

Качественное определение величины риска

написано Александр Астахов | 10 июня, 2023

Конечно, точно определить вероятность угрозы, величину уязвимости либо размер ущерба на практике обычно не представляется возможным, поэтому речь может идти только о числовых оценках в некотором диапазоне величин. Так, оценочные среднегодовые потери (ALE) могут лежать в диапазоне от 100 тыс. до 1 млн. рублей, либо в диапазоне от 100 млн. рублей до 500 млн. рублей, либо превышать 1 млрд. рублей. Каждому количественному диапазону можно сопоставить определенный качественный уровень риска. В результате приходим к качественной шкале оценки риска, которой сопоставляются некоторые приблизительные количественные оценки, без которых любая качественная шкала лишается смысла, т.к. перестает быть связанной с реальными потерями организации.

На рисунке приведен пример матрицы для определения величины риска. Такая матрица возникает в результате рассмотрения вероятности сценария инцидента с учетом влияния на бизнес. В этой матрице по горизонтали откладываются качественные значения вероятности успешной реализации угрозы (сценария инцидента), а по вертикали – качественные уровни ущерба (влияния на бизнес). Результирующий риск измеряется по шкале от 0 до 8, который может оцениваться по критериям принятия рисков, т.е. сравниваться с максимально допустимым уровнем риска, в качестве которого может быть выбрано, например, значение 3. Минимальный уровень риска, равный 0, соответствует очень низкой вероятности инцидента и очень низкому влиянию этого инцидента на бизнес, а максимальный уровень риска, равный 8, соответствует очень высокой вероятности инцидента и очень высокому влиянию на бизнес. Данная шкала рисков также может быть сведена к простому общему рейтингу риска, например: низкий риск: 0–2, средний риск: 3–5, высокий риск: 6–8. Все риски, значение которых превышает 3, будут нуждаться в

обработке.

	Вероятность сценария инцидента	Очень низкая (очень маловероятно)	Низкая (маловероя тно)	Средняя (возможно)	Высокая (вероятно)	Очень высокая (часто)
Влияние на бизнес	Очень низкое	0	1	2	3	4
	Низкое	1	2	3	4	5
	Среднее	2	3	4	5	6
	Высокое	3	4	5	6	7
	Очень высокое	4	5	6	7	8

Вероятность сценария инцидента в свою очередь может быть представлена вероятностью осуществления угрозы и уровнем уязвимости. Комбинируя угрозу и уязвимости, которые используются для ее реализации, мы получаем сценарий инцидента.

Для определения значения вероятности инцидента может использоваться следующая матрица.

Вероятность угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Значение вероятности сценария инцидента	0	1	2	1	2	3	2	3	4

После определения уровня (величины) рисков, их необходимо проранжировать с целью определения приоритетов обработки этих рисков. Следующая таблица может использоваться для связи факторов ущерба (ценность актива) и вероятности инцидента (угроза и уязвимость объединяются и становятся причиной конкретного инцидента). На первом шаге по predetermined шкале оценивается ущерб, например от 1 до 5 по каждому активу (столбец *b* в табл. С.7). На втором шаге по predetermined шкале оценивается вероятность осуществления инцидента, например, от 1 до 5 по каждому инциденту (столбец *c* в табл. С.7). На следующем шаге вычисляется величина риска путем умножения *b* на *c*. В конечном итоге инциденты могут быть проранжированы по степени их критичности. Следует отметить,

что в этом примере за 1 был принят самый низкий ущерб и самая низкая вероятность.

Таблица С.7 Матрица, ранжирующая инциденты по величине риска

Дескриптор инцидента (а)	Ущерб (стоимость ресурса) (b)	Вероятность осуществления (c)	Величина риска (d)	Категория инцидента (е)
Инцидент А	5	2	10	2
Инцидент В	2	4	8	3
Инцидент С	3	5	15	1
Инцидент D	1	3	3	5
Инцидент E	4	1	4	4
Инцидент F	2	4	8	3

Приведенные выше способы качественного определения уровня риска и ранжирования инцидентов по уровню риска служат примерами табличных методов оценки рисков. Выбор конкретного табличного метода и настройка соответствующих шкал является прерогативой конкретной организации.

Еще раз подчеркнем, что любому качественному уровню, выражаемому числовыми значениями либо словами «низкий», «средний», «высокий» и т.п., должны соответствовать определенные диапазоны оценочных количественных величин. Без такого сопоставления использование качественных шкал для оценки рисков, конечно, возможно, однако в этом случае оценка рисков утрачивает экономический смысл.

Поэтому на практике количественный подход всегда превращается в качественный и наоборот, в связи с чем противопоставление качественных и количественных методов оценки рисков является, вообще говоря, занятием довольно бессмысленным.

Процесс сопоставления качественным уровням рисков соответствующих количественных диапазонов прогнозируемого среднегодового ущерба организации будет рассмотрен далее в соответствующей главе.