

Обзор методов оценки риска

написано Александр Астахов | 10 июня, 2023

В этом разделе в соответствии с международным стандартом ISO 31010 описываются 39 методов оценки риска, из которых 31 метод стандартизирован, а 8 – реально применяются на практике.

Международный стандарт ISO/IEC 31010 определяет следующие общие (не только для ИБ) методы оценки риска (эти методы можно комбинировать и применять на разных этапах оценки: идентификация риска, анализ угроз и последствий, определение уровня риска, оценивание риска):

1. Мозговой штурм
2. Структурированные или частично структурированные интервью
3. Метод Дельфи
4. Контрольные листы
5. Предварительный анализ опасностей (РНА)
6. Исследование опасности и работоспособности (HAZOP)
7. Анализ опасности и критических контрольных точек (НАССР)
8. Оценка токсикологического риска
9. Структурированный анализ сценариев методом «Что, если?» (SWIFT)
10. Анализ сценариев
11. Анализ воздействия на бизнес (BIA)
12. Анализ первопричины (RCA)
13. Анализ видов и последствий отказов (FMEA)
14. Анализ дерева неисправностей (FTA)
15. Анализ дерева событий (ETA)
16. Анализ причин и последствий
17. Причинно-следственный анализ
18. Анализ уровней защиты (LOPA)
19. Анализ дерева решений
20. Анализ влияния человеческого фактора (HRA)
21. Анализ «галстук-бабочка»

22. Техническое обслуживание, направленное на обеспечение надежности
23. Анализ скрытых дефектов (SA)
24. Марковский анализ
25. Моделирование методом Монте-Карло
26. Байесовский анализ и сети Байеса
27. Кривые FN
28. Индексы риска
29. Матрица последствий и вероятностей
30. Анализ эффективности затрат (CBA)
31. Мультикритериальный анализ решений (MCDA)

Отметим, что на практике чаще применяются следующие не описанные в стандартах методы оценки риска:

1. Метод отрицания необходимости и/или возможности оценки риска
2. Метод отрицания наличия риска
3. Метод интуитивной оценки риска
4. Метод интуитивного принятия решений
5. Метод голосования
6. Метод голословных утверждений
7. Метод общих рассуждений
8. Моделирование угроз (российский метод)

Преимуществом данной группы методов является то, что они нересурсоемкие (за исключением моделирования нетиповых угроз) и самодостаточные (не требуют комбинирования с другими методами).