УДК 004.056.5:35

МЕТОДЫ ИЗМЕРЕНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ковальская Ирина Александровна, Тимофеев Дмитрий Сергеевич
Государственный ВУЗ «Национальный горный университет», kovalskaya_ira@mail.ru

Вопрос о рисках все активнее обсуждается и исследуется применительно к природе, техносфере, обществу, экономике и политике. К общим, определяющим понятие и проявления риска, относятся следующие свойства:

- **риск является многомерной характеристикой будущих состояний мира;**
- **риск связан со случайными явлениями и процессами;**
- **проявление риска – условное событие.**

Противодействием на источники риска являются установленные методы и методологии измерения рисков.

Ключевые слова – риск, оценка риска, метод измерения риска, риск информационной безопасности.

ВСТУПЛЕНИЕ

Количественная оценка вероятности и последствий от рисков информационной безопасности может осуществляться разными методами. Выбор того или иного способа зависит, в первую очередь, от объема доступной, в т.ч. статистической, информации о риске и требуемой точности оценок. Также приходится учитывать фактический уровень риска. Чем меньше вероятность наступления, тем труднее измерить риск.

Общий принцип при выборе методов измерения сводится к максимально возможному использованию доступных статистических данных. Если их нет, они недостаточны или неприменимы, фактический материал заменяется теоретическими гипотезами или экспертными оценками.

ОСНОВНАЯ ЧАСТЬ

Всего можно выделить четыре группы методов количественной оценки рисков информационной безопасности:

1. статистические методы;
2. вероятностно-статистические;
3. теоретико-вероятностные;
4. экспертные.

В основе статистических методов лежит оценка вероятности наступления случайного события исходя из относительной частоты появлений данного события в серии наблюдений. Данные методы являются наиболее предпочтительными, поскольку, во-первых, они достаточно просты, и, во-вторых, их оценки базируются на фактических данных.

Но статистические методы не применимы там, где нет достаточного объема информации по наблюдениям производительности информационной системы и предприятия в целом. Для корректной оценки рисков редких событий требуется очень больший объем статистических данных. Кроме того, сбор и обработка таких массивов информации может оказаться слишком долгой и дорогой.

Если имеющаяся статистическая информация недостаточно полная, то иногда возможно восполнить имеющиеся пробелы за счет анализа дополнительных косвенных данных или за счет логических рассуждений. Использование комбинации статистических данных и теоретических гипотез для оценки риска составляет основную идею вероятностно-статистических методов. Это расширяет область применения данной группы методов, но надежность полученных результатов может оказаться ниже, чем при использовании статистических методов.

Две предыдущие группы методов требуют наличия достаточного или хотя бы ограниченного объема статистических данных об исследуемом явлении. Однако при управлении рисками информационной безопасности приходится сталкиваться с необходимостью оценки редких событий, таких как раскрытие информации, прослушивание, замена и т.п., которые допускают тяжелые последствия. В прошлом данные события могли вообще не происходить в силу их "редкости" (т.е. малой вероятности) или уникальности рассматриваемых объектов. В этом случае статистика либо вообще отсутствует, либо относится к другим объектам, которые существенно отличаются от исследуемого. Это делает невозможным применение статистических и вероятностно-статистических методов.

Приходится использовать теоретико-вероятностные методы, в основе которых лежит построение математической модели изучаемого риска и теоретической оценки его параметров. Данные методы очень трудоемки и имеют относительно невысокую точность, но в ряде случаев являются единственным возможным научно-обоснованным способом оценки. В частности, они применяются при разработке деклараций промышленной безопасности предприятий.

ВЫВОДЫ

В ситуации, когда нет ни статистики, ни возможности построить математическую модель, остается использование опыта и знаний экспертов. Это имеет место при исследовании объектов с неопределенными параметрами или неизученными свойствами. Количественная оценка риска происходит на основе мониторинга системы, предприятия специально отобранными экспертами. При этом большое внимание должно уделяться

процедуре отбора экспертов и формированию шкал оценок.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Современные методы оценки информационной безопасности автоматизированных систем [Электронный ресурс]. – Режим доступа: http://www.nestor.minsk.by/sr/2006/10/sr61010.html

2. Я.Д.Вишняков, Н.Н. Радаев. Общая теория рисков – 2-е изд. – М. : Издательнский цент «Академия», 2008. – 368с.