DOI 10.37882/2223-2966.2024.03.33

ПРИМЕНЕНИЕ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ В УСЛОВИЯХ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

APPLICATION OF FUZZY COGNITIVE MAPS IN DECISION MAKING CONDITIONS TO ENSURING INFORMATION SECURITY

D. Suzdalsky

Summary. The article is devoted to the consideration of the features of the use of fuzzy cognitive maps in decision-making conditions to ensure information security. A fuzzy cognitive map was constructed, which made it possible to draw cause-and-effect conclusions about the influence of the selected factor-concepts on the level of information security thanks to direct communication chains and numerical data. It is concluded that the constructed NQF model allowed for causal inferences to be made based on direct chains and numerical data, while preliminary results are encouraging regarding the possibilities of using NQF by decision makers/ICT managers, allowing a clear understanding of the impact of cyber attacks on information security and provide a more focused view of the necessary protective actions.

Keywords: information security, cognitive map, modeling, threat, attack.

Суздальский Дмитрий Андреевич
Аспирант, Российский экономический университете им. Г.В. Плеханова
t7699690@gmail.com

Аннотация. Статья посвящена рассмотрению особенностей применения нечетких когнитивных карт в условиях принятия решений для обеспечения информационной безопасности. Построена нечеткая когнитивная карта, которая позволила сделать причинно-следственные выводы о влиянии выделенных факторов-концептов на уровень информационной безопасности благодаря прямым цепочкам связи и числовым данным. Сделан вывод о том, что построенная модель НКК позволила сделать причинно-следственные выводы на основе прямых цепочек и числовых данных, при этом предварительные результаты обнадеживают в отношении возможностей применения НКК лицами, которые принимают решения/менеджеров ИКТ, позволяя четко осознать влияние кибератак на ИБ и обеспечить более целенаправленный взгляд на необходимые защитные действия.

Ключевые слова: информационная безопасность, когнитивная карта, моделирование, угроза, атака.

Активная информатизация современного общества, развитие цифровых технологий и стремительное наращивание темпов Четвертой промышленной революции, которые в совокупности повлекли за собой увеличение потоков конфиденциальной информации, привели к необходимости обеспечения информационной безопасности (ИБ) в различных сферах общественной деятельности, поскольку любой процесс в финансовой, производственной, политической или социальной сфере напрямую связан с информационными ресурсами и использованием информационных технологий (ИТ). Информация может быть украдена, искажена, стать недоступной, потерять свою целостность и конфиденциальность — все это приводит к значительным материальным и репутационным потерям. Каждые 39 секунд в Интернете происходит новая атака, которая ежегодно обходится в триллионы долларов [1].

В связи с этим исследование влияния угроз на уровень защищенности информационных систем является актуальной и важной научно-практической задачей, которая характеризуется высокой степенью неопределенности и сложностью строгой формализации [2]. В современных исследованиях подчеркивается, что ИБ не целесообразно анализировать только как практику соблюдения требований при возникновении конкретных инцидентов, приводящих к дополнительным расходам, она должна быть структурирована и учитывать все возможные сценарии и варианты развития событий [3].

На практике решить эту проблему можно с помощью методов статистического анализа, в частности метода корреляционно-регрессионного анализа. Однако эти подходы требуют сложных расчетов, значительного объема экспериментальных данных, длительны по времени обработки и не обеспечивают возможности работы с показателями качества, определяемыми экспертами. В связи с этим, учитывая, что ИБ представляет собой сложную систему с недостаточным количеством аналитических данных для устранения неопределенности и прогнозирования, в процессе принятия решений большинство подходов опирается на экспертные оценки, теорию нечеткой логики и теорию графов. Данные методы хорошо формализуются при использовании нечетких когнитивных карт (НКК), которым свойственна простота, наглядность, гибкость, конструктивность, адаптация к недостаточности и неточности входных данных. Как утверждают исследователи, НКК имеют значительные перспективы

и возможности в области кибербезопасности и ИБ и могут стать мощным инструментом для изучения различных сценариев в процессе принятия решений [4].

В тоже время, необходимо отметить, что на сегодня существуют различные модификации НКК для моделирования сложных систем, они отличаются способами представления и методами анализа. Поэтому выбор наиболее приемлемой формы и способа в процессе управления ИБ требует проведения дальнейших исследований, что и обуславливает выбор темы данной статьи.

Возможности построения стратегий кибербезопасности с использованием НКК, подходы к разработке спектра сценариев информационных угроз с вариациями степени интенсивности влияния различных факторов, рассматривают в своих публикациях Васильев В.И., Вульфин А.М., Кириллова А.Д., Бочков А.П., Хомоненко А.Д., Барановский А.М., Shivanshu Shrivastava, A. Rajesh, P.K. Bora, Bin Chen, Mingjun Dai.

Над разработкой иерархического метода оценки ситуации кибербезопасности, который основан на онтологиях и НКК трудятся Лексиков Е.В., Яковенко А.Н.,

Таблица 1.

Описание концептов, участвующих в исследовании и оценке ИБ

Концепт	Описание	Нечеткая интерпретация
C1: Небезопасные сетевые протоколы	Из-за небезопасных сетевых протоколов (HTTP) злоумышленники могут проникнуть в сеть организации	-1: Низкий уровень несовместимости сетевых протоколов 0: Сетевой протокол средней несовместимости 1: Сетевой протокол с высокой степенью несовместимости
C2: Шифрование чувствительных данных	Разработка пользовательского кода, обеспечивающего шифрование в отдельных полях данных	-1: Низкий уровень поддержания ИБ 0: Среднее поддержание ИБ 1: Высокий уровень обеспечения ИБ
C3: Сбои в работе мобильных приложений	Операционные сбои происходят из-за того, что пользователи системы не готовы к принятию протоколов ИБ	-1: Низкий уровень операционных сбоев 0: Операционные сбои иногда происходят 1: Высокий уровень операционных сбоев
C4: Сертификация по кибербезопасности	Предоставляет обоснование того, почему проверяемые события считаются адекватными для поддержки расследования инцидентов безопасности на операционном сервере	-1: Абсолютный отказ от проверяемых событий 0: Среднее внимание к проверяемым событиям 1: Приоритетное внимание к проверяемым событиям
C5: Аутсорсинг облачных ИТ-услуг	Использование справочных служб, технической поддержки и провайдера для защиты конфиденциальности переданной на аутсорсинг информации	-1: Нет поддержки безопасности связи 0: Несколько видов поддержки безопасности коммуникаций 1: Приоритетное внимание к безопасности коммуникаций
C6: Управление ИТ	Обоснование стратегий безопасности, согласованных с бизнес-целями и поддерживающих их	-1: Абсолютный отказ от управления ИТ 0: Среднее внимание к управлению ИТ 1: Приоритетное внимание к управлению ИТ
C7: Средства контроля беспроводной связи	Разработка политики и процедур для эффективного внедрения выбранных мер безопасности и контроля	-1: Абсолютный отказ от доступа к политике 0: Среднее внимание к доступу 1: Приоритетное внимание к доступу
C8: Мобильные подключенные устройства	Отсутствие обновлений или отсутствие исправлений	-1: Низкий уровень поддержания ИБ 0: Средний уровень обеспечения ИБ 1: Высокий уровень обеспечения ИБ
C9: Критерии приемлемости поставщиков услуг	Установление базовых требований к безопасности и их преобразование в критерии приемлемости при выборе поставщиков	-1: Нет подтверждающих критериев приемлемости поставщика 0: Несколько критериев, подтверждающих правомочность поставщика 1: Большое количество критериев, подтверждающих правомочность поставщиков
C10: Инвестиции в ИТ	Инвестиции в ИТ для поддержания актуальности и безопасности систем	-1: Нет поддерживающих инвестиций в ИТ 0: Несколько поддерживающих ИТ-инвестиций 1: Большое количество поддерживающих ИТ-инвестиций
C11: Ошибки пользователей	Администраторы должны просвещать пользователей о кибербезопасности и мерах, которые они должны предпринять для повышения общей безопасности взаимодействия в Интернете	-1: Без поддержки образования 0: Немного поддерживающего образования 1: Широкий спектр поддерживающего образования

Гузаиров М.Б., Вульфин А.М., Картак В.М., Yangyang Sun, Xiangdong Jia, Xianghua Han, Mangang Xie, Liang Zhang.

В тоже время, несмотря на активный интерес ученых к данной проблематике, необходимо отметить, что ряд вопросов остается открытым и требует более детального исследования. Так, особого внимания заслуживают принципы использования НКК для изучения причинно-следственных связей в системе нарушения целостности информационных систем. В более углубленной проработке нуждаются подходы к получению усредненной оценки локальных рисков, сформированной с использованием ансамбля когнитивных карт.

Таким образом, цель статьи заключается в рассмотрении возможностей применения нечетких когнитивных карт в условиях принятия решения для обеспечения ИБ.

НКК — это алгоритм машинного обучения со структурой графа, имеющего вершины и ребра [5]. Структура НКК позволяет декомпозировать сложную систему на более мелкие компоненты, которые могут быть реализованы как вершины в моделях НКК, а их взаимодействие — как ребра [6]. Процедура построения НКК может быть определена в три основных шага.

Первый шаг: уточнить цель НКК, если она не определена, то поиск причинно-следственных связей сделает формирование НКК невыполнимым.

Второй этап: определение релевантных концепций, влияющих на принимаемое решение.

Третий этап: поиск причинно-следственных связей между понятиями, определенными на предыдущем этапе, причем эти связи должны быть абстрагированы от определений лиц, принимающих решения, с помощью таких инструментов, как анкеты и интервью.

Таким образом, с математической точки зрения, НКК можно описать как набор узлов (концепций) C_i с $i = 1, ..., n$, являющимся числом концепций в задаче, и все эти концепции вместе представляют собой вектор состояний $A = [A_1, ..., A_n]$. На значимость каждого понятия влияют величины связанных с ним понятий с соответствующим причинно-следственным весом, и для того, чтобы система понятий развивалась, вектор A должен многократно проходить через матрицу связей W. Соответствующая математическая модель имеет следующий вид:

$$A_i^{(K+1)} = f\left(A_i^k + \sum_{\substack{j=1 \\ j \neq i}}^{N} A_j^k W_{ji} \right)$$

где: $A_i^{(K+1)}$ — значение концепции C_i на шаге $k + 1$;

A_j^k — значение концепции C_j на шаге k;

W_{ji} — вес связи между C_j и C_i;

$f(x)$ — сигмоидная пороговая функция, определяемая следующим уравнением:

$$f = \frac{1}{1 + e^{-\lambda x}}$$

где l — положительная постоянная в определенном интервале, а $f(x)$ лежит между [0, 1].

Итак, для построения НКК, которая определяет состояние ИБ некой системы, прежде всего, необходимо сформировать множество наиболее весомых с точки зрения изучения данной проблемы концептов. В результате опроса и согласования мнений группы экспертов в данной предметной области были определены следующие концепты (см. табл. 1).

После того, как выбраны все концепты ИБ необходимо определить значения силы влияния между каждой парой концептов путем обработки данных, полученных в результате экспертного опроса [7]. Для этого зададим нечеткую лингвистическую шкалу, которая представляет собой упорядоченное множество лингвистических значений (термов) оценок наступления вероятных последствий, полученных в результате действия одного концепта на другой.

$$\text{Сила связи} = \left\{ \begin{matrix} \text{Не влияет, Очень слабая, Слабая} \\ \text{Средняя, Сильная, Очень сильная} \end{matrix} \right\}$$

Каждому из этих значений поставим в соответствие некоторый числовой диапазон, принадлежащий отрезку [0, 1] для положительных связей и отрезку [-1, 0] для отрицательных связей.

$$w_{ij} = \left\{ \begin{matrix} (0{,}85;1], \text{положительная очень сильная} \\ (0{,}6;0{,}85], \text{положительная сильная} \\ (0{,}35;0{,}6], \text{положительная средняя} \\ (0{,}15;0{,}35], \text{положительная слабая} \\ (0;0{,}15], \text{положительная очень слабая} \\ 0, \text{не влияет} \\ (0;-0{,}15], \text{отрицательная очень слабая} \\ (-0{,}15;-0{,}35], \text{отрицательная слабая} \\ (-0{,}35;-0{,}6], \text{отрицательная средняя} \\ (-0{,}6;-0{,}85], \text{отрицательная сильная} \\ (-0{,}85;1], \text{отрицательная очень сильная} \end{matrix} \right\}$$

НКК разработанная автором, которая иллюстрирует множественные причинно-следственные связи и характер взаимодействия выделенных концептов, изображена на рис. 1. Моделирование выполнено с использованием средств программного обеспечения Mental Modeler.

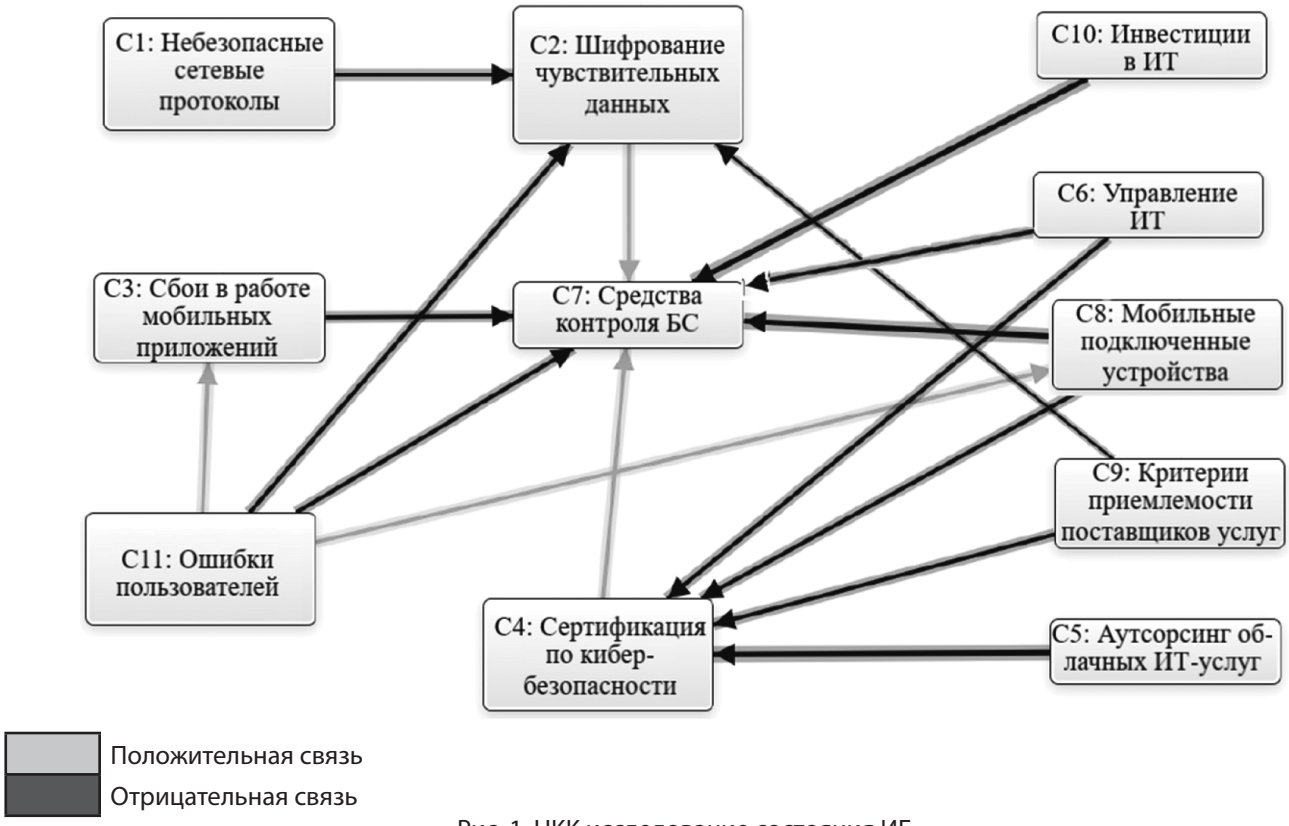

Рис. 1. НКК исследование состояния ИБ

В результате исследования полученной модели были определены ее наиболее весомые концепты: критерии приемлемости поставщиков услуг (C9), аутсорсинг облачных ИТ-услуг (C5) и управление ИТ (C6). С помощью сценарного моделирования установлено, что при максимально негативном влиянии каждого из этих концептов отдельно сертификация по кибербезопасности (C4) ухудшится соответственно на 0,29; 0,18 и 0,06.

Сравним влияние наиболее весомых концептов на защищенность исследуемой системы с помощью регрессионного анализа. Для достижения поставленной цели смоделируем десять разных сценариев, отражающих относительное изменение ИБ при заданных значениях выбранных концептов (таблица 2).

Построение сценариев способствует моделированию возможных последствий, вызванных общими факторами, которые влияют на ИБ определенным образом. Кроме того, эти сценарии могут поддержать процесс принятия решений при стратегическом планировании действий, нацеленных на предотвращение или смягчение уязвимостей, которые могут поставить под угрозу работу всех информационных систем [8]. Планирование действий по смягчению последствий, если оно осуществляется без должного внимания, может негативно повлиять на вероятность возникновения атак. Матричное представление нечеткой когнитивной карты (матрица весов wij), полученное в результате экспертных интервью и процесса моделирования, может изменить свою конфигурацию в зависимости от корректировок экспертов.

Таблица 2.

Значения исследуемых концептов, полученные в результате сценарного моделирования

i	*C9*	*C5*	*C6*	*C4*
1	1	1	1	0,8
2	0,9	-0,1	0,7	0,13
3	-0,1	-0,3	-0,1	-0,8
4	1	-0,2	1	0,16
5	-0,2	0,3	0,9	-0,4
6	0,8	0,2	-0,3	-0,1
7	1	-0,1	-0,2	0,6
8	-0,3	-0,5	0,8	0,1
9	0,7	0,8	0,9	0,5
10	0,5	-0,3	-0,1	0,2

Например, в сценарии 9 анализируется влияние на ИБ таких концептов как: критерии приемлемости поставщиков услуг — коэффициент (0,7), аутсорсинг облачных ИТ-услуг — (0,8), управление ИТ — (0,6) и сертификация по кибербезопасности (0,5). Рис. 2 наглядно иллюстрирует результаты этого сценарного анализа.

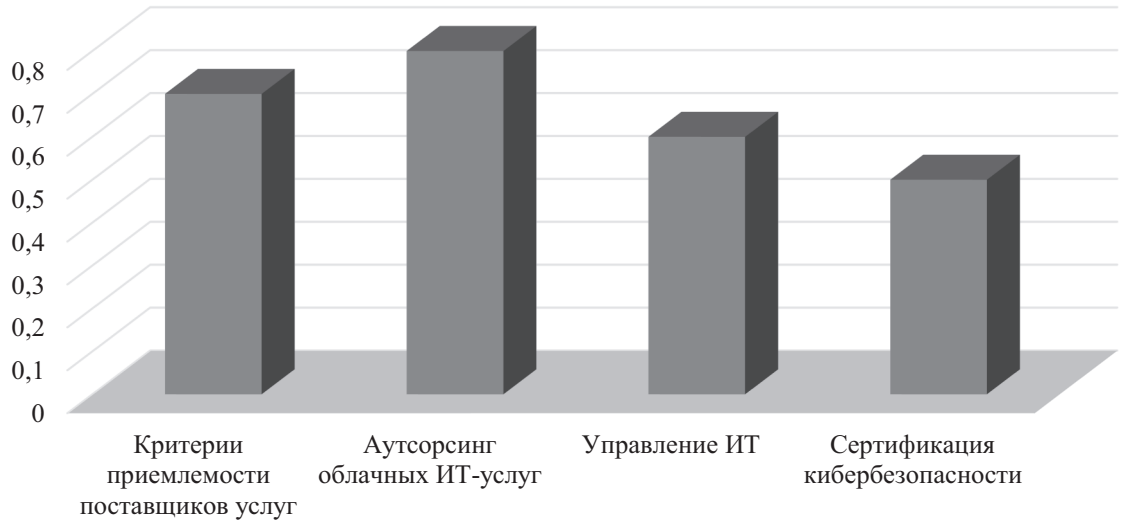

Рис. 2. Сценарий 9: анализ состояния ИБ

Этот сценарий подчеркивает связь с последствиями использования уязвимостей при выявлении обозначенных факторов. Так, например, если не будут должным образом разработаны критерии приемлемости поставщиков услуг и субъект будет пользоваться аутсорсингом облачных ИТ-услуг без внимания к защите конфиденциальных данных, к протоколам безопасности и технической поддержки, то вероятность атаки злоумышленников и прочих неправомерных действий в системе является максимальной.

Таким образом, подводя итоги отметим, что использование НКК для анализа факторов ИБ имеет значительный практический потенциал. Построенная в работе модель НКК позволила сделать причинно-следственные выводы на основе прямых цепочек и числовых данных, а также мнений экспертов по кибербезопасности. Предварительные результаты обнадеживают в отношении возможностей применения НКК лицами, которые принимают решения/менеджеров ИКТ, позволяя четко осознать влияние кибератак на ИБ и обеспечить более целенаправленный взгляд на необходимые защитные действия.

ЛИТЕРАТУРА

1. Цибизова Т.Ю. Мониторинг безопасности системы защиты информации критической информационной инфраструктуры на основе когнитивного моделирования // Известия Тульского государственного университета. Технические науки. 2023. № 6. С. 33–41.
2. Суздальский Д.А. Актуальные вопросы моделирования функционирования подсистемы информационной безопасности // Национальная ассоциация ученых. 2023. № 88-1. С. 47–52.
3. Палютина Г.Н. О применении когнитивного моделирования в адаптивной оценке рисков информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. 2023. № 4 (50). С. 43–52.
4. Kazymyr V., Posadska A. Researching the Cognitive Maps by Simulation Modeling // Technical Sciences and Technologies. 2021. № 1(7). P. 98–105.
5. Hordei O., Patsai B., The Use of Modeling in the Learning Process in the Formation of the Necessary Competencies // Economic Analysis. 2022. № 32(2). P. 62–72.
6. Чечулин А.А. Основные элементы методологии обеспечения информационной безопасности и защиты информации в компьютерных сетях // Информатизация и связь. 2022. № 3. С. 27–30.
7. Edward A. Cranford, Cleotilde Gonzalez Towards a Cognitive Theory of Cyber Deception // Cognitive Science. 2021. Volume 45, Issue 7. P. 78–84.
8. Kamal Kumar Gola Security analysis of fog computing environment for ensuring the security and privacy of information // Transactions on Emerging Telecommunications Technologies. 2023. Volume 34, Issue 10. P. 112–117.

Журнал «Современная наука: актуальные проблемы теории и практики»