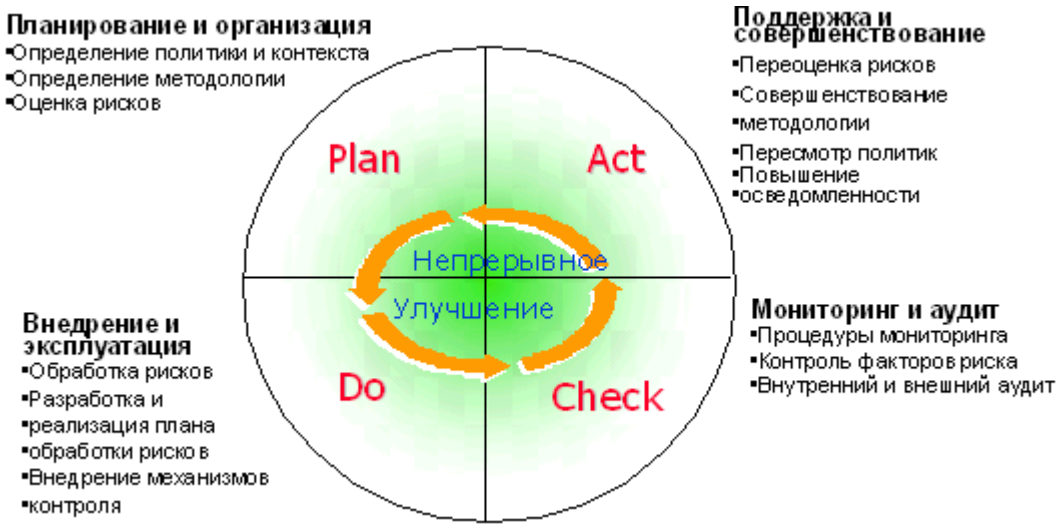
Процессная модель управления рисками

написано Александр Астахов | 10 июня, 2023

Поскольку процессы управления рисками являются составной частью общей системы управления организации, для их описания используется та же процессная модель, что и в других стандартах систем управления. Эта модель определяет четыре группы процессов: *Планирование – Реализация – Проверка – Действие (ПРПД)*, что отражает стандартный цикл управления, впервые описанный в работах Деминга. В то время как ISO 27001 описывает общий непрерывный цикл управления безопасностью, в стандартах BS 7799-3 и ISO 27005 содержится его проекция на процессы управления рисками.

Модель Деминга применительно к процессам управления рисками



Рассмотрим проекцию процессов управления рисками на процессную модель ПРПД более подробно по каждой группе процессов.

Планирование

На этапе *планирования* определяются политика, контекст и методология управления рисками, инвентаризуются (идентифицируются) активы и определяется их ценность, формулируются профили угроз и уязвимостей, оценивается

эффективность контрмер и производится обработка рисков. Руководство организации принимает соответствующие решения и утверждает план обработки рисков.

Согласно ISO 27001, оценка рисков информационной безопасности необходима для понимания требований информационной безопасности и рисков для бизнес-активов организации.

Она включает в себя следующие мероприятия:

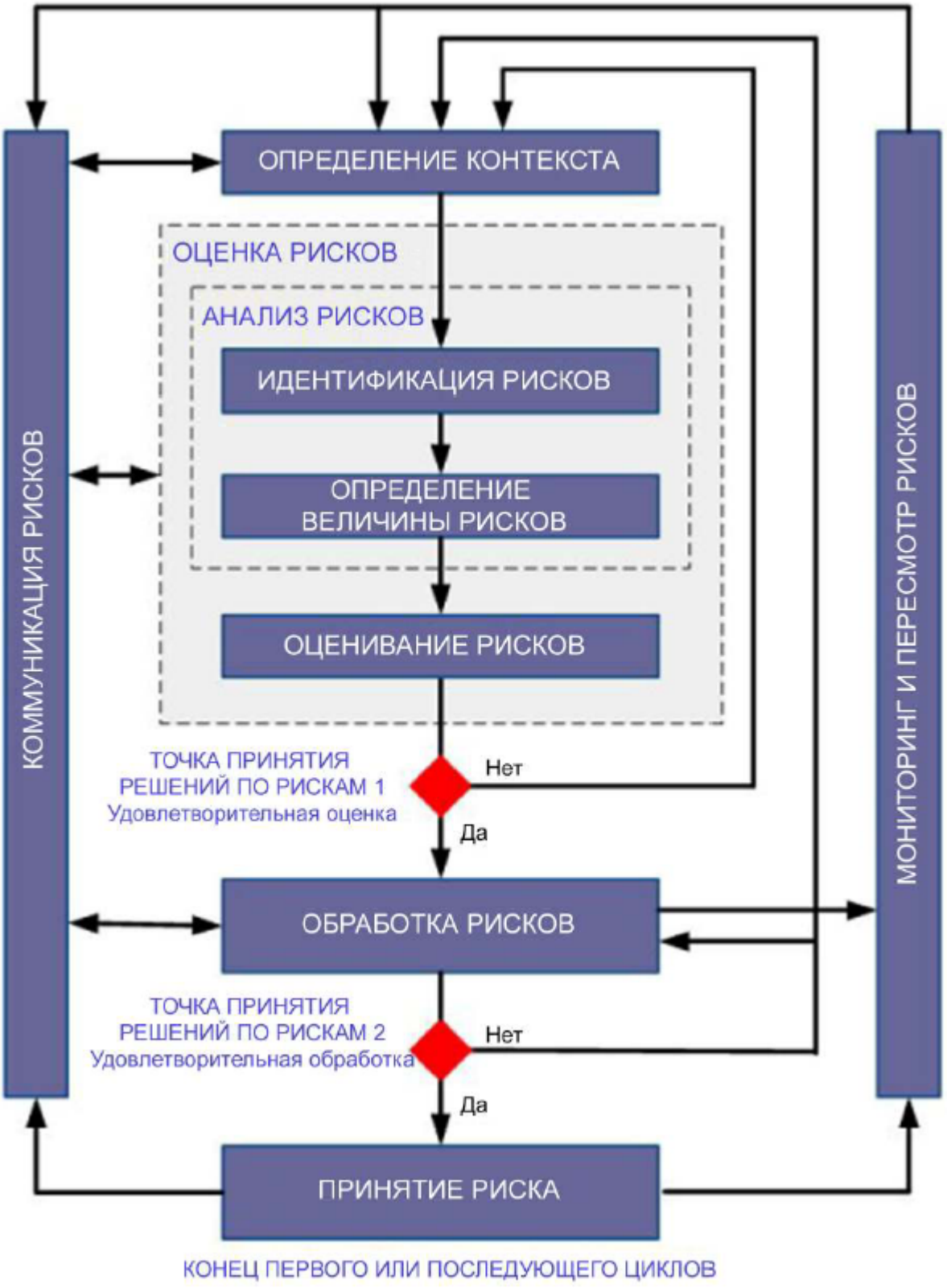
- идентификация активов;
- идентификация требований законодательства и бизнеса, применимых к идентифицированным активам;
- оценивание активов с учетом идентифицированных требований законодательства и бизнеса, а также последствий нарушения конфиденциальности, целостности и доступности;
- идентификация значимых угроз и уязвимостей для активов;
- оценка вероятности возникновения угроз и величины уязвимостей;
- вычисление рисков;
- оценивание рисков по заранее определенной шкале риска.

Следующим шагом в процессе управления рисками является идентификация подходящих мер по обработке рисков для каждого из рисков, идентифицированных в ходе оценки рисков. Управлять рисками можно путем комбинирования превентивных и детектирующих механизмов контроля, тактики избежания, страхования и/или простого принятия (сохранения) риска. После того как риск был оценен, должно быть принято бизнес-решение насчет принятия необходимых мер. Во всех случаях это решение должно быть экономически обоснованным и понятным для руководителей и владельцев бизнеса, в чью компетенцию входят принятие либо оспаривание данного решения.

На следующем рисунке изображен цикл управления рисками и показаны взаимосвязи процессов в рамках этого цикла. Процесс

управления рисками информационной безопасности включает определение контекста, оценку рисков, обработку рисков, принятие рисков, коммуникацию рисков, а также мониторинг и пересмотр рисков.

Взаимосвязь процессов управления рисками



Как показано на вышеприведенном рисунке, этот процесс может носить цикличный характер для деятельности по оценке и/или обработке рисков. Цикличный подход к проведению оценки рисков позволяет сделать оценку более глубокой и детализированной при каждой последующей итерации. При этом должен обеспечиваться баланс между минимизацией времени и усилий, затрачиваемых при определении механизмов контроля, и обеспечением надлежащей оценки высоких рисков.

Сначала определяется контекст. Затем проводится оценка рисков. Если в результате этого получено достаточно информации для эффективного определения мер, которые необходимо принять для уменьшения рисков до приемлемого уровня, то задача выполнена, и можно переходить к обработке рисков. Если информации недостаточно, проводится очередной цикл оценки рисков в пересмотренном контексте (например, критерии оценивания рисков, критерии принятия рисков или критерии оценки воздействия (ущерба)), возможно, для отдельных частей области оценки (см. на рисунке – «Точка принятия решения по рискам 1»).

Эффективность обработки рисков зависит от результатов их оценки. Возможно, обработка рисков не приведет сразу же к приемлемому уровню остаточного риска. В этом случае может потребоваться очередной цикл оценки рисков, после чего проводится дополнительная обработка рисков (см. на рисунке – «Точка принятия решения по рискам 2»).

Деятельность в сфере принятия рисков должна обеспечивать явное принятие рисков руководством организации. Это особенно важно в ситуации, когда внедрение механизмов контроля не осуществляется или откладывается, например, из-за их высокой стоимости.

В ходе всего процесса управления рисками информационной безопасности важно, чтобы информация о рисках и их обработке доводилась до сведения соответствующих руководителей и персонала. Даже до начала обработки рисков информация о

выявленных рисках может оказаться очень полезной для управления инцидентами и может помочь уменьшить потенциальный ущерб. Осведомленность менеджеров и персонала о рисках, характере имеющихся механизмов контроля, направленных на их уменьшение, а также о вопросах, вызывающих обеспокоенность организации, помогает урегулировать инциденты и непредвиденные события наиболее эффективным образом. Результаты по каждому действию в процессе управления рисками информационной безопасности и точкам принятия решений должны подробно документироваться.

Реализация

На этапе *реализации* производится внедрение необходимых механизмов безопасности и другие действия по реализации плана обработки рисков, которые могут включать в себя, например, заключение договоров страхования, соглашений об уровне сервиса и даже корректировку планов развития бизнеса в целях избежания определенных рисков.

Проверка

После принятия решений по обработке рисков и внедрения выбранных механизмов контроля должны начинаться непрерывные действия по управлению рисками. Эти действия включают в себя процесс мониторинга рисков и эффективности СУИБ, позволяющий гарантировать, что внедренные механизмы контроля функционируют надлежащим образом.

Действие

На этапе *проверки* отслеживается функционирование реализованных механизмов безопасности, контролируется изменение факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе *действия* осуществляется совершенствование процессов управления рисками по результатам мониторинга и аудита, в случае необходимости пересматриваются определенные риски,

используемые подходы и методы их оценки, вносятся изменения в нормативную и операционную документацию организации, уточняется контекст управления рисками. Постоянное совершенствование является существенной частью непрерывных действий по управлению рисками, предпринимаемых с целью повышения эффективности внедренных механизмов контроля для достижения целей, которые были установлены для СУИБ.

Далее описанный цикл управления рисками переходит на новый виток, вновь проходя стадии *Планирования*, *Реализации*, *Мониторинга* и *Совершенствования*. Процесс функционирования, развития и совершенствования СУИР реализуется по спирали. В конечном итоге все четыре группы процессов выполняются параллельно и непрерывно. Выходные данные одних процессов поступают на вход других.