

## УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ ЗАЩИЩЕННЫХ ЭКОНОМИЧЕСКИХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА НЕЧЕТКИХ ВРЕМЕННЫХ РЯДОВ

© 2016 Скляров Алексей Викторович

кандидат технических наук, доцент

© 2016 Тищенко Евгений Николаевич

доктор экономических наук, профессор

© 2016 Стрюков Михаил Борисович,

доктор физико-математических наук

© 2016 Шарыпова Татьяна Николаевна

кандидат экономических наук

Ростовский государственный экономический университет (РИНХ)

344002, г. Ростов-на-Дону, ул. Б. Садовая, д. 69

E-mail: SAV0701@mail.ru, celt@inbox.ru, TNT72@mail.ru

Предложен алгоритм управления информационными рисками защищенных экономических систем, реализующий идею лингвистической аппроксимации нечетких временных рядов, позволяющий обрабатывать гетерогенную информацию о параметрах объекта управления, представленную в виде сложных качественных лингвистических описаний и количественных данных, и обеспечивающий ряд существенных преимуществ перед традиционными методами экспертных оценок.

*Ключевые слова:* управление информационными рисками, нечеткий временной ряд, экспертные оценки, показатели ценности информационных активов.

Характерной чертой современных экономических отношений является повсеместное вовлечение информационных технологий во все стадии реализации бизнес-процессов. Организация коммерческой деятельности в новых условиях диктует новые требования к информационным ресурсам предприятия и информационным системам, в которых они обрабатываются. В этой связи вопросы применения защищенных экономических систем и управления их информационной безопасностью становятся определяющими. Одним из ключевых моментов построения такой системы является управление их информационными рисками. Методологической основой управления информационными рисками служит международный стандарт ИСО 27005-2008 «Информационная технология - Методы защиты - Менеджмент информационной безопасности», в котором разработаны рекомендации, оперирующие как количественными, так и качественными показателями и критериями безопасности. При этом получение количественных оценок ориентировано на анализ вероятности реализации угроз информационной безопасности и величины их последствий, выраженных в денежном исчислении. Следует отметить, что в силу ряда причин:

- неполноты или отсутствия знаний о поведении отдельных входящих в систему элементов и подсистем, а также взаимосвязей между ними;

- невозможности или ограниченной возможности экспериментального исследования процессов, не позволяющей получить достаточную статистическую информацию о наиболее важных характеристиках системы;

- необходимости применять многоцелевое, многокритериальное оценивание гетерогенных данных, - задача информационной безопасности является плохо формализуемой. Поэтому для ее решения привлекают методы экспертных оценок.

Однако при всей проработанности методов экспертных оценок они не лишены недостатков. Во-первых, их эффективность значительно зависит от профессионального уровня экспертов. Во-вторых, привлечение высококвалифицированных специалистов в качестве экспертов связано со значительными издержками. В-третьих, управление информационной безопасностью должно осуществляться непрерывно во времени, т.е. предполагает периодичность указанных мероприятий, что значительно усугубляет их значение.

Основываясь на том, что экспертные оценки представляют качественный, выраженный в

лингвистической форме аспект, описывающий отдельные состояния исследуемой системы в некоторый момент времени, являясь по существу качественной интервальной оценкой локального состояния, для их анализа целесообразно привлечь аппарат анализа нечетких временных рядов<sup>1</sup>. Под нечетким временным рядом понимают упорядоченную последовательность наблюдений над некоторым процессом, состояния которого изменяются во времени, если значение состояния процесса в момент наблюдения может быть выражено с помощью нечеткой метрики. При этом нечеткая метрика может быть сформирована непосредственно экспертом или получена на основе некоторого преобразования исходного временного ряда.

Моделирование нечетких временных рядов состоит в реализации следующих шагов:

1. Определение нечетких переменных - разбиение данных на множество интервалов (носителей нечетких множеств), определение лингвистических значений нечетких множеств и их функций принадлежности.

2. Формирование логических отношений между входными и выходными переменными.

3. Фазификация входных данных - определение степени принадлежности входных данных входным нечетким переменным.

4. Вычисление результата применения нечеткого правила для каждой импликации.

5. Вычисление результирующего отношения.

Задача анализа нечеткого временного ряда может быть сформулирована как задача лингвистической аппроксимации<sup>2</sup>.

Рассмотрим объект управления с одним выходом и  $n$  входами вида

$$y = f_y(x_1, x_2, \dots, x_n), \quad (1)$$

где  $y$  - выходная переменная;

$x_1, x_2, \dots, x_n$  - входные переменные.

В терминах рассматриваемой задачи в качестве входных переменных выступают количественные и качественные показатели ценности информационных активов, их уязвимости, вероятности возникновения угроз, степени тяжести потерь от нарушения сервисов безопасности и т.д., в качестве выходной - защитные меры. При этом для количественных переменных предполагаются известными области их изменений, а для качественных - множества всех их возможных значений.

Рассмотрим вектор фиксированных значений входных переменных:

$$X^* = (x_1^*, x_2^*, \dots, x_n^*), \quad x_i^* \in U_i, i = \overline{1, n}. \quad (2)$$

Задача управления информационными рисками состоит в том, чтобы на основе информации о векторе входов  $X^*$  определить выход  $y^* \in Y$ . Будем рассматривать входные и выходную переменные как лингвистические переменные, для оценки которых используются качественные термы из следующих терм-множеств:

$$A_i = \{a_i^1, a_i^2, \dots, a_i^p\}, \quad D = \{d_1, d_2, \dots, d_m\}, \quad (3)$$

где  $a_i^p$  -  $p$ -й лингвистический терм переменной  $x_i$ ;

$d_j$  -  $j$ -й лингвистический терм переменной  $y$ ;

$m$  - число различных решений в рассматриваемой области.

Лингвистические термы будем рассматривать как нечеткие множества. Для установления зависимости (1) возьмем  $N$  экспертных оценок, связывающих входы и выход объекта управления, и распределим их следующим образом:

$$N = k_1 + k_2 + \dots + k_m, \quad (4)$$

где  $k_j$  - число экспертных оценок, соответствующих выходному решению  $d_j$ ;

$m$  - число выходных решений.

Предполагается, что число отобранных экспертных оценок меньше полного перебора различных сочетаний уровней изменения входных переменных объекта.

Сформируем матрицу размерностью  $(n+1) \times N$  по следующему правилу:

-  $n$  столбцов матрицы соответствуют входным переменным  $x_i$ ;  $n+1$ -й столбец соответствует значениям  $d_j$  выходной переменной  $y$ ;

- каждая строка матрицы представляет некоторую комбинацию значений входных переменных, отнесенную экспертом к одному из возможных значений выходной переменной  $y$ , при этом: первые  $k_1$  строк соответствуют значению выходной переменной  $y = d_1$ ; вторые  $k_2$  строк - значению  $y = d_2$ , ..., последние строки - значению  $y = d_m$ ;

- элемент  $a_i^{jp}$ , стоящий на пересечении  $i$ -го столбца и  $jp$ -й строки, соответствует лингвистической оценке параметра  $x_i$  в строке нечеткой базы знаний с номером  $jp$ . При этом лингвистическая оценка  $a_i^{jp}$  выбирается из терм-множества, соответствующего переменной  $x_i$ .

Результат представлен в таблице.

Сформированная матрица представляет собой матрицу знаний, которая определяет систему логических высказываний типа <ЕСЛИ-ТО, ИНАЧЕ>, связывающих значения входных переменных  $x_i$  с одним из возможных типов решения  $d_j$ :

Номер комбинации входных значений	Входные переменные				Выходная переменная $y$
	$x_1$	$x_2$	... $x_i$ ...	$x_n$	
11	$a_1^{11}$	$a_2^{11}$	... $a_i^{11}$ ...	$a_n^{11}$	$d_1$
12	$a_1^{12}$	$a_2^{12}$	... $a_i^{12}$ ...	$a_n^{12}$	
...	...	...	...	...	
$1^{k_1}$	$a_1^{1k_1}$	$a_2^{1k_1}$	... $a_i^{1k_1}$ ...	$a_n^{1k_1}$	
...	...	...	...	...	$d_j$
$j^1$	$a_1^{j1}$	$a_2^{j1}$	... $a_i^{j1}$ ...	$a_n^{j1}$	
...	...	...	...	...	
$j^{k_j}$	$a_1^{jk_j}$	$a_2^{jk_j}$	... $a_i^{jk_j}$ ...	$a_n^{jk_j}$	
...	...	...	...	...	$d_m$
$m$	$a_1^{m1}$	$a_2^{m1}$	... $a_i^{m1}$ ...	$a_n^{m1}$	

$$\bigcup_{p=1}^{k_j} \left[ \bigcap_{i=1}^n (x_i = a_i^{jp}) \right] \longrightarrow y = d_j, \quad j = \overline{1, m}, \quad (5)$$

где  $k_j$  - количество правил, определяющих значение выходной переменной  $y = d_j$ .

Система логических высказываний (5) представляет собой нечеткую базу знаний<sup>3</sup>.

Таким образом, искомое соотношение (1), устанавливающее связь между входными параметрами  $x_i$  и выходной переменной  $y$ , формализовано в виде системы нечетких логических высказываний (5), которая базируется на введенной матрице знаний.

Для разработки алгоритма принятия решения, ставящего в соответствие фиксированному вектору входных переменных (2) решение  $y$ , на базе системы логических высказываний (5) составим систему нечетких логических уравнений, корни которых представляют собой значения функций принадлежности различных решений  $y$  при фиксированных значениях входных переменных.

$$\mu^{d_j}(x_1, x_2, \dots, x_n) = \bigvee_{p=1}^{k_j} \left[ \bigwedge_{i=1}^n \mu^{a_i^{jp}}(x_i) \right], \quad j = \overline{1, m}. \quad (6)$$

где  $\mu^{d_j}(x_1, x_2, \dots, x_n)$  - функция принадлежности вектора входных переменных значению выходной переменной  $d_j$ ;

$\mu^{a_i^{jp}}(x_i)$  - функция принадлежности параметра  $x_i$  нечеткому терму  $a_i^{jp}$ .

В качестве искомого решения выбирается решение с наибольшим значением функции принадлежности, для этого:

- зафиксируем вектор значений входных переменных (2);

- зададим функции принадлежности нечетких термов, используемых в нечеткой базе знаний (5) и определим значения этих функций для заданных значений входных переменных;

- используя логические уравнения (6), вычислим многомерные функции принадлежности

$\mu^{d_j}(x_1, x_2, \dots, x_n)$  вектора  $X^*$  для всех значений  $d_j$  выходной переменной  $y$ . При этом логические операции “И” и “ИЛИ” над функциями принадлежности заменяются на операции  $\min$  и  $\max$ ;

- определим значение  $d_j^*$ , функция принадлежности которого максимальна:

$$\mu^{d_j}(x_1^*, x_2^*, \dots, x_n^*) = \max_{j=1, m} (\mu^{d_j}(x_1^*, x_2^*, \dots, x_n^*)). \quad (7)$$

Таким образом, предложенный алгоритм управления информационными рисками защищенных экономических систем, реализуя идею лингвистической аппроксимации нечетких временных рядов, позволяет обрабатывать гетерогенную информацию о параметрах объекта управления, представленную в виде сложных качественных лингвистических описаний и количественных данных. Привлечение аппарата нечеткого логического вывода для решения задачи управления информационными рисками обеспечивает ряд существенных преимуществ перед традиционными методами экспертных оценок. К ним относятся: концептуальная легкость понимания, обусловленная базированием на естественном языке; гибкость и устойчивость к неточности и отсутствию исходных данных; возможность анализа сложных, нелинейных, нестационарных систем; легкость реализуется на матрице значений функций принадлежности, полученной из матрицы знаний, путем выполнения операций  $\min$  и  $\max$ .

<sup>1</sup> Song Q., Chissom B. (1993) Fuzzy time series and its models. *Fuzzy Sets and Systems*, 54, pp. 269-277.

<sup>2</sup> Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткая логика, генетические алгоритмы, нейронные сети. Винница, 1999.

<sup>3</sup> Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений. Москва, 1976.