Оценка риска

написано Александр Астахов | 10 июня, 2023
Оценка риска заключается в определении его уровня (качественной либо количественной величины) и сравнении этого уровня с максимально допустимым (приемлемым) уровнем, а также с уровнем других рисков.

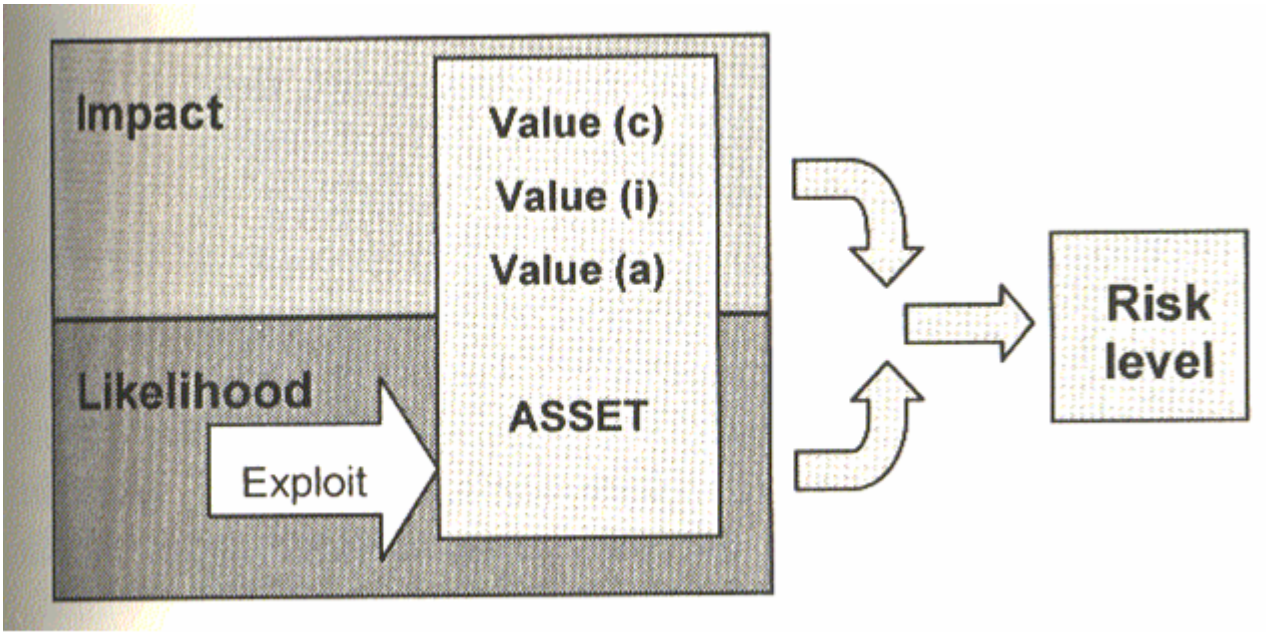
Уровень риска определяется путем комбинирования двух величин: вероятности события и размеров его последствий. Событие заключается в реализации угрозы, использующей уязвимости актива для воздействия на этот актив и нарушения его безопасности.

Под безопасностью информационного актива понимаются такие свойства информации, как конфиденциальность (защита от несанкционированного ознакомления), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения) и доступность (возможность за приемлемое время получить требуемую информационную услугу). Для упрощения дальнейшего изложения будем рассматривать только эту классическую триаду информационной безопасности, хотя к информационной безопасности относят также, по крайней мере, еще аутентичность (возможность подтверждения подлинности и достоверности документов) и неотказуемость (невозможность отрицания совершенных действий применительно к информационным активам).

Дополнительные «измерения» информационной безопасности необходимы для установления подотчетности (accountability) пользователей за действия, совершаемые ими в информационных системах. Например, некоторые злоумышленные или ошибочные действия, совершаемые в финансовой сфере, могут быть непосредственно не связаны с нарушением конфиденциальности, целостности или доступности какой-либо информации. Пользователь системы либо банковский служащий может перевести деньги с одного счета на другой, в последующем заявив о своей

непричастности к данному деянию. Безопасность каких-либо информационных активов в данном случае не нарушается, при этом одной из сторон наносится прямой финансовый ущерб посредством манипулирования с информационными активами и системами. Для избежания подобных ситуаций и нужна подотчетность.

Нарушение безопасности актива обычно наносит ущерб организации. Величина этого ущерба определяет ценность актива для организации.



Оценка риска включает идентификацию и оценку ценности активов, последствий для бизнеса, идентификацию и оценку угроз и уязвимостей, а также комбинирование этих факторов для определения уровня риска в количественных и качественных величинах.