МЕТОД ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ НА ОСНОВЕ МАТЕМАТИЧЕСКОГО АППАРАТА НЕЧЕТКОЙ ЛОГИКИ

Замула А.А., Одарченко А.С.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. Безопасности информационных технологий, тел. (057) 702-14-25,
E-mail: Alex040288@yandex.ru; факс (057) 702-14-25

In the given report questions of methods of an estimation of information risks are discussed. Existing techniques and algorithms of an estimation of risks and also an urgency and expediency of an estimation of information risks are considered. The method of estimation risks with use fuzzy logic are in detail considered.

Построение любой системы информационной безопасности должно начинаться с анализа рисков. Прежде чем проектировать систему информационной безопасности, необходимо точно определить, какие угрозы реально существуют для данной информационной системы, насколько они потенциально опасны. Грамотный учет существующих угроз и уязвимостей, выполненный на этой основе анализ рисков закладывает основу для выбора решения с необходимым уровнем информационной безопасности при минимальных затратах.

Обосновывается возможность оценки информационных рисков с применением аппарата нечеткой логики для организаций с различным уровнем автоматизации процессов обработки электронной информации. Говоря о рисках для организации, мы имеем в виду определенную вероятность и размер ущерба. Это может быть как прямой, так и косвенный ущерб, выраженный, например, в упущенной выгоде, вплоть до прекращения деятельности. В предупреждении таких ситуаций и заключается работа специалистов в области информационной безопасности (ИБ) по оценки информационных рисков.

Предлагаемый метод основывается на теории нечетких множеств (fuzzy sets) и является обобщением классической теории множеств и классической формальной логики. Метод оценивания рисков на основе нечеткой логики, по существу, является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин и риска. В простейшем случае это "табличная" логика, в общем случае – более сложная логика, отражающая реальные взаимосвязи, которые могут быть формализованы с помощью продукционных правил вида "ЕСЛИ, …, ТО". Кроме того, механизм нечеткой логики требует формирования оценок ключевых параметров и представления их в виде нечетких переменных. При этом необходимо учитывать множество источников информации и степень критичности, с точки зрения безопасности, информации. В общем случае это достаточно сложная задача. Однако, в каждом конкретном случае могут быть найдены и формально обоснованы достаточно убедительные ее решения. Механизм нечеткого вывода можно представить в виде последовательности этапов, в каждом из которых используются результаты предыдущего этапа. Каждая конкретная реализация механизма нечеткого вывода допускает некоторую свободу в выборе алгоритмов отдельных этапов обработки. Конкретные алгоритмы должны отражать специфику исследуемой системы, действующие взаимосвязи, а также вид и форму представления имеющихся априорных данных, на основе которых строится процедура вывода.

Для нечетких множеств, как и для обычных, определены основные логические операции. Самыми основными, необходимыми для расчетов, являются пересечение и объединение. Пересечение двух нечетких множеств (нечеткое "И"): A B: MFAB(x)=min(MFA(x),MFB(x)). Объединение двух нечетких множеств (нечеткое "ИЛИ"): A B: MFAB(x)=max(MFA(x), MFB(x)).

В теории нечетких множеств разработан общий подход к выполнению операторов пересечения, объединения и дополнения, реализованный в так называемых треугольных нормах и конормах. Приведенные выше реализации операций пересечения и объединения – наиболее распространенные случаи t-нормы и t-конормы. Для описания нечетких множеств вводятся понятия нечеткой и лингвистической переменных. Нечеткая переменная описывается набором (N,X,A), где N – это название переменной, X – универсальное множество (область рассуждений), A – нечеткое множество на X. Значениями лингвистической переменной могут быть нечеткие переменные, т.е. лингвистическая переменная находится на более высоком уровне, чем нечеткая переменная. Каждая лингвистическая переменная состоит из: названия; множества своих значений, которые также называются базовым терм-множеством T; универсального множества X; синтаксического правила G, по которому генерируются новые термы с применением слов естественного или формального языка; семантического правила P, которое каждому значению лингвистической переменной ставит в соответствие нечеткое подмножество множества X. Для каждого лингвистического терма из базового терм-множества T строят функции принадлежности.

Существует свыше десятка типовых форм кривых для задания функций принадлежности. Наибольшее распространение получили: треугольная, трапецеидальная и гауссова функции принадлежности.

Треугольная функция принадлежности определяется тройкой чисел (a,b,c), и ее значение в точке x вычисляется согласно выражению:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1-\dfrac{x-c}{c-b}, b\le x\le c\\ 0, \text{в остальных случаях}\end{cases}$$

При (b-a)=(c-b) имеем случай симметричной треугольной функции принадлежности, которая может быть однозначно задана двумя параметрами из тройки (a,b,c).

Аналогично для задания трапецеидальной функции принадлежности необходима четверка чисел (a,b,c,d).Значение функции вычисляется в соответствии с выражением:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ 1-\dfrac{x-c}{d-c}, c\le x\le c\\ 0, \text{в остальных случаях}\end{cases}$$

При (b-a)=(d-c) трапецеидальная функция принадлежности принимает симметричный вид (рис. 1).

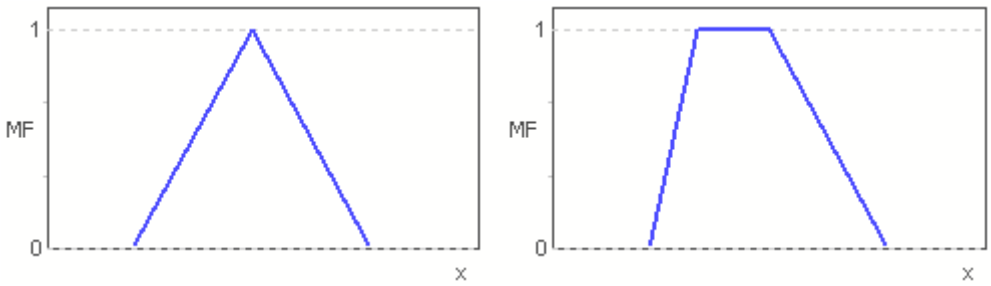

Рисунок 1. Типовые кусочно-линейные функции принадлежности.

Функция принадлежности гауссова типа описывается выражением

$$MF(x) = \exp\left[-\left(\frac{x-c}{\sigma}\right)^2\right],$$

и оперирует двумя параметрами. Параметр *c* обозначает центр нечеткого множества, а параметр σ отвечает за крутизну функции (рис.2).

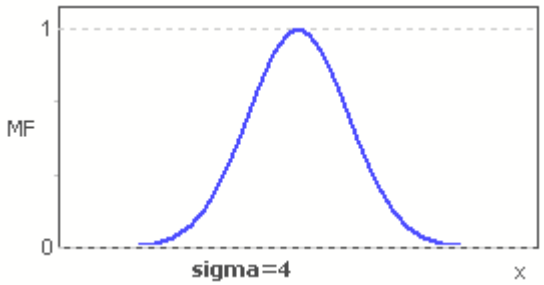

Рисунок 2. Гауссова функция принадлежности.

В докладе рассматривается метод получения оценок риска на основе нечеткой логики с предварительным оцениванием двух входных параметров: вероятность некоторого инцидента и ущерба от этого инцидента. Для реализации данного метода предлагается использовать два алгоритма: двухпараметрический алгоритм оценки риска с трехуровневыми шкалами входных параметров и двухпараметрический алгоритм с пятиуровневыми шкалами. Для первого алгоритма считаются заданными шкалы входных величин и информационного риска. Это шкалы, на которых определены нечеткие термы, соответствующие "большому", "среднему" и "низкому" значениям переменных, а логика связи входных величин и риска соответствует "табличному" механизму оценки риска, представленному в рекомендациях NIST 800-30 (табл.1).

Таблица 1. Оценка риска по трехуровневым шкалам

	Ущерб		
Вероятность	Большой	Средний	Низкий
Большая	Б	С	Н
Средняя	С	С	Н
Низкая	Н	Н	Н

Двухпараметрический алгоритм с пятиуровневыми шкалами ориентирован на методику CRAMM. где шкалы заданы следующим образом. Шкала вероятности содержит уровни: A – событие практически никогда не происходит; B – событие случается редко; C – вероятность события за рассматриваемый промежуток времени около 0,5 (событие вполне возможное при соответствующем стечении обстоятельств); D – скорее всего событие произойдет; E – событие, вероятнее всего, произойдет. Шкала ущерба содержит также пять уровней: N (Negligible) – ущерб, которым можно пренебречь; Mi (Minor) – незначительный ущерб, последствия которого легко устранить; Mo (Moderate) – умеренный ущерб; S (Serious) – серьезный ущерб, ликвидация которого возможна, но связана со значительными затратами; C (Critical) – критический ущерб, который ставит под сомнение возможность устранения его последствий.

Следуя методике CRAMM, шкалу для оценки риска задаем в виде последовательности чисел от 0 до 8, включительно. Зависимость риска от вероятности ущерба приведена в таблице 2.

Таблица 2. Шкала оценки риска по пятиуровневым шкалам

Вероятность	**Ущерб**				
	N	Mi	Mo	S	C
A	0	1	2	3	4
B	1	2	3	4	5
C	2	3	4	5	6
D	3	4	5	6	7
E	4	5	6	7	8

Несмотря на то, что в обоих алгоритмах входные переменные имели одинаковые значения, результаты при оценивании риска существенно отличаются. Это обуславливается низкой чувствительностью трехуровневого алгоритма в области высоких значений вероятности.

Предлагаемый метод получения оценок применим в инструментальных методиках оценки рисков NIST и CRAMM, и позволяет не только решить задачи по оценке рисков информационной безопасности, но и существенно расширить возможности указанных методик. В частности, метод позволяет снять ограничения на число учитываемых входных переменных и адекватно использовать качественные и количественные оценки входных параметров.

Метод получения оценок риска на основе нечеткой логики позволяет учитывать критичность входной информации и надежность (степень доверия) источников информации. Он обладает широкими возможностями, позволяющими адаптировать его к гетерогенным прикладным системам и встраивать в состав собственных разработок систем управления и оценки информационными рисками.