Количественное определение величины риска

написано Александр Астахов | 10 июня, 2023

Количественно величину риска, связанного с осуществлением конкретной угрозы безопасности в отношении конкретного актива, можно выразить при помощи следующей простой математической формулы:

.[Величина риска] = [Вероятность события] × [Размер ущерба],

где:

[Вероятность события] = [Вероятность угрозы] × [Величина уязвимости].

В этих формулах:

Вероятность события	Вероятность успешной реализации угрозы в отношении актива с использованием уязвимости и причинения ущерба организации
Вероятность угрозы	Вероятность того, что угроза в отношении актива будет реализовываться (успешность либо неуспешность реализации угрозы определяется величиной уязвимости). На практике для вычисления риска используется не математическая вероятность угрозы, а ожидаемое количество попыток реализации угрозы за определенный период времени. Специально, чтобы не было путаницы в стандартах, вместо математического термина probability используется понятие likelihood. Этот термин, хотя и переводится на русский так же, как «вероятность», на практике означает возможность реализации угрозы, характеризующуюся примерной частотой ее реализации за определенный период времени

Величина уязвимости	Вероятность того, что в случае реализации угрозы в отношении актива эта угроза будет реализована успешно с использованием данной уязвимости, т.е. безопасность актива в результате будет нарушена и организация понесет определенный ущерб

Для определения величины риска используются оценочные количественные значения, полученные путем экспертных оценок, прогнозирования, а также на основании статистических данных. Размер ущерба как правило выражается в денежных единицах, величина уязвимости принимает значения в диапазоне от 0 до 1, а вероятность угрозы является целым положительным числом, определяющим ожидаемое количество попыток реализации угрозы за определенный период времени.

Количественное определение величины риска:

[Величина риска] = [Вероятность угрозы]× [Величина уязвимости] × [Размер ущерба].

Для вычисления рисков удобно использовать период времени, равный одному году. В этом случае величина риска соответствует прогнозируемым среднегодовым потерям организации в результате инцидентов безопасности (Annual Loss Expectancy – ALE). Эту величину удобно использовать для соотнесения расходов на безопасность с величиной риска и для оценки возврата инвестиций, достигаемого за счет уменьшения величины риска, что соответствует определенному сокращению среднегодовых потерь организации.

Величина риска = Среднегодовые потери организации в результате осуществления угрозы в отношении актива с использованием уязвимости (ALE – AnnualLossExpectancy).

Это наиболее прагматичный и повсеместно используемый способ определения величины рисков. Потери организации выражаются в определенном денежном эквиваленте, ведь деньги – это наиболее универсальный инструмент для измерения ценности, применяемый в современном обществе. Каким бы ни был ущерб, материальный или нематериальный, прямой или косвенный, желательно его сопоставить определенной денежной величине. Иначе, что это за ущерб такой, ежели он ломаного гроша не стоит?

На практике оценка рисков всегда проводится на определенном уровне детализации. Все составляющие риска могут быть разложены на более мелкие составные элементы, что позволяет получить более точные и детализированные оценки рисков, и, наоборот, факторы риска могут быть сгруппированы для получения более общих оценок.

Поэтому формула для вычисления риска принимает следующий вид:

[Величина группы рисков] = [Ожидаемое количество попыток реализации группы угроз в течение года] × [Суммарная величина группы уязвимостей] × [Размер суммарного ущерба].

Практичная формула для определения величина рисков:

[Величина группы рисков] = [Ожидаемое количество попыток реализации группы угроз в течение года] × [Суммарная величина группы уязвимостей] × [Размер суммарного ущерба].

В зависимости от уровня детализации для одной организации могут рассматриваться от нескольких десятков до нескольких сотен и даже тысяч рисков информационной безопасности. Всегда следует начинать с высокоуровневой оценки рисков, которой соответствует наиболее низкий уровень детализации, повышая детализацию по мере необходимости. Поводом для проведения

более низкоуровневой (более детализированной) оценки рисков может служить то, что проведенная высокоуровневая оценка не предоставляет достаточной информации для принятия руководством организации обоснованных решений по обработке рисков.