УДК 004.89 DOI: 10.17587/it.24.657-664

В. И. Васильев, д-р техн. наук, проф., e-mail: vasilyev@ugatu.ac.ru,
А. М. Вульфин, канд. техн. наук, доц., e-mail: vulfin.alexey@gmail.com,
М. Б. Гузаиров, д-р техн. наук, проф., e-mail: guzairov@ugatu.su,
А. Д. Кириллова, магистр, e-mail: kirillova.andm@gmail.com,
Уфимский государственный авиационный технический университет

Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт

Рассматривается возможность получения интервальных количественных оценок рисков информационной безопасности с помощью нечетких серых когнитивных карт (Fuzzy Grey Cognitive Maps). Обсуждаются вопросы построения нечетких серых когнитивных карт на основе обработки знаний и опыта экспертов. Рассмотрены особенности применения данного класса когнитивных моделей на примере задачи оценки информационных рисков.

Ключевые слова: *информационные риски, когнитивное моделирование, интервальные оценки, нечеткие серые когнитивные карты*

Введение

Проблема оценки информационных рисков является одной из центральных проблем, вызывающих интерес у специалистов в области информационной безопасности (ИБ). Сегодня известно большое число методов и подходов (CRAMM, OCTAVE, COBRA, MSAT, RiskWatch, АванГард и др.), цель которых — дать качественную или количественную оценку рисков ИБ и в конечном итоге сформировать определенные рекомендации по выбору состава защитных мер, направленных на обеспечение заданного уровня защищенности информационной системы [1—3]. Вопросам оценки информационных рисков посвящены разделы ряда стандартов по ИБ (ГОСТ Р ИСО/МЭК 15408, 27001-27005, 13335, 18045, СТО БР ИББС и др.), руководящие документы ФСТЭК (Федеральной службы по техническому и экспертному контролю) России. В то же время, в силу наличия значительных факторов неопределенности проблема остается во многом открытой и требует для своего решения применения все новых подходов, базирующихся, в частности, на применении технологий интеллектуального анализа данных и когнитивного моделирования.

В последние годы внимание многих исследователей привлекают возможности, которые предоставляет для решения проблемы оценки рисков ИБ такое направление в изучении сложных, плохо формализуемых систем, как моделирование на основе построения нечетких когнитивных карт (НКК) (Fuzzy Cognitive Maps) [4—8]. В соответствии со сложившейся классификацией различают: простые (классические) НКК, обобщенные НКК, реляционные НКК, нечеткие продукционные НКК, НКК в базисе "истина—ложь—неопределенность" и многие другие. Известны успешные примеры применения аппарата НКК для решения задач оценки рисков нарушения ИБ [9—13].

Важное место среди семейства НКК занимают нечеткие "серые" когнитивные карты (НСКК) (Fuzzy Grey Cognitive Maps, FGCM), впервые предложенные в 2010 г. Хосе Салмероном [14]. Основное отличие НСКК от других разновидностей НКК — использование интервальных оценок (диапазонов) значений переменных состояния концептов и весов связей между этими концептами вместо использования значений (термов) лингвистических переменных, описываемых с помощью нечетких чисел или функций принадлежности нечет-

ких множеств, как это традиционно делается в НКК. Операции нечеткой логики заменяются при этом интервальной арифметикой над "серыми" (интервальными) числами (grey numbers).

Нечеткие серые когнитивные карты (которые с равным успехом можно назвать также "интервальными" НКК) считаются удачным расширением НКК, поскольку они лучше соответствуют представлениям экспертов, обладают большей интерпретируемостью и представляют больше степеней свободы лицу, принимающему решение (ЛПР) на основании результатов моделирования. Отсюда понятен тот интерес, который проявляется к применению НСКК в различных технических приложениях [8, 14]. Очевидно, что применение НСКК для решения задач интервального оценивания рисков ИБ имеет свои перспективы (ранее аналогичные предложения высказывались в работах [15, 16]).

Ниже приведены понятия "серой" системы, "серого" числа и "серой" переменной, рассмотрены особенности построения НСКК. На конкретном примере обсуждается методика расчета интервальных оценок информационных рисков с использованием НСКК.

1. Теоретические основы построения нечетких серых когнитивных карт

Фундаментом построения НСКК является теория серых систем (Grey Systems Theory), предложенная в 1989 г. Дж. Денгом [17]. Предметом изучения данной теории являются объекты и системы с высокой неопределенностью, представленные малыми выборками неполных и неточных данных. В зависимости от имеющейся известной информации изучаемые системы при этом делятся на три вида:

— "белые" системы (внутренняя структура и свойства системы полностью известны);

— "серые" системы (известна частичная информация о системе";

— "черные" системы (внутренняя структура и свойства системы полностью неизвестны).

В соответствии с терминологией теории серых систем НСКК — это когнитивная модель системы в виде ориентированного графа, заданного с помощью следующего набора множеств:

$$\text{НСКК} = \langle C, F, W \rangle, \qquad (1)$$

где $C = \{C_i\}$ — множество концептов (вершин графа) ($i = 1, 2, ..., n$); $F = \{F_{ij}\}$ — множество связей между концептами (дуг графа); $W = \{W_{ij}\}$ — множество отношений между концептами, определяющих веса указанных связей (дуг графа), $(i, j) \in \Omega$. Здесь $\Omega = \{(i_1, j_1), (i_2, j_2), ..., (i_L, j_L)\}$ — множество пар индексов смежных (связанных между собой) вершин, $L \leqslant n(n-1)$.

В отличие от традиционного понимания НКК, веса связей НСКК задаются с помощью "серых" (интервальных) чисел $\otimes W_{ij}$, определяемых как

$$\otimes W_{ij} \in [\underline{W}_{ij}, \overline{W}_{ij}],$$
$$\underline{W}_{ij} < \overline{W}_{ij}, \{\underline{W}_{ij}, \overline{W}_{ij}\} \in [-1, 1], \qquad (2)$$

где $\underline{W}_{ij}$ — нижняя граница серого числа $\otimes W_{ij}$; $\overline{W}_{ij}$ — верхняя граница серого числа. Таким образом, вес связи между i-м и j-м концептами ($C_i \to C_j$) может принимать любое значение в пределах заданного диапазона изменения $[\underline{W}_{ij}, \overline{W}_{ij}] \in [-1, 1]$. В частном случае, когда $\underline{W}_{ij} = \overline{W}_{ij}$, получаем $\otimes W_{ij} \in [\underline{W}_{ij}, \underline{W}_{ij}]$ — "белое" (четкое, обычное) число.

Предполагается, что изменение состояния концептов во времени описывается уравнениями

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} \otimes W_{ji} \otimes X_j(k)\right), \qquad (3)$$

$i = 1, 2, \ldots, n,$

где $\otimes X_i(k)$ — "серая" (интервальная) переменная состояния i-го концепта C_i, которая в каждый момент времени $k = 0, 1, 2, ...$ принимает некоторое значение внутри определенного интервала (диапазона изменения), заданного границами $\underline{X}_i(k)$ и $\overline{X}_i(k)$; $f(\cdot)$ — нелинейная функция активации i-го концепта, отображающая значения аргумента в интервал $[-1, 1]$. В качестве функции активации $f(\cdot)$, как правило, принимаются:

а) линейная функция с ограничением:

$$f(x) = \begin{cases} x, & \text{если } |x| \leqslant 1, \\ \operatorname{sign} x, & \text{если } |x| > 1; \end{cases} \qquad (4)$$

б) двухполярная сигмоидная функция (гиперболический тангенс):

$$f(x) = (1 - \mathbf{e}^{-x})/(1 + \mathbf{e}^{-x}) = \operatorname{th}\left(\frac{x}{2}\right); \qquad (5)$$

в) однополярная сигмоида:

$$f(x) = 1/(1 + \mathbf{e}^{-x}). \qquad (6)$$

Для решения системы уравнений (3) требуется задать начальные значения переменных состояния $\otimes X_i(0)$, которые также должны рассматриваться как серые числа $\otimes X_i(0) \in \in [\underline{X}_i(0), \bar{X}_i(0)]$. Наибольший интерес обычно представляет получение равновесного (установившегося) решения, которое представляет собой "серый" вектор $\lim\limits_{k\to\infty}[\otimes X_i(k)] = \otimes X^* \in [\underline{X}^*, \bar{X}^*]$ или предельный цикл (странный аттрактор).

Для определения устойчивости установившегося решения $\otimes X^*$ можно воспользоваться теоремой [18], согласно которой единственное равновесное (установившееся) решение уравнений вида (3) ("неподвижная точка") существует в том и только в том случае, если выполняется условие

$$\left(\sum_{i,j=1}^{n} W_{ij}^2\right)^{1/2} < H, \qquad (7)$$

где значение положительной константы H зависит от выбора функции активации концептов: $H = 1$ для функции (4); $H = 2$ для функции (5); $H = 4$ для функции (6). Очевидно, что проверка выполнения условия для уравнений (3) должна проводиться для верхних границ серых чисел $\bar{W}_{ij}$ $(i, j = 1, 2, \ldots n)$.

Более подробную информацию о построении НСКК и особенностях их применения можно найти в работах [14] или [8] (Chapter 14: Using Fuzzy Grey Cognitive Maps for Industrial Processes Control / Salmeron J. L., Papageorgiou E. I., pp. 237—252).

2. Пример оценки рисков с помощью НСКК

Допустим, что требуется оценить риски, связанные с нарушением конфиденциальности и целостности информации вследствие воздействия ряда угроз на информационные ресурсы (активы). Пусть НСКК для рассматриваемой ситуации принимает вид, представленный на рис. 1.

Здесь *1* — концепт C_1, представляющий собой угрозу, связанную с попыткой несанкционированного доступа (НСД) к информации; *2* — концепт C_2, представляющий угрозу, связанную с вредоносным программным воздействием (вирусными атаками); *3* — концепт C_3, характеризующий целевой объект угрозы — базу данных (БД), размещенную на сервере; *4* — концепт C_4, характеризующий электронный документооборот (ЭДО) организации; *5* — концепт C_5, характеризующий потенциальный ущерб, вызванный нарушением конфиденциальности информации; *6* — концепт C_6, характеризующий потенциальный ущерб вследствие нарушения целостности информации.

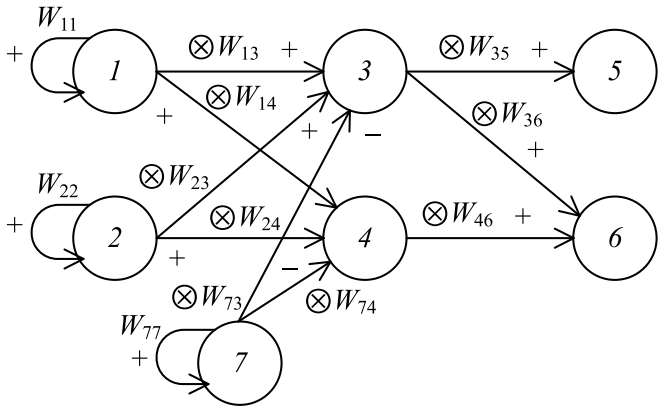

Рис. 1. Нечеткая серая когнитивная карта для оценки рисков ИБ

Переменные состояния: $\otimes X_1$ — вероятность возникновения угрозы типа НСД за определенный период времени; $\otimes X_2$ — вероятность возникновения угрозы типа "Вредоносное программное воздействие/вирусы" за тот же период времени; $\otimes X_3$ — доля утраченных или искаженных записей в БД к их общему количеству; $\otimes X_4$ — доля времени, затрачиваемого на простои или восстановление нормальной работы ЭДО, по отношению к общему времени; $\otimes X_5$ — ущерб от нарушения конфиденциальности информации; $\otimes X_6$ — ущерб от нарушения целостности; $\otimes X_7$ — стоимость контрмер по защите информации. Связи между концептами W_{13}, W_{14}, W_{23}, W_{24}, W_{35}, W_{36}, W_{46} считаются положительными, т. е. для пары концептов $C_i \to C_j$ увеличение переменной X_i приводит к увеличению переменной X_j, а связи W_{73}, W_{74} — отрицательными, т. е. увеличение переменной X_i приводит к уменьшению переменной X_j. Все переменные $\otimes X_1 \div X_7$ считаются нормированными; их значения принадлежат интервалу [0, 1].

Будем полагать, что при выборе серых значений весов $\otimes W_{ij}$ эксперт начинает с выбора "центров" соответствующих интервалов W_{ij}^0, ориентируясь на некоторую нечеткую шкалу, наподобие той, которая представлена в табл. 1.

Таблица 1

Оценка силы связи между концептами

Лингвистическое значение силы связи	Числовой диапазон
Не влияет	0
Очень_слабая	(0; 0,15]
Слабая	(0,15; 0,35]
Средняя	(0,35; 0,6]
Сильная	(0,6; 0,85]
Очень_сильная	(0,85; 1]

Следующим шагом, определяющим действия эксперта, будет выбор границ интервала $[\underline{W}_{ij}, \overline{W}_{ij}]$, определяющего серое значение силы связи $\otimes W_{ij}$. Это могут быть равноотстоящие от центрального значения W_{ij}^0 числа, например: $\otimes W_{ij} \in [W_{ij}^0 - \delta_{ij}, W_{ij}^0 + \delta_{ij}]$, где $\pm\delta_{ij}$ — разброс оценки относительно центра W_{ij}^0, но возможны и другие варианты.

Допустим, что эксперт оценил значения весов связей НСКК (рис. 1) определенным образом (табл. 2).

В табл. 2 в отдельном столбце приведены значения уровня "серости" (greyness) соответствующих "серых" чисел, определяемого как отношение размаха серого числа к общей длине диапазона его изменения [−1, 1]:

$$\Phi(\otimes W_{ij}) = \left|\overline{W}_{ij} - \underline{W}_{ij}\right|/2. \qquad (8)$$

Заметим, что концепты C_1, C_2, C_7 на рис. 1 имеют собственные циклы положительной обратной связи с весами $W_{11} = W_{22} = W_{77} = 1$. Это указывает на то, что данные концепты выступают в качестве независимых источников входных сигналов НСКК, отражающих воздействия на смежные концепты со стороны внешней среды (в работе [19] такие концепты названы *драйверами*).

Таблица 2

Значения весов связей НСКК

Вес связи	Значение веса связи	Серость (разброс оценки)
W_{13}	[0,65; 0,85]	0,1
W_{14}	[0,6; 0,75]	0,075
W_{23}	[0,6; 0,8]	0,1
W_{24}	[0,5; 0,7]	0,075
W_{35}	[0,6; 0,8]	0,1
W_{36}	[0,7; 0,85]	0,075
W_{46}	[0,5; 0,7]	0,1
W_{73}	[−0,6; −0,4]	0,1
W_{74}	[−0,6; −0,3]	0,15

Примем в качестве функции активации $f(\cdot)$ концептов C_3, C_4, C_5, C_6 двухполярную сигмоиду (5). Проверка выполнения условия (7) для данных, приведенных в табл. 2, показывает, что

$$\left(\sum_{i,j=3}^{6} \overline{W}_{ij}^2\right)^{1/2} = \sqrt{2,98} < 2,$$

т. е. установившиеся состояния НСКК для рассмотренных ниже сценариев будут устойчивы. Значения весов связей, выходящих из драйверов, т. е. концептов C_1, C_2 и C_7, согласно работе [18], в данном случае не учитываются.

Переходя непосредственно к расчетной части моделирования с помощью НСКК, рассмотрим следующие сценарии моделирования.

A. Угроза "Несанкционированный доступ" при отсутствии дополнительных мер защиты (контрмер), что соответствует начальным условиям

$$\otimes X(0) = \\ = \left([0,8;1],[0;0],[0;0],[0;0],[0;0],[0;0],[0;0]\right). \qquad (9)$$

B. Угроза "Вредоносное программное воздействие" при отсутствии дополнительных контрмер, что соответствует начальным условиям

$$\otimes X(0) = \\ = \left([0;0],[0,8;1],[0;0],[0;0],[0;0],[0;0],[0;0]\right). \qquad (10)$$

C. Угроза "Несанкционированный доступ" при использовании дополнительных контрмер, что соответствует начальным условиям

$$\otimes X(0) = \\ = \left([0,8;1],[0;0],[0;0],[0;0],[0;0],[0;0],[0,8;1]\right). \qquad (11)$$

D. Угроза "Вредоносное программное воздействие" при использовании дополнительных контрмер, что соответствует начальным условиям

$$\otimes X(0) = \\ = \left([0;0],[0,8;1],[0;0],[0;0],[0;0],[0;0],[0,8;1]\right). \qquad (12)$$

В качестве указанных контрмер могут выступать, например, межсетевые экраны, системы обнаружения атак, антивирусные программы и т. п.

Нетрудно видеть, что *для сценария A* расчетная схема моделирования существенно упрощается и принимает вид, представленный на рис. 2.

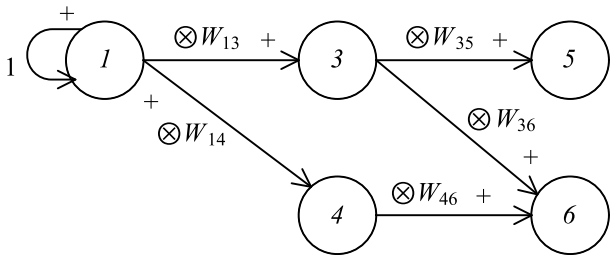

Рис. 2. Схема оценки рисков с помощью НСКК

Таблица 3

Верхние границы оценок состояния

$\bar{X}_i$	k							
	1	2	3	4	5	6	7	8
$\bar{X}_3$	0,40	0,55	0,60	0,62	0,63	0,63	0,63	0,63
$\bar{X}_4$	0,36	0,50	0,55	0,57	0,58	0,58	0,58	0,58
$\bar{X}_5$	0	0,16	0,21	0,33	0,39	0,42	0,43	0,43
$\bar{X}_6$	0	0,29	0,50	0,60	0,64	0,66	0,66	0,66

Таблица 4

Нижние границы оценок состояния

$\underline{X}_i$	k							
	1	2	3	4	5	6	7	8
$\underline{X}_3$	0,25	0,37	0,42	0,44	0,45	0,45	0,45	0,45
$\underline{X}_4$	0,24	0,34	0,39	0,41	0,42	0,42	0,42	0,42
$\underline{X}_5$	0	0,07	0,14	0,19	0,22	0,24	0,25	0,25
$\underline{X}_6$	0	0,15	0,28	0,37	0,41	0,44	0,45	0,45

Учитывая монотонный характер зависимостей $X_5 = f_1(X_1, X_3)$ и $X_6 = f_2(X_1, X_3, X_4)$, можно отдельно провести оценку сначала верхних границ переменной $\otimes X_5$ и переменной $\otimes X_6$:

$$\bar{X}_5 = f_1(\bar{X}_1, \bar{X}_3); \;\; \bar{X}_6 = f_2(\bar{X}_1, \bar{X}_3, \bar{X}_4),$$

а затем — аналогично оценку нижних границ $\otimes X_5$ и $\otimes X_6$:

$$\underline{X}_5 = f_1(\underline{X}_1, \underline{X}_3); \; \underline{X}_6 = f_2(\underline{X}_1, \underline{X}_3, \underline{X}_4).$$

Для исходных данных, приведенных в табл. 2, соответствующие схемы НКК для оценки верхней и нижней границ $\otimes X_5$ и $\otimes X_6$ принимают вид, представленный на рис. 3, *а*, *б*.

Далее, используя уравнения (3), можно рассчитать значения $\bar{X}_i(k)$ и $\underline{X}_i(k)$, определяющие изменение верхних и нижних границ переменных состояния концептов $X_i(k)$ во времени ($k = 1, 2, ...$). Выполнив соответствующие расчеты для схем НКК, представленных на рис. 3, *а*, *б*, для начальных условий (9) получим данные, приведенные в табл. 3, 4.

Как видно из табл. 3, 4, переменные состояния $\bar{X}_i(k)$ и $\underline{X}_i(k)$ за 7...8 тактов достигают своих установившихся значений, что является следствием выполнения условий устойчивости (7). В частности, для схемы на рис. 3, *а* имеем: $\left(\sum_{i,j=3}^{6} \bar{W}_{ij}^2\right)^{1/2} = \sqrt{1{,}85} = 1{,}36 < 2$, т. е. условие (7) выполняется. Таким образом, серый вектор состояния НСКК $\otimes X(k)$ сходится к установившемуся значению

$$\otimes X^*|_A = ([0{,}8;1],[0;0],[0{,}45;0{,}63],$$
$$[0{,}42;0{,}58],[0{,}25;0{,}43],[0{,}45;0{,}66]),$$

а искомые оценки рисков ИБ вследствие нарушения конфиденциальности и целостности информации будут определяться серыми числами:

$$\otimes X_5^*|_A \in [0{,}25;0{,}43]; \;\; \otimes X_6^*|_A \in [0{,}45;0{,}66]. \quad (13)$$

Значения "серости" для указанных установившихся значений переменных состояния следующие:

$$\Phi_1^*|_A = 0{,}2; \;\; \Phi_2^*|_A = 0; \Phi_3^*|_A = 0{,}18;$$
$$\Phi_4^*|_A = 0{,}16; \;\; \Phi_5^*|_A = 0{,}18; \;\; \Phi_6^*|_A = 0{,}21.$$

Следуя аналогичной процедуре, можно провести оценку диапазонов изменения рисков ИБ для сценария *B* (схема НСКК на рис. 4, *а*), сценария *C* (схема НСКК на рис. 4, *б*) и сценария *D* (схема НСКК на рис. 4, *в*).

После выполнения соответствующих расчетов с помощью уравнений (3) для начальных условий (10)—(12) получаем

для сценария B (рис. 4, *а*):

$$\otimes X_5^*|_B \in [0{,}23;0{,}42]; \;\; \otimes X_6^*|_B \in [0{,}41;0{,}65]; \quad (14)$$

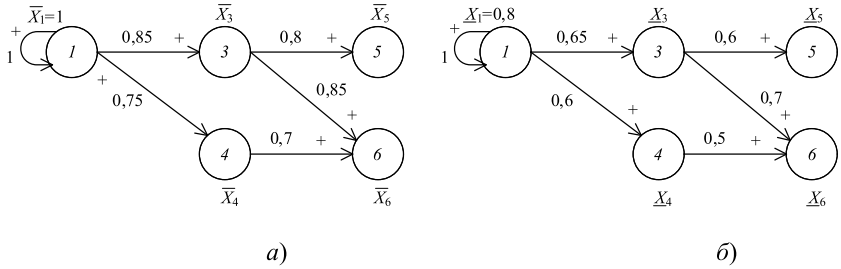

Рис. 3. Схемы НКК для оценки верхней и нижней границ рисков ИБ

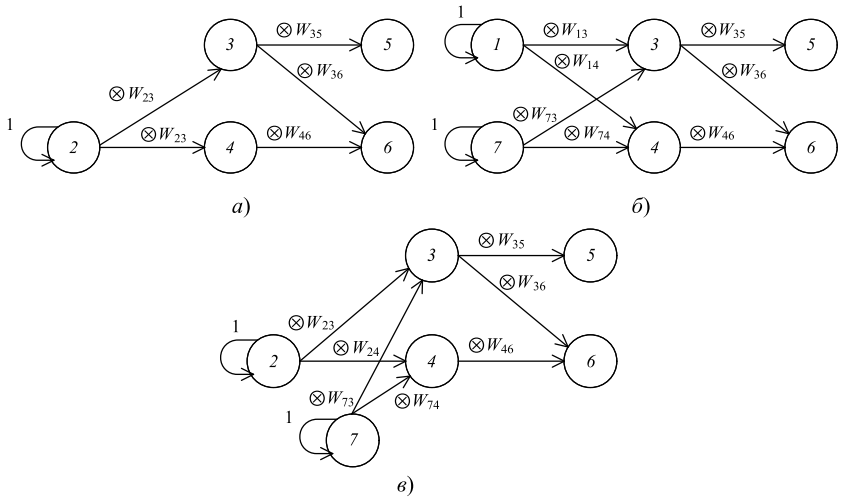

Рис. 4. Схемы НСКК для оценки рисков ИБ

для сценария C (рис. 4, *б*):

$$\otimes X_5^*|_C \in [0{,}1;\ 0{,}17];\ \otimes X_6^*|_C \in [0{,}22;\ 0{,}28]; \quad (15)$$

для сценария D (рис. 4, *в*):

$$\otimes X_5^*|_D \in [0{,}09;\ 0{,}15];\ \otimes X_6^*|_D \in [0{,}17;\ 0{,}22]. \quad (16)$$

В целях большей наглядности представим полученные результаты в виде диаграмм (рис. 5, *а*, *б*), где по оси абсцисс отложены значения чисел $\otimes X_5$ и $\otimes X_6$, а по оси ординат — указания на соответствующий сценарий (вариант) моделирования.

Как видно из рис. 5, обе рассмотренные угрозы ("НСД" и "Вредоносное программное воздействие") при отсутствии дополнительных контрмер по защите информации (сценарии *A* и *B*) приводят к значительным рискам, причем ущерб от нарушения целостности информации ($\otimes X_6$) превышает ущерб от нарушения ее конфиденциальности ($\otimes X_5$). Применение дополнительных контрмер позволяет в 2—2,5 раза снизить соответствующие риски. Диапазон интервальных оценок ("серость" чисел $\otimes X_5$ и $\otimes X_6$) при переходе от стратегии *A* и *B* к стратегиям *C* и *D* при этом уменьшается примерно в той же пропорции, т. е. в 2,5—3 раза, что и абсолютные значения верхней и нижней границ этих чисел.

В целом, на основе полученных результатов можно сделать следующие общие выводы:

1) применение НСКК позволяет перейти от "точечных" оценок мнений экспертов (что обычно подвергается сомнению) к более мягким интервальным оценкам исходных данных и, как следствие, к получению интервальных оценок конечных результатов, что является, с одной стороны, более достоверным, а с другой стороны, предоставляет ЛПР больший материал для принятия окончательного решения с учетом его опыта и предпочтений;

2) рассмотренные выше интервальные оценки в представлении исходных данных (табл. 2) могут, вообще говоря, отражать не "осторожность" конкретного эксперта в оценке силы взаимосвязей между концептами, а разброс мнений группы экспертов, имеющих свое собственное представление об изучаемой проблеме;

3) являясь расширением классических НКК Б. Коско, НСКК сохраняют наглядность, интерпретируемость и способность к обучению на реальных данных, т. е. общепризнанные преимущества технологий когнитивного моделирования сложных, плохо формализуемых систем;

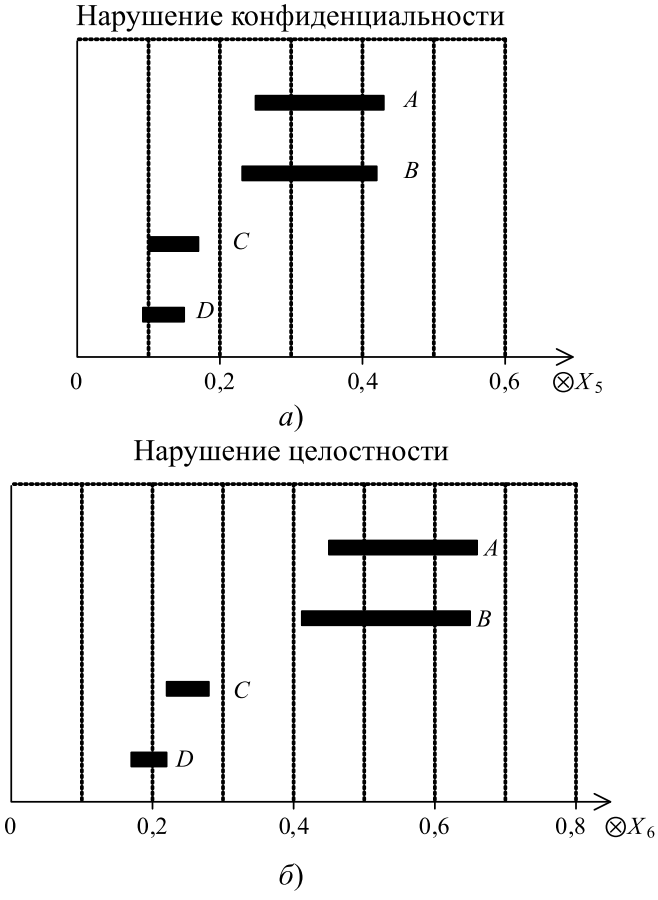

Рис. 5. Диаграммы значений рисков ИБ для различных сценариев

4) следующим шагом в исследовании возможностей применения НСКК для решения задачи оценки информационных рисков могло бы быть применение интуиционистских НКК [20], позволяющих отразить в интервальных оценках ("серых" числах) степень нерешительности (неуверенности, сомнения) экспертов в правильности этих оценок, т. е. внести элементы психологического анализа в процедуру получения этих оценок и соответственно моделирования плохо формализуемых процессов.

Заключение

Предложен подход к оценке информационных рисков в компьютерных системах, основанный на применении технологии когнитивного моделирования с использованием нечетких серых (интервальных) когнитивных карт. В отличие от классических способов построения нечетких когнитивных карт, в данном случае для оценки силы взаимосвязей между концептами используются интервальные оценки ("серые" числа), характеризующие некоторую меру естественной неопределенности (размытости) в суждениях эксперта или группы экспертов относительно взаимовлияния указанных концептов. В качестве численного примера построения и анализа НСКК рассмотрена задача оценки рисков (потенциального ущерба) от нарушения конфиденциальности и целостности информации, вызванных воздействием на информационные активы угроз типа "Несанкционированный доступ" и "Вредоносное программное воздействие/вирусы". Проанализированы основные этапы реализации соответствующей процедуры когнитивного моделирования. Отмечаются несомненные преимущества применения НСКК для решения задачи оценки информационных рисков, связанные с получением более достоверных оценок исходных данных и предоставлением лицу, принимающему решения, больше степеней свободы для принятия окончательного и более обоснованного решения по существу изучаемого вопроса.

Список литературы

1. **Петренко С. А., Симонов С. В.** Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2005. 384 с.

2. **Астахов А. М.** Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

3. **Аникин И. В.** Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях. Казань: Ред.-издат. центр "Школа", 2015. 224 с.

4. **Kosko B.** Fuzzy Cognitive Maps // Intern. Journal of Man-Machine Studies. 1986. Vol. 1. P. 65—75.

5. **Силов В. Б.** Принятие стратегических решений в нечеткой обстановке. М.: ИНПРО-РЕС, 1995. 228 с.

6. **Stylios C. D., Georgopoulos V. C., Groumpos P. P.** Introducing the theory of fuzzy cognitive maps in distributed systems // Proc. of the Twelfth IEEE Intern. Symposium on Intelligent Control, 16—18 July 1997, Istanbul, Turkey, 1997. P. 55—60.

7. **Papageorgiou E. I.** Review of Fuzzy Cognitive Maps Research During the Last Decade // IEEE Trans. on Fuzzy Systems. 2013. Vol. 21, N. 1. P. 66—79.

8. **Papageorgiou E. I.** (Ed.) Fuzzy Cognitive Maps for Applied Sciences and Engineering: From Foundations to Extensions and Learning Algorithms // Intelligent Systems Reference Library 54, Springer Science & Business Media. 2014. Vol. 54. 411 p.

9. **Гузаиров М. Б., Васильев В. И., Кудрявцева Р. Т.** Системный анализ информационных рисков с применением нечетких когнитивных карт // Инфокоммуникационные технологии. 2007. Т. 5, № 4. С. 42—48.

10. **Степанова Е. С., Машкина И. В., Васильев В. И.** Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности // Известия ЮФУ. Технические науки. Тематич. выпуск "Информационная безопасность". 2010. № 11 (112). С. 31—40.

11. **Ажмухамедов И. М.** Динамическая нечеткая когнитивная модель оценки уровня информационной безопасности информационных активов вуза // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика, 2012, № 2. С. 137—141.

12. **Yebiah-Bouteng E. O.** Using fuzzy cognitive maps (FCMs) to evaluate the vulnerabilities with ICT assets disposal policies // Intern. Journal on Electrical & Computer Science (IJECS-IJENS). 2012. Vol. 12, N. 05. P. 20—31.

13. **Васильев В. И., Вульфин А. М., Кудрявцева Р. Т.** Анализ и управление рисками информационной безопасностью с использованием технологии когнитивного моделирования // Доклады ТУСУР. 2017. Т. 20, № 4. С. 61—66.

14. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps // Expert Systems with Applications. Dec. 2010. Vol. 37, Iss. 12. P. 7581—7588.

15. **Shishkin V. M., Savkov S. V.** The Method of Interval Estimation of Risk-Analysis System // Proc. of the Second Intern. Conference on Security of Information and Networks (SIN'09), Oct. 6—10. 2009. Famagusta, North Cyprus, 2009. P. 3—7.

16. **Савков С. В., Шишкин В. М.** Разработка системы интервального оценивания информационных рисков // Изв. вузов. Приборостроение. 2011. Т. 54, № 9. С. 38—43.

17. **Deng J. L.** Introduction to grey systems theory // Journal on Grey Systems, 1989. N. 1. P. 1—24.

18. **Boutalis Y., Kottas T., Christodoulou M.** On the existence and uniqueness of solutions for the concept values in fuzzy cognitive maps // Decision and Control, 2008. CDC 2008. 47th IEEE Conference, Cancun: IEEE. 2008. P. 98—104.

19. **Knight Ch. J. K., Lloyd D. J. B., Penn A. S.** Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points. URL: www.inescid.pt/indicators/Ficherous/175.pdf, свободный (дата обращения: 08.04.2018).

20. **Papageorgiou E. I., Iakovidis D.** Intuitionistic fuzzy cognitive maps //IEEE Trans. on Fuzzy Systems, DOI: 10.1109/TFUZZ.2012.2214224.

V. I. Vasilyev, Professor, e-mail: vasilyev@ugatu.ac.ru,
A. M. Vulfin, Professor, e-mail: vulfin.alexey@gmail.com,
M. B. Guzairov, Professor, e-mail: guzairov@ugatu.su,
A. D. Kirillova, Master of Sc., e-mail: kirillova.andm@gmail.com,
Ufa State Aviation Technical University

Interval Estimation of Information Risks with use of Fuzzy Grey Cognitive Maps

The possibility of obtaining the interval quantitative estimates of information security risks with use of Fuzzy Grey Cognitive Maps in considered. The issues of constructing the fuzzy grey cognitive maps on the basic of knowledge processing and experts experience are discussed. The peculiarities of applying the given class of cognitive models on the example of evaluating the information risks are considered.

Keywords: *information risks, cognitive modelling, interval estimates, fuzzy grey cognitive maps*

DOI: 10.17587/it.24.657-664

References

1. **Petrenko S. A., Simonov S. V.** *Upravlenie informatsionnymi riskami. Ekonomicheski opravdannaya bezopasnost* (Information risk management. Economically proved security), Moscow, DMK Press, 2005. 384 p. (in Russian).

2. **Astahov A. M.** *Iskusstvo upravleniya informatsionnymi riskami* (The art of information risk management), Moscow, DMK Press, 2010. 312 p. (in Russian).

3. **Anikin I. V.** *Metody otsenki i upravleniya riskami informatsionnoj bezopasnosti v korporativnyh informatsionnyh setyah* (Methods for assessing and managing information security risks in corporate information networks), Kazan, Red.-izdat. centr "Shkola", 2015, 224 p. (in Russian).

4. **Kosko B.** Fuzzy Cognitive Maps, *Intern. Journal of Man-Machine Studies*, 1986, vol. 1, pp. 65—75.

5. **Silov V. B.** *Prinyatie strategicheskih reshenij v nechetkoj obstanovke* (Making strategic decisions in a fuzzy environment), Moscow, INPRO-RES, 1995, 228 p. (in Russian).

6. **Stylios C. D., Georgopoulos V. C., Groumpos P. P.** Introducing the theory of fuzzy cognitive maps in distributed systems, *Proc. of the Twelfth IEEE Intern. Symposium on Intelligent Control,* 16—18 July 1997, Istanbul, Turkey, 1997, pp. 55—60 (in Russian).

7. **Papageorgiou E. I.** Review of Fuzzy Cognitive Maps Research During the Last Decade, *IEEE Trans. on Fuzzy Systems*, 2013, vol. 21, no. 1, pp. 66—79.

8. **Papageorgiou E. I.** (Ed.) Fuzzy Cognitive Maps for Applied Sciences and Engineering: From Foundations to Extensions and Learning Algorithms, *Intelligent Systems Reference Library 54*, Springer Science & Business Media, 2014, vol. 54. 411 p.

9. **Guzairov M. B., Vasilyev V. I., Kudryavtseva R. T.** Sistemnyj analiz informatsionnyh riskov s primeneniem nechetkih kognitivnyh kart (The system analysis of information risks with application of fuzzy cognitive maps) *Infokommunikatsionnye Tekhnologii*, 2007, vol. 5, no. 4, pp. 42—48 (in Russian).

10. **Stepanova E. S., Mashkina I. V., Vasilev V. I.** Razrabotka modeli ugroz na osnove postroeniya nechetkoj kognitivnoj karty dlya chislennoj otsenki riska narusheniya informatsionnoj bezopasnosti (Development of threats model on the basis of fuzzy cognitive maps contraction for information risk numerical estimation), *Izvestiya YuFU. Tekhnicheskie nauki/Tematich. vypusk "Informatsionnaya bezopasnost",* 2010, no. 11 (112), pp. 31—40 (in Russian).

11. **Azhmuhamedov I. M.** Dinamicheskaya nechetkaya kognitivnaya model otsenki urovnya informatsionnoj bezopasnosti informatsionnyh aktivov vuza (Dynamic fuzzy cognitive model for assessing the level of information security of university's information assets), *Vestnik AGTU. Ser.: Upravlenie, Vychislitel'naya Tehnika i Informatika*, 2012, no. 2, pp. 137—141 (in Russian).

12. **Yebiah-Bouteng E. O.** Using fuzzy cognitive maps (FCMs) to evaluate the vulnerabilities with ICT assets disposal policies, *Intern. Journal on Electrical & Computer Science (IJECS-IJENS)*, 2012, vol. 12, no. 05, pp. 20—31.

13. **Vasilyev V. I., Vulfin A. M., Kudryavtseva R. T.** Analiz i upravlenie riskami informatsionnoj bezopasnostju s ispol'zovaniem tehnologii kognitivnogo modelirovaniya (Analysis and management of information security risks with using cognitive modeling technology), *Doklady TUSUR*, 2017, vol. 20, no. 4, pp. 61—66 (in Russian).

14. **Salmeron J. L.** Modelling grey uncertainty with Fuzzy Grey Cognitive Maps, *Expert Systems with Applications*, Dec. 2010, vol. 37, iss. 12, pp. 7581—7588.

15. **Shishkin V. M., Savkov S. V.** The Method of Interval Estimation of Risk-Analysis System, *Proc. of the Second Intern. Conference on Security of Information and Networks (SIN'09),* Oct. 6—10, 2009, Famagusta, North Cyprus, 2009, pp. 3—7.

16. **Savkov S. V., Shishkin V. M.** Razrabotka sistemy interval'nogo otsenivaniya informatsionnyh riskov (Development of a system of interval estimation of information risks), *Izv. vuzov. Priborostroenie*, 2011, vol. 54, no. 9, pp. 38—43 (in Russian).

17. **Deng J. L.** Introduction to grey systems theory, *Journal on Grey Systems*, 1989, no. 1, pp. 1—24.

18. **Boutalis Y., Kottas T., Christodoulou M.** On the existence and uniqueness of solutions for the concept values in fuzzy cognitive maps, *Decision and Control, 2008. CDC 2008. 47th IEEE Conference*, Cancun, IEEE, 2008, pp. 98—104.

19. **Knight Ch. J. K., Lloyd D. J. B., Penn A. S.** Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points, available at: www.inescid.pt/indicators/Ficherous/175.pdf (accessed 8 April 2018).

20. **Papageorgiou E. I., Iakovidis D.** Intuitionistic fuzzy cognitive maps, *IEEE Trans. on Fuzzy Systems*, DOI: 10.1109/TFUZZ.2012.2214224.