Калибровка шкалы оценки риска

написано Александр Астахов | 10 июня, 2023

Как мы уже разобрались выше, качественная оценка риска, не привязанная к какой-либо количественной шкале, может быть полезна для правильной расстановки приоритетов, однако сама по себе не дает представления о масштабах возможной проблемы и вероятных потерях организации. Для того чтобы качественная шкала оценки риска приобрела смысл для руководства организации, необходимо сопоставить ей количественные диапазоны среднегодовых потерь организации. Эту процедуру мы называем *калибровкой качественной шкалы оценки риска*.

Среднегодовые потери мы выражаем в денежных единицах. Этот способ является наиболее естественным. В деньгах могут быть выражены практически любые виды потерь. Если речь идет об ущербе для имиджа и репутации организации, то, очевидно, что формирование имиджа и его восстановление стоит определенных денег и соответствующие расходы также можно оценить. Поддается денежной оценке и упущенная коммерческая выгода, и потеря конкурентных преимуществ, и моральный ущерб, и отток клиентов. Открытие и закрытие уголовных дел, снятие и назначение руководства, ученые степени и звания, а также решение любых других проблем, включая проблемы со здоровьем, стоит определенной суммы денег. За деньги нельзя купить разве что любовь и еще некоторые вещи, которые не имеют никакого отношения к информационным рискам (хотя даже такие устоявшиеся представления некоторыми прагматиками все же подвергаются сомнению).

Если денежные единицы в каких-то случаях не подходят в качестве меры возможного ущерба, то можно использовать и другие меры ущерба, такие, например, как уровень лояльности клиентов или доля рынка. Главное, чтобы эти меры были понятны и удобны для руководства организации, которое должно принимать осознанные решения, опираясь на результаты оценки рисков.

Рассмотрим пример калибровки качественной шкалы оценки риска, в ходе которой определенным уровням риска сопоставляются соответствующие размеры среднегодовых потерь.

Пусть мы имеем информационный актив, ценности которого присвоено значение 2, что согласно принятым в организации критериям оценки финансового ущерба соответствует потерям порядка 3–5 млн. рублей. Возьмем среднее значение размера ущерба ~ 4 млн. руб. (для нас важна не точность, а порядок величины).

Вероятность угрозы в отношении данного актива оценивается как С (средняя), что соответствует примерно одному случаю в год согласно принятой у нас шкале оценки угроз. Это также может быть 2 или 3 случая в год либо один случай в два года, но не 100 случаев в год (это мы считаем высокой вероятностью) и не один раз в пять лет (это мы считаем низкой вероятностью).

Уровень уязвимости данного актива в отношении рассматриваемой угрозы оценивается как С (средний), что примерно соответствует 50% вероятности успешного осуществления угрозы. Другими словами, мы ожидаем, что примерно каждая вторая попытка компрометации данного актива будет успешной.

Согласно приведенной выше таблице оценки риска, данным значениям ценности актива (2), угрозы (С) и уязвимости (С) соответствует уровень риска – 4.

Среднегодовой ущерб (ALE) рассчитывается по формуле:

ALE = [размер ущерба] × [количество инцидентов в год] × [вероятность успешной реализации угрозы].

В нашем случае имеем:

ALE ~ 4000000 × 1 × 0,5 = 2000000 руб.

Таким образом, принимая риск, равный 4, в данном случае организация должна смириться со среднегодовыми потерями в несколько миллионов рублей. Аналогичным образом вычисляются

среднегодовые потери организации по каждому качественному уровню риска.

Организация в зависимости от масштабов своего бизнеса должна сама сформировать критерии оценки ущерба, шкалы оценки угроз и уязвимостей, а затем откалибровать свою качественную шкалу оценки риска. Так, если стоимость бизнеса организации составляет порядка 100 млн. руб., то для такой организации максимальный риск (равный 8 по нашей шкале) сопоставим с потерей всего бизнеса или его большей части. Минимальный уровень риска (равный 0 по нашей шкале) соответствует отсутствию среднегодовых потерь либо минимальным потерям, не превышающим, например, 10 тыс. руб. в год.

Для рассматриваемой организации откалиброванная качественная шкала оценки риска может выглядеть следующим образом:

- *Низкий риск:*

– уровень **0** – 0 < ALE < 10 тыс. руб.;

– уровень **1** – 10 тыс. руб. < ALE < 50 тыс. руб.;

– уровень **2** – 50 тыс. руб. < ALE < 150 тыс. руб.

- *Средний риск:*

– уровень **3** – 150 тыс. руб. < ALE < 300 тыс. руб.;

– уровень **4** – 300 тыс. руб. < ALE < 3 млн. руб.;

– уровень **5** – 3 млн. руб. < ALE < 10 млн. руб.

- *Высокий риск:*

– уровень **6** – 10 млн. руб. < ALE < 30 млн. руб.;

– уровень **7** – 30 млн. руб. < ALE < 50 млн. руб.;

- уровень **8** – 50 млн. руб. руб. < ALE.