
**Информационная технология -
Методы защиты – Менеджмент рисков
информационной безопасности**

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

ICS 35.040



Номер ссылки ISO/IEC 27005:2008 (E)
© ISO/IEC 2008

Данный документ – третья редакция технического перевода британского стандарта, ставшего международным - BS ISO/IEC 27005:2008. Автор перевода – старший эксперт по информационной безопасности [Гонцул В.А.](#) Все права охраняются согласно действующему законодательству. ЗАПРЕЩЕНО ЛЮБОЕ КОПИРОВАНИЕ БЕЗ РАЗРЕШЕНИЯ BSI, КРОМЕ РАЗРЕШЕННОГО В СООТВЕТСТВИИ С ЗАКОНОМ ОБ АВТОРСКОМ ПРАВЕ

Общие примечания переводчика по переводу в данной редакции:

1. Некоторые общие примечания переводчика:

- 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!
- для правильного понимания контекста выражений в стандарте переводчиком включены комментарии;
- данный стандарт существенно отличается от ISO/IEC 1st CD 27005 от 2005г.;

2. Буду рад за замечания коллег и правки перевода в режиме «исправления».

Оглавление

Предисловие.....	5
Введение.....	6
1 Область (границы) действия.....	7
2 Нормативные ссылки	7
3 Определения.....	7
4 Структура этого интернационального стандарта.....	8
5 Предпосылки.....	9
6 Краткий обзор процесса менеджмента риска информационной безопасности	10
7 Установление контекста	13
7.1 Общий анализ.....	13
7.2 Основные критерии	13
Критерии оценки риска.....	14
Критерии воздействия.....	14
Критерии допустимости риска.....	14
7.3 Область применения и границы	15
7.4 Организация менеджмента рисков информационной безопасности.....	16
8 Оценка рисков информационной безопасности	16
8.1 Общее описание оценки риска информационной безопасности	16
8.2 Анализ риска	17
8.2.1 Идентификация риска	17
8.2.1.1 Введение в идентификацию риска.....	17
8.2.1.2 Идентификация активов	17
8.2.1.3 Идентификация угроз.....	18
8.2.1.4 Идентификация существующих контролей.....	19
8.2.1.5 Идентификация уязвимости	20
8.2.1.6 Идентификация последствий	20
8.2.2 Оценка риска.....	21
8.2.2.1 Методологии оценки риска	21
8.2.2.2 Оценка последствий	22
8.2.2.3 Оценка вероятности инцидента	23
8.2.2.4 Оценки уровня риска.....	24
8.3 Оценка риска.....	24
9 Обработка рисков информационной безопасности	25
9.1 Общее описание обработки риска	25
9.2 Снижение риска	27
9.3 Сохранение риска	28
9.4 Предотвращение риска.....	28
9.5 Перенос риска	29
10 Сохранение риска информационной безопасности	29
11 Коммуникации риска информационной безопасности.....	30
12 Мониторинг и пересмотр риска информационной безопасности	31
12.1 Мониторинг и пересмотр факторов риска	31
12.2 Мониторинг, пересмотр и улучшение менеджмента рисков	32
Приложение А.....	34
Определение области применения и границ процесса менеджмента рисков информационной безопасности	34
А1 Исследование организации.....	34
А2 Список ограничений, затрагивающих организацию	35

А3 Список законодательных и регулирующих нормативов, применимых к организации	37
А4 Список ограничений, затрагивающих область применения	37
Приложение В	39
Идентификация и определение ценности активов, определение стоимости воздействия...	39
В.1 Примеры идентификации актива	39
В.1.1 Идентификация первичных активов	39
В.1.2 Перечень и описание поддержки активов	40
В.2 Оценка актива.....	44
В.3 Оценка воздействия	48
Приложение С	49
Примеры типичных угроз	49
Приложение D.....	53
Уязвимости и методы для оценки уязвимости	53
D.1 Примеры уязвимости.....	53
D.2 Технические методы для оценки уязвимости	57
Приложение Е	59
Подходы в оценке рисков информационной безопасности	59
Е.1 Оценка рисков информационной безопасности высокого уровня.....	59
Е.2 Подробная оценка риска информационной безопасности.....	60
Е.2.1 Пример матрицы с предопределёнными значениями	61
Е.2.2 Пример ранжирования мер угроз риска.....	63
Е.2.3 Пример оценки значения для вероятности и возможных последствий рисков ...	64
Приложение F	67
Ограничения для снижения риска	67
Библиография.....	70

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 первый выпуск [ISO/IEC 27005](#) представляет технический пересмотр стандартов, отмену и замену ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335-4:2000.

Введение

Этот интернациональный стандарт обеспечивает рекомендации для менеджмента риском информационной безопасности в организации, в особенности поддерживая требования СМИБ¹ (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.

Этот интернациональный стандарт относится к менеджерам и сотрудникам, которые заинтересованы в менеджменте риска информационной безопасности в пределах организации и где есть соответствующие внешние стороны, поддерживающие такие действия.

¹ Примечание переводчика – сокращенная аббревиатура ISMS (Information Security Management System) – это СМИБ (система менеджмента информационной безопасностью) в некоторых документах упоминается перевод как СУИБ (система менеджмента информационной безопасностью)

1 Область (границы) действия

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

Методы, описанные в этом стандарте, соответствуют общим понятием, моделям и процессам, указанным в [ISO/IEC 27001](#). Эти рекомендации предназначены, чтобы помочь реализовать достаточную информационную безопасность, основанную на подходе менеджмента рисками.

Для законченного понимания этого стандарта важно знакомство с понятиями, моделями, процессами и терминологией, описанной в [ISO/IEC 27001](#) и ISO/IEC 27002.

Этот международный стандарт является применимым ко всем типам организаций (например, коммерческие предприятия, правительственные агентства, некоммерческие организации), которые намереваются осуществлять менеджмент рисками, ставящими под угрозу информационную безопасность организации.

2 Нормативные ссылки

Для применения этого документа необходимы нижеуказанные документы, на которые делаются ссылки. Для датированных ссылок применяется только процитированное издание. Для не датированных ссылок применяется последнее издание документа, на который идёт ссылка.

[ISO/IEC 27001:2005](#), Информационная технология - Методы защиты - Системы менеджмента информационной безопасности - Требования

ISO/IEC 27002:2005, Информационная технология - Методы защиты - Практическое руководство для менеджмента информационной безопасностью

3 Определения

В этом документе применяются термины и определения данные в [ISO/IEC 27001](#) и ISO/IEC 27002.

3.1 Воздействие (impact)

неблагоприятное изменение уровня достигнутых бизнес целей

3.2 Риск информационной безопасности (Information security risk)

потенциальная угроза эксплуатации уязвимости актива или группы ценных свойств, вызывая, таким образом, вред организации

ПРИМЕЧАНИЕ, это измерение в терминах комбинации вероятности случая и его последствия.

3.3 Предотвращение риска (risk avoidance)

решение не быть вовлечённым или действие уйти из ситуации риска
[ISO/IEC Guide 73:2002²]

² Примечание переводчика - См. тут и далее 8-мь терминов в соответствии с ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения» (прим. переводчика)

3.4 Коммуникация риска³ (risk communication)

Обмен информацией о риске или совместное использование этой информации между лицом, принимающим решение и другими причастными сторонами
[ISO/IEC Guide 73:2002]

3.5 Количественная оценка риска (risk estimation)

Процесс присвоения значений вероятности и последствий риска.
[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ 1. В контексте этого интернационального стандарта, термин “activity” (деятельность) использован вместо термина “process” (процесс) для количественной оценки риска.

ПРИМЕЧАНИЕ 2. В контексте этого интернационального стандарта, термин “likelihood” (возможность) использован вместо термина “probability” “вероятность” для количественной оценки риска.

3.6 Идентификация риска (risk identification)

Процесс нахождения, составления перечня и описания элементов риска
[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ В контексте этого интернационального стандарта, термин «activity» (деятельность) использован вместо термина «process» (процесс) для идентификации риска.

3.7 Снижение риска (risk reduction)

Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском
[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ В контексте этого интернационального стандарта, термин “likelihood” (возможность) использован вместо термина “probability” (вероятность) для снижения риска.

3.8 Сохранение риска (risk retention)

Принятие бремени потерь или выгод от конкретного риска.
[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ В контексте рисков информационной безопасности, рассматривают только отрицательные последствия (потери) для сохранения риска.

3.9 Перенос риска (risk transfer)⁴

Разделение с другой стороной бремени потерь или выгод от риска.
[ISO/IEC Guide 73:2002]

ПРИМЕЧАНИЕ В контексте рисков информационной безопасности, рассматривают только отрицательные последствия (потери) для переноса риска.

4 Структура этого интернационального стандарта

³ Примечание переводчика – в данном стандарте не учитывается «риск коммуникаций», в котором учитываются риски в связи с передачей информации разными методами.

⁴ Примечание переводчика (для информации):

1. Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.

2. Перенос риска может быть осуществлен страхованием или другими соглашениями.

3. Перенос риска может создавать новый риск или модифицировать существующий риск.

4. Перемещение источника не является переносом риска

Этот стандарт содержит описание процесса менеджмента рисков информационной безопасности и его действий.

Основная информация предоставлена в Разделе 5.

Общий краткий обзор процесса менеджмента рисков информационной безопасности дан в Разделе 6.

Все действия менеджмента рисков информационной безопасности представлены как в Разделе 6, так и впоследствии описаны в следующих Разделах:

- установление состояния в Разделе 7,
- оценка риска в Разделе 8,
- обработка риска в Разделе 9,
- принятие риска в Разделе 10,
- перенос риска в Разделе 11,
- контроль и пересмотр рисков в Разделе 12.

Дополнительная информация для действий менеджмента рисков информационной безопасности представлена в приложениях. Установление области применения находит отражение в Приложении А (определяет область применения и границы процесса менеджмента рисков информационной безопасности). Идентификация, оценка активов и оценки воздействия обсуждаются в Приложении В (примеры для активов), Приложение С (примеры типичных угроз) и Приложение D (примеры типичных уязвимостей).

Примеры подходов оценки риска информационной безопасности представлены в Приложении Е.

Ограничения для снижения риска представлены в Приложении F.

Все действия менеджмента рисков как представлено от Раздела 7 до Раздела 12 структурированы следующим образом:

Вводная информация: Идентифицирует любую запрошенную информацию, чтобы выполнить деятельность.

Действие: Описывает деятельность.

Руководство реализации: Дает представление о выполнении действия. Часть этого руководства во всех случаях, возможно, не является всеохватывающим и таким образом могут быть другие более подходящие способы выполнить действие.

Выходная продукция: Идентифицирует любую информацию, полученную после выполнения мероприятий.

5 Предпосылки

Необходим системный подход к менеджменту рисков информационной безопасности, чтобы идентифицировать организационные потребности относительно требований информационной безопасности и создать эффективную систему менеджмента информационной безопасности (СМИБ). Этот подход должен быть подходящим для среды организации и в частности должен быть сбалансированным подходом полного менеджмента рисков предприятия. Все усилия по безопасности должны эффективным и своевременным способом обратиться к рискам, где и когда они необходимы. Менеджмент рисков информационной безопасности должен быть неотъемлемой частью всех действий менеджмента информационной безопасностью и это должно быть применено как к реализации, так и к непрерывности операции СМИБ.

Менеджмент рисков информационной безопасности должен быть непрерывным процессом. Процесс должен установить окружающую обстановку, оценить риски, обработать риски, используя план обработки риска, осуществить рекомендации и решения. Менеджмент рисков анализирует то, что может случиться и каковы возможные последствия могут быть прежде, чем решить то, что должно быть сделано и когда, чтобы снизить риск до приемлемого уровня.

Менеджмент рисков информационной безопасности должен содействовать следующему:

- идентификации рисков;
- оценивать риски в терминах их последствий к бизнесу и вероятности их в инцидентах;
- вероятности и последствия этих рисков должны быть доведены и поняты;
- приоритетности категорий для устанавливаемой обработки рисков;
- приоритету для действий, чтобы уменьшить появление рисков;
- вовлекаемым причастным сторонам⁵ (примечание переводчика – это не синоним с заинтересованными сторонами⁶!), когда решения менеджмента рисков приняты и держатся в курсе статуса менеджмента риском;
- эффективности контроля обработки риска;
- риски и процесс менеджмента рисков должны быть измеряемыми и регулярно пересматриваться;
- фиксировать информацию, чтобы улучшить подходы менеджмента рисков;
- менеджерам и квалифицированным специалистам, обрабатывающих информацию о рисках и предпринятых действиях, чтобы смягчить их.

Процесс менеджмента рисков информационной безопасности может быть применен к организации в целом, любой дискретной части организации (например, отделу, физическому местоположению, сервису), любой существующей информационной системе, запланированным или специфическим аспектам менеджмента (например, планированию непрерывности бизнеса).

6 Краткий обзор процесса менеджмента риска информационной безопасности

Процесс менеджмента риска информационной безопасности состоит из установления окружающей обстановки (Раздел 7), оценки риска (Раздел 8), обработки риска (Раздел 9), принятия риска (Раздел 10), коммуникации риска (Раздел 11), контроля риска и его пересмотра (Раздел 12).

⁵ Примечание переводчика: причастная сторона (stakeholder): любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечания:

1. Лицо, принимающее решение, также является причастной стороной.

2. Причастная сторона включает в себя заинтересованную сторону, но имеет более широкое значение, чем заинтересованная сторона

⁶ Примечание переводчика: заинтересованная сторона (interested party): Лицо или группа лиц, заинтересованные в деятельности или успехе организации. Примеры: потребители, владельцы, работники организации, поставщики, банкиры, ассоциации, партнёры или общество.

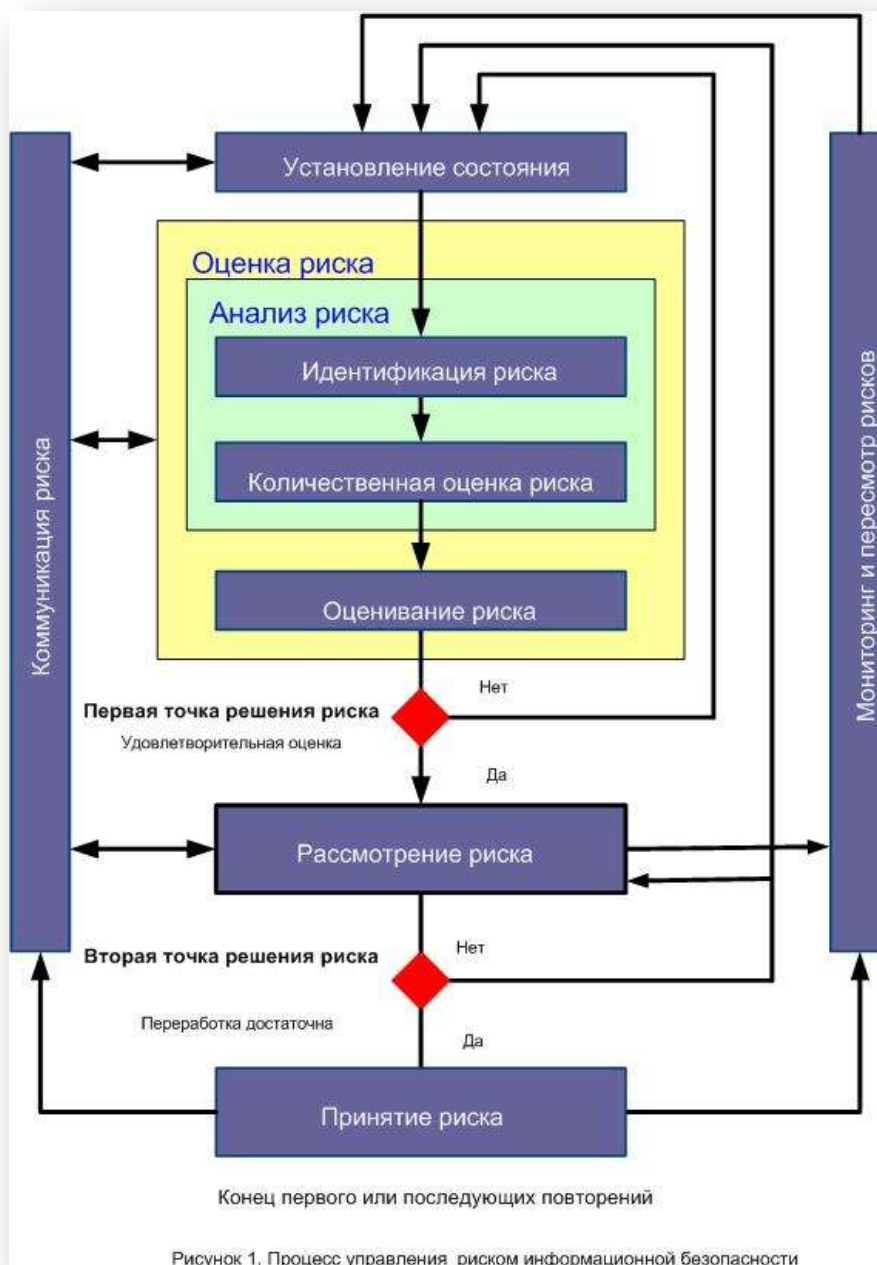


Рисунок 1 иллюстрирует, что процессы менеджмента риска являются обычно итерационными для оценки риска и/или действиям обработки рисков.

Итерационный подход к проведению оценки риска может увеличить глубину и детали оценки при каждой итерации. Итерационный подход обеспечивает хорошее равновесие между уменьшением времени и усилием, потраченным в идентификации контролей все ещё гарантируя, что высокие риски оценены соответственно.

Устанавливается сначала контекст. После этого проводится оценка риска. Если предоставлено достаточно информации, чтобы определить эффективные действия, требуемые для изменения рисков до приемлемого уровня, тогда задача закончена и следует обработка риска. Если информации будет недостаточно, то следует другая итерация оценки риска с пересмотренным контекстом (например, критерии оценки риска,

критерии допустимости риска или критерии воздействия) и возможно будет проводиться на ограниченных частях полной области применения (см. рис 1, точка решения риска 1).

Эффективность обработки риска зависит от результатов оценки риска. Возможно, что обработка риска не будет немедленно приводить к приемлемому уровню остаточного риска. В этой ситуации, другая итерация оценки риска с изменёнными контекстными параметрами (например, оценка риска, принятие риска или критерии воздействия), может в случае необходимости требоваться и сопровождаться дальнейшей обработкой риска (см. рис 1, точка решения риска 2).

Приёмный уровень риска должен гарантировать, что остаточные риски приняты явно⁷ менеджерами организации. Это особенно важно в ситуации, где реализация менеджмента не принята или отложена, например затраты.

Во время всего процесса менеджмента риска информационной безопасности важно, что риски и их обработка сообщены соответствующим менеджерам и служебному персоналу. Точная информация об идентифицированных рисках может быть очень ценной перед обработкой рисков, для того чтобы управлять инцидентами и помочь уменьшить потенциальный ущерб. Понимание менеджерами и служебным персоналом рисков, характера контроля на месте, смягчает риски и области тревоги к организации, способствуя решению инцидентов и неожиданных событий самым эффективным способом. Должны быть зарегистрированы детальные результаты каждой деятельности процесса менеджмента риском информационной безопасности и от второго пункта решения риска.

[ISO/IEC 27001](#) определяет, что менеджмент, осуществлённый в пределах области видимости, границ и контекста СМИБ должен быть основанным на рисках. Приложение процесса менеджмента риском информационной безопасности может удовлетворить это требование. Есть много подходов, которыми может быть успешно осуществлён процесс в организации. Организация должна использовать лучшие наборы любых подходов их обстоятельства для каждого определённого приложения процесса.

На этапе «планирования» СМИБ определяет состояния, проводит оценку риска, разрабатывает план обработки риска и принятие риска – это является всей частью фазы "плана". В "осуществлении" СМИБ поэтапно осуществляет действия и регулирование, требуемые чтобы уменьшать риск до приемлемого уровня, требуемых согласно плану обработки риска. В фазе "проверки" СМИБ определяет потребность менеджерам в пересмотрах оценки риска и их обработки в свете инцидентов и изменений обстановки. В фазе "исполнения" выполняются любые требуемые действия, включая дополнительное применение процессов менеджмента риском информационной безопасности.

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 контроль и рассмотрение рисков

⁷

Примечание переводчика: понятие «явно приняты менеджментом» обозначает, что менеджмент письменно в определённых документах принял остаточные риски.

Исполнение (Act)	Поддержка и улучшение рисков информационной безопасности Процесс менеджмента
------------------	--

7 Установление контекста

7.1 Общий анализ

Вводная информация: Вся информация об организации, относящаяся к установлению контекста менеджмента рисков информационной безопасности.

Действие: должно быть установлено состояние для менеджмента риском информационной безопасности, которое осуществляет установку основных критериев, необходимых для менеджмента рисков информационной безопасности (7.2), определение области применения и границ (7.3), установление соответствующей организации, осуществляющей менеджмент рисков информационной безопасности (7.4).

Руководство реализации:

Это является основным, чтобы определить цель менеджмента рисков информационного безопасности, поскольку это затрагивает весь процесс и область применения учреждение в частности. Эта цель может быть:

- поддержка СМИБ;
- юридическое согласие и доказательство должной старательности;
- подготовка плана непрерывности ведения бизнеса;
- подготовка плана реакции на инцидент;
- описание требований информационной безопасности для продукта, сервиса или механизма.

Руководство реализации для контекстных элементов учреждения должно было поддержать СМИБ, обсуждаемое в Разделе 7.2, 7.3 и 7.4 далее.

ОТМЕТЬТЕ, что [ISO/IEC 27001](#) не использует термин "контекст". Тем не менее, весь Раздел 7 имеет отношение с требованиями, "определяющий область действия и границы СМИБ" [4.2.1 а)], "определяющий политику СМИБ" [4.2.1 b)] и, "определяющий подходы оценки риска" [4.2.1 с)], определённые в [ISO/IEC 27001](#).

Выходная продукция: спецификация основных критериев, области применения и границ, и организации для процесса менеджмента риском 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 быть разработаны критерии оценки риска для того, чтобы оценить риск информационной безопасности организации и рассмотреть нижеуказанное:

- стратегическая оценка процесса информационного бизнеса;
- критичность вовлечённых информационных активов;
- юридические и регулирующие требования, обязательства по контракту;
- практическая и коммерческая важность доступности, конфиденциальности и целостности;
- ожидания причастных сторон и осознание отрицательных последствий для доброжелательности к организации и её репутации.

Дополнительно могут использоваться критерии оценки риска, чтобы определить приоритеты для обработки риска.

Критерии воздействия

Должны быть разработаны и определены критерии воздействия в терминах степени повреждения или стоимости для организации, вызванной случаем информационной безопасности при рассмотрении следующего:

- уровня классификации закреплённого информационного актива;
- нарушения информационной безопасности (например, потеря конфиденциальности, целостности и доступности);
- снижения работоспособности (для внутренних или третьих лиц);
- потеря коммерческой деятельности и финансового значения;
- разрушения планов и конечных сроков;
- ущерба репутации;
- нарушения юридических, регулирующих или договорных требований.

ПРИМЕЧАНИЕ Смотрите также [ISO/IEC 27001](#) [Раздел 4.2.1 d) 4] относительно идентификации критериев воздействия за потери, такие как конфиденциальность, целостность и доступности.

Критерии допустимости⁸ риска

Должны быть разработаны и определены критерии допустимости риска. Критерии допустимости риска часто зависят от политик организации, целей, объектов и интересов причастных сторон.

Организация должна определить свои собственные масштабы для уровней принятия риска. Нужно рассмотреть во время разработки следующее:

- критерии допустимости риска могут включать множественные пороги чувствительности с заданным целевым уровнем риска, но обеспечивающим для главных менеджеров принятие рисков выше этого уровня при определённых обстоятельствах;
- критерии допустимости риска могут быть выражены как отношение оценки прибыли (или другая бизнес выгода) к предполагаемому риску;
- различные критерии допустимости риска могут относиться к различным степеням риска, например риски, которые могли привести к несоблюдению инструкций или могут быть не приняты законы в то время,

⁸

Примечание переводчика: предполагаю, что синоним этого слова - это сохранение риска.

как может быть позволено принятие высоких рисков, если это определено как договорное требование;

- критерии допустимости риска могут включать требования для будущей дополнительной обработки, например, может быть принят риск, если одобрена обязательство к принятию мер, чтобы уменьшить риск до приемлемого уровня в пределах определённого периода времени.

Критерии допустимости риска могут отличаться согласно тому, как долго будет существовать ожидаемый риск, например риск, может быть связан с краткосрочной деятельностью или временными служащими. Должны быть установлены критерии допустимости риска, рассматривая следующее:

- бизнес критерии;
- юридические и регулирующие аспекты;
- обработку;
- технологию;
- финансы;
- социальные и гуманитарные факторы.

ОТМЕТЬТЕ, что критерии допустимости риска соответствуют “критериям для того, чтобы принять риски и идентифицировать приемлемый уровень риска”, определённый в [ISO/IEC 27001](#) Раздел 4.2.1 с) 2).

Подробная информация может быть найдена в Приложении А.

7.3 Область применения и границы

Организация должна определить область применения и границы менеджмента риском информационной безопасности.

Должна быть определена область применения процесса менеджмента риском информационной безопасности, чтобы гарантировать, что приняты во внимание в оценке риска все соответствующие активы. Кроме того, должны быть идентифицированы границы [смотрите также [ISO/IEC 27001](#) раздел 4.2.1 а)], чтобы обратиться к тем рискам, которые могли бы возникнуть в этих границах.

Должна быть собрана информация об организации, чтобы определить среду, в которой производится менеджмент и её значимость к процессу менеджмента рисков информационной безопасности.

Определяя область применения и границы, организация должна рассмотреть следующую информацию:

- стратегические бизнес цели организации, стратегии и политика;
- бизнес-процессы;
- функции организации и структуру;
- юридические, регулирующие и договорные требования, применимые к организации;
- политику информационной безопасности организации;
- подход организации к менеджменту риском в целом;
- информационные активы;
- местоположения организации и её географические характеристики;
- ограничения, затрагивающие организацию;
- ожидание причастных сторон;
- социокультурную среду;
- интерфейсы (то есть обмен информацией со средой).

Дополнительно организация должна обеспечить обоснование для любого исключения из области применения.

Примеры области применения менеджмента рисков могут быть приложением ИТ, ИТ инфраструктуры, бизнес-процесса или определённой части организации.

ОТМЕТЬТЕ, что область применения и границы менеджмента риском информационной безопасности связаны с областью применения и границами из СМИБ, требуемых в [ISO/IEC 27001](#) 4.2.1 а).

Дальнейшая информация может быть найдена в Приложении А.

7.4 Организация менеджмента рисков информационной безопасности

Должна быть установлена и утверждена организация и ответственность за процесс менеджмента рисков информационной безопасности. Нижеуказанное - главные роли и обязанности этой организации:

- разработка процесса менеджмента рисков информационной безопасности, подходящей для организации;
- идентификация и анализ имущества причастных сторон;
- определение ролей и ответственности всех сторон как внутренних, так и внешних к организации;
- создание необходимых отношений между организацией и причастными сторонами, так же как интерфейсы организации к функциям менеджмента рисков высокого уровня (например, менеджмент эксплуатационным риском), так же как интерфейсы к другим соответствующим программам или деятельности;
- определение решающих путей подъёма;
- подробное изложение отчётов, которые будут сохранены.

Эта организация должна быть одобрена соответствующими менеджерами организации.

ОТМЕТЬТЕ, что [ISO/IEC 27001](#) требует определения и обеспечения ресурсов, которые должны установить, обеспечить выполнение, управлять, контролировать, делать пересмотр, поддерживать и улучшать СМИБ [5.2.1 а)]. Организация для операций менеджмента риском может быть расценена как один из ресурсов, требуемых [ISO/IEC 27001](#).

8 Оценка рисков информационной безопасности

8.1 Общее описание оценки риска информационной безопасности

ОТМЕТЬТЕ, что в [ISO/IEC 27001](#) деятельность по оценке риска упоминается как процесс

Входная информация: Основные критерии, область применения, границы и организация для устанавливаемого процесса менеджмента рисков информационной безопасности.

Действие: Риски должны быть идентифицированы, определены и описаны количественно или качественно, расположены по приоритетам против критериев оценки риска и реальностям, относящимся к организации.

Руководство реализации:

Риск - комбинация последствий, которые следовали бы от возникновения нежелательного случая и вероятности возникновения случая. Оценка риска определяется количественными или качественными описаниями риска и даёт возможность менеджерам расположить по приоритетам риски согласно их серьёзности восприятия или другим установленным критериям.

Оценка риска состоит из следующих действий:

- анализ риска (раздел 8.2), который включает:
 - идентификацию риска (раздел 8.2.1);
 - количественную оценку риска (раздел 8.2.2);
- оценивание риска (раздел 8.3).

Оценка риска определяет ценность информационных активов, идентифицирует соответствующие угрозы и уязвимость, которые существуют (или могут существовать), идентифицирует существующие контроли и их эффект на идентифицированный риск, определяет потенциальные последствия и наконец располагает по приоритетам полученные риски и ранжирует их против набора критериев оценки риска в окружающей обстановке организации.

Оценка риска часто проводится за две (или больше) итерации. Сначала выполняется оценка высокого уровня, чтобы в дальнейшем гарантировать оценку идентифицированных потенциально высоких рисков. Следующая итерация может вовлечь дальнейшее всестороннее рассмотрение потенциально высоких рисков, показанных в начальной итерации. Если предоставлено недостаточно информации для оценки риска, тогда далее проводимые исследования детализируются, вероятно, и возможно использование различных методов на частях полной области применения.

Вышеуказанное относится к организации, чтобы выбрать собственный подход к оценке риска, основанной на стремлении и цели оценки риска.

Обсуждение о подходах оценки риска информационной безопасности может быть найдено в Приложении Е.

Выходная продукция: список оценённых рисков расположенных по приоритетам согласно критериям оценки риска.

8.2 Анализ риска

8.2.1 Идентификация риска

8.2.1.1 Введение в идентификацию риска

Цель идентификации риска состоит в том, чтобы определить то, что может случиться, вызвать возможные потери и получить сведения, как, где и почему могла бы случиться потеря. Шаги, описанные в следующих подпунктах 8.2.1, должны собрать входные данные для деятельности оценки риска.

ОТМЕТЬТЕ, что действия, описанные в последующих пунктах, могут быть проведены в различном порядке в зависимости от того, какая применялась методология.

8.2.1.2 Идентификация активов⁹

Вводная информация: Область применения и границы для оценки риска, которые будут проведены, список непосредственных составляющих с владельцами, местоположением, функцией и т.д.

Действие: активы в пределах установленной области применения должны быть идентифицированы (имеет отношение к [ISO/IEC 27001](#), пункт 4.2.1 d) 1)).

Руководство реализации:

⁹ 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 ИТ систему (в штате/ контракт);
- миссия ИТ системы (system mission) – процесс, выполняемый ИТ системой;
- сервис и поддерживающая инфраструктура (обслуживание СБТ, энергоснабжение, обеспечение климатических параметров и т.п.).

Актив – это то, что имеет ценность в организации и которое поэтому требует защиты. При идентификации активов нужно всегда помнить, что информация или система информационно-коммуникационных технологий состоит больше чем из аппаратных средств и программного обеспечения.

Идентификация актива должна быть выполнена на соответствующем уровне детализации, который предоставляют обоснованную информацию для оценки риска. Уровень детализации, используемый на идентификацию актива, будет влиять на количество информации в целом, собранной во время оценки риска. Уровень может быть доведён до совершенства в дальнейших итерациях оценки риска.

Должен быть идентифицирован владелец для каждого актива, обеспечивающий ответственность и подотчётность для актива. Владелец актива, возможно, не имеет прав собственности на актив, но несёт ответственность за его продукцию, разработку, обслуживание, использование и соответствующую безопасность. Владелец актива часто – самый подходящий человек, чтобы определить значение актива для организации (см. 8.2.2.2 для оценки актива).

Граница применения – периметр активов организации, определённый, чтобы управлять процессом менеджмента риском информационной безопасности.

Подробная информация относительно идентификации и оценки активов связанной с информационной безопасностью может быть найдена в Приложении В.

Выходная продукция: список из активов, которые будут в риск – менеджменте и список бизнес-процессов связанный со значимостью активов.

8.2.1.3 Идентификация угроз

Вводная информация: Информация относительно угроз, полученных из рассмотрения инцидентов, владельцев актива, пользователей и других источников, включая внешние каталоги угроз.

Действие: Угрозы и их источники должны быть идентифицированы (имеет отношение с [ISO/IEC 27001](#), пункт 4.2.1 d) 2)).

Руководство реализации:

У угрозы есть потенциал, чтобы вредить активам, таким как информация, процессы, системы и самой организации. Угрозы могут иметь естественную или человеческую природу и могут быть случайными или преднамеренными. Должны быть идентифицированы случайные и преднамеренные источники угрозы. Угроза может возникнуть внутри или снаружи организации. Угрозы должны быть идентифицированы в целом и отсортированы (например, несанкционированные действия, физическое повреждение, технические отказы) и затем соответствующие индивидуальные угрозы в пределах универсального идентифицированного класса. Это означает, что не будут пропущены никакие угрозы, включая непредвиденные, при ограниченном объёме необходимых действий.

Некоторые угрозы могут затронуть больше чем один актив. В таких случаях они могут вызывать различные воздействия в зависимости от того какие затронуты активы.

Вводная информация для идентификации угрозы и оценка вероятности возникновения (см. 8.2.2.3) может быть получена от владельцев актива или пользователей из штатных работников от менеджмента и специалистов по информационной безопасности, физических экспертов по безопасности, юридического отдела и других организаций, включая юридические органы, подразделений прогноза погоды, страховых компаний и национальных правительственные органов. Обращаясь к угрозам, нужно рассмотреть аспекты окружающей среды и культуры.

В текущей оценке нужно рассмотреть внутренний опыт от инцидентов и прошлые оценки угрозы. Чтобы завершить список универсальных угроз, относящихся к

делу, может, стоило бы изучить¹⁰ другие списки угроз (возможно определёнными для организации или бизнеса). Списки угроз и статистика доступны от индустриальных и национальных правительств, юридических органов, страховых компаний и т.д.

Нужно знать, используя список угроз или результаты более ранних оценок угроз, что существует непрерывное изменение соответствующих угроз, особенно если есть изменения бизнес среды или информационной системы.

Подробная информация относительно типов угроз может быть найдена в Приложении С.

Выходная продукция: список из угроз с идентификацией типа и источника угрозы.

8.2.1.4 Идентификация существующих контролей

Вводная информация: Документация из контролей, обработки рисков и реализации планов.

Действие: Должны быть идентифицированы существующие и запланированные контроли.

Руководство реализации:

Должна быть сделана идентификация существующих контролей чтобы избежать ненужной работы или финансовых затрат, например в дублировании контролей. Кроме того, идентифицируя существующие контроли, должна быть, осуществлена проверка, чтобы гарантировать, что контроли работают правильно - рекомендации уже существующих отчётов аудита СМИБ должны ограничить расход времени в этой задаче. Если контроли не работают, как ожидается, это может вызвать уязвимости. Должны быть рассмотрены ситуации, где выбран контроль (или стратегия) сбоя в эксплуатации и, следовательно, дополнительный контроль обязан эффективно адресоваться к идентифицированному риску. В СМИБ, согласно [ISO/IEC 27001](#), это поддержано измерением эффективности контролей. Способ оценить эффект контроля состоит в том, чтобы увидеть, как это уменьшает вероятность угрозы и ослабляется эксплуатационная уязвимость или воздействие инцидента. Пересмотр контролей и отчётов контролей также предоставляют информацию об эффективности существующих контролей.

Контроли, которые запланированы согласно плану реализации обработки риска, нужно рассматривать как уже осуществлённые.

Существующие или запланированные контроли могут быть идентифицированы как неэффективные, или не достаточные, или не оправданные. Контроли должны быть проверены, если они не оправданы или не достаточны, чтобы определить, должны ли они быть удалены, заменены другими, более подходящим контролями или должны ли остаться как есть, например, по причинам стоимости.

Для идентификации существующего или запланированного контроля, могут быть полезными следующие действия:

- пересмотр документов, содержащих информацию о контролях (например, план реализации и обработки рисков). Если процессы менеджмента информационной безопасности хорошо документированы все существующие или запланированные контроли и состояние их реализации должны быть доступными;
- согласование с людьми, ответственными за информационную безопасность (например, сотрудниками информационной безопасности и сотрудниками информационной безопасности системы, комендантом или менеджером по эксплуатации) и пользователями, относительно которых

¹⁰

Примечание переводчика: в стандарте принят термин «проконсультироваться».

действительно осуществлены контроли для информационного процесса или рассмотренной информационной системы;

- проведение проверок на местах физического контроля, сравнивая прибывающих со списком тех, кто должен быть в месте контроля, осуществления проверки относительно того, работают ли они правильно и эффективно, или
- пересмотр результатов внутренних ревизий.

Выходная продукция: список всех существующих и запланированных контролей, их состояния реализации и использования.

8.2.1.5 Идентификация уязвимости

Вводная информация: список известных угроз, списки активов и существующих контролей.

Действие: Должна быть идентифицирована уязвимость, которая может эксплуатировать угрозы, вызывая вред активам или организации (имеет отношение с [ISO/IEC 27001](#), пункт 4.2.1 d) 3)).

Руководство реализации:

Уязвимость может быть идентифицирована в следующих областях:

- организации;
- процессах и процедурах;
- практике менеджмента;
- персонале;
- физической среде;
- конфигурации информационной системы;
- аппаратных средствах, программном обеспечении или оборудовании связи;
- зависимости от внешних партнёров.

Присутствие уязвимости не вызывает вред сам по себе, должна быть угроза, представляющая возможность эксплуатировать её. Уязвимость, у которой нет никакой соответствующей угрозы, возможно, не требует реализации контроля, но уязвимость должна быть распознана и должен проводиться мониторинг на предмет изменений. Нужно отметить, что неправильно осуществлённый или работающей со сбоями контроль или неправильно используемый менеджмент могут быть самостоятельной уязвимостью. Контроль может быть эффективным или неэффективным в зависимости от среды, в которой он работает. Наоборот, угроза, у которой нет соответствующей уязвимости, возможно, не приведет к риску.

Уязвимость может быть связана со свойствами актива, который может использоваться в известном смысле или в намерении использования не в том предназначении, для которого куплен или сделан актив. Уязвимость, возникающую в результате различных причин, нужно рассматривать, например, встроенным или внешним средством к активу.

Примеры уязвимостей и методов для оценки уязвимостей могут быть найдены в Приложении D.

Выходная продукция: список уязвимостей относительно активов, угроз и контролей; список уязвимостей, которые не пересматриваются относительно идентифицированной угрозы.

8.2.1.6 Идентификация последствий

Вводная информация: список активов, список бизнес-процессов, список уместных угроз и уязвимостей, связанных с активами и их значимостью.

Действие: должны быть идентифицированы последствия потери конфиденциальности, целостности и доступности, которые могут иметь активы (см. [ISO/IEC 27001](#) пункт 4.2.1 d) 4)).

Руководство реализации:

Последствием может быть потеря эффективности, неблагоприятные эксплуатационные режимы, потери бизнеса, репутации, повреждения и т.д.

Эта деятельность идентифицирует ущерб или последствия к организации, которые могли быть вызвана инцидентным сценарием. Инцидентный сценарий - описание угрозы, эксплуатирующей определенную уязвимость или набор уязвимости в инциденте информационной безопасности (см. ISO/IEC 27002, пункт 13). Воздействие инцидентных сценариев определяет рассмотрение критериев воздействия, определенных во время установления активного состояния. Это может затронуть один или более активов или часть актива. Таким образом, активам возможно назначать значения и в финансовой стоимости и в последствиях к бизнесу, если им нанесен ущерб или они скомпрометированы. Последствия могут иметь временную природу или могут быть постоянными, как в случае уничтожения актива.

ОТМЕТЬТЕ, что [ISO/IEC 27001](#) описывает возникновение инцидентных сценариев как “отказы безопасности”.

Организации должны идентифицировать эксплуатационные последствия инцидентных сценариев в терминах (но не ограниченный перечень):

- расследование и время ремонта;
- (работа) потерянное время;
- потерянные возможности;
- благосостояние и безопасность;
- финансовая стоимость определенных навыков, чтобы возместить убытки
- имидж репутации и престижа

Подробности относительно оценки технической уязвимости могут быть найдены в оценке воздействий В.3.

Выходная продукция: список инцидентных сценариев с их последствиями, связанными с активами и бизнес-процессами.

8.2.2 Оценка риска

8.2.2.1 Методологии оценки риска

В зависимости от критичности активов может быть предпринят анализ рисков в различных степенях детализации, известной степени уязвимости и случившихся ранее инцидентов в организации. В зависимости от обстоятельств методология оценки может быть качественной или количественной или комбинация их. Практически, часто сначала используется качественная оценка, чтобы получить общую индикацию относительно уровня риска и показать главные риски. Обычно менее сложно и менее дорого провести оценку качественную, чем провести количественный анализ, потому что позже может быть необходимо предпринять более определенный или количественный анализ на главных рисках.

Форма анализа должна быть совместима с критериями оценки риска, разработанными, как часть установления состояния.

Далее подробно описаны методологии оценки:

(а) Качественная оценка:

Качественная оценка использует шкалу квалификации атрибутов, чтобы описать величину потенциальных последствий (например: низкие, средние или высокие) и вероятность, что эти последствия произойдут. Преимущество качественной оценки - вероятность своего понимания всем соответствующим персоналом, в то время как недостаток - зависимость от субъективного выбора масштаба.

Эти масштабы могут адаптироваться или откорректированы, чтобы удовлетворить обстоятельствам, и могут использоваться различные описания для различных рисков. Качественная оценка может использоваться:

- как начальная деятельность фильтра, чтобы идентифицировать риски, которые требуют более детального анализа;
- где этот вид анализа является соответствующим решением; или
- где числовые данные или ресурсы неадекватны для количественной оценки.

Качественный анализ должен использовать, где доступно фактическую информацию и данные.

(b) Количественная оценка:

Количественная оценка использует масштаб с числовыми значениями (а не описательные масштабы, используемые на качественной оценке) как для последствий, так и вероятности, используя данные из множества источников. Качество анализа зависит от точности и законченности числовых значений и обоснованности используемых моделей. Количественная оценка в большинстве случаев использует историю инцидентных данных, обеспечивая преимущество, что все это может быть связано непосредственно с реалиями информационной безопасности и проблемами организации. Недостаток - нехватка таких данных по новым рискам или слабым местам информационной безопасности. Имеется изъян количественного подхода там, где не доступны фактические проверяемые данные, таким образом, создаётся иллюзия ценности и точности оценки риска.

Путь, которым последствия и вероятность выражены и путь, которым они комбинируются, чтобы обеспечить уровень риска изменяются согласно типу риска и результатам, в которых должен использоваться вывод оценки риска. В анализе нужно рассмотреть и сообщать фактически неопределённость и изменчивость обоих результатов и их вероятности.

8.2.2.2 Оценка последствий

Вводные данные: список соответствующих идентифицированных инцидентных сценариев, включая идентификацию угроз, уязвимости, затрагивающие активы и последствия к активам и бизнес-процессам.

Действие: должно быть оценено бизнес воздействие на организацию, которое могло бы следовать из возможных или фактических инцидентов информационной безопасности, принимая во внимание последствия нарушения информационной безопасности, такие как потеря конфиденциальности, целостность или доступности активов (имеет отношение с [ISO/IEC 27001](#), пункт 4.2.1 е) 1)).

Руководство реализации:

После идентификации всех рассматриваемых активов должны быть приняты во внимание значения, назначенные на эти активы, и оценены последствия.

Значения воздействия на бизнес могут быть выражены в качественных и количественных значениях, но любой метод назначения значения в денежном эквиваленте может, в общем, обеспечить подробную информацию для принятия решения и, следовательно, облегчить более эффективный процесс принятия решения.

Оценка актива начинается с классификации активов согласно их критичности, в терминах важности активов к выполнению бизнес целей организации. Тогда установлена оценка, когда используя две меры:

- значение замены актива: стоимость чистого восстановления и замены информации (если вообще возможно), и
- последствия бизнес потерь или компрометации актива, такие как потенциальное неблагоприятное воздействие на бизнес и/или

юридические или регулирующие последствия от раскрытия, модификации, недостатка и/или разрушения информации и других информационных активов.

Эта оценка может быть определена от анализа воздействия на бизнес. Определённое последствием значение, для бизнеса, обычно значительно выше, чем простая стоимость замены, в зависимости от важности актива в организации на соединении с её бизнес целями.

Оценка актива - ключевой фактор в оценке воздействия инцидентного сценария, потому что инцидент может затронуть больше чем один актив (например, зависимые активы), или только часть актива. У различных угроз и уязвимостей будут различные воздействия на активы, такие как потеря конфиденциальности, целостности или доступности. Таким образом, оценка последствий связана с оценкой актива, основанной на анализе воздействия на бизнес.

Могут быть определены воздействия последствий на бизнес моделированием результатов событий или наборов событий, или экстраполяцией от экспериментальных исследований или прошлых данных.

Последствия могут быть выражены в терминах денежного эквивалента, критериях технического или человеческого воздействия, или других критериев, относящихся к организации. В некоторых случаях, больше чем одно числовое значение обязано определять последствия в течение различного времени, места, группы или ситуаций.

Должны быть измерены временные и финансовые последствия тем же самым подходом, что используется для определения вероятности угрозы и уязвимости. Должна быть поддержана логичность на количественном или качественном подходе.

Подробная информация по оценке актива и по оценке воздействия может быть найдена в Приложении В.

Выходная продукция: список оценённых последствий инцидентного сценария, выраженного относительно активов и критериев воздействия.

8.2.2.3 Оценка вероятности инцидента

Вводная информация: список идентифицированных соответствующих инцидентных сценариев, включая идентификацию угроз, затрагивающих активы, эксплуатируемую уязвимость и последствия к активам и бизнес-процессам. Кроме того, списки всех существующих и запланированных контролей, их эффективности, реализации и состояния использования.

Действие: должна быть оценена вероятность инцидентных сценариев (имеет отношение с [ISO/IEC 27001](#), раздел 4.2.1 е) 2)).

Руководство реализации:

После идентификации инцидентных сценариев (это необходимо, чтобы оценить вероятность каждого сценария и появления воздействия) используются качественные или количественные методики оценки. Для необходимого принятия во внимание того, как часто случаются угрозы, как легко может эксплуатироваться уязвимость, необходимо рассмотрение:

- случаев и соответствующей статистики для вероятности угрозы
- для преднамеренных источников угрозы: мотивацию и возможности, которые изменяются в течение долгого времени, ресурсы, доступные для возможных атакующих, так же как восприятие привлекательности и уязвимости активов для возможного атакующего;
- для случайных источников угрозы: географические факторы, например, близость к химическим или нефтяным предприятиям, возможности критических погодных условий, и факторы, которые могли влиять на человеческие ошибки и сбой оборудования;

- уязвимости, как индивидуальные, так и в агрегации;
- существующие контроли и как эффективно они уменьшают уязвимость.

Например, у информационной системы может быть уязвимость к угрозам маскировки пользовательской тождественности и неправильного употребления ресурсов. Уязвимость маскировки пользовательской тождественности может быть высокой из-за нехватки пользовательской аутентификации. С другой стороны, вероятность неправильного употребления ресурсов может быть низкой, несмотря на нехватку пользовательской аутентификации, потому что способы неправильного использования ресурсов ограничены.

Для точности оценки активы могут быть сгруппированы в зависимости от потребности или где это может быть необходимо, разбить активы на элементы и связать сценарии с элементами. Например, с географическим местоположением природу угроз, теми же самыми типам активами, которые могут изменяться или также могут изменяться эффективности существующих контролей.

Выходная продукция: Вероятность инцидентных сценариев (количественная или качественная).

8.2.2.4 Оценки уровня риска

Вводная информация: список инцидентных сценариев с их последствиями, связанными с активами и бизнес-процессами и их вероятностью (количественной или качественной).

Действие: должен быть оценён уровень риска для всех соответствующих инцидентных сценариев (имеет отношение с [ISO/IEC 27001](#), пункт 4.2.1 е) 4)).

Руководство реализации:

Оценка риска даёт значения вероятности и последствия риска. Эти значения могут быть количественными или качественными. Оценка риска основана на оценённых последствиях и вероятности. Дополнительно можно рассматривать выгоду расходов, проблемы причастных сторон и другие переменные, соответствующие для оценки риска. Предполагаемый риск - комбинация вероятности инцидентного сценария и его последствий.

Примеры различных информационных методов оценки риска безопасности или подходов могут быть найдены в Приложении Е.

Выходная продукция: список рисков с назначенными значениями уровней.

8.3 Оценка риска

Вводная информация: список рисков с назначенными значениями уровней и критерии оценки риска.

Действие: Уровень рисков должен быть сравнен с критериями оценки риска и приемлемыми критериями риска (имеет отношение с [ISO/IEC 27001](#), пункт 4.2.1 е) 4)).

Руководство реализации:

Основываясь на окружающей обстановке и характере заключений используемых для оценки риска и критериев устанавливается оценка риска (которая будет использоваться, чтобы принять решение). Эти решения и контекст должны более подробно повторно перерабатываться на данном этапе, когда больше известно о специфических идентифицированных рисках. Чтобы оценить риски, организации необходимо сравнить предполагаемые риски (используемые выборы методов или подходы обсуждается в Приложении Е) с критериями оценки риска, определёнными во время установления состояния.

Критерии оценки риска должны быть совместимы с определённым внешним и внутренним информационным окружением менеджмента рисков безопасности и для принятия решения должны приниматься во внимание цели организации, взгляды

заинтересованных сторон и т.д. В деятельности оценки риска принятое решение главным образом основано на приемлемом уровне риска. Однако нужно рассмотреть также последствия, вероятность и степень доверия к выявленному риску и анализу. Соединение частей из множества низких или средних рисков может привести к намного более высокому в целом риску, на что должно быть обращено соответственно внимание.

Необходимо рассмотреть следующее:

- свойства информационной безопасности: если один критерий не важен для организации (например, потеря конфиденциальности), то все риски, воздействующие на этот критерий, возможно, не уместны;
- важность бизнес-процесса или деятельности, поддержанной специфическим активом или устанавливаемый активом: если процесс настроен иметь низкое значение для рисков, сопряжённым с этим процессом нужно дать более низкий приоритет рассмотрения, чем рискам, которые воздействуют на более важные процессы или действия;

Оценка риска использует понимание риска, полученного анализом риска, чтобы принять решения о будущих действиях. Решения должны включать:

- деятельность, которую необходимо предпринять;
- приоритеты для рассмотрения обработки риска для оценивания уровня рисков.

В течение стадии оценки рисков, юридические и регулирующие требования – это факторы, которые должны быть приняты во внимание в дополнение к предполагаемым рискам.

Выходная продукция: список расположенных по приоритетам рисков согласно критериям оценки риска относительно инцидентных сценариев, которые приводят к этим рискам.

9 Обработка рисков информационной безопасности

9.1 Общее описание обработки риска

Вводная информация: список рисков расположенных по приоритетам согласно критериям оценки риска относительно инцидентных сценариев, которые приводят к этим рискам.

Действие: Должны быть выбраны контроли, чтобы снизить, сохранить, предотвратить или передать риски и определяется план обработки риска.

Руководство реализации:

Есть четыре опции, доступные для обработки риска: снижение риска (см. 9.2), сохранение риска (см. 9.3), предотвращение риска (см. 9.4) и передача риска (см. 9.5).

ОТМЕТЬТЕ [ISO/IEC 27001](#) 4.2.1. f) 2) использует термин "принимать риск" вместо того, чтобы "сохранить риск".

Рисунок 2 иллюстрирует деятельность обработки риска в пределах процесса менеджмента риском информационной безопасности как представлено на рисунке 1.

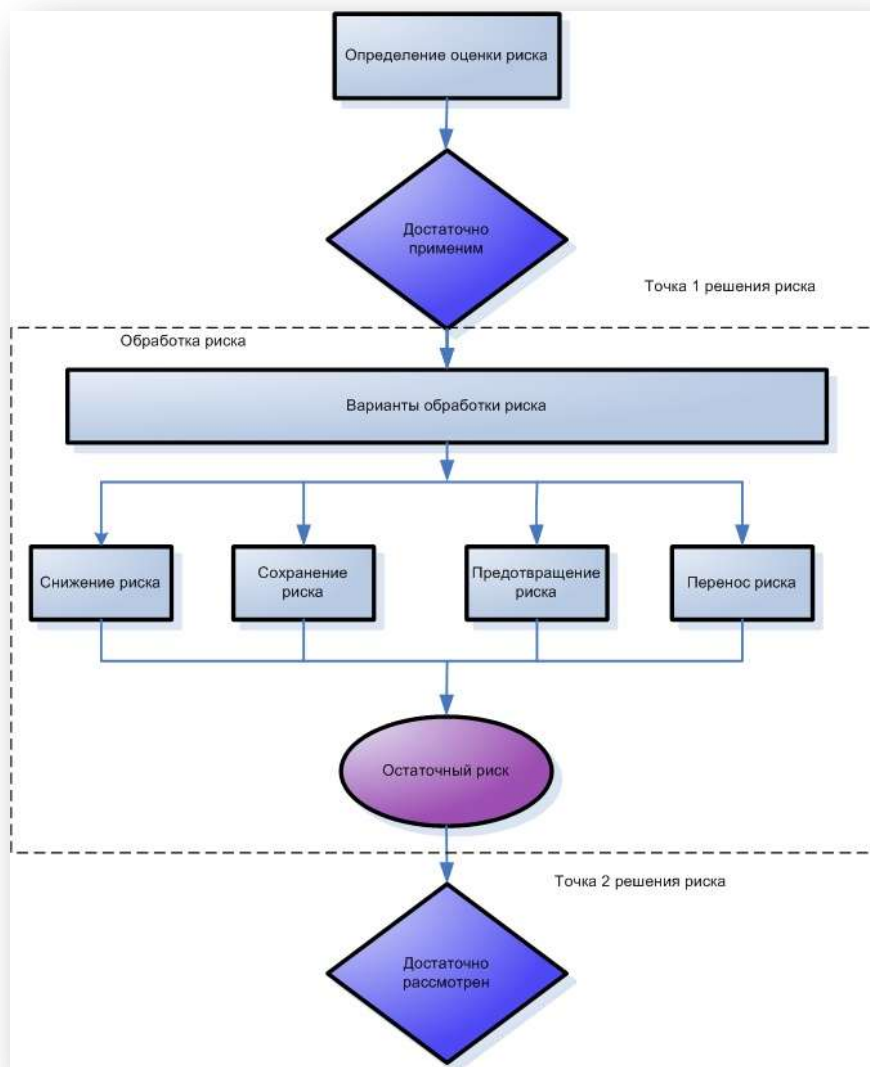


Рисунок 2 - деятельность обработки риска

Должны быть выбраны варианты обработки риска, основанные на результате оценки риска, ожидаемые расходы для того, чтобы осуществить этот предмет выбора и ожидаемые льготы от этих вариантов.

Должны быть осуществлены такие варианты, когда может быть получено внушительное снижение рисков с относительно низкими расходами. Дальнейшие выборы вариантов для усовершенствований могут быть неэкономными и должно быть принято решение относительно того, допустимы ли они.

Вообще, неблагоприятные последствия рисков должны быть сделаны столь же низкими, как это реально разумно и независимо от любых абсолютных критериев. Менеджеры должны рассмотреть редкие, но серьёзные риски. В таких случаях, возможно, должны быть осуществлены (например, менеджмент непрерывностью бизнеса, который как полагается, покрывает определённые высокие риски) контроли, которые не допустимы на строго экономических основаниях.

Все четыре варианта для обработки риска не являются взаимоисключающими. Иногда организация может существенно извлечь выгоду комбинацией вариантов, таких

как снижение вероятности рисков, снижение их последствий и передача или сохранение любых остаточных рисков.

Некоторые варианты обработки риска могут эффективно быть адресованы к более чем одному риску (например, обучение информационной безопасности и осведомлённость). Должен быть определён план обработки риска, который, безусловно, идентифицирует упорядочение по приоритетам, в которых должны быть осуществлены индивидуальные обработки риска и их периодичность. Могут быть установлены приоритеты, используя различные методики, включая ранжирование риска, анализ затрат и эффективность. На ответственности менеджеров организации решение равновесия между стоимостью осуществления контролей и принятия бюджета.

Идентификация существующих контролей может решить, что существующие контроли превышают текущие потребности в условиях сравнений стоимости, включая обслуживание. Если рассматривается удаление избыточных или ненужных контролей (особенно, если у контролей есть высокая стоимость обслуживания), должны быть приняты во внимание стоимостные факторы информационной безопасности. Так как контроли могут влиять друг на друга, удаление избыточных контролей может на месте уменьшить полную безопасность. Кроме того, может быть более дёшево оставить избыточный или ненужный менеджмент на месте, чем удалить его.

Нужно рассматривать опции обработки риска, принимая во внимание:

- как риск воспринят затронутыми партнёрами;
- самые соответствующие способы общения с партнёрами.

Установление состояния (см. 7.2 - критериев оценки риска) предоставляет информацию о юридических и регулирующих требованиях, которым должна подчиниться организация. К организациям должно применяться то, что ограничивает возможность несостоятельно осуществить и обработать варианты для снижения риска. Должны быть приняты во внимание все ограничения во время обработки риска - организационные, технические, структурные и т.д. - которые идентифицированы во время установление состояния учреждения.

Как только был определён план обработки риска, должны быть определены остаточные риски. Это затрагивает пересмотр или повторение оценки риска, принимая во внимание ожидаемые эффекты предложенной обработки риска. Дальнейшая итерация обработки риска может быть необходимой прежде, чем перейти к принятию риска, если остаточный риск все ещё не встречает приемные критерии риска организации. Подробная информация может быть найдена в ISO/IEC 27002, пункт 0.3.

Выходная продукция: план обработки риска и менеджеры организации, приводящие остаточные риски к приемному результату.

9.2 Снижение риска

Действие: уровень риска должен быть снижен через выбор контролей так, чтобы остаточный риск мог быть рассмотрен как являющийся приемлемым.

Руководство реализации:

Должны быть выбраны соответствующие и оправданные контроли, чтобы отвечать требованиям, идентифицированным в соответствии с оценкой риска и обработкой риска. Этот выбор должен принять во внимание приемные критерии риска, такие как юридические, регулирующие и договорные требования. Этот выбор должен также принять во внимание стоимость и период для реализации контролей или технические, экологические и культурные аспекты. Это часто необходимо, чтобы понизить общую стоимость монопольного использования системы с должным образом выбранными контролями информационной безопасности.

Вообще, контроли могут обеспечить один или больше указанных типов защиты: исправление, устранение, предотвращение, минимизация воздействия, сдерживание,

обнаружение, восстановление, контроль и понимание. Во время выбора контроля важно взвесить стоимость приобретения, реализации, администрирования, эксплуатации, контроля и обслуживания контролей против значения защищаемых активов. Кроме того нужно рассмотреть, возвращение инвестиций в терминах сокращения риска и потенциала, чтобы эксплуатировать новые возможности бизнеса, предоставленные определенными контролями. Дополнительно, должно быть дано рассмотрение специализированных навыков, которые могут быть необходимы, чтобы определить и осуществить новые контроли или изменить существующие.

ISO/IEC 27002 обеспечивает подробную информацию относительно контролей.

Есть много ограничений, которые могут затронуть выбор контролей. Технические ограничения, такие как требования производительности, управляемость (требования эксплуатационной поддержки) и проблемы совместимости могут препятствовать использованию определённых контролей, могут вызвать человеческую ошибку или аннулирование контролей, предоставление ложного понятия безопасности или даже более того - увеличение риска, при потере контроля (например, требования сложных паролей без надлежащего обучения, приводит пользователей к записыванию паролей). Кроме того может иметь место контроль, который затронет производительность. Менеджеры должны попытаться идентифицировать решение, которое удовлетворяет требованиям производительности, гарантируя достаточную информационную безопасность. Результат этого шага - список возможных контролей с их стоимостью, выгодой и приоритетом реализации.

Должны быть приняты во внимание различные ограничения в выборе контролей и во время имплементации. Рассматривают, как правило, следующие ограничения:

- временные;
- финансовые;
- технические;
- эксплуатационные;
- культурные;
- этические;
- экологические;
- юридические;
- лёгкости в использовании;
- персонала;
- для того, чтобы интегрировать новые и существующие контроли.

Необходимая информация относительно ограничений для сокращения риска может быть найдена в Приложении F.

9.3 Сохранение риска

Действие: Должно быть принято решение относительно сохранения риска без дальнейшего действия в зависимости от оценки риска.

ОТМЕТЬТЕ, [ISO/IEC 27001](#) пункт 4.2.1 f 2) “сознательное и объективное принятие рисков, если они, безусловно, удовлетворяют политику организации и критериям для того, чтобы принять риски” описывает ту же самую деятельность.

Руководство реализации:

Если уровень риска выполняет приемные критерии риска и нет никакой потребности в осуществлении дополнительных контролей, риск может быть сохранен.

9.4 Предотвращение риска

Действие: деятельность или условия, которое дают начало специфическому риску, которого нужно избежать.

Руководство реализации:

Когда идентифицированные риски считаются слишком высокими или стоимость осуществления других вариантов обработки риска превышает выгоду, может быть принято решение, чтобы избежать риска полностью, уходя из запланированной или существующей деятельности, совокупности видов деятельности или изменяя условия при которых управляют деятельностью. Например, вызванные природные риски могут быть более эффективно решены в стоимостном эквиваленте по сравнению с альтернативой, если физически переместить средства обработки информации в место, где риск не существует или находится под контролем.

9.5 Перенос риска

Действие: риск должен быть передан другой стороне, которая может наиболее эффективно управлять специфическим риском в зависимости от оценки риска.

Руководство реализации:

Перенос риска затрагивает решение разделить определённые риски с внешними сторонами. Перенос риска может создать новые риски или изменить существующие идентифицированные риски. Поэтому может быть необходимой дополнительная обработка риска.

Перенос может быть сделан страхованием, которое поддержит последствия или, заключая субподрядный договор на партнёра, роль которого будет должна контролировать информационную систему и предпринять непосредственные действия, чтобы остановить атаку прежде, чем она сделает определённый уровень повреждений.

Нужно отметить, что может быть возможна передача ответственности за риск менеджментом, но обычно передать ответственность за воздействие не возможно. Исполнители, как обычно, будут приписывать неблагоприятное воздействие, как ошибку самой организации.

10 Сохранение риска информационной безопасности

Вводные данные: план обработки риска и остаточная оценка риска подвергается приемному решению менеджеров организации.

Действие: решение сохранить риски и обязанности за решение должно быть принято и формально зарегистрировано (это связано с [ISO/IEC 27001](#) пункт 4.2.1 h)).

Руководство реализации:

Планы обработки риска должны описать, как оценённые риски были обработанными, до приемных критериев риска (см. приемные критерии риска раздел 7.2). Важно делать пересмотр ответственными менеджерами и осуществлять одобрение предложенных планов обработки риска, получающихся остаточных рисков и делать записи любых состояний, связанных с таким одобрением.

Приемные критерии остаточного риска могут быть определены так или иначе комплексными, быть ниже или выше принятого порога.

В некоторых случаях уровень остаточного риска, возможно, не встречает приемные критерии риска, потому что применяемые критерии не принимают во внимание преобладающие обстоятельства. Например, можно было бы утверждать, что необходимо принять риски, потому что стоимость снижения риска слишком высока, а ущерб, сопровождающий риски очень заманчив. Такие обстоятельства указывают, что приемные критерии риска неадекватны и должны быть, если возможно, пересмотрены. Однако, это не всегда возможно, чтобы своевременным способом пересмотреть приемные критерии риска. В таких случаях лицам, принимающим решения, вероятно, придётся сохранить риски, которые не встречают нормальные приемные критерии. Если это необходимо, лицо, принимающее решения, должно явно прокомментировать риски и внести оправдание для решения отменить нормальные приемные критерии риска.

Выходная продукция: список сохранённых рисков с обоснованием того, что встречается нормальные приемные критерии риска организации.

11 Коммуникации риска информационной безопасности

Вводная информация: все риски информации, полученные от действий менеджмента рисками (см. иллюстрацию 1).

Действие: Информация о риске должна обмениваться и/или разделяться между лицом, принимающим решение и другими заинтересованными сторонами.

Руководство реализации:

Коммуникации риска - деятельность, чтобы достигнуть соглашения по тому, как управлять рисками, обмениваясь и/или делясь информацией о риске между лицами, принимающими решение и другими причастными сторонами. Информация включает, но не ограничена существованием, природой, формой, вероятностью, серьёзностью, обработкой и приемлемостью рисков.

Эффективная коммуникация среди причастных сторон важна, так как это может оказать существенное влияние на решения, которые должны быть приняты. Коммуникации гарантирует, что ответственные за осуществление менеджмента риском и заинтересованные круги понимают основополагающий принцип, на котором приняты решения и почему требуются специфические действия. Коммуникации двунаправлены.

Восприятие риска может измениться из-за различий в предположениях, понятиях и потребностях, проблемах и проблемах причастных сторон, поскольку они имеют отношение с риском или проблемами при обсуждении. Причастные стороны, вероятно, сделают суждения по приемлемости риска основанными на их восприятии риска. Это особенно важно, чтобы гарантировать, что может быть идентифицировано восприятие риска причастными сторонами так же как их восприятие для извлечения выгод, зарегистрировать и ясно понять основные причины и адресацию.

Должны быть выполнены коммуникации рисков, чтобы достигнуть следующего:

- обеспечить гарантирование менеджментом организации результата риска;
- собрать информацию о риске;
- совместно использовать следствия оценки риска и представить план обработки риска;
- избегать и уменьшать распространения последствий нарушений правил информационной безопасности из-за нехватки взаимного понимания среди лиц, принимающих решения и причастных сторон;
- поддерживать принятие решений;
- получить новые знания информационной безопасности;
- координировать с другими сторонами и планами реакций уменьшение последствия любого инцидента;
- довести смысл ответственности о рисках лицам, принимающим решения и причастным сторонам;
- улучшить понимание.

Организация должна разработать планы коммуникации риска относительно нормальной эксплуатации так же как относительно чрезвычайных ситуаций. Поэтому, деятельность коммуникации риска должна выполняться непрерывно.

Координация между главными лицами, принимающими решения и причастными сторонами, может быть достигнута формированием комитета, где могут иметь место дебаты о рисках, их установленных приоритетах и соответствующей обработке и принятии.

Соответствующим подразделением коммуникаций важно сотрудничать с общественностью или коммуникациями в пределах организации, чтобы координировать

все задачи, связанные с риском коммуникаций. Это крайне важно в случае кризисных действий коммуникации, например, в ответ на специфические инциденты.

Выходная продукция: Понимание непрерывности процесса менеджмента риском информационной безопасности организации и их результатов.

12 Мониторинг и пересмотр риска информационной безопасности

12.1 Мониторинг и пересмотр факторов риска

Вводная информация: информация полного риска, полученная из действий менеджмента риском (см. рисунок 1).

Действие: Должны быть проверены и пересматриваться риски и их факторы (то есть значение активов, воздействий, угроз, уязвимости, вероятности возникновения), чтобы в ранней стадии идентифицировать любые изменения в окружении и поддерживать краткий анализ законченной картины риска.

Руководство реализации:

Риски не являются статическими. Угрозы, уязвимость, вероятность или последствия могут измениться резко без любой индикации. Поэтому необходим мониторинг, контролирующий обнаружения этих изменений. Это может быть поддержано внешними службами, которые предоставляют информацию относительно новых угроз или уязвимости.

Организации должны гарантировать, что непрерывно проверяется следующее:

- новые активы, которые были включены в область действия менеджмента риском;
- необходимая модификация значений актива, например из-за изменённых бизнес требований;
- новые угрозы, которые не были оценены и возможно активные внутри и снаружи организации;
- возможная новая или увеличенная уязвимость, позволяющая угрозам эксплуатировать эту новую или изменённую уязвимость;
- идентифицированная уязвимость, чтобы определить те, которые подвергаются новым или повторно появляющимся угрозам;
- увеличенное воздействие или последствия оценённых угроз, уязвимости и рисков в агрегации, приводящие к недопустимому уровню риска;
- инциденты информационной безопасности.

Новые угрозы, уязвимость, изменения в вероятности или последствиях могут увеличить риски, ранее оценённые как низкие. При пересмотре низких и принятых рисков нужно рассматривать каждый риск отдельно и все риски, поскольку агрегация их при оценке также суммируют потенциал их воздействия. Если риски не относятся к низкой или приемлемой категории риска, они должны быть обработаны, используя один или больше вариантов, которые рассматривают в разделе 9.

Факторы, которые затрагивают вероятность и последствия появления угроз, могут изменить варианты, которые затрагивают пригодность или стоимость различных вариантов обработки. Крупные изменения, затрагивающие организацию, должны быть причиной для более специфического пересмотра. Поэтому, действия по мониторингу риска должны регулярно повторяться, выбранные варианты для обработки риска должны периодически повторяться.

Результатом от мониторинга риска может быть вводная к другим действиям по пересмотру риска. Когда происходят ключевые изменения, организация должна регулярно делать пересмотр всех рисков и (согласно [ISO/IEC 27001](#), пункт 4.2.3).

Выходная продукция: Непрерывная регулировка менеджментом рисков в соответствии с бизнес целями организации и с приемными критериями риска.

12.2 Мониторинг, пересмотр и улучшение менеджмента рисков

Вводная информация: информация полного риска, полученная из действий менеджмента рисков (см. рисунок 1).

Действие: процесс менеджмента рисков информационной безопасности должен непрерывно попадать под мониторинг, повторяться и улучшаться по мере необходимости и соответствия.

Руководство реализации:

Продолжающийся мониторинг и пересмотр необходимы, чтобы гарантировать, что окружение, результат оценки риска и обработки риска, так же как и планы менеджмента остаются уместными и соответствующими к обстоятельствам.

Организация должна удостовериться, что процесс менеджмента рисков информационный безопасности и связанные с ним действия остаются соответствующими при существующих обстоятельствах и сопровождаются. Любые согласованные усовершенствования к процессу или действиям, необходимым, чтобы улучшить соответствие с процессом, должны быть зарегистрированы соответствующим менеджером, чтобы иметь гарантию, что не пропущен или недооценён никакой элемент риска и что предприняты необходимые действия и решения, чтобы обеспечить реальное понимание риска и компетентные ответы.

Организация должна дополнительно регулярно проверять, что критерии, имеющие обыкновение измерять риск и его элементы все ещё правильны и совместимы с бизнес целями, стратегиями и политикой и что всё это изменяется в бизнес окружении, учитывается соответственно во время процесса менеджмента риском информационной безопасности. Этот мониторинг и пересмотр деятельности должен быть адресован (но не ограничено перечнем):

- юридическим и относящимся окружением;
- окружением конкуренции;
- подходам оценки рисков;
- значениям актива и категориям;
- критериям воздействия;
- критериям оценки риска;
- одобрением критериев риска;
- общей стоимостью монопольного использования;
- необходимым ресурсам.

Организация должна гарантировать, что оценка риска и ресурсы обработки рисков непрерывно доступны для пересмотра рисков, адресованных к новым или изменённым угрозам или уязвимостям, а так же соответственно консультировать менеджмент.

Менеджмент риском может проводить мониторинг изменений или добавлений подходов, методологий или инструментальных средств, используемых в зависимости от:

- идентифицированных изменений;
- итераций оценки риска;
- стремлений управлять рисками процесса информационной безопасности (например, непрерывностью бизнеса, устойчивостью к инцидентам, соответствий);
- объекта процесса менеджмента риском информационной безопасности (например, организация, бизнес модуль, информационный процесс, его техническая реализация, приложение, подключение к Internet)

Выходная продукция: Уместность непрерывно обрабатывать менеджментом риски информационной безопасности в соответствии с бизнес целям организации или обновлением процессов.

Приложение А (информационное)

Определение области применения и границ процесса менеджмента рисков информационной безопасности

А1 Исследование организации

Оценка организации

Исследование организации выявляет характеристики элементов, идентифицирующих организации. Это касается намерений, бизнеса, миссий, значений и стратегий этой организации. Они должны быть идентифицированы вместе с элементами их разработки (например, заключение субподрядного договора).

Трудность этой деятельности заключается в точном понимании как структурирована организация. Идентификация её реальной структуры обеспечит понимание роли и важность каждого подразделения в достижении целей организации.

Например, факт, что руководитель службы информационной безопасности осуществляет доклад топ - менеджерам, а не IT менеджеру, указывает на причастность топ - менеджеров к информационной безопасности.

Основные намерения организации

Основные намерения организации могут быть определены как мотив, зачем она существует (её поле деятельности, её рыночный сегмент и т.д.).

Бизнес организации

Бизнес организации, определённый служащими и методиками ноу-хау даёт возможность достигнуть своей миссии. Это является определённым для поля деятельности организации и часто определяет свою культуру.

Миссия организации

При достижении организацией своих намерений достигается её миссии. Чтобы идентифицировать миссию должны быть идентифицированы оказанные услуги и/или произведённые продукты относительно конечных пользователей.

Значение организации

Главный принцип значений - чёткий кодекс поведения относился к осуществлению бизнеса. Это может коснуться персонала, отношений с внешними агентами (клиентами и т.д.), качеством поставляемых продуктов или оказанных услуг.

Возьмите, например, организации, цель которых - коммунальное обслуживание и бизнес которого - транспорт и чьи миссии включают транспортировки детей в школу и их неё. Её значения могут быть точностью сервиса и безопасности во время транспортировки.

Структура организации

Тут различные типы структуры:

- **дробная структура:** каждый раздел помещён под властью менеджера подразделения, ответственного за стратегические, административные и оперативные решения относительно его модуля;
- **функциональная структура:** функциональная власть осуществлена на процедурах, природе работы и иногда решений или планирования (например, продукция, IT, человеческие ресурсы, маркетинг и т.д.);

Комментарии:

- раздел в пределах организации с дробной структурой может быть организован как функциональная структура и наоборот;
- у организации, можно так сказать, есть матричная структура, если у неё есть элементы обоих типов структуры;
- в любой организационной структуре можно отличить следующие уровни:
 - уровень принятия решений (определение стратегических ориентаций);
 - уровень лидерства (координация и менеджмент);
 - оперативный уровень (продукция и мероприятия по поддержке).

Организационная структура

Структура организации представлена схематично в организационной структуре. Это представление должно выделить направления уведомлений и делегацию полномочий, но должно также включать другие отношения, которые даже если они не основаны на формальных полномочиях являются, тем не менее, направлениями потока информации.

Стратегия организации

Это требует формального выражения руководящих принципов организации. Руководство определяет стратегию организации и необходимую разработку, чтобы извлечь выгоду из проблем угроз и планируемых главных изменений.

A2 Список ограничений, затрагивающих организацию

Должны быть приняты во внимание все ограничения, затрагивающие организацию и определяющие ориентацию её информационной безопасности. Их источник может быть в пределах организации, когда имеется некоторый контроль над ними или вне организации и поэтому быть вообще неописанным. Наиболее важные ограничения ресурса (бюджет, персонал) и чрезвычайные ограничения.

Организация устанавливает, возможно, за длительный период, свои цели (относительно бизнеса, поведения и т.д.) фиксированные к определённой стезе. Это определяет то, чем это хочет стать и средства, которые должны будут быть осуществлены. В определении этого пути организация принимает во внимание события в методиках и ноу-хау выраженных пожеланиях пользователей, клиентов и т.д. Эта цель может быть выражена в форме стратегии действия или разработки с целью, например, уменьшения эксплуатационных расходов, улучшения качества сервиса и т.д.

Эта стратегия, вероятно, включает информацию и информационную систему (ИС), которая помогает в их применении. Следовательно, характеристики относительно тождественности, миссии и стратегий организации - фундаментальные элементы в анализе проблемы, так как нарушение информационного аспекта безопасности может привести к пересмотру прежнего мнения этих стратегических целей. Кроме того, это является основным, чтобы предложения о требованиях информационной безопасности остались совместимыми с правилами, использованием и средствами самой организации.

Список ограничений включает, но не ограничен:

Ограничения политической природы

Они могут коснуться правительственных администраций, общественных учреждений или в более широком понимании любой организации, которая должна применять правительственные решения. Это решения обычно относительно стратегической или

оперативной ориентации, которые должны быть применены подразделением правительственных органов для принятия решений.

Например, компьютеризация счетов или административных документов формирует проблемы информационной безопасности.

Ограничения стратегической природы

Ограничения могут явиться результатом запланированных или возможных изменений к структурам организации или ориентации. Они выражены в стратегических или оперативных планах организации.

Например, международное сотрудничество в совместном использовании важной информации может требовать соглашений относительно безопасного обмена.

Территориальные ограничения

Структура организации и/или цель могут ввести определённые ограничения, такие как распределение сайтов по всей национальной территории или за границей.

Примеры включают почтовые службы, посольства, банки, филиалы большой индустриальной группы и т.д.

Ограничения, являющиеся результатом экономического и политического климата

Операционная деятельность организации может быть глубоко изменена специфическими событиями, такими как потрясения или национальные и международные кризисы.

Например, некоторые службы должны быть в состоянии продолжить свою деятельность даже во время серьёзного кризиса.

Структурные ограничения

Природа структуры организации (дробной, функциональной или другой) может привести к определённой информационной политике безопасности и организации безопасности, адаптированной к структуре.

Например, международная структура должна быть в состоянии урегулировать требования безопасности, определённые для каждой страны.

Функциональные ограничения

Функциональные ограничения возникают непосредственно из общих или определённых миссий организации.

Например, организация, которая работает круглосуточно, должна гарантировать, что её ресурсы непрерывно доступны.

Ограничения относительно персонала

Природа этих ограничений значительно изменяется. Она связана с: уровнем ответственности, вербовкой, квалификацией, обучением, пониманием безопасности, побуждением, доступностью и т.д.

Например, у всего персонала оборонной организации должно быть разрешение обрабатывать конфиденциальную информацию.

Ограничения, возникающие в результате регистрации организации

Эти ограничения могут следовать из реструктурирования или установки новой национальной или международной политики, налагает определённые ограничения.

Например, создание подразделения безопасности.

Ограничения, связанные с методами

Методы, соответствующие ноу-хау организации должны будут быть наложены для аспектов, таких как проектное планирование, спецификации, разработка и так далее.

Например, типичное ограничение этого вида - потребность включить юридические обязательства организации в политику безопасности.

Ограничения культурной природы

Некоторые привычки работы в организации или основном бизнесе привели к определённой "культуре" в пределах организации, которая может быть несовместима с менеджментом безопасности. Эта культура - общая структура справочной информации персонала и может быть определена многими аспектами, включая образование, машинную команду, профессиональный опыт, опыт вне работы, мнения, философия, верования, социальное состояние и т.д.

Бюджетные ограничения

У рекомендуемых контролей безопасности может иногда быть очень высокая стоимость. Не всегда уместно строить инвестиции безопасности на рентабельности, финансовым подразделением организации вообще требуется экономическое оправдание.

Например, в частном секторе и некоторых общественных организациях общая стоимость контролей безопасности не должна превышать стоимость потенциальных последствий рисков. Поэтому высшее исполнительное руководство должно оценить и взять на себя вычисленные риски, если они хотят избежать чрезмерной стоимости безопасности.

A3 Список законодательных и регулирующих нормативов, применимых к организации

Должны быть идентифицированы регулирующие требования, применимые к организации. Они могут быть законами, декретами, определёнными инструкциями в поле действия или внутренними/внешними инструкциями организации. Это также касается контрактов и соглашений и более широко любых обязательств юридической или регулирующей природы.

A4 Список ограничений, затрагивающих область применения

Идентифицируя ограничения по возможностям необходимо перечислить те, которые оказывают влияние на область применения и определить те, которые, тем не менее, поддаются воздействию. Они добавляют и могут, возможно, откорректировать, ограничения организации, определённые выше. Следующие разделы представляют не исчерпывающий список возможных типов ограничений.

Ограничения, являющиеся результатом существующих ранее процессов

Прикладные проекты не обязательно разработаны одновременно. Некоторые зависят от существующих ранее процессов. Даже при том, что процесс может быть разделён на подпроцессы, процесс не обязательно находится под влиянием всех подпроцессов другого процесса.

Технические ограничения

Касательно инфраструктуры, технические ограничения вообще являются результатом установленных аппаратных средств, программного обеспечения, участков памяти или сайтов, помещающих процессы:

- файлов (требования относительно организации, менеджмента носителями, менеджмента правилами доступа и т.д.);
- общей архитектуры (требования относительно топологии (централизованный, распространённый, клиент-серверный), физической архитектуры и т.д.);
- прикладного программного обеспечения (требования относительно определённого программного дизайна, торговле стандартами и т.д.);

- упаковки программного обеспечения (требования относительно стандартов, уровня оценки, качества, согласия с нормами, безопасностью и т.д.);
- аппаратных средств (требования относительно стандартов, качества, согласия с нормами и т.д.);
- сетей коммуникации (требования относительно охвата, стандартов, способности, надёжности и т.д.);
- встраивания инфраструктур (требования относительно гражданского строительства, конструкции, высоких напряжений, низких напряжений и т.д.).

Финансовые ограничения

Реализация контролей безопасности часто ограничивается бюджетом, который может передать организация. Однако, финансовое ограничение, которое рассмотрят, должно все ещё быть продолженным, поскольку о распределении бюджета для безопасности можно договориться на основе исследования безопасности.

Экологические ограничения

Экологические ограничения являются результатом географической или экономической обстановки, в которой осуществлены процессы: страна, климат, естественные риски, географическая ситуация, экономический климат и т.д.

Временные ограничения

Нужно рассмотреть время, требуемое для того, чтобы осуществить менеджмент безопасности, относительно способности модернизировать информационную систему; если время реализации очень длительное, риски для которых был спроектирован менеджмент, возможно, изменится. Время - коэффициент определения для того, чтобы выбрать решения и приоритеты.

Ограничения, связанные с методами

Методы, соответствующие ноу-хау организации, должны использоваться для проектного планирования, спецификаций, разработка и так далее.

Организационные ограничения

Различные ограничения могут следовать из организационных требований:

- эксплуатации (требования относительно задержек, поставки служб, наблюдения, контроля, планы работы в чрезвычайных ситуациях, ухудшения работы и т.д.);
- обслуживания (требования для инцидентной диагностики, превентивных мер, быстрого исправления и т.д.);
- менеджмента человеческих ресурсов (требования относительно оператора и пользовательского обучения, квалификации для постов, таких как системный администратор или администратор данных и т.д.);
- административного менеджмента (требования относительно обязанностей и т.д.);
- менеджмента разработок (требования относительно инструментальных средств разработки, автоматизированной разработки программного обеспечения, приемных планов, организация, которая будет установлена, и т.д.);
- менеджмента внешними сношениями (требования относительно организации сторонних отношений, контрактов и т.д.).

Приложение В **(информационное)**

Идентификация и определение ценности активов, определение стоимости воздействия

В.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.

В.1.1 Идентификация первичных активов

Деятельность в идентификации первичных активов (действия бизнес процессов, информация) состоит в том, чтобы описать более точно эту область применения. Эта идентификация процессов выполняется представителями рабочей смешанной группы (менеджеры, специалисты по информационным системам и пользователи).

Обычно первичные активы – это основные процессы и информационная деятельности в области применения. Можно также рассматривать другие первичные активы, такие как процессы внутри организации, которые будут более соответствующими для составления политики информационной безопасности или плана непрерывности бизнеса. В зависимости от цели некоторые исследования не будут требовать исчерпывающего анализа всех элементов, составляющих область применения. В таких случаях границы исследования могут быть ограничены ключевыми элементами области применения.

Первичные активы имеют два типа:

1. Бизнес-процессы (или подпроцессы) и действия, например процессы:

- потеря которых или деградация, лишают возможности выполнять миссию организации;
- которые содержат секретные процессы или процессы, вовлекающие частную технологию;
- которые, если изменены, могут сильно затронуть выполнение миссии организации;
- которые необходимы для организации, чтобы выполнить договорные, юридические или регулирующие требования.

2. Информация:

Более широко, первичная информация включает главным образом:

- жизненно важную информацию для осуществления миссии или бизнеса;
- персональную информацию, которая может быть определена государством относительно права частной жизни;
- стратегическую информацию для достижения целей, определённую стратегическими ориентациями;
- информацию высокой стоимости на сбор которой, хранение, обработку и передачу требуется много времени и/или привлечение высоких финансовых затрат.

После этой деятельности у процессов и информации, которые идентифицированы как нечувствительные, в конечном итоге исследования не надо никакой определённой классификации. Это означает что, даже если такие процессы или информация поставлены под угрозу, организация все ещё достигнет своей миссии успешно.

Однако они часто наследуют осуществлённые контроли, чтобы защитить процессы и информацию, идентифицированную как чувствительную.

В.1.2 Перечень и описание поддержки активов

Область применения состоит из активов, которые должны быть идентифицированы и описаны. У этих активов есть уязвимости, которые являются пригодными для использования угрозами, стремящимися ослабить первичные активы области применения (процессы и информацию). Они имеют различные типы:

Аппаратные средства

Аппаратный тип состоит из всех физических элементов, поддерживающих процессы.

Аппаратура обработки данных (активная)

Оборудование для автоматической обработки информации, включая элементы, работающие самостоятельно.

Мобильное оборудование

Переносное компьютерное оборудование.

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

Установленное оборудование

Компьютерное оборудование используется в помещении организации.

Примеры: сервер, микрокомпьютер, используемый как рабочая станция.

Устройства обработки периферии

Оборудование, подключённое с компьютером через коммуникационный порт (последовательный, параллельный и т.д.) для того, чтобы ввести, перенаправить или передавать данные.

Примеры: принтер, сменный дисковод.

Носители данных (пассивные)

Это - носители для того, чтобы хранить данные или функции.

Электронные средства

Средства хранения информации, которые могут быть подключены к компьютерной сети или сети хранения данных. Несмотря на их компактный размер, эти носители могут содержать большое количество данных. Они могут использоваться со стандартным вычислительным оборудованием.

Примеры: гибкий диск, CD-ROM, резервный картридж, сменный аппаратный диск, ключи защиты памяти, лента.

Другие носители

Статические, неэлектронные носители, содержащие данные.

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

Программное обеспечение

Программное обеспечение состоит из всех программ содействующих обработке данных.

Операционная система

Все программы компьютера, составляющего операционное ядро от которого включаются все другие программы (службы или приложения). Операционная система включает ядро и основные функции или службы. В зависимости от архитектуры операционная система может быть монолитной или составлена из микроядра и ряда системных служб. Основные элементы операционной системы - все службы менеджмента оборудованием (центральный процессор, память, диск и сетевые интерфейсы), задание или менеджмент процессов и пользовательские службы менеджмента правами.

Программное обеспечение сервиса, обслуживание или обеспечение

Программное обеспечение характеризуется фактом того, что оно является дополнением службы операционной системы и не непосредственно сервисов пользователей или приложений (даже при том, что это является обычно основным или даже обязательным для глобальной эксплуатации информационной системы).

Пакет программного или стандартного программного обеспечения

Стандартное программное обеспечение или пакет программного обеспечения - это законченные коммерциализированные продукты как таковые (более чем опытные образцы или специфические разработки) с носителем информации, опубликованием и обслуживанием. Они оказывают услуги для пользователей и приложений, но не персонализированы или не специфичны как бизнес приложение.

Примеры: программное обеспечение менеджмента базой данных, программное обеспечение обмена электронными сообщениями, программное обеспечение для коллективной работы, справочное программное обеспечение, программное обеспечение web-сервера и т.д.

Бизнес приложения

Стандартное бизнес приложение

Это - коммерческое программное обеспечение, проектированное, чтобы дать пользовательский прямой доступ к службам и функциям, которых они требуют от их информационной системы в их профессиональной среде. Есть очень широкий круг теоретически безграничный диапазон полей применения.

Примеры: программное обеспечение учётных записей, программное инструментальное обеспечение менеджмента машинами, специфическое медицинское программное обеспечение, программное обеспечение менеджмента компетентностью персонала, административное программное обеспечение и т.д.

Специфические бизнес приложения

Это - программное обеспечение, в котором различные аспекты (прежде всего поддержка, обслуживание, обновление и т.д.) были специально разработаны, чтобы дать прямой пользовательский доступ к службам и функциям, которых требуются пользователю от их информационной системы. Есть очень широкое, теоретически неограниченное поле

применения.

Примеры: менеджмент счетов клиентов телекоммуникационных операторов в реальном времени и мониторинг приложений в реальном времени для запуска ракеты.

Сеть

Сетевой тип состоит из всех устройств передачи данных, используемых, чтобы связать несколько физически отдалённых компьютеров или элементов информационной системы.

Способы передачи и поддержки

Передача информации и носители передачи данных или оборудование характеризованы главным образом в соответствии с физическими и техническими характеристиками оборудования (точка-точка, широковещательное) и в соответствии с протоколами коммуникации (линия связи или сеть - уровни соединения 2 и 3 из 7-ми уровневой OSI- модели открытых систем).

Примеры: общественная сеть переключения телефонов (PSTN), Ethernet, Gigabit Ethernet, асимметричная цифровая абонентская линия (ADSL), беспроводные спецификации протокола (например, WiFi 802.11), технология Bluetooth, FireWire.

Пассивное или активное оборудование передачи

Этот подтип включает все устройства, которые не являются логическими завершёнными в телекоммуникациях (система технического зрения на информационную систему), но являются промежуточными или передающими устройствами. Передача характеризуется в соответствии с поддерживаемыми сетевыми протоколами коммуникации. В дополнение к основной функции передачи они часто включают маршрутизацию и/или функции и службы фильтрации, используя коммутаторы коммуникации и маршрутизаторы с фильтрами. Ими можно часто управлять дистанционно и обычно они способны к генерации журналов.

Примеры: мост, маршрутизатор, концентратор, автоматический коммутатор каналов.

Коммуникационные интерфейсы

Коммуникационные интерфейсы подключены к обрабатывающим устройствам для обработки, но характеризуются носителями и поддерживаемыми протоколами, любой установленной фильтрацией, ведением журналов или функциями предупреждения, мощностями и требованиями возможного удалённого администрирования.

Примеры: пакетная радиосвязь общего назначения (GPRS), адаптер Ethernet.

Персонал

Тип персонала состоит из всех групп людей, вовлечённых в информационную систему.

Лица, принимающие решения

Лица, принимающие решения - владельцы первичных активов (информации и функционала), менеджеры организации или специфического проекта.

Примеры: высшее исполнительное руководство, проектные лидеры.

Пользователи

Пользователи - персонал, кто обрабатывает чувствительные элементы в среде их деятельности и у кого есть специальная ответственность в этом отношении. У них могут быть специальные права доступа к информационной системе, чтобы выполнить их каждодневные задачи.

Примеры: менеджмент человеческими ресурсами, финансовый менеджмент, риск менеджеры.

Штатные сотрудники эксплуатации/обслуживания

Это - персонал, отвечающий за эксплуатацию и поддержание информационной системы. У них есть специальные права доступа к информационной системе, чтобы выполнить их каждодневные задачи.

Примеры: системный администратор, администратор данных, резервирования данных, компьютерная службы помощи (Help Desk), оператор развёртывания прикладных программ, офицеры безопасности.

Разработчики

Разработчики отвечают за разработку приложений организации. Они имеют доступ к части информационной системы с правами высокого уровня, но не предпринимают действия на промышленных данных.

Примеры: разработчики бизнес приложений.

Сайт

Тип сайта включает всю площадь, содержащую сферы деятельности или часть этой сферы и физические средства, требуемые для этой работы.

Местоположение

Условия эксплуатации

Это касается всех местоположений, в которых не могут быть применены средства организации безопасности.

Примеры: дома персонала, помещение другой организации, среда вне сайта (городская область, области риска).

Помещение

Это место ограниченное периметром организации применительно непосредственно с внешней стороной.

Это может быть границей физической защиты, полученной созданием физических барьеров или средства наблюдения вокруг созданий.

Примеры: учреждение, здания.

Зона

Зона сформирована физической защитной границей, формирующей разделение в пределах помещения организации. Это получено, созданием физических барьеров вокруг инфраструктур обработки информации организации.

Примеры: офисы, резервные зоны доступа, зоны безопасности.

Основные службы

Все службы, требуемые для работы оборудования организации.

Коммуникация

Службы передачи данных и оборудование обеспечения операторов.

Примеры: телефонная линия, учрежденческие АТС с исходящей и входящей связью, внутренние телефонные сети.

Коммунальные предприятия

Сервисы и средства (источники и электропроводка) требуемые для того, чтобы обеспечить питание оборудования информационных технологий и периферийных устройств.

Примеры: низковольтные источники питания напряжения, инвертор, головной узел канала электрической сети.

Водоснабжение

Вывоз отходов

Службы и средства (оборудование, контроль) для охлаждения и очищения воздуха.

Примеры: каналы водного охлаждения, кондиционеры.

Организация

Организацию характеризуют типы организационной структуры, состоящие из всех структур персонала, назначенных на задачу и процедур, управляющих этими структурами.

Власти

Это - формирование, от которого рассматриваемая организация получает свою власть. Они могут быть юридически присоединены или быть внешними. Это налагает ограничения на рассматриваемую организацию в терминах инструкций, решений и действий.

Примеры: менеджмент юридическим лицом, главным офисом организации.

Структура организации

Состоит из различных отраслей организации, включая её менеджмент пересекающимися функциями¹¹, под контролем менеджмента.

Примеры: менеджмент человеческими ресурсами, IT менеджмент, менеджер по закупкам, бизнес менеджмент подразделения, компоновка сервиса безопасности, сервис увольнения, менеджмент аудита.

Проектная или системная организация

Это касается организации, установленной для определённого проекта или сервиса.

Примеры: разработка нового прикладного проекта, проект миграции информационной системы.

Субподрядчики / поставщики / изготовители

Это - организации, которые предоставляют организации сервис или ресурсы и связанные с ней в соответствии с контрактом.

Примеры: компания менеджмента средствами, аутсорсингов компания, консультационная компании.

В.2 Оценка актива

Следующий шаг после идентификации актива должен согласовать шкалу, основанной на оценке по которой он будет применяться и критерии для назначения специфического местоположения в этой шкале к каждому активу. Из-за разнообразия активов, найденных в пределах большинства организаций, вероятно, что некоторые активы, у которых есть известное денежно-кредитное значение, будут оценены в местной валюте, в то время как другим, у которых есть более качественное значение, можно назначить расположение значения, например, от "очень низко" к "очень высоко". Решение использовать количественный масштаб против качественного масштаба является действительно вопросом предпочтения организации, но это должно относиться к оцениваемым активам. Оба типа оценки могут использоваться для того же самого актива.

Типичные термины, использованные для качественной оценки активов, включают слова, такие как: незначительный, очень низкий, низкий, средний, высокий, очень высокий и критический. Выбор и диапазон терминов, подходящих для организации строго зависит от потребностей организации в безопасности, размере организации, и других специфических факторов организации.

Критерии

¹¹

Примечание переводчика - процесс, в ходе которого разные группы сотрудничают для осуществления важных для всех групп функций, таких как обучение, стимулирование продаж, упаковка и т. д.

Используемые критерии, как основание для того, чтобы назначить значение на каждый актив, должны быть выписаны в однозначных терминах. Часто это - один из самых трудных аспектов оценки актива, так как значения некоторых активов, вероятно, придётся определять субъективно и так как, вероятно, делать определение будут много различных индивидуумов. Приемлемые критерии имеют обыкновение определять, что значение актива включает свою оригинальную стоимость, свою замену, или стоимость создания заново, или их значение может быть абстрактным, например, значение репутации организации.

Другое основание для оценки активов - стоимость, понесённая из-за потери конфиденциальности, целостности и доступности как результат инцидента. Также нужно соответствующе рассмотреть невозможность отказа от авторства, наблюдаемость, подлинность и надёжность. Такая оценка обеспечила бы важную размерность элемента значению актива в дополнение к стоимости замены, основанной на оценках неблагоприятных бизнес последствий, которые будут следовать из инцидентов безопасности с принятым стечением обстоятельств. Подчеркнём, что это позволит рассчитать результаты, которые необходимы фактору оценки риска.

Многие активы в течение оценки принимают несколько назначенных значений. Например: бизнес-план может быть оценён на основании трудозатрат, израсходованных чтобы разработать план, это может быть оценено в трудозатратах, чтобы ввести данные и это может быть оценено на основании его значения конкуренту. Каждое из назначенных значений наиболее вероятно будет значительно отличаться. Назначенное значение может быть максимумом всех возможных значений или может быть суммой некоторых или всеми возможными значениями. В конечном анализе должны быть тщательно определены, оценены или назначены значения на актив, так как конечное назначенное значение выступает в определение ресурсов, которые будут израсходованы для защиты актива.

Приведение к общему значению

В конечном счёте, все оценки актива должны быть приведены до общего значения. Это может быть сделано при помощи соответствующих критериев. Критерии, которые могут использоваться, чтобы оценить возможные последствия, следующие из потери конфиденциальности, целостности, доступности, невозможность отказа от авторства, наблюдаемости, подлинности или надёжности активов:

- нарушение законодательства и/или регулирования;
- ухудшение производительности бизнеса;
- потеря доброжелательности/негатив на репутации;
- нарушение, связанное с личной информацией;
- угроза персональной безопасности;
- отрицательные воздействия на приведение законов в жизнь;
- нарушение конфиденциальности;
- нарушение общественного порядка;
- финансовая потеря;
- перерыв бизнес деятельности;
- угроза экологической безопасности.

Другой подход, чтобы оценить последствия, может быть в:

- Прерывании сервиса:
 - неспособность оказать услугу.

- Потере доверия клиента:
 - потерь доверия во внутренней информационной системе;
 - вреде репутации.
- Разрушении внутренней работоспособности:
 - разрушения непосредственно в организации;
 - дополнительной внутренней стоимости.
- Разрушении работоспособности третьего лица:
 - разрушение у третьих лиц, проводящих операции с организацией;
 - различного типа повреждения.
- Нарушении законов / инструкции:
 - неспособности выполнить юридические обязательства.
- Нарушении условий контракта:
 - неспособности выполнить договорные обязательства.
- Опасности для персонала / пользовательской безопасности:
 - опасности для персонала организации и / или пользователей.
- Атаке на частную жизнь пользователей.
- Финансовых потерях.
- Финансовой стоимости для чрезвычайной ситуации или восстановления в терминах:
 - персонала;
 - оборудования;
 - исследований, отчётов экспертов.
- Потере товаров / денежных средств / активов.
- Потере клиентов, потере поставщиков.
- Судебных тяжбах и штрафах.
- Потере преимуществ конкурентоспособности.
- Потере технологической/технической главной роли.
- Потере эффективности/доверия.
- Потере технической репутации.
- Снижении роли в ведении переговоров.
- Индустриальных кризисах (ударах).
- Правительственных кризисах.
- Увольнении.
- Материальном ущербе.

Эти критерии - примеры проблем, которые рассматриваются для оценки актива. Для того чтобы выполнить оценки, организация должна выбрать критерии, относящиеся к её типу требований безопасности и бизнеса. Это могло бы означать, что некоторые из упомянутых выше критериев не применимы и что другие, возможно, должны быть добавлены в список.

Шкала

После установления рассмотренных ранее критериев организация должна договориться о шкале оценок, которой будет пользоваться вся организация. Первый шаг

должен выбрать число уровней, которые будут использоваться. Нет никаких правил относительно числа уровней, которые являются самыми подходящими. Больше уровней обеспечивает больший уровень степени детализации, но иногда великолепное дифференцирование делает в организации трудными присваивание всюду непротиворечивых оценок. Обычно принимается любое число уровней от трёх (например, низкий, средний и высокий уровень) до 10, которое может использоваться пока это совместимо с подходом организации относительно процесса используемого для оценки риска в целом.

Организация может определить свои собственные пределы для значений актива, как "низкое", "среднее" или "высокое". Эти пределы должны быть оценены согласно выбранным критериям (например, за возможную финансовую потерю их нужно оценить в денежно-кредитных значениях, но для рассмотрений, таких как угроза личной безопасности, денежно-кредитная оценка может быть сложной и возможно, не является соответствующей для всех организаций). В конце – концов, организация полностью решает, что рассматривать как являющееся "низким" или "высоким" последствием. Последствие, которое могло бы быть пагубным для маленькой организации, может быть низким или даже незначительным для очень большой организации.

Зависимости

Чем более значим актив в деле поддержки многочисленных бизнес-процессов, тем больше значение этого актива. Должны быть идентифицированы также зависимости активов на бизнес процессы и другие активы, так как это может влиять на значения активов. Например, должна быть сохранена конфиденциальность данных всюду по всему циклу жизни, во всех стадиях, включая хранение и обработку, то есть потребности безопасности хранения данных и обработки программ должны быть непосредственно связаны со значением, представляющим конфиденциальность данных, сохранность и обработку. Кроме того, если бизнес-процесс полагается на целостность определённых данных, производимых в соответствии с программой, входные данные этой программы должны иметь соответствующую надёжность. Кроме того, целостность информации будет зависеть от аппаратных средств и программного обеспечения, используемого для её хранения и обработки. Кроме того, аппаратные средства будут зависеть от источника питания и возможно кондиционирования воздуха. Таким образом, информация о зависимостях поможет идентификации угроз и особенно уязвимости. Дополнительно, это поможет убеждать, что активам дано истинное значение (через отношения зависимости), таким образом, указывая соответствующий уровень защиты.

Значения активов, от которых зависят другие активы, могут быть изменены следующим образом:

- если значения зависимых активов (например, данных) ниже или равны значению актива, который рассматривается (например, программное обеспечение), его значение остаётся тем же самым
- если значения зависимого актива (например, данные) больше, то значение актива, который рассматривают (например, программное обеспечение), должно быть соответственно увеличено согласно:
 - степени зависимости;
 - значению других активов.

У организации могут быть некоторые активы, которые доступны неоднократно, такие как копии программ или тот же самый тип компьютера, используемый в большинстве

офисов. Важно рассмотреть этот факт, делая оценку актива. С одной стороны, эти активы легко пропускаемы, поэтому должна быть предпринята предосторожность, чтобы идентифицировать все их; с другой стороны, они могут использоваться, чтобы уменьшить проблемы доступности.

Выходная продукция

Конечной выводной продукцией этого шага являются список активов и их значений относительно раскрытия (сохранение конфиденциальности), модификации (сохранение целостности, подлинности, невозможности отказа от авторства и наблюдаемости), отсутствия готовности и уничтожения (сохранение доступности и надёжности) и стоимости замены.

В.3 Оценка воздействия

Инцидент информационный безопасности может воздействовать на больше чем один актив или только часть актива. Воздействие связано в степени успеха инцидента. Как следствие, есть важное различие между значением актива и воздействием, следующим из инцидента. Воздействием считают наличие или непосредственный (эксплуатационный) эффект или будущий (бизнес) эффект, который включает финансовые и рыночные последствия.

Непосредственное (эксплуатационное) воздействие является прямым или косвенным.

Прямое воздействие:

- a) финансовое значение замены потерянного (части) актива;
- b) стоимость приобретения, конфигурации и инсталляции нового актива или резервной копии
- c) стоимость приостановленных операций из-за инцидента до восстановления услуги, оказанной активом (ами);
- d) которое приводит к нарушению правил информационной безопасности.

Косвенное воздействие:

- a) альтернативные издержки (финансовые ресурсы должны заменить или исправить актив, который будет использоваться в другом месте);
- b) стоимость прерванных операций;
- c) потенциальное неправильное употребление информации полученной через нарушение правил безопасности;
- d) нарушение установленных законом или регулирующих обязательств;
- e) нарушение норм нравственного поведения.

Также, первая оценка (без контроля любым видом) оценивает воздействие как очень близко к (комбинации) имеющему отношению значения актива. При любой следующей итерации воздействия на актив будут различаться (обычно, значительно уменьшаться) из-за присутствия и эффективности осуществляемых контролей.

Приложение С (информационное) Примеры типичных угроз

Следующий список даёт примеры типичных угроз. Список может использоваться в течение процесса оценки угрозы. Угрозы могут быть преднамеренными, случайными или экологическими (естественными) и иметь результат, например, нарушение или потеря основных 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 находятся 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
Радиационные неисправности	Электромагнитная радиация	A, D, E
	Тепловая радиация	A, D, E
	Электромагнитный импульс	A, D, E
Компрометация информации	Перехват и отправка компрометированного сигнала	D
	Удалённый шпионаж	D
	Подслушивание	D

Тип	Угрозы	Обозначение
Компрометация информации	Воровство носителей или документов	D
	Воровство оборудования	D
	Восстановление информации на носителях, отправленных на переработку или бракованных	D
	Обнаружение	A, D
	Данные из ненадёжных источников	A, D
	Вмешательство в аппаратные средства	D
	Вмешательство в программные средства	D
	Обнаружение позиции	D
Технические отказы	Отказ оборудования	A
	Сбой оборудования	A
	Ограничения информационной системы	A, D
	Программный сбой	A
	Нарушение ремонтпригодности информационной системы	A, D
Несанкционированные действия	Несанкционированное использование оборудования	D
	Мошенническое копирование программного обеспечения	D
	Использование поддельного или скопированного программного обеспечения	A, D
	Искажение данных	D
	Незаконная обработка данных	D
Компрометация функций	Ошибка в использовании	A
	Злоупотребление правами	A, D
	Подделка 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	Восстание Эго Вызов Статус Деньги	<ul style="list-style-type: none"> • Хакерство • Социальная инженерия • Вторжение в систему, нарушение • Несанкционированный доступ в систему
Компьютерный преступник	Разрушение информации Незаконное раскрытие информации Денежно-кредитная выгода Неправомерное чередование данных	<ul style="list-style-type: none"> • Компьютерное преступление (например, кибер-преследование) • Мошенническое действие (например, переигровка, подражание, перехват) • Информационное взяточничество • Имитация • Вторжение в систему
Террорист	Мечь Разведка Разрушение Шантаж Политические выгоды Освещение в печати	<ul style="list-style-type: none"> • Бомба/Терроризм • Информационная война • Системная атака (например, распределённый отказ в обслуживании) • Проникновение в систему • Вмешательство в систему

Источник угрозы	Мотивация	Возможные последствия
Индустриальный шпионаж (компании, иностранные правительства, другие правительственные интересы)	Конкурентоспособное преимущество Экономический шпионаж	<ul style="list-style-type: none"> • Экономическая разведка • Информационное воровство • Вторжение в персональные данные • Социальная разработка • Проникновение в систему • Несанкционированный доступ в систему (доступ к секретной, частной, и/или связанной с технологией информации)
Инсайдер (плохо обученные, рассерженные, злонамеренные, небрежные, нечестные или уволенные служащие)	Разведка Эго Любопытство Денежно-кредитная выгода Мсть Неумышленные ошибки и упущения (например, ошибка ввода данных, ошибка программирования)	<ul style="list-style-type: none"> • Нападение на служащего • Шантаж • Просмотр секрета фирмы • Неправильное компьютерное обращение • Мошенничество и воровство • Информационное взяточничество • Ввод фальсифицированных данных, разрушение 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

Следующая таблица даёт примеры уязвимостей в различных областях безопасности, включая примеры угроз, которые могли бы эксплуатировать эту уязвимость. Перечень может обеспечить справку во время оценки угроз и уязвимости, определить соответствующие инцидентные сценарии. Подчеркнём, что в некоторых случаях другие угрозы могут эксплуатировать также эту уязвимость.

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

Тип	Примеры уязвимости	Примеры угроз
	Широко распространённое программное обеспечение	Искажение данных
	Применение прикладных программ к фальшивым данным в терминах времени	Искажение данных
	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	Воровство носителей или документов
	Отказ менеджмента от проверки отчётов	Несанкционированное использование оборудования
	Нехватка доказательства отправки 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

Тип	Примеры уязвимости	Примеры угроз
	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
	Изъёмы понимания безопасности	Ошибка в использовании
	Нехватка механизмов мониторинга	Незаконная обработка данных
	Неконтролируемая работа внешним штатом или убирающим персоналом	Воровство носителей или документов
	Изъёмы политики для правильного использования носителей передачи данных и обмена сообщениями	Несанкционированное использование оборудования

Тип	Примеры уязвимости	Примеры угроз
Сайт 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	Воровство оборудования
	Изъёмы формальной процедуры для пользовательской регистрации и де-регистрации	Злоупотребление правом

Тип	Примеры уязвимости	Примеры угроз
Сайт организации	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
	Неадекватный ответ обслуживающего сервиса	Нарушение ремонтпригодности информационная система
	Изъяны или недостаточное соглашение сервисного обслуживание	Нарушение ремонтпригодности информационная система
	Изъяны процедуры контроля внесения изменений	Нарушение ремонтпригодности 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

Тип	Примеры уязвимости	Примеры угроз
	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	Воровство оборудования
	Нехватка формальной политики по использованию мобильной компьютерной техники	Воровство оборудования
	Нехватка менеджмента активами дистанционного резервирования	Воровство оборудования
	Нехватка или недостаточная политика «чистого стола и чистого экрана»	Воровство носителей или документов
	Нехватка санкций на средства обработки информации	Воровство носителей или документов
	Нехватка установленных контрольных механизмов в случае нарушений правил безопасности	Воровство носителей или документов
	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 Технические методы для оценки уязвимости

Чтобы идентифицировать уязвимости в зависимости от критичности информации и информационно-коммуникационных технологий (ICT) могут использоваться превентивные методы, такие как тестирование информационной системы, системных и доступных ресурсов (например, распределённые фонды, доступные технологии, проведение теста людей-экспертов). Испытательные методы включают:

- автоматизированный инструмент сканирования уязвимостей;
- тестирование безопасности и оценку;
- тестирование проникновения;
- пересмотр кода.

Чтобы просмотреть группу главных компьютеров или сеть на предмет известных уязвимых служб (например, систему, позволяющую анонимный протокол передачи файлов (FTP), передачу sendmail), используется автоматизированный инструмент сканирования уязвимости. Однако нужно отметить, что часть потенциальных уязвимостей, идентифицированных автоматизированным инструментом сканирования, возможно, не

представляет реальную уязвимость в контексте системной среды. Например, некоторые из этих инструментальных средств сканирования оценивают потенциальную уязвимость, не рассматривая среду сайта и требования. Часть уязвимостей, помеченных автоматизированным программным обеспечением сканирования, возможно, фактически не уязвима для определённого сайта, но может быть сконфигурирована, потому что обстановка требует этого. Таким образом, этот испытательный метод может произвести ошибочные допуски.

Тестирование безопасности и оценка являются другой методикой, которая может использоваться в идентификации уязвимости системы ИСТ во время процесса оценки риска. Это включает разработку и выполнение плана испытаний (например, испытательный скрипт, испытательные процедуры и ожидаемые результаты испытаний). Цель системного тестирования безопасности состоит в том, чтобы проверить эффективность контролей безопасности системы ИСТ, поскольку они были применены в эксплуатируемой среде. Цель состоит в том, чтобы гарантировать, что менеджмент использует одобренную спецификацию безопасности для прикладного программного обеспечения и оборудования и осуществляют политику безопасности организации или использует отраслевые стандарты.

Может использоваться тестирование проникновения, чтобы дополнить пересмотр контролей безопасности и гарантировать, что обеспечены различные аспекты системы ИСТ. Когда применяется тестирование проникновения в процессе оценки риска, результаты этого могут использоваться, чтобы оценить способность системы ИСТ противостоять намеренным попыткам обойти системную безопасность. Цель состоит в том, чтобы проверить систему ИСТ с точки зрения источника угрозы и идентифицировать потенциальные отказы в схемах системной защиты ИСТ.

Пересмотр кода является самым полным (но также и самым дорогим) в пути оценки уязвимости.

Результаты этих типов тестирования безопасности помогут идентифицировать уязвимости системы.

Важно отметить, что инструментальные средства проникновения и методики могут дать ложные результаты, если не успешно эксплуатируется уязвимость. Чтобы эксплуатировать специфическую уязвимость, нужно знать точную систему / приложение / и установленные исправления на проверенной системе. Если эти данные не известны во время тестирования, то это не может быть возможным для успешной эксплуатации специфической уязвимости (например, получая `remote reverse shell`¹²); однако, это все же возможно, чтобы разрушить или перезапустить проверяемый процесс или систему. В таком случае проверенный объект нужно также считать уязвимым.

Методы могут включать следующие действия:

- интервьюирование у людей и пользователей;
- анкетные опросы;
- физическое обследование;
- анализ документа.

¹² Примечание переводчика(для информации): `remote reverse shell` или `grs` - обратный (подключающийся) удаленный командный интерпретатор. Вместо прослушивания входящих подключений, он будет подключаться к `grs` в режиме прослушивания. Процесс прослушивания будет принимать подключения и получать командный интерпретатор с удаленного хоста. `grs` обеспечивает полную поддержку псевдотерминалов, полную поддержку OpenSSL (клиент-серверную аутентификацию и выбор комплектов шифрования), шифрование по алгоритму Twofish, простое шифрование с помощью XOR, сеансы открытым текстом, отслеживание "соседних" сеансов, возможность работы в виде демона, а также повторное подключение. `grs` точно компилируется и работает в ОС Linux, FreeBSD, NetBSD, OpenBSD и QNX.

Приложение Е **(информационное)** **Подходы в оценке рисков информационной безопасности**

Е.1 Оценка рисков информационной безопасности высокого уровня

Оценка высокого уровня позволяет определять приоритеты и хронологию в действиях. По различным причинам, таким как бюджет, это может быть не возможным для одновременного осуществления всех контролей и только к самым критическим рискам можно обратиться через процесс обработки риска. Также, может быть преждевременным начало детализированного менеджмента рисков, если реализация предусмотрена только один или два года. Чтобы достигнуть этой цели, оценка высокого уровня может начаться с оценки последствий высокого уровня вместо того, чтобы начинать с систематического анализа угроз, уязвимости, активов и последствий.

Другая причина начинать с оценки высокого уровня состоит в том, чтобы синхронизироваться с другими планами, связанными с изменением менеджмента (или непрерывностью бизнес). Например, это не является нормой к полностью безопасной системе или приложению, если запланировано произвести это на стороне в ближайшем будущем, хотя может все ещё стоить делать оценку риска, чтобы определить производящийся на стороне контракт.

Особенности итерации оценки риска высокого уровня могут включать следующее:

- Оценки риска высокого уровня может обратиться к более глобальному представлению организации и её информационных систем, рассматривая аспекты технологии как независимые от проблем бизнеса. Делая это, контекстный анализ концентрируется больше на эксплуатационной и бизнес среде, чем технологических элементах.
- Оценка риска высокого уровня может обратиться к более ограниченному перечню угроз и уязвимостей, группированных в определённых доменах или ускорить процесс, она может сосредоточиться на риске или на сценарии вместо их элементов.
- Риски, представленные в оценке рисков высокого уровня, часто являются более общими доменами риска, чем определёнными идентифицированными рисками. Поскольку сценарии или угрозы группированы в доменах, обработка рисков предлагает перечни контролей в этом домене. Тогда сначала пытаются предложить действия обработки риска и выбрать общий менеджмент, который проходит через целую систему.
- Тем не менее, наиболее соответствующее обеспечить менеджмент организационных и нетехнических контролей и технические аспекты менеджмента контролей, таких как резервное копирование и антивирусная защита для оценки риска высокого уровня или уровня общих технических гарантий, если это редко обращено к подробностям технологий.

Преимущества оценки риска высокого уровня следующие:

- начальное объединение простых подходов, вероятно, получит принятие программой оценки риска;
- это должно быть, возможно, чтобы построить организационно стратегический имидж программы информационной безопасности, то есть это будет действовать как хорошая

помощь в планировании;

- могут быть применены ресурсы и деньги, где они, вероятно, самые выгодные, и к системам для обращения сначала к самым большим потребностям защиты.

Поскольку начальные исследования риска на высоком уровне потенциально менее точны, так как потенциальный недостаток – это то, что некоторые бизнес-процессы или требования системы не могут быть детально идентифицированы за короткое время оценкой риска. Этого можно избежать, если есть адекватная информация относительно всех аспектов организации её информации и системы, включая информацию, полученную от оценки информационных инцидентов безопасности.

Оценка риска высокого уровня рассматривает бизнес значения информационных активов и риски с точки зрения бизнеса организации. В первом решающем пункте (см. рисунок 1), несколько критериев помогают в определении, адекватна ли оценка высокого уровня в обработке риска; эти критерии могут включать следующее:

- бизнес цели, которые будут достигнуты при использовании различных информационных активов;
- уровень каждого информационного актива, от которого зависит бизнес организации, то есть, зависят функции, которые организация считает важным по отношению к её выживанию или эффективному ведению бизнеса от каждого актива или от конфиденциальности, целостности, доступности, от возможности отказа от авторства, наблюдаемости, подлинности, надёжности информации, хранящейся и обрабатываемой на этом активе;
- уровень инвестиций в каждом информационном активе в терминах разработки, поддержания или замены актива, и
- информационные активы, для которых организация непосредственно определяет значение.

Решение становится более простым, когда оценены эти критерии. Если цели актива чрезвычайно важны для поведения бизнеса организации или если активы находятся в области высокого риска, то должна быть проведена вторая итерация детальной оценки риска для специфического информационного актива (или части его).

Общее правило применяется: если нехватка информационной безопасности может привести к существенным неблагоприятным последствиям в организации, её бизнес-процессам или её активам, то необходима вторая итеративная оценка риска на более детальном уровне, чтобы идентифицировать потенциальные риски.

Е.2 Подробная оценка риска информационной безопасности

Процесс подробной оценки риска информационной безопасности вовлекает всестороннюю идентификацию и оценку активов, оценку угроз этим активам и оценку уязвимости. Чтобы оценить риски и затем идентифицировать обработку риска используются следствия этих действий.

Шаг детальной оценки обычно требует большого количества времени, усилия и экспертизы, и может, поэтому быть самым подходящим для информационных систем с высоким риском.

Конечная стадия оценки риска информационной безопасности должна подробно оценить полные риски, которые является основой этого приложения.

Последствия могут быть оценены несколькими способами, включая использование количественных, например денежно-кредитных и качественных мер (которые могут быть

основаны на использовании таких прилагательных как умеренные или серьёзные), или комбинации обоих. Чтобы оценить вероятность осуществления угрозы должен быть установлен период времени, в течение которого актив будет иметь определённое значение или должен быть защищён. Вероятность появления определённой угрозы вызывается следующим:

- привлекательностью актива или возможностью применить воздействия, когда рассматривают преднамеренную человеческую угрозу;
- вероятностью преобразования уязвимости, эксплуатирующей актив, применимой к вознаграждению, если рассматривают преднамеренную человеческую угрозу;
- техническими возможностями агента угрозы, применяемого, чтобы обдумать человеческие угрозы, и
- восприимчивостью уязвимости к эксплуатации, применительно к технической и к нетехнической уязвимости.

Много методов используют таблицы и комбинируют субъективные и эмпирические меры. Важно, что организация использует метод, с которым удобно организации и в котором уверена организация и что это приведёт к повторяемым результатам. Несколько примеров основанных на методике таблиц даны ниже.

Е.2.1 Пример матрицы с предопределёнными значениями

В методах оценки риска этого типа фактические или предложенные физические активы оценены в терминах замены или стоимости реконструкции (то есть количественные измерения). Эта стоимость преобразована на тот же самый качественный масштаб, поскольку использовано для информации (см. ниже). Фактические или предложенные программные активы оценены таким же образом как физические активы с идентифицированной стоимостью покупки или реконструкции и затем преобразованы в тот же самый качественный масштаб, поскольку использованы для информации. Дополнительно находят, если у какого-нибудь прикладного программного обеспечения, есть свои собственные встроенные требования для конфиденциальности или целостности (например, если исходный текст самостоятельно коммерчески чувствителен), это оценивается таким же образом, что касается информации.

Значения для информации получены, беря интервью у выбранного бизнес менеджмента (“владельцев данных”), кто может говорить авторитетно о данных, определить значение и фактически чувствительность данных в использовании, сохранении, обработке или обращении. Интервью облегчают оценку значения и чувствительность информации в терминах случая самых плохих сценариев, которые, ожидаемы в разумных пределах случая от неблагоприятных бизнес последствий из-за несанкционированного раскрытия, несанкционированной модификации, уязвимости для переменных периодов времени и уничтожения.

Оценка достигнута если используются рекомендации по оценке информации, которые покрывают такие проблемы как:

- персональная безопасность;
- персональная информация;
- юридические и регулирующие обязательства;
- приведение законов в жизнь;
- реклама и экономические интересы;
- действия финансовых потерь/разрушений;

- общественный порядок;
- политика бизнеса и эксплуатации;
- потеря доброжелательности;
- контракт или соглашение с клиентом.

Рекомендации облегчают идентификацию значений в числовых значениях, например, от 0 до 4, значений, которые показаны в матрице примера ниже, таким образом, допуская распознаванию количественных значений, и где возможны только логические и качественные значения и так как количественные значения не возможны, например, для угрозы человеческой жизни.

Следующая главная деятельность - завершение анкетных опросов для каждого типа угрозы, для каждого группирования активов, с которыми имеет отношение тип угрозы, допуская оценку уровней угроз (вероятность вхождения) и уровней уязвимости (вероятность эксплуатации угрозами и вызова неблагоприятные последствия). Каждый ответ вопроса включён в таблицу кадров. Эти таблицы кадров суммируются через базу знаний и с диапазонами сравнений. Это идентифицирует уровни угроз на, собственно говоря, высокие, чтобы низко масштабировать и уровни уязвимости точно так же как показано в матрице примера ниже, дифференцируясь между типами соответствующих последствий. Чтобы завершить анкетные опросы должна быть собрана информация от интервью с соответствующим техническим персоналом и персоналом, работающим по договору, а так же е и осмотром физического местоположения и изучения документации.

Значения актива, угрозы и уровня уязвимости, относящиеся к каждому типу последствия, согласованы в матрице, так как это показано ниже, идентифицируя для каждой комбинации соответствующей мере риска в масштабе от 0 до 8. Значения помещены в матрицу структурным способом. Пример дан ниже:

	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 рассматривают соответствующую уязвимость и их соответствующую угрозу. Если есть уязвимость без соответствующей угрозы или угрозы без соответствующей уязвимости, то нет теперь никакого риска (но нужно предусмотреть, что эта ситуация изменяется). Теперь соответствующая строка в матрице идентифицирована значением актива, и соответствующий столбец идентифицирован вероятностью появления угрозы и вероятностью эксплуатации. Например, если у актива есть значение 3, угроза

"высока" и уязвимость "низкая", мера риска 5. Предположите, что у актива есть значение 2, например, для модификации, уровень угрозы "низких" и вероятность эксплуатации "высока", тогда мера риска 4. Размер матрицы, в терминах числа категорий вероятности угрозы, вероятности категорий эксплуатации и числа категорий оценки актива может быть откорректирована к потребностям организации. Дополнительные столбцы и строки требуют дополнительных мер по риску. Значение этого подхода находится в ранжировании рисков, которые будут использоваться.

Подобная Матрица как показано в Таблице E.1 b) следует из рассмотрения вероятности инцидентного сценария, отображённого против предполагаемого воздействия на бизнес. Вероятность инцидентного сценария дана угрозой, эксплуатирующей уязвимость с определённой вероятностью. Таблица отображает эту вероятность против воздействия на бизнес, связанного с инцидентным сценарием. Получающийся риск измерен в масштабе от 0 до 8, который может быть оценён против приемных критериев риска. Этот масштаб риска мог также быть отображён в простой оценке абсолютного риска, например как:

- 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 низко	0	1	2	3	4
	Низко	1	2	3	4	5
	Средне	2	3	4	5	6
	Высоко	3	4	5	6	7
	Очень высоко	4	5	6	7	8

Таблица E.1 b)

E.2.2 Пример ранжирования мер угроз риска

Матрица или таблица, такая как это показано в Таблице E.2 могут использоваться, чтобы связать коэффициенты последствий (значение актива) и вероятность осуществления угрозы (принимаяющей во внимание аспекты уязвимости). Первый шаг должен оценить последствия (значение актива) в предопределённом масштабе, например 1 - 5, каждого актива, которому угрожают (столбец "b" в таблице). Второй шаг должен оценить вероятность вхождения угрозы в предопределённом масштабе, например 1 - 5, каждой угрозы (столбец "c" в таблице). Третий шаг должен вычислить меру риска, умножением (b x c). Наконец угрозы могут быть ранжированы в порядке их связанной меры риска. Отметьте, что в этом примере, 1 взята как самое низкое последствие и самая низкая вероятность осуществлением угрозы.

Дескриптор(ы) опасностей	Последствия (активы) ценность (b)	Вероятность распространения угроз (c)	Мера риска (d)	Ранжирование опасности (e)
Угроза А	5	2	10	2
Угроза В	2	4	8	3
Угроза С	3	5	15	1
Угроза D	1	3	3	5
Угроза Е	4	1	4	4
Угроза F	2	4	8	3

Таблица Е.2

Как показано выше, это - процедура, которая разрешает сравнение и ранжирование в порядке приоритета различным угрозам с отличающимися последствиями и вероятностью вхождения, как показано здесь. В некоторых случаях это будет необходимо, чтобы связать денежно-кредитные значения с эмпирическими масштабами, используемыми здесь.

Е.2.3 Пример оценки значения для вероятности и возможных последствий рисков

В этом примере значение придано последствиям инцидентов информационной безопасности (то есть инцидентные сценарии) и на определении, каким системам нужно уделить первостепенное значение. Это сделано, оценивая два значения для каждого актива и риска, которые в комбинации определяют таблицу кадров для каждого актива. Когда для системы суммированы все таблицы кадров активов, тогда мера риска в той системе определена.

Первое, что нужно сделать - это определить значение на каждый актив. Это значение имеет отношение с потенциальными неблагоприятными последствиями, которые могут возникнуть, если активу угрожают. Для каждой соответствующей угрозы активу определено это значение.

Необходимо затем оценить значение вероятности. Это оценивается от комбинации вероятности появления угрозы и вероятности возможной эксплуатации уязвимости, смотрите Таблицу Е.3, выражающей вероятность инцидентного сценария.

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

Таблица Е.3

После того как назначена таблица кадров актив/угроза, находят пересечение значения и вероятности актива в Таблице Е.4. Активы/угрозы рассчитаны в Таблицы кадров, чтобы произвести таблицу кадров общего значения актива. Это значение может использоваться, чтобы дифференцировать значения активов между собой, являющихся частью 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

Конечный шаг должен рассчитывать все таблицы кадров всех активов системы, производя системную таблицу кадров. Это может использоваться, чтобы дифференцироваться между системами и определить, какой системы защите нужно уделить первостепенное значение.

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**

Рассматривая ограничения для снижения риска, должно быть принято во внимание следующие:

Временные ограничения:

Могут существовать много типов временных ограничений. Например, должны быть осуществлены контроли в пределах периода времени, приемлемого для менеджеров организации. Другой тип временного ограничения - может ли менеджмент быть осуществлён в пределах жизненного цикла информации или системы. Третий тип временного ограничения может быть промежутком времени, который определяют менеджеры организации приемлемым периодом, который будет сопоставлен специфическому риску.

Финансовые ограничения:

Контроли не должны быть более дорогими в осуществлении или поддержке, чем значение рисков, для которых спроектирована защита, кроме тех случаев, где это необходимо принудительно (например, по законодательству). Должно быть предпринято всевозможные усилия, чтобы с помощью контролей не превысить назначенный бюджет, и достигнуто финансовое преимущество. Однако в некоторых случаях это может быть не возможным для достижения желательной безопасности и уровня принятия риска, поэтому необходимо планировать ограничения. Поэтому происходит дискуссия менеджеров организации для резолюции по этому вопросу.

Должна быть предпринята большая осторожность, если бюджет сокращает количество или качество осуществляемых контролей, так как это может привести к неявному удержанию риска больше, чем запланировано. Всегда необходимо со значительной осторожностью использовать установленный бюджет как ограничивающий фактор для контролей.

Технические ограничения:

Можно легко избежать технических проблем, таких как совместимость программ или аппаратных средств, если они приняты во внимание во время выбора контролей. Кроме того, ретроспективной реализации контролей к существующему процессу или системе часто препятствуют технические ограничения. Эти трудности могут переместить равновесие контролей к процедурным и физическим аспектам безопасности. Это может быть необходимо, чтобы пересмотреть программу информационной безопасности, чтобы достигнуть целей безопасности. Это может произойти, когда контроли не отвечают ожидаемым результатам в сокращении рисков, не уменьшая производительность.

Эксплуатационные ограничения

Эксплуатационные ограничения, такие как потребность работы резервирования 24x7 могут привести к сложной и дорогостоящей реализации контролей, если они не встроены в дизайн с самого начала.

Культурные ограничения:

Могут быть определённые культурные ограничения к выбору контролей для страны, сектора, организации или даже отдела в пределах организации. Не все контроли могут быть

применены во всех странах. Например, что может быть возможным в Европе, например, осуществление досмотра сумок, не может быть возможным на Ближнем Востоке. Не могут быть проигнорированы культурные аспекты, потому что много контролей полагается на активную поддержку штатных сотрудников. Если сотрудники не поймут потребность в контроле или не найдут это культурно приемлемым, то контроль станет неэффективным в течение долгого времени.

Этические ограничения:

У этических ограничений могут быть изменения основных значений в менеджменте этики, основанные на социальных нормах. Это может запретить в некоторых странах осуществление контроля, такого как сканирование почты. Может также изменяться оценка информации о частной жизни в зависимости от этики региона или правительства. Ограничения могут представлять больший интерес в некоторых секторах промышленности, нежели в других, например, в правительстве и здравоохранении.

Экологические ограничения:

Экологические факторы могут влиять на выбор контролей, таких как пространственная пригодность, критические условия климата, окружающая естественная и городская география. Например, может требоваться корректировка на землетрясения в одних странах, но ненужная в других.

Юридические ограничения:

Могут затронуть выбор контролей юридического фактора, таких как защита персональных данных или безопасность в обработке информации, касающейся уголовного кодекса. Законодательное и регулирующее соответствия могут обязать использование определённых типов контролей, включая защиту данных и финансовый аудит; они могут также запретить использование некоторых контролей, например кодирования (шифрования). Могут также затронуть выбор контролей некоторых законов и постановлений, таких как отношения в трудовом законодательстве, пожарной охране, охране здоровья и безопасности, регуляторных секторов экономики и т.д.

Лёгкость в использовании:

Результатом слабого интерфейса человек-технология будет человеческая ошибка и это может сделать контроль бесполезным. Должны быть выбраны контроли, чтобы обеспечить оптимальную лёгкость в использовании, достигая приемлемого уровня остаточного риска в бизнесе. Будут воздействовать на эффективность контроли, которые являются трудными в использовании, поскольку пользователи могут попытаться обойти или проигнорировать их в максимально возможной степени. Сложные контроли доступа в пределах организации могут способствовать нахождению пользователями дополнительных, несанкционированных методов доступа.

Ограничения персонала:

Нужно рассмотреть расходы на подготовку, зарплаты и на специализированные наборы навыков для осуществления контролей и способность взаимозаменяемости штатных работников в неблагоприятных эксплуатационных режимах. Возможно, не готова экспертиза для осуществления запланированных контролей, или экспертиза может быть чрезмерно дорогостоящей для организации. Другие аспекты, таких как тенденция некоторых штатных сотрудников, выделяться среди других сотрудников возможностью не досматриваться службой безопасностью, может быть главным для имплементации политики безопасности и

действий. Также, критическая ситуация найма на работы привилегированными людьми и их результат исследования может привести к найму работника прежде, чем будет закончен отбор службой безопасности. Требование к отбору службой безопасности, которое будет закончено перед наймом, является нормальной и самой безопасной практикой.

Ограничения интегрирования новых и существующих контролей:

Часто пропускается интеграция новых контролей в существующие инфраструктуры и взаимозависимость между контролями. Не могут легко быть осуществлены новые контроли, если есть несовместимость или несовместимость с существующими контролями. Например, план использовать биометрических маркеров для контроля физического доступа может вызвать конфликт с базовой существующей системой контроля доступом типа PIN-pad. Стоимость изменения от существующих контролей до запланированных контролей должна включать элементы, которые будут добавлены к полной стоимости обработки риска. Может быть невозможным осуществить выбранные контроли из-за помех с текущими контролями.

Библиография

[1] ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards	[1] Руководство ISO/IEC 73:2002, 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] AS/NZS 4360:2004, Risk Management	[3] AS/NZS 4360:2004, Менеджмент рисков
[4] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook	[4] NIST Специальная публикация 800-12, Введение в компьютерную безопасность: Руководство NIST
[5] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology	[5] NIST Специальная публикация 800-30, Руководство менеджмента рисков для систем информационной технологии, рекомендации национального института стандартов и технологии