УДК 004.89 DOI: 10.17587/it.24.266-273

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,
Уфимский государственный авиационный технический университет

Оценка рисков информационной безопасности с использованием нечетких продукционных когнитивных карт[1]

Дана краткая характеристика современных подходов к анализу рисков информационной безопасности, связанных с качественной и количественной оценкой рисков. Отмечаются преимущества использования для этих целей нечетких когнитивных карт, обладающих, помимо своей наглядности и удобства восприятия, возможностью моделирования плохо формализуемых ситуаций и систем в условиях неопределенности, что является одним из основных препятствий при решении задач защиты информации.

Перечислены основные классы нечетких когнитивных карт, а также проблемы, возникающие при их построении и применении для решения задач анализа и управления информационными рисками. Приводятся обоснования в пользу выбора нечетких продукционных когнитивных карт. Даны базовые понятия и определения, лежащие в основе построения данного класса нечетких когнитивных карт. Рассмотрены характерные этапы процедуры оценки информационных рисков с использованием нечетких продукционных когнитивных карт. На примере оценки последствий от реализации вирусной атаки на информационный ресурс, размещенный на рабочей станции (АРМ оператора), анализируются особенности решения данной задачи с помощью таких карт. Обсуждается задача оптимального (рационального) выбора контрмер, имеющих своей целью уменьшение (или снижение до некоторого допустимого уровня) возможного ущерба от воздействия угрозы.

Ключевые слова: *информационная безопасность, анализ и управление риском, когнитивное моделирование, нечеткая продукционная когнитивная карта, оценка риска, контрмеры по защите информации*

Введение

Проблема обеспечения информационной безопасности приобретает в последние годы все большую остроту. Следствием этого является повышенное внимание общества и государства к созданию нормативной и законодательной базы, регламентирующей основные вопросы проведения аудита и оценки защищенности информационных систем, разработки, внедрения и эксплуатации систем защиты информации, успешно противодействующих возможным внешним и внутренним угрозам. За последние 10—15 лет создана обширная система национальных стандартов информационной безопасности (ГОСТ Р ИСО / МЭК 15408, 27001 — 27005, 15335, 18405, СТО БР ИББС и др.), в той или иной мере охватывающих общие вопросы анализа и управления информационными рисками.

Существует достаточно большое число методов и алгоритмов, позволяющих получить оценку уровня риска с последующим формированием рекомендаций по выбору необходимых мер защиты информации [1, 2]. Методы, предназначенные для качественной оценки рисков (такие, как метод экспертных оценок или схема нечеткого логического вывода), базируются на неполной исходной информации и дают общую, предварительную оценку уровня защищенности системы. Методы, основанные на количественной оценке рисков (например, методы ситуационного анализа, марковские модели, нейронные сети и др.), требуют для своего использования более полной информации об исследуемой системе и позволяют прогнозировать не только уровень риска, но и ожидаемый потенциальный ущерб от действия угроз, что может явиться базой для принятия более обоснованных решений по снижению уровня риска.

Важное место среди методов, направленных на получение качественной оценки рисков, за-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-48-020095.

нимают методы когнитивного моделирования, предназначенные для исследования плохо формализуемых ситуаций и проблем путем построения нечетких когнитивных карт (Fuzzy Cognitive Maps, FCM) [3—5]. Нечеткие когнитивные карты (НКК) впервые были предложены Б. Коско в 1986 г. в его широко известной работе [6]. Сегодня данный класс моделей существенно расширился и включает в себя обобщенные НКК [7, 8], реляционные НКК [5, 9], интервальные ("серые") НКК [4, 5], продукционные НКК [10, 11], НКК в базисе "истина—ложь—неопределенность" [12] и многие другие модификации НКК [4, 5, 13]. Можно указать достаточно большое число примеров успешного применения НКК для решения задач анализа и управления информационными рисками [14—18]. В основе построения этих моделей оценки рисков используется так называемая трехфакторная формула риска:

$$\text{Риск} = \text{Угроза} * \text{Уязвимость} * \text{Ценность ресурса}, \quad (1)$$

характеризующая происхождение и основные составляющие формирования риска. В данной работе рассмотрены особенности применения одного из перспективных классов когнитивных моделей — нечетких продукционных когнитивных карт для оценки рисков информационной безопасности. Основное внимание уделено методологическим аспектам решения данной задачи с выделением тех сложностей и узловых моментов, с которыми встречается технология когнитивного моделирования.

1. Нечеткие продукционные когнитивные карты

Нечеткие продукционные когнитивные карты (НПКК), или нечеткие когнитивные карты, основанные на правилах (*Rule Based Fuzzy Cognitive Maps*), впервые предложенные в 1999 г. Х. Карвало и Х. Томе [10], привлекают внимание многих исследователей в силу ряда своих несомненных преимуществ. Во-первых, они представляют собой действительно нечеткие системы, позволяющие описать качественное поведение сложных систем и их компонентов с помощью системы нечетких правил; во-вторых, они обладают значительной общностью, допуская использование различных видов нечетких связей (отношений), включая обратные связи, между входящими в их состав концептами; в-третьих, они учитывают фактор времени, позволяя моделировать динамику сложных, плохо формализуемых систем.

Под *нечеткой продукционной когнитивной картой* обычно понимается ориентированный граф (орграф), задаваемый парой множеств:

$$K = \{C, F\}, \quad (2)$$

где $C = \{C_i\}$ ($i = 1, 2, ..., n$) — множество узлов (вершин) орграфа, называемых *концептами*; $F = \{F_{ij}\}$ ($i, j = 1, 2, ..., n$) — множество дуг — связей (отношений) между концептами; n — число концептов НПКК. Предполагается, что переменная состояния X_i каждого концепта C_i рассматривается как лингвистическая переменная, принимающая значения из некоторого нечеткого терм-множества $\{T_{i1}, T_{i2}, ..., T_{im}\}$, подмножества (термы) которого T_{ik} ($k = 1, 2, ..., m$), в свою очередь, задаются функциями принадлежности: $T_{ik} = \{(\mu_{ik}(X_i), X_i)\}$, $\mu_{ik}: X_i \to [0, 1]$, где $X_i \in [0, 1]$ или $X_i \in [-1, 1]$. Различают два вида концептов: *уровни* (levels), которые представляют абсолютные значения состояния концепта в данный момент времени, и *вариации* (variations), которые представляют изменения состояния концепта по отношению к предыдущему моменту времени. Последнее важно для описания динамики поведения исследуемых систем. Для определения взаимного влияния концептов ($C_i \to C_j$) используются нечеткие продукционные правила, позволяющие представить предпосылки (условия) и заключения нечетких правил на основе нечетких множеств.

На рис. 1 приведен пример задания нечетких правил для определения влияния концепта C_i на концепт C_j.

Предполагается, что переменные X_i и X_j, характеризующие состояния концептов C_i и C_j, могут принимать значения из терм-множества {Очень_высокая (*VH*), Высокая (*H*), Средняя (*M*), Низкая (*L*), Очень_низкая (*VL*)}, задаваемые с помощью соответствующих функций принадлежности. Для реализации процедуры нечеткого логического вывода (применительно к конкретному "четкому" значению входной переменной X_i^* и получению "четкого" значения переменной X_j^* на выходе)

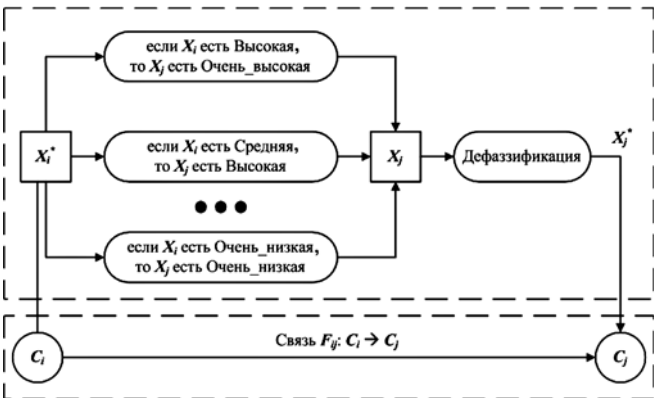

Рис. 1. Пример влияния концепта C_i на концепт C_j в НПКК

можно воспользоваться алгоритмом Мамдани [19]. Особенность реализации вычислительного процесса в данном случае состоит в выполнении последовательных преобразований (четкое значение X_i^* → фаззификация → нечеткий логический вывод → получение нечеткого множества для X_j → дефаззификация, вычисление четкого значения X_j^*) и т.д. для каждой последующей пары концептов $C_j \to C_{j+1} \to ...$ на пути следования в НПКК. На этапе дефаззификации (приведения к четкости) выходной переменной X_j используется метод взвешенного среднего:

$$X_j^* = \frac{\sum_{l=1}^{m} \alpha_l X_{jl}^o}{\sum_{l=1}^{m} \alpha_l}, \qquad (3)$$

где X_j^* — дефаззифицированное значение переменной состояния концепта C_j; X_{jl}^o (l = 1, 2, ..., m) — центральные значения нечетких подмножеств (термов) переменной X_j; α_l — уровень активности l-го правила, соответствующий конкретному значению входной переменной X_i^*; m — число термов (подмножеств) лингвистической переменной X_j (в примере m = 5).

В общем случае, если на концепт C_j оказывают непосредственное влияние k предшествующих концептов C_i, C_{i+1}, ..., C_{i+k-1}, то нечеткие продукционные правила принимают более сложный вид, например:

П$_1$: если X_i есть Высокая и X_{i+1} есть Высокая и ... и X_{i+k-1} есть Высокая, то X_j есть Очень_высокая;

...

П$_N$: если X_i есть Очень_низкая и X_{i+1} есть Очень_низкая и ... и X_{i+k-1} есть Очень_низкая, то X_j есть Очень_низкая;

Процедура нечеткого логического вывода здесь реализуется аналогично. Для выполнения операции логического И можно воспользоваться оператором MIN.

Основной недостаток НПКК — резкое возрастание числа продукционных правил при возрастании числа концептов. Так, в предыдущем примере для определения состояния одного концепта C_j (переменной X_j) при двух предшествующих взаимодействующих с ним концептах C_i, C_{i+1}, описываемых соответственно переменными состояния X_i и X_{i+1}, имеем k = 2, m = 5, а общее число указанных выше правил равно m^2 = 25. Конечно, не все эти правила будут активными (т. е. $\alpha_l \neq 0$) для конкретных "четких" значений входов X_i^* и X_{i+1}^*, поступающих с выходов концептов C_i и C_{i+1}. Более того, всегда активизируются лишь четыре правила, остальные правила не срабатывают. Тем не менее проблема высокой размерности базы правил НПКК остается и, вообще говоря, для ее решения необходимо применять специальные методы и способы [20].

2. Методика оценки риска с помощью НПКК (пример применения)

Допустим, что требуется оценить риск от возможного воздействия вирусной атаки на некоторый информационный ресурс, размещаемый на сервере, рассматривая в качестве уязвимости отсутствие обновлений антивирусного ПО.

Возвращаясь к упомянутой выше трехфакторной формуле риска (1), представим соответствующую ей схему расчета в виде НПКК на рис. 2, где C_1 — угроза; C_2 — уязвимость; C_3 — информационный ресурс; C_4 — реализация угрозы; C_5 — риск (потенциальный ущерб), соответственно X_1 — вероятность возникновения угрозы; X_2 — вероятность наличия уязвимости; X_3 — ценность (стоимость) информационного ресурса; X_4 — вероятность успешной реализации угрозы; $X_5 = R$ — уровень риска (значение ожидаемого потенциального ущерба).

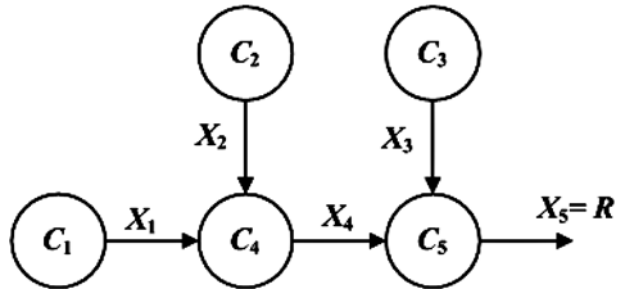

Рис. 2. Схема НПКК для оценки риска

Используя аппарат нечеткой логики, будем полагать, что каждая из указанных переменных состояния представляет собой лингвистическую переменную, принимающую одно из следующих значений: *L* — Low (Низкая (-ий)); *M* — Medium (Средняя(-ий)); *MH* — Medium High (Достаточно высокая (-ий)); *H* — High (Высокая (-ий)); *VH* — Very High (Очень высокая (-ий)). Каждое из этих нечетких подмножеств задается, в свою очередь, собственной функцией принадлежности (рис. 3).

На рис. 3 функции принадлежности нечетких подмножеств НПКК $\mu(X_1)$, $\mu(X_2)$, $\mu(X_3)$ имеют треугольную форму, а функции принадлежности $\mu(X_4)$, $\mu(X_5)$ являются столбчатыми (singletons).

Систему нечетких продукционных правил, описывающих состояние концептов C_4 и C_5, можно записать в виде:

концепт C_4:

$П_1$: Если X_1 есть Низкая и X_2 есть Низкая, то X_4 есть Низкая;

...

$П_{25}$: Если X_1 есть Очень_высокая и X_2 есть Очень_высокая, то X_4 есть Очень_высокая;

концепт C_5:

$П_{26}$: Если X_3 есть Низкая и X_4 есть Низкая, то X_5 есть Низкая;

...

$П_{50}$: Если X_3 есть Очень_высокая и X_4 есть Очень_высокая, то X_5 есть Очень_высокая.

Всего имеем: 2·5·5 = 50 правил, которые удобно представить в виде так называемых матриц риска (или таблиц решений) [21] (табл. 1, 2).

В клетках табл. 1 записаны соответствующие значения (термы) переменной X_4, в клетках табл. 2 — значения (термы) переменной $X_5 = R$, т. е. уровня риска.

Допустим, что в конкретном рассматриваемом случае входные переменные НПКК (т.е. три базовых фактора риска) принимают значения: $X_1^* = 0{,}85$, $X_2^* = 0{,}9$, $X_3^* = 0{,}75$. Обратившись к рис. 2 и приведенным таблицам, видим, что переменные X_1, X_2, X_3, X_4 принимают только значения MH и H, т. е. из 50 правил активными окажутся только 8 правил, соответствующих выделенным блокам из четырех соседних клеток в правом верхнем углу табл. 1 и 2. Таким образом, редуцированная система нечетких продукционных правил принимает вид:

1) если $X_1 = H$ и $X_2 = H$, то $X_4 = H$;
2) если $X_1 = H$ и $X_2 = VH$, то $X_4 = H$;
3) если $X_1 = VH$ и $X_2 = H$, то $X_4 = H$;
4) если $X_1 = VH$ и $X_2 = VH$, то $X_4 = VH$;

} концепт C_4

5) если $X_3 = H$ и $X_4 = H$, то $X_5 = H$;
6) если $X_3 = H$ и $X_4 = VH$, то $X_5 = H$;
7) если $X_3 = VH$ и $X_4 = H$, то $X_5 = H$;
8) если $X_3 = VH$ и $X_4 = VH$, то $X_5 = VH$.

} концепт C_5

Используя операции нечеткой логики [21] для заданных "четких" значений переменных X_1^*, X_2^*, X_3^*, получим значения уровней активностей данных правил:

$$\alpha_1 = 0{,}33;\ \alpha_2 = 0{,}67;\ \alpha_3 = \alpha_4 = 0{,}25;$$
$$\alpha_5 = 0{,}33;\ \alpha_6 = 0{,}67;\ \alpha_7 = \alpha_8 = 0{,}17.$$

Объединяя правила 1—4 и 5—8 с помощью логической связки ИЛИ (т.е. операции MAX), получаем функции принадлежности для переменных X_4 и X_5 (рис. 4).

Применяя формулу (3), вычисляем дефаззифицированные ("четкие") значения переменных

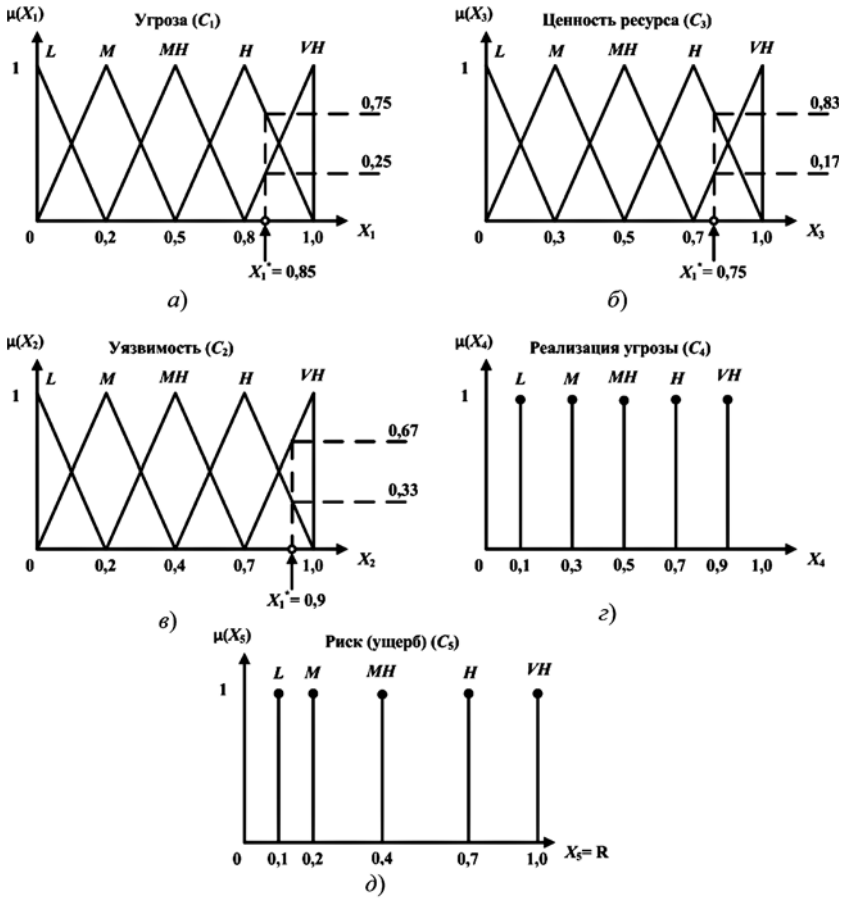

Рис. 3. Функции принадлежности нечетких множеств

X_1 \ X_2	L	M	MH	H	VH
VH	MH	H	H	H	VH
H	M	MH	H	H	H
MH	M	M	MH	MH	H
M	L	M	M	M	MH
L	L	L	L	M	M

Таблица 1. Реализация угрозы С4

X_3 \ X_4	L	M	MH	H	VH
VH	M	M	MH	H	VH
H	L	M	MH	H	H
MH	L	M	M	MH	MH
M	L	L	M	M	M
L	L	L	L	L	L

Таблица 2. Риск (ущерб) С5

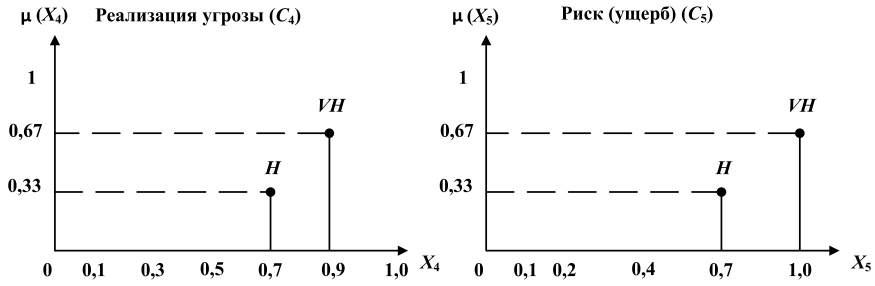

Рис. 4. Функции принадлежности нечетких переменных X_4 и X_5

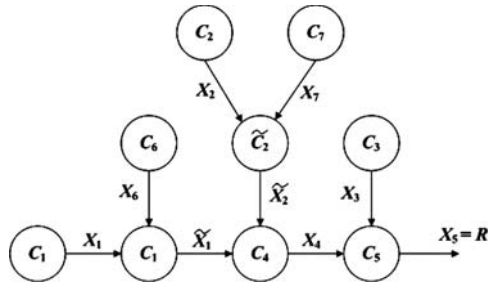

Рис. 5. Схема НПКК для оценки риска с учетом контрмер

$X_4^* = 0{,}83$; $X_5^* = 0{,}9$. Следовательно, искомое значение уровня риска R, т.е. ожидаемого потенциального ущерба от действия угрозы, равно 90 %.

Допустим теперь, что за счет применения специальных мер по защите информации (контрмер) требуется снизить уровень риска R до среднего (M) или низкого (L). В целях анализа эффективности различных способов управления риском воспользуемся НПКК, приведенной на рис. 5.

Здесь C_1, C_2, C_3 — соответственно угроза, уязвимость и информационный ресурс (как и в предыдущем примере, речь идет об оценке последствий от реализации вирусной атаки); C_4 и C_5 — реализация угрозы и риск (потенциальный ущерб); C_6 и C_7 — ресурсы, выделяемые на парирование (блокирование) угрозы и устранение уязвимости; $\widetilde{C}_1$ и $\widetilde{C}_2$ — модифицированные (скомпенсированные за счет принятия контрмер) угроза и уязвимость. Соответственно в качестве переменных состояния концептов выступают: X_1 — вероятность возникновения угрозы; $\widetilde{X}_1$ — вероятность скомпенсированной угрозы; $\widetilde{X}_2$ — вероятность скомпенсированной уязвимости; X_3 — ценность (стоимость) информационного ресурса; X_4 — вероятность успешной реализации угрозы; $X_5 = R$ — уровень риска (значение ожидаемого потенциального ущерба); X_6 и X_7 — затраты на парирование угрозы и уязвимости.

То обстоятельство, что вновь введенные промежуточные концепты $\widetilde{C}_1$ и $\widetilde{C}_2$, как и концепты C_4 и C_5, являются "двухвходовыми", позволяет представить базу нечетких продукционных правил НПКК в виде совокупности четырех раздельных таблиц, две из которых (приведенные выше) характеризуют изменение состояния концептов C_4 и C_5 в зависимости от состояния смежных концептов: $X_1 \times \widetilde{X}_2 \to X_4$ и $X_3 \times X_4 \to X_5$.

Дополнительные две таблицы будут определять состояния новых концептов $\widetilde{C}_1$ и $\widetilde{C}_2$ с учетом добавленных в НПКК внешних управляющих факторов C_6 и C_7: $X_1 \times X_6 \to \widetilde{X}_1$ и $X_2 \times X_7 \to \widetilde{X}_2$ (табл. 3 и 4).

Будем полагать, что функции принадлежности для нечетких переменных X_1, X_2, X_3, X_4, X_5 имеют тот же вид, что и на рис. 3. Для простоты принимаем, что функции принадлежности для переменных $\widetilde{X}_1$ и $\widetilde{X}_2$ имеют тот же вид, что и функции принадлежности переменных X_1 и X_2, а функции принадлежности для переменных X_6 и X_7 совпадают по внешнему виду с функцией принадлежности для переменной X_3 (напомним, что по оси абсцисс на графике рис. 3, *в*, отложены нормированные значения переменной).

Проведем оценку риска с помощью НПКК, представленной на рис. 5, используя следующие исходные данные: $X_1^* = 0{,}85$; $X_2^* = 0{,}9$; $X_3^* = 0{,}75$ (как и в предыдущем примере); $X_6^* = 0{,}9$; $X_7^* = 0{,}85$ (управляющие факторы). Легко видеть, что, как и ранее, при реализации механизма нечеткого логического вывода задействуется лишь часть правил, приведенных в табл. 1—4, т.е. для расчетов можно воспользоваться схемой, представленной на рис. 6.

Выполнив необходимые вычисления по схеме рис. 6 в соответствии с алгоритмом Мамдани [21], используя при этом для реализации логических операций И и ИЛИ операторы MIN и MAX, а при фаззификации — метод взвешенного среднего (3), полу-

X_1 \ X_6	L	M	MH	H	VH
VH	VH	H	MH	M	M
H	H	MH	MH	M	L
MH	MH	M	M	M	L
M	M	L	L	L	L
L	L	L	L	L	L

Таблица 3. Скомпенсированная угроза

X_2 \ X_7	L	M	MH	H	VH
VH	VH	H	MH	M	M
H	H	MH	MH	M	L
MH	MH	M	M	M	L
M	M	L	L	L	L
L	L	L	L	L	L

Таблица 4. Скомпенсированная уязвимость

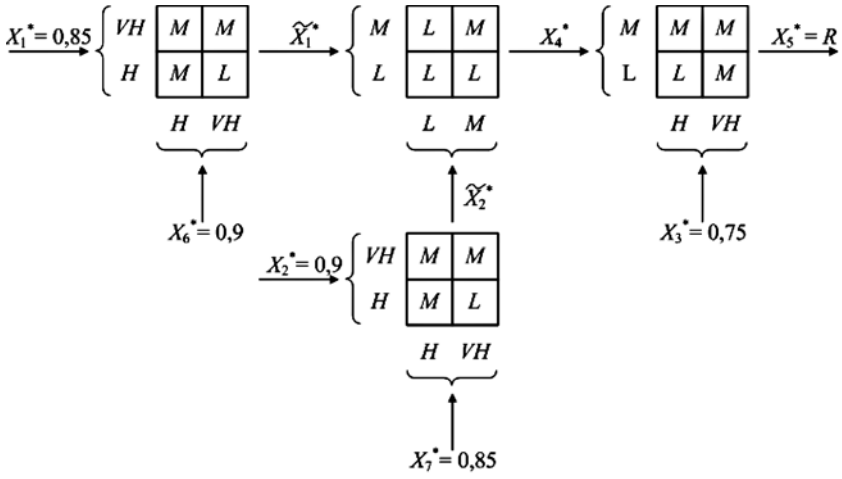

Рис. 6. Схема нечеткого логического вывода для оценки риска с учетом управляющих факторов

чим "четкие" (дефаззифицированные) значения промежуточных и выходной переменных НПКК:

$$\widetilde{X}_1^* = 0{,}13;\ \widetilde{X}_2^* = 0{,}16;\ X_4^* = 0{,}23;\ X_5^* = 0{,}26.$$

Таким образом, уровень риска R в результате принятия специальных мер по защите информации снизился с 90 до 26 %, т.е. в 3,5 раза.

Аналогичным образом можно проводить оценку риска для других исходных данных, отвечая на вопрос "Что будет, если...", рассматривая различные сценарии воздействия угроз и реализации защитных контрмер. Возможная постановка задачи — использование НПКК для выбора оптимального (рационального) способа защиты информации с учетом ограничений на значение риска и выделяемые ресурсы на реализацию контрмер. В данном случае можно рассматривать два варианта постановки задачи:

1) $R \to \min$ при $S_\Sigma \leqslant S_{\text{доп}}$;

2) $S_\Sigma \to \min$ при $R \leqslant R_{\text{доп}}$,

где S_Σ — суммарный объем средств (ресурсов), выделяемых на реализацию защитных мер (в рассмотренном примере $S_\Sigma = X_6^* + X_7^*$); $S_{\text{доп}}$ — заданный (максимально допустимый) объем выделенных средств; $R_{\text{доп}}$ — заданный (максимально допустимый) уровень риска.

Заключение

В данной работе рассмотрены особенности применения одного из перспективных классов когнитивных моделей — нечетких продукционных когнитивных карт (НПКК) для решения задачи оценки рисков информационной безопасности.

В основе построения данных моделей используется описание взаимодействия между концептами, образующими НПКК, с помощью системы нечетких правил (продукций), отражающих знания и опыт экспертов в данной предметной области.

На конкретном примере реализации вирусной атаки на информационный ресурс рассмотрены основные этапы исполнения алгоритма нечеткого логического вывода Мамдани — фаззификация исходных данных, работа с правилами, дефаззификация (приведение к четкости).

К числу преимуществ предложенного подхода к оценке рисков, помимо наглядности и учета факторов неопределенности, относятся также гибкость и универсальность использования НПКК, заключающиеся в возможности расширения перечня учитываемых угроз, уязвимостей, защищаемых информационных ресурсов, а также категорий оценки рисков по видам ущерба от нарушения конфиденциальности, целостности и доступности информации.

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. **Борисов В. В., Круглов В. В., Федулов А. С.** Нечеткие модели и сети. Изд. 2-е, стереотип. М.: Горячая линия — Телеком, 2012. 284 с.

4. **Glykos M. (Ed.)** Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications. Springer—Verlag, 2010.

5. **Papageorgiou E. (Ed.)** Fuzzy Cognitive Maps for Applied Science and Engineering: From Fundamentals to Extensions and Learning Algorithms. Springer-Verlag, 2014.

6. **Kosko B.** Fuzzy Cognitive Maps // Intern. Journal of Man-Machine Studies. 1986. Vol. 24. P. 65—75.

7. **Hagiwara M.** Extended Fuzzy Cognitive Maps // Proc. of the IEEE Conference on Fuzzy Systems, San-Diego, USA, 8—12 March, 1992. P. 161—172.

8. **Борисов В. В., Федулов А. С.** Обобщенные нечеткие когнитивные карты // Нейрокомпьютеры: разработка, применение. 2004. № 4. С. 3—20.

9. **Федулов А. С.** Нечеткие реляционные когнитивные карты // Известия РАН. Теория и системы управления. 2005. № 1. С. 120—132.

10. **Carvalho J. P., Tome J. A. B.** Rule Based Fuzzy Cognitive Maps: Fuzzy Causal Relations // Computational Intelligence for Modeling, Control and Automation: Evolutionary Computation & Fuzzy Logic for Intelligent Control, Knowledge Acquisition & Information Retrieval / Mohammadian (Ed.). — URL: www.inesc-id.pt/pt/indicadores/Ficheiros/1894.pdf (дата обращения: 24.09.2017).

11. **Борисов В. В., Федулов А. С., Устиненков Е. С.** Анализ динамики состояния сложных систем на основе обобщенных нечетких продукционных когнитивных карт // Нейрокомпьютеры: разработка, применение. 2007. № 1. С. 17—23.

12. **Kandasamy V., Smarandache F.** Fuzzy Cognitive Maps and Neutrosophic Cognitive Maps, 2003. URL: https://arxiv.org/ftp/math/papers/0311/0311063.pdf (дата обращения: 24.09.2017).

13. **Byung Sung Yoon, Jetter. A. S.** Comparative Analysis for Fuzzy Cognitive Mapping // 2016 Proceedings of PICMET'16: Technology for Social Innovation, 2016. P. 1897—1908.

14. **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.

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

16. **Ажмухаметов 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—142.

17. **Yeboah-Boateng E. O.** Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies // Intern. Journal on Electrical & Computer Sciences IJECS — IJENS. Oct. 2012. Vol. 12, N. 05. P. 20—31.

18. **Васильев В. И.** Интеллектуальные системы защиты информации: учеб. пособие для вузов. 3-е изд. М.: Инновационное машиностроение, 2017. 201 с.

19. **Mazarakis S., Matsavinos G., Groumpos P.** Simulating and Forecasting Qualitative Macroeconomic Models Using Rule-Based Fuzzy Cognitive Maps // Intern. Journal on Social, Behavioral, Economic, Business and Industrial Engineering. 2013. Vol. 7, N. 1. P. 147—152.

20. **Перминов Г. И., Леонова Н. В.** Применение нечеткой логики для решения когнитивной карты при использовании комбинации альтернатив // Аудит и финансовый анализ. 2014. № 4. С. 396—401.

21. **Shapiro A. F., Koissi M.-C.** Risk Assessment Applications of Fuzzy Logic, March 2015. URL: https://www.casact.org/education/annual/2015/presentations/C-13-Shapiro.pdf (дата обращения: 24.09.2017)

DOI: 10.17587/it.24.266-273

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

Evaluation of Information Security Risks with Use of Rule-Based Fuzzy Cognitive Maps

A brief overview of modern approaches to information security risk analysis connected with their qualitative evaluation is presented. The advantages of using fuzzy logic cognitive maps (FCM) for this purpose are besides their visualization and perception convenience also a possibility of modeling ill-defined situations and systems in the conditions of uncertainty. This circumstance is one of the main obstacles arising under their construction and application while solving the issues of information risk analysis and management.

The arguments for a choice of rule-based fuzzy cognitive maps (RBFCM) and the basic notions and definitions underlying the construction of this class of FCM are considered. The characteristic stages of information risk evaluation procedure with use of RBFCM are described. The example of evaluating the consequences from a virus attack action on some information asset with application of RBFCM is considered. The problem of optimal (rational) choice of countermeasures to decrease the possible loss from the threat action is discussed.

Keywords: *information security, risk analysis and management, cognitive modeling, rule-based fuzzy cognitive map, risk evaluation, countermeasures on information protection*

References

1. **Petrenko S. A., Simonov S. V.** *Upravlenie informacionnymi riskami. Ekonomicheski opravdannaya bezopasnost'.* (Information Risk Management. Economically justified safety), Moscow, DMK Press, 2005. 384 p. (in Russian).

2. **Astahov A. M.** *Iskusstvo upravleniya informacionnymi riskami* (The Art of Information Risk Management), Moscow, DMK Press, 2010. 312 p. (in Russian).

3. **Borisov V. V., Kruglov V. V., Fedulov A. S.** *Nechetkie modeli i seti.* (Fuzzy models and networks. Second edition, stereotype). Moscow, Goryachaya liniya — Telekom, 2012, 284 p. (in Russian).

4. **Glykos M. (Ed.)** *Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications*, Springer—Verlag, 2010.

5. **Papageorgiou E. (Ed.)** *Fuzzy Cognitive Maps for Applied Science and Engineering: From Fundamentals to Extensions and Learning Algorithms*, Springer-Verlag, 2014.

6. **Kosko B.** Fuzzy Cognitive Maps, *Intern. Journal of Man-Machine Studies*, 1986, vol. 24, pp. 65—75.

7. **Hagiwara M.** Extended Fuzzy Cognitive Maps, *Proc. of the IEEE Conference on Fuzzy Systems, San-Diego, USA, 8—12 March, 1992*, pp. 161—172.

8. **Borisov V. V., Fedulov A. S.** *Obobshchennye nechetkie kognitivnye karty* (Generalized fuzzy cognitive maps), *Nejrokomp'yutery: razrabotka, primenenie*, 2004, no. 4, pp. 3—20 (in Russian).

9. **Fedulov A. S.** *Nechetkie relyacionnye kognitivnye karty* (Fuzzy relational cognitive maps), *Izvestiya RAN. Teoriya i sistemy upravleniya*, 2005, no. 1, pp. 120—132 (in Russian).

10. **Carvalho J. P., Tome J. A. B.** Rule Based Fuzzy Cognitive Maps: Fuzzy Causal Relations, *Computational Intelligence for Modeling, Control and Automation: Evolutionary Computation & Fuzzy Logic for Intelligent Control, Knowledge Acquisition & Information Retrieval*, available at: www.inesc-id.pt/pt/indicadores/Ficheiros/1894.pdf (date of access: 24.09.2017).

11. **Borisov V. V., Fedulov A. S., Ustinenkov E. S.** *Analiz dinamiki sostoyaniya slozhnyh sistem na osnove obobshchennyh nechetkih produkcionnyh kognitivnyh kart* (Analysis of the dynamics of the state of complex systems based on generalized fuzzy production cognitive maps), *Nejrokomp'yutery: Razrabotka, Primenenie*, 2007, no. 1, pp. 17—23 (in Russian).

12. **Kandasamy V., Smarandache F.** Fuzzy Cognitive Maps and Neutrosophic Cognitive Maps, 2003, available at: https://arxiv.org/ftp/math/papers/0311/0311063.pdf (data of access: 24.09.2017).

13. **Byung Sung Yoon, Jetter. A. S.** Comparative Analysis for Fuzzy Cognitive Mapping, *2016 Proceedings of PICMET'16: Technology for Social Innovation*, 2016, pp. 1897—1908.

14. **Guzairov M. B., Vasilev V. I., Kudryavceva R. T.** *Sistemnyj analiz informacionnyh riskov s primeneniem nechetkih kognitivnyh kart* (System analysis of information risks with the use of fuzzy cognitive maps), *Infokommunikacionnye tekhnologii*, Samara, 2007, vol. 5, no. 4, pp. 42—48 (in Russian).

15. **Stepanova E. S., Mashkina I. V., Vasilev V. I.** *Razrabotka modeli ugroz na osnove postroeniya nechetkoj kognitivnoj karty dlya chislennoj ocenki riska informacionnoj bezopasnosti* (Development of a threat model based on the construction of a fuzzy cognitive map for the numerical assessment of the information security risk), *Izvestiya YUFU, Tekhnicheskie nauki, Tematich. vypusk "Informacionnaya bezopasnost'"*, Taganrog, Publishing house of TTI YUFU, 2010, no. 11 (112), pp. 31—40.

16. **Azhmuhametov I. M.** *Dinamicheskaya nechetkaya kognitivnaya model' ocenki urovnya informacionnoj bezopasnosti informacionnyh aktivov vuza* (Dynamic fuzzy cognitive model for assessing the level of information security of university's information assets), *Vestnik AGTU. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika*, 2012, no. 2, pp. 137—142.

17. **Yeboah-Boateng E. O.** Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies, *Intern. Journal on Electrical & Computer Sciences IJECS — IJENS*, Oct. 2012, vol. 12, no. 05, pp. 20—31.

18. **Vasilev V. I.** *Intellektual'nye sistemy zashchity informacii: ucheb. posobie dlya vuzov* (Intellectual systems of information protection: a textbook for high schools), Moscow, Innovacionnoe mashinostroenie, 2017, 201 p. (in Russian).

19. **Mazarakis S., Matsavinos G., Groumpos P.** Simulating and Forecasting Qualitative Macroeconomic Models Using Rule-Based Fuzzy Cognitive Maps, *Intern. Journal on Social, Behavioral, Economic, Business and Industrial Engineering*, 2013, vol. 7, no. 1, pp. 147—152.

20. **Perminov G. I., Leonova N. V.** *Primenenie nechetkoj logiki dlya resheniya kognitivnoj karty pri ispol'zovanii kombinacii al'ternativ* (The use of fuzzy logic for solving a cognitive map with using a combination of alternatives), *Audit i Finansovyj Analiz*, 2014, no. 4, pp. 396—401 (in Russian).

21. **Shapiro A. F., Koissi M.-C.** Risk Assessment Applications of Fuzzy Logic, March 2015, available at: https://www.casact.org/education/annual/2015/presentations/C-13-Shapiro.pdf (date of access: 24.09.2017).