ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27005 — 2010

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент риска информационной безопасности

ISO/IEC 27005:2008
Information technology — Security techniques — Information security risk management
(IDT)

Издание официальное

Москва
Стандартинформ
2011

Предисловие

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

Сведения о стандарте

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

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (ISO/IEC 27005:2008 «Information technology — Security techniques — Information security risk management»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.6).

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК ТО 13335-3—2007 и ГОСТ Р ИСО/МЭК ТО 13335-4—2007

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

Содержание

Введение

Настоящий стандарт представляет руководство по менеджменту риска информационной безопасности (ИБ) в организации, поддерживая, в частности, требования к системе менеджмента информационной безопасности (СМИБ) в соответствии с ИСО/МЭК 27001. Однако настоящий стандарт не предоставляет какой-либо конкретной методологии по менеджменту риска информационной безопасности. Выбор подхода к менеджменту риска осуществляется организацией и зависит, например от области применения СМИБ, контекста менеджмента риска или сферы деятельности. Ряд существующих методологий может использоваться в рамках структуры, описанной в настоящем стандарте для реализации требований СМИБ.

Настоящий стандарт предназначен для руководителей и персонала, занимающегося в организации вопросами менеджмента риска информационной безопасности, а также, при необходимости, для внешних сторон, имеющих отношение к этому виду деятельности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Менеджмент риска информационной безопасности

Information technology. Security techniques. Information security risk management

Дата введения — 2011 — 12— 01

1 Область применения

Настоящий стандарт представляет руководство по менеджменту риска информационной безопасности.

Настоящий стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска.

Знание концепций, моделей, процессов и терминологии, изложенных в ИСО/МЭК 27001 и ИСО/МЭК 27002, важно для полного понимания настоящего стандарта.

Настоящий стандарт применим для организаций всех типов (например, коммерческих предприятий, государственных учреждений, некоммерческих организаций), планирующих осуществлять менеджмент рисков, которые могут скомпрометировать информационную безопасность организации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК 27001:2005 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements)

ИСО/МЭК 27002:2005 Информационная технология. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности (ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice information security management)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом, следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27001, ИСО/МЭК 27002, а также следующие термины с соответствующими определениями:

Издание официальное

3.1 **влияние** (impact): Неблагоприятное изменение уровня достигнутых бизнес-целей.

3.2 **риск информационной безопасности** (information security risk): Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Примечание — Он измеряется исходя из комбинации вероятности события и его последствия.

3.3 **предотвращение риска** (risk avoidance): Решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее.
[ИСО/МЭК Руководство 73:2002][1)]

3.4 **коммуникация риска** (risk communication): Обмен информацией о риске или совместное использование этой информации лицом, принимающим решение, и другими причастными сторонами.
[ИСО/МЭК Руководство 73:2002]

3.5 **количественная оценка риска** (risk estimation): Процесс присвоения значений вероятности и последствий риска.
[ИСО/МЭК Руководство 73:2002]

Примечания

1 В контексте данного национального стандарта количественная оценка риска рассматривается как деятельность (activity), а не как процесс (process).

2 В контексте данного национального стандарта применительно к количественной оценке риска вместо термина «возможность, вероятность» (probability) используется термин «вероятность» (likelihood).

3.6 **идентификация риска** (risk identification): Процесс нахождения, составления перечня и описания элементов риска.
[ИСО/МЭК Руководство 73:2002]

Примечание — В контексте данного национального стандарта применительно к идентификации риска вместо термина «процесс» (process) используется термин «деятельность» (activity).

3.7 **снижение риска** (risk reduction): Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском.
[ИСО/МЭК Руководство 73:2002]

Примечание — В контексте данного национального стандарта применительно к количественной оценке риска вместо термина «возможность, вероятность» (probability) используется термин «вероятность» (likelihood).

3.8 **сохранение риска** (risk retention): Принятие бремени потерь или выгод от конкретного риска.
[ИСО/МЭК Руководство 73:2002]

Примечание — В контексте рисков ИБ применительно к сохранению риска рассматриваются только негативные последствия (потери).

3.9 **перенос риска** (risk transfer): Разделение с другой стороной бремени потерь или выгод от риска.
[ИСО/МЭК Руководство 73:2002]

Примечание — В контексте рисков ИБ применительно к переносу риска рассматриваются только негативные последствия (потери).

4 Структура национального стандарта

Настоящий стандарт содержит описание процесса менеджмента риска ИБ и связанных с ним видов деятельности.

Предпосылки создания стандарта описаны в разделе 5.

[1)] В Российской Федерации действует ГОСТ Р 51897.

Обзор процесса менеджмента риска ИБ дается в разделе 6.

Все виды деятельности, связанные с менеджментом риска ИБ, представленные в разделе 6, описываются далее в следующих разделах:

- Установление контекста — в разделе 7.
- Оценка риска — в разделе 8.
- Обработка риска — в разделе 9.
- Принятие риска — в разделе 10.
- Коммуникация риска — в разделе 11.
- Мониторинг и переоценка риска — в разделе 12.

Дополнительная информация о видах деятельности, связанных с менеджментом риска ИБ, приведена в приложениях. Установлению контекста способствуют сведения из приложения А (определение области применения и границ процесса менеджмента риска ИБ). Определение и установление ценности активов и оценка влияния обсуждаются в приложении В (примеры, касающиеся активов), в приложении С приведены примеры типичных угроз и в приложении D — примеры типичных уязвимостей.

Примеры подходов к оценке рисков ИБ представлены в приложении Е.

Ограничения, касающиеся снижения риска, представлены в приложении F.

Все виды деятельности, связанные с менеджментом риска, представленные в разделах 7—12, структурированы следующим образом:

Входные данные. Определяется информация, необходимая для выполнения деятельности.

Действие. Описывается деятельность.

Руководство по реализации. Представляется руководство по выполнению действия. Некоторые рекомендации данных руководств могут не подходить ко всем случаям, поэтому могут быть более уместными иные варианты действий.

Выходные данные. Описывается информация, полученная в результате выполнения деятельности.

5 Предпосылки создания стандарта

Систематический подход к менеджменту риска ИБ необходим для того, чтобы идентифицировать потребности организации, касающиеся требований ИБ, и создать эффективную СМИБ. Этот подход должен соответствовать условиям деятельности организации и, в частности, должен быть согласован с общим менеджментом рисков в масштабе организации. Усилия по обеспечению безопасности должны обеспечивать эффективное и своевременное реагирование на риски там и тогда, где и когда это необходимо. Менеджмент риска ИБ должен быть неотъемлемой частью всех видов деятельности, связанных с менеджментом ИБ, и должен применяться как на этапе внедрения, так и в процессе повседневного использования СМИБ организации.

Менеджмент риска ИБ должен быть непрерывным процессом. В рамках данного процесса следует устанавливать контекст, оценивать и обрабатывать риски, используя для реализации рекомендации и решения плана обработки рисков. До принятия решения о том, что и когда должно быть сделано для снижения риска до приемлемого уровня, в рамках менеджмента риска анализируется, что может произойти и какими могут быть возможные последствия.

Менеджмент риска ИБ должен способствовать:

- идентификации рисков;
- оценке рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения;
- осознанию и информированию о вероятности и последствиях рисков;
- установлению приоритетов в рамках обработки рисков;
- установлению приоритетов мероприятий по снижению имеющих место рисков;
- привлечению причастных сторон к принятию решений о менеджменте риска и поддержанию их информированности о состоянии менеджмента риска;
- эффективности проводимого мониторинга обработки рисков;
- проведению регулярного мониторинга и пересмотра процесса менеджмента риска;
- сбору информации для совершенствования менеджмента риска;
- подготовке менеджеров и персонала по вопросам рисков и необходимых действий, предпринимаемых для их уменьшения.

Процесс менеджмента риска ИБ может быть применен ко всей организации, к любой отдельной части организации (например, подразделению, филиалу, службе), к любой информационной системе, к имею-

щимся, планируемым или специфическим аспектам управления (например, к планированию непрерывности бизнеса).

6 Обзор процесса менеджмента риска информационной безопасности

Процесс менеджмента риска ИБ состоит из установления контекста (раздел 7), оценки риска (раздел 8), обработки риска (раздел 9), принятия риска (раздел 10), коммуникаций риска (раздел 11), а также мониторинга и переоценки риска информационной безопасности (раздел 12).

Как показано на рисунке 1, в процессе менеджмента риска ИБ процедуры оценки риска и/или обработки риска могут выполняться итеративно. Итеративный подход к проведению оценки риска может увеличить глубину и детализацию оценки при каждой последующей итерации. Итеративный подход позволяет сбалансировано затрачивать время и усилия на выбор мер и средств контроля и управления, в то же время по-прежнему обеспечивая соответствующую оценку высокоуровневых рисков.

Сначала устанавливается контекст, а затем проводится оценка риска. Если при этом удается получить достаточную информацию для эффективного определения действий, требуемых для снижения риска до приемлемого уровня, то задача выполнена, после чего следует обработка риска. Если информация является недостаточной, то проводится очередная итерация оценки риска в условиях пересмотренного контекста (например, критериев оценки рисков, критериев принятия рисков или критериев влияния), возможно в ограниченной части полной предметной области (см. рисунок 1, первая точка принятия решения).

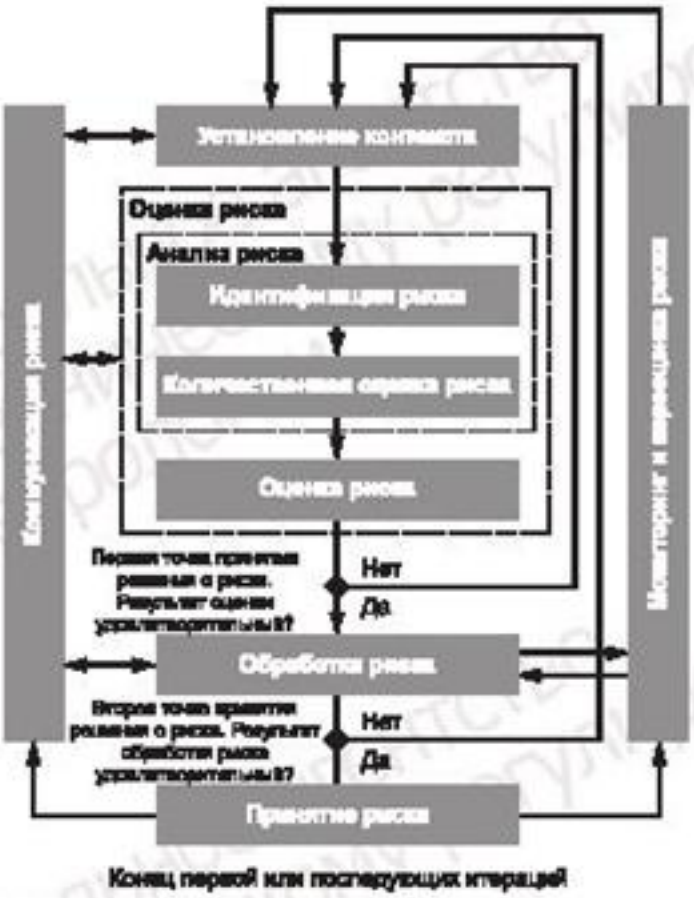

Рисунок 1 — Процесс менеджмента риска информационной безопасности

Эффективность обработки риска зависит от результатов оценки риска. Обработка риска может не обеспечить сразу же приемлемый уровень остаточного риска. В этой ситуации потребуется, если необходимо, еще одна итерация оценки риска с измененными параметрами контекста (например, критериев оценки риска, принятия риска и влияния), за которой последует очередная процедура обработки риска (см. рисунок 1, вторая точка принятия решения).

Процедура принятия риска должна обеспечивать однозначное принятие остаточных рисков руководством организации. Это особенно важно в ситуации, когда корректирующие меры не предпринимаются, или их принятие откладывается, например из-за стоимости.

В процессе менеджмента риска ИБ важно, чтобы о рисках и их обработке информировались соответствующие руководители и операционные сотрудники. Даже до обработки рисков информация об идентифицированных рисках может быть очень ценной для менеджмента инцидентов и может способствовать снижению потенциального ущерба. Осведомленность руководства и персонала о рисках, о характере мер и средств, применяемых для снижения рисков, и о проблемных областях в организации помогает максимально эффективно отреагировать на инциденты и непредвиденные события. Детализированные результаты каждого вида деятельности, входящего в процесс менеджмента риска ИБ, а также результаты, полученные из двух точек принятия решений о рисках, должны быть документированы.

В ИСО/МЭК 27001 определяется, какие меры и средства, реализуемые в рамках области применения, границ и контекста СМИБ, должны выбираться и применяться с учетом риска. Применение процесса менеджмента риска ИБ дает возможность выполнить это требование. Существует много подходов, посредством которых этот процесс может быть успешно внедрен в организации. В каждом случае применения этого процесса организация должна использовать тот подход, который наилучшим образом соответствует конкретным обстоятельствам.

В СМИБ установление контекста, оценка риска, разработка плана обработки риска и принятие риска являются частью фазы «планирование». В фазе «осуществление» СМИБ процедуры и меры, требуемые для снижения риска до приемлемого уровня, реализуются в соответствии с планом обработки риска. В фазе «проверка» СМИБ руководство определяет потребность в повторной оценке и обработке риска в свете инцидентов и изменившихся обстоятельств. В фазе «действие» осуществляются любые необходимые работы, включая дополнительное выполнение процесса менеджмента риска ИБ.

В таблице 1 показана взаимосвязь процедур менеджмента риска с четырьмя фазами процесса СМИБ.

Таблица 1 — Соотношение системы менеджмента информационной безопасности и процесса менеджмента риска информационной безопасности

Процесс СМИБ	Процесс менеджмента риска ИБ
Планирование	Установление контекста Оценка риска Планирование обработки риска Принятие риска
Осуществление	Реализация плана обработки риска
Проверка	Проведение непрерывного мониторинга и переоценки рисков
Действие	Поддержка и усовершенствование процесса менеджмента риска ИБ

7 Установление контекста

7.1 Общие положения

Входные данные. Вся информация об организации, имеющая отношение к установлению контекста менеджмента риска ИБ.

Действие. Должен быть установлен контекст менеджмента риска ИБ, что включает определение основных критериев, необходимых для менеджмента риска ИБ (в соответствии с 7.2), определение области применения и границ (в соответствии с 7.3), а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ (в соответствии с 7.4).

Руководство по реализации. Необходимо определить цель менеджмента риска ИБ, так как она влияет на общий процесс и на установление контекста в частности. Этой целью может быть:

- поддержка СМИБ;
- исполнение законодательно-нормативных требований и подтверждение проявленной организацией разумной предосторожности;
- подготовка плана обеспечения непрерывности бизнеса;
- подготовка плана реагирования на инциденты;
- описание требований ИБ для продукта, услуги или механизма.

Руководство по реализации для элементов установления контекста, необходимых для поддержки СМИБ, обсуждается в 7.2, 7.3, и 7.4.

Примечание — В ИСО/МЭК 27001 не используется термин «контекст». Однако весь раздел 7 данного стандарта связан с требованиями «определение сферы действия и границ СМИБ» [см. 4.2.1, перечисление a)], «определение политики СМИБ» [см. 4.2.1, перечисление b)] и «определение подхода к оценке риска» [см. 4.2.1, перечисление c)], установленными в ИСО/МЭК 27001.

Выходные данные. Спецификация основных критериев, сфера действия и границы, организационная структура для процесса менеджмента риска ИБ.

7.2 Основные критерии

В зависимости от области применения, объекта и целей менеджмента риска могут применяться разные подходы. Подходы, используемые на каждой из итераций, могут также различаться. Должен быть выбран или разработан соответствующий подход к оценке риска, учитывающий основные критерии, каковыми являются: критерии оценки риска, критерии влияния, критерии принятия риска.

Кроме того, организация должна оценивать, имеются ли необходимые ресурсы для:

- выполнения оценки рисков и создания плана по обработке рисков;
- определения и реализации политик и процедур, включая реализацию выбранных мер и средств контроля и управления;
- мониторинга мер и средств контроля и управления;
- мониторинга процесса менеджмента риска ИБ.

Примечание — См. также ИСО/МЭК 27001 (пункт 5.2.1) относительно обеспечения ресурсов для реализации и функционирования СМИБ.

Критерии оценки рисков

Должны быть разработаны критерии для оценки рисков информационной безопасности организации с учетом:

- стратегической ценности обработки бизнес-информации;
- критичности затронутых информационных активов;
- законодательно-нормативных требований и договорных обязательств;
- оперативного значения и значения для бизнеса доступности, конфиденциальности и целостности;
- ожидания и реакции причастных сторон, а также негативных последствий для нематериальных активов и репутации.

Кроме того, критерии оценки рисков могут использоваться для определения приоритетов при обработке рисков.

Критерии влияния

Критерии влияния должны разрабатываться и определяться исходя из степени ущерба или величины расходов, понесенных организацией вследствие события, связанного с ИБ, с учетом:

- уровня классификации информационного актива, на который оказывается влияние;
- нарушения ИБ (например утрата конфиденциальности, целостности и доступности);
- нарушения оперативной деятельности (как собственной, так и третьих сторон);
- потери ценности бизнеса и финансовой ценности;
- нарушения планов и конечных сроков;
- ущерба для репутации;
- нарушения законодательных, нормативных или договорных требований.

Примечание — См. также ИСО/МЭК 27001 [пункт 4.2.1, перечисление d) 4)] относительно определения критериев влияния возможной утраты конфиденциальности, целостности и доступности активов.

Критерии принятия риска

Критерии принятия риска должны быть разработаны и определены. Критерии принятия риска зачастую зависят от политик, намерений, целей организации и интересов причастных сторон.

Организация должна определять собственные шкалы для уровней принятия риска. При разработке следует учитывать следующее:

- критерии принятия риска могут включать ряд пороговых значений, когда указывается желаемый целевой уровень риска, но при условии, что при определенных обстоятельствах высшее руководство будет принимать риски, находящиеся выше этого уровня;

- критерии принятия риска могут выражаться как соотношение количественно оцененной прибыли (или иной выгоды бизнеса) к количественно оцененному риску;

- различные критерии принятия риска могут применяться к различным классам риска, например, могут не приниматься риски, связанные с неисполнением законодательно-нормативных требований, в то время как принятие рисков высокого уровня может быть допустимо, если это определено договорным обязательством;

- критерии принятия риска могут включать требования о проведении в будущем дополнительной обработки риска, например риск может быть принят, если принято решение и взяты обязательства предпринять меры по его снижению до приемлемого уровня в течение определенного периода времени.

Критерии принятия риска могут различаться в зависимости от того, насколько долго, предположительно, риск будет существовать, например риск может быть связан с временной или кратковременной деятельностью. Критерии принятия риска должны устанавливаться с учетом следующего:

- критериев бизнеса;
- особенностей законодательно-нормативной среды;
- операций;
- технологий;
- финансов;
- социальных и гуманитарных факторов.

Примечание — Критерии принятия риска соответствуют «критериям принятия рисков и определению приемлемого уровня риска», определенным в ИСО/МЭК 27001 [см. пункт 4.2.1, перечисление c) 2)].

Более подробную информацию можно найти в приложении А.

7.3 Область применения и границы

Организация должна определять область применения и границы менеджмента риска ИБ.

Область применения процесса менеджмента ИБ необходимо определять для того, чтобы все значимые активы принимались в расчет при оценке риска. Кроме того, необходимо определять границы [см. также ИСО/МЭК 27001, пункт 4.2.1, перечисление a)] для рассмотрения тех рисков, источники которых могут находиться за данными границами.

Должна быть собрана информация об организации для определения параметров среды, в которой функционирует организация, и их влияния на процесс менеджмента риска ИБ.

При определении области применения и границ должна учитываться следующая информация, касающаяся организации:

- стратегические цели бизнеса организации, стратегии и политики;
- бизнес-процессы;
- функции и структура организации;
- правовые, нормативные и договорные требования, применимые к организации;
- политика ИБ организации;
- общий подход организации к менеджменту риска;
- информационные активы;
- местоположение организации, ее подразделений и филиалов, а также их географические характеристики;
- ограничения, влияющие на организацию;
- ожидания причастных сторон;
- социокультурная среда;
- интерфейсы (т. е. обмен информацией с внешней средой).

Кроме того, организация должна обосновывать каждое исключение из области применения.

Примерами области применения менеджмента риска могут быть ИТ-приложение, ИТ-инфраструктура, бизнес-процесс или определенная часть организации.

Примечание — Область применения и границы менеджмента риска ИБ связаны с выполнением требования ИСО/МЭК 27001 [см. 4.2.1, перечисление a)] относительно определения области применения и границ СМИБ.

Более подробную информацию можно найти в приложении А.

7.4 Организационная структура менеджмента риска информационной безопасности

Для процесса менеджмента риска ИБ необходимо устанавливать и поддерживать организационную структуру и распределение обязанностей. Ниже перечисляются основные роли и области ответственности, присущие этой организационной структуре:

- разработка процесса менеджмента риска ИБ, подходящего для данной организации;
- выявление и изучение причастных сторон;
- определение ролей и обязанностей всех сторон, как внутренних, так и внешних по отношению к организации;
- установление требуемых взаимосвязей между организацией и причастными сторонами, а также взаимодействия с высокоуровневыми функциями менеджмента риска организации (например, менеджмента операционного риска), а также взаимодействия с другими значимыми проектами и видами деятельности;
- определение путей передачи принятия решений на более высокий уровень и/или другим специалистам;
- определение подлежащих ведению документов.

Эта организационная структура должна одобряться соответствующим руководством организации.

Примечание — ИСО/МЭК 27001 требует определения и выделения ресурсов, необходимых для установления, реализации, функционирования, мониторинга, пересмотра, поддержки и улучшения СМИБ [см. пункт 5.2.1, перечисление а)]. Организационная структура для операций менеджмента риска может рассматриваться как один из ресурсов, требуемых ИСО/МЭК 27001.

8 Оценка риска информационной безопасности

8.1 Общее описание оценки риска информационной безопасности

Примечание — В ИСО/МЭК 27001 деятельность по оценке риска определяется как процесс.

Входные данные. Установленные основные критерии, сфера действия и границы, структура процесса менеджмента риска информационной безопасности, принятые для организации.

Действие. Риски должны быть идентифицированы, количественно или качественно охарактеризованы, для них должны быть назначены приоритеты в соответствии с критериями оценки риска и целями организации.

Руководство по реализации. Риск представляет собой комбинацию последствий, вытекающих из нежелательного события и вероятности возникновения события. Оценка риска количественно или качественно характеризует риски и дает возможность руководителям назначать для них приоритеты в соответствии с осознаваемой ими серьезностью или другими установленными критериями.

Процесс оценки риска состоит из:

- анализа риска (в соответствии с 8.2), включающего идентификацию риска (в соответствии с 8.2.1) и установление значения риска (в соответствии с 8.2.2);
- оценки риска (в соответствии с 8.3).

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста.

Оценка риска часто проводится за две (или более) итерации. Сначала проводится высокоуровневая оценка для идентификации потенциально высоких рисков, служащих основанием для дальнейшей оценки. Следующая итерация может включать дальнейшее углубленное рассмотрение потенциально высоких рисков. В тех случаях, когда полученная информация недостаточна для оценки риска, проводится более детальный анализ, возможно, по отдельным частям сферы действия, и, возможно, с использованием иного метода.

Выбор подхода к оценке риска в зависимости от задач и целей оценки риска осуществляет руководство организации.

Обсуждение подходов к оценке риска ИБ можно найти в приложении Е.

Выходные данные. Перечень оцененных рисков в соответствии с назначенными приоритетами согласно критериям оценки риска.

8.2 Анализ риска

8.2.1 Идентификация риска

8.2.1.1 Введение в идентификацию риска

Цель идентификации риска — определить, что могло бы произойти при нанесении возможного ущерба, и получить представление о том, как, где и почему мог иметь место этот ущерб. Этапы, описанные ниже, должны объединять входные данные для деятельности по количественной оценке риска.

Примечание — Виды деятельности, описанные ниже, могут быть выполнены в различном порядке, в зависимости от применяемой методологии.

8.2.1.2 Определение активов

Входные данные. Сфера действия и границы проведения оценки риска, перечень, включающий владельцев, местоположение, функцию и т. д.

Действие. Должны быть определены активы, входящие в установленную сферу действия [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 1)].

Руководство по реализации. Активом является что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите. При определении активов следует иметь в виду, что информационная система состоит не только из аппаратных и программных средств.

Определение активов следует проводить с соответствующей степенью детализации, обеспечивающей информацию, достаточную для оценки риска. Степень детализации, используемая при определении активов, влияет на общий объем информации, собранной во время оценки риска. Эта информация может быть более детализирована при последующих итерациях оценки риска.

Для установления учетности и ответственности в отношении каждого актива должен быть определен владелец. Владелец актива может не обладать правами собственности на актив, но он несет ответственность за его получение, разработку, поддержку, использование и безопасность. Чаще всего владелец актива является наиболее подходящим лицом, способным определить реальную ценность актива для организации (см. 8.2.2 на предмет определения ценности активов).

Границей анализа является периметр активов организации, управляемый в рамках процесса менеджмента риска ИБ.

Более подробную информацию об определении активов и их ценности в части ИБ можно найти в приложении В.

Выходные данные. Перечень активов, подлежащих менеджменту риска, и перечень бизнес-процессов, связанных с активами, а также их значимость.

8.2.1.3 Определение угроз

Входные данные. Информация об угрозах, полученная в результате анализа инцидента от владельцев активов, пользователей, а также из других источников, включая списки внешних угроз.

Действие. Угрозы и их источники должны быть определены [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 2)].

Руководство по реализации. Угроза может причинить ущерб активам организации, таким как информация, процессы и системы. Угрозы могут возникать в результате природных явлений или действий людей, они могут быть случайными или умышленными. Должны быть установлены и случайные, и преднамеренные источники угроз. Угрозы могут проистекать как из самой организации, так и из источника вне ее пределов. Угрозы должны определяться в общем и по виду (например неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы определяются внутри родового класса. Это означает, что ни одна угроза, включая неожиданные угрозы, не будет упущена, но объем требуемой работы, несмотря на это, сокращается.

Некоторые угрозы могут влиять более чем на один актив. В таких случаях они могут быть причиной различных влияний в зависимости от того, на какие активы оказывается воздействие.

Входные данные для определения и количественной оценки вероятности возникновения угроз (см. 8.2.2.3) могут быть получены от владельцев активов или пользователей, персонала отдела кадров, руководства организации и специалистов в области ИБ, экспертов в области физической безопасности, специалистов юридического отдела и других структур, а также от юридических организаций, метеорологических служб, страховых компаний, национальных правительственных учреждений. При анализе угроз должны учитываться аспекты среды и культуры.

Опыт, извлеченный из инцидентов, и предыдущие оценки угроз должны быть учтены в текущей оценке. При необходимости для заполнения перечня общих угроз может быть целесообразным справиться в других реестрах угроз (возможно, специфичных для конкретной организации или бизнеса). Списки угроз и их статистику можно получить от промышленных предприятий, федерального правительства, юридических организаций, страховых компаний и т. д.

Используя списки угроз или результаты предыдущих оценок угроз, не следует забывать о том, что происходит постоянная смена значимых угроз, особенно, если изменяются бизнес-среда или информационные системы.

Более подробную информацию о типах угроз можно найти в приложении С.

Выходные данные. Перечень угроз с определением их вида и источника.

8.2.1.4 Определение существующих мер и средств контроля и управления

Входные данные. Документация по мерам и средствам контроля и управления, планы по реализации обработки риска.

Действие. Должны быть определены существующие и планируемые меры и средства контроля и управления.

Руководство по реализации. Во избежание лишней работы или расходов, например, при дублировании мер и средств контроля и управления, необходимо определить существующие меры и средства контроля и управления. Кроме того, при определении существующих мер и средств контроля и управления следует провести проверку, чтобы убедиться в правильности функционирования мер и средств контроля и управления — обращение к существующим отчетам по аудиту СМИБ должны сокращать время, затрачиваемое на решение этой задачи. Ненадлежащее функционирование мер и средств контроля и управления может стать причиной уязвимости. Следует уделить внимание ситуации, когда выбранные меры и средства контроля и управления (или стратегия) не выполняют своих функций, и для эффективного и своевременного реагирования на идентифицированные риски требуются дополнительные меры и средства контроля и управления. В СМИБ, в соответствии с ИСО/МЭК 27001, это поддерживается измерением эффективности мер и средств контроля и управления. Один из способов количественной оценки действия мер и средств контроля и управления — выявить, как оно снижает вероятность возникновения угрозы, затрудняет использование уязвимости и возможности влияния инцидента. Проверки, проводимые руководством, и отчеты по аудиту также обеспечивают информацию об эффективности существующих мер и средств контроля и управления.

Меры и средства контроля и управления, которые планируется реализовать в соответствии с планами реализации обработки риска, должны быть определены тем же самым способом, который уже был реализован.

Существующие или планируемые меры и средства контроля и управления могут быть отнесены к разряду неэффективных, недостаточных или необоснованных. Если их посчитали необоснованными или недостаточными, меру и средство контроля и управления необходимо подвергнуть проверке, чтобы определить, подлежат ли они удалению, замене более подходящими, или стоит оставить их, например из соображений стоимости.

Для определения существующих или планируемых мер и средств контроля и управления могут быть полезны следующие мероприятия:

- просмотр документов, содержащих информацию о средствах контроля (например, планы обработки рисков), если процессы менеджмента ИБ документированы должным образом, то информация о всех существующих или планируемых мерах и средствах контроля и управления, а также о состоянии их реализации должна быть доступна;
- проверка, проводимая совместно с сотрудниками, отвечающими за ИБ (например, сотрудником, занимающимся обеспечением ИБ, сотрудником, отвечающим за безопасность информационной системы, комендантом здания или руководителем работ) и пользователями, касающаяся того, какие меры и средства контроля и управления действительно реализованы для рассматриваемого информационного процесса или информационной системы;
- обход здания с целью осмотра физических средств контроля, сравнение существующих средств контроля с перечнем тех, которые должны быть реализованы, и проверка существующих средств контроля на предмет правильной и эффективной работы;
- рассмотрение результатов внутренних аудитов.

Выходные данные. Перечень всех существующих и планируемых мер и средств контроля и управления, их нахождение и состояние использования.

8.2.1.5 Выявление уязвимостей

Входные данные. Перечни известных угроз, перечни активов и существующих мер и средств контроля и управления.

Действие. Необходимо выявить уязвимости, которые могут быть использованы угрозами для нанесения ущерба активам или организации [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 3)].

Руководство по реализации. Уязвимости могут быть выявлены в следующих областях:
- организация работ;
- процессы и процедуры;
- установившийся порядок управления;
- персонал;
- физическая среда;
- конфигурация информационной системы;
- аппаратные средства, программное обеспечение и аппаратура связи;
- зависимость от внешних сторон.

Наличие уязвимости само по себе не наносит ущерба, поскольку необходимо наличие угрозы, которая сможет воспользоваться ею. Для уязвимости, которой не соответствует определенная угроза, может не потребоваться внедрение средства контроля и управления, но она должна осознаваться и подвергаться мониторингу на предмет изменений. Следует отметить, что неверно реализованное, неправильно функционирующее или неправильно используемое средство контроля и управления само может стать уязвимостью. Меры и средства контроля и управления могут быть эффективными или неэффективными в зависимости от среды, в которой они функционируют. С другой стороны, угроза, которой не соответствует определенная уязвимость, может не приводить к риску.

Уязвимости могут быть связаны со свойствами актива. Способ и цели использования актива могут отличаться от планируемых при приобретении или создании актива. Необходимо учитывать уязвимости, возникающие из разных источников, например те, которые являются внешними или внутренними по отношению к активу.

Примеры уязвимостей и методы их оценки можно найти в приложении D.

Выходные данные. Перечень уязвимостей, связанных с активами, угрозами и мерами и средствами контроля и управления; перечень уязвимостей, не связанных с выявленной угрозой, подлежащей рассмотрению.

8.2.1.6 Определение последствий

Входные данные. Перечень активов, бизнес-процессов, угроз и уязвимостей, где это уместно, связанных с активами, и их значимость.

Действие. Должны быть определены последствия для активов, вызванные потерей конфиденциальности, целостности и доступности [см. ИСО/МЭК 27001, пункт 4.2.1, перечисление d) 4)].

Руководство по реализации. Последствием может быть снижение эффективности, неблагоприятные операционные условия, потеря бизнеса, ущерб, нанесенный репутации и т. д.

Эта деятельность определяет ущерб или последствия для организации, которые могут быть обусловлены сценарием инцидента. Сценарий инцидента — это описание угрозы, использующей определенную уязвимость или совокупность уязвимостей в инциденте ИБ (см. ИСО/МЭК 27002, раздел 13). Влияние сценариев инцидентов обусловливается критериями влияния, определяемыми в течение деятельности по установлению контекста. Влияние может затрагивать один или несколько активов, а также часть актива. Поэтому активам может назначаться ценность, обусловленная как их финансовой стоимостью, так и последствиями для бизнеса в случае их порчи или компрометации. Последствия могут быть временными или постоянными, как это бывает в случае разрушения активов.

Примечание — В ИСО/МЭК 27001 описывается происхождение сценариев инцидентов как «недостатков безопасности».

Организации должны определять операционные последствия сценариев инцидентов на основе (но не ограничиваясь):
- времени на расследование и восстановление;
- потерь (рабочего) времени;
- упущенной возможности;
- охраны труда и безопасности;
- финансовых затрат на приобретение специфических навыков, необходимых для устранения неисправности;
- репутации и иного «неосязаемого капитала».

Подробности, касающиеся оценки технических уязвимостей, можно найти в В.3 (приложение В).

Выходные данные. Перечень сценариев инцидентов с их последствиями, связанными с активами и бизнес-процессами.

8.2.2 Установление значения[2] риска

8.2.2.1 Методология установления значения риска

Анализ риска может быть выполнен с различной степенью детализации в зависимости от критичности активов, распространенности известных уязвимостей и прежних инцидентов, касавшихся организации. Методология установления значения риска может быть качественной, количественной, или комбинированной, в зависимости от обстоятельств. На практике установление качественного значения часто используется вначале для получения общих сведений об уровне риска и выявления основных значений рисков. Позднее может возникнуть необходимость в осуществлении более специфичного установления количественного анализа основных значений рисков, поскольку обычно выполнение качественного анализа по сравнению с количественным является менее сложным и затратным.

Форма анализа должна согласовываться с критериями оценки риска, разработанными как часть установления контекста.

Далее более подробно описываются детали методологии установления значения риска.

Для установления качественного значения используется шкала квалификации атрибутов, с помощью которой описываются величины возможных последствий (например низкий, средний и высокий) и вероятности возникновения этих последствий. Преимущество установления качественного значения заключается в доступности для понимания всем соответствующим персоналом, а недостатком — зависимость от субъективного выбора шкалы.

Такие шкалы могут быть адаптированы или скорректированы в соответствии с обстоятельствами, для разных рисков могут использоваться разные описания. Установление качественного значения может использоваться:

- как начальная деятельность по тщательной проверке для идентификации рисков, требующих более детального анализа;
- там, где этот вид анализа способствует принятию решения;
- там, где числовые данные или ресурсы являются неадекватными для установления количественного значения.

Качественный анализ должен использовать фактическую информацию и доступные данные.

Для установления количественной оценки используется шкала с числовыми значениями (а не описательные шкалы, используемые при установлении качественного значения) как последствий, так и вероятности, с применением данных из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев для установления количественного значения используются фактические данные за прошедший период. Преимущество заключается в том, что установление количественного значения может быть напрямую связано с целями информационной безопасности и проблемами организации. Недостатки количественного подхода могут иметь место, когда фактические проверяемые данные недоступны, поэтому создается иллюзия ценности и точности установления количественного значения риска.

Способ выражения последствий риска и вероятности его возникновения, а также способы их комбинирования для получения информации об уровне риска изменяются в зависимости от вида риска и цели, для достижения которой должны использоваться выходные данные оценки риска. При анализе риска следует учитывать неопределенность и изменяемость последствий риска, а также вероятность его возникновения и сообщать о них эффективным образом.

8.2.2.2 Оценка последствий

Входные данные. Перечень определенных значимых сценариев инцидентов, включая выявление угроз, уязвимостей и затронутых активов, а также последствий для активов и бизнес-процессов.

Действие. Должно быть оценено влияние на бизнес организации, которое может быть результатом предполагаемых или фактических инцидентов ИБ с учетом последствий нарушения ИБ, таких, как потеря конфиденциальности, целостности или доступности активов [связано с ИСО/МЭК 27001, 4.2.1, перечисление е) 1)].

Руководство по реализации. После определения всех проверяемых активов, присвоенная им ценность должна учитываться при оценке последствий.

---

[2] Контекст настоящего пункта стандарта требует использования термина «установление значения риска» (risk estimation), отличного от термина «количественная оценка риска» (risk estimation), определенного ГОСТ Р 51897.

Значение влияния на бизнес может быть выражено в качественной или количественной формах. Тем не менее более наглядным является метод присвоения денежного выражения, который, как правило, дает больше информации для принятия решений и, следовательно, делает процесс принятия решений более эффективным.

Определение ценности активов начинается с классификации активов в соответствии с их критичностью с точки зрения важности активов для осуществления бизнес-целей организации. Затем ценность активов определяется с использованием двух мер:

- восстановительной стоимости актива — стоимости его очистки с целью восстановления и замены информации (если это возможно);

- последствий для бизнеса от потери или компрометации актива, например возможные неблагоприятные последствия для бизнеса и/или законодательные или регулирующие последствия раскрытия, модификации, недоступности и/или разрушения информации, а также других информационных активов.

Это определение ценности может быть установлено на основе анализа влияния на бизнес. Ценность, определяемая последствиями для бизнеса, обычно значительно выше просто восстановительной стоимости и зависит от значимости актива для организации при выполнении ее бизнес-целей.

Определение ценности активов является ключевым фактором оценки влияния сценария инцидента, поскольку инцидент может затрагивать более одного актива (например, зависимые активы), или только часть актива. Различные угрозы и уязвимости могут иметь различное влияние на активы, например потеря конфиденциальности, целостности и доступности. Поэтому оценка последствий связана с определением ценности активов или становится связанной, исходя из анализа влияния на бизнес.

Последствия или влияние на бизнес могут определяться путем моделирования результатов события или совокупности событий, экстраполяции экспериментальных исследований или данных за прошедшее время.

Последствия могут быть выражены с помощью денежных, технических персональных критериев влияния или других критериев, значимых для организации. В отдельных случаях для определения последствий, различающихся по времени, месту, группам или ситуациям, требуется более одного цифрового значения.

Последствия, различающиеся по времени или финансам, должны измеряться с использованием того же подхода, который применяется в отношении вероятности угрозы и уязвимости. Должна поддерживаться последовательность количественного или качественного подхода.

В приложении В приводится более подробная информация, касающаяся определения ценности активов и оценки влияния.

Выходные данные. Перечень оцененных последствий сценария инцидентов, выраженных с учетом активов и критериев влияния.

8.2.2.3 Оценка вероятности инцидента

Входные данные. Перечень определенных значимых сценариев инцидентов, включая определение угроз, затрагиваемые активы, используемые уязвимости и последствия для активов и бизнес-процессов. Кроме того, перечни всех существующих и планируемых мер и средств контроля и управления, уровень их эффективности, реализации и использования.

Действие. Должна быть оценена вероятность действия сценариев инцидентов [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление e) 2)].

Руководство по реализации. После определения сценариев инцидентов необходимо оценить вероятность действия каждого сценария и его влияние с использованием качественного или количественного метода установления значения. Необходимо принимать во внимание частоту возникновения угроз и простоту использования уязвимости, с учетом:

- опыта и соответствующей статистики вероятности возникновения угроз;

- для источников умышленных угроз — мотивации и возможности, которые будут меняться с течением времени, ресурсов, доступных для потенциальных нарушителей, а также восприятия потенциальным нарушителем привлекательности и уязвимости активов;

- для источников случайных угроз — территориальных факторов, например близость к химическому или нефтеперерабатывающему заводу, возможность экстремальных погодных условий и факторов, которые могут вызывать ошибки персонала и сбои оборудования;

- уязвимостей как отдельных, так и в совокупности;

- существующих мер и средств контроля и управления и того, насколько эффективно они снижают уязвимости.

Например, информационная система может иметь уязвимость по отношению к угрозам имитации личности пользователя и злоупотреблению ресурсами. Уязвимость, связанная с имитацией личности пользователя, может быть высокой из-за отсутствия аутентификации пользователей. С другой стороны, вероятность злоупотребления ресурсами может быть низкой, несмотря на отсутствие аутентификации пользователей, поскольку способы злоупотребления ресурсами ограничены.

В зависимости от требуемой точности активы могут быть сгруппированы или разбиты на элементы, и может возникать необходимость соотнесения сценариев с элементами. Например в зависимости от местоположения характер угроз в отношении одних и тех же видов активов может меняться или может различаться эффективность существующих мер и средств контроля и управления.

Выходные данные. Вероятность действия сценариев инцидентов (в количественном или качественном выражении).

8.2.2.4 Установление значений уровня рисков

Входные данные. Перечень сценариев инцидентов с их последствиями, касающимися активов и бизнес-процессов, и их вероятность (в количественном или качественном выражении).

Действие. Должны быть установлены значения уровня рисков для всех значимых сценариев инцидентов [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление e) 4)].

Руководство по реализации. При установлении значений рисков присваиваются значения вероятности возникновения риска и его последствий. Эти значения могут быть выражены качественно или количественно. Установление значений рисков основывается на оцененных последствиях и их вероятности. Кроме того, оно может также учитывать стоимость и эффективность, проблемы причастных сторон и другие переменные, используемые при оценке риска. Установленное значение риска является комбинацией значений вероятности сценария инцидента и его последствий.

В приложении Е приводятся примеры различных методов и подходов к установлению значения рисков ИБ.

Выходные данные. Перечень рисков с уровнями присвоенных значений.

8.3 Оценка риска

Входные данные. Перечень рисков с уровнями присвоенных значений и критериями оценки риска.

Действие. Должны сравниваться уровни рисков с критериями оценки рисков и критериями принятия рисков [связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление e) 4)].

Руководство по реализации. Характер решений, связанных с оценкой рисков, и критерии оценки рисков, которые будут использованы для принятия этих решений, должны определяться при установлении контекста. Эти решения и контекст должны более детально анализироваться на этапе получения большего объема информации о конкретных идентифицированных рисках. Для оценки рисков организация должна сравнивать установленные значения рисков (с использованием выбранных методов, рассматриваемых в приложении Е) с критериями оценки риска, выбранными на этапе установления контекста.

Критерии оценки риска, используемые для принятия решений, должны согласовываться с определенным внешним и внутренним контекстом менеджмента риска ИБ и учитывать цели организации, мнения причастных сторон и т. д. Решения, связанные с оценкой риска, обычно основываются на приемлемом уровне риска. Однако также должны учитываться последствия, вероятность, степень уверенности при идентификации и анализе риска. Совокупность множества рисков низкого и среднего уровня в итоге может иметь результатом общий риск более высокого уровня.

При этом необходимо учитывать следующее:

- свойства ИБ — если один критерий не актуален для организации (например, потеря конфиденциальности), то все риски, влияющие на этот критерий, могут быть также не актуальными;

- значимость бизнес-процесса или деятельности, поддерживаемых конкретным активом или совокупностью активов, если процесс определен как имеющий низкую значимость, связанным с ним рискам следует уделять меньше внимания, чем рискам, влияющим на более важные процессы или деятельность.

Оценка риска основывается на понимании риска, полученном при анализе риска, и используется при принятии решений о будущих действиях. Решения должны включать в себя следующее:

- необходимость в некой деятельности;

- приоритеты при обработке риска с учетом установленных значений уровней рисков.

На стадии оценки риска в дополнение к рискам с установленными значениями должны приниматься в расчет договорные, юридические и нормативные требования.

Выходные данные. Перечень рисков с назначенными приоритетами в соответствии с критериями оценки рисков, касающимися сценариев инцидентов, которые приводят к этим рискам.

9 Обработка риска информационной безопасности

9.1 Общее описание обработки риска

Входные данные. Перечень рисков с назначенными приоритетами в соответствии с критериями оценки рисков, касающимися сценариев инцидентов, которые приводят к этим рискам.

Действие. Должны быть выбраны меры и средства контроля и управления для снижения, сохранения, предотвращения или переноса рисков, а также определен план обработки рисков.

Руководство по реализации. Для обработки риска имеется четыре варианта: снижение риска (см. 9.2), сохранение риска (см. 9.3), предотвращение риска (см. 9.4) и перенос риска (см. 9.5).

Примечание — В ИСО/МЭК 27001 [см. пункт 4.2.1, перечисление f) 2)] вместо термина «сохранение риска» («retaining risk») используется термин «принятие риска» («accepting risk»).

На рисунке 2 иллюстрируется деятельность по обработке риска в рамках процесса менеджмента риска ИБ.

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности.

Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах. Дополнительные варианты повышения эффективности могут быть неэкономичными, и необходимо принимать решение о целесообразности их применения.

Неблагоприятные последствия рисков необходимо снижать до разумных пределов независимо от каких-либо абсолютных критериев. Редкие, но серьезные риски должны рассматриваться руководством. В таких случаях может возникнуть необходимость реализации мер и средств контроля и управления, которые являются необоснованными по причинам затратности (например меры и средства контроля и управления непрерывности бизнеса, для охвата высоких специфических рисков).

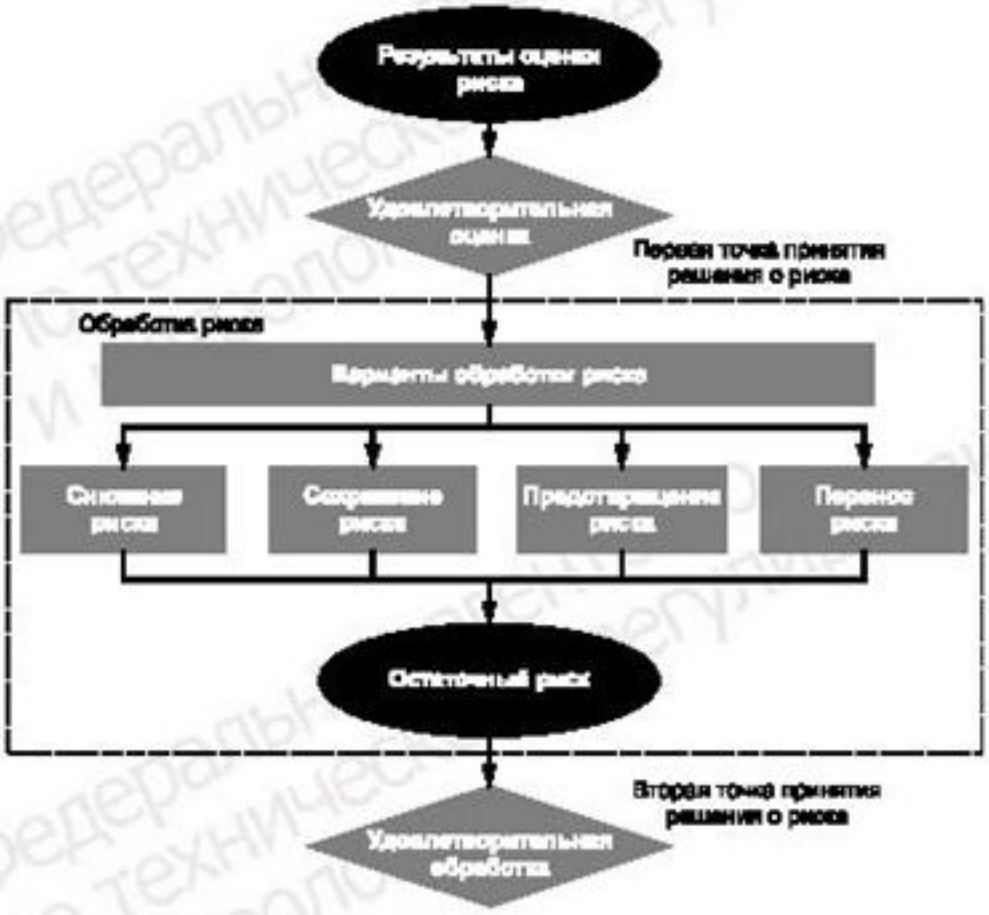

Рисунок 2 — Деятельность по обработке риска

Четыре варианта обработки риска не являются взаимоисключающими. В отдельных случаях организация может получить значительную выгоду от объединения вариантов, таких, как снижение вероятности риска, уменьшение последствий и перенос или сохранение любого остаточного риска.

Некоторые варианты обработки риска могут быть эффективными для более чем одного риска (например обучение и осведомленность в части ИБ). План обработки риска должен четко определять порядок приоритетов, при соблюдении которого должна реализовываться обработка отдельного риска. Порядок приоритетов может устанавливаться с использованием различных методов, включая ранжирование рисков и анализ «затраты—выгоды». В обязанности руководства входит принятие решения о балансе между затратами на реализацию мер и средств контроля и управления и бюджетными отчислениями.

При определении существующих мер и средств контроля и управления может быть установлено, что существующие меры и средства контроля и управления превышают текущую потребность в показателях сравнения затрат, включая поддержку. В случае удаления избыточных или ненужных мер и средств контроля и управления (особенно, если расходы на их поддержку велики) должны учитываться факторы ИБ и стоимости. Поскольку меры и средства контроля и управления оказывают влияние друг на друга, удаление избыточных мер и средств контроля и управления может в итоге снизить эффективность использования всех оставшихся мер и средств обеспечения безопасности. Кроме того, может быть менее затратным оставить избыточные или ненужные средства контроля, чем удалить их.

Для разных вариантов обработки риска должно учитываться:

- как риск осознается затрагиваемыми сторонами;
- наиболее подходящие способы обмена информацией с этими сторонами.

Установление контекста (см. 7.2 «Основные критерии») предоставляет информацию о законодательных и нормативных требованиях, которым необходимо следовать организации. Отказ от следования указанным требованиям является риском для организаций, поэтому должны быть рассмотрены варианты решений, ограничивающие эту возможность. Все ограничения — организационные, технические, структурные и др., которые определяются в течение деятельности, связанной с установлением контекста, следует учитывать в течение обработки риска.

После уточнения плана обработки риска необходимо определить остаточные риски. Это включает обновление или повторную операцию оценки риска с учетом ожидаемого эффекта от предполагаемой обработки риска. Если остаточные риски по-прежнему не будут удовлетворять критериям принятия риска организации, может возникнуть необходимость в дополнительной итерации обработки риска, прежде чем перейти к принятию риска.

Выходные данные. План обработки риска и остаточные риски – предмет обсуждения для принятия решения руководством организации.

9.2 Снижение риска

Действие. Уровень риска должен быть снижен путем выбора меры и средства контроля и управления так, чтобы остаточный риск мог быть повторно оценен как допустимый.

Руководство по реализации. Должны быть выбраны соответствующие и обоснованные меры и средства контроля и управления, чтобы удовлетворять требованиям, определенным путем оценки и обработки рисков. Такой выбор должен учитывать критерии принятия рисков, а также законодательные, нормативные и договорные требования. При выборе должны также учитываться стоимость и время реализации мер и средств контроля и управления или технические аспекты, аспекты среды и культурные аспекты. С помощью соответствующим образом выбранных мер и средств контроля безопасности зачастую можно снизить общие расходы владельца системы.

В целом меры и средства контроля и управления могут обеспечивать один или несколько из перечисленных видов защиты: исправление, исключение, предупреждение, уменьшение влияния, сдерживание, обнаружение, восстановление, мониторинг и информированность. Во время выбора мер и средств контроля и управления важно установить баланс между стоимостью приобретения, реализации, администрирования, функционирования, мониторинга и поддержки мер и средств контроля и управления и ценностью защищаемых активов. Кроме того, необходимо учитывать рентабельность инвестиций с точки зрения снижения риска, и потенциал для использования новых возможностей бизнеса, предоставляемых определенными мерами и средствами контроля и управления. Дополнительно следует обратить внимание на специализированные навыки, которые могут потребоваться для определения и реализации новых мер и средств контроля и управления или модификации существующих.

В ИСО/МЭК 27002 дается подробная информация по выбору мер и средств контроля и управления.

Существует много ограничений, которые могут влиять на выбор мер и средств контроля и управления. Технические ограничения, такие, как требования к функционированию, проблемы управляемости (требования операционной поддержки) и совместимости, могут препятствовать использованию определенных мер и средств контроля и управления или могут вводить ошибку оператора, либо аннулирующую эти меры и средства контроля и управления, внушая ложное чувство безопасности, либо даже увеличивающую риск, как если бы не имелось никаких мер и средств контроля и управления (например, требование использования сложных паролей без соответствующего обучения, которое может приводить к записи паролей пользователями). Более того, может возникнуть ситуация, когда меры и средства контроля и управления будут влиять на производительность. Руководство должно стремиться принять такое решение, которое будет удовлетворять требованиям производительности, гарантируя в то же время достаточную ИБ. Результатом этого первого шага является перечень возможных мер и средств контроля и управления с указанием их стоимости, эффективности и приоритета реализации.

При формировании рекомендаций и в процессе реализации должны учитываться различные ограничения. Типичными ограничениями являются:

- временные ограничения;
- финансовые ограничения;
- технические ограничения;
- операционные ограничения;
- культурные ограничения;
- этические ограничения;
- ограничения, связанные с окружающей средой;
- юридические ограничения;
- ограничения, связанные с простотой использования;
- кадровые ограничения;
- ограничения, касающиеся интеграции новых и существующих мер и средств контроля и управления.

Более подробную информацию об ограничениях, сопутствующих решениям по снижению риска, можно найти в приложении F.

9.3 Сохранение риска

Действие. Решение сохранить риск, не предпринимая дальнейшего действия, следует принимать в зависимости от оценки риска.

Примечание — В ИСО/МЭК 27001 [см. пункт 4.2.1, перечисление f) 2)] описывается та же самая деятельность: «осознанное и объективное принятие рисков при условии, что они, несомненно, отвечают политикам и критериям организации, касающимся принятия рисков».

Руководство по реализации. Если уровень риска соответствует критериям принятия риска, то нет необходимости реализовывать дополнительные меры и средства контроля и управления, и риск может быть сохранен.

9.4 Предотвращение риска

Действие. Отказ от деятельности или условия, вызывающего конкретный риск.

Руководство по реализации. Если идентифицированные риски считаются слишком высокими или расходы на реализацию других вариантов обработки риска превышают выгоду, может быть принято решение о полном предотвращении риска путем отказа от планируемой или существующей деятельности, или их совокупности, или изменения условий, при которых осуществляется деятельность. Например, в отношении рисков, вызываемых природными факторами, наиболее экономически выгодной альтернативой может быть физическое перемещение средств обработки информации туда, где этого риска не существует или он контролируется.

9.5 Перенос риска

Действие. Риск должен быть перенесен на сторону, которая может наиболее эффективно осуществлять менеджмент конкретного риска, в зависимости от оценки риска.

Руководство по реализации. Перенос риска включает в себя решение разделить определенные риски с внешними сторонами. Перенос риска может создавать новые риски или модифицировать существующие идентифицированные риски. Поэтому может быть необходима дополнительная обработка риска.

Перенос может быть осуществлен путем страхования, которое будет поддерживать последствия, или путем заключения договора субподряда с партнером, чья роль будет заключаться в проведении мони-

торинга информационной системы и осуществлении незамедлительных действий по прекращению атаки, прежде чем она приведет к определенному уровню ущерба.

Следует заметить, что может быть возможным перенести ответственность за менеджмент риска, но, как правило, невозможно перенести ответственность за ущерб. Клиенты обычно воспринимают неблагоприятное влияние ущерба как ошибку организации.

10 Принятие риска информационной безопасности

Входные данные. Наличие плана обработки риска и оценки остаточного риска является необходимым условием решения руководства организации о принятии риска.

Действие. Должно быть принято решение о принятии рисков и установлена ответственность за это решение, что должно быть официально зарегистрировано [это связано с ИСО/МЭК 27001, пункт 4.2.1, перечисление h)].

Руководство по реализации. В планах обработки рисков должен быть описан способ оценки рисков, которые следует обрабатывать, для того чтобы соответствовать критериям принятия рисков (см. 7.2 «Основные критерии»). Важно, чтобы ответственные руководители проверяли и поддерживали предлагаемые планы обработки рисков и вытекающие из них остаточные риски, а также регистрировали все условия, связанные с такой поддержкой.

Критерии принятия риска могут быть более многогранными, чем только определение того, находится ли остаточный риск выше или ниже единого порогового значения.

В некоторых случаях уровень остаточного риска может не соответствовать критериям принятия риска, поскольку применяемые критерии не учитывают превалирующих обстоятельств. Например, может быть доказано, что необходимо принимать риски по причине привлекательности выгод или по причине значительных расходов, связанных со снижением риска. Такие обстоятельства показывают, что критерии принятия риска неадекватны и должны быть по возможности пересмотрены. Однако не всегда бывает возможным пересмотреть критерии принятия риска своевременно. В таких случаях руководители, принимающие решения, могут быть обязаны принять риски, которые не соответствуют стандартным критериям принятия рисков. Если это необходимо, руководитель, принимающий решение, должен дать комментарий, касающийся рисков, с обоснованием решения, выходящего за рамки стандартного критерия принятия рисков.

Выходные данные. Перечень принятых рисков с обоснованием рисков, не соответствующих стандартным критериям принятия риска организации.

11 Коммуникация риска информационной безопасности

Входные данные. Вся информация о рисках, полученная в результате деятельности по менеджменту риска (см. рисунок 1).

Действие. Должен осуществляться обмен информацией о риске или ее совместное использование лицом, принимающим решение, и другими причастными сторонами.

Руководство по реализации. Коммуникация риска представляет собой деятельность, связанную с достижением соглашения о том, как осуществлять менеджмент риска путем обмена и/или совместного использования информации о риске лицами, принимающими решения, и другими причастными сторонами. Информация включает в себя наличие, характер, форму, вероятность, серьезность, обработку и приемлемость рисков, но этими факторами не ограничивается.

Эффективная коммуникация между причастными сторонами имеет большое значение, поскольку она может оказывать существенное влияние на решения, которые должны быть приняты. С помощью коммуникации сотрудники, отвечающие за осуществление менеджмента риска, и лица, относящиеся к заинтересованным кругам, достигают понимания основы, на которой принимаются решения, и причины необходимости выполнения определенных действий. Коммуникация является двунаправленным процессом.

Осознание риска может быть разным из-за различий в предположениях, понятиях, потребностях, проблемах и беспокойствах причастных сторон, связанных с риском или обсуждаемыми проблемами. Причастные стороны, как правило, выносят суждения о приемлемости риска на основе своего осознания риска. Поэтому очень важно обеспечить, чтобы осознание риска причастными сторонами, а также осознание ими выгод могло быть определено и документировано, а лежащие в основе причины были четко поняты и учтены.

Коммуникация риска должна осуществляться с целью достижения следующего:

- обеспечения доверия к результатам менеджмента риска организации;
- сбора информации о риске;
- совместного использования результатов оценки риска и представления плана обработки риска;
- предотвращения или снижения возможности возникновения и последствий нарушений ИБ из-за отсутствия взаимопонимания между принимающими решения лицами и причастными сторонами;
- поддержки принятия решений;
- получения новых знаний об ИБ;
- координации с другими сторонами и планирования реагирования с целью уменьшения последствий какого-либо инцидента;
- выработки чувства ответственности по отношению к рискам у лиц, принимающих решения, и причастных сторон;
- повышения осведомленности.

Организация должна разрабатывать планы коммуникации риска как для повседневной работы, так и для чрезвычайных ситуаций. Следовательно, деятельность, связанная с коммуникацией риска, должна выполняться непрерывно.

Координация между лицами, принимающими окончательные решения, и иными причастными сторонами может быть достигнута путем создания комитета, который будет обсуждать проблемы возникновения рисков, назначать приоритеты и вырабатывать решения по обработке и принятию рисков.

Важно поддерживать сотрудничество с соответствующим отделом по связям с общественностью или информационным отделом организации, чтобы координировать все задачи, связанные с коммуникацией риска. Это крайне важно в случаях сообщения о действиях в кризисных ситуациях, например в ответ на определенные инциденты.

Выходные данные. Постоянное понимание процесса менеджмента риска ИБ организации.

12 Мониторинг и переоценка риска информационной безопасности

12.1 Мониторинг и переоценка факторов риска

Входные данные. Вся информация о рисках, полученная в результате деятельности по менеджменту риска (см. рисунок 1).

Действие. Должны подвергаться мониторингу и переоценке риски и их факторы (т. е. ценность активов, влияние, угрозы, уязвимости, вероятность возникновения) с целью определения любых изменений в контексте организации на ранней стадии, и должно поддерживаться общее представление о всей картине риска.

Руководство по реализации. Риски не являются статичными. Угрозы, уязвимости, вероятность или последствия могут изменяться неожиданно, без каких-либо признаков изменений. Поэтому для выявления изменений необходим непрерывный мониторинг. Он может поддерживаться внешними сервисами, которые предоставляют информацию о новых угрозах или уязвимостях.

Организации должны обеспечивать проведение непрерывного мониторинга следующих факторов:

- новых активов, которые были включены в область действия менеджмента риска;
- необходимой модификации ценности активов, например, вследствие изменившихся бизнес-требований;
- новых угроз, которые могут действовать вне и внутри организации и которые еще не были оценены;
- вероятности того, что новые или возросшие уязвимости могут сделать возможным использование их угрозами;
- выявленных уязвимостей для определения тех из них, которые становятся подверженными новым или повторно возникающим угрозам;
- возросшего влияния или последствий оцененных угроз, уязвимостей и рисков, объединенное действие которых имеет результатом неприемлемый уровень риска;
- инцидентов ИБ.

Новые угрозы, уязвимости или изменения вероятности или последствий могут увеличивать риски, ранее оцененные как низкие. Процесс переоценки низких и принятых рисков должен рассматривать каждый риск отдельно, а также все риски как единое целое, чтобы оценивать их возможное суммарное влияние. Если риски не попадают в категорию низких или приемлемых рисков, они должны обрабатываться с использованием одного или нескольких вариантов, рассмотренных в разделе 9.

Факторы, влияющие на вероятность и последствия возникающих угроз, могут изменяться, как могут изменяться факторы, влияющие на применимость или стоимость различных вариантов обработки. Основные изменения, влияющие на организацию, должны служить основанием для более детальной переоценки. Следовательно, деятельность по мониторингу риска должна регулярно повторяться, и выбранные варианты обработки риска должны периодически переоцениваться.

Результаты деятельности по мониторингу риска могут быть входными данными для другой деятельности по переоценке риска. Организация должна переоценивать все риски регулярно, а также когда имеют место существенные изменения (в соответствии с ИСО/МЭК 27001, пункт 4.2.3).

Выходные данные. Постоянное согласование менеджмента риска с бизнес-целями организации и критериями принятия риска.

12.2 Мониторинг, анализ и улучшение менеджмента риска

Входные данные. Вся информация о рисках, полученная в результате деятельности по менеджменту риска (см. рисунок 1).

Действие. Процесс менеджмента риска ИБ подлежит постоянному мониторингу, анализу и улучшению.

Руководство по реализации. Постоянный мониторинг и переоценка необходимы для того, чтобы контекст, результат оценки и обработки риска, а также планы менеджмента оставались уместными и соответствующими обстоятельствам.

Организация должна вселять уверенность, что процесс менеджмента риска ИБ и связанная с ним деятельность остаются соответствующими при существующих обстоятельствах, и они соблюдаются. О любых согласованных улучшениях процесса или действиях, необходимых для повышения соответствия этому процессу, следует уведомлять руководителей, чтобы быть уверенными в том, что не существует ни одного риска или элемента риска, упущенного или недооцененного, что предпринимаются необходимые действия и принимаются решения для получения реалистичного представления о риске и способности реагировать на него.

Кроме того, организация должна регулярно убеждаться в том, что критерии, используемые для измерения риска и его элементов, по-прежнему остаются обоснованными и согласующимися с ее бизнес-целями, стратегиями и политиками и что изменения бизнес-контекста принимаются во внимание на адекватном уровне во время процесса менеджмента риска ИБ. Эта деятельность по мониторингу и переоценке должна учитывать (но не ограничиваться) следующее:

- правовой контекст и контекст окружающей среды;
- контекст конкуренции;
- подход к оценке риска;
- ценности и категории активов;
- критерии влияния;
- критерии оценки риска;
- критерии принятия риска;
- полную стоимость владения активами;
- необходимые ресурсы.

Организация должна обеспечивать постоянную доступность оценки и обработки риска для переоценки риска, рассмотрения новых или изменившихся угроз или уязвимостей и соответствующего уведомления руководства.

Мониторинг менеджмента риска может иметь результатом модификацию или дополнение подхода, методологии или инструментальных средств, используемых в зависимости от следующего:

- выявленных изменений;
- итерации оценки риска;
- цели процесса менеджмента риска ИБ (например непрерывность бизнеса, устойчивость к инцидентам, совместимость);
- объекта процесса менеджмента риска ИБ (например, организация, бизнес-подразделение, информационный процесс, его техническая реализация, приложение, подключение к Интернету).

Выходные данные. Постоянная значимость процесса менеджмента риска ИБ для бизнес-целей организации или обновления процесса.

Приложение А
(справочное)

Определение области применения и границ процесса менеджмента риска информационной безопасности

А.1 Анализ организации

Анализ организации. Изучение организации дает возможность воспроизвести характерные элементы, определяющие особенности организации. Оно касается цели, бизнеса, назначения, ценностей и стратегий этой организации, которые должны быть определены наряду с элементами, способствующими их разработке (например, заключение контрагентских договоров).

Трудность такой деятельности заключается в полном понимании структуры организации. Определение ее реальной структуры дает понимание роли и значимости каждого подразделения в достижении целей организации.

Пример — Тот факт, что ответственный за ИБ отчитывается перед высшим руководством, а не перед руководством ИТ, может указывать на участие высшего руководства в проблемах ИБ.

Основная цель организации. Основная цель организации может определяться сферой ее деятельности, сегментом рынка и др.

Бизнес организации. Бизнес организации, определяемый техническими приемами, применяемыми ее сотрудниками и накопленным ими опытом (ноу-хау), дает ей возможность реализовывать свое назначение. Он является специфичной областью деятельности организации и зачастую определяет культуру ее труда.

Назначение организации. Организация достигает своей цели посредством реализации своего назначения. Для определения ее назначения должны быть определены предоставляемые сервисы и/или производимая продукция.

Ценность организации. Ценностями являются основные нормы или четко определенный кодекс поведения, выполняемые для осуществления бизнеса. Это может касаться персонала, отношений с внешними сторонами (например, клиентами), качества поставляемой продукции или предоставляемых сервисов.

Пример — Рассмотрим организацию, целью которой является предоставление услуг населению, бизнесом — транспортные услуги, а назначение заключается в перевозке детей в школу и обратно. Ее ценностями могут быть пунктуальность предоставления услуг и безопасность перевозок.

Структура организации. Существуют разные типы структур:

- филиальная структура, в которой каждое подразделение работает под началом руководителя подразделения, ответственного за принятие стратегических, административных и операционных решений, касающихся его подразделения;
- функциональная структура, в которой функциональные полномочия осуществляются относительно процедур, характера работы и, иногда, принятия решений или составления планов (например производство, ИТ, кадры, маркетинг и т. д.).

Замечания:

- подразделение, существующее в пределах организации с филиальной структурой, может быть организовано как функциональная структура и наоборот;
- структура организации, имеющей элементы обоих типов структуры, называется матричной.

При любой организационной структуре могут различаться следующие уровни:

- уровень принятия решений (определение стратегической ориентации);
- уровень руководства (координация и менеджмент);
- операционный уровень (виды деятельности, связанные с производством и поддержкой).

Диаграмма организации. Структура организации представляется схематически в виде диаграммы организации. При таком представлении следует выделять линии отчетности и делегирования полномочий, кроме того, следует также включать в диаграмму и другие связи, которые, даже если они не основываются на каких-либо формальных полномочиях, являются тем не менее линиями информационного потока.

Стратегия организации. Для нее требуется формальное выражение руководящих принципов организации. Стратегия определяет направление и развитие организации, необходимые для извлечения выгоды из задач, стоящих перед ее бизнесом и планируемых ею основных изменений.

А.2 Перечень ограничений, влияющих на организацию

Следует учитывать все ограничения, влияющие на организацию и определяющие направленность ее ИБ. Источник ограничений может находиться в пределах организации, и в этом случае она имеет некоторый контроль над ними, или за пределами организации и, следовательно, не может контролироваться. Наиболее важными являются ограничения ресурсов (бюджетных, кадровых) и ограничения, связанные с чрезвычайными обстоятельствами.

Организация устанавливает свои цели (касающиеся ее бизнеса, режима работы и т. д.), способствующие выбору ее пути, возможно, на длительный период времени. Она определяет, какой организацией она хочет стать, и выбирает средства, которые для этого потребуются. При выборе своего пути организация учитывает эволюцию методов и ноу-хау, пожелания пользователей, клиентов и др. Этот путь может быть выражен в форме стратегий эксплуатации или разработки с намерением, например снизить эксплуатационные расходы, повысить качество обслуживания и т. д.

Такие стратегии, вероятно, будут включать в себя информацию и информационные системы, способствующие их реализации. Следовательно, свойства, касающиеся особенностей, назначения и стратегий организации, являются основополагающими элементами в анализе проблемы, поскольку нарушение аспекта ИБ может привести к переосмыслению целей этих стратегий. Кроме того, важно, чтобы предложения, касающиеся требований ИБ, находились в соответствии с правилами, режимами эксплуатации и средствами, применяемыми в организации.

Перечень включает в себя, но не ограничивается, следующие ограничения.

Ограничения политического свойства. Они могут касаться правительственной администрации, общественных учреждений или любой организации, которая должна применять решения, принятые на государственном уровне. Такими обычно являются решения, касающиеся стратегии или эксплуатационной направленности, принятые правительственным подразделением или организацией, уполномоченной в соответствии с законодательством принимать решения, и которые должны быть выполнены.

Пример — Компьютеризация счетов или административных документов влечет за собой проблемы с информационной безопасностью.

Ограничения стратегического свойства. Они могут возникать в результате запланированных или возможных изменений структуры или направленности организации. Они могут отражаться в стратегических или эксплуатационных планах организации.

Пример — Международное сотрудничество в области совместного использования чувствительной информации может потребовать соглашений, касающихся безопасного обмена.

Территориальные ограничения. Структура и/или цель организации могут обусловливать определенные ограничения, такие, как распределение рабочих площадок по территории своей страны или за рубежом.

Пример — Включают в себя почтовую службу, посольства, банки, филиалы крупной промышленной группы и т. д.

Ограничения, на возникновение которых влияет состояние экономики и политики. Функционирование организации может сильно изменяться вследствие определенных событий, таких, как забастовки или национальные или международные кризисы.

Пример — Некоторые сервисы могут продолжать функционирование даже во время серьезных кризисных ситуаций.

Структурные ограничения. Тип структуры организации (филиальная, функциональная или другая) может иметь следствием определенную политику ИБ и организацию безопасности, адаптированную к структуре.

Пример — Международная структура должна быть способна приводить в соответствие требования безопасности, принятые в каждой отдельной стране.

Функциональные ограничения. Функциональные ограничения возникают непосредственно из основного или специфического назначения организации.

Пример — Организация, работающая круглосуточно, должна непрерывно обеспечивать доступность своих ресурсов.

Ограничения, касающиеся персонала. Природа этих ограничений значительным образом варьируется. Они связаны с уровнем ответственности, наймом сотрудников, квалификацией, обучением, осведомленностью в вопросах безопасности, мотивацией, доступностью и т. д.

Пример — Персонал оборонной организации должен иметь соответствующий допуск к обработке информации ограниченного доступа.

Ограничения, проистекающие из списка дел организации. Такие ограничения могут быть результатом реструктуризации или планирования новых национальных или международных политик, с установлением определенных конечных сроков.

Пример — Создание службы безопасности.

Ограничения, связанные с методами. Методы, соответствующие ноу-хау организации, необходимо устанавливать в отношении таких аспектов, как планирование проекта, технические условия, разработка и т. д.

Пример — Типичным ограничением такого рода является необходимость включения правовых обязательств организации в политику безопасности.

Ограничения культурного свойства. В некоторых организациях рабочие традиции или основной бизнес привели к созданию определенной культуры организации, которая может быть несовместима с мерами и средствами контроля и управления безопасностью. Такая культура является основной эталонной системой персонала и может определяться многими аспектами, включающими в себя образование, обучение, профессиональный опыт, работу, на которую распространяется жизненный опыт, мнения, философию, убеждения, чувства, социальный статус и т. д.

Бюджетные ограничения. Рекомендуемые меры и средства контроля и управления безопасностью могут иметь иногда очень высокую стоимость. Несмотря на то что не всегда уместно строить инвестирование безопасности на экономической эффективности, финансовые отделы организации требуют, как правило, экономического обоснования.

Пример — В организациях частного сектора и некоторых общественных организациях совокупные расходы на меры и средства контроля и управления безопасностью не должны превышать издержек от возможных последствий рисков. Высшее руководство должно поэтому оценивать и принимать просчитанные риски, если оно желает избежать чрезмерных расходов, связанных с обеспечением безопасности.

А.3 Перечень законодательных и нормативных положений, имеющих отношение к деятельности организации

Должны определяться нормативные требования, имеющие отношение к видам деятельности организации. К их числу могут быть отнесены законы, постановления, специальные инструкции, относящиеся к сфере деятельности организации или внутренним/внешним нормам. Это касается также договоров и соглашений и, в общем, любых обязательств юридического свойства.

А.4 Перечень ограничений, влияющих на область применения

При определении ограничений желательно перечислить те из них, которые влияют на область применения, и определить те, на которые возможно некоторое воздействие. Они добавляются к ограничениям организации, перечисленным выше, и, возможно, могут изменить их. Далее представляется перечень возможных типов ограничений, который не является исчерпывающим.

Ограничения, возникающие из ранее существовавших процессов. Проекты приложений не обязательно разрабатываются одновременно. Некоторые из них зависят от ранее существовавших процессов. Даже если процесс может быть разбит на подпроцессы, не обязательно на данный процесс будут влиять все подпроцессы другого процесса.

Технические ограничения. Технические ограничения, относящиеся к инфраструктуре, в основном возникают от установленных аппаратных и программных средств, а также от помещений или площадок, где осуществляются процессы:

- архивы (файлы) — требования, касающиеся организации, менеджмент носителей, менеджмент правил доступа и т. д.;
- общая архитектура — требования, касающиеся топологии (централизованная, распределенная, клиент-сервер), физическая архитектура и т. д.;
- прикладные программы — требования, касающиеся проектирования специфичного программного обеспечения, рыночные стандарты и т. д.;
- пакеты программ — требования, касающиеся стандартов, уровня оценки, качества, соответствия нормам, безопасности и т. д.;
- аппаратные средства — требования, касающиеся стандартов, качества, соответствия нормам и т. д.;
- сети связи — требования, касающиеся покрытия, стандартов, емкости, надежности и т. д.;
- инфраструктура сооружений и инженерных коммуникаций — требования, касающиеся гражданского строительства, конструкций, высокого напряжения, низкого напряжения и т. д.

Финансовые ограничения. Реализация мер и средств контроля и управления безопасностью часто ограничивается тем бюджетом, который может выделить организация. Однако финансовое ограничение должно по-прежнему оставаться последним, подлежащим рассмотрению, поскольку вопрос о выделении бюджетных средств на безопасность может быть решен на основе анализа безопасности.

Ограничения, связанные со средой. Они обусловлены географической или экономической средой, в которых процессы реализуются: страна, климат, природные риски, территориальное расположение, состояние экономики и др.

Ограничения по времени. Время, необходимое для реализации мер и средств контроля и управления безопасностью, должно определяться с учетом возможности модернизации информационной системы. Если на реализацию затрачивается очень много времени, то риски, для которых разрабатывались меры и средства контроля и управления, могут измениться. Время является определяющим фактором при принятии решений и выборе приоритетов.

Ограничения, касающиеся методов. Методы, соответствующие ноу-хау организации, должны использоваться в отношении планирования проекта, технических условий, разработки и др.

Организационные ограничения. Различные ограничения могут следовать из требований организации, а именно:

- эксплуатация — требования, касающиеся длительности производственного цикла, предоставления услуг, наблюдения, мониторинга, планов действий в чрезвычайных ситуациях, ухудшения работы и др.;
- поддержка — требования к поиску неисправностей, связанных с инцидентом, превентивным действиям, быстрому исправлению и др.;
- менеджмент кадровых ресурсов — требования, касающиеся обучения операторов и пользователей, квалификации, необходимой для таких должностей, как системный администратор или администратор данных и др;
- административный менеджмент — требования, касающиеся обязанностей и др.;
- менеджмент разработки — требования, касающиеся инструментальных средств разработки, систем автоматизированной разработки программ, планов приемочного контроля, обеспечения организации и др.;
- менеджмент внешних отношений — требования, касающиеся формирования отношений с третьими сторонами, договоров и т. д.

Приложение В
(справочное)

Определение и установление ценности активов и оценка влияния

В.1 Примеры определения активов

Для установления ценности активов организация должна в первую очередь определить все свои активы на соответствующем уровне детализации. Могут различаться два вида активов:

- основные активы, включающие бизнес-процессы, бизнес-деятельность и информацию;
- вспомогательные (поддерживающие) активы, от которых зависят основные составные части области применения всех типов, включающие аппаратные средства, программное обеспечение, сеть, персонал, место функционирования организации, структуру организации.

В.1.1 Определение основных активов

Данная деятельность заключается в определении основных активов (бизнес-процессы и бизнес-деятельность, информация). Такое определение осуществляется сотрудниками совместной рабочей группы, участвующими в процессе (руководители, специалисты в сфере информационных систем и пользователи).

Основными активами обычно являются базовые процессы и информация о деятельности организации в ее сфере действия. Могут рассматриваться также и другие основные активы, такие, как процессы жизнедеятельности организации, которые будут иметь отношение к формированию политики ИБ или плана непрерывности бизнеса. В зависимости от цели, иногда не требуется исчерпывающий анализ всех элементов, входящих в процесс менеджмента риска. В таких случаях рамки изучения могут быть ограничены наиболее значимыми элементами.

Основные активы бывают двух типов.

1 Бизнес-процессы (или подпроцессы) и бизнес-деятельность, например:

- процессы, утрата или ухудшение которых делает невозможным реализацию целей и задач организации;
- процессы, содержащие засекреченные процессы или процессы, созданные с использованием патентованной технологии;
- процессы, модификация которых может значительно повлиять на реализацию целей и задач организации;
- процессы, которые необходимы организации для выполнения договорных, законодательных или нормативных требований.

2 Информация. В общем основная информация включает в себя:

- информацию, необходимую для реализации назначения или бизнеса организации;
- информацию личного характера, которая определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни;
- стратегическую информацию, необходимую для достижения целей, определяемых направлением стратегии организации;
- ценную информацию, сбор, хранение, обработка и передача которой требуют продолжительного времени и/или связаны с большими затратами на ее приобретение.

Процессы и информация, которые не были определены как чувствительные относительно данной деятельности, не будут иметь определенной классификации в оставшейся части исследования. Это означает, что если такие процессы или информация будут скомпрометированы, организация по-прежнему будет успешно осуществлять свое назначение. Тем не менее они часто наследуют меры и средства контроля и управления, реализуемые для защиты процессов и информации, определенных как чувствительные.

В.1.2 Перечень и описание вспомогательных активов

Сфера рассмотрения включает активы, которые должны быть определены и описаны. Этим активам присущи уязвимости, которые могут быть использованы угрозами, нацеленными на порчу основных активов сферы рассмотрения (процессов и информации). Они могут быть различных типов.

Аппаратные средства

Тип «аппаратные средства» включает все физические элементы, поддерживающие процессы.

Аппаратура обработки данных (активная). Аппаратура автоматизированной обработки информации состоит из элементов, необходимых для независимой работы.

Мобильная аппаратура. Портативная вычислительная техника.

Пример — Портативный компьютер (ноутбук), карманный компьютер.

Стационарная аппаратура. Вычислительная техника, используемая в помещениях организации.

Пример — Сервер, микрокомпьютер, используемый в качестве рабочей станции.

Периферийное обрабатывающее оборудование. Аппаратура, подсоединенная к компьютеру посредством связного порта (соединение через последовательные, параллельные каналы и т. п.) для ввода, перемещения или передачи данных.

Пример — Принтер, сменный дисковод.

Носитель данных (пассивный)

Это носители для хранения данных или функций.

Электронный носитель. Носитель информации, который может быть подсоединен к компьютеру или компьютерной сети для хранения данных. Несмотря на компактный размер, такие носители могут содержать большой объем данных. Они могут использоваться со стандартной вычислительной аппаратурой.

Пример — Гибкие диски, CD ROM, резервный картридж, сменный жесткий диск, ключ защиты памяти, магнитная лента.

Другие носители. Статичные, неэлектронные носители, содержащие данные.

Примеры — Бумага, слайд, диапозитив, документация, факс.

Программное обеспечение

Программное обеспечение включает программы, содействующие работе устройства по обработке данных.

Операционная система. Такое наименование подразумевает включение всех программ компьютера, создающего операционную основу, на которой исполняются все другие программы (сервисы или приложения). Оно означает включение ядра и основных функций или сервисов. В зависимости от архитектуры операционная система может быть монолитной или состоящей из микроядра и совокупности системных сервисов. Главными элементами операционной системы являются все сервисы менеджмента оборудования (центральное процессорное устройство, запоминающее устройство, диски и сетевые интерфейсы), сервисы менеджмента задач или процессов, а также сервисы менеджмента пользователей и прав пользователей.

Программное обеспечение обслуживания, сопровождения или администрирования. Программное обеспечение дополняет сервисы операционной системы, но не обслуживает непосредственно пользователей или приложения (даже если это обычно является важным или обязательным для общей работы информационной системы).

Пакетное программное обеспечение или стандартные программы. Стандартные программы или пакетное программное обеспечение являются завершенными продуктами, предназначенными для получения прибыли (а не одноразовыми или специфическими разработками), продаваемыми вместе с носителем, версией и сопровождением. Они обеспечивают сервисы для пользователей и приложений, но не являются персонифицированными или специфичными в отличие от бизнес-приложений.

Пример — Программное обеспечение управления базой данных, программное обеспечение электронного обмена сообщениями, программное обеспечение коллективного пользования, программное обеспечение каталогов, программное обеспечение Web-сервера и т. д.

Бизнес-приложение

Стандартное бизнес-приложение. Коммерческое программное обеспечение, предназначенное для предоставления пользователям прямого доступа к сервисам и функциям, требуемым ими от своей информационной системы в своем профессиональном контексте. Существует огромное разнообразие видов такого программного обеспечения.

Пример — Программное обеспечение учетных записей, программное обеспечение управления станками, программное обеспечение медицинского наблюдения за пациентами, программное обеспечение менеджмента компетентности персонала, административное программное обеспечение и т. д.

Специфическое бизнес-приложение. Программное обеспечение, в котором различные аспекты (главным образом, поддержка, сопровождение, модернизация и т. д.) были разработаны специально для предоставления пользователям прямого доступа к сервисам и функциям, требуемым ими от своей информационной системы. Существует огромное, разнообразие видов такого программного обеспечения.

Пример — Менеджмент счетов клиентов операторов дальней связи, приложение мониторинга запуска ракет в реальном времени.

Сеть

Тип «сеть» состоит из всех телекоммуникационных устройств, используемых для соединения нескольких физически удаленных компьютеров или элементов информационной системы.

Среда и поддержка. Среда или оборудование связи и дальней связи характеризуются, главным образом, физическими и техническими характеристиками оборудования («точка—точка», ретрансляция) и протоколами связи (канальный или сетевой — уровни 2 и 3 семиуровневой модели взаимодействия открытых систем).

Пример — Коммутируемая телефонная сеть общего пользования (PSTN — Public Switching Telephone Network), Ethernet, Gigabit Ethernet, асимметричная цифровая абонентская линия (ADSL — Asymmetric Digital Subscriber Line), стандарты на беспроводную связь (например, WiFi 802.11), спецификация Bluetooth, стандарт FireWire.

Пассивные или активные ретрансляторы. Данный подтип включает все устройства, являющиеся не оконечными, а промежуточными устройствами связи. Ретрансляторы характеризуются поддерживающими сетевыми протоколами связи. В дополнение к базовому ретранслятору они зачастую обеспечивают функции и сервисы маршрутизации и/или фильтрации с использованием связных коммутаторов и маршрутизаторов с фильтрами. Управление ими зачастую может осуществляться на расстоянии, и обычно они способны генерировать журналы регистрации.

Пример — Мост, маршрутизатор, концентратор, коммутатор, автоматический коммутатор каналов.

Связной интерфейс. Связные интерфейсы процессоров подсоединены к процессорам, но характеризуются средой и поддерживающими протоколами, любыми установленными функциями фильтрации, регистрации или генерации предупреждений и их функциональными возможностями, а также возможностью и необходимостью удаленного управления.

Пример — Пакетная радиосвязь общего назначения (GPRS — General Packet Radio Service), Ethernet-адаптер.

Персонал

Тип «персонал» состоит из всех групп сотрудников, участвующих в работе информационной системы.

Лицо, принимающее решения. Лицами, принимающими решения, являются владельцы основных активов (информации и функций) и руководители организации или определенного проекта.

Пример — Высшее руководство, руководитель проекта.

Пользователи. Пользователями является персонал, обрабатывающий чувствительные элементы в контексте своей деятельности и несущий в этой связи определенную ответственность. Они могут обладать особыми правами доступа к информационной системе, необходимыми им для решения своих повседневных задач.

Пример — Руководитель отдела кадров, руководитель финансового отдела, руководитель, осуществляющий менеджмент риска.

Персонал по эксплуатации и сопровождению. Это персонал, занимающийся эксплуатацией и сопровождением информационной системы. Он обладает особыми правами доступа к информационной системе, необходимыми ему для решения своих повседневных задач.

Пример — Системный администратор, администратор данных, оператор резервирования, справочного стола, развертывания приложений, сотрудники службы безопасности.

Разработчики. Разработчики занимаются разработкой приложений организации. Они обладают высокоуровневыми правами доступа к части информационной системы, но не выполняют каких-либо действий в отношении данных, связанных с выпуском продукции.

Пример — Разработчики бизнес-приложений.

Место функционирования организации

Тип «место функционирования организации» включает в себя все площадки, имеющие отношение к области применения или части области применения, и физические средства, необходимые для ее функционирования.

Внешняя среда. Внешней средой являются все места, в которых не могут применяться средства обеспечения безопасности организации.

Пример — Жилища персонала, помещения другой организации, среда за пределами места функционирования организации (городская зона, опасная зона).

Владения организации. Это пространство ограничивается периметром организации, непосредственно контактирующим с внешней средой. Речь может идти о физической защитной границе, обеспечиваемой созданием физических барьеров, или о средствах наблюдения, установленных вокруг зданий.

Пример — Штат организации, здания.

Зона. Зона создается физической защитной границей, образующей отдельные участки на территории организации. Она обеспечивается с помощью создания физических барьеров вокруг инфраструктур обработки информации организации.

Пример — Офисы, зарезервированная зона доступа, безопасная зона.

Основные сервисы. Все сервисы, необходимые для функционирования оборудования организации.

Связь. Телекоммуникационные сервисы и оборудование, обслуживаемые оператором.

Пример — Телефонная линия, АТС организации с исходящей и входящей связью, внутренние телефонные сети.

Коммуникации. Сервисы и средства (источники и электропроводка), необходимые для снабжения энергией информационно-технологического оборудования и периферийных устройств;

Пример — Источники электропитания с низким напряжением, инвертор, распределительное устройство электрической цепи.

- водоснабжение;
- удаление отходов;
- сервисы и средства (оборудование, контроль) для охлаждения и очистки воздуха.

Пример — Трубы водяного охлаждения, кондиционеры воздуха.

Организация

Тип «организация» связан с описанием схемы организации, состоящей из всех кадровых структур, выполняющих некую работу, и процедур, управляющих этими структурами.

Административные органы. Структуры, от которых указанная организация получает свои полномочия. Они могут быть юридически оформленными филиалами организации или внешними структурами. Это налагает ограничения на оцениваемую организацию в плане правил, решений и действий.

Пример — Контролирующая организация, правление организации.

Структура организации. Она состоит из различных отделений организации, включая деятельность организации с пересекающимися функциями под управлением ее руководства.

Пример — Кадровый менеджмент, менеджмент ИТ, снабженческий менеджмент, менеджмент бизнес-подразделений, служба безопасности зданий, пожарная служба, менеджмент аудита.

Организация проекта или системы. Организация, созданная для определенного проекта или сервиса.

Пример — Проект разработки нового приложения, проект миграции информационной системы.

Контрагенты/поставщики/изготовители. Организация, обеспечивающая данную организацию сервисом или ресурсами и связанная с ней договором.

Пример — Компания по управлению оборудованием, аутсорсинговая компания, консалтинговые компании.

В.2 Установление ценности активов

Следующий шаг после определения активов состоит в согласовании используемой шкалы ценностей и критериев для присвоения каждому активу определенного положения на шкале, основанного на установлении ценности. Вследствие разнообразия активов, встречающихся в большинстве организаций, вероятно, что некоторые активы, имеющие известную денежную ценность, будут оценены в единицах местной валюты, тогда как другим, обладающим в большей степени качественной ценностью, может быть присвоена ценность, колеблющаяся, например, в пределах от «очень низкой» до «очень высокой». Решение о том, какую шкалу использовать, количественную или качественную, в действительности является вопросом предпочтения организации, но она должна быть уместна для оцениваемых активов. Оба вида определения ценности могут быть использованы для одного и того же актива.

Типичные термины, используемые для качественного установления ценности активов, включают следующие определения: пренебрежимо малая, очень низкая, низкая, средняя, высокая, очень высокая, критичная. Выбор и диапазон терминов, подходящих для организации, сильно зависят от потребности в безопасности организации, размера организации и других, характерных для организации факторов.

Критерии

Критерии, используемые в качестве основы для присвоения ценности каждому активу, должны быть записаны в однозначных выражениях. Это часто является одним из наиболее сложных аспектов установления ценности активов, поскольку ценность некоторых активов, возможно, должна устанавливаться субъективно и принимать решения, вероятно, будут разные люди. Возможные критерии, используемые для определения ценности актива, включают его исходную стоимость, стоимость его замены или воссоздания, или ценность, которая может быть абстрактной, например ценность репутации организации.

Еще одной основой для установления ценности активов являются расходы, понесенные из-за потери конфиденциальности, целостности и доступности в результате инцидента. Неотказуемость, учетность, подлинность и надежность также должны рассматриваться соответствующим образом. Такое установление ценности обеспечит изменения важных элементов ценности актива в дополнение к восстановительной стоимости, основанных на приблизительных оценках неблагоприятных последствий для бизнеса, вытекающих из инцидентов безопасности

с предполагаемой совокупностью обстоятельств. Следует подчеркнуть, что при этом подходе принимаются во внимание последствия, которые необходимо включать в оценку риска.

Многим активам в ходе установления ценности могут присваиваться несколько значений ценности. Например, бизнес-план может оцениваться на основе труда, затраченного на его разработку, он может оцениваться на основе труда, необходимого для ввода данных, или он может оцениваться на основе его значимости для конкурентов. Все эти присвоенные значения ценности скорее всего будут существенно различаться. Присвоенное значение может быть максимальным из всех возможных значений или суммой некоторых или всех возможных значений. В окончательном анализе должно быть тщательно определено, какое значение или значения ценности присваиваются активу, потому что окончательная присвоенная ценность включается в определение ресурсов, которые должны быть затрачены на защиту актива.

Сведение к общей основе

В конечном счете все установления ценности активов должны быть сведены к общей основе. Это можно сделать с помощью критериев, приведенных ниже. Критерии, которые могут использоваться для оценки возможных последствий, вытекающих из потери конфиденциальности, целостности, доступности, неотказуемости, учетности, подлинности или надежности активов, включают:

- нарушение законодательства и/или норм;
- ухудшение функционирования бизнеса;
- потеря «неосязаемого капитала»/негативное влияние на репутацию;
- нарушения, связанные с личной информацией;
- создание угрозы личной безопасности;
- неблагоприятное влияние на обеспечение правопорядка;
- нарушение конфиденциальности;
- нарушение общественного порядка;
- финансовые потери;
- нарушение бизнес-деятельности;
- создание угрозы для безопасности окружающей среды.

Другим подходом к оценке последствий могут быть:

- прерывание сервиса — невозможность обеспечения сервиса;
- утрата доверия клиента — утрата доверия международной информационной системе, потеря репутации;
- нарушение внутреннего функционирования — нарушения внутри самой организации, дополнительные внутренние расходы;
- нарушение функционирования третьей стороны — нарушения в функционировании третьих сторон, ведущих дела с организацией, различные виды убытков;
- нарушение законов/норм — неспособность выполнения правовых обязательств;
- нарушение договора — неспособность выполнения договорных обязательств;
- опасность для персонала/безопасность пользователей — опасность для персонала и/или пользователей организации;
- вторжение в частную жизнь пользователей;
- финансовые потери;
- финансовые потери, связанные с чрезвычайными обстоятельствами или ремонтом — касающиеся персонала, касающиеся оборудования, касающиеся исследований, отчетов экспертов;
- потеря товаров/фондов/активов;
- потеря клиентов, потеря поставщиков;
- судебные дела и штрафы;
- потеря конкурентного преимущества;
- потеря технологического/технического лидерства;
- потеря эффективности/надежности;
- потеря технической репутации;
- снижение способности к заключению соглашений;
- промышленный кризис (забастовки);
- правительственный кризис;
- увольнения;
- материальный ущерб.

Эти критерии являются примерами проблем, которые должны рассматриваться при установлении ценности активов. Для проведения оценок организации нужно выбрать критерии, уместные для ее вида бизнеса и требований безопасности. Это может означать, что некоторые из перечисленных выше критериев неприменимы и может потребоваться дополнение к этому списку.

Шкала

После установления критериев для рассмотрения организации следует согласовать шкалу, которая будет использоваться в масштабах организации. Первым шагом является принятие решения о числе используемых уровней. Не существует правил, определяющих наиболее уместное число уровней. Большее число уровней обеспечивает больший уровень детализации, но иногда слишком мелкая дифференциация затрудняет присвоение

согласованных оценок в масштабе организации. Обычно может использоваться любое число уровней от 3 (например низкий, средний и высокий) до 10 в соответствии с подходом, используемым организацией для всего процесса оценки риска.

Организация может установить собственные пределы ценности активов, такие, как «низкий», «средний» или «высокий». Эти пределы должны оцениваться в соответствии с выбранными критериями, (так, для возможных финансовых потерь пределы должны быть указаны в денежном выражении, но при рассмотрении, например угрозы личной безопасности, определить их денежную ценность может быть затруднительно и неприемлемо для всех организаций). Наконец, решение о том, что считать незначительными или серьезными последствиями, полностью зависит от организации. Последствия, катастрофические для небольшой организации, могут быть незначительными или даже пренебрежимо малыми для очень крупной организации.

Зависимости

Чем более значимые и многочисленные бизнес-процессы поддерживаются активом, тем больше ценность этого актива. Должна быть также определена зависимость одних активов от других, поскольку это может влиять на ценность активов. Например, конфиденциальность данных должна сохраняться в течение всего их жизненного цикла, на всех стадиях, включая хранение и обработку, т. е. необходимость обеспечения безопасности хранения данных и программ обработки данных должна быть напрямую связана с ценностью, отображающей конфиденциальность хранящихся и обрабатываемых данных. Также, если бизнес-процесс зависит от целостности определенных данных, создаваемых программой, входные данные этой программы должны иметь соответствующую степень надежности. Кроме того, целостность информации будет зависеть от аппаратных и программных средств, используемых для ее хранения и обработки. Аппаратные средства, в свою очередь, будут зависеть от энергоснабжения и, возможно, от кондиционирования воздуха. Таким образом, информация о зависимостях поможет в определении угроз и особенно в выявлении уязвимостей. Кроме того, это поможет обеспечить правильное присвоение значения ценности активам (благодаря зависимым взаимосвязям), показывая, таким образом, соответствующий уровень защиты.

Ценность активов, от которых зависят другие активы, может изменяться следующим образом:

- если ценность зависимых активов (например данных) ниже или равна ценности рассматриваемого актива (например, программного обеспечения), его ценность остается такой же;
- если ценность зависимых активов (например данных) выше ценности рассматриваемого актива (например, программного обеспечения), его ценность должна быть увеличена в соответствии со степенью зависимости или ценностью других активов.

У организации могут быть некоторые активы, являющиеся доступными более одного раза, такие, как копии компьютерных программ или компьютеры одного и того же вида, использующиеся в большинстве офисов. Этот факт необходимо учитывать при установлении ценности активов. С одной стороны, эти активы легко упустить из виду, поэтому следует заботиться о том, чтобы определить каждый из них; с другой стороны, они могут быть использованы для уменьшения проблем доступности.

Результат

Окончательным результатом этого шага будет перечень активов и их ценности по отношению к раскрытию (сохранение конфиденциальности), модификации (сохранение целостности, подлинности, неотказуемости и учетности), недоступности и разрушению (сохранение доступности и надежности) и восстановительной стоимости.

В.3 Оценка влияния

Инцидент ИБ может оказывать влияние более чем на один актив или только на часть актива. Влияние связано со степенью успешности инцидента. Как следствие, существует важное различие между ценностью актива и влиянием, являющимся результатом инцидента. Влияние рассматривается как имеющее либо незамедлительный (операционеый) эффект, либо будущий (бизнес-) эффект, который включает финансовые и рыночные последствия.

Непосредственное (операционное) влияние бывает прямым или косвенным.

Прямое:

- финансовая восстановительная стоимость потерянного актива (части актива);
- стоимость приобретения, конфигурирования и установки нового актива или резервной копии;
- стоимость приостановленных из-за инцидента операций, пока услуга, предоставляемая активом (активами), не будет восстановлена;
- влияние приводит к нарушению ИБ.

Косвенное:

- издержки упущенных возможностей (финансовые ресурсы, необходимые для замены или восстановления актива, могли быть использованы где-либо еще);
- стоимость прерванных операций;
- возможное злоупотребление информацией, полученной в результате нарушения безопасности;
- нарушение установленных законом или нормативных обязательств;
- нарушение этических норм поведения.

Первая оценка (без мер и средств контроля и управления любого рода) будет оценивать влияние как очень близкое к ценности связанного с этим актива или комбинации активов. При каждой последующей итерации для этого (этих) актива (активов) влияние будет отличаться (обычно будет гораздо ниже) вследствие наличия и эффективности реализованных мер и средств контроля и управления.

Приложение С
(справочное)

Примеры типичных угроз

В приведенной ниже таблице С.1 даны примеры типичных угроз. Этот перечень может использоваться в процессе оценки угроз. Угрозы могут быть умышленными, случайными или связанными с внешней средой (природными) и могут иметь результатом, например ущерб или потерю важных сервисов. В приведенном ниже перечне для каждой угрозы указывается ее происхождение: «У» (умышленная), «С» (случайная), «П» (природная) угроза. «У» обозначает все умышленные действия, направленные на информационные активы, «С» обозначает все действия персонала, которые могут случайно нанести ущерб информационным активам, а «П» обозначает все инциденты, не основанные на действиях персонала. Угрозы перечисляются не в приоритетном порядке.

Таблица С.1 — Примеры типичных угроз

Вид	Угрозы	Происхождение
Физический ущерб	Пожар	С, У, П
	Ущерб, причиненный водой	С, У, П
	Загрязнение	С, У, П
	Крупная авария	С, У, П
	Разрушение оборудования или носителей	С, У, П
	Пыль, коррозия, замерзание	С, У, П
Природные явления	Климатическое явление	П
	Сейсмическое явление	П
	Вулканическое явление	П
	Метеорологическое явление	П
	Наводнение	П
Утрата важных сервисов	Авария системы кондиционирования воздуха или водоснабжения	С, У
	Нарушение энергоснабжения	С, У, П
	Отказ телекоммуникационного оборудования	С, У
Помехи вследствие излучения	Электромагнитное излучение	С, У, П
	Тепловое излучение	С, У, П
	Электромагнитные импульсы	С, У, П
Компрометация информации	Перехват компрометирующих сигналов помех	У
	Дистанционный шпионаж	У
	Прослушивание	У
	Кража носителей или документов	У
	Кража оборудования	У
	Поиск повторно используемых или забракованных носителей	У
	Раскрытие	С, У
	Данные из ненадежных источников	С, У
	Преступное использование аппаратных средств	У
	Преступное использование программного обеспечения	С, У
	Определение местонахождения	У

Окончание таблицы С.1

Вид	Угрозы	Происхождение
Технические неисправности	Отказ оборудования	С
	Неисправная работа оборудования	С
	Насыщение информационной системы	С, У
	Нарушение функционирования программного обеспечения	С
	Нарушение сопровождения информационной системы	С, У
Несанкционированные действия	Несанкционированное использование оборудования	У
	Мошенническое копирование программного обеспечения	У
	Использование контрафактного или скопированного программного обеспечения	С, У
	Искажение данных	У
	Незаконная обработка данных	У
Компрометация функций	Ошибка при использовании	С
	Злоупотребление правами	С, У
	Фальсификация прав	У
	Отказ в осуществлении действий	У
	Нарушение работоспособности персонала	С, У, П

Особое внимание следует уделять источникам угроз, происходящих от деятельности человека (см. таблицу С.2).

Таблица С.2 — Источники угрозы

Источник угрозы	Мотивация	Действие угрозы
Хакер, взломщик	Вызов Самомнение Бунтарство Статус Деньги	Хакерство Социальная инженерия Проникновение в систему, взлом Несанкционированный доступ к системе
Лицо, совершающее компьютерное преступление	Разрушение информации Незаконное раскрытие информации Денежная выгода Несанкционированное изменение данных	Компьютерное преступление (например компьютерное преследование) Мошенническая деятельность (например воспроизведение, выдача себя за другого, перехват) Информационный подкуп Получение доступа обманным путем Проникновение в систему
Террорист	Шантаж Разрушение Использование в личных интересах Месть Политическая выгода Охват среды (передачи данных)	Взрыв/Терроризм Информационная война Системная атака (например распределенный отказ в обслуживании) Проникновение в систему Порча системы
Промышленный шпионаж (сведения секретного характера компании, иностранные правительства, другие правительственные объединения)	Конкурентное преимущество Экономический шпионаж	Получение оборонного преимущества Получение информационного преимущества Экономическая эксплуатация Хищение информации Покушение на неприкосновенность личной жизни

Окончание таблицы С.2

Источник угрозы	Мотивация	Действие угрозы
Промышленный шпионаж (сведения секретного характера компании, иностранные правительства, другие правительственные объединения)		Социальная инженерия Проникновение в систему Несанкционированный доступ к системе (доступ к секретной информации, являющейся собственностью фирмы и/или связанной с технологией)
Инсайдеры (плохо обученные, недовольные, злонамеренные, беспечные, нечестные или уволенные служащие)	Любопытство Самомнение Разведка Денежная выгода Месть Ненамеренные ошибки и упущения (например ошибка ввода данных, ошибка в составлении программы)	Нападение на служащего Шантаж Просмотр информации, являющейся собственностью фирмы Неправильное использование компьютера Мошенничество и хищение Информационный подкуп Вредоносное программное обеспечение (например вирус, логическая бомба, Троянский конь) Продажа информации личного характера «Жучки» в системе Проникновение в систему Вредительство в системе Несанкционированный доступ к системе

Приложение D
(справочное)

Уязвимости и методы оценки уязвимости

D.1 Примеры уязвимостей

В приведенной таблице D.2 даны примеры уязвимостей в различных сферах безопасности, включая примеры угроз, которые могут использовать эти уязвимости. Эти перечни могут быть полезными во время оценки угроз и уязвимостей для определения сценария значимого инцидента. Следует подчеркнуть, что в некоторых случаях эти уязвимости могут использоваться и другими угрозами.

Таблица D.1 — Примеры уязвимостей и угроз

Вид	Примеры уязвимостей	Примеры угроз
Аппаратные средства	Недостаточное техническое обслуживание/неправильная установка носителей данных	Нарушение ремонтопригодности информационных систем
	Отсутствие программ периодической замены	Ухудшение состояния носителей данных
	Чувствительность к влажности, пыли, загрязнению	Образование пыли, коррозия, замерзание
	Чувствительность к электромагнитному излучению	Электромагнитное излучение
	Отсутствие эффективного контроля изменений конфигурации	Ошибка в использовании
	Чувствительность к колебаниям напряжения	Потеря электропитания
	Чувствительность к колебаниям температуры	Метеорологические явления
	Незащищенное хранение	Хищение носителей данных или документов
	Небрежное (безответственное) размещение	Хищение носителей данных или документов
	Неконтролируемое копирование	Хищение носителей данных или документов
Программные средства	Отсутствующее или недостаточное тестирование программных средств	Злоупотребление правами
	Широко известные дефекты программных средств	Злоупотребление правами
	Отсутствие «завершения сеанса» при уходе с рабочего места	Злоупотребление правами
	Списание или повторное использование носителей данных без надлежащего удаления информации	Злоупотребление правами
	Отсутствие «следов» аудита	Злоупотребление правами
	Неверное распределение прав доступа	Злоупотребление правами
	Широко распределенное программное обеспечение	Порча данных
	Применение прикладных программ для несоответствующих, с точки зрения времени, данных	Порча данных
	Сложный пользовательский интерфейс	Ошибка в использовании
	Отсутствие документации	Ошибка в использовании

Продолжение таблицы D.1

Вид	Примеры уязвимостей	Примеры угроз
Программные средства	Неправильные параметры установки	Ошибка в использовании
	Неправильные данные	Ошибка в использовании
	Отсутствие механизмов идентификации и аутентификации, таких, как аутентификация пользователей	Фальсификация прав
	Незащищенные таблицы паролей	Фальсификация прав
	Плохой менеджмент паролей	Фальсификация прав
	Активизация ненужных сервисов	Нелегальная обработка данных
	Недоработанное или новое программное обеспечение	Сбой программных средств
	Нечеткие или неполные спецификации для разработчиков	Сбой программных средств
	Отсутствие эффективного контроля изменений	Сбой программных средств
	Неконтролируемая загрузка и использование программных средств	Тайные действия с программными средствами
	Отсутствие резервных копий	Тайные действия с программными средствами
	Отсутствие физической защиты здания, дверей и окон	Хищение носителей данных или документов
	Отказ в обеспечении отчетов по менеджменту	Неавторизованное использование оборудования
Сеть	Отсутствие подтверждения отправления или получения сообщения	Отказ в осуществлении действий
	Незащищенные линии связи	Перехват информации
	Незащищенный чувствительный трафик	Перехват информации
	Плохая разводка кабелей	Отказ телекоммуникационного оборудования
	Единая точка отказа	Отказ телекоммуникационного оборудования
	Отсутствие идентификации и аутентификации отправителя и получателя	Фальсификация прав
	Ненадежная сетевая архитектура	Дистанционный шпионаж
	Передача паролей в незашифрованном виде	Дистанционный шпионаж
	Неадекватный сетевой менеджмент (устойчивость маршрутизации)	Насыщение информационной системы
	Незащищенные соединения сети общего пользования	Неавторизованное использование оборудования
Персонал	Отсутствие персонала	Нарушение работоспособности персонала
	Неадекватные процедуры набора персонала	Разрушение оборудования или носителей данных
	Недостаточное осознание безопасности	Ошибка в использовании
	Ненадлежащее использование программных и аппаратных средств	Ошибка в использовании

Продолжение таблицы D.1

Вид	Примеры уязвимостей	Примеры угроз
Персонал	Отсутствие осведомленности о безопасности	Ошибка в использовании
	Отсутствие механизмов мониторинга	Нелегальная обработка данных
	Безнадзорная работа внешнего персонала или персонала организации, занимающегося уборкой	Хищение носителей данных или документов
	Отсутствие политик по правильному использованию телекоммуникационной среды и обмена сообщениями	Неавторизованное использование оборудования
Место функционирования организации	Неадекватное или небрежное использование физического управления доступом к зданиям и помещениям	Ухудшение состояния носителей данных
	Размещение в местности, предрасположенной к наводнениям	Затопление
	Нестабильная электрическая сеть	Отсутствие электропитания
	Отсутствие физической защиты здания, дверей и окон	Хищение аппаратуры
Организация	Отсутствие формальной процедуры для регистрации и снятия с регистрации пользователей	Злоупотребление правами
	Отсутствие формального процесса для пересмотра (надзора) прав доступа	Злоупотребление правами
	Отсутствие или недостаточные условия (касающиеся безопасности) в договорах с клиентами и/или третьими сторонами	Злоупотребление правами
	Отсутствие процедуры, касающейся мониторинга средств обработки информации	Злоупотребление правами
	Отсутствие регулярных аудитов (надзора)	Злоупотребление правами
	Отсутствие процедур идентификации и оценки риска	Злоупотребление правами
	Отсутствие сообщений об ошибках, зафиксированных в журнале регистрации администратора и оператора	Злоупотребление правами
	Неадекватная ответственность за техническое обслуживание	Нарушение обслуживания информационной системы
	Отсутствующее или неудовлетворительное соглашение об уровне сервиса	Нарушение обслуживания информационной системы
	Отсутствие процедуры контроля изменений	Нарушение обслуживания информационной системы
	Отсутствие формальной процедуры контроля документации, касающейся системы менеджмента ИБ	Порча данных
	Отсутствие формальной процедуры надзора за записями системы менеджмента ИБ	Порча данных
	Отсутствие формального процесса санкционирования общедоступной информации	Данные из ненадежных источников
	Отсутствие надлежащего распределения обязанностей по обеспечению информационной безопасности	Отказ в осуществлении деятельности

Окончание таблицы D.1

Вид	Примеры уязвимостей	Примеры угроз
Организация	Отсутствие планов обеспечения непрерывности бизнеса	Отказ оборудования
	Отсутствие политики по использованию электронной почты	Ошибка в использовании
	Отсутствие процедур введения программного обеспечения в операционные системы	Ошибка в использовании
	Отсутствие записей в журнале регистрации администратора и оператора	Ошибка в использовании
	Отсутствие процедур для обработки секретной информации	Ошибка в использовании
	Отсутствие обязанностей по обеспечению информационной безопасности в должностных инструкциях	Ошибка в использовании
	Отсутствие или недостаточные условия (касающиеся информационной безопасности) в договорах со служащими	Нелегальная обработка данных
	Отсутствие оговоренного дисциплинарного процесса в случае инцидента безопасности	Хищение оборудования
	Отсутствие формальной политики по использованию портативных компьютеров	Хищение оборудования
	Отсутствие контроля над активами, находящимися за пределами организации	Хищение оборудования
	Отсутствующая или неудовлетворительная политика «чистого стола и пустого экрана»	Хищение носителей информации или документов
	Отсутствие авторизации средств обработки информации	Хищение носителей информации или документов
	Отсутствие установленных механизмов мониторинга нарушений безопасности	Хищение носителей информации или документов
	Отсутствие регулярных проверок, проводимых руководством	Неавторизованное использование оборудования
	Отсутствие процедур сообщения о слабых местах безопасности	Неавторизованное использование оборудования
	Отсутствие процедур, обеспечивающих соблюдение прав на интеллектуальную собственность	Использование контрафактных или копированных программных средств

D.2 Методы оценки технических уязвимостей

Профилактические методы, такие, как тестирование информационной системы, могут быть использованы для эффективного выявления уязвимостей в зависимости от критичности системы информационных и телекоммуникационных технологий (ИКТ) и доступных ресурсов (например, выделенных фондов, доступной технологии, лиц, имеющих опыт проведения тестирования). Методы тестирования включают:

- автоматизированные инструментальные средства поиска уязвимостей;
- тестирование и оценка безопасности;
- тестирование на проникновение;
- проверка кодов.

Автоматизированные инструментальные средства поиска уязвимостей используются для просмотра группы хостов или сети на предмет наличия известных уязвимых сервисов (например, система разрешает использование анонимного протокола передачи файлов, ретрансляцию отправленной почты). Следует, однако, отметить,

что некоторые из потенциальных уязвимостей, идентифицированных автоматизированными инструментальными средствами поиска уязвимостей, могут не представлять реальных уязвимостей в контексте системной среды. Например некоторые из этих средств поиска определяют потенциальные уязвимости, не учитывая среду и требования сайта. Некоторые из уязвимостей, отмеченных автоматизированными инструментальными средствами поиска уязвимостей, могут в действительности не быть уязвимостями для конкретного сайта, а быть сконфигурированными таким образом, как этого требует среда. Таким образом, этот метод тестирования может давать ошибочные результаты исследования.

Другим методом, который может использоваться для выявления уязвимостей системы ИКТ во время процесса оценки риска, является тестирование и оценка безопасности. Он включает в себя разработку и осуществление плана тестирования (например, сценарий тестирования, процедуры тестирования и ожидаемые результаты тестирования). Цель тестирования безопасности системы состоит в тестировании эффективности мер и средств контроля и управления безопасности системы ИКТ, которые были применены в операционной среде. Задача заключается в том, чтобы удостовериться, что применяющиеся меры и средства контроля и управления соответствуют утвержденной спецификации безопасности для программных и аппаратных средств, обеспечивают реализацию политики безопасности организации или соответствуют отраслевым стандартам.

Тестирование на проникновение может использоваться как дополнение к проверке мер и средств контроля и управления безопасности и обеспечение защиты различных аспектов системы ИКТ. Когда тестирование на проникновение используется в процессе оценки риска, оно может применяться для оценки способности системы ИКТ противостоять умышленным попыткам обойти защиту системы. Его задача состоит в тестировании системы ИКТ с точки зрения источника угрозы и выявлении потенциальных сбоев в структурах защиты системы ИКТ.

Проверка кодов является наиболее тщательным (но также и самым дорогостоящим) способом оценки уязвимостей.

Результаты этих видов тестирования безопасности помогут выявить уязвимости системы.

Важно отметить, что методы и средства тестирования на проникновение могут давать ложные результаты, если уязвимость не была успешно использована. Чтобы использовать конкретную уязвимость, нужно знать точную систему/приложение/исправления, установленные на тестируемой системе. Если во время тестирования эти данные неизвестны, успешное использование конкретной уязвимости может быть невозможным (например достичь удаленного обратного соединения), однако по-прежнему возможно взломать или перезапустить тестируемый процесс или систему. В таком случае тестируемый объект тоже должен считаться уязвимым.

Методы могут включать следующие виды деятельности:

- опрос сотрудников и пользователей;
- анкетирование;
- физический осмотр;
- анализ документов.

Приложение Е
(справочное)

Подходы к оценке риска информационной безопасности

Е.1 Высокоуровневая оценка риска информационной безопасности

Высокоуровневая оценка дает возможность определять приоритеты и хронологию действий. По разным причинам, например, бюджетным, одновременная реализация всех мер и средств контроля и управления не всегда возможна, и с помощью процесса обработки риска могут рассматриваться только наиболее критичные риски. Также может быть преждевременным начинать детальный менеджмент риска, если реализация предусматривается только через год или два. Для достижения этой цели высокоуровневая оценка может начаться с высокоуровневой оценки последствий, а не с систематического анализа угроз, уязвимостей, активов и последствий.

Причиной начать с высокоуровневой оценки является синхронизация с другими планами, связанными с управлением изменениями (или обеспечением непрерывности бизнеса). Например не имеет смысла обеспечивать полную защиту системы или приложения, если в ближайшем будущем планируется привлечь для работы с ними внешние ресурсы, хотя, возможно, стоит выполнить оценку риска, чтобы определить целесообразность заключения договора о привлечении внешних ресурсов.

Особенности итерации высокоуровневой оценки риска могут включать следующее.

Высокоуровневая оценка риска может быть связана с более глобальным рассмотрением организации и ее информационных систем, когда технологические аспекты рассматриваются как независимые от проблем бизнеса. В результате этого анализ контекста больше сосредотачивается на бизнес- и эксплуатационной среде, чем на технологических компонентах.

Высокоуровневая оценка риска может быть связана с более ограниченным перечнем угроз и уязвимостей, сгруппированных в определенных сферах, или для ускорения процесса она может сосредотачиваться на сценариях риска или нападений вместо их компонентов.

Риски, представленные в высокоуровневой оценке риска, часто носят более общий характер, чем конкретно идентифицированные риски. Когда сценарии или угрозы группируются в сферы, обработка риска предлагает перечни мер и средств контроля и управления для конкретной сферы. Деятельность по обработке риска затем стремится, прежде всего, предложить и выбрать общие меры и средства контроля и управления, являющиеся действенными во всей системе.

Вследствие того, что при использовании высокоуровневой оценки риска редко рассматриваются технологические детали, она более уместна для обеспечения организационных и нетехнических средств контроля, а также аспектов менеджмента технических средств контроля или ключевых и общих технических защитных мер, таких, как резервное копирование и антивирусные программы.

Преимущества высокоуровневой оценки риска таковы:

- включение первоначального простого подхода, вероятно, необходимо для одобрения программы оценки риска;
- должно быть возможным создание стратегической картины программы обеспечения безопасности организации, т. е. она будет действовать как хорошая помощь в планировании;
- ресурсы и денежные средства могут быть применены там, где они наиболее полезны, и системы, вероятно, больше всего нуждающиеся в защите, будут рассмотрены первыми.

Поскольку первоначальные анализы риска выполняются на высоком уровне и потенциально могут быть менее точными, единственный возможный недостаток состоит в том, что некоторые бизнес-процессы или системы не могут быть определены как нуждающиеся во вторичной, более детальной оценке риска. Этого можно избежать, если существует адекватная информация обо всех аспектах организации, ее информации и системах, включая информацию, полученную в результате оценка инцидентов ИБ.

При использовании высокоуровневой оценки риска рассматривается ценность для бизнеса информационных активов и риски с точки зрения бизнеса организации. В первой точке принятия решения (см. рисунок 1) несколько факторов помогают в определении того, является ли высокоуровневая оценка адекватной для обработки риска; этими факторами могут быть:

- бизнес-цели, которые должны быть достигнуты посредством использования различных информационных активов;
- степень зависимости бизнеса организации от каждого информационного актива, т. е., являются ли функции, которые организация считает критичными для своего выживания или эффективного ведения бизнеса, зависящими от каждого актива или от конфиденциальности, целостности, доступности, неотказуемости, учетности, подлинности и надежности информации, хранящейся и обрабатываемой в данном активе;
- уровень инвестиций в каждый информационный актив с точки зрения разработки, поддержки или замены актива;
- информационные активы, которым организация напрямую присваивает ценность.

После того как эти факторы оценены, решение становится проще. Если цели актива крайне важны для ведения бизнеса организации или если активы имеют высокий уровень риска, то для конкретного информационного актива (или его части) должна быть проведена вторая итерация, детальная оценка риска.

Здесь применяется следующее общее правило: если отсутствие ИБ может привести к значительным неблагоприятным последствиям для организации, ее бизнес-процессов или ее активов, то необходима вторая итерация оценки риска на более детальном уровне для идентификации потенциальных рисков.

Е.2 Детальная оценка риска информационной безопасности

Детальный процесс оценки риска ИБ включает тщательное определение и установление ценности активов, оценку угроз этим активам и оценку уязвимостей. Результаты этой деятельности используются для оценки рисков, а затем для определения способа обработки риска.

Детальная последовательность действий обычно требует продолжительного времени, значительных усилий и компетентности и поэтому может быть наиболее пригодной для информационных систем с высоким уровнем риска.

Окончательным этапом детальной оценки риска ИБ является оценка общих рисков, находящаяся в фокусе данного приложения.

Последствия могут оцениваться несколькими методами, включая количественные, например денежные, и качественные меры (с использованием таких определений, как «умеренные» или «серьезные») или их комбинации. Для оценки вероятности возникновения угрозы должны быть установлены временные рамки, в которых актив будет обладать ценностью или нуждаться в защите. На вероятность возникновения конкретной угрозы оказывают влияние следующие факторы:

- привлекательность актива или возможное воздействие — применимо при рассмотрении умышленной угрозы со стороны персонала;
- простота преобразования актива, использующего уязвимость за вознаграждение, — применимо при рассмотрении умышленной угрозы со стороны персонала;
- технические возможности действующего фактора угрозы — применимо при рассмотрении умышленной угрозы со стороны персонала;
- чувствительность уязвимости к использованию — применимо к техническим и нетехническим уязвимостям.

Во многих методах используются таблицы и объединяются субъективные и эмпирические меры. Важно, чтобы организация использовала метод, который является для нее наиболее удобным, в котором организация уверена и который будет обеспечивать повторяемость результатов. Несколько примеров, основанных на таблицах методов, приведено ниже.

Е.2.1 Пример 1 — Таблица с заранее определенными значениями

В методах оценки риска данного вида фактические или предполагаемые физические активы оцениваются с точки зрения стоимости замены или восстановления (т. е. количественные меры). Эта стоимость затем переводится в ту же качественную шкалу, которая используется для информации (см. ниже). Фактические или предполагаемые программные активы оцениваются таким же образом, как и физические активы, — определяется стоимость приобретения или восстановления, а затем переводится в ту же качественную шкалу, которая используется для информации. Кроме того, если считается, что любая прикладная программа имеет собственные присущие ей требования в отношении конфиденциальности или целостности (например, если исходный текст программы сам по себе является коммерчески критичным), она оценивается таким же образом, как и информация.

Ценность информации определяется из опросов отдельных представителей бизнес-менеджмента (владельцев информации), которые могут авторитетно судить о данных с целью определения ценности и критичности фактически используемых данных или данных, которые должны храниться, обрабатываться или оцениваться. Опросы облегчают оценку значимости и критичности информации с точки зрения сценариев наихудших вариантов, возникновение которых можно предполагать исходя из неблагоприятных последствий для бизнеса, обусловленных несанкционированным раскрытием, несанкционированной модификацией, недоступностью в течение различных периодов времени и разрушением.

Ценность определяется использованием принципов определения ценности информации, которые охватывают следующие проблемы:

- личная безопасность;
- личная информация;
- юридические и нормативные обязательства;
- соблюдение законов;
- коммерческие и экономические интересы;
- финансовые потери/нарушение деятельности;
- общественный порядок;
- политика и операции бизнеса;
- потеря «неосязаемого капитала»;
- договор или соглашение с клиентом.

Принципы облегчают определение значений ценности по числовой шкале, как, например, на шкале от 0 до 4, показанной в приведенном ниже примере (см. таблицу Е.1а), осуществляя таким образом присвоение количественных значений, если это возможно и обоснованно, и качественных значений там, где количественные значения невозможны, например в случае создания опасности для человеческой жизни.

Следующим важным этапом деятельности является заполнение ряда опросных листов для каждого вида угрозы, каждой группы активов, с которой связан данный вид угрозы, чтобы сделать возможной оценку уровней угроз (вероятности возникновения) и уровней уязвимостей (простоты использования угроз для создания неблагоприятных последствий). Каждый ответ на вопрос дает баллы. Эти баллы складываются с использованием базы знаний и сравниваются с диапазонами. Это идентифицирует уровни угроз, например, по шкале от высокого до низкого и, аналогично, уровни уязвимостей, как показано в таблице Е.1*а*, с проведением различий между видами последствий. Информация для заполнения опросных листов должна собираться из опросов технического персонала, представителей отдела кадров, из данных обследований фактического месторасположения и проверки документации.

Ценность активов, уровни угроз и уязвимостей, относящиеся к каждому виду последствий, приводятся в табличной форме (матрице), представленной в таблице Е.1*а*, чтобы для каждой комбинации идентифицировать соответствующую меру риска на основе шкалы от 0 до 8. Значения заносятся в матрицу структурированным образом.

Таблица Е.1*а* — Ценность активов, уровни угроз и уязвимостей

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	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 актива рассматриваются уместные уязвимости и соответствующие им угрозы. Если существует уязвимость без соответствующей угрозы или угроза без соответствующей уязвимости, то в настоящее время риск отсутствует (но следует принимать меры в случае изменения этой ситуации). Соответствующая строка в таблице устанавливается по значению ценности актива, а соответствующая колонка устанавливается по степени вероятности возникновения угрозы и простоте использования. Например если актив имеет ценность 3, угроза является «высокой», а уязвимость «низкой», то мера риска будет равна 5. Предположим, что актив имеет ценность 2 и, например для модификации уровень угрозы является «низким», а простота использования «высокой», тогда мера риска будет равна 4. Размер таблицы с точки зрения числа категорий вероятности угроз, категорий простоты использования и числа категорий определения ценности активов может быть адаптирован к потребностям организации. Для дополнительных мер риска потребуются дополнительные колонки и строки. Ценность данного подхода заключается в ранжировании рисков, требующих рассмотрения.

Аналогичная матрица, как показано в таблице Е.1*а*, является результатом рассмотрения степени вероятности сценария инцидента, отображенного на количественно оцененное влияние бизнеса. Вероятность сценария инцидента дана посредством угрозы, использующей уязвимость с определенной вероятностью. Таблица отображает эту вероятность влияния на бизнес, связанную со сценарием инцидента. Получаемый в результате риск измеряется по шкале от 0 до 8, может быть оценен относительно критериев принятия риска. Данная шкала рисков может также отображаться на простой общий рейтинг рисков, например следующим образом:

- низкий риск: 0—2;
- средний риск: 3—5;
- высокий риск: 6—8.

Таблица Е.1*b* — Степень вероятности сценария инцидента

	Степень вероятности сценария инцидента	Очень низкая (очень маловероятная)	Низкая (маловероятная)	Средняя (возможная)	Высокая (вероятная)	Очень высокая (частая)
Влияние на бизнес	Очень низкое	0	1	2	3	4
	Низкое	1	2	3	4	5
	Среднее	2	3	4	5	6
	Высокое	3	4	5	6	7
	Очень высокое	4	5	6	7	8

Е.2.2 Пример 2 — Ранжирование угроз посредством мер риска

Матрица или таблица может быть использована, чтобы связать факторы последствий (ценность активов) с вероятностью возникновения угрозы (принимая в расчет аспекты уязвимости). Первый шаг состоит в оценке последствий (ценности активов) по заранее определенной шкале, например от 1 до 5, для каждого находящегося под угрозой актива (колонка «*b*» в таблице Е.2). Второй шаг состоит в оценке степени вероятности возникновения угрозы по заранее определенной шкале, например от 1 до 5, для каждой угрозы (колонка «*c*» в таблице Е.2). Третий шаг состоит в вычислении меры риска путем умножения ($b \times c$). Наконец, угрозы могут быть ранжированы в порядке соответствующей меры риска. Отметим, что в этом примере «1» соответствует наименьшим последствиям и самой низкой степени вероятности возникновения.

Таблица Е.2 — Ранжирование угроз посредством мер риска

Идентификатор угрозы (*a*)	Последствия (ценность актива) (*b*)	Степень вероятности возникновения угрозы (*c*)	Мера риска (*d*)	Ранжирование угроз (*e*)
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Как показано выше, это является процедурой, позволяющей сопоставлять и ранжировать в порядке назначенных приоритетов различные угрозы с разными последствиями и вероятностью возникновения. В некоторых случаях будет необходимо результаты, полученные здесь по эмпирическим шкалам, представлять в денежном выражении.

Е.2.3 Пример 3 — Оценка ценности для вероятности рисков и их возможных последствий

В этом примере особое внимание уделяется последствиям инцидентов ИБ (сценариям инцидентов) и определению того, каким системам следует отдавать предпочтение. Это выполняется путем оценки двух значений — для каждого актива и риска, комбинация которых будет определять баллы для каждого актива. Когда суммируются все баллы активов системы, определяется мера риска для этой системы.

Сначала каждому активу присваивается ценность. Это значение связано с возможными неблагоприятными последствиями, которые могут возникать, если актив находится под угрозой. Эта ценность присваивается активу для каждого случая возникновения соответствующей активу угрозы. Потом оценивается значение вероятности. Оно оценивается исходя из комбинации степени вероятности возникновения угрозы и простоты использования уязвимости (см. таблицу Е.3, выражающую вероятность осуществления сценария инцидентов).

Таблица Е.3 — Оценка ценности для степени вероятности и возможных последствий рисков

Уровни угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение степени вероятности	0	1	2	1	2	3	2	3	4

Затем, находя пересечение линий значения ценности актива и значения степени вероятности в таблице Е.4, присваиваются баллы активу/угрозе. Баллы актива/угрозы подсчитываются, чтобы получить итоговые баллы для актива. Эта цифра может использоваться для проведения различий между активами, составляющими часть системы.

Таблица Е.4 — Ценности актива и значения степени вероятности

Значение степени вероятности	Ценность актива				
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

Окончательный шаг заключается в подсчете всех итоговых баллов активов системы, чтобы получить баллы системы. Эта цифра может использоваться для проведения различий между системами и определения того, защите какой системы следует отдавать предпочтение.

В последующих примерах все значения выбраны случайно.

Предположим, что система С имеет три актива: А1, А2 и А3. Также предположим, что существуют две угрозы У1 и У2, применимые к системе С. Пусть ценность актива А1 будет 3, допустим также, что ценность актива А2 равна 2, а ценность актива А3 равна 4.

Если для А1 и У1 степень вероятности угрозы низкая, а простота использования уязвимости средняя, то значение степени вероятности равно 1 (см. таблицу Е.3).

Баллы для актива/угрозы А1/У1 могут быть выведены из таблицы Е.4 на пересечении линий ценности актива 3 и значения степени вероятности 1, т. е. равные 4. Аналогичным образом, пусть для А1/У2 степень вероятности угрозы будет средней, а простота использования уязвимости будет высокой, что даст для А1/У2 значение 6.

Теперь могут быть вычислены итоговые баллы актива А1У, т. е. равные 10. Итоговые баллы актива вычисляются для каждого актива и применимой угрозы. Итоговые баллы системы вычисляются путем суммирования А1У + А2У + А3У, что дает СУ.

Различные системы могут сравниваться для установления приоритетов, а также различных активов в пределах одной системы.

Приведенные выше примеры показаны с точки зрения информационных систем, однако аналогичный подход может быть применен и к бизнес-процессам.

Приложение F
(справочное)

Ограничения, относящиеся к снижению риска

При рассмотрении ограничений, относящихся к снижению риска, нужно принимать в расчет следующие ограничения.

Временные ограничения

Может существовать много видов временных ограничений. Например меры и средства контроля и управления должны быть реализованы в течение временного периода, приемлемого для руководства организации. Еще один вид временного ограничения — могут ли мера и средство контроля и управления быть реализованы в течение срока службы системы или информации? Третьим видом временного ограничения может быть период времени, который руководство организации считает приемлемым для подверженности определенному риску.

Финансовые ограничения

Реализация или поддержка мер и средств контроля и управления не должна быть более дорогостоящей, чем ценность активов, которые они предназначены защищать, за исключением случаев, когда обеспечение соответствия является обязательным (например по законодательству). Должны прилагаться все усилия, чтобы не превысить установленный бюджет и достичь финансовой выгоды благодаря использованию мер и средств контроля и управления. Однако в некоторых случаях может не быть возможности достичь желаемой безопасности и уровня принятия риска вследствие бюджетных ограничений. Поэтому для разрешения такой ситуации потребуется решение руководства организации.

Следует проявлять большую осторожность, если из-за сокращения бюджета сокращается количество или качество мер и средств контроля и управления, подлежащих реализации, так как это может приводить к неявному сохранению более высокого риска, чем планировалось. Бюджет, установленный для мер и средств контроля и управления, должен использоваться как ограничивающий фактор, но со значительной осторожностью.

Технические ограничения

Технических проблем, таких, как совместимость программ или аппаратных средств, легко можно избежать, если учитывать их во время выбора мер и средств контроля и управления. Кроме того, реализация использующихся ранее мер и средств контроля и управления для существующего процесса или системы часто затрудняется техническими ограничениями. Эти трудности могут сдвигать баланс мер и средств контроля и управления в сторону процедурных и физических аспектов обеспечения безопасности. Может возникнуть необходимость в пересмотре программы обеспечения ИБ для достижения целей безопасности. Это может происходить, когда меры и средства контроля и управления не соответствуют ожидаемым результатам снижения риска без уменьшения производительности.

Операционные ограничения

Операционные ограничения, такие, как необходимость работать в режиме 24×7, выполняя, кроме того, резервное копирование, могут приводить к сложной и дорогостоящей реализации мер и средств контроля и управления, если они не были заложены в проект с самого начала.

Культурные ограничения

Культурные ограничения, касающиеся выбора мер и средств контроля и управления, могут быть характерны для страны, сектора, организации или даже отдела в организации. Не все меры и средства контроля и управления могут применяться во всех странах. Например возможно реализовать досмотр сумок в странах Европы, но не в ряде стран Ближнего Востока. Культурные аспекты нельзя игнорировать, потому что многие меры и средства контроля и управления зависят от активной поддержки персонала. Если сотрудники не понимают необходимости применения мер и средств контроля и управления или не считают их приемлемыми с точки зрения культурных традиций, с течением времени эти меры и средства контроля и управления станут неэффективными.

Этические ограничения

Этические ограничения могут иметь серьезные последствия для мер и средств контроля и управления, поскольку этические принципы меняются на основе норм морали. Это может препятствовать реализации таких мер и средств контроля и управления, как, например сканирование сообщений электронной почты в некоторых странах. Секретность информации может также меняться в зависимости от региональных или государственных этических принципов. Они могут в большей степени касаться одних отраслей экономики и в меньшей степени — других, например правительственного сектора и отрасли здравоохранения.

Ограничения, связанные с окружающей средой

Факторы окружающей среды, такие, как доступное пространство, экстремальные климатические условия, окружающая природная и городская среда, могут влиять на выбор мер и средств контроля и управления. Например обеспечение сейсмостойкости может быть необходимым в некоторых странах, но ненужным в других.

Юридические ограничения

Правовые факторы, такие, как обеспечение защиты личных данных или положения уголовного кодекса, касающиеся обработки информации, могут оказывать влияние на выбор мер и средств контроля и управления.

Обеспечение соответствия законодательным и нормативным требованиям может предписывать использование определенных видов мер и средств контроля и управления, включая обеспечение защиты данных и финансовый аудит, но может также не допускать использования некоторых мер и средств контроля и управления, например шифрования. Другие законы и нормы, такие, как трудовое право, предписания пожарного отдела, правила техники безопасности и охраны здоровья и нормы экономического сектора и др., тоже могут влиять на выбор мер и средств контроля и управления.

Простота использования

Неудовлетворительное взаимодействие «человек—технология» будет вызывать ошибки персонала и может приводить к бесполезности мер и средств контроля и управления. Меры и средства контроля и управления должны выбираться с целью обеспечения оптимальной простоты использования наряду с достижением приемлемого уровня остаточного риска для бизнеса. Применение трудно используемых мер и средств контроля и управления будет влиять на их эффективность, так как пользователи могут пытаться обходить или игнорировать их, насколько это возможно. Сложные средства управления доступом, применяемые в организации, могут способствовать использованию альтернативных несанкционированных методов доступа.

Кадровые ограничения

Следует учитывать доступность и затраты на оплату совокупности специализированных навыков для реализации мер и средств контроля и управления, а также возможность перемещения персонала между подразделениями организации при неблагоприятных условиях работы. У персонала может отсутствовать требуемая квалификация для реализации планируемых мер и средств контроля и управления или ее получение может быть крайне затратным для организации. Другие аспекты, например тенденция к дискриминации одних сотрудников другими, не проходившими проверку надежности, могут иметь серьезные последствия для политик безопасности и практических приемов обеспечения безопасности. Кроме того, необходимость найма на работу специалистов соответствующей квалификации и нахождение таких кандидатур может приводить к найму до завершения проверки надежности. Требование завершения проверки надежности до оформления найма является обычной и наиболее безопасной практикой.

Ограничения, касающиеся интеграции новых и существующих мер и средств контроля и управления

На интеграцию новых мер и средств контроля и управления в существующей инфраструктуре и взаимозависимость мер и средств контроля и управления часто не обращают внимания. Новые меры и средства контроля и управления могут быть трудно реализуемыми при наличии несочетаемости или несовместимости с существующими мерами и средствами контроля и управления. Например план по использованию биометрических признаков для осуществления физического контроля доступа может вступать в противоречие с существующей системой управления доступом, основанной на наборе PIN-кода. Стоимость изменения мер и средств контроля и управления с существующих на запланированные должна быть добавлена к общим расходам на обработку риска. Возможно, что реализация выбранных мер и средств контроля и управления будет невозможна из-за несочетаемости или несовместимости с существующими мерами и средствами контроля и управления.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ИСО/МЭК 27002:2005	—	*
ИСО/МЭК Руководство 73:2002	MOD	ГОСТ Р 51897—2002 «Менеджмент риска. Термины и определения»
ИСО/МЭК 16085:2006	IDT	ГОСТ Р ИСО/МЭК 16085—2007 «Менеджмент риска. Применения в процессах жизненного цикла систем и программного обеспечения»

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

Примечание — В настоящей таблице использованы следующие условные обозначение степени соответствия стандарта:
- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Библиография

[1] ИСО/МЭК Руководство 73:2002 (ISO/IEC Guide 73:2002) Менеджмент риска. Словарь. Руководство по применению в стандартах (Risk management. Vocabulary. Guidelines for use in standards)

[2] ИСО/МЭК 16085:2006 (ISO/IEC 16085: 2006) Проектирование систем и программного обеспечения. Процессы жизненного цикла. Менеджмент риска (Systems and Software Engineering. Life Cycle Processes. Risk Management)

[3] Менеджмент риска (AS/NZS 4360: 2004 Risk Management)

[4] Специальная публикация НИСТ 800—12. Введение в компьютерную безопасность. Справочник НИСТ (NIST Special Publication 800—12, An Introduction to Computer Security: The NIST Handbook)

[5] Специальная публикация НИСТ 800—30. Руководство по менеджменту риска для систем информационных технологий. Рекомендации для национального института стандартов и технологий (NIST Special Publication 800—30, Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology)

УДК 001.4:025.4:006.354 ОКС 35.040

Ключевые слова: менеджмент риска информационной безопасности, риск информационной безопасности, процесс менеджмента риска, оценка риска, обработка риска, принятие риска, коммуникация риска, мониторинг риска, пересмотр риска, система менеджмента информационной безопасности, информационная безопасность, информационная система

Редактор *К. С. Савинова*
Технический редактор *В. Н. Прусакова*
Корректор *Л. Я. Митрофанова*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 26.05.2011. Подписано в печать 14.07.2011. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 5,58. Уч.-изд. л. 5,35. Тираж 176 экз. Зак. 529

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