НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ, № 2, 2006

УДК 000.684

И. А. Кочевская

ОБЩИЕ МЕТОДЫ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ В ОТНОСИТЕЛЬНОМ ВЫРАЖЕНИИ

Длительная практика деятельности людей в условиях риска привела к осознанию того, что невозможно предложить единую меру риска, применимую во всех случаях. В практических ситуациях, особенно в условиях доступности различных видов информации, полезно проанализировать оценки рисковой ситуации и выбрать наиболее приемлемый вариант, взвесив все показатели риска.

Существует объективная основа и субъективные причины возникновения риска, порожденные внешними условиями и внутренними факторами. Они изменяют его возможности, расширяют или ограничивают их тем самым увеличивают или уменьшают риск. Если разделить внешнюю вреду на подсреды, то изменения в одной из них могут породить ценную реакцию перемен в других.

Невозможно заранее предвидеть и момент изменения даже в одной, а тем более одновременного изменения в двух и более средах.

Все это создает неопределенность обстановки и при этом зачастую приходится принимать решения без достаточной информации о ее изменениях и влияющих на него факторов. Эта неопределенность практически не зависит от деятельности человека и объективно порождает риск его деятельности. Объективная основа обуславливает субъективную сторону риска через личность (человека) и его деятельность.

В статье [1], применительно к понятию информационного риска, были рассмотрены способы оценки риска в абсолютном выражении. Поскольку в силу ряда причин абсолютная оценка не всегда является возможной, то представляется целесообразным рассмотреть количественную оценку информационных рисков в относительном выражении.

Под осуществлением несанкционированного доступа (НД) понимается событие [2], которое приводит к следующему: нарушение конфиденциальности, нарушение целостности, отказ в обслуживании. Вероятность осуществления НД по определенному каналу будем называть риском, а канал, по которому НД может быть осуществлен, фактором риска.

Следовательно, если рассматривать вероятность наступления произвольного события, в данном случае НД, то следует считать это число как количество появлений события в бесконечной (достаточной длинной) серии попыток НД.

Обозначим:

$A_i, i = \overline{1, N}$ - событие, приводящее к4 осуществлению НД.

i – канал, по которому несанкционированный доступ может быть осуществлен, $i \in N$.

P_i, $i = \overline{1, N}$ - вероятность осуществления события A_i обусловленного фактором риска i

Рассмотрим несколько основных методов решения задачи количественной оценки информационного риска в относительном выражении.

Если рассматривать попытки НД к ИС как неограниченно большую серию испытаний (пуассоновский поток), тогда в этом случае вероятность

$P_i, i = \overline{1N}$ - вероятность осуществления A_i, обусловленного фактором риска i.

Рассмотрим несколько основных методов решения задачи количественной оценки информационного риска в относительном выражении.

Если рассматривать попытки НД к ИС как неограничено большую серию испытаний (пуассоновский поток), тога в этом случае вероятность реализации НД по i-му каналу можно записать как:

$$P_i = \frac{M(x_i)^m}{m!} e^{-M(x_i)}$$

где P_i – вероятность того, что атака на ИС по *i*–му каналу приведет к несанкционированному доступу *m* раз.

В упомянутой уже работе [2] предполагается методика оценки P_i с учетом изменения ценности информации со временем, и с учетом вероятности осуществления несанкционированного доступа.

В определенных случаях как меру риска используют безмерную характеристику математического ожидания – *коэффициент вариации* (v) поскольку одно и тоже значение дисперсии $\sigma^2(x)$ воспринимается по-разному в зависимости от размера среднего ожидаемого результата $M(x)$ [3].

$$v = \frac{\sigma(x)}{M(x)} \qquad (2)$$

Коэффициент вариации можно рассматривать как количество единиц среднеквадратического отклонения, которое приходится на единицу математического ожидания..

Коэффициент вариации, как безразмерная величина, дает возможность сравнивать результаты двух проектов, в абсолютном выражении несравнимых, т.е. таких, результаты которых оцениваются различными наименованиями.

Можно сказать, что решение задачи минимизации относительного риска (v → max) равносильна решению двухкритериальной задачи, которая требует одновременной максимизации степени защищенности информации при минимизации затрат на нее (R → max, x→min). Это еще раз подчеркивает, что показатель риска на основе коэффициента вариации достаточно весомый.

Для коэффициента вариации тоже используют шкалы, которые помогают ориентироваться в возможных разбросах его значений в (табл. 1). Как и любые другие шкалы, они определяются видом анализируемой деятельности и предпочтениями особы принимающей решение [4].

Таблица 1. Шкала для коэффициента вариации $v = \frac{\sigma(x)}{M(x)}$

Величина $v = \frac{\sigma(x)}{M(x)}$	Степень риска
= 0,1	Низкий
0,1-0,25	Средний
=0,25	высокий

При оценке информационных рисков используются безразмерные показатели, которые называются *коэффициентами риска* и при этом в каждом случае оговаривается какой из них имеется в виду.

То есть, коэффициенты риска: k_1 и k_2 :

$$\kappa_1 = \frac{L}{C} и \kappa_2 = \frac{L \cdot p}{C} \qquad (3)$$

где L - максимальная возможная величина убытка;

C – объем денежных ресурсов;

p - вероятность убытка.

В числе этих формул просматриваются введенные ранее количественные меры риска, а знаменатели сопоставляют с величиной затрат.

Принятый риск оценивается условиями:

$$k_1 > \xi_1 \; и \;\; k_2 < \xi_2$$

где ξ_1 и ξ_2 - границы ограничения риска, который определяется возможностями субъекта (предприятия, организации, частного лица).

Для этих коэффициентов задаются шкалы, которые дают возможность ориентироваться в их границах и значениях.

Для коэффициента $\kappa_1 = \frac{L}{C}$ предложены шкалы, приведенные в табл. 2 и табл. 3.

Неоднозначность шкал поясняется их достаточной условностью. Понятно, что они должны быть разными не только для каждого вида деятельности, но и для каждого принятия решения. При этом шкалы помогают ориентироваться в обстановке, связанной с риском.

Также используют обратные коэффициенты $\frac{C}{L}$ и $\frac{C}{L \cdot p}$, которые называются *коэффициентами покрытия рисков.* Исходя из содержания введенных граничных ограничений (4), эти коэффициенты должны ограничиваться снизу $\frac{1}{k_1} > \xi_1$ и $\frac{1}{k_2} \xi_2$

Таблица 3. Шкала для коэффициента $\kappa_1 = \frac{L}{C}$

Величина $\frac{L}{C}$	Степень риска
0,0-0,1	Минимальный
0,1-0,3	Малый
0,3-0,4	Средний
0,4-0,6	Высокий
0,6-0,8	Максимальный
0,8-1,0	Критический

Таблица 4. Шкала для коэффициента $\kappa_2 = \frac{L \cdot p}{C}$

Величина $\kappa_2 = \frac{L \cdot p}{C}$	Степень риска
=0,25	Принятый
0,25-0,5	Допустимый
0,5-0,75	Критический
=0,75	Катастрофический

Под коэффициентом риска планируемых показателей понимается отношение ожидаемых отрицательных и неотрицательных отклонений от запланированного уровня.

$$K = \frac{M^-}{M^+} \qquad (5)$$

M^- - отклонение в левую сторону, M^+ - отклонение в правую сторону.

Таблица 5. Шкала для коэффициента $K = \frac{M^-}{M^+}$

Величина	Градации риска (поведение в условиях риска)
<0,2	Пессимистическое
0,2-0,4	Осторожное
0,4-0,6	Среднерискованное
0,6-0,8	Рискованное
0,8-1,0	Высокого уровня риска
>1,0	Азартное

Приведенные выше шкалы, помогают провести оценку рисков хоть и весьма приближенно, зато без высоких затрат времени и средств.

Выводы: применительно к понятию информационного риска рассмотрены основные способы количественной оценки риска в относительном выражении.

Поскольку количественные показатели могут использоваться не всегда. То представляется целесообразным рассмотреть в дальнейшем качественную оценку рисков.

Список литературы

1. Кочевская И.А. Общие методы количественной оценки информационных рисков в абсолютном выражении.

2. Широчин В.П., Мухин В.Е., Крамар Д.И. Анализ рисков в задачах мониторинга безопасности компьютерных систем и сетей // «Захист інформації» № 1 (14) 2003р.

3. Машина Н.І. Економічний ризик і методи його вимірювання: Навчальний посібник. _ Київ: Центр навчальної літератури, 2003. – 188с.

4. Браіловський М.М., ЛазарєвГ.П., Дорошко В.О.Захист інформації у банківській діяльності. – К.: ТОВ «ПоліграфКолналтінг», 204. – 216 с.

УДК 000.684

С.Р. Коженевский, Г.Т.Солдатенко

ПАССИВНЫЕ МЕТОДЫ БОРЬБЫ С УТЕЧКОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ

Проблема обеспечения информационной безопасности в Украине, как и на всех странах мира, не утрачивает своей актуальности, поскольку она непосредственно связана с национальной безопасностью страны.

В конце пришлого и начале этого столетия начала происходить существенная переоценка ценностей цивилизации. К сожалению, в сфере информационных ресурсов, приобретающей первостепенное значение в научно-техническом, социально-экономическом и политическом развитии мирового общества уделяется, на наш взгляд, недостаточно внимания. Развитие рыночных отношений в нашей стране обострило проблему безопасности информации, при этом одновременно стали стремительно развиваться два процесса.

- **первый** – по защите информационных ресурсов;
- **второй** – по добыванию информации или причинению ей ущерба, вплоть до трагических ситуаций.

Информационная безопасность страны базируется на правовой и нормативных базах. В Украине это отражено в ст..17 Конституции Украины «Про інформацію» о 02.10.1992г., «Про державну таємницю» от 21.09.1999 г.и в других документах согласно перечня нормативных актов Украины по вопросам технической защиты информации от 23.04.2001 г.

Тенденции развития современного мира характеризуется созданием единого глобального информационного пространства на планете, а следовательно, проблема информационной безопасности становится проблемой коллективной, а не отдельно взятой страны. Изучение юридических проблем, связанных с расследованием компьютерных преступлений, привело, например, к разработке «Проекта Европейской Конвенции о киберпреступности» [1], в США – к пересмотру «Национальной информационной стратегии, как основе внешней и внутренней политики США в XXI веке» [2], а в России помимо Федеральных законов «Об информации, информатизации и защите информации» и «Об участии в международном информационном обмене принята «Доктрина информационной безопасности РФ».