ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

**Р 50.1.088—
2013**

Менеджмент риска

РУКОВОДСТВО ПО ОЦЕНКЕ РИСКА ДЛЯ ОПАСНОСТЕЙ СО СТОРОНЫ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Издание официальное

Москва
Стандартинформ
2015

Предисловие

1 РАЗРАБОТАНЫ Автономной некоммерческой организацией «Научно-исследовательский центр контроля и диагностики технических систем» (АНО «НИЦ КД»)

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 10 «Менеджмент риска»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1668-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

Информация об изменениях к настоящим рекомендациям публикуется в ежегодном указателе «Руководящие документы, рекомендации и правила», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Содержание

Введение

Как правило, при оценке угроз безопасности организации со стороны персонала рассматривают доступ сотрудников к активам организации, последствия, которые это представляет для организации, и достаточность контрмер. Все это является основой процесса обеспечения безопасности организации. Крайне важны также для обеспечения безопасности риски, которым подвержена организация со стороны воздействия человеческого фактора.

Настоящие рекомендации могут быть полезны организации при:

- оценке угроз со стороны действий персонала и причастных сторон;
- ранжировании рисков для организации;
- определении контрмер для снижения этих рисков;
- распределении ресурсов на обеспечение безопасности.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Менеджмент риска

РУКОВОДСТВО ПО ОЦЕНКЕ РИСКА ДЛЯ ОПАСНОСТЕЙ СО СТОРОНЫ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Risk management.Guidance for risk assessment of dangers from the human factor

Дата введения — 2014—12—01

1 Область применения

В настоящих рекомендациях на простом примере показано применение метода оценки риска организации для опасностей со стороны действий персонала или партнеров, имеющих доступ к активам организации.

Показаны приемы качественной оценки вероятности последствий опасного события с применением условной шкалы и использования таких оценок для определения качественной оценки риска.

2 Нормативные ссылки

ГОСТ Р 51897—2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения

ГОСТ Р ИСО/МЭК 31000—2010 Менеджмент риска. Принципы и руководство

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины и определения по ГОСТ Р 51897—2011.

4 Общие положения

4.1 Безопасность от действий человеческого фактора

Обеспечение безопасности от действий человеческого фактора — это система менеджмента, включающая политику и процедуры, направленная на снижение риска для организации от опасностей со стороны персонала или подрядчиков, имеющих законный доступ к активам или в помещения организации. Тех, кто имеет законный доступ, называют «посвященными лицами».

Издание официальное

В настоящих рекомендациях люди, имеющие законный доступ к активам организации, но не относящиеся к штату или подрядчикам (например, почтовые работники) не отнесены к посвященным лицам.

Существует много мер защиты организации от несанкционированных действий персонала и подрядчиков, которые обычно используют для обеспечения безопасности организации. Большая часть из них относится к указанным в таблице 1 категориям.

Таблица 1 — Основные мероприятия защиты от несанкционированных действий

Меры обеспечения безопасности	Мероприятия
Меры обеспечения безопасности до включения в штат организации лиц, принимаемых на работу	1) Проверки: - проверка данных при приеме на работу, - оценка возможности включения в посвященные лица, - проверка службой национальной безопасности[1)]
Меры обеспечения безопасности после включения в штат организации лиц, принятых на работу	2) Проверки: - проверка данных при приеме на работу, - оценка поведения, - проверка службой национальной безопасности; 3) управление доступом; 4) внедрение культуры безопасности; 5) социальная инженерия; 6) выявление наличия контроля и вторжения; 7) расследования
[1)] Проверка службой национальной безопасности существенно отличается от мероприятий защиты в организации. Такую проверку применяют только к особым должностям в организации.	

4.2 Менеджмент риска в области защиты от опасностей со стороны человеческого фактора

Обеспечение безопасности организации позволяет предотвратить ряд преступных посягательств и преступлений посвященного лица (краж, хищений, поджогов, актов вандализма, общественных беспорядков, проведения террористических актов). Разработка мероприятий по безопасности может быть трудоемкой, дорогостоящей и может привести к затруднениям в деятельности организации, поэтому необходимо определение адекватных риску организации и значимым последствиям мер по обеспечению безопасности. Менеджмент риска является основой для обеспечения эффективной безопасности организации. Общая схема менеджмента риска приведена на рисунке 1.

Рисунок 1 — Схема менеджмента риска

Менеджмент риска включает в себя:

- **оценку риска** (Должен быть определен риск организации, в том числе вероятность опасного события и возможные последствия);

- **выполнение** (Для снижения вероятности и последствий нежелательного события до допустимого уровня должны быть определены и выполнены меры по обеспечению безопасности);

- оценку эффективности контрмер (Должны быть определены корректирующие действия и эффективность предпринятых мер по обеспечению безопасности).

Процесс менеджмента риска включает проведение постоянной оценки риска и анализ эффективности контрмер. Большое значение для процесса менеджмента риска имеет систематическое исследование опасностей, последствий и контрмер с учетом обязательств перед причастными сторонами. Обсуждения данных о мерах, принятых для обеспечения безопасности, позволяют достичь взаимопонимания с партнерами и другими причастными сторонами.

Процесс оценки риска включает этапы идентификации опасностей и последствий (см. также ГОСТ Р ИСО/МЭК 31000).

Настоящие рекомендации посвящены оценке риска для опасностей со стороны воздействия человеческого фактора. Схема оценки риска приведена на рисунке 2.

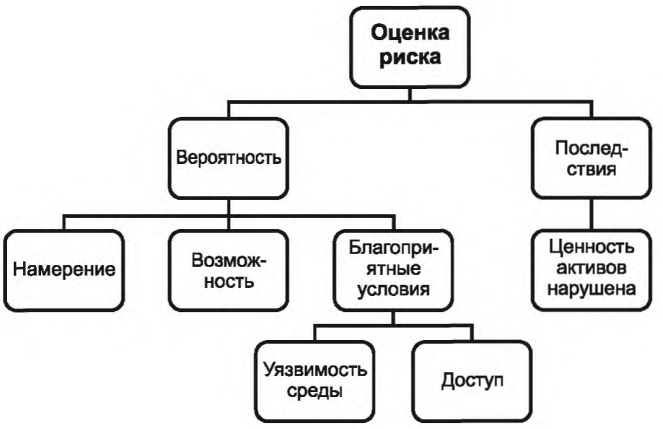


Рисунок 2 — Схема оценки риска

Обычно под риском понимают сочетание вероятности реализации события и его последствий[1)].

Реализация события включает три составляющие: намерение, возможности и благоприятные условия. Намерение характеризует решимость посвященного лица совершить преступную акцию. Возможности определяют наличие у посвященного лица навыков, знаний и ресурсов для успешного выполнения попытки преступной акции.

Благоприятные условия — это комбинация доступа, который посвященное лицо имеет к активам организации (на основе его положения и функциональных обязанностей) и уязвимости среды (например, среда постоянно контролируемая телекамерами менее уязвима для некоторых опасностей, чем среда, не оснащенная этими средствами).

Последствия необходимо рассматривать с точки зрения ценности активов и всех возможных последствий. Например, мошенничество посвященного лица может повлечь финансовые последствия и снижение репутации организации.

4.3 Относительные и абсолютные оценки риска

В некоторых случаях для определения оценки риска используют количественные меры, которые являются абсолютными или относительными. Абсолютная оценка риска показывает вероятность события и его последствие в количественных мерах, таких как финансовая стоимость или потери человеческих жизней. Относительная оценка риска лишь указывает место данного события при ранжировании вероятностей и последствий.

Часто невозможно получить абсолютные оценки риска, поэтому применяют смешанные подходы, в которых используют такие значения для вероятности и последствий, как «очень низкий», «очень высокий» и др. В этом случае необходимо, чтобы все участники однозначно понимали эти термины. Сами эксперты должны быть в состоянии присвоить событию соответствующее значение.

[1)] См. также Федеральный закон «О техническом регулировании» № 184 ФЗ от 27.12.2002 г.

4.4 Уровни оценки риска

Существует три уровня, для которых могут быть определены оценки опасностей со стороны воздействия человеческого фактора:

1) Уровень организации.
2) Уровень группы.
3) Уровень сотрудника.

В первом случае исследуют и ранжируют типы опасностей со стороны посвященного лица, которые представляют опасность для организации в целом. Во втором случае исследуют группы с различными возможностями причинения вреда организации, а в третьем случае исследуют документированные соглашения с каждым сотрудником отдельно.

Большинство практиков считают полезным начать с самого простого и высшего уровня — оценки риска организации, который обеспечивает краткий обзор опасностей и возможность рассмотрения контрмер в целом. Оценка риска на уровне группы требует больше времени и усилий, но может привести к выявлению групп сотрудников, которые дают повод для сомнений в их лояльности. Оценка на уровне сотрудника является самой сложной, когда исследуют каждого сотрудника для определения общих возможностей конкретного посвященного лица.

Выбор уровня оценки риска зависит от особенностей организации и персонала. Следует помнить, что каждому подходу соответствует свой тип решений. Например, если оценка риска для организации показывает наличие незначительной угрозы внесения посвященным лицом бомбы в здание организации, это может исключить требование о сдаче сумок, пакетов и другой ручной клади в камеру хранения при входе в здание. Оценка риска на уровне группы может показать, что у определенной группы сотрудников имеется доступ к очень конфиденциальной или значимой для организации информации, поэтому за ними необходим более высокий уровень наблюдений. Если на уровне отдельного сотрудника, у какого-то работника имеется высокий уровень возможностей нанесения вреда организации, то для этого работника может потребоваться специальный менеджмент риска.

4.5 Проведение оценки риска безопасности персонала

Оценки риска наиболее эффективны, если они являются неотъемлемой частью системы менеджмента риска.

Наилучшие результаты могут быть получены, когда группа оценки риска включает в себя:

- специалистов по безопасности в области человеческих ресурсов;
- специалистов, хорошо знающих функции работников;
- специалистов в области внешних контактов.

Процесс оценки риска должен быть интерактивным с использованием групповых обсуждений. Ценность этих обсуждений может быть повышена при наличии квалифицированного руководителя и использовании наглядных пособий. Составление участниками обсуждения большого количества схем, таблиц (см. приложение Б), также помогает повысить эффективность этих обсуждений.

5 Оценка риска на уровне организации

5.1 Общие положения

Оценка риска на уровне организации идентифицирует диапазон опасностей со стороны посвященного лица, которые ранжируют в соответствии с их вероятностью и последствиями. Это формирует понимание внутренних рисков для организации. Также это составляет основу для разработки и внедрения мер по обеспечению безопасности от несанкционированных действий со стороны персонала и причастных сторон.

Результаты оценки риска на уровне организации должны быть зафиксированы в таблице, форма которой приведена в таблице 2.

Таблица 2 — Форма таблицы данных для оценки риска

Внутренняя опасность для организации	Вероятность (1—5)	Предположения относительно вероятности	Последствия (1—5)	Предположения относительно последствий	Ранг риска (1—4)	Контрмеры		
						Существующие	Существующие меры достаточны?	Новые

Таблицу оценки риска заполняют по мере получения данных. После заполнения таблица содержит полный перечень внутренних опасностей.

5.2 Этап 1. Идентификация внутренних опасностей

Пример заполнения таблицы 2 на этапе 1приведен в таблице 3.

Таблица 3 — Пример заполнения таблицы 2 на этапе 1

Этап 1	Этап 2		Этап 3	
Внутренняя опасность	Вероятность (1—5)	Предположения относительно вероятности	Последствия (1—5)	Предположения относительно последствий
Например, работник организации вводит вирус в ИТ-систему[1)]				
Например, работник организации проносит взрывное устройство в здание				

На первом этапе необходимо идентифицировать внутренние опасности организации и сделать запись о них в первой колонке таблицы. Перечень внутренних опасностей приведен в приложении А. Каждая опасность должна быть определена в описательной форме: посвященное лицо осуществляет действия в несанкционированных целях, что требует его доступа в организацию.

Опасности должны быть тщательно и четко определены, если на основе оценки риска должны быть приняты важные решения.

5.2.1 Диапазон опасностей

При определении опасностей следует изучить полный перечень несанкционированной деятельности посвященного лица, включая (но не ограничиваясь) физическое нападение, злоупотребление интеллектуальной собственностью и несанкционированное раскрытие значимой (для деятельности организации) или конфиденциальной информации.

5.2.2 Определение опасностей посвященного лица

Следует учитывать, что посвященное лицо может иметь намерение использовать свой законный доступ к активам организации в несанкционированных целях.

5.2.3 Уровень детализации опасностей

Опасности должны быть определены на уровне детализации, позволяющем рассматривать контрмеры для каждой опасности. Очень широкого определения опасности, такого как «бомбы» или «утечки информации» недостаточно, потому что они не содержат достаточной информации для контрмер. С другой стороны, использование слишком узких определений может дать слишком большое количество опасностей, исходящих от посвященного лица.

5.3 Этап 2. Оценка вероятности

Пример заполнения таблицы 2 на этапе 2 приведен в таблице 4.

Таблица 4 — Пример заполнения таблицы 2 на этапе 2

Этап 1	Этап 2		Этап 3	
Внутренняя опасность	Вероятность (1—5)	Предположения относительно вероятности	Последствия (1—5)	Предположения относительно последствий
Например, работник вводит вирус в ИТ-систему	2	Наличие у работника системных прав администратора, необходимых для преодоления защиты ИТ-системы		
Например, работник приносит взрывное устройство в здание организации	1	Сотрудник принес взрывное устройство в сумке		

[1)] ИТ — информационные технологии.

Для каждой опасности определяют вероятность ее реализации и указывают в колонке «Вероятность». При оценке вероятности не следует рассматривать последствия реализации опасности. Оценки вероятности и последствий реализации опасности следует делать независимо друг от друга. На данном этапе не следует пытаться определять вероятности с высокой точностью. Достаточно установить вероятности опасностей относительно друг друга в баллах от 1 (маловероятно) до 5 (очень вероятно).

Часто бывает полезно просмотреть весь перечень исследуемых опасностей и назначить опасностям оценки вероятности от 1 до 5 (5 — наиболее вероятной опасности, а оценку 1 — наименее вероятной). Шкала оценки вероятности опасного события приведена на рисунке 3.

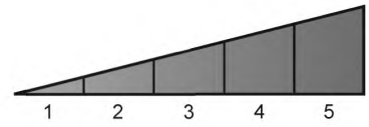


Рисунок 3 — Шкала оценки вероятности опасного события

В результате все опасные события должны быть расположены в порядке возрастания вероятности их реализации.

Все предположения, использованные при оценке вероятности, должны быть зарегистрированы в колонке «Предположения относительно вероятности». Эта информация может быть полезна при разработке контрмер. Необходимо также учитывать частоту реализации опасного события. Опасное событие может произойти в течение одного года или нескольких лет. Если сделаны предположения относительно времени, в течение которого реализуются опасные события, эти предположения следует учитывать на всех этапах анализа.

При оценке вероятности следует рассмотреть следующие вопросы:

- насколько реально, что в отношении организации будет выполнено данное противоправное действие?
- организация уже подвергалась данному типу противоправного действия ранее? Это подтверждает уместность и возможность реализации опасности, но не обязательно повышает вероятность данного опасного события. Следует помнить, что отсутствие рассматриваемых опасных событий в прошлом не означает, что они не будут происходить в будущем;
- какова ситуация с безопасностью в организации и в соответствующей отрасли?
- существуют ли в организации проверки персонала, направленные на выявление у сотрудников возможностей выполнения исследуемого противоправного действия?
- насколько эффективны существующие в организации планы действий в непредвиденных обстоятельствах и существующие контрмеры?

5.4 Этап 3. Оценка последствий

Пример заполнения таблицы 2 на этапе 3 приведен в таблице 5.

Таблица 5 — Пример заполнения таблицы 2 на этапе 3

Этап 1	Этап 2		Этап 3	
Внутренняя опасность	Вероятность (1—5)	Предположения относительно вероятности	Последствия (1—5)	Предположения относительно последствий
Например, сотрудник ввел вирус в ИТ-систему	2	Наличие у работника системных прав администратора, необходимых для преодоления защиты ИТ-системы	2	Нарушение работы ИТ-системы в течение 24 часов
Например, сотрудник принес взрывное устройство в здание организации	1	Сотрудник принес взрывное устройство в сумке	5	Погибло менее 50 человек

Последствия опасного события оценивают аналогично по шкале от 1 (самые слабые последствия) до 5 (самые значимые последствия). Шкала оценки последствий приведена на рисунке 4.

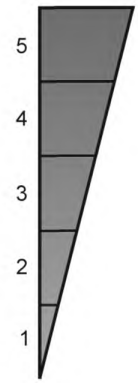


Рисунок 4 — Шкала оценки последствий опасного события

Несмотря на то что шкала является относительной, она должна быть основана на значимых для организации факторах, таких как:

- количество или значимость для организации нарушенных или разрушенных рабочих мест;
- наличие травм среди персонала и населения;
- финансовые потери;
- потери для репутации организации;
- время, необходимое для восстановления деятельности организации;
- адекватность планов на случай нештатных ситуаций и существующих контрмер.

В колонке «Предположения относительно последствий» необходимо зафиксировать предположения, использованные при оценке значимых последствий.

Последствия каждого опасного события должны быть зарегистрированы в таблице в колонке «Последствия».

5.5 Этап 4. Ранжирование риска

Пример заполнения таблицы 2 на этапе 4 приведен в таблице 6.

Таблица 6 — Пример заполнения таблицы 2 на этапе 4

Этап 1	Этап 2		Этап 3		Этап 4
Внутренняя опасность	Вероятность (1—5)	Предположения относительно вероятности	Последствия (1—5)	Предположения относительно последствий	Приоритет риска
Например, сотрудник ввел вирус в ИТ-систему	2	Наличие у работника системных прав администратора, необходимых для преодоления защиты ИТ-системы	2	Нарушение работы ИТ-системы в течение 24 часов	2
Например, сотрудник принес взрывное устройство в здание организации	1	Сотрудник принес взрывное устройство в сумке	5	Погибло < 50 человек	4

На основе оценок вероятности и последствий ранжируют риски для рассматриваемых опасностей.

В некоторых случаях в качестве риска рассматривают произведение баллов, присвоенных вероятности и последствиям, считая, что меньшее значение произведения соответствует меньшему риску и наоборот. Однако это не всегда приемлемо, поскольку ситуации с низкой вероятностью и значимыми последствиями и ситуации с высокой вероятностью и небольшими последствиями в этом случае могут быть неразличимы.

Внедрение контрмер, как правило, оказывает существенное влияние на вероятность и последствия, причем степень влияния может значительно отличаться для различных опасностей. Полученные данные о вероятности и последствиях объединяют в матрице риска.

В матрице риска показан риск, соответствующий каждой опасности. Матрица риска обеспечивает наглядное представление ситуации с учетом использованных предположений.

Чем выше в матрице риска расположено опасное событие, тем более значимые последствия оно вызывает, чем правее — тем выше вероятность его реализации (см. рисунок 5). Часто анализ матрицы риска требует пересмотра результатов, полученных на предыдущих этапах.

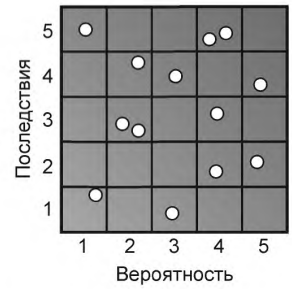


Рисунок 5 — Матрица риска

Все новые предположения относительно вероятности или последствий опасных событий, сделанные в результате анализа матрицы риска или изменения прежних предположений должны быть зафиксированы в таблице оценки риска.

Ранжирование риска проводят после ранжирования всех опасных событий в матрице риска. Опасные события в верхнем правом углу матрицы риска соответствуют самой высокой вероятности и самым значимым последствиям. Им соответствует ранг 1. Опасные события в нижнем левом углу матрицы риска соответствуют самой низкой вероятности и наименее значимым последствиям. Им соответствует минимальный ранг, например ранг 4. Примеры ранжирования риска представлены на рисунке 6.

На практике ранжирование рисков по четырем категориям применяет большая часть организаций. Однако может быть использовано другое количество категорий риска. Например, три или пять категорий.

Деление матрицы на пять или большее количество категорий риска обеспечивает большую точность, но может потребовать больше времени для анализа.

На основе ранжирования рисков принимают решение о распределении ресурсов.

Ранг риска для каждой опасности должен быть указан в соответствующей колонке таблицы данных.

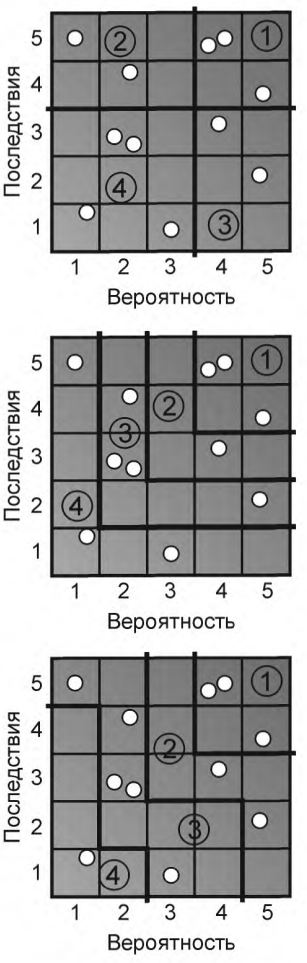


Рисунок 6 — Примеры ранжирования риска

5.6 Этап 5. Контрмеры

Этот этап выполняют более подробно при оценке риска на уровне группы. При выполнении оценки риска на уровне группы, нельзя завершать работу анализом контрмер на уровне организации. Однако при этом допустимо более общее рассмотрение контрмер на уровне организации. Пример заполнения таблицы 2 на этапе 5 приведен в таблице 7.

Т а б л и ц а 7 — Пример заполнения таблицы 2 на этапе 5

Этап 5		
Контрмеры		
Существующие	Существующие контрмеры достаточны?	Новые
Применение антивирусной защиты	- Работа системы может быть нарушена отдельными сотрудниками; - Личные устройства USB могут быть связаны с компьютерами организации	- Введение двух правил приостановки антивирусной защиты; - Запрет пользования USB портами на компьютерах
Проведение в течение дня выборочного досмотра сумок	- В ночное время проверки не проводят; - Согласие на досмотр сумки не фиксируется	- Введение выборочного досмотра сумок во внеурочное время; - Введение процесса фиксирования досмотра сумок

Начиная с риска категории 1 в колонке «Существующие» указывают все применяемые в настоящее время контрмеры.

Каждая контрмера должна быть проанализирована на достаточность. По каждой контрмере могут быть заданы следующие вопросы:

- прошли ли сотрудники службы безопасности соответствующее обучение, позволяющее отличать подозрительные объекты от прочих?
- какова вероятность ошибок при обнаружении подозрительных объектов на основе проводимых проверок?
- имеется ли резервный аппарат для досмотра сумок в случае отказа основного?

В колонке «Существующие контрмеры»достаточно сделать записи обо всех сомнениях, а в колонке «Новые» указывают необходимые контрмеры.

Затем проводят анализ всех контрмер и определяют, позволяют ли они поддерживать риск на допустимом уровне. При необходимости в колонке «Существующие контрмеры достаточны?» делают дополнительные записи, используя рекомендации экспертов, и определяют новые контрмеры, которые указывают в колонке «Новые».

5.7 Этап 6. Создание абсолютной шкалы оценки последствий

Для большинства организаций это дополнительный этап, который применяют для обоснования или определения затрат на выполнение контрмер.

Используя информацию, представленную в таблице данных для каждого опасного события, необходимо рассмотреть затраты, связанные с его последствиями, использованные предположения и их влияние на затраты.

В каждом случае необходимо проанализировать почему последствиям присвоено то или иное значение. Если последствия могут быть представлены в денежном выражении, то каковы предполагаемые потери? Если последствия связаны с человеческими жертвами, то каково предполагаемое количество жертв? Если последствия связаны с причинением вреда имуществу организации, то каково предполагаемое количество поврежденного имущества.

Это позволяет построить шкалу для грубой оценки потерь в денежном выражении, в виде количества человеческих жертв, количества разрушенных объектов и других единицах.

Необходимо обратить внимание, что шкала не обязательно должна быть линейной. Она может быть показательной, или деления шкалы могут изменяться нерегулярно.

Сначала составляют абсолютные шкалы для различных типов последствий, а затем формируют объединенную абсолютную шкалу, поместив их рядом друг с другом (см. рисунок 7). Такой подход исключает необходимость сопоставления потерь различных типов друг с другом (например, гибель людей с финансовыми потерями).

Преимуществом этого этапа является то, что он позволяет проверить последовательность выводов и заключений, сделанных в процессе оценки риска. В результате часть решений может быть изменена.

Финансовые потери	
5	Более 5 млн. руб.
4	От 4 до 5 млн. руб.
3	От 3 до 4 млн. руб.
2	От 2 до 3 млн. руб.
1	Менее 2 млн. руб.

Человеческие жертвы	
5	Гибель более 6 чел.
4	Гибель от 1 до 5 чел.
3	Травмы получили более 100 чел.
2	Гибель от 50 до 100 чел.
1	Гибель менее 50 чел.

Потери имущества	
5	Разрушено здание
4	Разрушено помещение администрации и 5 подразделений
3	Разрушено помещение администрации и 3 подразделения
2	Администрация не работает
1	Не работает одно подразделение

5 Потери более 5 млн. руб.
Гибель более 6 чел.
Разрушено здание

4 Потери от 4 до 5 млн. руб.
Гибель от 1 до 5 чел.
Разрушение помещений администрации и пяти подразделений

3 Потери от 3 до 4 млн. руб.
Более 100 чел. получили травмы
Разрушение помещений администрации и трех подразделений

2 Потери от 2 до 3 млн. руб.
От 50 до 99 чел. получили травмы
Администрация не работает

1 Потери менее 2 млн. руб.
Менее 50 чел. получили травмы
Не работает одно подразделение

Рисунок 7 — Абсолютная шкала последствий

5.8 Заключительные этапы

Оценка риска включает идентификацию опасностей и оценку слабых мест менеджмента риска. Оставшиеся два этапа включают в себя разработку и внедрение контрмер на основе оценки риска и анализа эффективности контрмер. Перечень предположений, сделанных на этапе оценки риска, особенно полезен на данном этапе.

На основе анализа матрицы риска видно, что под воздействием контрмер опасные события перемещаются вниз и влево.

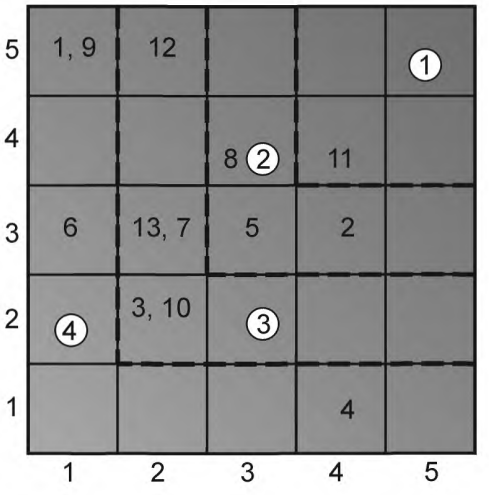
При работе с относительными величинами обнаружить снижение вероятности и/или последствий сложнее. Использование абсолютной шкалы в значимых для принятия решений единицах измерения (например, сокращения предполагаемых абсолютных затрат) повышает возможность выявления способов снижения риска.

6 Анализ оценки риска на уровне организации

В данном разделе показана оценка риска на уровне организации на основе примера заполнения таблицы сценариев опасных событий (см. таблицу 8), таблицы оценки риска (см. таблицу 9) и матрицы риска (см. рисунок 8).

Таблица 8 — Сценарии опасных событий

№ опасного события	Сценарий опасного события
1	Сотрудник приносит в здание бомбу и она взрывается
2	Сотрудник передает информацию третьему лицу (мошенничество)
3	Сотрудник вводит вирус в ИТ-систему
4	Сотрудник, действующий в одиночку, переводит небольшое количество денежных средств (менее 10 000 руб.) на несанкционированный счет
5	Сотрудник помогает третьему лицу получить доступ к значимой для организации информации с устройства ключевых логгеров
6	Сотрудник совершает нападение на персонал с ножом
7	Сотрудник раскрывает результаты деятельности организации на конец года раньше срока (в прессе)
8	Сотрудник передает информацию человеку, связанному с экстремистской организацией или организованной преступностью
9	Сотрудник способствует третьему лицу в преступных посягательствах или проникновению в здание (с бомбой)
10	Сотрудник выполняет нападение на ИТ-систему с целью нарушения обслуживания пользователей
11	Сотрудник раскрывает информацию о системе обеспечения безопасности и, таким образом, помогает краже
12	Сотрудник привозит бомбу на подземную автостоянку организации
13	Группа сотрудников (2 или более человек) участвуют в тайном сговоре о проведении незаконной выплаты



① — область наивысшего риска (риск 1)

Рисунок 8 — Матрица риска, соответствующая таблице 8

Таблица 9 — Таблица оценки риска

№ опасного события	Сценарий опасного события	Вероятность 1—5	Предположения относительно вероятности	Последствия 1—5	Предположения относительно последствий	Категория риска
1	Сотрудник проносит бомбу в здание и она взрывается	1	Проводят выборочные досмотры сумок	5	Менее 50 случаев гибели людей	4
2	Сотрудник передает информацию третьему лицу (мошенничество)	4	- Информация прошла и включает данные о кредитной карте, банковском счете и другой информации для постоянных клиентов; - У большого количества сотрудников есть такая возможность	3	- Участие в крупном мошенничестве (потеря более 100 000 руб.); - Снижение репутации вследствие большого количества пострадавших клиентов	2
3	Сотрудник вводит вирус в ИТ-систему	2	- Действуют механизмы защиты от вирусов; - Чтобы обойти защиту от вирусов необходимы права системного администратора	2	- Повреждение данных; - Нарушение работы ИТ-системы в течение 24 часов; - Функции ИТ-системы нарушены; - Некоторое снижение репутации организации; - Резервное копирование системы исправно	3
4	Сотрудник (действуя в одиночку) переводит небольшое количество денежных средств (менее 10 000 руб) на несанкционированный счет	4	- Методы авторизации не применяются; - У многих сотрудников есть такая возможность	1	Потеря менее 10 000 руб.	4
5	Сотрудник помогает третьему лицу получить доступ к значимой информации с устройства ключевых логгеров	3	- Низкая бдительность (недостаток средств контроля доступа); - Существенная угроза коммерческого шпионажа	3	Существенная потеря репутации организации	2
6	Сотрудник совершает нападение на персонал с ножом	1	- Ранее эта опасность была только внешней (не со стороны сотрудников); - Выборочные досмотры сумок	3	Менее пяти человек получили ранение	4
7	Сотрудник раскрывает результаты деятельности организации на конец года раньше срока (в прессе)	2	- Ограниченный персонал знает информацию; - Ограниченный прецедент (происходит один раз в течение нескольких лет)	3	- Существенная потеря репутации организации; - Падение на бирже стоимости акции (не продолжительное)	3
8	Сотрудник передает информацию человеку, связанному с экстремистской организацией или организованной преступностью	3	- Сотрудник не знаком со спецификой и не осознает последствия раскрытия информации	4	- Конфиденциальная информация открыта для прессы; - Возможен существенный отток постоянных клиентов; - Репутация организации существенно подорвана	2

Окончание таблицы 9

№ опасного события	Сценарий опасного события	Вероятность 1—5	Предположения относительно вероятности	Последствия 1—5	Предположения относительно последствий	Категория риска
9	Сотрудник помогает третьему лицу в преступных посягательствах или войти в здание (принести бомбу)	1	- Некоторые люди имеют намерение сделать взрывное устройство; - Нет прецедентов	5	- То же, что в случае, когда сотрудник приносит в здание самодельное взрывное устройство; - Погибших менее 50 чел.	4
10	Сотрудник выполняет нападение на ИТ-систему с целью нарушения обслуживания пользователей	2	- Недостаток технических знаний; - Ранее внешняя угроза; - Доступность технической информации позволяет это выполнить; - Имеется резервное копирование информации	2	- Нарушение системы в течение 24 часов; - Отрицательные последствия для репутации организации; - Минимальная потеря клиентов; - Потеря доверия потребителей	3
11	Сотрудник раскрывает информацию о системе безопасности и таким образом помогает краже	4	- Имеются прецеденты; - Имеются явные свидетельства опасности; - Это просто сделать	4	- Потери в сумме более 1000 000 рублей; - Нет пострадавших; - Высокая потеря репутации	1
12	Сотрудник привозит бомбу на подземную автостоянку организации	2	- Доступность автостоянки; - Выборочные проверки транспортных средств; - Процедуры проверок неэффективны	5	- Количество раненых и убитых менее 200 человек; - Повреждение здания, не позволяющее использовать его продолжительное время, возможное перемещение персонала	3
13	Группа сотрудников (2 или более человек) участвуют в тайном сговоре о проведении незаконной оплаты	2	Для выполнения требуется двойная авторизация	3	Потери в сумме более 100 000 руб.; Существенная потеря репутации организации	3

7 Оценка риска на уровне группы

Оценка риска на уровне группы позволяет получить существенно больше сведений о риске организации со стороны воздействия человеческого фактора. В частности, она позволяет определить контрмеры, которые должны быть применены к отдельным руководителям или сотрудникам.

В качестве исходной информации используют результаты оценки риска на уровне организации. При этом особое внимание уделяют группам сотрудников, имеющих возможность выполнить опасные действия и имеющих доступ к активам организации, в том числе к информации, материалам, системам, зданию и персоналу.

Оценку риска на уровне группы должна выполнять команда, включающая специалистов в области человеческих ресурсов, руководителей службы безопасности и других необходимых экспертов.

Результаты оценки риска на уровне группы должны быть зафиксированы в таблице. Форма таблицы приведена в таблице 10.

Таблица 10 — Форма таблицы оценки риска на уровне группы

Опасности со стороны посвященного лица в порядке убывания их последствий	Группа высоких возможностей	Причины	Доступ	Опасности	Контрмеры		
					существующие	существующие меры достаточны?	новые

Таблицу заполняют последовательно в соответствии с этапами оценки риска.

7.1 Этап 1. Идентификация и ранжирование опасностей со стороны посвященного лица

Пример заполнения таблицы 10 на этапе 1 показан в таблице11.

Таблица 11 — Пример заполнения таблицы 10 на этапе 1

Этап 1	Этап 2	Этап 3	Этап 4	
Опасности со стороны посвященного лица в порядке убывания их последствий				
Сотрудник раскрывает конфиденциальную информацию				

Оценка должна начинаться с идентификации и ранжирования опасностей со стороны посвященного лица и перечисления их в первой колонке таблицы.

7.2 Этап 2. Выполнение начальной идентификации групп с большими возможностями

Пример заполнения таблицы 10 на этапе 2 показан в таблице12.

Таблица 12 — Пример заполнения таблицы 10 на этапе 2

Этап 1	Этап 2	Этап 3	Этап 4	
Опасности со стороны посвященного лица в порядке убывания их последствий	Группа сотрудников с большими возможностями			
Сотрудник раскрывает конфиденциальную информацию	Старшие менеджеры			
	Системные администраторы			

Цель этого этапа состоит в идентификации сотрудников, на которых должна сконцентрироваться оценка риска. Оценку необходимо проводить достаточно быстро; более детальная оценка будет выполнена на последующих этапах.

Необходимо рассмотреть каждую опасность и определить, какие группы сотрудников обладают большей возможностью реализации этой опасности. Выводы следует основывать на:

1) Степени доступа сотрудников к активам в соответствии с рассматриваемой опасностью.

2) Уязвимости окружающей среды по отношению к опасным действиям сотрудника.

Возможности реализации опасностей для групп сотрудников до некоторой степени связаны с обязанностями сотрудников в организации. Например, если рассматриваемая опасность связана с ИТ-системами, то одной из групп с высокими возможностями реализации опасности являются администраторы ИТ-систем. Однако в некоторых группах нет корреляции с непосредственными служебными обязанностями сотрудников, поэтому важно рассмотреть обязанности всех сотрудников группы.

Результаты определения групп с наибольшими возможностями следует записать в таблицу оценки риска.

Полезно обратить внимание на численность группы. Если группа является очень многочисленной, это может означать, что в организации имеется помещение или место, обеспечивающее возможность реализации опасного события.

Численность группы может повлиять на вероятность опасного события, определенную при оценке риска на уровне организации. Например, вероятность того, что посвященное лицо повредит главную

базу данных, может быть увеличена, если возможность такого акта имеется у большой группы сотрудников. В этом случае следует исправить матрицу риска.

Численность группы может также повлиять на последствия опасного события. Например, кража сотрудником ноутбука оказывает слабое влияние на работу организации, но многочисленные кражи могут привести к значительным последствиям. В этом случае необходимо повторно рассмотреть оценку риска на уровне организации и определить необходимость внесения изменений в матрицу риска. Изменение последствий может привести к необходимости пересмотра контрмер.

7.3 Этап 3. Описание возможностей реализации опасного события

Пример заполнения таблицы 10 на этапе 3 показан в таблице13.

Таблица 13 — Пример заполнения таблицы 10 на этапе 3

Этап 1	Этап 2	Этап 3	Этап 4	
Опасности со стороны посвященного лица в порядке убывания их последствий	Группа сотрудников с большими возможностями	Возможности		
Сотрудник раскрывает конфиденциальную информацию	Старшие менеджеры	Старшие менеджеры имеют доступ к большому объему конфиденциальной информации		
	Системные администраторы	Системные администраторы могут получить несанкционированный доступ, используя навыки работы с ИТ-системой		

В колонке «Возможности», записывают факторы, обеспечивающие группам сотрудников высокий уровень возможностей реализации опасности. Эти возможности должны быть рассмотрены на этапе 3 и зафиксированы в таблице.

Указанные на данном этапе причины помогают определению необходимых контрмер, поэтому важно указывать достаточное количество деталей.

7.4 Этап 4. Шкала возможностей

Пример заполнения таблицы 10 на этапе 4 показан в таблице14.

Таблица 14 — Пример заполнения таблицы 10 на этапе 4

Этап 1	Этап 2	Этап 3	Этап 4	
			Доступ	Уязвимость
Опасности со стороны посвященного лица в порядке убывания их последствий	Группа с большими возможностями	Возможности		
Сотрудник раскрывает конфиденциальную информацию	Старшие менеджеры	Старшие менеджеры имеют доступ к большому объему конфиденциальной информации	B	B
	Системные администраторы	Системные администраторы могут получить несанкционированный доступ, используя навыки работы с ИТ-системой	C	C
Примечание — B — высокий/высокая; C — средний/средняя.				

На данном этапе доступ и уязвимость оценивают более системно и используют стандартизованные шкалы для сопоставления. Шкалы затем используют для определения общей меры возможности реализации опасности.

При рассмотрении доступа следует определить степень доступа сотрудников (имеющуюся или возможную) к определенным активам. Для этого может быть использована следующая шкала доступа В, С, Н (см. таблицу 15).

Таблица 15 — Шкала доступа В, С, Н

Шкала доступа (В, С, Н)	Определение
Высокий (В)	Регулярный доступ, предусмотренный функциональными обязанностями
Средний (С)	Возможен доступ в определенных ситуациях
Низкий (Н)	Несанкционированный доступ

Для оценки уязвимости следует использовать таблицу оценки уязвимости. Рекомендуется оценивать уязвимость рабочего места как высокую, среднюю, низкую.

На данном этапе группы сотрудников необходимо оценить относительно доступа к активам организации. Затем необходимо объединить полученные данные и сформировать общую меру возможностей в баллах от 1 до 5.

Необходимо определить как перевести доступ и уязвимость в возможности. Для этого можно построить матрицу (см. рисунок 9) и затем решить, как разместить числа 1, 2, 3, 4, и 5 на основе комбинаций доступа и уязвимости. Матрица на рисунке 9 представляет одну из возможных схем оценки возможностей.

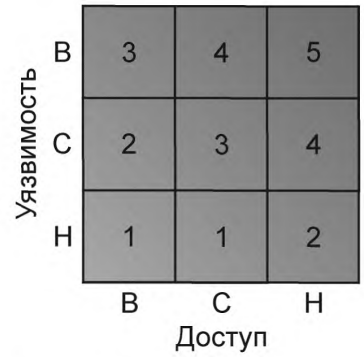


Рисунок 9 — Матрица возможностей

Оценку возможностей, соответствующую каждой комбинации доступа и уязвимости, указывают в каждой клетке матрицы.

Матрица возможностей помогает оценить сотрудника с точки зрения его возможностей реализации опасности (см. рисунок 10).

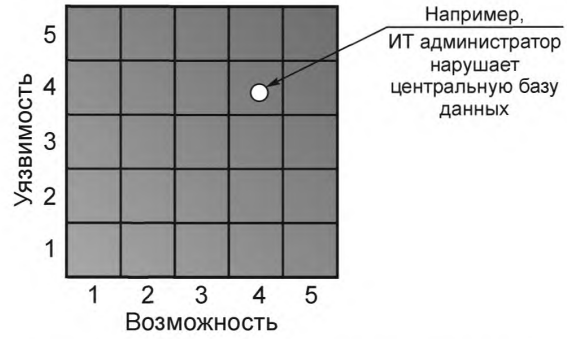


Рисунок 10 — Матрица возможностей и уязвимости

7.5 Этап 5. Анализ контрмер

Пример заполнения таблицы 10 на этапе 5 показан в таблице16.

Таблица 16

Этап 1	Этап 2	Этап 3	Этап 5		
Опасность	Группа сотрудников с высокими вероятностями		Контрмеры		
			Существующие	Существующие меры достаточны?	Новые
Персонал раскрывает коммерчески важную/ конфиденциальную информацию	Старшие менеджеры		- Соглашения о конфиденциальности; - Защитная маркировка; - Пронумерованные копии	- Брандмауэр не обнаруживает передачу документов с защитной маркировкой; - Служба безопасности реже проводит досмотр сумок старших менеджеров	- Настройка брэндмауэра на блокирование документов с защитной маркировкой; - Контроль выполнения досмотра сумок персонала
	Системные администраторы		Проверка компьютерной техники	- Система компьютерной проверки обнаруживает, но не предотвращает несанкционированный доступ	- Внедрение системы сигнализации и предупреждения для оповещения о неправомерном доступе

Как и в случае оценки риска организации, необходимо начать с перечисления в столбце «Существующие» всех существующих контрмер, которые помогают предотвратить реализацию рассматриваемой угрозы.

Затем необходимо рассмотреть каждую контрмеру и определить ее достаточность. Если угроза определена как «Посвященное лицо вводит вирус в основную компьютерную систему» и группой с наибольшей вероятностью являются сотрудники агентства информационных технологий, то существующие контрмеры могут включать проверку благонадежности перед приемом на работу, которая оговорена в контракте между организацией и агентством информационных технологий. Но без контроля выполнения таких проверок маловероятно, что наличие контракта будет достаточной контрмерой.

В столбце «Существующие меры достаточны?» необходимо указать недостатки и пробелы в контрмерах, а в столбце «Новые» указать действия, необходимые для их устранения.

Затем необходимо рассмотреть все перечисленные контрмеры применительно к группе с самой высокой вероятностью и решить, достаточны ли они для ограничения возможности реализации опасности и поддержания риска на допустимом уровне. Следует записать все сомнения в столбце «Существующие меры достаточны?» и затем использовать знания группы и, при необходимости, консультации экспертов по применению новых контрмер. Новые контрмеры перечисляют в столбце «Новые».

После определения групп с высокой вероятностью реализации опасностей с рангом риска 1 и рассмотрения контрмер в каждом случае следует повторить процедуру для всех остальных опасностей с другими рангами риска.

Если времени для выполнения оценки риска не достаточно, можно принять решение об анализе опасностей только с наиболее высоким рангом риска. Важно помнить, что могут существовать факторы, которые проявятся только во время оценки риска на уровне группы, например, фактор большого размера группы.

7.6 Примеры оценки риска на уровне группы:

7.6.1 Оценка возможностей посвященных лиц, выбранных для оценки риска

В таблице 17 приведены примеры опасностей со стороны посвященных лиц, которым соответствует наиболее значимый риск для организации.

Таблица 17

Опасность со стороны посвященного лица	Ранг риска	Какие группы обладают высокими возможностями реализации опасного события?	Причины	Доступ (В, С, Н)	Уязвимость (В, С, Н)
Сотрудник раскрывает конфиденциальную информацию	1	Сотрудники службы безопасности	- Сотрудники размещены таким образом, что могут идентифицировать уязвимые места для несанкционированных действий	В	С
		Сотрудники службы безопасности (охрана)	- Сотрудники размещены таким образом, что могут идентифицировать уязвимые места для несанкционированных действий	С	С
Сотрудник показывает результаты деятельности организации на конец года раньше срока	3	Высшее руководство	- Доступ к информации ограниченного распространения; - Существующие контакты в СМИ	В	С
		Отдел печати (внутренний/внешний)	- Доступ к информации ограниченного распространения	В	В
Сотрудник совершает атаку на ИТ-систему	3	ИТ-персонал; Бывший ИТ-персонал за прошедшие два года	- Наличие у сотрудников навыков и возможностей для реализации угрозы; - Знание системы; - Знание уязвимостей системы	С	Н
Сотрудник вводит вирус в информационную систему	3	ИТ-персонал (с надлежащим доступом и правами администратора); ИТ-подрядчики; Бывший ИТ-персонал за прошедшие два года	- Наличие у сотрудников навыков и возможностей для реализации угрозы (их права администратора дают возможность приостановить защиту от вируса); - Знание уязвимостей системы	В	С
Сотрудник проносит бомбу в здание и она взрывается	4	У всех сотрудников есть такая возможность, но имеют большую возможность следующие сотрудники: подрядчики, ИТ-инженеры, обслуживающий персонал, клининговый персонал	- Злоумышленники действуют в нерабочее время, когда проверки безопасности не так часты; - Досмотр сумок производится выборочно	С	С
		Охранники	Существует возможность не соблюдать меры безопасности	С	В
Примечание — В — высокий/высокая; С — средний/средняя; Н — низкий/низкая					

7.6.2 Оценка контрмер

В таблице 18 приведен пример анализа контрмер для данных таблицы 17.

Таблица 18

Сценарий угрозы	Группа	Контрмеры		
		Существующие	Существующие меры достаточны?	Новые
Сотрудник раскрывает конфиденциальную информацию	Сотрудники службы безопасности	- Проверка сотрудников службы безопасности на наличие судимости; - применение технических средств контроля доступа; - сотрудники организации обладают различной культурой безопасности	Недостаточный контроль доступа к секретной информации	- Проведение тренинга по приобретению необходимых знаний; - проведение ротации персонала на ключевых постах обеспечения безопасности; - персонал организации должен оценить свою культуру безопасности
	Сотрудники службы безопасности (охрана)	- Проверка сотрудников службы безопасности на наличие судимости; - применение технических средств контроля доступа; - сотрудники организации обладают различной культурой безопасности		- Проведение тренинга по приобретению необходимых знаний; - проведение ротации персонала на ключевых постах обеспечения безопасности; - персонал организации должен оценить свою культуру безопасности
Сотрудник проносит бомбу в здание и она взрывается	Подрядчики, ИТ-инженеры, обслуживающий персонал, клининговый персонал	- Выборочный досмотр сумок (в дневное время); - редкие проверки подрядчиков	- Применение стандартов; - порядок проверок изменяется в зависимости от сигналов системы сигнализации; - недостаточная проверка подрядчиков	- Выборочный досмотр сумок (в ночное время); - технические средства обнаружения взрывчатых веществ; - ежегодные тренинги по безопасности; - проверка подрядчиков такая же, как проверка постоянного персонала с тем же уровнем доступа
	Охрана	Выборочный досмотр сумок (в дневное время)	- Применение стандартов; - порядок проверок изменяется в зависимости от сигналов системы сигнализации; - отдельные охранники находятся в дружеских отношениях и не проверяют друг друга	- Введение новой системы контроля охранников при выборочном досмотре сумок
Сотрудник раскрывает результаты работы организации на конец года в прессе раньше срока	Высшее руководство	- Документы пронумерованы и имеют ограниченное распространение; - проверка адресов электронной почты; - использование защитной маркировки; - политика «чистого стола» и принцип наличия «необходимых знаний»	Нет ограничений по распечатке электронных писем или их пересылке на внешний адрес	- Шифрование значимой и конфиденциальной информации для уменьшения риска ее передачи по электронной почте; - ограничение доступа нелояльных сотрудников к значимой и конфиденциальной информации;

Продолжение таблицы 18

Сценарий угрозы	Группа	Контрмеры		
		Существующие	Существующие меры достаточны?	Новые
				- продвижение эффективной культуры безопасности; - запрет на доступ в здание с камерой или мобильным телефоном
	Отдел печати	- Соглашения о конфиденциальности; - документы пронумерованы и имеют ограниченное распространение; - использование защитной маркировки; - политика «чистого стола» и принцип наличия «необходимого знания»	- Низкое соответствие политике «чистого стола»; - Нет ограничений по распечатке электронных писем или их пересылке на внешний адрес	- Обеспечение полного соответствия политике «чистого стола»; - усиление аспектов защиты от распечатки информации; - шифрование значимой и конфиденциальной информации для уменьшения риска ее передачи по электронной почте
Сотрудник совершает атаку на ИТ-систему[1)]	ИТ-персонал	- Наличие системы видеонаблюдения; - контроль и естественное наблюдение коллегами; - применение системы резервного копирования	- Система видеонаблюдения не охватывает некоторые ключевые места; - не проводится ежегодная оценка безопасности и отсутствует система информирования о проблемах и опасениях	- Внедрение правила нахождения сотрудника в серверной комнате с сопровождением; - предоставление системы, позволяющей сотрудникам сообщать о проблемах и опасениях, касающихся своих коллег
	Бывший ИТ-персонал	- Автоматическое удаление полномочий при возврате идентификационной карты сотрудника (ИД-карты)	- Каталог сотрудников не обновляется сразу, увеличивая потенциал для атак методами социальной инженерии	- Информирование штата сотрудников о необходимости повышенных мер безопасности в отношении бывших сотрудников; - автоматизация процесса удаления разрешений и допусков сотрудника из базы данных персонала, когда он возвращает свою ИД-карту
Сотрудник вводит вирус в информационную систему	ИТ-персонал (с надлежащим доступом и правами администратора)	- Применение антивирусного программного обеспечения; - политика проверки на вирусы; - система видеонаблюдений	- Антивирусное программное обеспечение может быть выключено сотрудником с правами администратора; - проверка является ретроспективной и не обеспечивает своевременное срабатывание системы сигнализации и предупреждение	- Требование подтверждающей авторизации на отключение или приостановку работы антивирусного программного обеспечения; - ограничение на использование коммуникационных устройств (например, накопителей с интерфейсом USB или DVD-дисков);

Окончание таблицы 18

Сценарий угрозы	Группа	Контрмеры		
		Существующие	Существующие меры достаточны?	Новые
				- наблюдение за информационными системами в реальном времени и предупреждение о подозрительных действиях
	ИТ-подрядчики (с правами администратора)	- Применение антивирусного программного обеспечения; - политика проверки на вирусы; - система видеонаблюдений	- ИТ-подрядчиков иногда принимают в штат до завершения их проверки; - антивирусное программное обеспечение может быть выключено сотрудником с правами администратора; - проверка является ретроспективной и не обеспечивает своевременное срабатывание системы сигнализации и предупреждение	- Обеспечение постоянного сопровождения любого ИТ-подрядчика, принятого до завершения его проверки; - требование подтверждающей авторизации на отключение или приостановку работы антивирусного программного обеспечения; - ограничение на использование коммуникационных устройств (например, накопителей с интерфейсом USB или DVD-дисков); - наблюдение за информационными системами в реальном времени и предупреждение о подозрительных действиях

[1] Атака с целью нарушения нормального обслуживания пользователей.

7.6.3 Оценка риска опасностей со стороны персонала

Подход оценки риска на уровне группы начинается с рассмотрения опасностей для организации со стороны персонала и подрядчика. При этом рассматривают возможности сотрудников различных профессий и должностей. Главным преимуществом такого подхода является то, что контрмеры могут быть применены к сотрудникам определенной профессии. Однако этот подход включает качественную оценку риска и не позволяет количественно определить риск со стороны сотрудников определенной профессии.

Вместе или вместо такого подхода можно использовать количественный подход. Для этого производят подсчет возможностей для реализации опасного события сотрудниками, занимающими определенную должность, и последствий этого события. Путем объединения этих результатов можно оценить общий уровень риска со стороны сотрудников с определенной должностью. Преимуществом такого подхода является то, что должности могут быть расположены в соответствии с этими результатами, а контрмеры — соотнесены с допустимыми значениями. Например, может быть принято решение, что для сотрудника любой должности, которая находится в первой десятке по возможности осуществления угроз, проводится проверка на наличие правонарушений в прошлом.

На практике часто считают, что такой подход обеспечивает простое правило принятия решений. Однако у этого подхода существует два недостатка:

1) Он не способствует детальному рассмотрению опасностей и способов их реализации сотрудниками с различными должностями. Обычно рассматривают обоснованные наихудшие последствия действий сотрудников с определенными должностями. Например, можно предположить, что обоснован-

ной наихудшей опасностью со стороны бухгалтера, является мошенничество, а возможность бухгалтера совершить, например, физическое нападение, не рассматривают. Распределение контрмер с использованием такого подхода является менее точным и всесторонним.

2) Для того чтобы подсчитать вероятность и последствия, необходимо разработать числовые шкалы, учитывающие диапазон должностных обязанностей и возможных опасностей, что является сложной задачей.

8 Оценка риска со стороны отдельных сотрудников

На индивидуальном уровне выполняют анализ возможностей (т. е. преступных намерений и склонности к их выполнению) отдельных сотрудников, а также определяют вероятности осуществления ими определенных действий. Индивидуальный риск является сочетанием этих оценок, поэтому высокая оценка основывается на высокой вероятности и высоких возможностях сотрудника.

Процесс оценки риска на этом уровне требует существенно больших затрат ресурсов чем оценка на уровне организации или группы. Также технически очень трудно достоверно оценить намерения и склонности людей. Поэтому лишь небольшое количество организаций использует этот подход. Некоторые организации используют оценку со стороны отдельных сотрудников для небольшой части персонала, входящего в группу (или группы) с самым высоким уровнем риска, выявленную с помощью оценки риска на уровне группы.

Приложение А
(справочное)

Перечень опасностей со стороны посвященного лица

Данный перечень не является исчерпывающим, но может быть полезен при анализе опасностей для организации.

ДОСТУП К ИНФОРМАЦИИ

Хищение информации / интеллектуальной собственности

Раскрытие опасной для организации информации. Раскрытие конфиденциальной информации для партнеров или заинтересованных сторон. Раскрытие конфиденциальной информации обществу

Искажение существующих данных

Повреждение данных организации; фальсификация данных организации; уничтожение/перемещение данных

Неправильное использование информации

Распространение информации среди несанкционированных пользователей внутри/вне организации

ДОСТУП К ИТ-СИСТЕМАМ

Хищение элементов

Хищение используемых ИТ-систем и представление возможностей пользования ими заинтересованным сторонам

Раскрытие источника информации

Раскрытие конфиденциальных источников информации заинтересованными сторонами

Взлом ИТ-системы

Взлом ИТ-системы для копирования информации, ее дальнейшего использования хакерами, в том числе для контроля использования ИТ-систем

Вредительство в отношении существующих систем/данных

Вредительство в отношении существующих систем – разрушение систем, например, разрушение с помощью внедрения вируса

Вредительство в отношении существующих данных — фальсификация данных

Вредительство в отношении существующих данных — разрушение/удаление данных

Размещение «жучков» в телефонной системе

Использование «жучков» для контроля телефонной сети

Использование «жучков» для прослушивания телефонных переговоров

Злоупотребления ИТ-системами

Облегченный доступ третьей стороне к ИТ-системам (записи предполагаемых последствий в колонке «предположения относительно последствий»)

Доступность будущих систем и разработок

Доступность будущих систем и разработок — разрушение/повреждение будущих систем и разработок

Доступность будущих систем и разработок — разрушение доступа к будущим системам и разработкам, раскрытие доступа определенным сторонам

ДОСТУП К САЙТАМ, ЗДАНИЯМ, МАТЕРИАЛАМ И МЕХАНИЧЕСКИМ СИСТЕМАМ

Облегченный доступ третьей стороне в здание

Облегченный доступ третьей стороне в здание, например, через пожарные выходы (записи предположений в колонке «предположения относительно последствий»)

Фальсификация действий службы безопасности

Сообщение о действиях службы безопасности другим сторонам

Облегчение доступа к информации третьей стороне

Облегчение доступа к информации третьей стороне (записи предположений в колонке «предположения относительно последствий»)

Хищение товаров/материалов

Хищение /распространение опасных материалов (например, радиоактивных материалов или оружия)

Хищение /распространение не опасных материалов (например, паспортов, водительских прав, документов о судимости, удостоверений и др.

Вредительство в отношении товаров/материалов/здания

Вредительство в отношении объектов доступа — повреждение складов для создания дефицита, нарушение рабочих инструкций для нарушения функционирования складов; вредительство в отношении объектов; вредительство в отношении пищи и воды; повреждение лифтов, эскалаторов, подъемников, приводящее к человеческим жертвам; повреждение почтовой системы, нарушающее рабочий процесс

Раскрытие информации о недвижимости и системе безопасности

Раскрытие информации о здании, например, о его уязвимых местах (заинтересованным сторонам)

Раскрытие информации об имеющихся системах средств защиты, видов охраны режимов и мерах безопасности

Передача информации об имеющихся системах и мерах безопасности заинтересованным сторонам

Прямая атака на здание (например, взрыв)

Прямая атака на механические системы

Физическое разрушение систем/файлов

Физическое разрушение систем (например, центра ИТ)

Физическое разрушение файлов (например, сжигание)

Доступ к разработанным/разрабатываемым технологиям

Доступ к разработанным/разрабатываемым технологиям - уничтожение

Доступ к разработанным/разрабатываемым технологиям - саботаж

Доступ к разработанным/разрабатываемым технологиям — раскрытие информации для общества

Использование записывающих устройств

Введение и использование записывающих устройств/сканеров/устройств незаконного подключения к международной телефонной системе, разглашение информации

ДОСТУП К ПЕРСОНАЛУ

Раскрытие конфиденциальной информации

Раскрытие общественности и заинтересованным сторонам информации, собранной в процессе неофициальных бесед и личных встреч

Склонение людей к сбору и передаче информации

Установление взаимоотношений с целью приобретения сведений (долгосрочных) об известных людях за взятки

Вербовка — коммерческий шпионаж — нападения/угрозы людям/группам сотрудников

Физическое нападение на отдельных сотрудников

Физическое нападение на группы сотрудников

Проведение массового нападения на сотрудников с нанесением травм и ранений

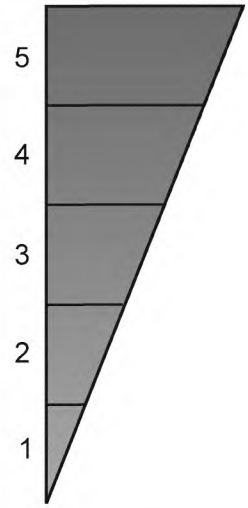
Оскорбление свободы личности / группы людей (например, взятие заложников)

Угрозы персоналу

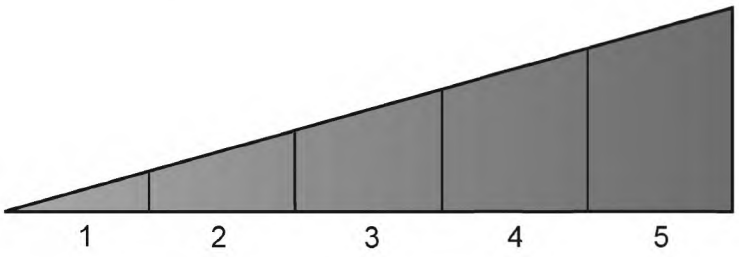
Приложение Б
(справочное)

Диаграммы, рекомендуемые для использования при проведении анализа риска

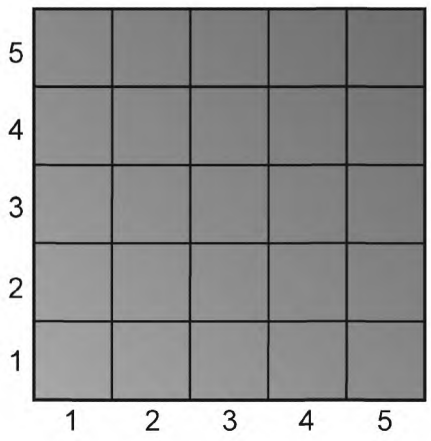
При проведении анализа риска рекомендуется использовать диаграммы, приведенные на рисунке Б1. Их можно копировать, увеличивать и использовать на заседаниях мозгового штурма.



А — Диаграмма последствий опасного события



Б — Диаграмма оценки вероятности опасного события



С — Матрица риска

Рисунок Б.1 — Диаграммы, рекомендуемые для использования при проведении анализа риска

УДК 658.562.012.7:65.012.122:006.354 ОКС 03.120.30 Т59

Ключевые слова: персонал, человеческий фактор, опасности, последствия, риск, анализ риска, оценка риска, инцидент, контрмеры, менеджмент риска, абсолютная шкала

Редактор *С.Д. Золотова*
Технический редактор *В.Н. Прусакова*
Корректор *Ю.М. Прокофьева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 20.03.2015. Подписано в печать 08.04.2015. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,35. Тираж 100 экз. Зак. 1532.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru