МЕЖДУНАРОДНЫЙ СТАНДАРТ

BS ISO/IEC 27005:2011

ISO/IEC 27005

ВТОРОЕ ИЗДАНИЕ
2011-06-10

Информационная технология - Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности

***Technologies de l'information — Techniques de sécurité — Gestion du* risque en sécurité de l'information**

Номер ссылки ISO/IEC 27005:2011 (SE)

Данный документ – первая редакция технического перевода британского стандарта, ставшего международным - BS ISO/IEC 27005:2011. Автор перевода – заместитель директора департамента инфраструктурных решений по информационной безопасности АО «СИТРОНИКС ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УКРАИНА» Гонцул В.А.

Данный стандарт:

- предоставляет руководство по менеджменту риска информационной безопасности в организации, поддерживая, в частности требования к СМИБ в соответствии с ISO/IEC 27001;

- не предоставляет какой-либо конкретной методологии по менеджменту риска информационной безопасности;

- выбор подхода к менеджменту риска осуществляется организацией, применяющих этот стандарт и зависит, например, от области применения СМИБ, контекста менеджмента риска или сферы деятельности.

- 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.

Общие примечания переводчика по переводу в данной редакции:

- напоминаю, что в связи с принятием ISO/IEC 27005, ISO/IEC 13335-3:1999 и ISO/IEC 13335-4:2001 становятся недействительными, т.е. необходимо обращать внимание Заказчика, что ДСТУ ISO/IEC 13335-3:2003 и ДСТУ ISO/IEC 13335-4:2005 уже потеряли актуальность (на Украине на данный момент ISO/IEC 27005 не принят, поэтому вышеуказанные ДСТУ являются действующими стандартами!);

- для правильного понимания контекста выражений в стандарте переводчиком включены комментарии;

- данные стандарт отличается от ISO/IEC 27005:2008 гармонизацией терминов с ISO/IEC 27000:2009 и Руководством ISO 73:2009[1];

- прошу так же обратить внимание на уже осуществлённые переводы ISO 31000:2009 «Менеджмент риска – Принципы и руководящие указания» (см. здесь: http://www.tnpa.by/tnpa/TnpaFiles/pdf/STB_ISO_31000.pdf) и ISO Guide 73-2009 (см. здесь: http://www.tnpa.by/tnpa/TnpaFiles/pdf/STB_ISO_Guide_73.pdf) и конечно же проект ГОСТ Р ISO/IEC 27005, подготовленный ООО "НПФ "Кристалл" и ФГУ "ГНИИИ ПТЗИ ФСТЭК России на основе собственного аутентичного перевода стандарта ISO/IEC 27005:2008.

[1] Примечание переводчика:
Доставшийся мне швейцарский ISO 73:2009 иногда не совпадает по примечаниям к терминам ISO 27005:2011. Печально, но факт!!!

Оглавление

Предисловие

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) образуют специализированную систему международной стандартизации. Государственные организации, являющиеся членами ISO или IEC, участвуют в разработке международных стандартов посредством технических комитетов, созданных соответствующими организациями для работы в определённых технических областях. Международные технические комитеты ISO и IEC сотрудничают в областях, представляющих интерес для обеих организаций.

Кроме того, совместно с ISO и IEC в работе участвуют другие государственные и негосударственные международные организации.

Подготовка международных стандартов ведётся согласно правилам, изложенным во второй части Директив ISO/IEC.

Разработанные варианты международных стандартов, принятые объединённым техническим комитетом, передаются организациям-участникам для утверждения.

Для принятия стандарта в качестве международного необходимо одобрение не менее 75% национальных органов, участвующих в голосовании.

Необходимо обратить внимание на то, что некоторые элементы данного международного стандарта могут попадать под действие патентных прав.

Организации ISO и IEC не должны нести ответственности за определение каких-либо из этих патентных прав.

ISO/IEC 27001 был подготовлен совместным техническим комитетом ISO/IEC JTC 1, Информационных технологий, Подкомиссией технологий безопасности SC 27.

Этот второй выпуск ISO/IEC 27005 отменяет и заменяет первое издание ISO/IEC 27005:2008, которое было пересмотрено техническим комитетом.

Введение

Этот интернациональный стандарт обеспечивает рекомендации для менеджмента риском информационной безопасности в организации, в особенности поддерживая требования СМИБ[2] (ISMS) согласно ISO/IEC 27001. Однако этот интернациональный стандарт не обеспечивает определённой методологии для менеджмента рисков информационной безопасности. Этот стандарт предназначен для определения в организации подхода к менеджменту рисков в зависимости, например, от области действия СМИБ, области применения менеджмента рисков или сектора промышленности. Чтобы осуществить требования СМИБ многие существующие методологии могут воспользоваться структурой, описанной в этом интернациональном стандарте.

Данный 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.

[2] Примечание переводчика – сокращённая аббревиатура ISMS (Information Security Management System) – это СМИБ (система менеджмента информационной безопасностью) в некоторых документах, например СОУ Н НБУ, упоминается значение как СУИБ (система управления информационной безопасностью), в российских используется значение СМИБ.

1 Область (границы) применения

Данный стандарт обеспечивает рекомендации для менеджмента рисков информационной безопасности, которые включают информацию и менеджмент рисков безопасности технологий телекоммуникации.

Данный стандарт поддерживает общие концепции, определённые в ISO/IEC 27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска.

Знание концепций, моделей, процессов и терминологии, изложенных в ISO/IEC 27001 и ISO/IEC 27002, важно для полного понимания данного интернационального стандарта.

Данный 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

Следующие упомянутые документальные источники необходимы для применения данного документа. Для документов с обозначенной датой применимо только упоминаемое издание. Для документов без обозначенной даты применимо последнее издание упомянутого документа (включая любые поправки).

ISO/IEC 27001:2005, Информационная технология - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности - Требования.

ISO/IEC 27002:2005, Информационная технология - Методы и средства обеспечения безопасности - Кодекс установившейся практики для менеджмента информационной безопасности.

3 Определения

В этом документе целенаправленно применяются термины и определения ISO/IEC 27000, которые следуют использовать в дальнейшем.

Примечания:

Различия в определениях между ISO/IEC 27005:2008 и этим международным стандартом показаны в Приложении G.

3.1 Последствия (consequence):

результат события (3.3), влияющего на цели.

Примечания:

1. Результатом события может быть одно или более последствий
2. Последствия могут быть ранжированы от позитивных до негативных. Однако применительно к аспектам безопасности последствия всегда негативные.
3. Последствия могут быть выражены качественно и количественно.
4. Начальные последствия могут вырасти через цепную реакцию.

3.2 Менеджмент (control):

мера, которая изменяет риск (определение 3.9).

[Руководство ISO 73:2009]

Примечания:

1. Средства менеджмента для информационной безопасности включают любой процесс, политику, процедуру, направляющую линию, практику или организационную структуру, которая может быть административной, технической, управляющей, или законодательно принятой, которые изменяют риск информационной безопасности.
2. Средств менеджмента, возможно, не всегда проявляют намеченный или принятый эффект изменения.
3. Менеджмент также используется в качестве синонима для гарантии или контрмеры.

3.3 Событие (event):

Возникновение или изменение определённого набора обстоятельств.
[Руководство ISO 73:2009]
Примечания:

1. Событие может возникать один раз или несколько и может иметь несколько причин.
2. Событие может состоять в том, что что-либо не произошло.
3. Событие может иногда упоминаться как «инцидент» или «происшествие»[3].

3.4 Внешний контекст (external context):

Внешняя среда, в которой организация стремится к достижению своих целей
[Руководство ISO 73:2009]
Примечания:
Внешний контекст может включать:

- культурную, социальную, политическую, правовую, законодательную, финансовую, технологическую, экономическую, природную и рыночную среду на международном, региональном, национальном или локальном уровне;
- основные факторы и тенденции, влияющие на цели организации;
- взаимосвязи с заинтересованными сторонами, их восприятие и ценности.

3.5 Внутренний контекст (internal context):

Внутренняя среда, в которой организация стремится к достижению своих целей
[Руководство ISO 73:2009]
Примечания:
Внутренний контекст может включать:

- руководство, организационную структуру, функции и обязательства;
- политику, цели и стратегии для их достижения;
- возможности, рассматриваемые в отношении ресурсов и знаний (например, капитал, время, персонал, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (как официальные, так и неофициальные);
- взаимосвязи с внутренними заинтересованными сторонами, их восприятие и ценности;
- культуру организации;
- стандарты, руководящие указания и модели, принятые организацией;
- форму и объем контрактных взаимоотношений.

[3] Примечание переводчика, из ISO/IEC Guide 73:2009, в оригинале стандарта этого пункта примечания нет: «События без последствий может упоминаться как «аварийная остановка», «инцидент», угроза серьёзного инцидента» или «опасное событие»»

3.6 Уровень риска (level of risk):

Величина риска (3.9) или комбинации рисков, выраженная как сочетание последствий (3.1) и их возможности (3.7) возникновения.
[Руководство ISO 73:2009]

3.7 Возможность (likelihood):

Вероятность наступления некоторого события.
[Руководство ISO 73:2009]
Примечания:

1. В терминологии менеджмента риска термин «возможность» используется в отношении возможности того, что может произойти, либо определённое, измеренное или установленное объективно или субъективно, качественно или количественно, либо описанное с использованием общих условий или математически (например, вероятность или периодичность в заданный период времени).
2. Английский термин «likelihood» не имеет прямого эквивалента в некоторых языках, вместо него часто используют термин «probability». Однако, в английском языке термин «probability» часто интерпретируют в узком смысле, как математический термин. Следовательно, в терминологии менеджмента риска термин «likelihood» используют с тем намерением, что он должен иметь ту же самую широкую интерпретацию, которую термин «probability» имеет во многих языках, кроме английского языка.

3.8 Остаточный риск (residual risk):

Риск (3.9), сохраняющийся после обработки риска (3.17)
[Руководство ISO 73:2009]
Примечания:

1. Остаточный риск может содержать в себе неидентифицированный риск.
2. Остаточный риск может также называться как «сохраняемый риск».

3.9 Риск (risk):

Влияние неопределённости на цели.
[Руководство ISO 73:2009]
Примечания:

1. Влияние – это отклонение от предполагаемого (положительного и/или отрицательного).
2. Цели могут иметь различные аспекты (например, финансовые цели, цели охраны здоровья и безопасности, экологические цели) и могут применяться на различных уровнях (стратегических, в масштабах организации, проекта, продукции или процесса).
3. Риск обычно характеризуется возможными событиями (3.3) и последствиями (3.1) или их сочетанием.
4. Риск обычно выражается в виде сочетания последствий события (включая изменения в обстоятельствах) и связанной с ним возможностью (3.9) возникновения.
5. Неопределённость – это недостаточность (даже частичная) информации, связанной с пониманием события или знаниями о нем, его последствиями или возможностью возникновения.

6. Информационная безопасность ассоциируется с потенциалом угроз, которые используют уязвимости информационного актива или группу информационных активов и таким образом наносят ущерб организации[4].

3.10 Анализ риска (risk analysis):

Процесс понимания происхождения риска и определения уровня риска (3.6)
[Руководство ISO 73:2009]
Примечания:

1. Анализ риска обеспечивает основу для оценивания риска и принятия решений, касающихся обработки риска.
2. Анализ риска включает количественную оценку риска.

3.11 Оценка риска (risk assessment):

Общий процесс идентификации риска (3.15), анализа риска (3.10) и оценивания риска (3.14).
[Руководство ISO 73:2009]

3.12 Обмен информацией и консультирование относительно риска (risk communication and consultation):

Непрерывные и повторяющиеся процессы, которые проводит организация, для предоставления, разделения или получения информации, а так же ведения диалога с заинтересованными сторонами (3.18) относительно менеджмента риска (3.9)
[Руководство ISO 73:2009]
Примечания:

1. Информация может касаться наличия, характера, формы, возможности (3.6.1.1), важности, оценивания, приемлемости и обработки в рамках менеджмента риска.
2. Консультирование – это двусторонний процесс квалифицированного обмена информацией между организацией и заинтересованными сторонами до принятия решения по определённому вопросу или перед определением указаний по этому вопросу. Консультирование является:

- процессом, который оказывает влияние на принятие решения посредством влияния, а не принуждения;
- входными данными для процесса принятия решения, а не совместным принятием решения.

3.13 Критерии риска (risk criteria):

Аспекты, в соответствии с которыми осуществляют оценивание риска (3.9)
[Руководство ISO 73:2009]
Примечания:

1. Критерии риска основываются на целях организации и внешнем и внутреннем контексте.
2. Критерии риска могут быть установлены на основании стандартов, законов, политик и других требований.

3.14 Оценивание риска (risk evaluation):

Процесс сравнения результатов анализа риска (3.10) с установленными критериями риска (3.13) для определения, является ли риск и/или его величина приемлемыми или допустимыми.

[4] Примечание переводчика: Данного пункта примечаний нет в Руководство ISO 73:2009.

[Руководство ISO 73:2009]
Примечание:
Оценивание риска способствует принятию решения в отношении обработки риска.

3.15 Идентификация риска (risk identification):

Процесс выявления, исследования и описания рисков.
[Руководство ISO 73:2009]

Примечание:

1. Идентификация включает идентификацию источников риска, событий, их причин и возможных последствий.
2. Идентификация риска может включать статистические данные, теоретический анализ, обоснованную точку зрения и заключение специалиста, а также потребности заинтересованной стороны.

3.16 Менеджмент риска (risk management):

Скоординированная деятельность по руководству и управлению организацией в отношении риска.
[Руководство ISO 73:2009]
Примечание:
Этот Международный стандарт использует термин 'процесс', чтобы описать риск-менеджмент повсюду. Элементы в пределах процесса менеджмента риска называют «действиями».

3.17 Обработка риска (risk treatment):

Процесс изменения риска.
[Руководство ISO 73:2009]
Примечания:

1. Обработка риска может включать:
    - избегание риска посредством принятия решения не начинать или не продолжать деятельность, в результате которой возникает риск;
    - принятие риска или увеличение риска для достижения цели;
    - устранение источника риска;
    - изменение возможности возникновения;
    - изменение последствий;
    - разделение риска с другой стороной или сторонами (включая договоры и финансирование риска;
    - принятие риска на основании обоснованного решения.
2. Обработка риска, имеющего отрицательные последствия, иногда упоминается как «снижение риска», «устранение риска», «предотвращение риска» и «уменьшение риска».
3. Обработка риска может создавать новые риски или изменять существующие риски.

3.18 Заинтересованная сторона (stakeholder):

Лицо или организация, которые могут воздействовать, подвергаться воздействию, или осознают, что на них влияет какое-либо решение или действия.
[Руководство ISO 73:2009]
Примечание:
Лицо, принимающее решение, может быть заинтересованной стороной.

4 Структура интернационального стандарта

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

Информация о предпосылках создания стандарта приводится в разделе 5.

Основной обзор процесса менеджмента риска информационной безопасности даётся в разделе 6.

Все виды деятельности, связанные с менеджментом риска информационной безопасности, 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;
- Обмен информацией относительно риска - в разделе 11;
- Мониторинг и пересмотр риска - в разделе 12.

Дополнительная информация о видах деятельности, связанных с менеджментом риска информационной безопасности, представлена в приложениях. Установление контекста рассматривается в Приложении A (определение области применения и границ процесса менеджмента риска информационной безопасности). Идентификация и определение ценности активов и оценок влияния обсуждаются в Приложении B (примеры, касающиеся активов), Приложении C (примеры, касающиеся типичных угроз) и Приложении D (примеры, касающиеся типичных уязвимостей).

Примеры подходов к оценке рисков информационной безопасности представлены в Приложении E.

Ограничения, касающиеся снижения риска, представлены в приложении F.

Различия между ISO/IEC 27005:2008 и ISO/IEC 27005:2011 показаны в Приложении G.

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

Входные данные: Идентифицируется любая информация, требуемая для выполнения деятельности.

Действие: Описывается деятельность.

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

Выходные данные: Идентифицируется любая информация, полученная после выполнения деятельности.

5 Информация о предпосылках создания стандарта

Систематический подход к менеджменту риска информационной безопасности необходим для того, чтобы идентифицировать потребности организации, касающиеся требований информационной безопасности и создать эффективную систему менеджмента информационной безопасности (СМИБ). Этот подход должен быть применимым к среде организации и, в частности, должен поддерживать менеджмент рисков для всей организации. Усилия по обеспечению безопасности должны эффективно и своевременно рассматривать риски там и тогда, где и когда это необходимо. Менеджмент рисков информационной безопасности должен быть неотъемлемой частью всех видов деятельности, связанных с менеджментом информационной безопасности, а также должен применяться для реализации и поддержки функционирования СМИБ организации.

Менеджмент риска информационной безопасности должен быть непрерывным процессом. Данный процесс должен устанавливать контекст, поддерживать оценку и обработку рисков, обеспечивать использование плана обработки риска для реализации, содействовать выработке рекомендаций и решений. Менеджмент риска связан с анализом того, что может произойти, и какими могут быть возможные последствия, прежде чем выработать решение о том, что и когда должно быть сделано для снижения риска до приемлемого уровня.

Менеджмент риска информационной безопасности должен способствовать следующему:

- идентификации рисков;
- оценки рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения;
- изучения вероятности и потенциальных последствий данных рисков;
- установлению порядка приоритетов в рамках обработки рисков;
- установлению приоритетов мероприятий по снижению имеющих место рисков;
- привлечению заинтересованных сторон к принятию решений о менеджменте рисков и поддержанию их информированности о состоянии менеджмента риска;
- эффективности проводимого мониторинга обработки рисков;
- проведению регулярного мониторинга и пересмотра процесса менеджмента рисков;
- сбору информации для усовершенствования подхода к менеджменту рисков;
- подготовке менеджеров и персонала в части сфере рисков и необходимых действий, предпринимаемых для их уменьшения.

Процесс менеджмента рисков информационной безопасности может быть применён ко всей организации, любой отдельной части организации (например, подразделению, физическому местоположению, сервису), любой информационной системе, существующим, планируемым или имеющимся аспектам управления (например, планированию непрерывности бизнеса).

6 Обзор процесса менеджмента рисков информационной безопасности

Процесс менеджмента рисков информационной безопасности состоит из установления контекста (раздел 7), оценки риска (раздел 8), обработки риска (раздел 9), принятия риска (раздел 10), обмен информацией относительно риска (раздел 11), а также мониторинга и пересмотра риска (раздел 12).

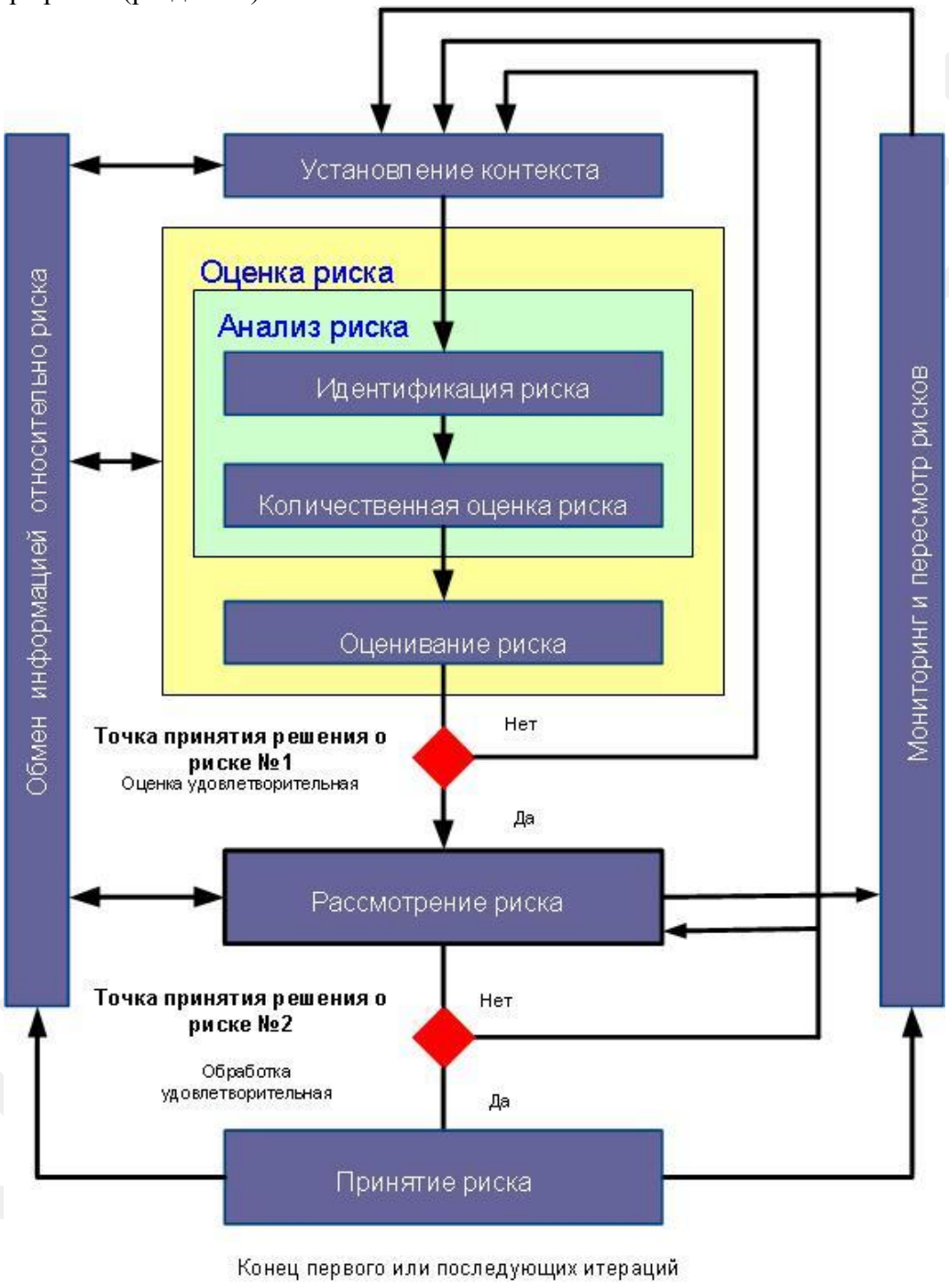

Рисунок 1. Процесс менеджмента риска информационной безопасности

Как показано на рисунке 1, процесс менеджмента риска информационной безопасности может быть итеративным для таких видов деятельности, как оценка риска и/или обработка риска. Итеративный подход к проведению оценки риска может увеличить глубину и детализацию оценки при каждой итерации. Итеративный подход даёт хороший баланс между уменьшением времени и усилия, затрачиваемого на определение средств контроля,

в то же время, по-прежнему обеспечивая уверенность в том, что высокоуровневые риски рассматриваются соответствующим образом.

Контекст впервые устанавливается тогда, когда проводится оценка высокоуровневого риска. Если она обеспечивает достаточную информацию для эффективного определения действий, требуемых для снижения риска до приемлемого уровня, то задача является выполненной и следует обработка риска. Если информация является недостаточной, то проводится другая итерация оценки риска с помощью пересмотренного контекста (например, критерии оценки рисков, критерии принятия рисков или критерии влияния), возможно на ограниченных частях полной области применения (см. рисунок, точка принятия решений о риске № 1).

Эффективность обработки риска зависит от результатов оценки риска. Возможно, что обработка риска не будет сразу же приводить к приемлемому уровню остаточного риска. В этой ситуации может потребоваться, если необходимо, другая итерация оценки риска с изменёнными параметрами контекста (например, оценка риска, принятие риска или критерии влияния), за которой последует дополнительная обработка риска (см. рисунок, точка принятия решений о риске № 2).

Деятельность по принятию риска должна обеспечивать уверенность в том, что остаточные риски однозначно принимаются руководством организации. Это особенно важно в ситуации, когда внедрение средств контроля не осуществляется или откладывается, например, из-за стоимости.

Важно, чтобы во время всего процесса менеджмента рисков информационной безопасности и их обработки осуществлялась обмен информацией относительно риска соответствующему руководству и операционному персоналу. Даже до обработки рисков информация об идентифицированных рисках может быть очень ценной для осуществления менеджмента инцидентов и может способствовать снижению потенциального ущерба. Осведомлённость руководства и персонала о рисках, природе средств контроля, применяемых для снижения рисков, и проблемных областях организации помогает им в рассмотрении инцидентов и неожиданных событий наиболее эффективным образом. Детализированные результаты каждой деятельности, входящей в процесс менеджмента рисков информационной безопасности, и результаты, полученные из двух точек принятия решений о рисках, должны быть документированы.

В ISO/IEC 27001 определяется, какие средства контроля, реализуемые в рамках области применения, границ и контекста СМИБ, должны основываться на риске. Применение процесса менеджмента риска ИБ может удовлетворять это требование. Существует много подходов, посредством которых процесс может быть успешно внедрён в организации. В любом случае организация должна использовать подход, наилучшим образом соответствующий её обстоятельствам каждого конкретного применения процесса.

В СМИБ установление контекста, оценка риска, разработка плана обработки риска и принятие риска являются частью фазы "планирование". В фазе "осуществление" СМИБ действия и средства контроля, требуемые для снижения риска до приемлемого уровня, реализуются в соответствии с планом обработки риска. В фазе "проверка" СМИБ менеджеры определяют потребность в пересмотре обработки риска в свете инцидентов и изменений обстоятельств. В фазе "действие" осуществляются любые необходимые работы, включая повторное инициирование процесса менеджмента риска ИБ.

В таблице суммируются виды деятельности, связанной с менеджментом риска, значимые для четырёх фаз процесса СМИБ.

Следующая таблица суммирует действия менеджмента риском информационной безопасности, относящиеся к четырём фазам процесса СМИБ:

Таблица 1. Регулирование СМИБ и процесс менеджмента риском информационной безопасности

Процесс СМИБ	Процесс менеджмента риском информационной безопасности
Планирование (Plan)	Установление контекста Оценки риска Разработка плана обработки риска Принятие риска
Осуществление (Do)	Реализация плана обработки риска
Проверка (Check)	Непрерывный мониторинг и рассмотрение рисков
Действие (Act)	Поддержка и улучшение рисков информационной безопасности Процесс менеджмента

7 Установление контекста

7.1 Общий анализ

Входные данные: Вся информация об организации, уместная для установления контекста менеджмента риска информационной безопасности.

Действие: Должен быть установлен контекст менеджмента риска информационной безопасности, что включает установление основных критериев, необходимых для менеджмента риска информационной безопасности (в соответствии с 7.2), определение сферы действия и границ (в соответствии с 7.3) и установление соответствующей структуры для осуществления менеджмента риска информационной безопасности (в соответствии с.7.4).

Руководство по реализации:

Необходимо определить цель менеджмента риска информационной безопасности, так как она влияет на общий процесс и на установку контекста, в частности. Этой целью может быть:

- поддержка системы менеджмента информационной безопасности;
- правовое соответствие и свидетельство должного внимания;
- подготовка плана обеспечения непрерывности бизнеса;
- подготовка плана реагирования на инциденты;
- описание требований информационной безопасности для продукта, услуги или механизма.

Руководство по реализации для элементов установления контекста, необходимых для поддержки системы менеджмента информационной безопасности, обсуждается ниже в 7.2 и 7.4.

Примечание:

В ISO/IEC 27001 не используется термин "контекст". Однако весь раздел 7 связан с требованиями "определение сферы действия и границ системы менеджмента информационной безопасности" [см. 4.2.1 перечисление a)], "определение политики системы менеджмента информационной безопасности [см. 4.2.1 перечисление b)] и "определение подхода к оценке риска [см. 4.2.1 перечисление c)], определёнными в ISO/IEC 27001.

Выходные данные: Спецификация основных критериев, сфера действия и границы, структура для процесса менеджмента риска информационной безопасности.

7.2 Основные критерии

В зависимости от области применения и целей менеджмента риском могут быть применены различные подходы. Также могут быть различными подходы для каждой итерации.

Должен быть выбран или разработан соответствующий подход менеджмента риском, который обращается к основным критериям, таким как: критерии оценки риска, воздействие на критерии, критерии допустимости риска.

Дополнительно организация должна оценить, доступны ли необходимые ресурсы для:

- выполнения оценки риска и установления плана обработки риска;
- определения и осуществления политики и процедуры, включая реализацию выбранного менеджмента;
- контроль мониторинга;
- мониторинг процесса менеджмента риском информационный безопасности.

ПРИМЕЧАНИЕ, смотрите также ISO/IEC 27001 (Раздел 5.2.1) относительно ресурсов СМИБ и условий для реализации и обслуживания.

Критерии оценки риска

Должны разрабатываться критерии для оценивания рисков информационной безопасности организации, учитывая следующее:

- стратегическая ценность обработки бизнес-информации;
- критичность затрагиваемых информационных активов;
- правовые и регулирующие требования и договорные обязательства;
- операционная важность и важность для бизнеса доступности, конфиденциальности и целостности;
- ожидания восприятия причастных сторон, а также негативные последствия для "неосязаемого капитала" и репутации.

Кроме того, критерии оценивания рисков могут использоваться для определения приоритетов для обработки рисков.

Критерии воздействия

Критериями влияния должны разрабатываться и определяться, исходя из степени ущерба или расходов для организации, вызываемых событием, связанным с информационной безопасностью, учитывая следующее:

- уровень классификации информационного актива, на который оказывается влияние;
- нарушения информационной безопасности (например, утрата конфиденциальности, целостности и доступности);
- ухудшенные операции (внутренние или третьих сторон);
- потеря ценности бизнеса и финансовой ценности;
- нарушение планов и конечных сроков;
- ущерб для репутации;
- нарушение законодательных, регулирующих или договорных требований.

Примечание - Смотрите также ISO/IEC 27001 [4.2.1 перечисление d) 4)], относительно идентификации критериев 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 многие пороговые значения, с желаемым целевым уровнем риска, но при условии, что при определённых обстоятельствах высшее руководство будет принимать риски, находящиеся выше указанного уровня;
- критерии принятия риска могут выражаться как соотношение количественно оценённой выгоды (или иной выгоды бизнеса) к количественно оценённому риску;
- различные критерии принятия риска могут применяться к различным классам риска, например, риски, которые могут иметь результатом несоответствие директивам и законам, не могут быть приняты, в то время как принятие рисков высокого уровня может быть разрешено, если это определено в договорном требовании;
- критерии принятия риска могут включать требования, касающиеся будущей дополнительной обработке, например, риск может быть принят, если имеется одобрение и согласие на осуществление действия по его снижению до приемлемого уровня в рамках определённого 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 учётом следующего:

- критериев бизнеса;
- правовых и регулирующих аспектов;
- операций;
- технологий;
- финансов;
- социальных и гуманитарных факторов.

Примечание - Критерии принятия риска соответствуют "критериям принятия рисков и идентификации приемлемого уровня риска", определённым в ISO/IEC 27001 [см. 4.2.1 перечисление c) 2)].

Более подробную информацию можно найти в приложении A.

7.3 Область применения и границы

Организация должна определять область применения и границы менеджмента риска информационной безопасности.

Область применения процесса менеджмента информационной безопасности необходимо определять для обеспечения того, чтобы все значимые активы принимались в расчёт при оценке риска. Кроме того, необходимо определять границы [см. также ISO/IEC 27001, 4.2.1 перечисление a)] для рассмотрения тех рисков, источники которых могут находиться за данными границами.

Должна быть собрана информация об организации для того, чтобы определить среду в которой она функционирует и иную, необходимую для процесса менеджмента рисков информационной безопасности информацию.

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

- стратегические цели бизнеса организации, стратегии и политики;
- процессы бизнеса;
- функции и структура организации;
- правовые, регулирующие и договорные требования, применимые к организации;
- политика информационной безопасности организации;
- общий подход к менеджменту риска организации;
- информационные активы;
- местоположение организации и географические характеристики;
- ограничения, влияющие на организацию;
- ожидания причастных сторон;
- социокультурная среда;
- интерфейсы (т.е. обмен информацией со средой).

Кроме того, организация должна обеспечивать обоснование для каждого исключения из области применения.

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

Примечание - Область применения и границы менеджмента риска информационной безопасности связаны с областью применения и границами СМИБ, требуемыми в ISO/IEC 27001 [см. 4.2.1 перечисление а)].

Более подробную информацию можно найти в приложении А.

7.4 Организационная структура менеджмента риска информационной безопасности

Необходимо устанавливать и поддерживать организационную структуру и обязанности для процесса менеджмента риска информационной безопасности. Ниже перечисляются главные роли и обязанности, присущие такой организационной структуре:

- разработка процесса менеджмента риска информационной безопасности, подходящего для данной организации;
- идентификация и анализ 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 интерфейсов для организационных функций менеджмента рисков высокого уровня (например, менеджмент операционного риска), а также интерфейсов с другими значимыми проектами и видами деятельности;
- определение путей эскалации принятия решений;
- определение подлежащих ведению документов.

Эта организационная структура должна одобряться соответствующим руководством организации.

Примечание - ISO/IEC 27001 требует определения обеспечения ресурсов, необходимых для установления, реализации, функционирования, мониторинга, пересмотра, поддержки и улучшения СМИБ [см. 5.2.1 перечисление а)]. Организация операций менеджмента риска может рассматриваться как один из ресурсов, требуемых ISO/IEC 27001.

8 Оценка рисков информационной безопасности

8.1 Общее описание оценки риска информационной безопасности

ОТМЕТЬТЕ, В ISO/IEC 27001 деятельность по оценке риска определяется как процесс.

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

Действие: Риски должны быть идентифицированы, количественно определены или качественно описаны и расставлены в соответствии с приоритетами согласно критериям оценивания риска и уместным для организации целям.

Руководство по реализации:

Риск представляет собой комбинацию последствий, вытекающих из нежелательного события, и вероятности возникновения события. Оценка риска количественно определяет или качественно описывает риски и даёт возможность руководителям расставлять риски в соответствии с приоритетами согласно воспринимаемой серьёзности или другим установленным критериям.

Оценка риска состоит из следующих мероприятий:

- идентификацию риска (в соответствии с 8.2);
- анализ степени риска (в соответствии с 8.3)
- оценивание риска (в соответствии с 8.4).

Оценка риска определяет ценность информационных активов, идентифицирует применимые угрозы и уязвимости, которые существуют (или могут существовать), идентифицирует существующие средства контроля и их влияние на идентифицированные риски, определяет потенциальные последствия и, наконец, расставляет выведенные риски в соответствии с приоритетами и ранжирует их по критериям оценивания риска, зафиксированным при установке контекста.

Оценка риска часто проводится, используя две (или более) итерации. Сначала проводится высокоуровневая оценка для идентификации потенциально высоких рисков, оправдывающих дальнейшую оценку. Следующая итерация может включать дальнейшее углублённое рассмотрение потенциально высоких рисков, обнаруженных при первоначальной итерации. В тех случаях, когда это предоставляет недостаточную информацию для оценки риска, затем проводится дальнейший детальный анализ, вероятно, для частей полной сферы и, возможно, используя иной метод.

Выбор собственного подхода к оценке риска на основе задач и цели оценки риска зависит от самой организации.

Обсуждение подходов к оценке риска информационной безопасности можно найти в приложении Е.

Выходные данные: Перечень оценённых рисков, расставленных в соответствии с приоритетами согласно критериям оценивания риска.

8.2 Анализ риска

8.2.1 Идентификация риска

8.2.1.1 Введение в идентификацию риска

Целью идентификации риска является определение того, что могло бы произойти, чтобы нанести потенциальный, и чтобы получить представление о том, как, где и почему мог иметь место этот вред. Этапы, описанные ниже, должны собирать входные данные для деятельности по количественной оценке риска.

Примечание - Виды деятельности, описанные ниже, могут проводиться в различном порядке в зависимости от применяемой методологии.

8.2.1.2 Идентификация активов[5]

Входные данные: Область применения и границы для подлежащей проведению оценке риска, перечень составных частей, включающий владельцев, местоположение, функцию и т.д.

Действие: Должны быть идентифицированы активы, входящие в установленную область применения [связано с ISO/IEC 27001, 4.2.1 перечисление d) 1)].

Руководство по реализации:

Активом является нечто, имеющее ценность для организации и, следовательно, нуждающееся в защите. При идентификации активов следует иметь в виду, что информационная система состоит не только из аппаратных и программных средств.

Идентификацию активов следует осуществлять на соответствующем уровне детализации, обеспечивающем достаточную информацию для оценки риска. Уровень детализации, используемый при идентификации активов, влияет на общий объем информации, собранной во время оценки риска. Этот уровень может быть более детализирован при дальнейших итерациях оценки риска.

Для каждого актива должен быть определён владелец, чтобы обеспечить учёность и ответственность за каждый актив. Владелец актива может не обладать правами собственности на актив, но он несёт соответствующую 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 на предмет определения ценности активов).

Границей пересмотра является периметр активов организации, определённый как подлежащий менеджменту посредством процесса менеджмента риска информационной безопасности.

Более подробную информацию об идентификации и определения ценности активов в части информационной безопасности можно найти в приложении B.

Выходные данные: Перечень активов, подлежащий менеджменту риска, и перечень бизнес-процессов, связанных с активами, и их значимость.

8.2.1.3 Идентификация угроз

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

Действие: Угрозы и их источники должны быть идентифицированы [связано с ISO/IEC 27001, 4.2.1 перечисление d) 2)].

Руководство по реализации:

Угроза обладает потенциалом причинения вреда активам, а, следовательно, и организациям, таким как информация, процессы и системы. Угрозы могут быть природного происхождения или от действий людей, они могут быть случайными или умышленными. Должны быть идентифицированы и случайные, и умышленные источники угроз. Угроза может проистекать как из самой организации, так и вне её пределов. Угрозы должны идентифицироваться в общем и по виду (например, неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы

[5] Примечание переводчика: В прикладных методах анализа рисков обычно рассматриваться следующие классы активов:

- оборудование (физические ресурсы);
- программное обеспечение (системное, прикладное, утилиты, другие вспомогательные программы);
- информационные ресурсы (базы данных, файлы, все виды документации);
- системные интерфейсы (внешние и внутренние возможные соединения);
- люди, которые пользуются и поддерживают IT систему (в штате/ контракт);
- миссия IT системы (system mission) – процесс, выполняемый IT системой;
- сервис и поддерживающая инфраструктура (обслуживание СВТ, энергоснабжение, обеспечение климатических параметров и т.п.).

идентифицируются внутри родового класса. Это означает, что ни одна угроза, включая неожиданные, не будет упущена, но объем требуемой работы, несмотря на это, ограничен.

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

Входные данные для идентификации и измерения вероятности возникновения угроз (см. 8.2.2.3) могут быть получены от владельцев активов или пользователей, персонала отдела кадров, руководства организации и специалистов в сфере ИБ, экспертов в сфере физической безопасности, юридического отдела и других структур, включая правовые органы, метеорологические службы, страховые компании, национальные правительственные учреждения. При рассмотрении угроз должны учитываться аспекты среды и культуры.

Внутренний опыт, полученный в результате инцидентов, и прошлые оценки угроз должны быть учтены в текущей оценке. Может быть целесообразно справиться в других реестрах угроз (возможно, специфичных для организации или бизнеса), чтобы заполнить перечень общих угроз, где это имеет значение. Реестры и статистику угроз можно получить от промышленных организаций, национальных правительств, правовых органов, страховых компаний и т.д.

Используя реестры угроз или результаты прежних 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 идентификацией вида и источника.

8.2.1.4 Идентификация существующих средств контроля

Входные данные: Документирование средств контроля, планов реализации обработки риска.

Действие: Существующие и планируемые средства контроля следует идентифицировать.

Идентификация существующих средств контроля должна быть сделана, чтобы избежать ненужной работы или расходов, например, при дублировании средств контроля. Кроме того, во время идентификации существующих средств контроля следует провести проверку, чтобы удостовериться, что средства контроля функционируют правильно - ссылка на уже существующие отчёты по аудиту СМИБ должны ограничивать время, затрачиваемое на эту задачу. Если средства контроля не работают, как ожидалось, это может стать причиной уязвимости. Следует уделить внимание ситуации, когда выбранные средства контроля (или стратегия) отказываются работать и поэтому требуются дополнительные средства контроля для эффективного рассмотрения идентифицированного риска. В СМИБ, в соответствии с ISO/IEC 27001, это поддерживается измерением эффективности средств контроля. Одним из способов количественно оценить действие средств контроля - посмотреть, как оно уменьшает вероятность угрозы и простоту использования уязвимости или влияние инцидента. Пересмотры, осуществляемые менеджерами и отчёты по аудиту, также обеспечивают информацию об эффективности существующих средств контроля.

Средство контроля, которые планируется реализовать в соответствие с планами реализации обработки риска, должны учитываться тем же самым способом, который уже был реализован.

Существующее или планируемое средство контроля может идентифицироваться как неэффективное или недостаточное, или необоснованное. Если его посчитали необоснованным или недостаточным, средство контроля необходимо проверить, чтобы определить стоит ли его удалить, заменить его другим, более подходящим, или стоит оставить его на месте, например, по стоимостным причинам.

Для идентификации существующих или планируемых средств контроля могут быть полезны следующие мероприятия:

- просмотр документов, содержащих информацию о средствах контроля (например, планы обработки рисков). Если процессы менеджмента информационной безопасности задокументированы должным образом, то все существующие или планируемые средства контроля и состояние их реализации должны быть там доступны;
- проверка вместе с людьми, отвечающими за информационную безопасность (например, служащий, занимающийся обеспечением информационной безопасности, служащий, отвечающий за безопасность информационной системы, комендант здания или руководитель работ) и пользователями, какие средства контроля действительно реализованы для рассматриваемого информационного процесса или информационной системы;
- обход здания с проведением осмотра физических средств контроля, сравнение реализованных средств контроля с перечнем тех, которые должны быть, и проверка реализованных средств контроля на предмет правильной и эффективной работы или;
- рассмотрение результатов внутренних аудитов.

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

8.2.1.5 Идентификация уязвимости

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

Действие: Необходимо идентифицировать уязвимости, которые могут быть использованы угрозами, чтобы нанести ущерб активам или организации [связано с ISO/IEC 27001, 4.2.1 перечисление d) 3)].

Руководство по реализации:

Уязвимости могут быть идентифицированы в следующих областях:

- организация работ;
- процессы и процедуры;
- установившиеся нормы управления;
- персонал;
- физическая среда;
- конфигурация информационной системы;
- аппаратные средства, программное обеспечение и аппаратура связи;
- зависимость от внешних сторон.

Наличие уязвимости не причиняет вреда само по себе, так как необходимо наличие угрозы, которая воспользуется ею. Уязвимость, не имеющая соответствующей угрозы, может не требовать внедрения средства контроля, но должна осознаваться и подвергаться мониторингу на предмет измерений. Следует отметить, что неверно реализованное или неправильно функционирующее средство контроля или средство контроля, которое неправильно используется, само может быть уязвимостью. Средство контроля может быть эффективным или неэффективным в зависимости от среды, в которой оно функционирует. И наоборот, угроза, не имеющая соответствующей уязвимости, может не приводить к риску.

Уязвимости могут быть связаны со свойствами актива, которые могут использоваться способом и с целью, отличающимися от тех, которые планировались при приобретении или создании актива. Уязвимости, возникающие из различных источников, подлежат рассмотрению, например, те которые являются внешними или внутренними по отношению к активу.

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

Выходные данные: Перечень уязвимостей, связанных с активами, угрозами и средствами контроля; перечень уязвимостей, которые не связаны с подлежащей рассмотрению идентифицированной угрозой.

8.2.1.6 Идентификация последствий

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

Действие: Должны быть идентифицированы последствия для активов, которые могут быть результатом потери конфиденциальности, целостности и доступности [см. ISO/IEC 27001, 4.2.1 перечисление d) 4)]. Последствием может быть потеря эффективности, неблагоприятные операционные условия, потеря бизнеса, ущерб, нанесённый репутации и т.д.

Эта деятельность идентифицирует ущерб для организации или последствия для организации, которые могут быть обусловлены сценарием инцидента, оказываемой угрозой, использующей определённую уязвимость в инциденте ИБ (см. ISO/IEC 27002, раздел 13). Влияние сценариев инцидентов следует определять, используя критерии влияния, определённые в течение деятельности, связанной с установлением контекста. Оно может затронуть один или большее количество активов; или часть актива. Поэтому активам может назначаться ценность в зависимости от их финансовой стоимости и по причине последствий для бизнеса в случае их порчи или компрометации. Последствия могут быть временными или постоянными, как в случае разрушения активов.

Примечание - В ISO/IEC 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 специфические навыки, необходимые для устранения неисправности;
- репутации и иного "неосязаемого капитала".

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

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

8.2.2 Измерение риска

8.2.2.1 Методология измерения риска

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

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

Далее более подробно описываются детали методологии оценки:

A) качественная оценка.

Качественная оценка использует шкалу квалификации атрибутов для описания величины возможных последствий (например, низкий, средний и высокий) и вероятности возникновения этих последствий. Преимущество качественной оценки заключается в простоте её понимания всем соответствующим персоналом, а недостатком является зависимость от субъективного выбора шкалы.

Такие шкалы могут быть адаптированы или скорректированы таким образом, чтобы удовлетворять требованиям обстоятельств, а для разных рисков могут использоваться разные описания. Качественная оценка может использоваться:

- как начальная деятельность по тщательной проверке для идентификации рисков, требующих более детального анализа;
- там, где этот вид анализа является соответствующим для принятия решения;
- там, где числовые данные или ресурсы являются неадекватными для количественной оценки.

Качественный анализ должен использовать фактическую информацию и данные, где они доступны;

b) количественная оценка.

Количественная оценка использует шкалу с числовыми значениями (а не описательные шкалы, используемые в качественной оценке) и последствий, и вероятности, применяя данные из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев количественная оценка использует фактические данные за прошлый период, обеспечивая преимущество в том, что она может быть напрямую связана с целями информационной безопасности и проблемами организации. Недостатки количественного подхода могут иметь место тогда, когда фактические проверяемые данные недоступны, поэтому создаётся иллюзия ценности и точности оценки риска.

Способ выражения последствий и вероятности и способы их объединения для обеспечения сведений об уровне риска изменяются в соответствии с видом риска и целью, для которой должны использоваться выходные данные оценки риска. Неопределённость и изменяемость последствий и вероятности следует учитывать при анализе и сообщать о них эффективным образом.

8.2.2.2 Оценка последствий

Входные данные: Перечень идентифицированных значимых сценарием инцидентов, включая идентификацию угроз, уязвимостей и затронутых активов, последствий для активов и бизнес-процессов.

Действие: Влияние бизнеса на организацию, которое может быть результатом возможных или фактических инцидентов ИБ должно быть оценено с учётом последствий нарушения информационной безопасности, таких как потеря конфиденциальности, целостности или доступности активов [связано с ISO/IEC 27001, 4.2.1 перечисление e) 1)].

Руководство по реализации:

После идентификации всех пересматриваемых активов ценность, присвоенная этим активам, должна учитываться при оценке последствий.

Это значение влияния бизнеса может быть выражено в качественной или количественной формах, однако, любой метод присвоения денежного значения может, в общем, дать больше информации для принятия решений и, следовательно, сделает возможным более эффективный процесс принятия решений.

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

восстановительной стоимости актива:

- стоимости очистки с целью восстановления и замены информации (если это возможно); и
- последствия для бизнеса от потери или компрометации актива, например, возможные неблагоприятные деловые и/или законодательные или регулирующие последствия раскрытия, модификации, недоступности и/или разрушения информации и других информационных активов.

Это определение ценности может быть определено из анализа влияния на бизнес. Ценность определяется последствиями для бизнеса, обычно значительно выше просто восстановительной стоимости и зависит от важности актива для организации при выполнении её бизнес-целей.

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

Последствия или влияние бизнеса могут определяться путём моделирования результатов события или совокупности событий, или экстраполяции экспериментальных исследований или данных за прошедшее время.

Последствия могут быть выражены с точки зрения денежных, технических или персональных критериев влияния, или других критериев, значимых для организации. В отдельных случаях для определения последствий, связанных с различным временем, местами, группами или ситуациями, требуется больше чем одно цифровое значение.

Последствия, связанные со временем или финансами, должны измеряться посредством того же подхода, который используется в отношении вероятности угрозы и уязвимости. Должна поддерживаться последовательность количественного или качественного подхода.

В приложении В приводится более подробная информация по определению ценности активов и оценке влияния.

Выходные данные: Перечень оценённых последствий сценария инцидентов, выраженных по отношению к активам и критериям влияния.

8.2.2.3 Оценка вероятности инцидента

Входные данные: Перечень идентифицированных уместных сценариев инцидентов, включая идентификацию угроз, затрагиваемые активы, используемые уязвимости и последствия для активов и бизнес-процессов. Кроме того, список всех существующих и планируемых средств контроля, их эффективности и состояния реализации и использования.

Действие: Должна быть оценена вероятность действия сценариев инцидентов [связано с ISO/IEC 27001, 4.2.1 перечисление e) 2)].

Руководство по реализации:

После идентификации сценариев инцидентов необходимо оценить вероятность каждого сценария и возникающее влияние, используя качественные или количественные методы оценки. Здесь нужно учитывать тот факт, как часто возникают угрозы и насколько легко могут быть использованы уязвимости, рассматривая:

- опыт и применимую статистику вероятности угроз;
- для источников умышленных угроз: мотивацию и возможности, которые будут меняться с течением времени, и доступные для возможных

нарушителей ресурсы, а также восприятие привлекательности и уязвимости активов возможным нарушителем;

- для источников случайных угроз: географические факторы, например, близость к химическому или нефтеперерабатывающему заводу, возможность экстремальных погодных условий и факторы, которые могут оказывать влияние на ошибки персонала и сбои оборудования;
- уязвимости, в индивидуальном плане и в совокупности;
- существующие средства контроля и то, насколько эффективно они снижают уязвимости.

Например, у информационной системы может быть уязвимость 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, потому что способы злоупотребления ресурсами ограничены.

В зависимости от потребности в точности активы могут быть сгруппированы или может возникать необходимость разбиения активов на элементы и связывания сценариев с элементами. Например, для географических местоположений характер угроз одним и тем же видам активов может меняться или может различаться эффективность существующих средств контроля.

Выходные данные: Вероятность действия сценариев инцидентов (количественная или качественная).

Входные данные: Перечень сценариев инцидентов с их последствиями, касающимися активов, и бизнес-процессов и их вероятности (количественных или качественных).

Действие: Должно быть осуществлено измерение уровня рисков для всех значимых сценариев инцидентов [связано с ISO/IEC 27001, 4.2.1 перечисление e) 4)]. При измерении риска присваиваются значения вероятности и последствий риска. Эти значения могут быть качественными или количественными. Измерение риска основывается на оценённых последствиях и вероятности. Кроме того, оно может также учитывать стоимостные преимущества, проблемы причастных сторон и другие переменные, используемые при оценивании риска. Измеренный риск является комбинацией вероятности нежелательного сценария и его последствий.

В приложении E приводятся примеры различных методов и подходов к измерению рисков информационной безопасности.

Выходные данные: Перечень рисков с присвоенными уровнями значений.

8.2.2.4 Измерение уровня риска

Входные данные: Перечень сценариев инцидентов с их последствиями, касающимися активов, и бизнес-процессов и их вероятности (количественных или качественных).

Действие: Должно быть осуществлено измерение уровня рисков для всех значимых сценариев инцидентов [связано с ISO/IEC 27001, 4.2.1 перечисление e) 4)].

При измерении риска присваиваются значения вероятности и последствий риска. Эти значения могут быть качественными или количественными. Измерение риска основывается на оценённых последствиях и вероятности. Кроме того, оно может также учитывать стоимостные преимущества, проблемы причастных сторон и другие переменные, используемые при оценивании риска. Измеренный риск является комбинацией вероятности нежелательного сценария и его последствий.

В приложении Е приводятся примеры различных методов и подходов к измерению рисков информационной безопасности.

Выходные данные: Перечень рисков с присвоенными уровнями значений.

8.3 Оценивание риска

Входные данные: Перечень рисков с присвоенными уровнями значений и критерии оценивания риска.

Действие: Уровни рисков должны сравниваться с критериями оценивания риска и критериями принятия риска [связано с ISO/IEC 27001, 4.2.1 перечисление e) 4)].

Руководство по реализации:

Характер решений, относящихся к оцениванию риска, и критерии оценивания риска, которые будут использованы для принятия этих решений, должны были быть определены при установлении контекста. Эти решения и контекст должны быть более детально пересмотрены на данном этапе, когда стало известно больше информации о конкретных идентифицированных рисках. Для оценивания рисков организации должны сравниваться измеренные риски (используя выбранные методы, которые рассматриваются в приложении Е) с критериями оценивания риска, выбранными на этапе установления контекста.

Критерии оценивания риска, используемые для принятия решений, должны согласовываться с определённым внешним и внутренним контекстом менеджмента риска информационной безопасности и принимать в расчёт цели организации, мнения причастных сторон и т.д. Решения, связанные с оцениванием риска, обычно основываются на приемлемом уровне риска. Однако последствия, вероятность, степень уверенности в идентификации и анализе риска должны быть также учтены. Совокупность множества рисков низкого и среднего уровня может дать в итоге общий риск более высокого уровня.

При этом следует учесть следующее:

- свойства информационной безопасности:

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 определён как имеющий низкую значимость, связанные с ним риски должны рассматриваться в меньшей степени, чем риски, влияющие на более важные процессы или деятельность.

Оценивание риска основывается на понимании сути риска, полученном на этапе анализа риска, для принятия решений о будущих действиях. Решения должны включать в себя следующее:

- должна ли быть предпринята какая-то деятельность;
- приоритеты при обработке риска, учитывающие измеренные уровни рисков.

На стадии оценивания риска к факторам, которые должны приниматься в расчёт, в дополнение к получившим измеренное значение рискам, дополняются правовые и регулирующие требования.

Выходные данные: Перечень рисков, с назначенными приоритетами в соответствии с критериями оценивания риска в отношении сценариев инцидентов, которые приводят к этим рискам.

9 Обработка рисков информационной безопасности

9.1 Общее описание обработки риска

Входные данные: Перечень рисков с назначенными приоритетами в соответствии с критериями оценивания риска в отношении сценариев инцидентов, которые приводят к этим рискам.

Действие: Должны быть выбраны средства контроля для уменьшения, сохранения, избежание или переноса рисков и определён план обработки рисков.

Руководство по реализации:

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

Примечание - В ISO/IEC 27001 [см. 4.2.1 перечисление f) 2)] вместо термина "сохранение риска" ("retaining risk") используется термин "принятие риска" ("accepting risk").

На рисунке иллюстрируется деятельность по обработке риска в рамках процесса менеджмента риска информационной безопасности.

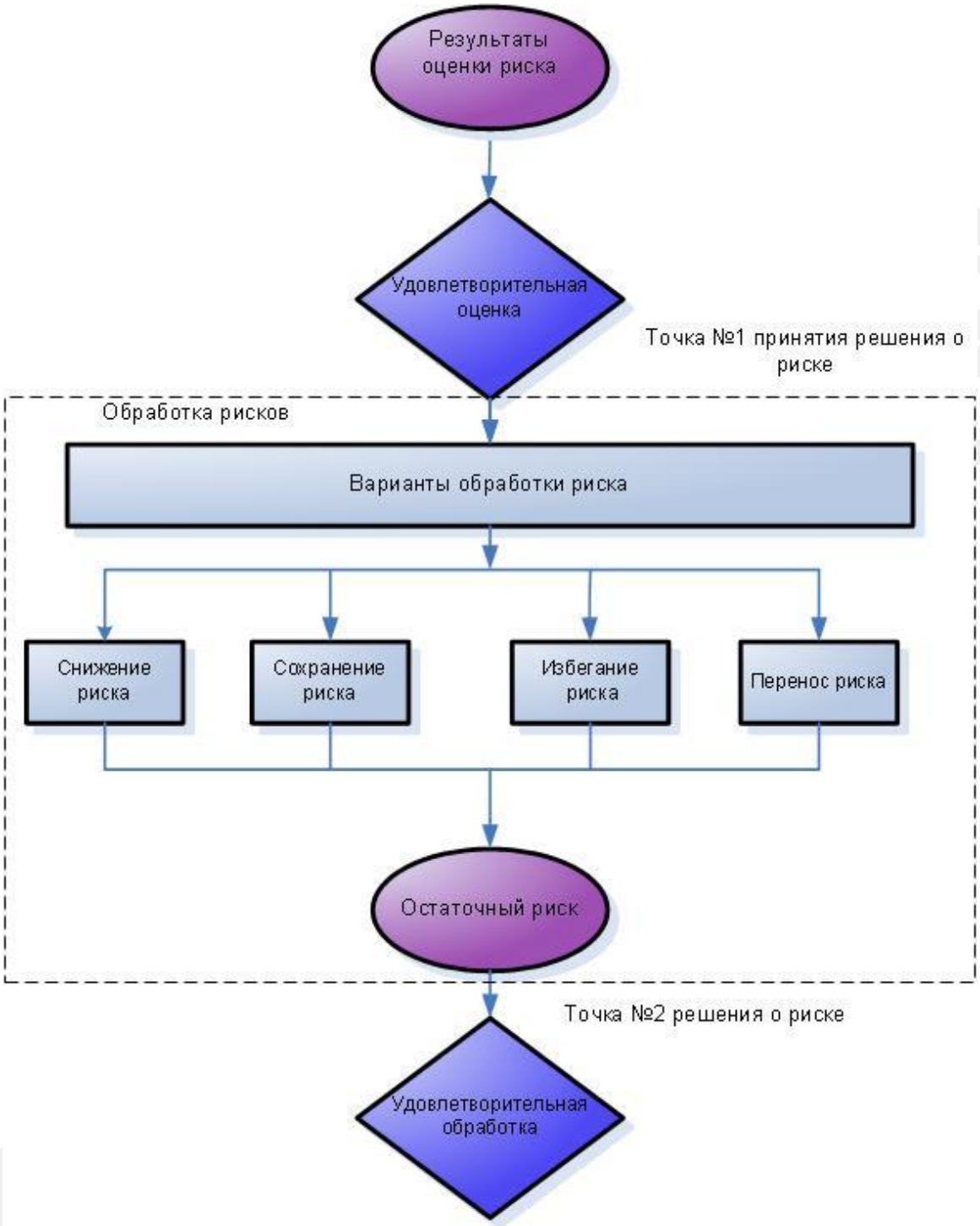

Рисунок 2 - деятельность обработки риска

Варианты обработки риска должны выбираться на основе результатов оценки риска, ожидаемой стоимости реализации этих вариантов и ожидаемой выгоды от этих вариантов.

Когда значительное снижение риска может быть достигнуто при относительно небольших затратах, такие варианты должны реализовываться. Дополнительные варианты улучшений могут быть неэкономичными, и решение необходимо изучать в отношении того, являются ли они оправданными.

Неблагоприятные последствия рисков необходимо снижать до разумных пределов и независимо от каких-либо абсолютных критериев. Менеджеры должны рассматривать редкие, но серьёзные риски. В таких случаях может возникнуть

необходимость реализации средств контроля, которые являются необоснованными по строго экономическим причинам (например, средства контроля непрерывности бизнеса, рассматриваемые для охвата специфических высоких рисков).

Четыре варианта обработки рисков не являются взаимоисключающими. Иногда организация может значительно выиграть от объединения вариантов, таких как снижение вероятности риска, уменьшение их последствий и перенос или сохранение любых остаточных рисков.

Некоторые виды обработки рисков могут быть эффективными для более чем одного риска (например, обучение и осведомлённость в части информационной безопасности). План обработки риска должен чётко определять порядок приоритетов, в котором должна реализовываться обработка отдельных рисков. Порядок приоритетов может устанавливаться с использованием различных методов, включая ранжирование рисков и анализ "затраты-выгода". В обязанности руководства входит принятие решения о балансе между затратами на реализацию средств контроля и бюджетными отчислениями.

Идентификация существующих средств контроля может определять те существующие средства контроля, которые превышают текущую потребность также и с точки зрения сравнения затрат, включая поддержку. Если рассматривается удаление избыточных или ненужных средств контроля (особенно, если расходы на поддержку этих средств контроля велики), должны приниматься во внимание факторы информационной безопасности и стоимости. Поскольку средства контроля оказывают влияние друг на друга, удаление избыточных средств контроля может в итоге снизить эффективность использования всех оставшихся средств обеспечения безопасности. Кроме того, может быть дешевле оставить избыточные или ненужные средства контроля, чем удалить их.

Варианты обработки риска должны учитывать:

- как риск осознается затрагиваемыми сторонами;
- наиболее соответствующие пути коммуникации с этими сторонами.

Установление контекста (см. 7.2 - Критерии оценивания риска) даёт информацию о правовых и регулирующих требованиях, которым необходимо следовать организации. Для организаций является риском отказ от соответствия указанным требованиям, в этой связи должны быть рассмотрены варианты обработки для ограничения этой возможности. Все ограничения - организационные, технические, структурные и др., которые определяются в течение деятельности, связанной с установлением контекста, следует принимать во внимание в течение обработки риска.

После того как был определён план обработки риска, необходимо определить остаточные риски. Это включает обновление или повторную операцию оценки риска, принимая во внимание ожидаемый эффект от предполагаемой обработки риска. Если остаточные риски по-прежнему не будут удовлетворять критериям принятия риска организации, может возникнуть необходимость дальнейшей 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 посредством выбора средства контроля так, чтобы остаточный риск мог быть повторно оценён как допустимый.

Руководство по реализации:

Должны быть выбраны соответствующие и обоснованные средства контроля для того, чтобы удовлетворять требованиям, идентифицированным с помощью оценки риска и процесса обработки риска. Такой выбор должен учитывать критерии принятия рисков, а также правовые, регулирующие и договорные требования. Этот выбор должен также

принимать в расчёт стоимость и период реализации средств контроля или технические аспекты, аспекты среды или культурные аспекты. Зачастую можно снизить общие расходы владельца системы с помощью соответствующим образом выбранных средств контроля безопасности.

В целом, средства контроля могут обеспечивать один или несколько из следующих видов защиты: исправление, исключение, предупреждение, уменьшение влияния, сдерживание, обнаружение, восстановление, мониторинг и информированность. Во время выбора средств контроля важно "взвешивать" стоимость приобретения, реализации, администрирования, функционирования, мониторинга и поддержки средств контроля по отношению к ценности защищаемых активов. Кроме того, рентабельность инвестиций с точки зрения снижения риска, и потенциал для использования новых возможностей бизнеса, предоставляемых определёнными средствами контроля. Дополнительно следует обратить внимание на специализированные навыки, которые могут потребоваться для определения и реализации новых средств контроля или модификации существующих.

В ISO/IEC 27002 даётся подробная информация по выбору средств контроля.

Существует много ограничений, которые могут влиять на выбор средств контроля. Технические ограничения, такие как требования к функционированию, вопросы управляемости (требования операционной поддержки) и совместимости могут препятствовать использованию определённых средств контроля или могут вводить ошибку персонала, или аннулирующую средство контроля, вселяя ложное чувство безопасности, или даже увеличивающую риск, по отношению к тому как если бы не имелось никакого средства контроля (например, требования использования сложных паролей без соответствующего обучения, что может привести к записи паролей пользователями). Более того, может произойти так, что средства контроля будут влиять на производительность. Менеджеры должны работать над идентификацией решения, которое удовлетворяет требованиям производительности, в то же время гарантирует достаточную информационную безопасность. Результатом этого первого шага является перечень возможных средств контроля с их стоимостью, выгодой и приоритетом реализации.

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

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

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 оценивания риска.

Примечание - В ISO/IEC 27001 [см. 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 средства контроля и риск может быть сохранен.

9.4 Предотвращение риска

Действие: Следует отказаться от деятельности или условия, вызывающего конкретный риск.

Руководство по реализации:

Когда идентифицированные риски считаются слишком высокими или расходы на реализацию других вариантов обработки риска превышают выгоду, может быть принято решение о полном предотвращении риска путём прекращения программы или отказа от планируемой или существующей деятельности, или совокупности действий или изменения условий, при которых проводится деятельность (действия). Например, в отношении рисков, вызываемых природными факторами, наиболее экономически выгодной альтернативой может быть физическое перемещение средств обработки информации туда, где этот риск не существует или находится под контролем.

9.5 Перенос риска

Действие: Риск должен быть передан (перенесён) той стороне, которая может наиболее эффективно осуществлять менеджмент конкретного риска, в зависимости от оценивания риска.

Руководство по реализации:

Перенос риска включает в себя решение разделить определённые 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 осуществлён страхованием, которое будет поддерживать последствия, или с помощью заключения договора субподряда с "партнёром", чья роль будет заключаться в проведении мониторинга информационной системы и осуществлении немедленных действий по прекращению атаки, прежде чем она приведёт к определённому уровню ущерба.

Следует заметить, что может быть возможным перенести ответственность, связанную с менеджментом риска, но, обычно, невозможно перенести ответственность за ущерб. Клиенты обычно принимают неблагоприятное влияние ущерба, как ошибку организации.

10 Принятие риска информационной безопасности

Входные данные: План обработки риска и оценка остаточного риска является объектом решения руководства организации о принятии риска.

Действие: Должно быть принято и формально зарегистрировано решение о принятии рисков и ответственности за это решение [это связано с ISO/IEC 27001, 4.2.1 h)].

Руководство по реализации:

В планах обработки риска должно описываться то, как оценивать риски, которые следует обрабатывать для того, чтобы соответствовать критериям принятия рисков (см.

7.2 "Основные критерии"). Важно, чтобы ответственные менеджеры пересматривали и поддерживали предлагаемые планы обработки риска и вытекающие из них остаточные риски, а также регистрировали все условия, связанные с поддержкой принятых решений.

Критерии принятия риска могут быть более многогранным аспектом, чем просто 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, поскольку применяемые критерии не учитывают превалирующие обстоятельства. Например, может быть доказано, что необходимо принимать риски по причине выгод, связанных с рисками, которые могут быть очень привлекательными, или потому что расходы, связанные со снижением риска, очень высоки. Такие обстоятельства показывают, что критерии принятия риска являются неадекватными и должны быть по возможности пересмотрены. Однако, не всегда возможно пересмотреть критерии принятия риска своевременно. В таких случаях лица, принимающие решения могут быть обязаны принять риски, которые не соответствуют стандартным критериям принятия. Если это необходимо, лицо, принимающее решение, должно явным образом прокомментировать риски и включить обоснование для решения, превышающего стандартный критерий принятия рисков.

Выходные данные: Перечень принятых рисков с обоснованием тех рисков, которые не соответствуют стандартным критериям принятия риска организации.

11 Обмен информацией относительно риска информационной безопасности

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

Действие: Принимающие решение лица и другие причастные стороны должны обмениваться и/или совместно использовать информацию о риске.

Руководство по реализации:

Обмен информацией относительно риска представляет собой деятельность, связанную с достижением соглашения о том, как осуществлять менеджмент рисков путём обмена и/или совместного использования информации о риске между лицами, принимающими решения, и другими причастными сторонами. Такая информация включает в себя, но не ограничивается, существованием, природой, формой, вероятностью, серьёзностью, обработкой и приемлемостью рисков.

Эффективный обмен информацией относительно между причастными сторонами имеет большое значение, поскольку она может оказывать существенное влияние на решения, которые должны быть приняты. Обмен информацией будет обеспечивать уверенность в том, что лица, отвечающие за осуществление менеджмента риска, и лица, относящиеся к заинтересованным кругам, понимают основу, на которой принимаются решения, и причины необходимости определённых действий. Обмен информацией относительно риска является двунаправленным.

Осознание риска может отмечаться из-за различий в предположениях, понятиях, потребностях, проблемах и беспокойствах причастных сторон, которые связаны с риском или обсуждаемыми проблемами. Причастные стороны, вероятно, 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 идентифицировано и задокументировано, а лежащие в основе причины были чётко поняты и учтены.

Обмен информацией относительно риска должен 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 возникновения и последствий нарушений информационной безопасности из-за отсутствия взаимопонимания между принимающими решения лицами и причастными сторонами;
- поддержки принятия решений;
- получения новых знаний об информационной безопасности;
- координации с другими сторонами и планирования реагирования для уменьшения последствий какого-либо инцидента;
- выработки чувства ответственности по отношению к рискам у лиц, принимающих решения, и причастных сторон;
- повышения осведомлённости.

Организация должна разрабатывать планы обмена информацией относительно риска, как для обычного функционирования, так и для чрезвычайных ситуаций. Следовательно, деятельность по обмену информации должна выполняться непрерывно.

Координация между лицами, принимающими окончательные решения, и иными причастными сторонами, может быть достигнута посредством формирования соответствующих коллегиальных органов (комитетов), где могут проходить обсуждения вопросов о рисках, их приоритезации и выработке решений по обработке и принятию рисков.

Важно сотрудничать с соответствующим отделом по связям с общественностью или коммуникациям в организации, чтобы координировать все задачи, связанные с обменом информацией относительно риска. Это критически важно в случаях сообщения о действиях в кризисных ситуациях, например, в ответ на определённые инциденты.

Выходные данные: Постоянное понимание процесса менеджмента риска информационной безопасности организации.

12 Мониторинг и пересмотр риска информационной безопасности

12.1 Мониторинг и пересмотр факторов риска

Входные данные: Вся информация о рисках, полученная в результате действий по менеджменту риска (см. рисунок 2).

Действие: Риски и их факторы (т. е. ценность активов, влияние, угрозы, уязвимости, вероятность возникновения) должны подвергаться мониторингу и пересмотру с целью идентификации любых изменений в контексте организации на ранней стадии, и поддерживать пересмотр всей картины риска.

Руководство по реализации:

Риски не остаются статичными. Угрозы, уязвимости, вероятность или последствия могут изменяться неожиданно, без каких-либо признаков. Поэтому для обнаружения таких изменений необходим непрерывный мониторинг. Это может поддерживаться внешними сервисами, которые обеспечивают информацию о новых угрозах или уязвимостях.

Организации должны обеспечивать, чтобы проводился непрерывный мониторинг следующих факторов:

- новые активы, которые были включены в область действия менеджмента риска;

- необходимая модификация ценности активов, например, вследствие изменившихся бизнес-требований;
- новых угроз, которые могут быть активными вне и внутри организации, и которые ещё не оценивались;
- вероятности того, что новые или увеличившиеся уязвимости могут позволить угрозам использовать эти новые или изменившиеся уязвимости;
- идентифицированные уязвимости для определения тех уязвимостей, которые становятся подверженными новым или повторно возникающим угрозам;
- повышенное влияние последствий оценённых угроз, уязвимостей и рисков, объединение которых имеет результатом неприемлемый уровень риска;
- инциденты информационной безопасности.

Новые угрозы, уязвимости или изменения вероятности или последствий могут увеличивать риски, которые ранее были оценены как низкие. Процесс пересмотра низких и принятых рисков должен рассматривать каждый риск отдельно, а также все эти риски как совокупное целое, чтобы оценивать их потенциальное 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 существующих угроз, могут изменяться, как могут изменяться факторы, влияющие на применимость или стоимость различных вариантов обработки. Главные изменения, влияющие на организацию, должны служить основанием для более специфического пересмотра. Следовательно, действия по мониторингу риска должны регулярно повторяться, и выбранные варианты обработки риска должны периодически пересматриваться.

Результаты действия по мониторингу риска может быть входными данными к другим действиям по пересмотру рисков. Организация должна пересматривать все риски регулярно, и когда имеют место значительные риски (в соответствии с ISO/IEC 27001, 4.2.3).

Выходные данные: Непрерывное согласование менеджмента рисков с бизнес-целями организации и критериями принятия риска.

12.2 Мониторинг, анализ факторов риска

Входные данные: Вся информация о рисках, полученная в результате действий по менеджменту риска (см. рисунок 2).

Действие: Процесс менеджмента риска информационной безопасности должен постоянно подвергаться мониторингу, пересмотру и улучшению, необходимым и соответствующим образом.

Руководство по реализации:

Постоянный мониторинг и пересмотр необходимы для обеспечения уверенности в том, что контекст, результат оценки риска и обработки риска, а также планы менеджмента остаются уместными и соответствующими обстоятельствам.

Организации должны обеспечивать уверенность в том, что процесс менеджмента риска информационной безопасности и связанные с ним действия остаются соответствующими при текущих обстоятельствах и соблюдаются. О любых согласованных улучшениях процесса или действиях, необходимых для повышения соответствия процессу, следует уведомлять соответствующих менеджеров, чтобы обеспечить уверенность в том, что не существует ни одного риска или элемента риска, упущенного или недооценённого, и что необходимые действия предпринимаются, и

решения принимаются для получения реалистичного представления риска и способности реагировать на него.

Кроме того, организация должна регулярно проверять, что критерии, используемые для измерения риска и его элементов, по-прежнему остаются действительными и согласующимися с бизнес-целями, стратегиями и политиками, и что изменения бизнес-контекста принимаются во внимание на адекватном уровне во время процесса менеджмента риска информационной безопасности. Эта деятельность по мониторингу и пересмотру должна уделять внимание (но не ограничиваться) следующему:

- правовому контексту и контексту окружающей среды;
- контексту конкуренции;
- подходу к оценке риска;
- ценности и категориям активов;
- критериям влияния;
- критериям оценивания риска;
- критериям принятия риска;
- полной стоимости эксплуатации активов;
- необходимым ресурсам.

Организация должна обеспечивать уверенность в том, что ресурсы оценки риска и обработки риска были постоянно доступны для пересмотра 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:

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

Выходные данные: Непрерывная значимость процесса менеджмента риска информационной безопасности для бизнес-целей организации.

Приложение А
(информационное)
Определение области применения и границ процесса менеджмента рисков информационной безопасности

А.1 Анализ организации

Анализ организации. Изучение организации даёт возможность воспроизвести характерные элементы, определяющие особенности организации. Это касается цели, бизнеса, назначения, ценностей и стратегий организации. Они должны быть определены наряду с элементами, способствующими их развитию (например, заключение контрагентских договоров).

Трудность такой деятельности заключается в точном понимании структуры организации. Определение её реальной структуры даёт понимание роли и важности каждого подразделения в достижении целей организации.

Например, тот факт, что ответственный по информационной безопасности отчитывается перед высшим руководством, а не перед руководством ИТ, может указывать на участие высшего руководства в вопросах информационной безопасности

Основная цель организации. Основная цель организации может определяться как причина того, почему она существует (её сфера деятельности, сегмент рынка и т.д.).

Её бизнес. Бизнес организации, определяемый методами и накопленным опытом (ноу-хау) её сотрудников, даёт ей возможность реализовывать своё назначение. Он является специфичным полем деятельности организации и зачастую определяет её культуру труда.

Её назначение. Организация достигает своей цели посредством реализации своего назначения. Для определения её назначения, обеспечиваемые сервисы и изготавливаемые продукты должны быть определены по отношению к конечному пользователю.

Её ценности. Ценностями являются основные принципы или хорошо определённый кодекс поведения, применяемые для осуществления бизнеса. Это может касаться персонала, отношений с внешними агентами (клиентами, например), качества поставляемых продуктов или обеспечиваемых сервисов.

В качестве примера возьмём организацию, целью которой является государственная служба, бизнесом (деятельностью) - транспортные услуги, а назначение заключается в перевозке детей в школу и обратно. Её ценностями могут быть пунктуальность сервиса и безопасность перевозок.

Структура организации. Существуют разные типы структуры:

- филиальная структура: каждое подразделение работает под руководством менеджера подразделения, ответственного за принятие стратегических, административных и операционных решений, касающихся его подразделения;
- функциональная структура: функциональное руководство осуществляется относительно процедур, сущности работы и, иногда, принятия решений или планирования (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 на диаграмме организации. При таком представлении главное место должно отводиться линиям отчётности и делегирования полномочий, кроме того, оно также должно включать в себя и другие отношения, которые, даже если они не основываются на каких-либо формальных полномочиях, являются, тем не менее, линиями информационного потока.

Стратегия организации. Для этого требуется формальное выражение руководящих принципов организации. Стратегия организации определяет направление и развитие, необходимые для извлечения выгоды из вопросов "делания ставок" и планируемых ею основных изменений.

A.2 Перечень ограничений, влияющих на организацию

Следует принимать во внимание все ограничения, влияющие на организацию и определяющие цели её информационной безопасности. Их источник может находиться в пределах организации, и в данном случае она имеет некоторый контроль над ними, или за пределами организации и, следовательно, не может контролироваться. Отдельными наиболее важными являются ограничения ресурсов (бюджетных, кадровых) и ограничения, связанные с непредвиденными случаями.

Организация устанавливает свои цели (касающиеся её бизнеса, режима работы и т.д.), подчиняя их определённому образу действий, возможно, в течение длительного периода времени. Она определяет, какой организацией она хочет стать, и средства, которые для этого потребуются. Устанавливая такую последовательность действий, организация принимает во внимание эволюцию методов и ноу-хау, высказанные пожелания пользователей, клиентов и т.д. Данная цель может быть выражена 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, характеристики, касающиеся особенности, назначения и стратегии организации, являются основополагающими элементами в анализе проблемы, поскольку аспект нарушения безопасности может привести к переосмыслению этих стратегических целей. Кроме того, важно, чтобы предложения относительно требований безопасности находились в соответствии с правилами, режимами эксплуатации и средствами, применяемыми в организации.

Перечень ограничений включает в себя, но не ограничивается, следующим:

Ограничения политического свойства

Они могут касаться правительственных администраций, общественных учреждений или, говоря в общем, любой организации, которая должна применять правительственные решения. Такими обычно являются решения, касающиеся стратегии или эксплуатационной ориентации, принятые правительственным подразделением или организацией, принимающей решения, и которые должны быть применены.

Например, компьютеризация счетов или административных документов влечёт за собой проблемы с информационной безопасностью.

Ограничения стратегического свойства

Ограничения могут возникать в результате запланированных или возможных изменений структуры или ориентации организации. Они могут отражаться в стратегических или эксплуатационных генеральных планах организации.

Например, международное сотрудничество в области совместного использования чувствительной информации может потребовать соглашений, касающихся безопасного обмена.

Территориальные ограничения

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

Примеры 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 определённых событий, таких как забастовки или национальные или международные кризисы.

Например, некоторые сервисы могут продолжать функционирование даже во время серьёзных кризисов.

Структурные ограничения

Тип структуры организации (филиальная, функциональная или другая) может иметь следствием определённую политику информационной безопасности и организацию безопасности, адаптированную к структуре.

Например, международная структура должна быть способна согласовывать требования безопасности, присущие каждой стране.

Функциональные ограничения

Функциональные ограничения возникают непосредственно из главного или специфического назначения организации.

Например, 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, осведомлённостью в вопросах безопасности, мотивацией, доступностью и т.д.

Например, весь персонал оборонной организации должен иметь допуск для обработки совершенно секретной информации.

Ограничения, на возникновение которых влияет календарь организации

Такие ограничения могут быть результатом реструктуризации или планирования новых национальных или международных политик, устанавливающих определённые конечные сроки.

Например, создание секретного отдела.

Ограничения, связанные с методами

Методы, соответствующие накопленному опыту (ноу-хау) организации, необходимо устанавливать в отношении таких аспектов, как планирование проекта, спецификации, разработка и т.д.

Например, 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 определённой "культуры" организации, которая может быть несовместимой со средствами управления безопасностью. Такая культура является основной "системой отсчёта" персонала, и она 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 средства управления безопасностью могут стоить иногда очень дорого. Несмотря на то, что не всегда уместно строить инвестирование безопасности на экономической эффективности, финансовые отделы организации требуют, как правило, экономического обоснования.

Например, в частном секторе и некоторых общественных организациях совокупные расходы на средства управления безопасностью не должны превышать издержек от возможных последствий рисков. Высшее руководство должно, поэтому, оценивать и принимать вычисленные риски, если оно желает избежать чрезмерных расходов, связанных с обеспечением безопасности.

A.3 Перечень законодательных и регулирующих норм, имеющих отношение к деятельности организации

Должны определяться регулирующие 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, вообще, любых обязательств юридического свойства.

A.4 Перечень ограничений, влияющих на область применения

При идентификации ограничений желательно перечислить те, которые влияют на область применения, и определить те, на которые все же возможно некоторое воздействие. Они дополняются к ограничениям организации, перечисленным выше, и, возможно, могут изменить их. Далее представляется перечень возможных типов ограничений, не являющийся 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, что на данный процесс будут влиять все подпроцессы другого процесса.

Технические ограничения

Технические ограничения, относящиеся к инфраструктуре, в основном возникают в результате эксплуатации аппаратных и программных средств, 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, распределённая, клиент-сервер), физическая архитектура и т.д.);
- прикладное программное обеспечение (требования, касающиеся проектирования специфичного программного обеспечения, рыночные стандарты и т.д.);
- пакеты программного обеспечения (требования, касающиеся стандартов, уровня оценивания, качества, соответствия нормам, безопасности и т.д.);
- аппаратные средства (требования, касающиеся стандартов, качества, соответствия нормам и т.д.);
- сети связи (требования, касающиеся покрытия, стандартов, ёмкости, надёжности и т.д.);
- инфраструктура сооружений и инженерных коммуникаций (требования, касающиеся гражданского строительства, конструкций, высокого напряжения, низкого напряжения и т.д.).

Финансовые ограничения

Реализация средств управления безопасностью зачастую ограничивается тем бюджетом, который может выделить организация. Однако, финансовое ограничение должно по- прежнему оставаться последним, что подлежит рассмотрению, поскольку вопрос о выделении бюджета на безопасность может быть решён на основе анализа безопасности.

Ограничения, связанные со средой

Ограничения, связанные со средой, возникают от географической среды или состояния экономики, в которой процессы реализуются: страна, климат, природные риски, географическая ситуация, состояние экономики и т.д.

Ограничения по времени

Время, необходимое для реализации средств управления безопасностью, должно рассматриваться в отношении возможности модернизации информационных систем; если время реализации очень длительное, то риски, для которых разрабатывалось управление, изменяются. Время является определяющим фактором при выборе решений и приоритетов.

Ограничения, касающиеся методов

Методы, подходящие для секретов производства (ноу-хау) организации, должны использоваться в отношении планирования проекта, спецификации, разработки и т.д.

Организационные ограничения

Различные ограничения могут следовать из требований организации, а именно:

- эксплуатация (требования, касающиеся длительности производственного цикла, обеспечения сервисов, наблюдения, мониторинга, "чрезвычайных" планов, ухудшения работы и т.д.);
- поддержка (требования к поиску неисправностей, связанных с инцидентом, превентивным действиям, быстрому исправлению и т.д.);
- менеджмент кадровых ресурсов (требования, касающиеся обучения оператора и пользователя, квалификации, необходимой для таких должностей, как системный администратор или администратор данных и т.д.);
- административный менеджмент (требования, касающиеся обязанностей и т.д.);
- менеджмент разработки (требования, касающиеся инструментальных средств разработки, систем автоматизированной разработки программ, планов приёмочного контроля, обеспечения организации и т.д.);
- менеджмент внешних отношений (требования, касающиеся организации отношений с третьей стороной, договоров и т.д.).

Приложение B
(информационное)
Идентификация и определение ценности активов, определение стоимости воздействия

B.1 Примеры идентификации актива

Чтобы определить ценность актива, организация сначала должна идентифицировать свои активы (на соответствующем уровне детализации). Можно отличить два вида активов:

- первичные активы:
    - бизнес-процессы и действия;
    - информация;
- активы поддержки (на которые полагаются первичные элементы области применения) всех типов:
    - аппаратные средства;
    - программное обеспечение;
    - сеть;
    - персонал;
    - сайт;
    - организационная структура.

B.1.1 Идентификация первичных активов

Что касается более точного описания области применения, данная деятельность заключается в идентификации основных активов (бизнес-процессы и бизнес-деятельность, информация). Такая идентификация осуществляется представителями совместной рабочей группы, принимающей участие в процессе (менеджеры, специалисты в сфере информационных систем, пользователи и др.).

Основными активами обычно являются базовые процессы и информация о деятельности организации в границах процесса менеджмента риска. Могут рассматриваться также и другие основные активы, такие как процессы жизнедеятельности организации, которые будут иметь отношение к формированию политики информационной безопасности или плана непрерывности бизнеса. Основными активами являются информационные активы или "неосязаемые активы", которые необходимо защищать. В зависимости от цели, для некоторых случаев не потребуется исчерпывающий анализ всех элементов, входящих в границы процесса 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 выполнение целевой задачи организации;
- процессы, включающие в себя секретные процессы или процессы, созданные с использованием высокоуровневой технологии;
- процессы, модификация которых может значительно повлиять на выполнение назначения организации;
- процессы, которые необходимы организации для выполнения договорных, правовых или регулирующих требований;

2. информация:

Говоря более обобщённо, основная информация, главным образом, включает в себя:

- информацию, необходимую для реализации назначения или бизнеса организации;
- информацию личного характера, если она может быть определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни;
- стратегическую информацию, необходимую для достижения целей, определяемых стратегией деятельности организации;
- информацию с высокой себестоимостью, сбор, хранение, обработка и передача которой требуют продолжительного времени и/или связаны с большими затратами на её приобретение.

Процессы и информация, которые не были идентифицированы как чувствительные относительно данной деятельности, не будут иметь определённой классификации в оставшейся части исследования. Это означает, что если даже такие процессы или информация будут скомпрометированы, организация по-прежнему будет успешно осуществлять свою деятельность.

Тем не менее, они часто будут наследовать средства управления, реализуемые для защиты процессов и информации, идентифицированных как чувствительные.

B.1.2 Перечень и описание вспомогательных средств

Сфера рассмотрения состоит из активов, которые должны быть идентифицированы и описаны. Этим активам присущи уязвимости, которые могут быть использованы угрозами, нацеленными на ухудшение основных активов сферы рассмотрения (процессов и информации). Они могут быть различных типов:

Аппаратные средства

Тип "аппаратные средства" включает в себя все физические элементы, поддерживающие процессы.

Аппаратура обработки данных (активная)

Аппаратура автоматизированной обработки информации состоит из элементов, которые требуются ей для независимой работы.

Мобильная аппаратура

Портативная вычислительная техника.

Примеры: портативный компьютер (ноутбук), PDA- персональный цифровой секретарь (карманный компьютер).

Стационарная аппаратура

Вычислительная техника, используемая в помещениях организации.

Примеры: сервер, микрокомпьютер, используемый в качестве рабочей станции.

Периферийное обрабатывающее оборудование

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

Примеры: принтер, сменный дисковод.

Носитель данных (пассивный)

Это носители для хранения данных или функций.

Электронный носитель

Носитель информации, который может быть подсоединён 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.

Примеры: гибкие диски, CD ROM, резервный картридж, сменный жёсткий диск, ключ защиты памяти, магнитная лента.

Другие носители

Статичные, неэлектронные носители, содержащие данные.

Примеры: бумага, слайд, диапозитив, документация, факс.

Программное обеспечение

Программное обеспечение состоит из всех программ, содействующих 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 операционной системы и иных сопутствующих приложений. В зависимости от архитектуры операционная система может быть монолитной или состоя шей 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, характеризуемое тем фактором, что оно дополняет сервисы операционной системы, но не обслуживает непосредственно пользователей или приложения (даже если это обычно является важным или даже обязательным для общей работы информационной системы).

Пакетное программное обеспечение или стандартное программное обеспечение

Стандартное программное обеспечение или пакетное программное обеспечение являются завершёнными продуктами, предназначенными для получения прибыли (а не являющимися 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.

Примеры: программное обеспечение менеджмента базы данных, программное обеспечение электронного обмена сообщениями, программное обеспечение коллективного пользования, программное обеспечение директорий, программное обеспечение Web-сервера и т.д.

Бизнес-приложение

Стандартное бизнес-приложение

Таковым является коммерческое программное обеспечение, предназначенное для предоставления пользователям прямого доступа к сервисам и функциям, требуемым ими от своей информационной системы в своём профессиональном контексте. Существует огромное, практически безграничное разнообразие видов такого программного обеспечения.

Примеры: программное обеспечение учётных 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

Таковым является программное обеспечение, в котором различные аспекты (главным образом, поддержка, сопровождение, модернизация и т.д.) были разработаны специально, чтобы предоставлять пользователям прямой доступ к сервисам и функциям, требуемым ими от своей информационной системы. Существует огромное, практически безграничное, разнообразие видов такого программного обеспечения.

Примеры: 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 удалённых 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 7-уровневой модели взаимодействия открытых систем).

Примеры: 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 в себя 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, используя связные коммутаторы и маршрутизаторы с фильтрами. Управление ими зачастую может осуществляться на расстоянии, и обычно они способны генерировать журналы регистрации.

Примеры: мост, маршрутизатор, концентратор, 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 удалённого управления.

Примеры: пакетная радиосвязь общего назначения (GPRS - General Packet Radio Service), Ethernet-адаптер.

Персонал

Тип "персонал" состоит из всех групп лиц, участвующих в работе информационной системы

Лицо, принимающее решения

Лицами, принимающими решения, являются владельцы основных активов (информации и функций) и менеджеры организации или определённого проекта.

Примеры: высшее руководство, руководитель проекта.

Пользователи

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

Примеры: менеджмент кадровых ресурсов, финансовый менеджмент, менеджер 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.

Примеры: системный администратор, администратор данных, оператор резервирования, справочного стола, использования приложений, сотрудники службы безопасности.

Разработчик

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 о выпуске продукции.

Примеры: 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 её функционирования.

Размещение

Внешняя среда

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

Примеры: 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.

Примеры: штат организации, здания.

Зона

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

Примеры: офисы, зарезервированная зона доступа, безопасная зона.

Основные сервисы

Все сервисы, необходимые для функционирования оборудования организации.

Связь

Телекоммуникационные сервисы и оборудование, обслуживаемые оператором.

Примеры: телефонная линия, учрежденческая АТС 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.

Примеры: источники электропитания с низким напряжением, инвертор, распределительное устройство электрической цепи.

Водоснабжение

Удаление отходов

Сервисы и средства (оборудование, контроль) для охлаждения и очистки воздуха.

Примеры: 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

Это такие структуры, от которых указанная организация получает свои полномочия. Они могут быть юридически аффилированными или внешними. Это налагает ограничения на оцениваемую организацию в плане правил, решений и действий.

Примеры: контролирующая организация, правление организации.

Структура организации

Она состоит из различных отделений организации, включая деятельность организации с пересекающимися функциями под управлением её менеджмента.

Примеры: кадровый менеджмент, менеджмент ИТ, снабженческий менеджмент, менеджмент бизнес-подразделений, служба безопасности зданий, пожарная служба, менеджмент аудита.

Организация проекта или системы

Здесь речь идёт об организации, созданной для определённого проекта или сервиса.

Примеры: проект разработки нового приложения, проект миграции информационной системы.

Контрагенты/поставщики/изготовители

Это организация, обеспечиваются данную организацию сервисом или ресурсами, и связанная с ней договором.

Примеры: компания по управлению оборудованием, аутсорсинговая компания, консалтинговые компании.

B.2 Определение ценности активов

Следующий шаг после определения активов состоит в согласовании используемой шкалы и критериев присваивания каждому активу определённого положения на шкале, основанного на ценности. Вследствие разнообразия активов, встречающихся в большинстве организаций, вероятно, что некоторые активы, имеющие известную денежную ценность, будет 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 определения ценности активов, включают такие определения, как: 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 определения ценности активов, поскольку ценность некоторых активов, возможно, должна определяться субъективно и поскольку много разных людей, вероятно, будут принимать решения. 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.

Ещё одной основой для определения ценности активов являются расходы, понесённые из- за потери конфиденциальности, целостности и доступности в результате инцидента. Неотказуемость, учётность, подлинность и надёжность также должны рассматриваться соответствующим образом. Такое определение ценности должно

обеспечить 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 определения 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 ценности для конкурентов. Все эти присвоенные значения ценности скорее всего будет значительно отличаться. 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 счёте, все определения ценности активов должны быть сведены к общей основе. Это можно сделать с помощью критериев, таких, как приведённые ниже. Критерии, которые могут использоваться для оценки возможных последствий, вытекающих из потери конфиденциальности, целостности, доступности, неотказуемости, учётности, подлинности или надёжности активов, включают:

- нарушение законодательства и/или предписаний;
- 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 может быть:

- прерывание сервиса:
  - невозможность обеспечения сервиса;
- утрата доверия клиента:
  - утрата доверия международной информационной системе;
  - потеря репутации;
- нарушение внутреннего функционирования:
  - непосредственно в организации;
  - дополнительные внутренние расходы;
- нарушение функционирования третьей стороны:
  - помехи для третьих сторон, ведущих дела с организацией;
  - различные виды убытков;
- нарушение законов/предписаний:
  - 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 непредвиденными случаями или ремонтом:
        - касающиеся персонала;
        - касающиеся оборудования;
        - касающиеся исследований, отчётов экспертов;
    - потеря товаров/денежных средств/активов;
    - потеря клиентов, потеря поставщиков;
    - судебные дела и штрафы;
    - потеря конкурентного преимущества;
    - потеря технологического/технического лидерства;
    - потеря эффективности/надёжности;
    - потеря технической репутации;
    - снижение способности к заключению соглашений;
    - промышленный кризис (забастовки);
    - правительственный кризис;
    - увольнения;
    - материальный ущерб.

Эти критерии являются примерами вопросов, которые должны рассматриваться при определении ценности активов. Для проведения оценок организации нужно выбрать критерии, уместные для её вида бизнеса и требований безопасности. Это может означать, что некоторые из перечисленных выше критериев будут неприменимыми и что может потребоваться добавить другие к этому списку.

Шкала

После установления критериев для рассмотрения организация должна согласовать шкалу, которая будет использоваться в масштабах организации. Первым шагом является принятие решения о числе используемых уровней. Не существует правил, касающихся того, какое число уровней является наиболее уместным. Большее количество уровней обеспечивает больший уровень детализации, но иногда слишком тонкое разграничение 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 определить собственные границы для ценности активов, такие как "низкая", "средняя" или "высокая". Эти границы должны оцениваться в соответствии с выбранными критериями, (например, для возможных финансовых потерь они должны быть даны в денежном выражении, но при рассмотрении такого вопроса как угрозы личной безопасности, определить денежную ценность может быть затруднительно и может быть неуместно для всех организаций). Наконец, решение о том, что считать "слабыми" или "сильными" последствиями, полностью зависит от организации. Последствия, которые могут быть катастрофическими для небольшой организации, могут быть слабыми или даже незначительными для очень крупной организации.

Зависимости

Чем более значимые и многочисленные бизнес-процессы поддерживаются активом, тем больше ценность этого актива. Должна быть также идентифицирована зависимость активов от других активов, 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. потребности безопасности хранения данных и программ обработки данных должны быть напрямую

связаны с ценностью, представляющей конфиденциальность хранящихся и обрабатываемых данных. Также, если бизнес-процесс зависит от целостности определённых данных, создаваемых программой, входные данные этой программы должны иметь соответствующую степень надёжности. Кроме того, целостность информации будет зависеть от аппаратных и программных средств, используемых для её хранения и обработки. Аппаратные средства будут также зависеть от энергоснабжения и, возможно, от кондиционирования воздуха. Таким образом, информация о зависимостях поможет в идентификации угроз и особенно уязвимостей. Кроме того, это поможет обеспечить, чтобы активам присваивалось правильное значение ценности (благодаря зависимым взаимосвязям), показывая, таким образом, соответствующий уровень защиты.

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

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

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

Результат

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

B.3 Оценка влияния

Инцидент безопасности 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, происходящим в результате инцидента. Влияние рассматривается как имеющее либо незамедлительный (операционный) эффект, либо будущий (бизнес-) эффект, который включает финансовые и рыночные последствия.

Непосредственное (операционное) влияние бывает прямым или косвенным.

Прямое:

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

Косвенное:

a) a) издержки упущенных возможностей (финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте);
b) стоимость прерванных операций;
c) c) возможное злоупотребление информацией, полученной в результате нарушения безопасности;
d) нарушение установленных законом или регулятивных обязательств;
e) e) нарушение этических норм поведения.

Как таковая, первая оценка (без защитных мер любого рода) будет оценивать влияние как очень близкое к (комбинации) ценности связанного с этим актива (активов). В каждой следующей итерации для этого (этих) актива (активов) влияние будет отличаться (обычно будет гораздо ниже) из-за наличия и эффективности реализованных средств контроля.

Приложение C
(информационное)
Примеры типичных угроз

В приведённой ниже таблице C.1 даны примеры типичных угроз. Этот список может использоваться во время процесса оценки угроз. Угрозы могут быть умышленными, случайными или связанными с внешней средой (природными) и могут иметь результатом, например, ущерб или утрату важных сервисов. Следующий список указывает релевантные для каждого типа угрозы, где D (преднамеренные), A (случайные элемент), E (экологические). D используется для всех намеренных акций, нацеленных на информационные активы, A используется для всех человеческих действий, которые могут случайно повредить информационные активы и E используется для всех инцидентов, которые не основаны на человеческих действиях. Группы угроз не перечисляются в приоритетном порядке.

Тип	Угрозы	Обозначение
Физическое повреждение	Огонь	A, D, E
	Повреждения водой	A, D, E
	Загрязнение	A, D, E
	Значительный инцидент	A, D, E
	Уничтожение оборудования или носителей	A, D, E
	Пыль, коррозия и обледенение	A, D, E
Естественные события	Климатические явления	E
	Сейсмическое явление	E
	Вулканическое явление	E
	Метеорологическое явление	E
	Наводнение	E
Потеря необходимых сервисов	Отказ кондиционирования или системы водоснабжения	A, D
	Потеря электропитания	A, D, E
	Отказ телекоммуникационного оборудования	A, D
Неисправности вследствие излучения	Электромагнитное излучение	A, D, E
	Тепловое излучение	A, D, E
	Электромагнитный импульс	A, D, E
Компрометация информации Компрометация информации	Перехват и отправка компрометированного сигнала	D
	Дистанционный шпионаж	D
	Подслушивание	D
	Кража носителей или документов	D
	Кража оборудования	D

Тип	Угрозы	Обозначение
	Восстановление информации на носителях, отправленных на переработку или бракованных	D
	Обнаружение(раскрытие)	A, D
	Данные из ненадёжных источников	A, D
	Вмешательство в аппаратные средства	D
	Вмешательство в программные средства	D
	Обнаружение местоположения	D
Технические отказы	Отказ оборудования	A
	Сбой оборудования	A
	Насыщение информационной системы	A, D
	Программный сбой	A
	Нарушение ремонтопригодности информационной системы	A, D
Несанкционированные действия	Несанкционированное использование оборудования	D
	Мошенническое копирование программного обеспечения	D
	Использование контрафактного или скопированного программного обеспечения	A, D
	Искажение данных	D
	Незаконная обработка данных	D
Компрометация функций	Ошибка в использовании	A
	Злоупотребление правами	A, D
	Фальсификация прав	D
	Отрицание действий	D
	Нарушение работоспособности персонала	A, D, E

Особое внимание должно быть обращено на человеческие источники угрозы. Они соответственно перечислены в следующей таблице:

Источник угрозы	Мотивация	Возможные последствия
Хакер, крекер(взломщик)	Восстание Эго (самомнение) Вызов (бунтарство) Статус Деньги	• Хакерство • Социальная инженерия • Вторжение в систему, взлом • Несанкционированный доступ в систему
Компьютерный преступник	Разрушение информации Незаконное раскрытие информации Денежно-кредитная выгода Несанкционированное изменение данных	• Компьютерное преступление (например, кибер-преследование) • Мошенническое действие (например, воспроизведение, подражание, перехват) • Информационный подкуп • Имитация • Вторжение в систему
Террорист	Месть Разведка Разрушение Шантаж Политические выгоды Освещение в печати	• Взрыв/Терроризм • Информационная война • Системная атака (например, распределённый отказ в обслуживании) • Проникновение в систему • Вмешательство в систему
Индустриальный шпионаж (компании, иностранные правительства, другие правительственные интересы)	Конкурентное преимущество Экономический шпионаж	• Экономическая разведка • Информационная кража • Хищение персональных данных • Социальная разработка (покушение на неприкосновенность личной жизни) • Проникновение в систему • Несанкционированный доступ в систему (доступ к секретной, частной, и/или связанной с технологией информации)

Источник угрозы	Мотивация	Возможные последствия
Инсайдер (плохо обученные, недовольные, злонамеренные, небрежные, нечестные или уволенные служащие)	Разведка Эго Любопытство Денежная выгода Месть Неумышленные ошибки и упущения (например, ошибка ввода данных, ошибка программирования)	• Нападение на служащего • Шантаж • Просмотр секрета фирмы • Неправильное использование компьютера • Мошенничество и хищение • Информационный подкуп • Ввод фальсифицированных данных, разрушение(искажение) данных • Перехват • Вредоносный код (например, вирус, логическая бомба, троянский конь) • Продажа персональной информации • Системные ошибки • Вторжение в систему • Системный саботаж • Несанкционированный доступ в систему

Приложение D
(информационное)
Уязвимости и методы для оценки уязвимости

D.1 Примеры уязвимости

В приведённой ниже таблице D.1 даны примеры уязвимостей в различных сферах безопасности, включая примеры угроз, которые могут использовать эти уязвимости. Эти списки 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.

Тип	Примеры уязвимости	Примеры угроз
Аппаратные средства	Недостаточное обслуживание / дефектная инсталляция с носителей данных	Нарушение ремонтопригодности информационной системы
	Изъяны схем для периодических замен	Разрушение оборудования или носителей
	Восприимчивость к влажности, пыли, загрязнению	Пыль, коррозия, обледенение
	Чувствительность к электромагнитной радиации	Электромагнитная радиация
	Изъяны эффективного контроля внесения изменений конфигурации	Ошибка в использовании
	Восприимчивость к изменениям напряжения	Потеря источника питания
	Восприимчивость к температурным изменениям	Метеорологическое явление
	Незащищённое хранение	Кража носителей или документов
	Недостаток в осторожности при уничтожении	Кража носителей или документов
	Неконтролируемое копирование	Кража носителей или документов

Тип	Примеры уязвимости	Примеры угроз
Программное обеспечение	Отсутствие или недостаточное программное тестирование	Злоупотребление правами
	Известные недостатки в программном обеспечении	Злоупотребление правами
	Нет 'выхода из системы' при оставлении рабочей станции	Злоупотребление правами
	Передача или многократное использование носителей данных без надлежащего стирания	Злоупотребление правами
	Малое число ревизий	Злоупотребление правами
	Неправильное распределение прав доступа	Злоупотребление правами
	Широко распространённое программное обеспечение	Искажение данных
	Применение прикладных программ к фальшивым данным в терминах времени	Искажение данных

Тип	Примеры уязвимости	Примеры угроз
	Сложный пользовательский интерфейс	Ошибка в использовании
	Изъяны в документировании	Ошибка в использовании
	Установлен неправильный параметр	Ошибка в использовании
	Некорректные даты	Ошибка в использовании

Тип	Примеры уязвимости	Примеры угроз
Сеть	Изъяны идентифицирующих и опознавательных механизмов для пользовательской аутентификации	Подделывание прав
	Незащищённые таблицы паролей	Подделывание прав
	Плохой менеджмент паролями	Подделывание прав
	Запущены ненужные службы	Незаконная обработка данных
	Недоработанное или новое программное обеспечение	Программный сбой
	Неясные или неполные спецификации для разработчиков	Программный сбой
	Изъяны эффективного контроля внесения изменений	Программный сбой
	Неконтролируемая загрузка и использование программного обеспечения	Подделка программного обеспечения
	Изъяны в процедуре резервного копирования	Подделка программного обеспечения
	Изъяны физической защиты здания, дверей и окон	Кража носителей или документов
	Отказ менеджмента от проверки отчётов	Несанкционированное использование оборудования
	Нехватка доказательства посылки или получения сообщения	Отрицание действий
	Незащищённые линии связи	Подслушивание
	Незащищённый чувствительный трафик	Подслушивание
	Плохая совместная проводка	Отказ телекоммуникационного оборудования
	Единственная точка отказа	Отказ телекоммуникационного оборудования
	Изъяны идентификации и аутентификация отправителя и получателя	Подделывание прав
	Опасная сетевая архитектура	Удалённый шпионаж
	Передача паролей в открытом виде	Удалённый шпионаж
	Неадекватный менеджмент сетью (способность системы противостоять ошибкам маршрутизации)	Насыщенность информационной системы
	Незащищённые подключения общедоступной сети	Несанкционированное использование оборудования

Тип	Примеры уязвимости	Примеры угроз
Персонал	Отсутствие персонала	Нарушение доступности персонала
	Неадекватные процедуры вербовки	Уничтожение оборудования или носителей
	Недостаточное обучение безопасности	Ошибка в использовании
	Неправильное использование программного обеспечения и оборудования	Ошибка в использовании
	Изъяны понимания безопасности	Ошибка в использовании
	Нехватка механизмов мониторинга	Незаконная обработка данных
	Неконтролируемая работа внешним штатом или убирающим персоналом	Кража носителей или документов
	Изъяны политики для правильного использования носителей передачи данных и обмена сообщениями	Несанкционированное использование оборудования

Тип	Примеры уязвимости	Примеры угроз
Сайт (место функционирования) организации	Неадекватное и небрежное использование физического контроля доступа к зданию и помещениям	Уничтожение оборудования или носителей информации
	Местоположение в области, восприимчивой к затоплению	Нестабильная мощность сети
	Наводнение	Потеря источника питания
	Нехватка физической защиты создания, дверей и окон	Кража оборудования
	Изъяны формальной процедуры для пользовательской регистрации и де-регистрации	Злоупотребление правом
	Изъяны формального процесса для пересмотра права доступа (диспетчерский менеджмент)	Злоупотребление правом
	Дефицит или недостаточные условия (относительно безопасности) в контрактах с клиентами и/или третьими лицами	Злоупотребление правом
	Изъяны в процедуре для контроля над средствами обработки информации	Злоупотребление правом
	Изъяны регулярных ревизий (диспетчерский менеджмент)	Злоупотребление правом
	Нехватка процедур выявления риска и оценки	Злоупотребление правом
	Недостаточность информации в записях отчётов о неисправности журналах администратора и пользователя	Злоупотребление правом

Тип	Примеры уязвимости	Примеры угроз
Сайт (место функционирования) организации	Неадекватный ответ обслуживающего сервиса	Нарушение ремонтопригодности информационная система
	Изъяны или недостаточное соглашение сервисного обслуживание	Нарушение ремонтопригодности информационная система
	Изъяны процедуры контроля внесения изменений	Нарушение ремонтопригодности информационная система
	Изъяны формальной процедуры для менеджмента документацией СМИБ	Искажение данных
	Изъяны формальных процедур записей для СМИБ, которые делает диспетчерский менеджмент	Искажение данных
	Изъяны формального разрешения для процесса общего доступа информации	Данные из ненадёжных источников
	Изъяны надлежащего распределения обязанностей информационной безопасности	Отрицание действий
	Изъяны планов непрерывности	Отказ оборудования
	Изъяны политики использования почтовой	Ошибка в использовании
	Нехватка процедур для того, чтобы ввести программное обеспечение в эксплуатируемые системы	Ошибка в использовании
	Нехватка отчётов в файлах регистрации администратора и оператора	Ошибка в использовании
	Нехватка процедур для обработки секретных данных	Ошибка в использовании
	Изъяны обязанностей информационной безопасности в описаниях заданий	Ошибка в использовании
	Изъяны или недостаточные условия (относительно информационной безопасности) в контрактах со служащими	Незаконная обработка данных
	Нехватка определённого дисциплинарного процесса в случае информационного инцидента безопасности	Кража оборудования
	Нехватка формальной политики по использованию мобильной компьютерной техники	Кража оборудования
	Нехватка менеджмента активами дистанционного резервирования	Кража оборудования
	Нехватка или недостаточная политика «чистого стола и чистого экрана»	Кража носителей или документов
	Нехватка санкций на средства обработки информации	Кража носителей или документов
	Нехватка установленных контрольных механизмов в случае нарушений правил	Кража носителей или документов

Тип	Примеры уязвимости	Примеры угроз
Сайт (место функционирования) организации	безопасности	
	Нехватка регулярных пересмотров контролей	Несанкционированное использование оборудования
	Нехватка процедур для того, чтобы сообщить об уязвимости безопасности	Несанкционированное использование оборудования
	Нехватка процедур согласования условий с интеллектуальной собственностью	Использование подделки или скопированного программного обеспечения

D.2 Методы оценки технических уязвимостей

Профилактические методы, такие как тестирование информационной системы, могут быть использованы для эффективной идентификации 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 оценивание безопасности;
- тестирование на проникновение;
- проверка кодов.

Автоматизированные инструментальные средства поиска уязвимостей используются для просмотра группы хостов или сети на предмет известных уязвимых сервисов (например, система разрешает использование анонимного протокола передачи файлов (FTP), ретрансляцию отправленной почты). Следует, однако, отметить, что некоторые из потенциальных уязвимостей, идентифицированных автоматизированными инструментальными средствами поиска уязвимостей, могут не представлять реальных уязвимостей в контексте среды системы. 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, потому что этого требует среда. Таким образом, этот метод может давать ошибочные результаты исследования.

Другим методом, который может использоваться для идентификации уязвимостей системы ИКТ во время процесса оценки риска, является тестирование и оценивание 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 средств контроля безопасности системы ИКТ, которые были применены в операционной среде. Задача заключается в том, чтобы удостовериться, что применяющиеся средства контроля соответствуют утверждённой 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 средств контроля безопасности и обеспечение уверенности в том, что защита различных аспектов системы ИКТ обеспечена. Когда тестирование на проникновение используется в процессе оценки риска, оно может применяться для оценки способности системы ИКТ противостоять умышленным попыткам обойти средства контроля безопасности системы. Его задача состоит в тестировании системы ИКТ, с точки зрения

источника угрозы, и в Идентификации 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 идентифицировать 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/исправление, установленные на тестируемой системе. Если во время тестирования эти данные неизвестны, может быть невозможно успешно использовать конкретную уязвимость (например, достичь удалённого обратного соединения), однако все же возможно взломать или перезапустить тестируемый процесс или систему. В таком случае тестируемый объект тоже должен считаться уязвимым.

Методы могут включать в себя следующие вицы деятельности:

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

Приложение E
(информационное)
Подходы в оценке рисков информационной безопасности

E.1 Оценка рисков информационной безопасности высокого уровня

Высокоуровневая оценка даёт возможность определения приоритетов и хронологии действий. По разным причинам, таким как бюджет, одновременная реализация всех средств контроля может быть невозможна, и могут рассматриваться только наиболее критичные риски посредством процесса обработки риска. Также может быть преждевременно начинать детальный менеджмент риска, если реализация предусматривается только в течение года или двух. Для достижения этой цели высокоуровневая оценка может начаться с высокоуровневой оценки последствий, а не с систематического анализа угроз, уязвимостей, активов и последствий.

Другой причиной начать с высокоуровневой оценки является синхронизация с другими планами, связанными с менеджментом изменений (или обеспечением непрерывности бизнеса). Например, нелогично обеспечивать полную защиту системы или приложения, если планируется в ближайшем будущем привлечь для работы с ними внешние ресурсы, хотя все же, возможно, стоит выполнить связанную с риском оценку, чтобы определить вопрос договора о привлечении внешних ресурсов.

Особенности итерации высокоуровневой оценки риска могут включать следующее:

- высокоуровневая оценка риска может иметь дело с более глобальным рассмотрением организации и её информационных систем, когда технологические аспекты рассматриваются как независимые от вопросов, связанных с бизнесом. В результате этого анализ контекста больше сосредотачивается на бизнес- и эксплуатационной среде, чем на технологических компонентах;
- при использовании высокоуровневой оценки риска может рассматриваться более ограниченный перечень угроз и уязвимостей, распределённых по определённых сферам, или для ускорения процесса она может сосредотачиваться на сценариях риска или нападений вместо их элементов;
- риски, представленные в высокоуровневой оценке риска, часто являются более общими сферами риска, чем конкретно идентифицированными рисками. Когда сценарии или угрозы распределяются по сферам, обработка риска предлагает списки средств контроля для каждой сферы. Мероприятия, связанные с обработкой риска, затем пытаются, прежде всего, предложить и выбрать общие средства контроля, являющиеся действенными во всей системе;
- однако из-за того, что при использовании высокоуровневой оценки риска редко рассматриваются технологические детали, она более уместна для обеспечения организационных и нетехнических средств контроля, а также общих аспектов менеджмента технических средств контроля или основных и распространённых технических защитных мер, таких как резервное копирование и антивирусные программы.

Преимущества оценки риска высокого уровня следующие:

- включение первоначального простого подхода, вероятно, должно получить одобрение программы оценки риска;

- должна появиться возможность построения 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 являются менее точными, единственный возможный недостаток состоит в том, что некоторые бизнес-процессы или системы могут не быть идентифицированы как нуждающиеся во вторичной, детальной оценке риска. Этого можно избежать, если существует адекватная информация обо всех аспектах организации, её информации и системах, включая информацию, полученную в результате оценивания инцидентов информационной безопасности.

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; эти факторы могут включать следующее:

- 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, учёности, подлинности и надёжности 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.

Когда 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 информационной безопасности может привести к существенным неблагоприятным последствиям для организации, её бизнес-процессов или её активов, то необходима вторая итерация оценки риска на более детальном уровне для идентификации потенциальных рисков.

E.2 Детальная оценка риска информационной безопасности

Детальный процесс оценки риска информационной безопасности включает в себя тщательную идентификацию и определение ценности активов, оценку угроз этим активам и оценку уязвимостей. Результаты этих мероприятий потом используются для оценки рисков, а затем для идентификации оправданных средств контроля безопасности.

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

Окончательным этапом детальной оценки риска информационной безопасности является оценка общих рисков, находящаяся в центре внимания данного приложения.

Последствия могут оцениваться несколькими методами, включая использование количественных, например денежных, и качественных мер (которые могут быть основаны на использовании таких прилагательных, как умеренные или серьёзные) или их комбинации. Для оценки вероятности возникновения угрозы должны быть установлены временные рамки, в течение которых актив будет обладать ценностью или нуждаться в защите. На вероятность возникновения конкретной угрозы оказывает влияние следующее:

- привлекательность актива или возможное воздействие - применимо при рассмотрении умышленной угрозы со стороны персонала;
- простота преобразования, использующего уязвимость, актива в 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.

Многие методы используют таблицы и объединяют субъективные и эмпирические меры. Более важно, чтобы организация использовала метод, который является для организации удобным, в котором организация уверена и который будет давать воспроизводимые результаты. Несколько примеров основанных на таблицах методов приведено ниже.

E.2.1 Пример матрицы с предопределёнными 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 - Идентифицируется стоимость приобретения или восстановления, а затем переводится в ту же качественную шкалу, которая используется для информации. Кроме того, если считается, что любая прикладная программы 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 говорить о данных, чтобы определить ценность и критичность фактически используемых данных или данных, которые должны храниться, обрабатываться или оцениваться. Опросы облегчают оценку ценности и критичности информации с точки зрения сценариев наихудших случаев, возникновение которых можно разумно предполагать, исходя из неблагоприятных бизнес- последствий, обусловленных несанкционированным раскрытием, несанкционированной модификацией, недоступностью в течение различных периодов времени и разрушением.

Определение ценности выполняется с использованием принципов определения ценности информации, которые охватывают такие вопросы, как:

- личная безопасность;
- личная информация;
- юридические и регулятивные обязательства;
- правоприменение;
- коммерческие и экономические интересы;
- финансовые потери/нарушение деятельности;

- общественный порядок;
- политика и операции бизнеса;
- потеря "неосязаемого капитала";
- договор или соглашение с клиентом.

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

Следующим важным мероприятием 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 угрозами, чтобы вызвать неблагоприятные последствия). Каждый ответ на вопрос даёт баллы. Эти баллы складываются, используя базу знаний, и сравниваются с диапазонами. Это идентифицирует уровни угроз, скажем, на шкале от высокой до низкой и, аналогично, уровни уязвимостей, как показано в приведённом ниже примере таблицы, проводя различия между видами последствий, как будет уместно. Информация для заполнения опросных листов должна собираться из опросов соответствующего технического персонала, представителей отдела кадров, из данных инспекций фактического месторасположения и проверки документации.

Ценность активов, уровни угроз и уязвимостей, относящиеся к каждому виду последствий, приводятся к табличной форме (матрице), такой как представлена ниже, чтобы для каждой комбинации идентифицировать соответствующую меру риска на основе шкалы от 0 до 8. Значения заносятся в матрицу структурированным образом. Пример приведён ниже (см. таблицу Е.1а):

	Вероятность возникновения - угроза	**Низкая(Н)**			**Средняя(С)**			**Высокая(В)**		
	Ослабления в эксплуатации	**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
Значение актива	**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**

Таблица Е.1 а)

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 проявлять осторожность в случае изменения этой ситуации). Теперь соответствующая строка в таблице устанавливается по значению ценности актива, а соответствующая колонка устанавливается по 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 E1 b) является результатом рассмотрения вероятности сценария инцидента, отображённого на количественно оценённое влияние бизнеса. Вероятность сценария инцидента дана посредством угрозы, использующей уязвимость с определённой вероятностью. Таблица отображает эту вероятность на влияние на бизнес, связанное со сценарием инцидента. Получаемый в результате риск измеряется по шкале от 0 до 8, он может быть оценён по отношению к критериям принятия риска. Данная шкала рисков может также отображаться для простого общего рейтинга рисков, например, следующим образом:

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

	Вероятность инцидентного сценария	Очень низкая (очень маловероятно)	Низкая (маловероятно)	Средняя (возможный)	Высокая (применимый)	Очень высокая (часто встречающаяся)
Воздействие 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

Таблица E.1 b)

E.2.2 Пример ранжирования мер угроз риска

Матрица или таблица может быть использована, чтобы связать факторы последствий (ценность активов) с вероятностью возникновения угрозы (принимая в расчёт аспекты уязвимости). Первый шаг состоит в оценивании последствий (ценности активов) по заранее определённой шкале, например, от 1 до 5, для каждого находящегося под угрозой актива (колонка "b" в таблице E.2). Второй шаг состоит в оценивании вероятности возникновения угрозы по заранее определённой шкале, например, от 1 до 5, для каждой угрозы (колонка "c" в таблице). Третий шаг состоит в вычислении меры риска путём умножения ($b^x c$). Наконец, угрозы могут быть ранжированы в порядке соответствующей меры риска. Отметьте, что в этом примере 1 - соответствует наименьшим последствиям и самой низкой вероятности возникновения.

Дескриптор(ы) опасностей	Последствия (активы) ценность (b)	Вероятность распространения угроз (c)	Мера риска (d)	Ранжирование опасности (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

Таблица E.2

Как показано выше, это процедура, позволяющая сопоставлять и ранжировать в порядке приоритетов различные угрозы с разными последствиями и вероятностью возникновения. В некоторых случаях будет необходимо связывать денежные значения с использованными здесь эмпирическими шкалами.

E.2.3 Пример оценка ценности для вероятности и возможных последствий рисков

В этом примере особое внимание уделяется последствиям инцидентов информационной безопасности (то есть, сценариям инцидентов) и определению того, каким системам следует отдавать приоритет. Это выполняется путём 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 угрозы активу.

Потом оценивается значение вероятности. Оно оценивается, исходя из комбинации вероятности возникновения угрозы и простоты использования уязвимости, смотри таблицу E.3 выражающую вероятность осуществления сценария инцидентов.

Вероятность	**Низкая**			**Средняя**			**Высокая**		
Уровень уязвимости	**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
Вероятное значение вышеуказанного	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**

Таблица E.3

Затем, находя пересечение значения ценности актива и значения 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.

Ценность актива	**0**	**1**	**2**	**3**	**4**
Вероятностные значения					
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**

Таблица Е.4

Окончательный шаг заключается в подсчёте всех итоговых баллов активов для активов системы, чтобы получить баллы системы. Эта цифра может использоваться для проведения различий между системами и определения того, обеспечению защиты какой системы следует назначать приоритет.

В следующих примерах беспорядочно выбраны все значения.

Предположите, что у Системы S есть три актива A1, A2 и A3. Также предположите, что есть две угрозы T1 и T2, применимые к системе S. Позвольте значению A1 быть 3, так же позвольте значению актива A2 быть 2 и значение актива A3 быть 4.

Если для A1 и T1 вероятность угрозы низка и вероятность эксплуатации уязвимости является средней, то значение вероятности 1 (см. Таблицу Е.3).

Таблица кадров актива/угрозы A1/T1 может быть получена из Таблицы Е.4 как пересечение актива, оценённого 3 и оценённой вероятности 1, то есть 4. Точно так же для A1/T2 предполагается вероятности угрозы, являющейся средней и вероятность эксплуатации уязвимости высока, смотрим таблицу кадров A1/T2 6.

Теперь может быть вычислена таблица кадров суммы баланса A1T, то есть 10. В Таблице кадров вычислены суммы баланса для каждого актива и соответствующей угрозы. Рассчитываем полную системную таблицу кадров, добавляя A1T + A2T + A3T, чтобы дать ST.

Теперь могут быть сравнены различные системы, чтобы установить приоритеты и также различные активы в пределах одной системы.

Вышеуказанные примеры показаны в терминах информационных систем, однако, подобный подход может быть применён к бизнес-процессам.

Приложение F
(информационное)
Ограничения для снижения риска

При рассмотрении ограничений, относящихся к снижению риска, нужно принимать в расчёт следующие ограничения:

***Временные ограничения**:*

Может существовать много видов временных ограничений. Например, средства контроля должны быть реализованы в течение временного периода, приемлемого для руководителей организации. Ещё один вид временного ограничения - может ли средство контроля быть реализовано в течение срока службы системы или информации. Третьим видом временного ограничения может быть период времени, который руководители организации считают подходящим для подверженности определённому риску.

***Финансовые ограничения**:*

Реализация или поддержка средств контроля 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 средств контроля. Однако в некоторых случаях может не быть возможности достичь желаемой безопасности и уровня принятия риска из-за бюджетных ограничений. Поэтому для разрешения такой ситуации потребуется решение руководителей организации.

Следует проявлять большую осторожность, если бюджет сокращает число или качество средств контроля, подлежащих реализации, так как это может приводить к неявному сохранению более высокого риска, чем планировалось. Установленный для средств контроля бюджет должен использоваться как ограничивающий фактор только со значительной осторожностью.

***Технические ограничения**:*

Технических проблем, таких как совместимость программ или аппаратных средств, легко можно избежать, если их учитывать во время выбора средств контроля. Кроме того, ретроспективная реализация средств контроля для существующего процесса или системы часто затрудняется техническими ограничениями. Эти трудности могут сдвигать баланс средств контроля к процедурным и физическим аспектам безопасности. Может возникнуть необходимость пересмотреть программу обеспечения информационной безопасности, чтобы достичь целей безопасности. Это может происходить, когда средства контроля не отвечают ожидаемым результатам по снижению риска без уменьшения продуктивности.

***Операционные ограничения**:*

Операционные ограничения, такие как потребность работать 24 часа в день, производя все же при этом резервное копирование, могут приводить к сложной и дорогостоящей реализации средств контроля, если они не встраиваются в проект с самого начала.

***Культурные ограничения**:*

Культурные ограничения, касающиеся выбора средств контроля, могут быть характерными для страны, сектора, организации или даже отдела в организации. Не все средства контроля могут применяться во всех странах. Например, возможно реализовать досмотр сумок в странах Европы, но не в странах Ближнего Востока. Культурные

ограничения нельзя игнорировать, потому что многие средства контроля зависят от активной поддержки персонала. Если персонал не понимает необходимость в средстве контроля или не считает его культурно приемлемым, средство контроля станет неэффективным с течением времени.

***Этические ограничения**:*

Этические ограничения могут иметь серьёзные следствия для средств контроля, так как этические принципы меняются на основе социальных норм. Это может препятствовать реализации таких средств контроля, как сканирование сообщений электронной почты, в некоторых странах. Секретность информации может также меняться в зависимости от этических принципов региона или правления. Они могут больше касаться одних секторов индустрии, чем других, например, правительства и здравоохранения.

***Ограничения, связанные с окружающей средой**:*

Факторы окружающей среды, такие как доступное пространство, экстремальные климатические условия, окружающая природная и городская география, могут влиять на выбор средств контроля. 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 средств контроля. Обеспечение соответствия законодательным и регулятивным требованиям может предписывать определённые виды средств контроля, включая обеспечение защиты данных и финансовый аудит, но может также не допускать использования других средств контроля, например, шифрования. Другие законы и предписания, такие как трудовое право, предписания пожарного отдела, правила техники безопасности и охраны здоровья и предписания экономического сектора и т.д., тоже могут влиять на выбор средств контроля.

***Простота использования**:*

Плохой интерфейс человек-технология будет вызывать ошибки персонала и может приводить к бесполезности контроля. Средства контроля должны выбираться с целью обеспечения оптимальной простоты использования наряду с достижением приемлемого уровня остаточного риска для бизнеса. Применение средств контроля, которые трудно использовать, будет влиять на их эффективность, так как пользователи могут пытаться обходить или игнорировать их, насколько это возможно. Сложные средства управления доступом в организации могут способствовать нахождению пользователями альтернативных несанкционированных методов доступа.

***Кадровые ограничения**:*

Следует учитывать доступность и затраты на оплату совокупности специализированных навыков для реализации средств контроля, а также возможность перемещения персонала на разные площадки при неблагоприятных рабочих условиях. Требуемое мастерство для реализации планируемых средств контроля может не быть легко доступным или может быть чрезмерно дорогостоящим для организации. Другие аспекты, такие как тенденция дискриминации некоторыми членами персонала других членов персонала, не проходивших проверку надёжности, могут иметь важные следствия для политик безопасности и практических приёмов обеспечения безопасности. Кроме того, необходимость найма нужных людей для работы и нахождение нужных людей может приводить к найму до завершения проверки надёжности. Требование завершения проверки надёжности до оформления найма представляет собой нормальную и наиболее безопасную практику.

***Ограничения, касающиеся интеграции новых и существующих средств контроля**:*

На интеграцию новых средств контроля в существующую инфраструктуру и взаимозависимости средств контроля часто не обращают внимание. Новые средства контроля может быть нелегко реализовать при наличии несочетаемости или несовместимости с существующими средствами контроля. Например, план по использованию биометрических признаков для физического контроля доступа может вступать в конфликт с существующей системой управления доступом, основанной на наборе личного Идентификационного номера. Стоимость изменения средств контроля с существующих на планируемые должна включать элементы, которые будут добавляться к общим расходам на обработку риска. Возможно, что реализация выбранных средств контроля будет невозможна из-за взаимных помех от существующих средств контроля.

Приложение G
(Информативное)

Различия в определениях между ISO/IEC 27005:2008 и ISO/IEC 27005:2011

Примечание: Это Приложение предназначается для пользователей ISO/IEC 27001:2005. Поскольку некоторые термины и определения отличаются в Руководстве ISO 73:2009 относительно используемых в ISO/IEC 27001:2005, и в последствии в ISO/IEC 27005:2008, это Приложение обобщает все соответствующие изменения.

ISO/IEC 27005:2008 даёт определение терминам	**Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008**	**Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011**
н/д	н/д	3.1 Последствия (consequence): результат события (3.3), влияющего на цели. Примечания: 1. Результатом события может быть одно или более последствий 2. Последствия могут быть ранжированы от позитивных до негативных. Однако применительно к аспектам безопасности последствия всегда негативные. 3. Последствия могут быть выражены качественно и количественно. 4. Начальные последствия могут вырасти через цепную реакцию.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	Менеджмент (control) средства управления риском, включая политики, процедуры, руководства, методы или организационные структуры, которые могут быть административными, техническими, управляющими, или легальными по природе. Примечание, Менеджмент также используется в качестве синонима для гарантии или контрмеры. [ISO/IEC 27002:2005]	3.2 Менеджмент (control): мера, которая изменяет риск (определение 3.9). [Руководство ISO 73:2009] Примечания: 1. Средства менеджмента для информационной безопасности включают любой процесс, политику, процедуру, направляющую линию, практику или организационную структуру, которая может быть административной, технической, управляющей, или законодательно принятой, которые изменяют риск информационной безопасности. 2. Средств менеджмента, возможно, не всегда проявляют намеченный или принятый эффект изменения. 3. Менеджмент также используется в качестве синонима для гарантии или контрмеры.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	н/д	3.3 Событие (event): Возникновение или изменение определённого набора обстоятельств. [Руководство ISO 73:2009] Примечания: 1. Событие может возникать один раз или несколько и может иметь несколько причин. 2. Событие может состоять в том, что либо не произошло. 3. Событие может иногда упоминаться как «инцидент» или «происшествие».

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	н/д	3.4 Внешний контекст (external context): Внешняя среда, в которой организация стремится к достижению своих целей [Руководство ISO 73:2009] Примечания: Внешний контекст может включать: • культурную, социальную, политическую, правовую, законодательную, финансовую, технологическую, экономическую, природную и рыночную среду на международном, региональном, национальном или локальном уровне; • основные факторы и тенденции, влияющие на цели организации; • взаимосвязи с заинтересованными сторонами, их восприятие и ценности.
3.1 Влияние (impact): Неблагоприятное изменение уровня достигнутых бизнес-целей		Определение удалено

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
3.2 Риск информационной безопасности (information security risk): Возможность того, что данная угроза будет использовать уязвимости актива или группы активов и, тем самым, нанесёт вред организации. Примечание - Он измеряется исходя из комбинации вероятности события и его последствия.		Определение удалено (см. примечание 6 в 3.9)

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	н/д	3.5 Внутренний контекст (internal context): Внутренняя среда, в которой организация стремится к достижению своих целей [Руководство ISO 73:2009] Примечания: Внутренний контекст может включать: • руководство, организационную структуру, функции и обязательства; • политику, цели и стратегии для их достижения; • возможности, рассматриваемые в отношении ресурсов и знаний (например, капитал, время, персонал, процессы, системы и технологии); • информационные системы, информационные потоки и процессы принятия решений (как официальные, так и неофициальные); • взаимосвязи с внутренними заинтересованными сторонами, их восприятие и ценности; • культуру организации; • стандарты, руководящие указания

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
		и модели, принятые организацией; • форму и объем контрактных взаимоотношений.
н/д	н/д	3.6 Уровень риска (level of risk): Величина риска (3.9) или комбинации рисков, выраженная как сочетание последствий (3.1) и их возможности (3.7) возникновения. [Руководство ISO 73:2009]

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	н/д	3.7 Возможность (likelihood): Вероятность наступления некоторого события. [Руководство ISO 73:2009] Примечания: 1. В терминологии менеджмента риска термин «возможность» используется в отношении возможности того, что может произойти, либо определённое, измеренное или установленное объективно или субъективно, качественно или количественно, либо описанное с использованием общих условий или математически (например, вероятность или периодичность в заданный период времени). 2. Английский термин «likelihood» не имеет прямого эквивалента в некоторых языках, вместо него часто используют термин «probability». Однако, в английском языке термин «probability» часто интерпретируют в узком смысле, как математический термин.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
		Следовательно, в терминологии менеджмента риска термин «likelihood» используют с тем намерением, что он должен иметь ту же самую широкую интерпретацию, которую термин «probability» имеет во многих языках, кроме английского языка.
н/д	Остаточный риск(residual risk): риск, остающийся после обработки риска [ISO/IEC 27001:2005]	3.8 Остаточный риск (residual risk): Риск (3.9), сохраняющийся после обработки риска (3.17) [Руководство ISO 73:2009] Примечания: 1. Остаточный риск может содержать в себе неидентифицированный риск. 2. Остаточный риск может также называться как «сохраняемый риск».

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
	Риск (risk): комбинация вероятности события и его последствий [ISO/IEC 27002:2005]	3.9 Риск (risk): Влияние неопределённости на цели. [Руководство ISO 73:2009] Примечания: 1. Влияние – это отклонение от предполагаемого (положительного и/или отрицательного). 2. Цели могут иметь различные аспекты (например, финансовые цели, цели охраны здоровья и безопасности, экологические цели) и могут применяться на различных уровнях (стратегических, в масштабах организации, проекта, продукции или процесса). 3. Риск обычно характеризуется возможными событиями (3.3) и последствиями (3.1) или их сочетанием. 4. Риск обычно выражается в виде сочетания последствий события (включая изменения в обстоятельствах) и связанной с ним возможностью (3.9) возникновения. 5. Неопределённость – это

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
		недостаточность (даже частичная) информации, связанной с пониманием события или знаниями о нем, его последствиями или возможностью возникновения. 6. Информационная безопасность ассоциируется с потенциалом угроз, которые используют уязвимости информационного актива или группу информационных активов и таким образом наносят ущерб организации[6].
н/д	Анализ риска (risk analysis): Систематическое использование информации для выявления источников и для оценки степени риска Примечание: Анализ риска предоставляется на основе оценки значительности риска, обработки и принятие риска[7] [ISO/IEC 27001:2005]	3.10 Анализ риска (risk analysis): Процесс понимания происхождения риска и определения уровня риска (3.6) [Руководство ISO 73:2009] Примечания: 1. Анализ риска обеспечивает основу для оценивания риска и принятия решений, касающихся обработки риска. 2. Анализ риска включает количественную оценку риска.

[6] Примечание переводчика: Данного пункта примечаний нет в Руководстве ISO 73:2009.
[7] Примечание переводчика: Этого примечания в терминах ISO/IEC 27001:2005 я не нашёл.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	оценка риска (risk assessment): Общий процесс анализа риска и оценивания риска. [ISO/IEC 27001:2005]	3.11 Оценка риска (risk assessment): Общий процесс идентификации риска (3.15), анализа риска (3.10) и оценивания риска (3.14). [Руководство ISO 73:2009]
3.3 предотвращение риска (risk avoidance) решение не включать, или уйти из ситуации с риском. [Руководство ISO 73:2002]		Определение удалено

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
3.4 Обмен информацией относительно риска (risk communication): обмен или обмен информацией о риске между принимающим решения лицом и другими заинтересованными сторонами		3.12 Обмен информацией и консультирование относительно риска (risk communication and consultation): Непрерывные и повторяющиеся процессы, которые проводит организация, для предоставления, разделения или получения информации, а так же ведения диалога с заинтересованными сторонами (3.18) относительно менеджмента риска (3.9) [Руководство ISO 73:2009] Примечания: 3. Информация может касаться наличия, характера, формы, возможности (3.6.1.1), важности, оценивания, приемлемости и обработки в рамках менеджмента риска. 4. Консультирование – это двусторонний процесс квалифицированного обмена информацией между организацией и заинтересованными сторонами до принятия решения по определённому вопросу или перед определением указаний по этому вопросу. Консультирование

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
		является: • процессом, который оказывает влияние на принятие решения посредством влияния, а не принуждения; • входными данными для процесса принятия решения, а не совместным принятием решения.
н/д	н/д	3.13 Критерии риска (risk criteria): Аспекты, в соответствии с которыми осуществляют оценивание риска (3.9) [Руководство ISO 73:2009] Примечания: 1. Критерии риска основываются на целях организации и внешнем и внутреннем контексте. 2. Критерии риска могут быть установлены на основании стандартов, законов, политик и других требований.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
3.5 оценка риска (risk estimation) обработка, чтобы присвоить значения вероятности и последствиям риска [Руководство ISO/IEC 73:2002] Примечания: 1. В контексте этого Международного стандарта, термин "действие" используется вместо термина "процесс" для оценки риска. 2. В контексте этого Международного стандарта, термин возможность (likelihood) используется вместо термина "вероятность"(probability) для оценки риска.		Определение удалено

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	Оценивание риска (risk evaluation): Процесс сравнения оценённого риска с данными критериями риска для определения значимости риска. [ISO/IEC 27001:2005]	3.14 Оценивание риска (risk evaluation): Процесс сравнения результатов анализа риска (3.10) с установленными критериями риска (3.13) для определения, является ли риск и/или его величина приемлемыми или допустимыми. [Руководство ISO 73:2009] Примечание: Оценивание риска способствует принятию решения в отношении обработки риска.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
3.6 Идентификация риска (risk identification): Процесс поиска, перечисления и описания риска [Руководство ISO/IEC 73:2002] Примечание: В контексте этого Международного стандарта, термин "действие"(activity) используется вместо термина "процесс"(process) для выявления риска.		3.15 Идентификация риска (risk identification): Процесс выявления, исследования и описания рисков. [Руководство ISO 73:2009] Примечание: 3. Идентификация включает идентификацию источников риска, событий, их причин и возможных последствий. 4. Идентификация риска может включать статистические данные, теоретический анализ, обоснованную точку зрения и заключение специалиста, а также потребности заинтересованной стороны.

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	Менеджмент риска (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска. [ISO/IEC 27001:2005]	3.16 Менеджмент риска (risk management): Скоординированная деятельность по руководству и управлению организацией в отношении риска. [Руководство ISO 73:2009] Примечание: Этот Международный стандарт использует термин «процесс», чтобы описать риск-менеджмент повсюду. Элементы в пределах процесса менеджмента риска называют «действиями».
3.7 Снижение риска (risk reduction) меры, предпринятые, чтобы уменьшить вероятность, отрицательные последствия, или оба фактора, связанных с риском [Руководство ISO/IEC 73:2002] ОТМЕТЬТЕ В контексте этого Международного стандарта, термин «возможность» (likelihood) используется вместо термина "вероятность" (probability) для снижения риска.		Этот термин заменяется «модификацией риска» и в настоящий момент перекрывается обработкой риска

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
3.8 сохранение риска (risk retention): Принятие бремени потерь или выгод от конкретного риска. [Руководство ISO/IEC 73:2002] Примечание: В контексте рисков информационной безопасности для сохранения риска рассматриваются только негативные последствия (потери).		Этот термин в настоящий момент перекрывается обработкой риска
3.9 перенос риска (risk transfer): Разделение с другой стороной бремени потерь или выгод от риска. [Руководство ISO/IEC 73:2002] Примечание: В контексте рисков информационной безопасности для переноса риска рассматриваются только негативные последствия (потери).		Этот термин заменяется «совместным использованием риска» и в настоящий момент перекрывается обработкой риска

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
н/д	обработка риска (risk treatment): Процесс выбора и осуществления мер по модификации риска. Примечание: В настоящем стандарте термин «средство управления» (control) используется как синоним термина «мера» (measure). [ISO/IEC 27001:2005]	3.17 Обработка риска (risk treatment): Процесс изменения риска. [Руководство ISO 73:2009] Примечания: 1. Обработка риска может включать: • избегание риска посредством принятия решения не начинать или не продолжать деятельность, в результате которой возникает риск; • принятие риска или увеличение риска для достижения цели; • устранение источника риска; • изменение возможности возникновения; • изменение последствий; • разделение риска с другой стороной или сторонами (включая договоры и финансирование риска; • принятие риска на основании обоснованного решения. 2. Обработка риска, имеющего

ISO/IEC 27005:2008 даёт определение терминам	Термины, определённые в ISO/IEC 27000:2009, используемые в ISO/IEC 27005:2008	Термины, определённые в Руководстве ISO 73:2009, используемые в ISO/IEC 27005:2011
		отрицательные последствия, иногда упоминается как «снижение риска», «устранение риска», «предотвращение риска» и «уменьшение риска». 3. Обработка риска может создавать новые риски или изменять существующие риски.
н/д	н/д	3.18 Заинтересованная сторона (stakeholder): Лицо или организация, которые могут воздействовать, подвергаться воздействию, или осознают, что на них влияет какое-либо решение или действия. [Руководство ISO 73:2009] Примечание: Лицо, принимающее решение, может быть заинтересованной стороной.
	угроза [threat] возможная причина нежелательного инцидента, который может закончиться ущербом для системы или организации [ISO/IEC 27002:2005]	Текущее определение применяется от ISO/IEC 27000:2009

Библиография

[1] ISO/IEC Guide 73:2009, Risk management — Vocabulary — Guidelines for use in standards	[1] Руководство ISO/IEC 73:2009, Менеджмент рисков - Словарь - Рекомендации для использования в стандартах
[2] ISO/IEC 16085:2006, Systems and software engineering — Life cycle processes — Risk management	[2] ISO/IEC 16085:2006, Системы и разработка программного обеспечения – жизненный цикл процессов - Менеджмент риском
[3] ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management	ISO/IEC 27002:2005, Информационные технологии. Свод правил по менеджменту защитой информации.
[4] ISO 31000:2009, Risk management — Principles and guidelines	[4] ISO 31000:2009, Риск менеджмент – Принципы и руководства
[5] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook	[5] NIST Специальная публикация 800-12, Введение в компьютерную безопасность: Руководство
[6] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology	[6] NIST Специальная публикация 800-30, Руководство менеджмента рисков для систем информационной технологии, рекомендации национального института стандартов и технологии