АНАЛИЗ РИСКОВ КИБЕРБЕЗОПАСНОСТИ С ПОМОЩЬЮ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Васильев В.И.[1], Вульфин А.М.[2], Герасимова И.Б.[3], Картак В.М.[4]

Цель исследования: получение качественной и количественной оценки показателей риска с учетом совокупности объективных и субъективных факторов неопределенности, влияющих на эти показатели для задач комплексной оценки рисков обеспечения кибербезопасности автоматизированных систем управления и контроля технологических процессов (АСУ ТП) промышленных объектов в условиях возможного воздействия на эти системы потенциальных внешних и внутренних угроз.

Метод исследования: оценка рисков кибербезопасности АСУ ТП путем построения и моделирования ансамбля нечетких когнитивных карт, базирующихся на основе положений теории интервальных нечетких множеств.

Результаты: рассмотрено применение классических, серых и интуиционистских нечетких когнитивных карт для решения задачи оценки рисков кибербезопасности промышленных объектов. Показано, что средневзвешенная оценка локального риска, формируемая с помощью ансамбля из трех разнородных нечетких когнитивных карт, уменьшается по сравнению с использованием отдельных когнитивных карт (например, входящей в ансамбль серой нечеткой когнитивной картой), т.е. неопределенность (разброс) оценки состояний концептов при этом существенно снижается.

Практическая значимость: приведен пример применения предложенной методики для оценки рисков обеспечения целостности телеметрической информации в промышленной сети автоматизированной системы управления технологическими процессами нефтедобывающего предприятия и непрерывности технологического процесса. Данная методика позволяет получить качественную и количественную оценку показателей риска с учетом всей совокупности объективных и субъективных факторов неопределенности.

Ключевые слова: кибербезопасность, оценка рисков, когнитивное моделирование, интервальные нечеткие множества, обобщенная нечеткая когнитивная карта, ансамбль нечетких когнитивных карт, целостность информации.

DOI:10.21681/2311-3456-2020-2-11-21

Введение

Одним из непременных условий построения эффективной цифровой экономики является обеспечение надежной и безопасной работы автоматизированных систем управления сложными технологическими процессами (АСУ ТП), составляющих основу производственного цикла на современных промышленных предприятиях. В то же время, как показывает статистика последних лет, резко возросло число случаев, связанных с попытками или успешной реализацией целенаправленных (targeted) атак на компьютеры АСУ. Так, согласно данным «Лаборатории Касперского»[5], общий процент промышленных компьютеров в мире, на которых было обнаружено и заблокировано вредоносное ПО, в первом полугодии 2019 г. составил 41,21%, т.е. практически каждый второй компьютер подвергся атаке. В России аналогичный показатель составил 44,8%. Атакам в равной степени подвергались предприятия энергетики, машиностроения, нефтегазового сектора и других не менее важных отраслей, что, безусловно, свидетельствует об остроте складывающейся ситуации и необходимости принятия неотложных мер для ее улучшения.

Усилиями ученых и специалистов всего мира сегодня активно формируется необходимая законодательная и нормативно-правовая база для решения задач, связанных с обеспечением кибербезопасности АСУ ТП промышленных объектов [1]. В качестве основополагающих документов в этой сфере, принятых в нашей стра-

1 Васильев Владимир Иванович, доктор технических наук, профессор, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: vasilyev@ugatu.ac.ru

2 Вульфин Алексей Михайлович, кандидат технических наук, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: vulfin.alexey@gmail.com

3 Герасимова Ильмира Барыевна, доктор технических наук, доцент, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: tarot_gera@mail.ru

4 Картак Вадим Михайлович, доктор физико-математических наук, доцент, Уфимский государственный авиационный технический университет, г. Уфа, Россия. E-mail: kvmail@mail.ru

5 Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2019. URL: https://ics-cert.kaspersky.ru/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/ (дата обращения: 13.03.2020).

не, можно отметить Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Приказы Федеральной службы по техническому и экспертному контролю (ФСТЭК) России № 31 от 14.03.2014 г. и № 239 от 25.12.2017 г., стандарты серии 62443 и 56205. В отличие от задач информационной безопасности, где главной целью является обеспечение конфиденциальности информации в процессе ее сбора, хранения и передачи в информационных системах, на первый план при обеспечении кибербезопасности АСУ ТП выдвигается прежде всего требование обеспечения непрерывности и целостности самого ТП.

В основе перечисленных выше нормативных документов используется методология системного риск-ориентированного подхода к обеспечению кибербезопасности АСУ ТП [2, 3]. В идеологическом плане, данная методология близка к получившей в последние годы методологии когнитивного моделирования, суть которой заключается в построении и последующем анализе нечетких когнитивных карт (Fuzzy Cognitive Maps, FCM) с использованием знаний и опыта экспертов-специалистов в рассматриваемой проблемной области [4-8].

Согласно определению[6] Б. Коско [9], нечеткая когнитивная карта (НКК) – это ориентированный граф, заданный с помощью кортежа множеств

$$\text{НКК} =< C, F, W >,$$

где $C = \{C_i\}$ – множество концептов – вершин графа, в качестве которых выступают факторы, наиболее значимые с точки зрения изучения рассматриваемой системы (проблемы); $F = \{F_k\}$ – множество направленных дуг графа – связей между концептами; $W = \{W_{ij}\}$ – множество вес связей НКК, которые могут быть как положительными $(W_{ij} > 0)$, так и отрицательными $(W_{ij} < 0)$ т.е. «усиливающими» или «ослабляющими» влияние концепта C_i на концепт C_j.

Значения весов (силы связей) W_{ij} могут задаваться с помощью нечеткой лингвистической шкалы, представляющей собой упорядоченное множество лингвистических значений (термов). Каждому из указанных значений лингвистической переменной обычно ставится в соответствие некоторый числовой диапазон, принадлежащий отрезку [0,1] для положительных связей (см. Таблицу 1) или отрезку [- 1,0] для отрицательных связей.

Состояние рассматриваемой НКК в произвольный дискретный момент времени $t = 0,1,2,$ описывается уравнениями состояния следующего вида

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

где $X_i(t)$ – значение переменной состояния *i*-го концепта C_i в момент времени *t*; $X_i(t+1)$ значение этой переменной в момент времени $(t+1)$; *n* – число концептов НКК; f – нелинейная функция концепта, например, функция гиперболического тангенса, отображающая значения аргумента в интервал [-1,1].

Для расчета переменных состояния $X_i(t)$, $(i = 1,2,\ldots,n)$ с помощью уравнений (1) необходимо задать начальные условия, т.е. вектор $X(0) = (X_1(0), X_2(0), \ldots, X_n(0))^T$. Наибольший интерес представляет получение установившихся значений $X_i^* = \lim_{x \to \infty} X_i(t)$.

Таблица 1.

Оценка силы связей между концептами

Лингвистическое значение	Числовой диапазон	Обозначение терма	Точечная оценка нечеткой силы связи
Не_влияет	0	Z	0
Очень_слабая	(0; 0,15]	VL	0,100
Слабая	(0,15; 0,35]	L	0,250
Средняя	(0,35; 0,6]	M	0,475
Сильная	(0,6; 0,85]	H	0,725
Очень_сильная	(0,85; 1]	VH	0,925

6 Kosko B. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. 1986. Vol. 1. pp. 65-75.

Не останавливаясь подробно на вопросе о выборе состава концептов НКК и перечня их взаимосвязей (подобная задача обсуждается, например, в [8]), отметим, что не менее маловажной является задача оценки силы связей (весов) НКК. В качестве возможных путей решения данной проблемы рядом авторов были предложены специальные конструкции (расширения) НКК, связанные с представлением силы связей НКК в виде некоторых интервальных оценок. К числу подобных структур НКК относятся такие разновидности НКК, как серые НКК (Grey FCM) [10], интервально-значные НКК (Interval-Valued FCM) [11], грубые НКК (Rough FCM) [12], интуиционистские НКК (Intuitionistic FCM)[7] [13].

Ниже основное внимание будет уделено применению, помимо классической НКК, также двух вариантов расширения НКК, а именно – серой и интуиционистской НКК (будем называть их обобщенными НКК), для решения задачи оценки рисков кибербезопасности АСУ ТП промышленных объектов. Особый интерес представляет анализ возможности построения ансамблей НКК для повышения эффективности оценки риска за счет использования нескольких вариантов формализации знаний и опыта эксперта. Этот вопрос практически не освещен в литературе, за исключением ряда работ [14-17], посвященных главным образом использованию указанных когнитивных моделей при построении систем обнаружения атак и оценке связанных с ними информационных рисков.

Обобщенные нечеткие когнитивные карты

Переходя к рассмотрению обобщенных НКК, будем полагать, что уравнения состояния НКК (1) в общем виде могут быть переписаны как

$$X_i(t+1) = f\left(X_i(t) \oplus \left(\bigoplus_{\substack{j=1 \\ (j \neq i)}}^{n} W_{ji} \otimes X_j(t) \right) \right), \quad (2)$$

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

где веса связей W_i и переменные состояния $X_i(t+1)$, $X_i(t)$ представляют собой интервальные числа, определяемые как элементы некоторых нечетких интервальных множеств; $\oplus$ и $\otimes$ – операции сложения и умножения интервальных чисел, заданные на нечетких интервальных множествах; f – функция активации.

В качестве основы для построения НКК могут использоваться различные способы задания интервальных нечетких множеств (НМ).

Серые НКК (СНКК)

Под серым множеством (grey set) $A \subseteq X$ понимается множество

$$A = \left\{ < x, \left[\underline{x}, \overline{x} \right] > | \; x \in X \right\}, \quad (3)$$

элементами которого являются серые числа $x \in \left[\underline{x}, \overline{x} \right] \leq A$, т.е. числа, которые могут принимать любые значения в пределах некоторого диапазона $\left[\underline{x}, \overline{x} \right] \in [0,1]$, где $\underline{x}$ и $\overline{x}$ – соответственно нижняя и верхняя граница серого числа x; X – универсальное множество. Число $\delta x = x - \underline{x}$ называется серостью (greyness) числа x, а $x^0 = \left(\overline{x} - \underline{x} \right) / 2$ – «отбеленным» (центральным) значением этого числа.

Веса связей между концептами серой НКК задаются в виде серых чисел $\left[\underline{W}_{ij}, \overline{W}_{ij} \right]$; переменные состояния концептов также представляют собой серые числа $\left[\underline{X}_i, \overline{X}_i \right]$, вычисляемые с помощью уравнений (2).

Интуиционистские НКК (ИНКК)

Понятие интуиционистского нечеткого множества (intuitionistic fuzzy set) было впервые введено в 1986 г. болгарским математиком К. Атанасовым.

Под интуиционистским нечетким множеством при этом понимается множество вида

$$A = \left\{ < x, \mu_A(x), \nu_A(x) > | \; x \in X \right\}, \quad (4)$$

где $\mu_A(x)$ и $\nu_A(x)$ определяют соответственно степень принадлежности и степень непринадлежности элемента $x \in X$ (интуиционистского нечеткого числа) множеству $A \subseteq X$; $0 \leq \mu_A(x) \leq 1$; $0 \leq \nu_A(x) \leq 1$. Существенное отличие от «обычных» нечетких множеств заключается в выполнении условия: $\mu_A(x) + \nu_A(x) \leq 1$, т.е. допускается случай, когда сумма значений $\mu_A(x)$ и $\nu_A(x)$ меньше единицы. Таким образом, в рассмотрение вводится еще один параметр, называемый степенью нерешительности (сомнения, неуверенности – hesitancy degree) и определяемый как

$$\pi_A(x) = 1 - \mu_A(x) - \nu_A(x); \quad 0 \leq \pi_A(x) \leq 1. \quad (5)$$

Имеется в виду, что эксперт зачастую затрудняется определить значения функции принадлежности $\mu_A(x)$ и непринадлежности $\nu_A(x)$ элемента x множеству A в силу недостоверности располагаемых им данных или отсутствия у него достаточно полной информации. При этом всегда имеет место равенство $\mu_A(x) + \nu_A(x) + \pi_A(x) = 1$. Очевидно, что если $\pi_A(x) = 0$, то мы имеем дело с обычным нечетким множеством, где $\mu_A(x) + \nu_A(x) = 1$.

Веса связей в интуиционистской НКК задаются в виде значений принадлежности и непринадлежности

7 Papageorgiou E.I., Iakovidis D.K. Intuitionistic Fuzzy Cognitive Maps // IEEE Transactions on Fuzzy Systems, April 2013, vol. 21, № 2, pp. 342-354. DOI:10.1109/TFUZZ.2012.2214224.

веса W_{ij} соответствующему нечеткому подмножеству, т.е. парой чисел $< W_{ij}^{\mu}, W_{ij}^{\nu} >$, или с помощью значений принадлежности и степени нерешительности $< W_{ij}^{\mu}, W_{ij}^{\pi} >$ Эти способы задания весов равноценны, поскольку всегда выполняется условие

$$W_{ij}^{\pi} = 1 - W_{ij}^{\mu} - W_{ij}^{\nu}.$$

В отношении расчета переменных состояния концептов, авторами работы [13] предложены два различных подхода: 1) концепция интуиционистского НМ, основанная на введении понятия степени нерешительности W_{ij}^{π}, используется только при определении силы взаимного влияния концептов W_{ij} (соответствующий вариант интуиционистской НКК получил в [13] обозначение iFCM-I); 2) интуиционистская оценка нерешительности используется как при определении силы взаимного влияния W_{ij}, так и для определения текущего состояния каждого концепта C_i на основе уравнения (1), т.е. состояние каждого концепта описывается парой значений $< X_i^{\mu}, X_i^{\nu} >$ в терминах принадлежности и непринадлежности соответствующему подмножеству (значению лингвистической переменной X_i), – данный вариант интуиционистской НКК авторы [13] назвали iFCM-II).

Учитывая более высокую сложность модели iFCM-II по сравнению с моделью iFCM-I, выберем для дальнейшего анализа более простой вариант интуиционистской НКК – когнитивную карту iFCM-I, уравнения состояния которой принимают в данном случае следующий вид [10]:

$$X_i(t+1) = f\left(X_i(t) + \sum X_i(t) W_{ji}^{\mu}\left(1 - W_{ji}^{\pi}\right)\right), \quad (i = 1, 2, \ldots, n). \quad (6)$$

Заметим, что весовой фактор $W_{ji}^{\mu}\left(1 - W_{ji}^{\pi}\right)$ принимает нулевое значение, если 2 концепта C_j и C_i не связаны между собой $\left(W_{ji} = 0\right)$ или если степень нерешительности W_{ji}^{π} становится равной 1.

Перейдем непосредственно к задаче оценке рисков кибербезопасности АСУ ТП с использованием сценарного моделирования на основе рассмотренных выше разновидностей НКК и их ансамбля.

Использование аппарата обобщенных НКК для оценки риска кибербезопасности сети АСУ ТП нефтедобывающего предприятия

В качестве исследуемого объекта защиты рассматривается АСУ ТП нефтедобывающего предприятия, интегрированная в комплексную систему оперативного контроля и управления в реальном масштабе времени, и позволяющая передавать накапливаемые технологические данные в системы управления производственными процессами вышележащих уровней. Технологическая цепочка включает основные элементы: добыча нефти, сбор нефти, подготовка нефти, транспортировка товарной нефти.

Обобщенная структурная схема территориально распределенной системы обустройства месторождения [18, 19] и транспорта товарной нефти (ТТН), представлена на рис. 1, где: УПН – установка подготовки нефти; ЦПС – центральный пункт сбора; НПС – нефтеперекачивающая станция; ПСП – приемо-сдаточный пункт; ГСС – газосборная сеть; 1 – ВПТ – внутри промысловой трубопровод; ДС – добывающие скважины; НС – нагнетающая скважина; ВС – водозаборная скважина; КС – куст скважин; 2 – водовод; 3 – нефтесборный трубопровод; МН – магистральный нефтепровод; АГЗУ – автоматическая групповая замерная установка; ДНС – дожимная насосная станция; УПСВ – установка предварительного сбора воды; КНС – кустовая насосная станция.

Согласно терминологии ГОСТ 62443, необходимо реализовать несколько стадий анализа и моделирования объекта защиты. Первой стадией является создание референсной модели объекта защиты, позволяющей выделить основные виды деятельности, технологические цепочки и процессы, АСУ и прочие активы, распределенные по 5 логическим уровням.

Подсистемы АСУ ТП месторождения можно рассматривать как отдельные зоны безопасности, объединяемые по принципу единства выполняемых функций и требований к безопасности их реализации. Ввиду сложности анализируемого объекта, рассмотрим фрагмент референсной модели архитектуры АСУ ТП месторождения, включающий основные элементы АСУ кустовых площадок, телекоммуникационное оборудование, линии связи и т.п. (рис. 2).

Основные последствия реализации атак на АСУ кустовых площадок:

- останов кустовой площадки;
- блокировка систем противоаварийной защиты;
- блокировка автоматизированных систем пожаротушения;
- потеря возможности мониторинга параметров оборудования и ТП;
- перевод объекта в аварийный режим.

Согласно отчетам «Лаборатории Касперского» и Positive Technologies[8] [20, 21], наиболее часто подвергаются атакам следующие элементы промышленных систем: SCADA-системы, ПЛК, инфраструктура и ОС, сетевые протоколы.

Для рассматриваемого фрагмента референсной модели архитектуры АСУ ТП кустовых площадок на основе данных BSI[9], предлагается проанализировать возможные векторы атак, реализуемые внутренним зло-

8 Уязвимости в АСУ ТП: итоги 2018 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019/ (дата обращения: 13.03.2020).

9 Обеспечение кибербезопасности промышленного IT- контура. URL: https://www.pta-expo.ru/spb/ethernet/2014/prosoft_ProSoft_2.pdf (дата обращения: 13.03.2020).

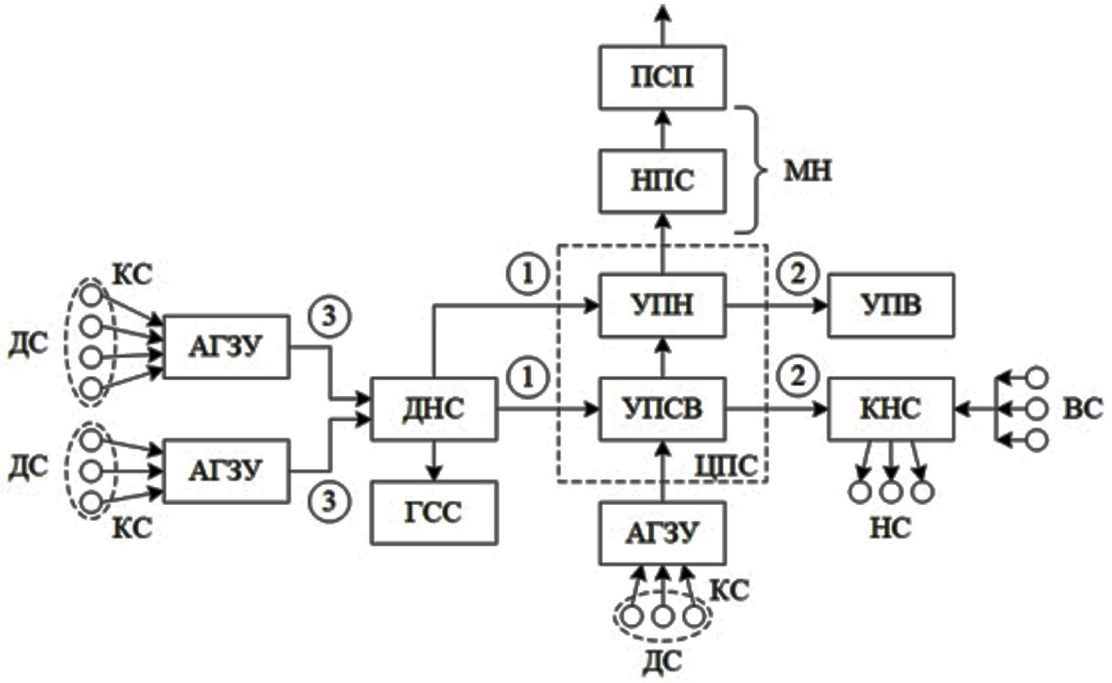


Рис. 1. Обобщенная структурная схема территориально-распределенной системы обустройства месторождения и транспорта товарной нефти

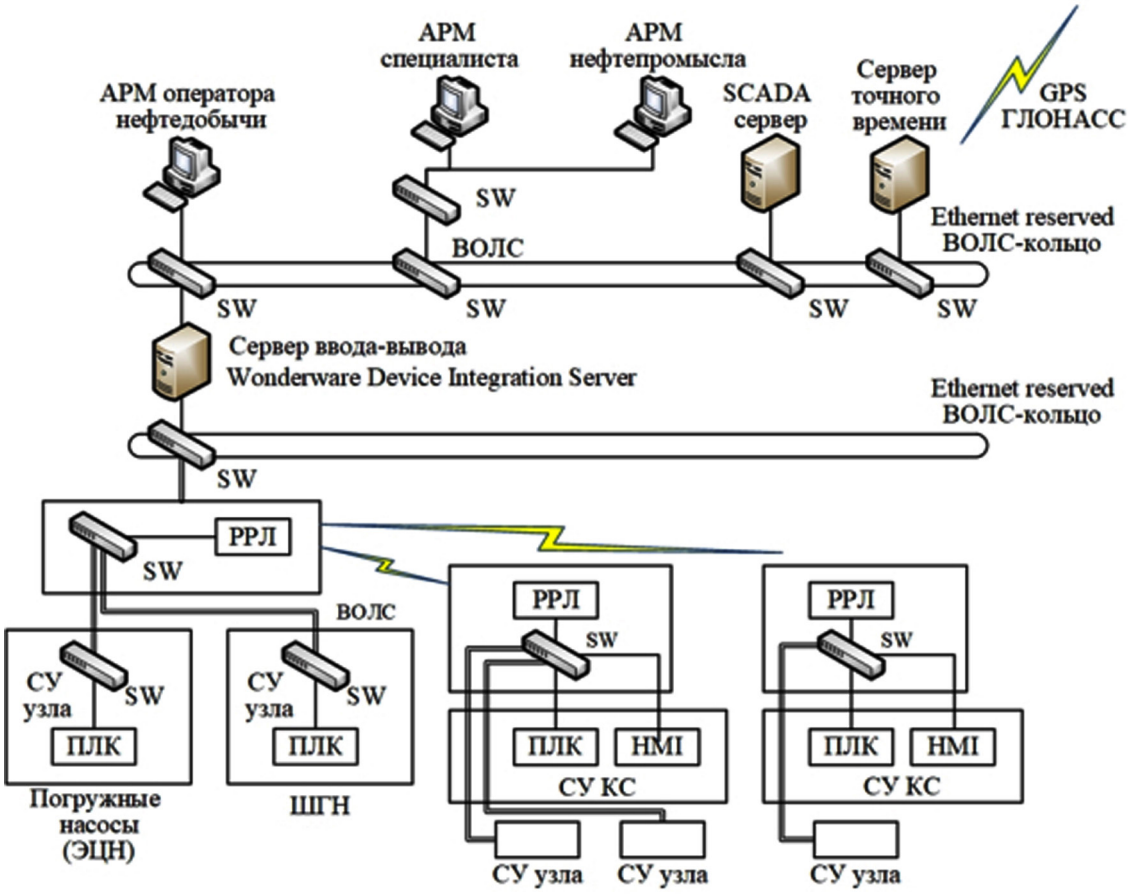


Рис. 2. Фрагмент референсной модели архитектуры АСУ ТП кустовых площадок

DOI:10.21681/2311-3456-2020-2-11-21

умышленником (в последнем случае это такие атаки, как подмена исполняемых файлов ПО серверов и АРМ, перезапись проектов ПЛК в ходе работы системы, отказ в обслуживании оборудования).

Исходя из сформированного списка векторов атак и последствий их реализации, рассмотрим задачу анализа рисков кибербезопасности промышленных объектов с учетом воздействия на систему возможных внутренних угроз, используя в качестве инструмента моделирования аппарат когнитивного моделирования. Когнитивная карта для оценки рисков кибербезопасности АСУ ТП кустовых площадок представлена на рис. 3.

Основные концепты когнитивной карты приведены в таблице 2.

Рассмотрим три варианта реализации НКК (обычная НКК, серая НКК и интуиционистская НКК). В таблице 3 приведены значения весов связей между концептами, определенные экспертами.

Рассмотрим сценарий когнитивного моделирования воздействия внутреннего злоумышленника (активация концепта-драйвера C_1), эксплуатирующего уязвимости программных и аппаратных компонент системы, с применением указанных вариантов построения НКК.

Для НКК и интуиционистской когнитивной карты изменение во времени состояний концептов приведено на рис. 4.

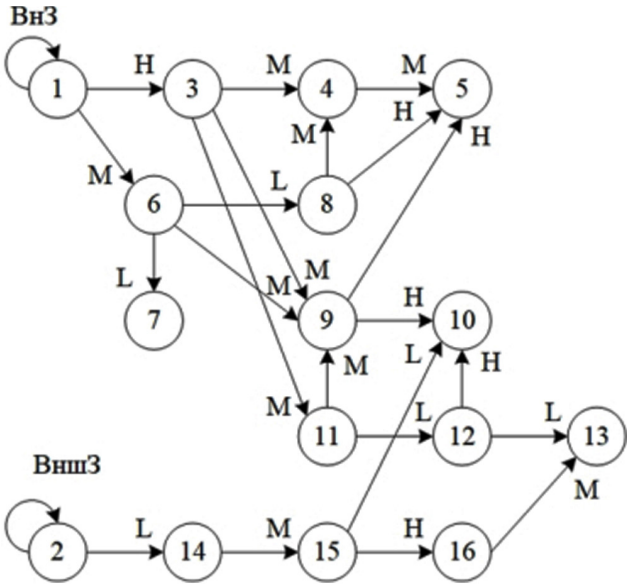


Рис. 3. Когнитивная карта для оценки рисков кибербезопасности АСУ ТП

Таблица 2

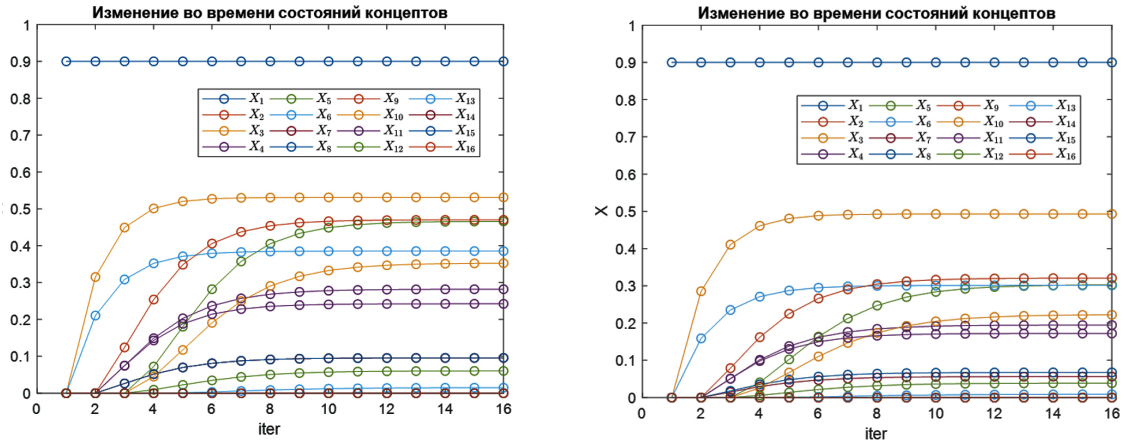
Список концептов когнитивной карты анализа рисков кибербезопасности промышленного объекта

Концепт	Название концепта
C_1	Воздействие внутреннего злоумышленника
C_2	Воздействие внешнего злоумышленника
C_3	Физический доступ к АРМ оператора
C_4	Авторизация с правами легитимного пользователя системы
C_5	Несанкционированное управление кустовой площадкой. Целевой концепт (X_5).
C_6	Эксплуатация уязвимостей сетевого оборудования и/или ошибок конфигурации.
C_7	Отказ в обслуживании сети нижнего уровня промышленного объекта. Целевой концепт (X_7).
C_8	Прослушивание сетевого трафика и перехват данных учетных записей пользователей
C_9	Изменение алгоритма управления объектами промышленной системы за счет модификации конфигурационных файлов PLC (использование протоколов HTTP + FTP)
C_{10}	Нарушение логики работы промышленного объекта. Целевой концепт (X_{10}).
C_{11}	Доступ к ОС через протоколы SSH/Telnet (эксплуатация уязвимостей удаленного доступа)
C_{12}	Эксплуатация уязвимостей датчиков сбора параметров технического объекта (-ов) и подмена конфигурационных файлов
C_{13}	Модификация актуальных параметров телеметрии (нарушение целостности). Целевой концепт (X_{13}).
C_{14}	Подмена сигнала точного времени в зоне приема антенны (GPS/ГЛОНАСС)
C_{15}	Установка некорректного времени на сервере точного времени (NTP)
C_{16}	Нарушение последовательности технологических событий, отображаемых в SCADA системе

Таблица 3

Веса связей между концептами НКК

Вес связи $C_i \to C_j$	**Обычная НКК**	**Серая НКК**	**Интуиционистская НКК (iFCM-I)**	
W_{ij}	W_{ij}	$\left[\underline{W}_{ij}, \overline{W}_{ij}\right]$	W_{ji}^{μ}	W_{ji}^{π}
W_{11}	1	[1; 1]	1	0
W_{13}	0,725	[0,6; 0,85]	0,725	0,1
W_{16}	0,475	[0,35; 0,6]	0,475	0,25
W_{22}	1	[1; 1]	1	0
$W_{2\,14}$	0,25	[0,15; 0,35]	0,25	0,1
W_{34}	0,475	[0,35; 0,6]	0,475	0,25
W_{39}	0,475	[0,35; 0,6]	0,475	0,25
$W_{3\,11}$	0,475	[0,35; 0,6]	0,475	0,25
W_{45}	0,475	[0,35; 0,6]	0,475	0,25
W_{67}	0,25	[0,15; 0,35]	0,25	0,25
W_{68}	0,25	[0,15; 0,35]	0,25	0,1
W_{69}	0,475	[0,35; 0,6]	0,475	0,25
W_{84}	0,475	[0,35; 0,6]	0,475	0,25
W_{85}	0,725	[0,6; 0,85]	0,725	0,1
W_{95}	0,725	[0,6; 0,85]	0,725	0,1
$W_{9\,10}$	0,725	[0,6; 0,85]	0,725	0,1
$W_{11\,9}$	0,475	[0,35; 0,6]	0,475	0,25
$W_{11\,12}$	0,25	[0,15; 0,35]	0,25	0,1
$W_{12\,10}$	0,725	[0,6; 0,85]	0,725	0,25
$W_{12\,13}$	0,25	[0,15; 0,35]	0,25	0,1
$W_{14\,15}$	0,475	[0,35; 0,6]	0,475	0,25
$W_{15\,10}$	0,25	[0,15; 0,35]	0,25	0,1
$W_{15\,16}$	0,725	[0,6; 0,85]	0,725	0,1
$W_{16\,13}$	0,475	[0,35; 0,6]	0,475	0,25



а) *б)*

Рис. 4. Изменение во времени состояний концептов НКК (а) и ИНКК (б)

Изменение параметров состояний концептов СНКК («серость» и «белизна» оценки состояния) показаны на рис. 5.

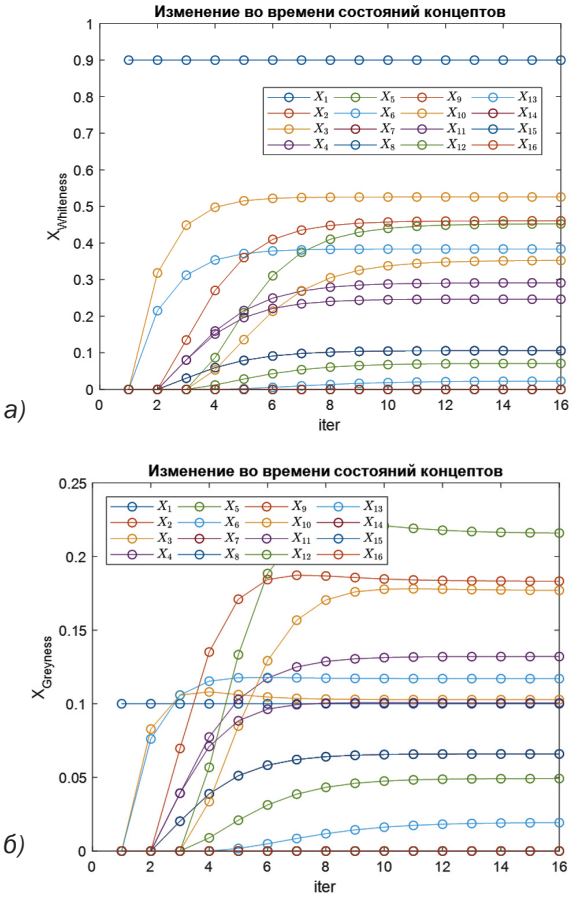


Рис. 5. Изменение во времени состояний концептов СНКК: (а) стабилизация «белого» значения концепта (б) стабилизация «серости» концепта

В таблице 4 и на рис. 6 показаны результаты моделирования локальных относительных рисков угроз кибербезопасности промышленного объекта для целевых концептов: C_5, C_7, C_{10},C_{13}.

Таблица 4

Итоговые результаты моделирования локальных относительных рисков угроз кибербезопасности промышленного объекта

Тип НКК	R_5	R_7	R_{10}	R_{13}
НКК	0,466	0,096	0,353	0,015
СНКК	0,453	0,106	0,353	0,023
ИНКК	0,303	0,057	0,223	0,009
$\underline{R_i}$, СНКК	0,237	0,040	0,176	0,003
$\overline{R_i}$, СНКК	0,669	0,171	0,530	0,042

Тип НКК	R_5	R_7	R_{10}	R_{13}
Среднее для всех карт	0,407	0,086	0,310	0,015
Отклонение	0,070	0,020	0,058	0,005

Под локальным относительным риском R_i понимается потенциальный ущерб, наносимый *i*-ому активу АСУ ТП предприятия (в относительных единицах) и приводящий к нарушению целостности телеметрической информации, содержащей сведения о балансе материальных потоков на объекте (дебит жидкости, энергетические затраты и др.), и к нарушению хода самого ТП. Предполагается, что значение риска вычисляется как $R_i = X_i^*$, где X_i^* – установившееся значение состояния i-го целевого концепта (i = 5, 7, 10, 13).

Заметим, что средневзвешенная оценка локальных рисков, формируемая с помощью ансамбля когнитивных карт (см. таблицу 4), более предпочтительна с точки зрения разброса оценок состояния целевых концептов, чем использование отдельных НКК. Разброс оценок состояния концептов ансамбля меньше, чем разброс оценок их серых значений с помощью СНКК, в среднем в 1,5-1,7 раза, что говорит о снижении влияния фактора субъективности на результаты оценки рисков.

Как следует из рис. 6 и таблицы 4, наибольшее значение риска $R_5 = X_5^* = 0,41$ соответствует целевому концепту C_5 («Несанкционированное управление кустовой площадкой»), что в свою очередь, указывает на необходимость принятия дополнительных мер по снижению этого показателя. Это может быть сделано в частности посредством применения соответствующих средств защиты информации: межсетевых экранов для сегментирования промышленной сети, локализации сетевого трафика внутри виртуальных сетей и т.п. Основные недостатки существующей конфигурации связаны с использованием учетных записей и параметров промышленных контроллеров и сетевого оборудования, задаваемых производителем по умолчанию. Аналогичные мероприятия, направленные на снижение других показателей риска, позволят обеспечить предъявляемые требования к обеспечению кибербезопасности АСУ ТП. Как показало сценарное моделирование, применение указанных средств защиты и организационных мер позволяет снизить оценку локальных рисков на 10-15 %.

Таким образом, применение предложенной методики нечеткого когнитивного моделирования позволяет дать обоснованную качественную и количественную оценку показателей рисков обеспечения кибербезопасности АСУ ТП промышленного объекта с учетом мнений экспертов – специалистов в рассматриваемой предметной области, что в свою очередь, может явиться основой для выбора эффективных защитных контрмер в соответствии с требованиями существующих нормативных документов.

Заключение

Рассмотрена процедура оценки рисков обеспечения кибербезопасности промышленной сети АСУ ТП

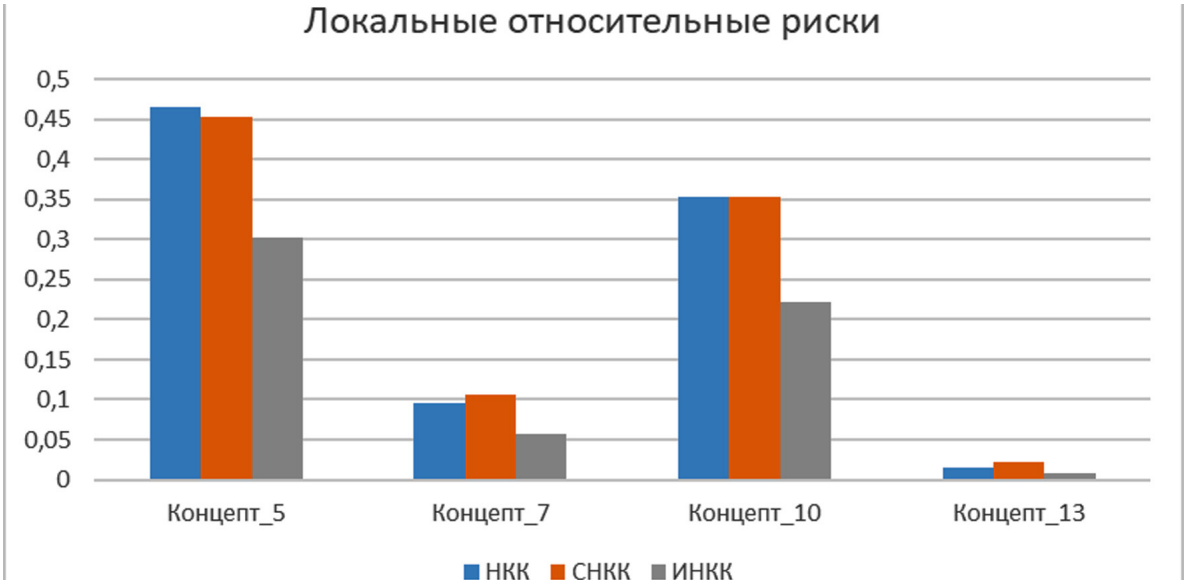


Рис. 6. Локальные относительные риски R_i для целевых концептов C_5, C_7, C_{10} C_{13}

нефтедобывающего предприятия с использованием когнитивного моделирования на основе классических, серых и интуиционистских НКК и их ансамбля. Реализованы основные стадии анализа и моделирования объекта защиты, согласно ГОСТ 62443: построен фрагмент референсной модели архитектуры АСУ ТП месторождения, включающий основные элементы АСУ кустовых площадок. Рассмотрено применение предложенной методики для оценки рисков обеспечения целостности телеметрической информации в промышленной сети и непрерывности технологического процесса.

При использовании технологий когнитивного моделирования в рамках предложенной методики одной из основных проблем является оценка силы связей концептов. Необходимо учитывать субъективное мнение каждого эксперта, и не сводить эти мнения к некоторой усредненной числовой оценке, а применять способы учета возникающей неопределенности за счет различных подходов к формализации знаний экспертов при построении НКК. Применение ансамбля нечетких когнитивных карт позволяет учесть неопределенность мнений экспертов в оценке локального риска по сравнению с оценками, получаемыми отдельными НКК.

Таким образом, предложенная методика позволяет получить качественную и количественную оценку показателей риска с учетом совокупности объективных и субъективных факторов неопределенности.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 20-08-00668 А и 18-08-00638 А.

Рецензент: *Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, МГТУ им. Н.Э. Баумана, г. Москва, Россия, E-mail: a.markov@bmstu.ru*

Литература

1. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции). // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4(30). С. 66-74. DOI:10.14529/secur180410.
2. Массель А.Г., Гаськова Д.А. Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики // Энергетическая политика. 2018. № 5. С. 62-72.
3. Массель Л.В. и др. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17).
4. Foreman C., Turner M., Perusich K. Educational Modules in Industrial Control Systems for Critical Infrastructure Cyber Security. In ASEE Annual Conference and Exposition, Conference Proceedings. 2015. Vol. 122. pp. 01.
5. Stylios C.D., Bourgani E., Georgopoulos V.C. Impact and Applications of Fuzzy Cognitive Map Methodologies. In Beyond Traditional Probabilistic Data Processing Techniques: Interval, Fuzzy etc. Methods and Their Applications. Springer, Cham, 2020. pp. 229-246.
6. Горелова Г.В. Когнитивные исследования сложных систем // Системный анализ в проектировании и управлении. 2019. Т. 23. № 3.
7. Захарова А.А., Подвесовский А.Г., Исаев Р.А. Математическое и программное обеспечение поддержки когнитивного моделирования слабоструктурированных организационно-технических систем // СРТ2019 Международная научная конференция Нижегородского государственного архитектурно-строительного университета и Научно-исследовательского центра физико-технической информатики. 2019. С. 131-141.

8. Кулинич А.А. Ситуационный, когнитивный и семиотический подходы к принятию решений в организациях // Открытое образование. 2016. Т. 20. № 6. С. 9-16.
9. Osoba O.A., Kosko B. Fuzzy cognitive maps of public support for insurgency and terrorism // The Journal of Defense Modeling and Simulation. 2017. Vol. 14. No. 1. pp. 17-32. DOI: 10.1177/ 1548512916680779
10. Salmeron J.L., Palos-Sanchez P.R. Uncertainty propagation in fuzzy grey cognitive maps with Hebbian-like learning algorithms // IEEE transactions on cybernetics. 2017. Vol. 49. No. 1. pp. 211-220.
11. Hajeck P., Prochazka O. Interval-valued fuzzy cognitive maps for supporting business decisions. In Proceedings of IEEE International Conference on Fuzzy Systems, Vancouver, BC, Canada, July 2016, pp. 531-536. DOI: 10.1109 / FUZZ-IEEE.2016.7737732
12. Espinosa M.L., Depaire B., Vanhoof K. Fuzzy Cognitive Maps with Rough Concepts. In Proceeding of the 9th IFIP WG 12.5 International Conference, AIAI 2013: Artificial Intelligence Applications and Innovations, Paphos, Cyprus, Sept. 30 – Oct. 2, 2013, pp. 527-536. DOI: 10.1007/978-3-642-41142-7
13. Hajek P., Froelich W., Prochazka O. Intuitionistic Fuzzy Grey Cognitive Maps for Forecasting Interval-Valued Time Series // Neurocomputing. 2020. DOI: 10.1016/j.neucom.2020.03.013
14. Salmeron J.L. A Fuzzy Grey Cognitive Map-based Intelligent Security System. In Proceeding of 2015 IEEE International Conference on Grey Systems and Intelligent Services, Leicester, UK, August 2015. DOI: 10.1109 / GSIS.2015.7301813
15. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. 2018. Т. 24. № 10. С. 657-664.
16. Lei Y., Liu J., Yin H. Intrusion detection techniques based on improved intuitionistic fuzzy neural networks // 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS). IEEE, 2016. pp. 518-521.
17. Reji M. et al. A genetic-Fuzzy Approach for Detection of Worm Attack in Ad-Hoc Wireless Networks // Indian Journal of Public Health Research & Development. 2017. Vol. 8. No. 4. pp. 1312-1321.
18. Хачатуров В.Р. и др. Системы планирования и проектирования для нефтегазобывающих регионов и месторождений: математические модели, методы, применение // Исследовано в России. 2012. № 15. С. 158.
19. Шадькова Д.К., Коркишко А.Н. Стоимостной инжиниринг как основа управления проектом обустройства месторождения на примере компании ПАО «ГАЗПРОМ НЕФТЬ» // Фундаментальные исследования. 2017. Т. 4. № 12. С. 930-934.
20. Грачков И.А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. 2018. Т. 25. № 1. С. 90-98. DOI:10.26583/bit.2018.1.09.
21. Сабиров Р.А., Увайсов С.У. Применение средств обеспечения информационной безопасности в промышленных системах управления // Север России: стратегии и перспективы развития: Материалы III Всероссийской научно-практической конференции, г. Сургут, 2017, с. 140-143.

ANALYSIS OF CYBERSECURITY RISK WITH USE OF FUZZY COGNITIVE MAPS

Vasilyev V.I.[10], Vulfin A.M.[11], Gerasimova I.B.[12], Kartak V.M.[13]

Purpose: *obtaining of qualitative and quantitative assessment of risk indices with account of the set of objects and subjective uncertainty factors affecting these indices.*

Methods: *automated technological processes control and monitoring systems risk assessment by means of construction and simulation of Ensemble Fuzzy Cognitive maps, based on provisions of the theory of interval fuzzy sets.*

Results: *The usage of classical, grey and intuitionistic fuzzy cognitive maps for solving the problem of cybersecurity risk assessment of industrial objects is considered. It is shown that average-weighted estimate of local risk, forming with use of ensemble of 3 different fuzzy cognitive maps, is reduced compared with using separate cognitive maps (e.g., grey fuzzy cognitive map in the ensemble composition), i.e. the uncertainty (variance) of concepts state assessment here considerably reduces.*

Practical relevance: *The example of using the offered technique for risk assessment of telemetric information integrity in industrial network of oil-producing enterprise automated technological processes control and monitoring*

10 Vladimir Vasilyev, Dr.Sc., Professor, Ufa State Aviation Technical University, Ufa, Russia. E-mail: vasilyev@ugatu.ac.ru
11 Alexey Vulfin, Ph.D., Ufa State Aviation Technical University, Ufa, Russia. E-mail: vulfin.alexey@gmail.com
12 Ilmira Gerasimova, Dr.Sc., Associate Professor, Ufa State Aviation Technical University, Ufa, Russia. E-mail: tarot_gera@mail.ru
13 Vadim Kartak, Dr.Sc., Associate Professor, Ufa State Aviation Technical University, Ufa, Russia. E-mail: kvmail@mail.ru

systems is presented. The offered technique allows us to obtain qualitative and quantitative assessment of risk indices with account of all set of objective and subjective uncertainty factors.

Keywords: *cybersecurity, risk assessment, cognitive modeling, interval fuzzy sets, generalized fuzzy cognitive map, ensemble of fuzzy cognitive maps, information integrity.*

References

1. Vasil`ev V.I., Kirillova A.D., Kuharev S.N. Kiberbezopasnost` avtomatizirovanny`kh sistem upravleniia promy`shlenny`kh ob``ektov (sovremennoe sostoianie, tendentcii). // Vestneyk UrFO. Bezopasnost` v informatcionnoi` sfere. 2018. № 4(30). S. 66-74. DOI:10.14529/secur180410.
2. Massel` A.G., Gas`kova D.A. Metody` i podhody` k obespecheniiu kiberbezopasnosti ob``ektov tcifrovoi` e`nergetiki // E`nergeticheskaia politika. 2018. № 5. S. 62-72.
3. Massel` L.V. i dr. Kiberopasnost` kak odna iz strategicheskikh ugroz e`nergeticheskoi` bezopasnosti Rossii // Voprosy` kiberbezopasnosti. 2016. № 4 (17).
4. Foreman C., Turner M., Perusich K. Educational Modules in Industrial Control Systems for Critical Infrastructure Cyber Security. In ASEE Annual Conference and Exposition, Conference Proceedings. 2015. Vol. 122. pp. 01.
5. Stylios C.D., Bourgani E., Georgopoulos V.C. Impact and Applications of Fuzzy Cognitive Map Methodologies. In Beyond Traditional Probabilistic Data Processing Techniques: Interval, Fuzzy etc. Methods and Their Applications. Springer, Cham, 2020. pp. 229-246.
6. Gorelova G.V. Kognitivny`e issledovaniia slozhny`kh sistem // Sistemny`i` analiz v proektirovanii i upravlenii. 2019. T. 23. № 3.
7. Zaharova A.A., Podvesovskii` A.G., Isaev R.A. Matematicheskoe i programmnoe obespechenie podderzhki kognitivnogo modelirovaniia slabostrukturirovanny`kh organizatcionno-tekhnicheskikh sistem // CPT2019 Mezhdunarodnaia nauchnaia konferentciia Nizhegorodskogo gosudarstvennogo arhitekturno-stroitel`nogo universiteta i Nauchno-issledovatel`skogo centra fiziko-tekhnicheskoi` informatiki. 2019. S. 131-141.
8. Kulinich A.A. Situatcionny`i`, kognitivny`i` i semioticheskii` podhody` k priniatiiu reshenii` v organizatciiakh // Otkry`toe obrazovanie. 2016. T. 20. № 6. C. 9-16.
9. Osoba O.A., Kosko B. Fuzzy cognitive maps of public support for insurgency and terrorism // The Journal of Defense Modeling and Simulation. 2017. Vol. 14. No. 1. pp. 17-32. DOI: 10.1177/ 1548512916680779
10. Salmeron J.L., Palos-Sanchez P.R. Uncertainty propagation in fuzzy grey cognitive maps with Hebbian-like learning algorithms // IEEE transactions on cybernetics. 2017. Vol. 49. No. 1. pp. 211-220.
11. Hajeck P., Prochazka O. Interval-valued fuzzy cognitive maps for supporting business decisions. In Proceedings of IEEE International Conference on Fuzzy Systems, Vancouver, BC, Canada, July 2016, pp. 531-536. DOI: 10.1109 / FUZZ-IEEE.2016.7737732
12. Espinosa M.L., Depaire B., Vanhoof K. Fuzzy Cognitive Maps with Rough Concepts. In Proceeding of the 9th IFIP WG 12.5 International Conference, AIAI 2013: Artificial Intelligence Applications and Innovations, Paphos, Cyprus, Sept. 30 – Oct. 2, 2013, pp. 527-536. DOI: 10.1007/978-3-642-41142-7
13. Hajek P., Froelich W., Prochazka O. Intuitionistic Fuzzy Grey Cognitive Maps for Forecasting Interval-Valued Time Series // Neurocomputing. 2020. DOI: 10.1016/j.neucom.2020.03.013
14. Salmeron J.L. A Fuzzy Grey Cognitive Map-based Intelligent Security System. In Proceeding of 2015 IEEE International Conference on Grey Systems and Intelligent Services, Leicester, UK, August 2015. DOI: 10.1109 / GSIS.2015.7301813
15. Vasil`ev V.I., Vul`fin A.M., Guzairov M.B., Kirillova A.D. Interval`noe ocenivanie informatcionny`kh riskov s pomoshch`iu nechetkikh sery`kh kognitivny`kh kart // Informatcionny`e tekhnologii. 2018. T. 24. № 10. C. 657-664.
16. Lei Y., Liu J., Yin H. Intrusion detection techniques based on improved intuitionistic fuzzy neural networks // 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS). IEEE, 2016. pp. 518-521.
17. Reji M. et al. A genetic-Fuzzy Approach for Detection of Worm Attack in Ad-Hoc Wireless Networks // Indian Journal of Public Health Research & Development. 2017. Vol. 8. No. 4. pp. 1312-1321.
18. Hachaturov V.R. i dr. Sistemy` planirovaniia i proektirovaniia dlia neftegazoby`vaiushchikh regionov i mestorozhdenii`: matematicheskie modeli, metody`, primenenie // Issledovano v Rossii. 2012. № 15. C. 158.
19. Shad`kova D.K., Korkishko A.N. Stoimostnoi` inzhiniring kak osnova upravleniia proektom obustroi`stva mestorozhdeniia na primere kompanii PAO «GAZPROM NEFT`» // Fundamental`ny`e issledovaniia. 2017. T. 4. № 12. C. 930-934.
20. Grachkov I.A. Informatcionnaia bezopasnost` ASU TP: vozmozhny`e vektora ataki i metody` zashchity` // Bezopasnost` informatcionny`kh tekhnologii`. 2018. T. 25. № 1. S. 90-98. DOI:10.26583/bit.2018.1.09.
21. Sabirov R.A., Uvai`sov S.U. Primenenie sredstv obespecheniia informatcionnoi` bezopasnosti v promy`shlenny`kh sistemakh upravleniia // Sever Rossii: strategii i perspektivy` razvitiia: Materialy` III Vserossii`skoi` nauchno-prakticheskoi` konferentcii, g. Surgut, 2017, s. 140-143.