Обзор методов оценки риска

написано Александр Астахов | 14 июня, 2023

Неопределенность оценки риска

При оценке риска мы имеем дело с неопределенностью при оценке угроз, уязвимостей, контролей и последствий. Оперируя с неопределенными величинами, мы получаем в итоге также неопределенность. Любой оценке риска присуща значительная неопределенность. Понимание степени этой неопределенности крайне важно для правильной интерпретации результатов оценки. Неопределенность определяется величиной погрешности результатов оценки. Чувствительность оценки – это изменение оценки в зависимость от изменения конкретных входных параметров.

На самом деле, довольно часто значение риска, которое мы в итоге получаем, выражается ни каким-то одним числом (качественным уровнем или количественным ALE), а распределением вероятностей диапазона последствий. Ведь последствия, наступающие в результате реализации угроз, носят вероятностный характер. Например, системный сбой с определенной вероятностью может привести к значительному ущербу, но существует вероятность, что ущерба не наступит. Это может зависеть от конкретной ситуации. Поэтому мы будем иметь в данном случае ни одно значение риска, а распределение значений по вероятностям.

Подходы к оценке риска

Существует три подхода к оценке вероятностей (угроз, последствий и т.п.): статистика, прогнозирование и экспертные оценки. В третьем случае, помимо известного со школьной скамьи метода Дельфи, могут применяться также методы попарного сравнения, ранжирования по показателям оценки и абсолютных

оценок. Но применять все это довольно сложно и дорого, поэтому применяется в основном, то что описано ниже.

Международный стандарт ISO/IEC 31010 определяет 31 метод оценки риска. Следующие 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 (PHA)
6. Исследование опасности и работоспособности (HAZOP)
7. Анализ опасности и критических контрольных точек (HACCP)
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)

Практичные методы оценки риска

Методы оценки риска, которые мы реально применяем на практике, состоят в следующей:

1. Мозговой штурм (идентификация новых угроз, прогнозирование, поиск нестандартных решений за счет стимулирования образного мышления группы). В широком смысле, мозговой штурм – это любое обсуждение в группе.

2. Частично структурированные интервью – основной метод. Из-за ресурсных ограничений, недостатка времени, а также недостатка квалифицированных или заинтересованных специалистов, оценку риска чаще всего приходится проводить в одиночку, опрашивая всех, кто может предоставить какие-либо полезные сведения. До экспертных методов, предполагающих коллективное обсуждение, дело не доходит. Разве что на стадии согласования конечных результатов и принятия решений.

3. В случае, если вероятность события очень мала, а последствия очень значительны, стандартный количественный способов вычисления риска как значения среднегодовых потерь ALE не работает, т.к. по этому методу мы будем получать произведения бесконечно больших и бесконечно малых величин. Такие риски надо выделять в отдельную категорию и применять к ним методы анализа воздействия на бизнес (BIA) в рамках процесса управления непрерывностью бизнеса (BCM). Цели BIA – идентификация ключевых бизнес-процессов, систем и последствий нарушения их функционирования для бизнеса с целью планирования процедур и ресурсов для их восстановления. Способы реализации данного метода на практике все те же – интервью и мозговой

штурм.

4. Анализ дерева событий (ETA) необходим, например, при анализе жизненного цикла сложных сетевых угроз (сценариев развития инцидента, атаки), когда в ходе пентеста мы получаем цепочку скомпроментированных хостов и целый набор взаимосвязанных уязвимостей, причем одна без другой не может быть использована.

Непрактичные методы оценки риска

Про остальные методы, описание которых можно найти в стандартах, можно сказать следующее.

Метод Дельфи – слишком трудоемкий и затратный по времени, поэтому он себя не окупает.

Различные методы структурированного анализа опасностей (HAZOP, HACCP, SWIFT и др.), во-первых, трудоемки, во-вторых, разработаны для специфичных областей применения, в третьих, предполагают групповую работу.

Народные методы оценки риска

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

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 не ресурсоёмкие (за исключением моделирования нетиповых угроз) и самодостаточные (не требуют комбинирования с другими методами).