УДК 002.6

В.И. Васильев, А.М. Вульфин, Р.Т. Кудрявцева

Анализ и управление рисками информационной безопасности с использованием технологии когнитивного моделирования

Обсуждаются вопросы применения технологии когнитивного моделирования для решения задач анализа и управления информационными рисками. Даны краткие сведения, относящиеся к методологии построения нечетких когнитивных карт (НКК). На примере реализации вирусной атаки и построения системы антивирусной защиты рассмотрены основные этапы когнитивного анализа: формирование множества концептов и связей НКК, анализ устойчивости и выбор весов связей НКК, численная оценка риска (ущерба) от реализации угрозы для различных вариантов реализации контрмер по защите информации. На основании приведенных результатов вычислительных экспериментов сформулированы рекомендации по продолжению исследований.

Ключевые слова: информационная безопасность, управление информационными рисками, нечеткая когнитивная карта, устойчивость.

doi: 10.21293/1818-0442-2017-20-4-61-66

Широкое внедрение компьютерных технологий во все сферы нашей жизни, включая задачи автоматизации управления производственными и технологическими процессами на крупных и средних предприятиях различных отраслей, неизбежно сталкивается с проблемой информационной безопасности. Сегодня вопросы обеспечения информационной безопасности (ИБ) прописаны в новой редакции Доктрины информационной безопасности, принятой в декабре 2016 г., ряде федеральных законов, многих международных и национальных стандартах (ГОСТ Р ИСО/МЭК 15408, 27001–27005, 13335, 18045, СТО БР ИББС и др.), руководящих документах Федеральной службы технического и экспортного контроля (ФСТЭК) России. В основе этих документов – использование рискориентированного подхода, суть которого заключается в выявлении основных факторов, влияющих на защищенность информационной (автоматизированной) системы, и на основе проведенного анализа формировании определенного набора организационных и технических мер (контрмер), способствующих снижению риска ИБ и обеспечению заданного (допустимого) уровня защищенности системы.

Существующие методы оценки рисков традиционно делят на две большие группы, связанные с качественной и количественной оценкой уровня рисков [1, 2]. К первой группе методов относятся такие получившие широкую известность методы, как OCTAVE, CRAMM, COBRA, MSAT, КОНДОР и др., целью которых является выявление и анализ основных факторов, влияющих на уровень риска, определение их уровня относительной значимости и общая качественная оценка уровня защищенности исследуемой системы с выдачей рекомендаций по обеспечению соответствия уровня защищенности требованиям нормативных документов (стандартов).

В основе применяемых при этом методик, как правило, используются опросные карты, предоставляемые экспертам, на которые те должны ответить «да», «нет», «частично» и т.п., после чего проводится соответствующая статическая обработка мнения экспертов по определенным правилам.

Вторая группа методов включает в себя такие известные методы, как и RiskWatch, АванГард, ГРИФ, позволяющие дать количественную оценку объема потерь (ущерба) от воздействия возможных угроз на каждый ценный ресурс информационной системы, выяснить причины возникновения риска с подробным анализом уязвимостей, оценить экономическую эффективность принятия тех или иных контрмер. Недостатком данной группы методов является необходимость наличия на предприятии достоверной статистики по инцидентам в сфере ИБ, включая оценки объема потерь от угроз ИБ.

В последние годы для решения задач управления рисками все чаще стали применять методы когнитивного моделирования, основанные на построении нечетких когнитивных карт, выступающих в качестве неформальных качественных моделей на предварительном (концептуальном) уровне изучения исследуемой системы. Преимуществами нечетких когнитивных карт (Fuzzy Cognitive Maps, FCM), впервые предложенных в 1986 г. Б. Коско [2], являются их простота и наглядность, выявление структуры причинно-следственных связей между элементами сложной системы, трудно поддающейся количественному анализу традиционными методами, использование знаний и опыта экспертов в конкретной предметной области, адаптация к неопределенности исходных данных и условий решаемой задачи. Сегодня существует большое число разновидностей нечетких когнитивных карт (НКК) – простые (классические) НКК [2, 3], обобщенные НКК [4], реляционные НКК [5], нечеткие продукционные карты [6, 7], НКК в базисе «истина–ложь–неопределенность» [8] и многие другие [9]. Основные направления исследований в данной области связаны с дальнейшей разработкой математических основ построения НКК, оценкой адекватности, структурной сложности и устойчивости НКК, выбором алгоритмов их обучения, обеспечивающих желаемые

характеристики НКК для достижения поставленных целей [10–17]. Вопросы применения НКК для решения задач анализа и управления рисками обсуждаются в [18–21].

Предлагаемая ниже статья ставит своей целью показать на примере те возможности и ограничения, которые предоставляет технология когнитивного моделирования в классе простых НКК для получения качественной оценки рисков ИБ и выбора рационального способа управления риском, обеспечивающего снижение влияния угрозы и уязвимости на информационный ресурс.

Нечеткие когнитивные карты

Под *нечеткой когнитивной картой* понимается модель исследуемой системы (объекта, проблемы) в форме ориентированного графа (орграфа), заданного с помощью набора множеств

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

где $\mathbf{C} = \{C_i\}$ – множество вершин графа, называемых *концептами*, в качестве которых выступают факторы (понятия), наиболее существенные с точки зрения изучения рассматриваемой системы; $\mathbf{F} = \{F_k\}$ – множество направленных дуг графа – связей между концептами; $\mathbf{W} = \{W_{ij}\}$ – множество весов дуг (связей).

Предполагается, что связи между концептами могут быть положительными, «усиливающими» влияние концепта C_i на концепт C_j ($W_{ij} > 0$), или отрицательными, «ослабляющими» влияние концепта C_i на концепт C_j ($W_{ij} < 0$). В простейшем случае $W_{ij} = +1$ или $W_{ij} = -1$, при этом говорят о *знаковом* орграфе. Значения весов (силы связей) W_{ij} могут задаваться с помощью нечеткой лингвистической шкалы, представляющей собой упорядоченное множество лингвистических значений (термов) оценок силы связи, например, вида

СИЛА_СВЯЗИ = {Не_влияет; Слабая; Средняя; Сильная; Очень_сильная}.

Каждому из этих значений ставится в соответствие некоторый числовой диапазон, принадлежащий отрезку [0, 1] для положительных связей (пример – табл. 1), или отрезку [–1, 0] для отрицательных связей.

Таблица 1

Оценка силы связи между концептами

Лингвистическое значение	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]

Предполагается, что, отвечая на вопрос о силе связи между концептом C_i и концертом C_j, эксперт выбирает одно из приведенных здесь лингвистических значений и некоторую «точечную» оценку силы связи – число внутри этого диапазона (если экспертов несколько, то в качестве веса W_{ij} принимается среднее из данных ими оценок). Более подробные рекомендации относительно выбора весов НКК можно найти в [22].

Знаковый орграф полностью задается своей *матрицей смежности*

$$\mathbf{W} = \begin{Vmatrix} W_{11} & W_{12} & \dots & W_{1n} \\ W_{21} & W_{22} & \dots & W_{2n} \\ \dots & \dots & \dots & \dots \\ W_{n1} & W_{n2} & \dots & W_{nn} \end{Vmatrix}, \qquad (2)$$

элементы которой W_{ij} принимают значения +1 (положительная связь), –1 (отрицательная связь) или 0 (отсутствие связи); n – число концептов НКК.

В общем случае для взвешенного орграфа с произвольными значениями весов $W_{ij} \in [-1, 1]$ можно говорить о динамике изменения его состояния во времени. Состояние орграфа (НКК) при этом определяется совокупностью состояний его концептов C_i, ($i = 1, 2, \dots, n$), каждое из которых описывается переменной состояния $X_i(t)$, принимающей значения из интервала [0, 1]. Последнее достигается путем нормирования первоначальных («физических») переменных состояния $\overline{X_i}$ по формуле

$$X_i = \frac{\overline{X}_i - X_{i\min}}{\overline{X}_{i\max} - \overline{X}_{i\min}}, \qquad (3)$$

где $\overline{X}_{i\ \min}$ и $\overline{X}_{i\ \max}$ – минимальное и максимальное значения переменной $\overline{X}_i$, ($i = 1, 2, \dots, n$).

Знаковый орграф считается линейным, его уравнения состояния записываются как

$$X(t+1) = \mathbf{W} \cdot X(t), \qquad (4)$$

где $\mathbf{X} = (X_1, X_2, \dots, X_n)^T$ – вектор состояния орграфа; $\mathbf{W}$ – матрица смежности; $t = 0, 1, 2, \dots$ – дискретное время.

Для взвешенного орграфа с произвольно заданными значениями весов W_{ij} уравнения состояния обычно записываются в следующем виде:

$$X_i(t+1) = f\left(\sum_{j=1}^{n} W_{ji}\, X_j(t)\right), \quad (i = 1, 2, \dots, n), \qquad (5)$$

где f – некоторая нелинейная «сжимающая» функция, отображающая значения аргумента в единичный интервал [0, 1].

Этому условию удовлетворяет, например, сигмоидная функция

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

Важным этапом анализа НКК является анализ устойчивости ее равновесных состояний для знакового орграфа, который сводится к вычислению собственных чисел матрицы смежности, т.е. корней характеристического уравнения

$$|\,\mathbf{W} - \lambda \cdot \mathbf{I}\,| = 0, \qquad (7)$$

где $\mathbf{I}$ – единичная матрица размера $n \times n$; λ – комплексная переменная.

Согласно [10] необходимо различать *импульсную устойчивость* орграфа, когда для заданного ненулевого начального состояния $X_i(0)$ одной из его вершин, например $X_1(0) = 1$, $X_2(0) = \dots = X_n(0) = 0$, последовательность значений импульсов $p_i(t) = X_i(t) - X_i(t-1)$ ограничена в любой момент времени $t = 1, 2, \dots$ для

любой его вершины, и *абсолютную устойчивость*, когда для каждой вершины орграфа (i = 1, 2, …, n) ограничена последовательность значений $X_i(t)$, t = 1, 2, … . При этом справедливо следующее:

Утверждение 1. [10]. Знаковый орграф импульсно (абсолютно) устойчив, если все ненулевые собственные числа матрицы **W** равны по абсолютной величине единице.

При определении устойчивости взвешенного орграфа можно воспользоваться другим утверждением, основанным на оценке абсолютных значений весов НКК [15].

Утверждение 2. Взвешенный орграф, описываемый уравнениями (5), (6), абсолютно устойчив, причем существует единственное равновесное (установившееся) решение этих уравнений («неподвижная точка») X^* в том и только в том случае, если

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{n} W_{ij}^2\right)^{\frac{1}{2}} < 4, \qquad (8)$$

где n – число концептов НКК.

Общая постановка процедуры анализа НКК включает в себя два этапа.

Задача анализа: для заданных начальных условий ($X_1(0)$, $X_2(0)$, …, $X_n(0)$), используя уравнения (4) или (5), (6), рассчитать переходные процессы $X_i(t)$, (t = 0, 1, 2, …), вызванные этими начальными условиями или некоторым внешним воздействием; определить установившиеся (равновесные) значения переменных состояния X_i^*.

Задача синтеза: найти такие скорректированные значения весов связей W_{ij}, а возможно и добавить новые концепты или связи, при которых обеспечивались бы желаемые установившиеся значения X_i^* целевых концептов C_e (l = 1, 2, …, n_1; $n_1 < n$) – выходов НКК.

Анализ и управление информационными рисками

Рассмотрим следующий пример. Допустим, что необходимо проанализировать последствия от реализации вирусной атаки на некоторый информационный ресурс, расположенный на рабочей станции (АРМ оператора). Тогда в соответствии с известной 3-факторной формулой оценки риска: РИСК = УГРОЗА × УЯЗВИМОСТЬ × УЩЕРБ [1] можно воспользоваться схемой НКК, приведенной на рис. 1.

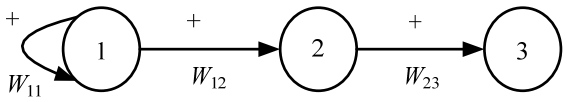

Рис. 1. Нечеткая когнитивная карта для оценки риска

Здесь *1* – концепт C_1, представляющий собой угрозу (вирусную атаку); *2* – концепт C_2, характеризующий уязвимость (например, отсутствие обновлений антивирусного ПО); *3* – концепт C_3, характеризующий ущерб от нарушения целостности информации вследствие реализации угрозы C_1 через уязвимость C_2.

Переменные состояния: X_1 – вероятность возникновения угрозы; X_2 – вероятность успешной реализации уязвимости; X_3 – величина ущерба от воздействия угрозы (в относительных единицах).

Рассмотрим 2 варианта представления НКК; а) в виде знакового орграфа; б) в виде взвешенного графа.

В первом случае будем полагать, что все веса НКК на рис. 1 принимают одинаковые значения, равные +1: $W_{11} = W_{12} = W_{23} = 1$ (положительные связи). Наличие цикла положительной обратной связи для концепта C_1 указывает на то, что данный концепт выступает в качестве независимого входа (источника), характеризующего воздействие на соседние концепты со стороны внешней среды (в [13] подобные концепты названы *драйверами*). Матрица смежности в данном случае принимает вид

$$\mathbf{W} = \begin{Vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{Vmatrix}.$$

С целью анализа устойчивости НКК составим характеристическое уравнение

$$|\,\mathbf{A} - \lambda \cdot \mathbf{I}\,| = \begin{vmatrix} 1-\lambda & 1 & 0 \\ 0 & -\lambda & 1 \\ 0 & 0 & -\lambda \end{vmatrix} = \lambda^2 (1-\lambda) = 0,$$

корни которого (т.е. собственные числа матрицы **W**) в данном случае принимают значения $\lambda_{1,2} = 0$; $\lambda_3 = 1$. Следовательно, в соответствии с приведенным выше Утверждением 1 данный орграф является импульсно (абсолютно) устойчивым.

Переходя к взвешенному орграфу (см. рис. 1), предположим, что эксперт назначил следующие значения весов связей НКК: $W_{11} = 1$, $W_{12} = W_{23} = 0{,}8$ (т.е. связи между концептами C_1, C_2 и C_3 – «сильные»). Введение цикла положительной обратной связи для концепта C_1 ($W_{11} = 1$) позволяет принудительно «удерживать» его начальное состояние $X_1(0) = 1$ в последующие моменты времени, принимая в дальнейшем $X(t) = 1$ для всех t = 1, 2, … . Воспользовавшись уравнениями состояния (5), (6) для начальных условий $X(0)$ = (1, 0, 0), находим установившееся (равновесное) значение переменной X_3, т.е. риска; $X_3^* = R$ = = 0,63. Таким образом, максимальное значение ущерба от реализации угрозы (вирусной атаки) при отсутствии специальных мер защиты составляет 0,63, т.е. 63% от максимальной границы возможного ущерба $R_{\max} = 1$.

Потребуем, чтобы за счет принятия дополнительных контрмер риск снизился до некоторого минимального (допустимого) уровня. При этом можно воспользоваться следующими рекомендуемыми способами управления риском [1]:

– уменьшение вероятности воздействия угрозы на информационные ресурсы;

– уменьшение вероятности использования уязвимости;

– уменьшение возможного ущерба путем обнаружения нежелательных событий, реагирования и восстановления ресурса.

Рассмотрим два варианта управления риском, реализующих указанные способы (рис. 2).

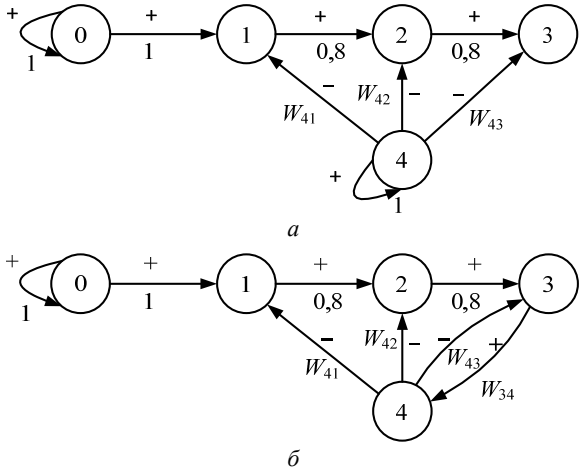

Рис. 2. Схемы НКК для управления риском:
а – «жесткое» (централизованное) управление;
б – «мягкое» (адаптивное) управление

На рис. 2: C_1 – угроза (вирусная атака); C_2 – уязвимость (отсутствие обновления антивирусного ПО); C_3 – ущерб от реализации угрозы; C_4 – контрмеры по защите информации. Дополнительно введенные отрицательные связи с весами W_{41}, W_{42}, W_{43} характеризуют соответственно влияние контрмер на основные факторы, определяющие уровень риска:

- $C_4 \to C_1$: распознавание и блокирование вируса на ранней стадии;
- $C_4 \to C_2$: обновление антивирусного ПО;
- $C_4 \to C_3$: частичное или полное восстановление искаженной информации.

Дополнительно введенный концепт C_0 выполняет функцию драйвера, обеспечивая значение вероятности «исходной» угрозы $X_0(t) = 1$ для всех $t = 0, 1, 2, \ldots$. Переменная X_1 характеризует вероятность «модифицированной» угрозы с учетом влияния концепта C_4. Переменная X_4 в обоих случаях (рис. 2, *а*, *б*) определяет ресурсы, выделенные на реализацию мер защиты информации. Дополнительная связь $C_3 \to C_4$ с весом W_{34} характеризует учет результатов контроля (мониторинга) за состоянием защищаемой информации C_4. Различие между двумя указанными выше вариантами состоит в том, что в 1-м случае (рис. 2, *а*) ресурсы концепта-драйвера C_4 жестко выделяются в фиксированном объеме и затем перераспределяются по выполняемым функциям защиты, а во 2-м случае (рис. 2, *б*) величина этих ресурсов зависит от фактического состояния защищенности информации (ущерба) C_3 и может варьироваться в определенных пределах.

НКК на рис. 2, *а* имеет 2 контура положительной обратной связи ($C_0 \to C_0$, $C_4 \to C_4$) для драйверов C_0 и C_4, а НКК на рис. 2, *б*: 1 контур положительной обратной связи ($C_0 \to C_0$) и 3 контура отрицательной обратной связи ($C_4 \to C_3 \to C_4$; $C_4 \to C_2 \to C_3 \to C_4$; $C_4 \to C_1 \to C_2 \to C_3 \to C_4$). Матрицы смежности для обоих вариантов запишутся соответственно как

$$\mathbf{W}_a = \begin{Vmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & 1 \end{Vmatrix}; \quad \mathbf{W}_б = \begin{Vmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & -1 & -1 & 0 \end{Vmatrix},$$

откуда получаем характеристические уравнения: $|\mathbf{W}_a - \lambda\cdot\mathbf{I}| = \lambda^2(1-\lambda)^3 = 0$; $|\mathbf{W}_б - \lambda\cdot\mathbf{I}| = \lambda^2(1-\lambda)(\lambda^2 - \lambda + 1)$. Учитывая, что корни этих уравнений принимают значения $\lambda_{1,2} = 0$; $\lambda_{3,4,5} = 1$ (для варианта а) и $\lambda_{1,2} = 0$; $\lambda_3 = 1$; $\lambda_{4,5} = \frac{1}{2} \pm j\frac{\sqrt{3}}{2}$ (для варианта *б*), можно сделать вывод о том, что оба этих варианта НКК импульсно (абсолютно) устойчивы.

Допустим далее, что изначально заданные значения весов связей $W_{12} = W_{23} = 0{,}8$ сохраняются, а значения весов W_{41}, W_{42}, W_{43}, W_{34} назначаются экспертом (соответствующие варианты задания весов для каждой из двух схем, приведенных на рис. 2, *а*, *б*, представлены в табл. 2). Легко проверить, что условие устойчивости (8) во всех случаях выполняется (веса связей-драйверов $W_{00} = W_{01} = 1$ и $W_{44} = 1$ в данном случае не учитываются [14]). Таким образом, оператор в правой части уравнений (5) является оператором сжатия и, следовательно, для заданных начальных условий $X(0) = (1, 0, 0, 0, 1)^т$ – для схемы на рис. 2, *а* и $X(0) = (1,0,0,0,0)^т$ – для схемы на рис. 2, *б* достигается установившееся (равновесное) состояние $X^* = (X_0^*, X_1^*, X_2^*, X_3^*, X_4^*)^т$. Результаты моделирования, полученные с помощью разработанного авторами автоматизированного пакета FCMBuilder [23], приведены в табл. 2.

Анализ результатов, приведенных в табл. 2, позволяет сделать определенные выводы:

1. Использование НКК дает некоторую сравнительную базу для выбора вариантов построения системы защиты информации, исходя из приемлемого уровня обеспечения рисков ИБ. Так, вариант а-4

Таблица 2

Результаты моделирования

№ варианта	W_{41}	W_{42}	W_{43}	W_{34}	X_1^*	X_2^*	$X_3^*=R$	X_4^*
а-1	–0,8	–0,5	–0,5	0	0,55	0,49	0,47	1
а-2	–0,5	–0,8	–0,5	0	0,62	0,43	0,46	1
а-3	–0,8	–0,8	–0,5	0	0,55	0,41	0,46	1
а-4	–0,8	–0,8	–0,8	0	0,55	0,41	0,38	1
б-1	–0,8	–0,5	–0,5	0,5	0,63	0,56	0,55	0,57
б-2	–0,5	–0,8	–0,5	0,5	0,67	0,52	0,53	0,57
б-3	–0,8	–0,8	–0,5	0,5	0,63	0,51	0,53	0,57
б-4	–0,8	–0,8	–0,8	0,5	0,63	0,51	0,48	0,59

оказывается предпочтительнее вариантов а-1 – а-3, поскольку он предлагает уделить одинаково серьезное внимание всем 3 компонентам риска (парирование угрозы – ликвидация уязвимости – устранение последствий от реализации угрозы), что соответствует так называемому «принципу равнопрочности» защиты.

2. Возможное разбиение полученных решений по уровням риска (например, $0{,}55 < R \le 0{,}65$ – высокий уровень; $0{,}45 < R \le 0{,}55$ – средний уровень; $0{,}35 < R \le 0{,}45$ – низкий уровень риска) является в значительной степени условным; столь малый разрыв между верхней и нижней границей риска объясняется, прежде всего, сжимающим характером сигмоидной функции (6), причем эффект сжатия проявляется тем сильнее, чем больше концептов располагается на пути от источника до целевого фактора.

3. Приоритет в пользу выбора решений, соответствующих схеме НКК на рис. 2, *а*, по сравнению со схемой НКК на рис. 2, *б* обусловлен главным образом большим объемом ресурсов, выделенных на реализацию контрмер в 1-м случае (переменная $X_4^* = 1$), в то время как во 2-м случае максимальное значение объема ресурсов достигает лишь величины $X_4^* = 0{,}59$ для варианта б-4.

4. Несмотря на то, что сигмоидная функция (6) представляет собой оператор сжатия, что гарантирует (в силу утверждения 2) существование и устойчивость равновесного состояния НКК, условие (8) является достаточно жестким требованием по отношению к значениям весов НКК, что может послужить серьезным ограничением при построении НКК большой размерности, содержащих большое число концептов и связей.

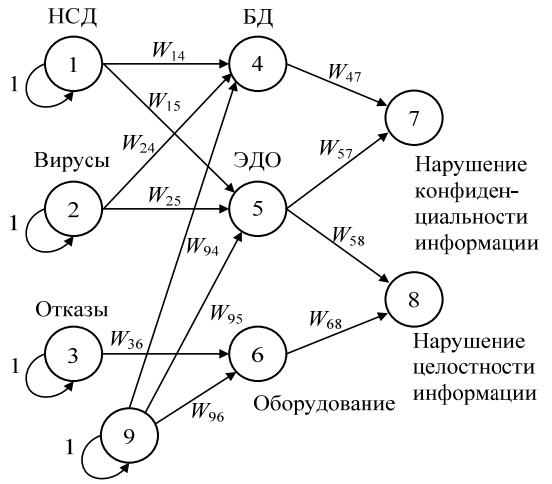

Рис. 3. НКК, характеризующая влияние совокупности угроз на возникновение рисков, связанных с нарушением конфиденциальности и целостности информации

Следует отметить, что рассмотренной выше пример (схемы НКК на рис. 1, 2) имеет главным образом методический характер. Реальные ситуации, возникающие на практике, требуют построения и исследования более сложных по своему составу НКК, включающих достаточно большое число концептов и связей. На рис. 3 приведён пример такой НКК, характеризующей влияние некоторой совокупности угроз на возникновение рисков, связанных с нарушением конфиденциальности и целостности информации.

Здесь C_1, C_2 и C_3 – угрозы, связанные соответственно с попытками несанкционированного доступа (НСД) к информации, вирусной атакой и отказами оборудования; C_4, C_5 и C_6 – уязвимости, вызванные отсутствием надлежащей защиты базы данных (БД), электронного документооборота (ЭДО) и оборудования; C_7 и C_8 – ущерб (потери) от нарушения конфиденциальности и целостности информации; C_1 – контрмеры по защите информации. Пользуясь изложенной выше методикой, можно не только оценить возможные риски от воздействия угроз, но и выбрать правильную (рациональную) стратегию защиты информации.

Заключение

Целью данной статьи было показать те возможности и преимущества, которые предоставляет технология когнитивного моделирования (в частности, аппарат нечетких когнитивных карт) для решения задачи анализа и управления информационными рисками. Особенностью применения данной технологии является акцент на выявление наиболее существенных факторов, оказывающих влияние на постановку задачи, и получение необходимого результата, оценка существующих между ними причинно-следственных связей, возможность сравнительного анализа различных вариантов принятия решений. Полученные при этом качественные модели в виде НКК особенно полезны на этапе предварительной оценки рисков информационной безопасности, при отсутствии достоверной статистики об имеющихся и потенциальных возможных инцидентов ИБ.

В качестве перспективного направления исследований, связанных с решением задач анализа и управления информационными рисками, следует ожидать применение реляционных НКК и нечетких продукционных карт, обладающих в силу большей общности рядом дополнительных преимуществ по сравнению с рассмотренным выше классом нечетких когнитивных карт Б. Коско.

Литература

1. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК-Пресс, 2010. – 312 с.

2. Kosko B. Fussy Cognitive Maps // International Journal of Man-Machine Studies. – 1986. – Vol. 1. – P. 65–75.

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

4. Hagiwara M. Extended Fuzzy Cognitive Maps // Proceedings of the IEEE Conf. on Fuzzy Systems, 8–12 March 1992, San-Diego, USA. – San-Diego: IEEE, 1992. – P. 161–172.

5. Федулов А.С. Нечеткие реляционные когнитивные карты // Изв. Российской академии наук. Теория и системы управления. – 2005. – № 1. – С. 120–132.

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

7. Борисов В.В. Анализ динамики состояния сложных систем на основе обобщенных нечетких продукционных когнитивных карт / В.В. Борисов, А.С. Федулов, Е.С. Устиненко // Нейрокомпьютеры: разработка, применение. – М.: Радиотехника, 2007. – № 1. – С. 17–23.

8. Kandasamy W.B.V. Fuzzy Cognitive Maps and Neutrosophic Cognitive Maps / W.B.V. Kandasamy, F. Smarandache. – 2003 [Электронный ресурс]. – Режим доступа: https://arxiv.org/ftp/math/papers/0311/ 0311063.pdf, свободный (дата обращения: 01.09.2017).

9. Papageorgiou E.I. Review of Fuzzy Cognitive Maps Research During the Last Decade / E.I. Papageorgiou, I.A. Salmeron // IEEE Trans. on Fuzzy Systems. – 2013. – Vol. 21, № 1. – P. 66–79.

10. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам / под ред. А.И. Теймана. – М.: Наука, Гл. ред. физ.-мат. лит, 1986. – 496 с.

11. Glykas M. (ed.). Fuzzy Cognitive Maps: Advances in theory, methodologies, tools and applications. // Springer Science & Business Media. – 2010. – Т. 247 [Электронный ресурс]. – Режим доступа: http://www.springer.com/us/ book/9783642032196, свободный (дата обращения: 01.09.2017).

12. Papageorgiou E. (ed.). Fuzzy Cognitive Maps for Applied Sciences and Engineering: From Foundations to Extensions and Learning Algorithms // Springer Science & Business Media. – 2014. – Т. 54 [Электронный ресурс]. – Режим доступа: http://www.springer.com/us/book/ 9783642397387, свободный (дата обращения: 01.09.2017).

13. Knight CR.J.K. Linear and Sigmoidal Fuzzy Cognitive Maps: An Analysis of Fixed Points / CR.J.K. Knight, D.J.B. Lloyd, A.S. Penn [Электронный ресурс]. – Режим доступа: https://pdfs.semantiescholar.org/, свободный (дата обращения: 01.09.2017).

14. Carvalho J.P. Issues in the Stability of Fuzzy Cognitive Maps and Rule – Based Fuzzy Cognitive Maps / J.P. Carvalho, Y.A.B. Tome [Электронный ресурс]. – Режим доступа: URL: www.inesc-id.pt/indicators/Ficherois/119.pdf, свободный (дата обращения: 01.09.2017).

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

16. Marchenko A.S. Investigating Stability Analysis Issues for Fuzzy Cognitive Maps / A.S. Marchenko, I.L. Ermolov, P.P. Groumpos et al. [Электронный ресурс]. – Режим доступа: URL: kcc.teiep.gr/stylios/pdf/, свободный (дата обращения: 01.09.2017).

17. Boutalis Y. Adaptive estimation of fuzzy cognitive maps with proven stability and parameter convergence / Y. Boutalis, Th.L. Kottas, M. Chrstodoulou // Journal IEEE Trans. On Fuzzy Systems. – 2009. – Vol. 17, Iss. 4. – P. 874–889.

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

19. Степанова У.С. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности / У.С. Степанова, И.В. Машкина, В.И. Васильев // Изв. ЮФУ. Технические науки. – Тематич. вып. «Информационная безопасность». – Таганрог: ТТИ ЮФУ. – 2010. – № 11 (112). – С. 31–40.

20. 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.

21. Yebjah-Bouteng E.O. Using fuzzy cognitive maps (FCMs) To evaluate the vulnerabilities with ICT assets disposal policies // Intern. Journal on Electrical & Computer Sciences IJECS-IJENS. – 2012. – Vol. 12, № 05. – P. 20–31.

22. Кулинич А.А. Компьютерные системы моделирования когнитивных карт. Подходы и методы // Проблемы управления. – М., 2010. – № 3. – С. 2–16.

23. Васильев В.И. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт / В.И. Васильев, Р.Т., Кудрявцева, В.А. Юдинцев // Вестник УГАТУ, 2014. – Т. 18, № 3 (64). – С. 253–260.

Васильев Владимир Иванович
Д-р техн. наук, профессор каф. вычислительной техники и защиты информации (ВТиЗИ)
Уфимского государственного авиационного технического ун-та (УГАТУ)
Тел.: +7-917-350-11-39
Эл. почта: vasilyev@ugatu.ac.ru

Вульфин Алексей Михайлович
Канд. техн. наук, доцент каф. ВТиЗИ УГАТУ
Тел.: +7-917-40-02-189
Эл. почта: vulfin.alexey@gmail.com

Кудрявцева Рима Тимиршаиховна
Канд. техн. наук, доцент каф. ВТиЗИ УГАТУ
Тел.: +7-917-454-67-66
Эл. почта: cudrt@mail.ru

Vasilyev V.J., Vulfin A.M., Kudryavtseva R.T.

Analysis and management of information security risks using cognitive modeling technology

The issues of applying the cognitive modeling technology to solve the problems of information risks analysis and management are discussed. The brief information related to the methodology of fuzzy cognitive maps (FCM) construction is presented. On the example of a virus attack and building an antivirus system, the main stages of cognitive analysis are considered: generating a set of FCM concepts and links, analysis of FCM stability and selection of FCM links weights, numerical evaluation of risk (damage) from the threat action for different variants of countermeasures implementation for information protection. Based on the obtained computer experiments results the recommendations for the further research are formulated.

Keywords: information security, information risks management, fuzzy cognitive map, stability.