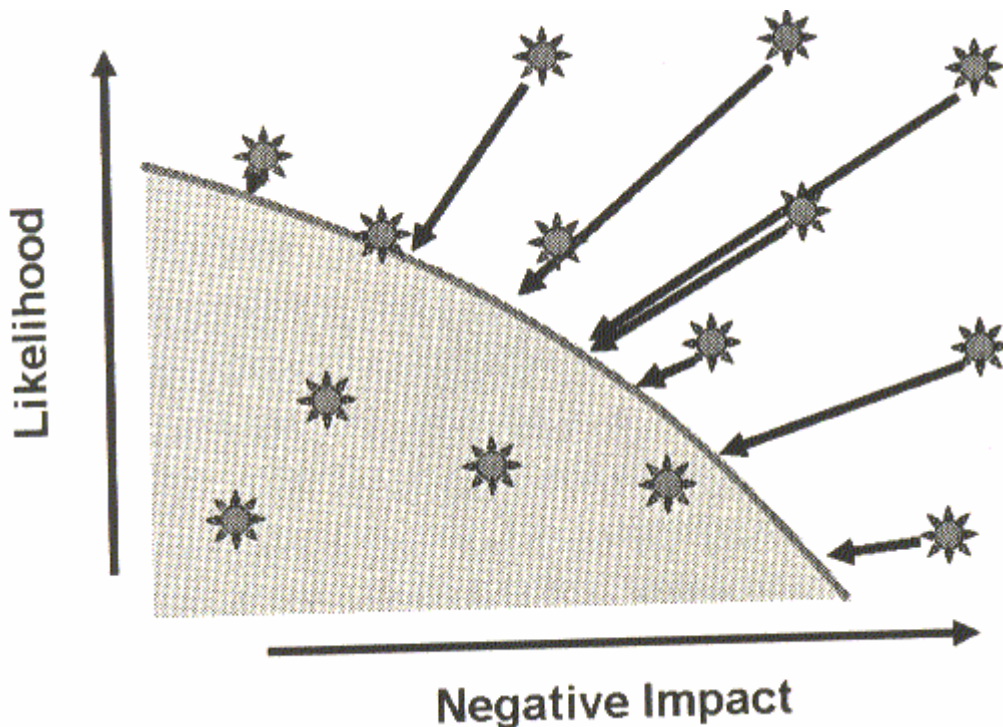


Процесс обработки рисков

написано Александр Астахов | 11 июня, 2023

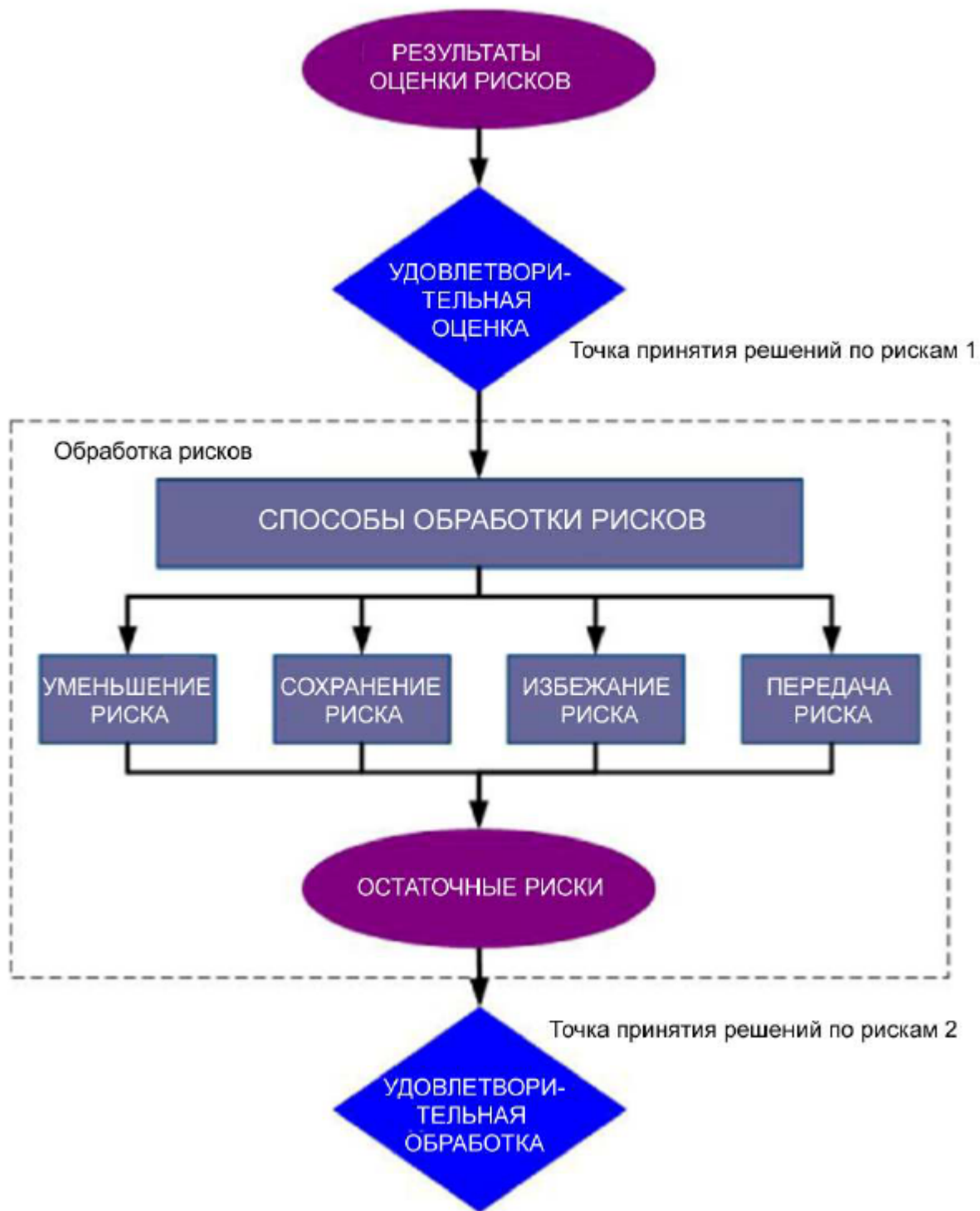
Целью обработки рисков является их уменьшение до приемлемого уровня путем уменьшения вероятности инцидента либо минимизации возможного ущерба. Однако не все риски возможно либо целесообразно уменьшать. Если организация не располагает необходимыми для этого ресурсами, например временем или квалификацией, то она может временно допустить высокий риск либо передать его третьей стороне путем заключения договора страхования или аутсорсинга. Возможен также вариант избежания риска путем отказа от рискованных операций либо переноса этих операций в более безопасное место.



Процесс обработки рисков включает в себя подготовку, выбор и принятие решений по способам обработки рисков. Способы эти могут быть самыми разными. Главное, чтобы они были реализуемы и экономически оправданы. При инвестировании денег в уменьшение риска в результате должен получаться положительный возврат инвестиций, который представляет собой разницу между затратами на безопасность и величиной предотвращаемого ущерба. Разница эта должна быть весьма существенной. Желательно, чтобы возврат инвестиций превышал затраты на безопасность в разы.

На вход этого процесса поступают результаты оценки рисков в виде отчета и прилагающегося к нему реестра информационных рисков. Если эти данные являются достаточными, тогда для каждой группы рисков принимаются решения по их обработке путем выбора одного из четырех способов обработки рисков либо их комбинации. При этом используются критерии принятия рисков, определяемые политикой организации в области управления рисками.

Результатом процесса обработки рисков является план обработки рисков, содержащий перечни мероприятий для каждой группы рисков и оценку остаточных рисков.



Выбираемые для уменьшения рисков механизмы контроля должны быть экономически обоснованы, т.е. обеспечивать положительный возврат инвестиций. Однако не все механизмы контроля можно легко экономически обосновать. Например, обеспечение непрерывности бизнеса вынуждено иметь дело с такими рисками, как природные и антропогенные катастрофы, которые с большой вероятностью могут вообще никогда не наступить. Для механизмов обеспечения непрерывности бизнеса сложно посчитать возврат инвестиций, т.к. зачастую не существует оценки среднегодовых

потерь.

Способы обработки рисков не являются взаимоисключающими. Например, мы можем уменьшить риск до определенного уровня, а остаточный риск передать третьей стороне.

Определенные способы обработки рисков могут воздействовать сразу на группу рисков, – например, такой множественный эффект дает обучение.

В ходе обработки рисков могут быть сделаны выводы в том числе и об избыточности некоторых механизмов контроля. Однако, прежде чем от них оказываться, следует оценить их влияние на другие механизмы. Многие механизмы контроля взаимосвязаны. Эффективность одних механизмов может снижаться до нуля в отсутствии других. Например, слабые пароли сводят на нет существующие в системе механизмы разграничения доступа, антивирусные средства и средства обнаружения вторжений требуют непрерывного обновления сигнатур, а политики безопасности не работают в отсутствии программы обучения и повышения осведомленности персонала.

Приемлемая величина остаточного риска не должна превышать максимально допустимый уровень риска, утвержденный руководством, который может быть сопоставим, например, со стандартными издержками одного производственного процесса организации. После выбора способов обработки риска следует оценить остаточный риск, и если этот риск не приемлем, тогда необходимо повторить обработку.

В случае если оценочная величина остаточного риска превышает максимально допустимый уровень риска, то для его уменьшения должны быть выбраны дополнительные механизмы контроля, обеспечивающие наилучший возврат инвестиций и позволяющие уменьшить остаточный риск до приемлемого уровня.

В случае невозможности либо экономической нецелесообразности уменьшения риска до приемлемого уровня должны быть рассмотрены варианты передачи данного риска третьей стороне, в качестве

которой может выступать страховая компания или компания, предоставляющая услуги по аутсорсингу ИТ процессов и сервисов безопасности, а также варианты избежания риска, связанные с отказом от рискованных операций либо их заменой на менее рискованные.

В случае отсутствия других приемлемых вариантов обработки риска, превышающего установленный в организации максимально допустимый уровень, руководством компании может быть принято решение о принятии данного риска.