сети)

Несоответствующие процедуры набора кадров

– (возможна, например, опасность намеренного повреждения)

Г.7 Общие уязвимые места

Отказ системы вследствие отказа одного из элементов

– (возможна, например, опасность сбоев в функционировании сервисов связи) ;

Неадекватные результаты проведения технического обслуживания

– (возможна, например, опасность аппаратных отказов) .

Приложение Д
(справочное)
Типология методов анализа риска

Анализ рисков состоит из нескольких этапов, которые обсуждаются в данной части настоящего стандарта, а также в других его частях. Перечислим эти этапы:

– идентификация и оценка ресурсов (оценка возможного негативного воздействия на бизнес);

– оценка опасностей;

– оценка уязвимых мест;

– оценка существующих и планируемых средств защиты;

– оценка риска.

На заключительном этапе должна быть проведена оценка всех рисков, что является основным процессом в данном Приложении. Как было установлено ранее, ресурсы, которые имеют ценность и характеризуются определенной степенью уязвимости, подвергаются риску всякий раз, когда присутствует опасность для них. Оценка рисков представляет собой оценку соотношения потенциальных негативных воздействий на бизнес в случае нежелательных инцидентов и уровня оцененных опасностей и уязвимых мест. Риски фактически являются мерами незащищенности системы и связанной с ней организации. Величина рисков зависит от:

– ценности ресурсов;

– опасностей и связанной с ними вероятности того, что произойдет опасное для ресурсов событие;

– легкости реализации опасностей в уязвимых местах с оказанием нежелательного воздействия;

– существующих или планируемых средств защиты, которые снижают степень уязвимости, опасности и нежелательных воздействий.

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

Воздействие может быть оценено несколькими способами, в том числе количественно, например, в денежных единицах, и качественно (который может быть основан на использовании прилагательных типа умеренное или серьезное), или комбинацией обоих. Чтобы оценивать воздействие необходимо рассчитать вероятность появления угрозы, время ее существования, время сохранения ценности ресурса и целесообразность защиты ресурса. На вероятность появления угрозы оказывают влияние следующие факторы:

1. Привлекательность ресурса - данный фактор применим при рассмотрении опасности намеренного воздействия людей.

2. Легкость использования ресурса для получения материального вознаграждения - данный фактор применим при рассмотрении опасности намеренного воздействия людей.

3. Технические возможности создателя угрозы – данный фактор применим при рассмотрении опасности намеренного воздействия людей.

4. Возможность возникновения опасности.

5. Возможность использования уязвимых мест – применимо к уязвимым местам как технического, так и нетехнического характера.

Во многих методах используются таблицы и различные комбинации субъективных и эмпирических мер. В настоящее время нельзя говорить о правильном или неправильном методе. Более важно, чтобы организация пользовалась тем методом, который удобен для нее, внушает доверие и дает воспроизводимые результаты. Ниже приводится несколько примеров по способам, основанным на применении таблиц.

Пример 1. Матрица с заранее определенными значениями

В методах анализа риска такого типа фактические или предполагаемые физические ресурсы оцениваются на основе стоимости их замены или восстановления (то есть, количественно). Затем эти количественные величины оценки преобразуются в шкалу качественных оценок, такую же, которая используется применительно к ресурсам данных (см. ниже). Фактические или предполагаемые программные ресурсы оцениваются таким же способом, как и физические ресурсы с определением стоимости их покупки или восстановления, а затем эти количественные величины оценки преобразуются в шкалу качественных оценок, такую же, которая используется применительно к ресурсам данных. Кроме того, если выяснится, что какое-либо прикладное программное обеспечение имеет свои внутренние требования по конфиденциальности или целостности (например, если исходный код сам является коммерческой тайной), его оценивают таким же способом, как ресурсы данных.

Величины ценности ресурсов данных получают путем интервьюирования избранных сотрудников, занятых в сфере бизнеса («владельцев данных»), которые могут давать компетентные суждения относительно данных, определять ценность и секретность данных, находящихся в использовании или подлежащих хранению или обработке с обеспечением доступа к ним. Такие интервью облегчают оценку ценности и секретности ресурсов данных с учетом самых неблагоприятных вариантов развития событий, которые можно ожидать, руководствуясь разумными основаниями, и которые могут оказать негативное воздействие на бизнес вследствие несанкционированного раскрытия информации, несанкционированной модификации, изменения отказа от совершенных действий, недоступности информации в различные периоды времени и уничтожения информации.

Оценка производится на основе руководящих указаний по оценке ресурсов данных, которые охватывают следующие вопросы:

– личная безопасность;
– персональные данные;
– обязанности соблюдать требования законов и подзаконных актов;
– правовое принуждение;
– коммерческие и экономические интересы;
– финансовые потери/нарушение нормального хода работ;
– общественный порядок;
– политика компании в области бизнеса и деловая активность;
– потеря репутации.

– Эти руководящие указания облегчают определение значений на числовой шкале, например, на шкале от 1 до 4, которая предусмотрена для матрицы, используемой в качестве примера (см. ниже), позволяя, таким образом, использовать, там, где это возможно, количественные оценки, а, где невозможно – логические и качественные оценки, например, при оценивании степени опасности для жизни людей.

– Важной работой является также составление пар вопросников по каждому типу опасности для каждой группы ресурсов, к которым относится данный тип опасности. Это обеспечит возможность оценки уровней опасности (вероятности возникновения опасно-

сти) и уровней уязвимости (легкости реализации опасностей в уязвимых местах с оказанием нежелательного воздействия). За ответ на каждый вопрос начисляются очки. Очки накапливаются с использованием базы знаний и сравниваются с рангами. Это позволяет определить уровни опасности (например, по шкале с диапазоном уровней от высокого до низкого) и аналогично им – уровни уязвимости, как показано на примере приведенной ниже матрицы, применительно к различным уровням воздействия. Ответы на вопросы, содержащиеся в вопросниках, получают в результате интервьюирования соответствующих технических специалистов, работников организации и специалистов по эксплуатации помещений, а также на основе физического обследования мест размещения аппаратуры и проверки состояния документации.

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

– Ценности ресурсов, а также уровни опасности и уязвимости, соответствующие каждому типу воздействия вводятся в матрицу, подобную той, что приведена ниже, для определения каждого сочетания соответствующих мер риска по шкале от 1 до 8. Значения величин размещаются в матрице в структурированной форме. Рассмотрим следующий пример (таблица 1):

Таблица 1

	Уровни опасности	Низкий			Средний			Высокий		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Ценность ресурса	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

Для каждого ресурса рассмотрены уязвимые места и соответствующие им опасности. Если имеются уязвимые места без соответствующей опасности или опасности без соответствующего уязвимого места, то можно считать, что в данное время риск отсутствует (Необходимо, однако, сохранять бдительность на случай возможного изменения ситуации!). Затем идентифицируется соответствующий ряд матрицы по ценности ресурса, а соответствующая колонка по степени опасности и уязвимости. Например, если ценность ресурса равна 3, опасность характеризуется как 'высокая', а уязвимость - как 'низкая', мера риска равна 5. Предположим теперь, что ценность ресурса равна 2; при оценке, например, угрозы модификации ресурса опасность характеризуется как 'низкая', а уязвимость - как 'высокая'. В этом случае мера риска будет равна 4. Размер матрицы с точки зрения числа категорий, характеризующих степень опасности, степень уязвимости и ценность ресурса выбирается в зависимости от потребностей организации. Дополнительные колонки и ряды дадут дополнительное количество мер риска. Ценность данного подхода состоит в ранжировании соответствующих рисков.

Пример 2. Ранжирование опасностей по мерам риска

Для установления взаимозависимости между факторами воздействия (ценность ресурса) и вероятностью реализации опасности (с учетом аспектов уязвимости) может использоваться матрица или таблица (см. таблицу 2). Первый шаг - оценка воздействия (ценности ресурса) по заранее определенной шкале, например, от 1 до 5, для каждого подвергаемого опасности ресурса (колонка 'b' в таблице). Второй шаг - оценка вероятности реализации опасности по заранее определенной шкале, например, от 1 до 5, для каждой опасности (колонка 'c' в таблице). Третий шаг - расчет мер риска путем перемножения результатов первых двух шагов (b x c). Теперь, наконец, можно проранжировать опасности по величине их коэффициента 'подверженности воздействиям'. Отметим, что в данном примере, цифрой 1 обозначаются самое малое воздействие и самая низкая вероятность реализации опасности.

Таблица 2

Дескриптор опасностей (a)	Оценка воздействия (ресурса) (b)	Вероятность реализации опасности (c)	Мера риска (d)	Ранг опасности (e)
Опасность A	5	2	10	2
Опасность B	2	4	8	3
Опасность C	3	5	15	1
Опасность D	1	3	3	5
Опасность E	4	1	4	4
Опасность F	2	4	8	3

Как показано выше, такая процедура позволяет сравнивать и ранжировать по приоритетности разные опасности с различными воздействиями и вероятности реализации опасности. В некоторых случаях будет необходимо связывать денежные единицы с используемыми здесь эмпирическими шкалами.

Пример 3. Оценка частоты и возможного ущерба, связанного с рисками

В данном примере основное внимание уделяется воздействию нежелательных инцидентов и определению приоритетных систем. Для этого оцениваются два значения для каждого ресурса и риска, которые в сочетании определяют числовой показатель для каждого ресурса. Путем суммирования числовых показателей всех ресурсов данной системы определяется мера риска для данной системы информационных технологий.

Прежде всего, для каждого ресурса назначается величина ценности. Эта величина связана с возможным повреждением ресурса, на который нацелена угроза. Ценность ресурса назначается для каждой опасности, которой может подвергнуться данный ресурс.

Далее необходимо определить показатель частоты. Он оценивается по сочетанию вероятности реализации опасности к легкости реализации опасностей в уязвимых местах (см. таблицу 3).

Таблица 3

Уровни опасности	Низкий			Средний			Высокий		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Показатель частоты	0	1	2	1	2	3	2	3	4

Затем по таблице 4 определяют числовые показатели по ресурсам/опасностям, находя пересечение колонки ценности ресурса и строки показателя частоты. Числовые показатели по ресурсам/опасностям суммируют и находят общий числовой показатель ресурса. Это число может быть использовано для определения различий между ресурсами, образующими часть системы.

Таблица 4

Ценность ресурса / Показатель частоты	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

Последняя операция состоит в суммировании числовых показателей по всем ресурсам системы для определения числового показателя системы. Это число может быть использовано для определения различий между системами, а также для того, чтобы определить, какие средства защиты системы следует использовать в первую очередь.

В нижеприведенных примерах все значения величин выбраны случайным образом.

Предположим, что в Системе S имеется три ресурса: A1, A2 и A3. Предположим также, что данная система может подвергаться двум опасностям: T1 и T2. Пусть ценность ресурса A1 будет равна 3, ценность ресурса A2 - 2 и ценность ресурса A3 - 4.

Если для сочетания ресурса A1 и опасности T1 вероятность реализации опасности мала, а легкость реализации опасности в уязвимых местах имеет среднюю величину, то показатель частоты будет равен 1 (см. Таблицу 3).

Числовой показатель для сочетания ресурса A1 и опасности T1 может быть взят из таблицы 4 на пересечении ценности ресурса, равной 3, и показателя частоты, равного 1. В данном случае этот числовой показатель будет равен 4. Аналогичным образом, примем для сочетания ресурса A1 и опасности T2 среднюю вероятность реализации опасности и высокую легкость реализации опасности в уязвимых местах. Тогда числовой показатель для сочетания ресурса A1 и опасности T2 будет равен 6.

Затем можно подсчитать величину общего числового показателя A1T, который будет равен 10. Общий числовой показатель ресурсов рассчитывается для каждого ресурса и угрожающих ему опасностей. Общий числовой показатель системы ST определятся путем суммирования A1T + A2T + A3T.

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

Пример 4. Разграничение между допустимыми и недопустимыми рисками

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

В соответствии с таким подходом применяемая матрица уже не содержит не числа, а только буквы T (для допустимых рисков) и N (для недопустимых рисков), обозначающие, является данный риск допустимым или не является. Так, например, матрица, используемая в Методе 3, может быть преобразована в:

Таблица 5

Величина ущерба / Показатель частоты	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, является только примером. Пусть читатель сам обозначит границу между допустимыми и недопустимыми рисками.

Приложение
(справочное)
Библиография

[1] "Руководящие указания по управлению обеспечением безопасности информационных технологий" (Часть 1).

УДК 681.324:006.354 **МКС 35.040**

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

Для заметок

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

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