РИСК-МЕНЕДЖМЕНТ ПО ТРЕБОВАНИЯМ МЕЖДУНАРОДНОГО СТАНДАРТА ISO/IEC 27001. ОДИН ИЗ СПОСОБОВ УВИДЕТЬ БУДУЩЕЕ БЕЗ МАШИНЫ ВРЕМЕНИ

Дмитриев Александр Анатольевич
Учредитель, главный редактор
журнала "Das Management",
ведущий аудитор ISO 9001, ISO/IEC 27001, BS 25999

Все без исключения современные системы менеджмента, связанные с вопросами безопасности, основываются на риск-менеджменте. Среди наиболее известных: система управления охраной труда и здоровьем (OHSAS 18001), система экологического менеджмента (ISO 14001), система управления непрерывностью бизнеса (BS 25999), а также система управления информационной безопасностью (ISO/IEC 27001).

Риск-менеджмент – это инструмент, который позволяет:
- предвидеть негативные явления;
- основывать свое предвидение на фактах.

Для выбора того или иного инструмента менеджмента важно понимать выгоды его применения. Выгоды риск-менеджмента можно кратко выразить следующим образом:
- сокращение затрат на обеспечение производства в среднесрочной и долгосрочной перспективе;
- сокращение стоимости потерь на восстановление активов;
- готовность к сбоям в работе предприятия и его отдельных процессов;
- повышения рейтинга надежности предприятия.

Решение вопросов безопасности (экологической, информационной и др.) связано с тем, что мы, будучи разумными людьми, понимаем то, что рано или поздно возникнут проблемные ситуации в том или ином процессе на предприятии. Дальновидный менеджер всегда имеет желание предотвратить негативные ситуации, которые могут возникнуть на предприятии. Примерами таких ситуаций могут служить: пожар на складе, выход из строя критичного оборудования, получение производственной травмы, несвоевременная поставка запчастей, отсутствие работника по причине болезни, авария на электрической подстанции, резкое падение спроса на продукцию, резкое увеличение стоимости ресурсов и др. Из примеров видно, что проблемы взяты из реальной жизни. Регулярно на каждом крупном предприятии происходят крупные и мелкие проблемы. Для тех, кто хочет управлять этими проблемами, разработан весьма подходящий инструмент – риск-менеджмент. Отходя от словарных фраз, необходимо пояснить, что означает «управлять проблемами». Управлять проблемами, которые могут произойти в будущем, это значит:
- знать эти проблемы, т.е. иметь четкий их перечень, и понимать степень важности каждой проблемы, расставить их в порядке убывания с точки зрения серьезности проблемы;
- разработать и выполнить мероприятия по предупреждению наиболее серьезных проблем;
- проверить результативность предпринятых действий, т.е. убедиться в том, что выбранные меры действительно помогают;
- оценить всю проделанную работу с точки зрения внесения улучшений в перечень проблем, в выбор подходящих мер по предупреждению проблем, в проверку результативности мер.

Данные четыре пункта четко следуют знаменитому циклу Демига: Планируй-Делай-Проверяй-Воздействуй. Весь процесс риск-менеджмента можно представить в виде следующих шести шагов.

ШАГ 1. Описание актива

Начало работы риск-менеджера состоит в том, чтобы определить важные для бизнеса активы. Под понятием «актив» в данном случае стоит понимать все, что имеет ценность для предприятия. Это может быть все, что вы посчитаете важным для работы бизнеса. Например токарный станок, здание цеха, шкаф, бумажный или электронный документ, деньги в любом виде и даже персонал. В зависимости от сферы применения риск-менеджмента необходимо выбрать определенную категорию активов. Специалисту по информационной безопасности достаточно ограничиться только информационными активами. Информационный актив – это материальный или нематериальный объект, который является информацией или содержит информацию, или необходим для обработки информации.

Первая практическая задача риск-менеджера – создать реестр активов. Проще говоря, реестр активов – это таблица, которая в полной мере отразит сущность активов. Для удовлетворения требований стандарта ISO/IEC 27001 необходимо описать активы, используя следующие атрибуты:

- Наименование актива.
Лучше использовать типичные (стандартные) наименования активов. Например «Персональный компьютер бухгалтерии № 12» можно задекларировать так: «ПК 12 тип Б». Это позволит Вам получить в результате простую и наглядную таблицу.

- Владелец актива.
Владельцем стоит назначать лицо, которое реально работает с активом и способно влиять на свойства и состояние актива.

- Местонахождения актива.
Местонахождение актива чаще всего определяют территориально согласно проекту здания, сооружения. Например: «Цех №1», «Бухгалтерия», «Кабинет №2».

- Категория актива.
Категорирование активов позволяет сгруппировать схожие активы и упростить работу с ними. Выбор категорий – дело индивидуальное. Например для информационной безопасности часто выбирают следующие категории: «Бумажные документы (БД)», «Электронные документы

(ЭД)», «Программное обеспечение (ПО)», «Компьютерная техника (КТ)», «Сетевое оборудование (СО)», «Вспомогательное оборудование (ВО)», «Персонал (П)», «Виртуальная информация (ВО)». Пример реестра информационных активов приведен в первом разделе Таблицы 1.

При подготовке реестра активов важно помнить «золотые» правила:

- **важно определять только по-настоящему важные для бизнеса активы; подробный список активов превратит риск-менеджмент в трудоемкий процесс, что в конечном итоге приведет к финансовым потерям бизнеса;**
- **важно группировать похожие и сложные активы. Например для информационной безопасности нормальным может быть определение в качестве одного актива следующего набора:** системный блок ПК + монитор + клавиатура + мышь + все электронные документы, размещенные на дисках ПК + все программное обеспечение, установленное на ПК.

Таблица 1

ШАГ 1. Описание актива				ШАГ 2. Описание риска	ШАГ 3. Первоначальная оценка риска		
Актив	Владелец	Место расположения	Категория актива		Вероятность	Ущерб	РИСК
Архив бумажных документов № 4	Зав. канцелярии	Кабинет № 15	БД	Потеря нескольких папок вследствие невнимательности персонала	7	7	**49**
				Недоступность актива вследствие потери ключа от архива	3	3	**9**
Персональный компьютер Тип "А" № 192	Главный бухгалтер	Кабинет № 27	КТ	Полная потеря информации вследствие выхода из строя жесткого диска	3	9	**27**
				Частичная потеря информации вследствие действия вирусов	7	5	**35**
Участок локальной сети Тип "В" № 15	Сис. админ.	Цех № 2	СО	Выход из строя вследствие действий третьих лиц	3	7	**21**
				Частичное повреждение вследствие случайного порыва кабеля	7	5	**35**

ШАГ 2. Описание риска

Следующий шаг нашей работы состоит в том, чтобы обозначить проблемы по каждому активу. В работе риск-менеджера принято называть возможные проблемы «рисками». Согласно определения, **риск** — это возможная опасность какого-либо неблагоприятного исхода.

Далее важно разобраться как правильно описать проблему (риск). Для этого необходимо понимать природу риска. Каждый риск можно описать одним предложением, в котором четко обозначена пара: «угроза» и «уязвимость» актива. Давайте разберемся с этими понятиями.

- Угроза. Для ее определения необходимо дать ответ на вопрос: «Что именно может случиться с активом?».
Рассмотрим примеры угроз. Возьмем для примера информационный актив – «архив с бумажной документацией №4» и дадим ему условный код «АБД №4». Угрозами в данном случае могут быть: полное уничтожение, частичное уничтожение, отсутствие доступа, неактуальность документации и др.
- Уязвимость. Ответим на вопрос: «По какой причине может возникнуть проблема?». Например, полное уничтожение актива может произойти по следующим причинам: пожар, залив водой, кража и др.

Теперь давайте посмотрим на примеры описания рисков для актива «АБД №4»:

- Риск 1. Полное уничтожение вследствие пожара
- Риск 2. Полное уничтожение вследствие кражи
- Риск 3. Частичное уничтожение вследствие халатности персонала
- Риск 4. Отсутствие доступа вследствие потеря ключа от помещения

Как видно из примеров для каждого актива может быть разное количество проблем. При желании можно поставить себе цель и описать по каждому активу 50-100 рисков. Но этого делать не следует. Рекомендуется определять только существенные риски, не стоит распыляться. В среднем для одного актива стоит определять 2-3 риска. Этого достаточно.

ШАГ 3. Первоначальная оценка риска

Для оценки риска удобно использовать простой и понятный метод расчета. Именно простота позволит адекватно оценить риски и при необходимости скорректировать их значение. Наиболее простой для расчета риска является следующая формула:

$$\text{Риск} = \underline{\text{Вероятность}} * \underline{\text{Ущерб}}$$

Как видно из формулы для расчета риска необходимо знать две переменные величины: вероятность и ущерб. Рассчитать вероятность или ущерб с помощью математического аппарата в предполагаемой негативной ситуации практически невозможно. Единственный разумный способ – метод экспертных оценок. Говоря другими словами, нам просто необходимо знать природу того или иного риска в условиях конкретного предприятия. Можно привлечь для этой работы таких специалистов, которые обладают необходимыми знаниями. Для снижения погрешности таких оценок лучше всего использовать методику выбора вариантов.

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ

Вероятность возникновения	Описание
Очень низкая	Маловероятно
Низкая	1 раз в 3 года
Средняя	1 раз в 1 год
Высокая	Несколько раз в год
Очень высокая	Раз в месяц и чаще

Определение вероятности возникновения угрозы для конкретного информационного актива. Предлагаемый вариант оценки вероятности является максимально простым и надежным:

ОПРЕДЕЛЕНИЕ УЩЕРБА

Определение ущерба, который может нанести конкретная угроза конкретному информационному активу. Оценить ущерб зачастую гораздо сложнее, чем вероятность. Существуют различные подходы по оценке ущерба. Наиболее понятный – оценка ущерба в денежном выражении. К сожалению не всегда и не все активы можно точно оценить в деньгах. Например, такой актив как имидж предприятия крайне сложно оценить. Поэтому распространенным подходом является табличная оценка. Один из возможных вариантов табличной оценки:

Потенциальный ущерб	Величина/серьезность ущерба
Низкий	Небольшие проблемы (величина ущерба до 100$)
Средний	Значительные проблемы (величина ущерба до 1000$) Негативная реакция клиентов, партнеров, инвесторов к предприятию
Высокий	Серьезные финансовые проблемы / убыточность предприятия (величина ущерба более 10000$) Формирование негативного отношения клиентов, партнеров, инвесторов к предприятию
Очень высокий	Может привести к банкротству Может привести к закрытию предприятия

На основании оценки ущерба и вероятности возникновения риска необходимо рассчитать значение (величину) риска, используя следующую таблицу.

Вероятность / Ущерб	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Низкий	**1**	**3**	**5**	**7**	**9**
Средний	**3**	**9**	**15**	**21**	**27**
Высокий	**5**	**15**	**25**	**35**	**45**
Очень высокий	**7**	**21**	**35**	**49**	**63**

Как мы убедились превратить описание риска в простую цифру достаточно несложно. Сложность заключается в объеме этой работы. Например: Вы определили 200 активов, описали по 3 риска к каждому активу – получили в результате 600 рисков. Работа специалиста или группы специалистов по оценке вероятности и ущерба может занять продолжительное время. Кроме того, сочетание творческой работы с монотонным выбором значения может привести к весьма неточным результатам. Поэтому крайне важно выполнить все советы и рекомендации, относящиеся к первому и второму ШАГу риск-менеджмента.

ШАГ 4. Определение целевого показателя и определение мер по обработке риска

Все предприятия живут в условиях ограниченности ресурсов. Искусство руководителя заключается в том, чтобы использовать имеющиеся ресурсы с максимальной отдачей. Риск-менеджмент является одним из инструментов, способным решать данную проблему. После третьего ШАГа риск-менеджмента мы уже четко видим степень важности той или иной проблемы. На первый взгляд все достаточно просто. Теперь можно решать все проблемы друг за другом, следуя по степени важности. Для большинства предприятий это нереально. Обработка рисков требует затрат определенных ресурсов, в т.ч. финансовых. На этом ШАГе мы должны определиться - сколько способно тратить предприятие на предупреждение негативных проблем.

Для этого необходимо проделать определенную циклическую работу. Эта работа заключается в экспериментальном подборе критерия приемлемости рисков. По требованиям стандарта ISO/IEC 27001 критерий должен быть определен. Учитывая то, что все риски к этому моменту мы выразили в цифрах, подбор критерия заключается в выборе одного численного значения. Значения рисков согласно таблицы расчета рисков лежат в диапазоне от 1 до 63. Нашим критерием, к примеру, может быть значение «25». Согласно терминам стандарта ISO/IEC 27001 данный критерий называется критерием приемлемости рисков. В этом случае критерий говорит нам о следующем:

Цветовая маркировка	Диапазон значений риска	Решение о дальнейшей обработке риска
Зеленый	**1-21**	Риски данной группы считаются незначительными для активов предприятия. Обработка рисков не требуется.
Желтый	**25-63**	Риски данной группы считаются значительными для активов предприятия. Меры по обработке рисков разрабатываются в обязательном порядке.

Основной вопрос заключается в выборе подходящем критерия для конкретного предприятия. Ниже приведен один из вариантов определения критерия, опробованный на практике.

Алгоритм определения критерия приемлемости рисков:

1	Выбрать значение критерия исходя из первостепенной важности обработки рисков. Необходимо проработать перечень рисков и отталкиваясь от реалий бизнеса, предположить определенное значение риска. В вышеуказанном примере мы выбрали значение «25».
2	Прописать конкретные меры по обработке рисков со значением «25» и выше. Перед выбором определенных мер необходимо знать, что для этого существует всего четыре варианта обработки риска: √ применение определенных мер для снижения (смягчения) риска; √ разумное и целевое принятие рисков, обеспечивающее их полное удовлетворение политикам организации и ее критериям принятия рисков; √ полное избегание рисков; √ перенос бизнес-рисков на другие стороны, например на страховщиков, поставщиков и пр. При определении мер обработки риска необходимо использовать всю широту возможных направлений, среди них: административные, учебные, технические и др. Это творческий процесс. Зачастую этот процесс не менее продолжительный, чем описание активов и описание рисков. Однако на практике элемент творчества возбуждает интерес к выполнению этой работы.
3	Прописать ресурсы, необходимые для реализации мер. После того, как меры будут определены, необходимо просчитать ресурсы для их реализации. В перечне ресурсов могут присутствовать финансовые средства, человеческие ресурсы, организационные работы и многое другое. Важно, чтобы описанные ресурсы были понятны для руководства.
4	Определить являются ли требуемые средства доступными на текущий период (как правило на один год). Этот ответ можно получить у первого руководителя либо у другого лица, принимающего решение о выделении ресурсов. На этом этапе будет видно следующее: - умение риск-менеджера представить запрос на выделение ресурсов в доступном, простом и понятном виде; - желание руководства по предупреждению возможных проблем предприятия; - величину желания, выраженную в конкретных деньгах и других ресурсах.
5	Если требуемые ресурсы получить не реально, риск-менеджер должен пройти еще раз по вышеуказанному алгоритму. При этом необходимо повысить критерий приемлемости рисков, например до значения «35». Далее необходимо пересчитать ресурсы исходя из того, что многие описанные меры уже будут вычеркнуты из списка. Далее опять на поклон к руководителю. И так до тех пор, пока не получите положительное решение по выделению ресурсов. Этот объем ресурсов является бюджетом риск-менеджера и дает возможность перейти от слов к делу.
6	Стандарт ISO/IEC 27001 требует документально оформить методику по оценке рисков и критерий приемлемости рисков. Лучше всего сделать эту работу в этот момент.
7	Создать два списка. Первый список включит в себя высокие риски, подлежащие обработке. Второй список будет содержать риски, которые мы обрабатывать не будем. Т.е. эти риски мы понимаем и принимаем как есть.
8	Перечень высоких рисков и мер по их обработке необходимо превратить в «План по обработке рисков». Для этого необходимо распределить ответственность за выполнение тех или иных мер, определить сроки их выполнения. Также может понадобиться детализировать мероприятия, чтобы они были понятны конкретным исполнителям. Есть смысл утвердить у руководителя «План по обработке рисков».
9	Перечень малых рисков нужно превратить в «Положение о принятии рисков». Этот документ по требованиям ISO/IEC 27001 должен быть подписан первым руководителем. И этот момент часто является проблемным. Некоторые руководители не имеют желание брать на себя дополнительную ответственность.
10	Реализовать план по обработке рисков. Риск-менеджер имеет право внести изменения в план по обработке рисков. В этом случае в плане документируются изменения, фиксируется версия и дата изменения в плане.

Таблица 2

ШАГ 1. Описание актива	ШАГ 2. Описание риска	ШАГ 3. Начальная оценка рисков	ШАГ 4. Критерий приемлемости рисков	ШАГ 4. Критерий приемлемости рисков		ШАГ 5. Повторная оценка рисков
				Меры	Ресурсы	
Архив бумажных документов № 4	Потеря нескольких папок вследствие невнимательности персонала	**49**	**35**	1. Разработка правил по работе с архивом. 2. Обучение персонала 3. Проведение регулярной инвентаризации документов	• 120$ • 8 ч/д работы зав. канцелярией	**21**
Персональный компьютер Тип "А" № 192	Полная потеря информации вследствие выхода из троя жесткого диска	**27**		---	---	**27**

ШАГ 5. Повторная оценка риска

Повторная оценка необходима для того, чтобы проверить результативность реализованных мероприятий. Этот этап также позволяет снизить погрешность, которая неизбежна при выборе мер путем мозгового штурма. Хотя при этом сама повторная оценка также проводится экспертным путем. Важно использовать одну и туже методику по расчету рисков, а также привлекать для оценки все тех же специалистов/экспертов. Это даст возможность получить сравнимые результаты. Не удивляйтесь, если выбранные, оплаченные и реализованные меры не изменят значения некоторых рисков. Это нормально. Каждый человек имеет право ошибаться. Эту ситуацию зачастую даже нельзя назвать ошибкой. Выбирая меры для обработки потенциальных проблем, приходится много предполагать и угадывать. Опытный и грамотный риск-менеджер будет ошибаться так же как новичок, но при этом процент ошибок будет значительно меньше. Поэтому процесс повторной оценки полезен и необходим по требованиям стандарта ISO/IEC 27001.

ШАГ 6. Пересмотр всего процесса риск-менеджмента

По истечению определенного времени необходимо пересмотреть все пять проделанных шагов с точки зрения их актуальности для сегодняшнего дня. ISO 27001 требует проведения пересмора минимум один раз в год. Также пересмотр обязателен в случае серьезных изменений в структуре бизнеса или возникновения серьезных неучтенных проблем. На этом этапе процесс риск-менеджмента замыкается в кольцо и работа начинается с первого ШАГа. Конечно же на этом этапе значительно меньше работы, т.к. вся работа будет заключатся в корректировке уже существующего реестра активов, реестра рисков и реестра мер по обработке риска. Также на этапе пересмотра зачастую пересматривают само значение критерия приемлемости риска, группу экспертов по оценке рисков, расставляют приоритеты в выборе мер.

Завершая данную статью хочется отметить важнейшие аспекты риск-менеджмента и дать определенные полезные рекомендации.

Прежде всего, не стоит искать сложные математические методики по расчету рисков. Математики в этом процессе к счастью, или к сожалению, очень мало. Настоятельно рекомендую это учесть.

Рабочий процесс риск-менеджмента держится на следующих китах:

- скрупулезное и точное ведение реестра активов;
- наличие знаний у специалистов, описывающих риски, о природе возникновения возможных рисков по отношению ко всем значимым активам предприятия;
- опыт и глубина знаний специалистов, которые на основании своих субъективных суждений опишут вероятность и ущерб для каждого риска;
- наличие калькулятора или таблицы Excel для расчета математического значения риска;
- логичное и оперативное выделение средств на обработку рисков согласно бюджета либо согласно реальным возможностям предприятия.

Среди всего вышеуказанного следует выделить две основных составляющих риск-менеджмента:

- адекватное руководство (работающее на перспективу);
- опытная и грамотная команда, поддерживающая процесс риск-менеджмента.

На сегодняшний день полезными для любого риск-менеджера могут оказаться следующие основополагающие нормы:

- ISO 31000. Риск-менеджмент. Принципы и руководство по внедрению.
- ISO/IEC Guide 73. Риск-менеджмент. Словарь.

Для риск-менеджера, работающего с вопросами информационной безопасности, могут быть также полезны следующие стандарты:

- NIST 800-30. Руководство по риск-менеджменту для информационных систем.
- BSI Standard 100-3. Риск-менеджмент на основе методики «ИТ-Грундшутц».

Для удобства читателя на интернет-сайте журнала Das Management размещена электронная таблица для управления рисками.