

Управление рисками

Часть 3. Выбор мер по обработке рисков

Это третья – заключительная – часть статьи посвящена вопросам выбора средств управления (controls) рисками.

После того, как риски выявлены и оценены (см. Часть 1 и 2 данной статьи), наступает время выбора мер для обработки этих рисков.

Подход стандарта ISO/IEC 17025:2017 в этом отношении кратко сформулирован во Введении:

Данный документ требует от лабораторий планировать и осуществлять мероприятия для обработки рисков и возможностей. Мероприятия, связанные с рисками и возможностями, служат основой для повышения результативности системы менеджмента, достижения более высоких результатов и предотвращения негативных последствий. Лаборатории несут ответственность за решение, в отношении каких рисков и возможностей должны предприниматься меры¹. [1, с. iv]

Здесь необходимо заметить, что стандарт, с одной стороны, требует «планировать и осуществлять мероприятия для обработки рисков и возможностей», но, с другой стороны не содержит требований документирования процесса оценки рисков и документирования результатов такой оценки. В примечании к п. 8.5.2 поясняется: «Несмотря на то, что в этом документе [имеется в виду ISO/IEC 17025:2017 – прим. автора] указывается, что организация планирует меры по обработке рисков, формальных методов управления рисками или документированного процесса управления рисками не требуется. Лаборатории могут сами решать, разрабатывать или нет более объемную методологию управления рисками, чем это требуется в настоящем документе, например, путем применения других руководств или стандартов».

В Таблице 1 приведены четыре основных стратегии по обработке рисков, которые могут быть применены к каждому из выделенных на предыдущем этапе риску.

Таблица 1 Стратегии обработки рисков

Стратегия	Описание
снижение риска	Предполагает принятие мер, которые снижают риск вплоть до полного его исключения. В рамках двухфакторной оценки это означает, что принимаемые меры либо уменьшают вероятность негативного события, либо уменьшают серьезность его последствий, либо и то, и другое одновременно. <i>Например, чтобы снизить риск кражи принятых к работе дорогостоящих средств измерения, лаборатория устанавливает сигнализацию.</i>
избегание риска	Предполагает отказ от совершения действий, несущих в себе риски. <i>Например, не располагая возможностями надежного хранения, лаборатория не берет в работу дорогостоящие средства измерения.</i>
принятие риска	В рамках этой стратегии риск осознается, но никаких мер не предпринимается. <i>Например, располагая возможностями надежного хранения, лаборатория не предпринимает никаких дополнительных мер по обеспечению сохранности дорогостоящих средств измерения.</i>
разделение риска	При выборе этой стратегии риск либо передается другой стороне, либо разделяется с ней. Характерный пример такой стратегии – страхование. <i>Например, лаборатория заключает договор страхования от кражи и повреждения для дорогостоящих средств измерения, принимаемых в работу.</i>

В Таблице 2 приведены типовые стратегии для различных категорий риска.

¹ Здесь и далее перевод автора

Таблица 2 Типовые стратегии

Уровень риска	Стратегия			
	Снижение риска	Избегание риска	Принятие риска	Разделение риска
низкий	✘	✘	✓	✘
средний	✓	○	○	✓
высокий	✓	✓	○	✓

	значение
✓	наиболее вероятная
✘	вряд ли целесообразная
○	возможная при условии

При использовании двухфакторного метода оценки в расчет берется вероятность события и серьезность негативных последствий, которые оно может вызвать в отношении рассматриваемой цели. Следовательно, те меры по управлению риском, которые мы предполагаем предпринять, должны влиять либо на вероятность, либо на серьезность последствий. Если при проверке предполагаемой меры невозможно указать на такого рода влияние, значит, мера выбрана неверно.

Рассмотрим это на примерах рисков приведенных в Табл. 2 второй части с использованием информации из Табл. 2 - 4 первой части статьи.

Допустим, у нас есть данные, что были случаи, когда средства измерения принимались в работу без соответствующей проверки, предусмотренной процедурой приема; используя критерии, приведенные в Табл. 2 первой части, мы оцениваем это событие как вероятное (3 балла). При этом последствия – на основании критериев из Табл. 3 – оцениваем как серьезные, т.е. тоже 3 балла.

Итоговая оценка такого риска составит $3 \times 3 = 9$ баллов, он попадает в категорию «средний риск» (если мы не очень склонны к риску и классифицируем риски так, как это приведено в Табл. 4А первой части). Таблица 2, приведенная выше, говорит о том, что для рисков среднего уровня типичными являются стратегии снижения и разделения. Мы полагаем, что риск значимый и в отношении него надо принимать меры по снижению.

Допустим, руководство решает ввести серьезные финансовые наказания для сотрудника, принимавшего средство измерения с нарушением процедуры². Соответственно, необходимо оценить влияние этой меры на вероятность события и серьезность последствий, если оно все же произойдет.

Итак, повлияет ли введение финансового наказания на вероятность нарушения? Скорей всего, да, т.к. угроза наказания повысит риск для нарушителя и, скорее всего, снизит вероятность отклонения от процедуры, т.е. нарушения все же будут происходить, но реже.

Если это все-таки случится, будут ли последствия меньшими, нежели до введения мер финансового характера? Очевидно, что нет, последствия будут теми же.

И мы можем провести мысленный эксперимент, оценив риск, который останется после реализации предложенной меры. Такие риски так и называются – остаточные. Стандарт ISO/IEC 17025:2017 не требует оценки таких рисков, но и не запрещает.

Итак, представим, что руководство ввело в действие финансовые меры и предположим, что в этом случае нарушение можно будет оценить как редкое (2 балла). Т.к. серьезность последствий предлагаемая мера не изменяет, то итоговая оценка остаточного риска составит $2 \times 3 = 6$ баллов. Он снова попадает (по Табл. 4А) в категорию средних и мы приходим к выводу, что одной рассматриваемой меры недостаточно.

Звучит еще одно предложение: давайте перед тем как пускать средство измерения в работу, проводить повторный его контроль.

Хорошо, проверим, как влияет эта мера на риск.

Снижает ли эта мера вероятность нарушения сотрудником процедуры первичного приема? Нетрудно видеть, что нет, не снижает. А вот на последствиях сказаться вполне может, т.к. при повторной проверке могут быть выявлены несоответствия средства измерения требованиям и оно не пойдет в работу (например, загрязненным или неисправным).

Оценим остаточный риск при реализации этой меры (с учетом введения финансового наказания).

² Все примеры мер носят учебный характер, даны исключительно для иллюстрации тех или иных положений статьи и не являются рекомендуемыми

Предположим, что повторный контроль будет действенным и приведет к снижению последствий до уровня «слабое влияние» (1 балл). Тогда итоговая оценка остаточного риска при реализации двух мер составит $2 \times 1 = 2$ балла. По Табл. 4А это низкий риск, в отношении которого уже можно использовать стратегию принятия риска.

Соответствующий фрагмент реестра рисков мог бы выглядеть следующим образом.

Таблица 3 Фрагмент реестра риска (пример)

<u>Цель:</u> своевременно и в полном объеме представить заказчику точные и достоверные результаты, содержащие объективные и независимые заключения.				
<u>Последствия:</u> результаты выданы несвоевременно, не в полном объеме, содержат неточные и недостоверные результаты, необъективные заключения.				
Описание риска	Вероятность	Серьезность последствий	Оценка риска	Меры по обработке риска
<u>Риски, связанные с нарушением правил</u>				
Принятие в работу объектов без проверки их на соответствие требованиям (например, поверив на слово заказчику)	3	3	9	1. Ввести финансовую ответственность сотрудника, проводящего прием средства измерения 2. Ввести процедуру проверки средства измерения перед началом работ

При выборе мер обработки рисков необходимо отчетливо понимать источники риска. Например, нарушение сотрудником процедуры проверки принимаемого средства измерения может быть вызвано разными причинами:

- незнанием этой процедуры,
- отсутствием этой процедуры в момент ее применения,
- неактуальностью использованной процедуры,
- неисправностью примененных инструментов и т.д.,
- недостоверностью предоставленной заказчиком информации,

Определенная систематизация возможных источников (причин) приведена на Рис. 2 во второй части данной статьи. Вот как можно использовать этот рисунок для тех причин, что перечислены выше:

- незнание процедуры: люди – компетентность – не соответствует требованиям,
- отсутствие процедуры в момент применения: правила – отсутствуют,
- неактуальность процедуры: правила – непригодны,
- неисправность примененных инструментов: оборудование – не работает (или неверно настроено),
- недостоверность предоставленной заказчиком информации: информация – недостоверная.

Как можно использовать Табл. 2 при оценке рисков (формировании реестра рисков)?

Первый шаг: построить поток работ, т.к. оценка рисков должна проводиться для каждой работы.

Чтобы, с одной стороны, не усложнять пример, а с другой сделать его все-таки наглядным, предположим, что наш поток работ выглядит следующим образом (Рис. 1).

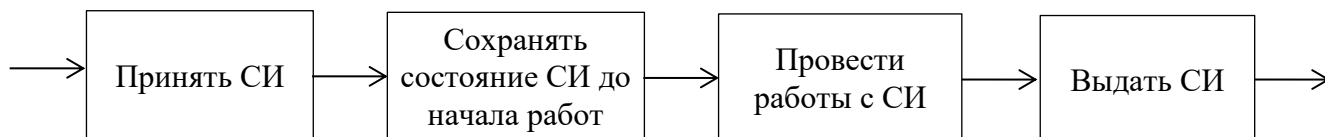


Рисунок 1 Поток работ

Рассмотрим, как могла бы проходить оценка рисков (например, в формате мозгового штурма).

На первом этапе мы должны определить риски (составить реестр) для работы №1. В соответствии с рекомендацией №2 из заключения Части 2 статьи устанавливаем цель работы №1: принять СИ и передать его на хранение в соответствии с имеющейся процедурой. При этом предполагается, что принятое СИ полностью соответствует установленным требованиям.

Для формирования реестра обращаемся к Рис.2 второй части статьи и по каждому элементу задаем вопросы.

Есть ли риск принять несоответствующее требованиям СИ из-за отсутствия информации? При ответе на вопрос экспертно оцениваем вероятность такого события и серьезность его последствий. Если общее мнение команды, что риск невелик, то принимаем решение не включать его в реестр и переходим к следующей позиции.

Есть ли риск принять несоответствующее требованиям СИ из-за недостоверной информации? Кто-то из участников команды вспоминает, что такие случаи были и даже приводили к неприятным для организации последствиям. Общее мнение: включить риск в реестр для формальной оценки и формирования мер.

И т.д. по каждому элементу.

В итоге реестр может выглядеть примерно так (Табл. 4).

Таблица 4 Заготовка реестра риска

<u>Цель:</u> принять СИ, полностью соответствующее требованиям с соблюдением установленной процедуры.				
<u>Последствия:</u> невозможность выполнить требуемые работы, нарушение обязательств перед заказчиком, угроза безопасности проведения работ.				
Описание риска	Вероятность	Серьезность последствий	Оценка риска	Меры по обработке риска
<u>Риски, связанные с информацией</u>				
Принятие в работу несоответствующих СИ из-за недостоверной информации, предоставленной заказчиком				
<u>Риски, связанные с людьми</u>				
Принятие несоответствующего СИ из-за незнания процедуры приемки				
Принятие несоответствующего СИ в силу сговора приемщика и заказчика				
Принятие несоответствующего СИ в силу некритичности приемщика (вера заказчику на слово без проверки)				
<u>Риски, связанные с оборудованием</u>				
Принятие несоответствующего СИ в силу отсутствия необходимого оборудования для проверки				
Принятие несоответствующего СИ в силу неработоспособности необходимого оборудования для проверки				
...				

Безусловно, Рис. 2 второй части статьи дает лишь возможные варианты источников рисков, каждая организация вправе сама разрабатывать подобную классификацию, наиболее для нее подходящую.

Завершая статью, хотел бы обратить внимание, что стандарт ISO/IEC 17025:2017 предусматривает два варианта построения системы менеджмента лаборатории:

- вариант А основывается на выполнении требований разделов 4-7 и 8.2-8.9 стандарта ISO/IEC 17025:2017,

- вариант Б предполагает построение СМК на основе стандарта ISO 9001:2015 и выполнение требований разделов 4-7 ISO/IEC 17025:2017.

Лаборатория, выбравшая вариант Б, должна понимать, что стандарт ISO 9001:2015 предъявляет гораздо более широкие требования к оценке рисков, нежели ISO/IEC 17025:2017. Эти требования предусматривают два уровня оценки рисков:

- стратегический, где исходной информацией служит результат анализа контекста и требований заинтересованных сторон и

- оперативный, где оцениваются риски для каждого вида деятельности, которым лаборатория планирует управлять, как процессом.