

Принятие решения по обработке риска

написано Александр Астахов | 11 июня, 2023

«Принять решение легче, если у вас нет выбора».

Нарасимха Рао, индийский политик

Принятие решения по обработке рисков – ключевой и наиболее ответственный момент в процессе управления рисками. Решение по рискам – это бизнес-решение, как правило, оказывающее влияние на всю дальнейшую деятельность организации. Поэтому приниматься это решение должно лицом, находящимся на соответствующем уровне властной иерархии и отвечающим за весь бизнес или ту его часть, которая подвергается риску. Руководитель информационной безопасности должен принимать решения на своем уровне относительно того, как оптимальным образом воплотить в жизнь решения своего руководства по обработке информационных рисков.

Для того чтобы руководство могло принять правильное решение, сотрудник, отвечающий за управление рисками в организации, должен предоставить ему соответствующую информацию. Решение по бизнес-рискам должен принимать руководитель бизнеса либо лицо, которому он делегирует ответственность за определенные направления бизнеса. Руководитель службы информационной безопасности или риск-менеджер готовит решение по рискам для руководства организации.

Форма представления руководству организации информации для принятия решения по рискам определяется стандартным алгоритмом делового общения и может включать в себя следующие основные пункты:

- *Сообщение о проблеме:* в чем заключается угроза для бизнеса (источник, объект, способ реализации) и в чем

причина ее существования?

- *Степень серьезности проблемы:* чем это грозит организации, ее сотрудникам, руководству, акционерам?
- *Предлагаемое решение:* что предлагается сделать для исправления ситуации, во сколько это обойдется, кто это должен делать и что требуется непосредственно от руководства? (Используя оценки ROI для обоснования предлагаемого решения).
- *Альтернативные решения:* какие еще способы решения проблемы существуют (альтернативы есть всегда, и у руководства должна быть возможность выбора). Для сравнения альтернативных решений, помимо экономического обоснования (оценок ROI), могут также использоваться соображения о времени реализации решения, учитываться морально-этические аспекты и любые другие факторы, которые целесообразно принимать во внимание.
- *Каков остаточный риск?* Не превышает ли он приемлемого уровня? Если уровень остаточного риска не устраивает руководство, то потребуются дополнительная обработка риска.

Такой обстоятельный доклад о рисках, подкрепленный реестром информационных рисков и планом обработки рисков, обоснованным с точки зрения возврата инвестиций, и опирающийся на согласованные с руководством критерии оценки ущерба и принятия рисков, позволяет принимать наиболее взвешенные и эффективные решения по рискам. В этом случае СУИР предоставляет руководству организации эффективный механизм подготовки и принятия решений, превращая эту задачу из крайне запутанной проблемы, требующей для своего разрешения сильной интуиции и умения принимать нестандартные решения в условиях недостатка и противоречивости исходных данных, в обычную повседневную рутину. Функция руководства по существу сводится лишь к контролю предлагаемых решений, корректировкам бюджета, согласованию сроков и выделяемых ресурсов. В некоторых случаях от руководства потребуется политическая воля для принятия

остаточных рисков, не укладывающихся в установленные рамки, либо изменения критериев принятия рисков.

Принятие взвешенных и эффективных решений в условиях нечеткой и неполной информации – основная функция любого руководителя. Процесс этот достаточно субъективный. Такой же субъективный характер носят и решения, принимаемые руководителями. Информационная безопасность здесь исключением не является.

Зачастую используемые руководителями методы принятия решений не отвечают требованиям современного мира с его избытком информации и высоким ритмом жизни. Руководителей здесь подстерегают различные трудности и психологические ловушки. Тема принятия эффективных управленческих решений простирается далеко за рамки этой книги, поэтому отошлем читателя, заинтересовавшегося данным вопросом, к специальной литературе, которая с избытком представлена на книжных полках, например к Гарвардской классике.