Transaction of Azerbaijan National Academy of Sciences, Series of Physical-Technical and Mathematical Sciences: Informatics and Control Problems, Vol. XXXV, No.6, 2015
www.icp.az/2015/6-08.pdf

УДК 519.712.3

Э.Т. АЛИЕВ, В.И. ГАСАНОВ, З.Р. ДЖАМАЛОВ, А.К. ХУДАДОВА

НЕЧЁТКАЯ КОГНИТИВНАЯ МОДЕЛЬ ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разработана и описана типовая нечёткая когнитивная модель для оценки уровня информационной безопасности на предприятиях. За основу выбрана когнитивная карта, охватывающая достаточно большой спектр факторов влияния на информационную безопасность, причинно-следственные связи между которыми представлены в виде ограниченного набора нечётких импликативных правил.

Ключевые слова: нечёткая когнитивная модель, когнитивная карта, информационная безопасность, система нечеткого вывода

1. Введение. Система комплексного обеспечения информационной безопасности, как и любая организационно-технологическая система, является системой гуманистического типа, т.е. системой, в которой существенная роль принадлежит суждениям и знаниям человека [1]. В отличие от механистических систем, поведение которых допускает численное описание, гуманистические системы являются слабо структурируемыми и гораздо более сложными. Поэтому адекватное управление системой комплексного обеспечения информационной безопасности (СКОИБ) является весьма сложной, слабо структурированной и, соответственно, трудно формализуемой процедурой.

Существующие разработки подобных систем предусматривают применение системного подхода, позволяющего консолидировать разные по своей природе процессы, протекающие в информационной системе. Так, например, в работе [2] описан системный подход к построению комплексной защиты информационной системы предприятия и изложена методика построения такой системы с применением технических и программных (криптографических) средств защиты. Основные принципы и методы аудита информационной безопасности на основе процессорного подхода изложены в [3], где также приведены некоторые методы оценивания информационной безопасности. Однако наиболее основательно системный подход к решению задач безопасности информационных технологий был изложен в работе В. Домарева [4], который предложил трехмерную модель, включающую основные этапы, направления и методы обеспечения безопасности различных систем.

Тем не менее, на сегодняшний день одним из наиболее адекватных инструментов для описания и исследования слабо структурированных систем является *когнитивное моделирование,* которое уже долгое время активно применяется при построении информационных систем поддержки принятия решений в условиях неопределённости [5-8]. При этом основным преимуществом математического аппарата когнитивного анализа является предоставляемая им возможность адаптации моделируемой системы к возможным изменениям во внешней среде[1] [9].

На современной стадии развития информационной и смежных технологий любая СКОИБ, как субстанция, является всего лишь автоматизированной, т.е. не может существовать сама по себе или, другими словами, в отрыве от человека. Она служит человеку и им же оценивается. Поэтому понятие информационной безопасности имеет не только объективную, но и субъективную составляющую, поскольку в конечном итоге оценка

[1] В этом смысле когнитивное моделирование схоже нейросетевому. Однако его субъектность и масштабы применения несравнимо выше.

ее уровня осуществляется самим человеком. Это является достаточно важным фактором, который обуславливает необходимость применения качественных категорий для оценки уровня безопасности, т.е. термов лингвистических переменных, являющихся, как известно, основными структурными единицами естественного языка субъекта управления. Как следствие, именно данная парадигма и объясняет необходимость применения математического аппарата нечёткой логики. В конечном итоге, субъективное мышление ответственного за принятие решений становится причиной появления диапазона так называемой «условной приемлемости» в шкале оценок информационной безопасности [10].

2. Постановка задачи. Основными шагами на пути обеспечения информационной безопасности являются: предвидение, предотвращение, локализация и устранение ущерба от воздействия опасности. При этом сама оценка уровня информационной безопасности всегда относительна, а желание приписать ей числовое значение неприемлемо с точки зрения дальнейшей интерпретации комплексных результатов. Информационная безопасность (ИБ) – это комплексное понятие и не может рассматриваться в виде простой совокупности своих взаимосвязанных и/или взаимозависимых составляющих, т.к. каждая из них критически значима. Поэтому при комплексной оценке ИБ численное описание (или усреднение) составных критериев оценки являются совершенно неприемлемыми.

В работе [4] сформулированы следующие специфические особенности, которые необходимо учитывать при создании СКОИБ:

- неполнота и неопределенность исходной информации о составе и характере угроз;
- наличие многокритериальных задач выбора альтернатив, связанных с необходимостью учета большого числа частных показателей;
- наряду с количественными наличие качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения систем комплексной оценки ИБ;
- невозможность применения классических методов оптимизации.

Учитывая приведенные требования, необходимо разработать такую модель для комплексной оценки уровня ИБ, чтобы на ее основе можно было бы унифицировать подходы к управлению комплексной безопасностью информационной системы.

3. Нечёткая когнитивная модель слабо структурированных систем: общие принципы построения. Когнитивное моделирование слабо структурированных систем предусматривает разработку формальных моделей и методов, позволяющих учитывать так называемые когнитивные возможности субъекта управления, подразумевающие его восприятие, представление, познание в предметной области, понимание и объяснение промежуточных проблем при решении задач управления в условиях неопределенности. При этом основным инструментом такого исследования является когнитивная карта, которая отражает индивидуальные и/или субъективные представления исследуемой проблемы, явления.

Когнитивная карта включает в себя базисные факторы (компоненты) и причинно-следственные связи между ними [5, 9]. С содержательной точки зрения базисные факторы отождествляют и ограничивают наблюдаемые явления как внутри исследуемой системы, так и в окружающей ее среде. Эти факторы интерпретируются субъектом управления как существенные, ключевые параметры или, другими словами, как признаки наблюдаемых экзогенных и эндогенных явлений и процессов.

По сути когнитивная карта – это ориентированный граф над множеством факторов, отражающий, в нашем случае, способ структурирования слабоструктурированных систем и состояний. Изучение взаимодействия факторов в рамках когнитивной карты позволяет оценивать распространение их влияний и, тем самым, описывать поведение (состояния)

исследуемой системы. В свою очередь, анализ когнитивной карты поведения исследуемой системы подразумевает нахождение наиболее значимых факторов влияния и оценку воздействие этих факторов друг на друга. Это предоставляет возможность применять классические методы теории систем, в частности, для моделирования, анализа динамики и управления.

Рассмотрим нечёткую когнитивную модель для оценки уровня комплексной безопасности, на основе заимствованного из [11] тривиального примера когнитивной карты, позволяющей в общих чертах анализировать проблему обеспечения информационной безопасности при обработке данных с использованием средств вычислительной техники (рис. 1).

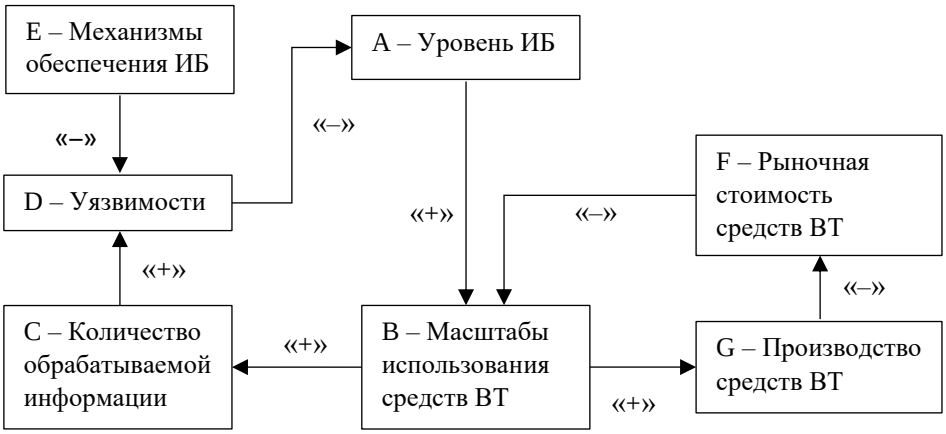

Рис. 1. Когнитивная карта для анализа проблемы обеспечения ИБ

Как видно из рис. 1, проблема ИБ в упрощенной форме описывается в виде неполносвязной структуры, состоящей из семи концептов (факторов): A, B, C, D, E, F, G, и дуг, отражающих соответствующие причинно-следственные связи между отдельными из них. В данном случае это знаковый граф, в котором знак «–» означает, что при увеличении исходного фактора значение зависящего от него факторы уменьшается, и наоборот. А знак «+» означает, что увеличение исходного фактора влечет за собой увеличение зависимого.

Рассмотрим поведение замкнутой подсистемы $A \rightarrow B \rightarrow C \rightarrow D \rightarrow A$ при увеличении масштабов применения ВТ в какой-то организации. Очевидно, что увеличение этих масштабов повлечет за собой увеличение количества обрабатываемой информации, а это, в свою очередь, увеличит степень уязвимости средств ВТ, что неминуемо понизит уровень ИБ и, как следствие, приведет к уменьшению масштабов применения средств ВТ. Это означает, что процесс «затухания» воздействующего на подсистему через фактор B сигнала приведет к стабилизации всего замкнутого контура, т.е. будет осуществляться противодействие отклонению.

Представленная на рис. 1 схема анализа ИБ является все же тривиальной, т.к. на практике взаимодействия двух факторов, например, B и C осуществляются по более сложным функциональным закономерностям, которые в привычной традиционно математической форме очень трудно формализовать. Поэтому возникает необходимость применять механизм нечёткого логического вывода для описания причинно-следственных связей между концептами из сферы ИБ, а сам анализ проводить на основе так называемых нечётких когнитивных карт [12]. В этом случае узловые факторы когнитивной карты интерпретируются как нечёткие множества, а причинно-следственные связи между ними устанавливаются на основе ограниченного набора нечётких лингвистических правил,

определяющих в том числе и весовые коэффициенты связей между факторами. Подобное формальное описание поведения слабо структурированной системы и, в частности, проблемы ИБ называют нечёткой когнитивной моделью.

Сами нечёткие правила формируются в импликативной форме «Если …, тогда …», например, в виде:

«Если x_{k1} есть A_{k1} и x_{k2} есть A_{k2} и …. и x_{kn} есть A_{kn}, тогда y есть B_k»,

где x_{kj} (j=1÷n; k=1, 2, …) входные характеристики, представленные как лингвистические переменные; y – выходная лингвистическая переменная; A_{kj} и B_k – термы (значения) соответствующих лингвистических переменных, описываемых в виде нечётких множеств.

4. Типовая нечёткая когнитивная модель для оценки ИБ. На рис. 1 представлена упрощенная когнитивная карта для анализа проблемы обеспечения ИБ. Однако для оценки уровня ИБ необходимо учитывать исключительно большое количество разноплановых факторы, влияющих на требуемый уровень ИБ. Поэтому для формирования достаточно полного перечня таких факторов произведена их классификация и структуризация принимаемых ими возможных значений. Сформированные перечень классов факторов, списки факторов внутри каждого из классов, и структуризация возможных значений факторов, исполненная в виде термов соответствующих лингвистических переменных, приведены в табл. 1.

Табл. 1
Факторы, влияющие на уровень ИБ

Наименование класса	Наименование фактора	Значение фактора
Особенность обрабатываемой информации	Степень конфиденциальности	1) Очень высокая; 2) Высокая; 3) Средняя; 4) Невысокая
	Объемы	1) Очень большие; 2) Большие; 3) Средние; 4) Малые
	Интенсивность обработки	1) Очень высокая; 2) Высокая; 3) Средняя; 4) Низкая
Архитектура системы	Геометрические размеры системы	1) Очень большие; 2) Большие; 3) Средние; 4) Незначительные
	Территориальная распределенность системы	1) Очень большая; 2) Большая; 3) Средняя; 4) Незначительная
	Структурированность компонентов системы	1) Полностью отсутствует; 2) Частичная; 3) Достаточно высокая; 4) Полная
Условия функционирования системы	Расположение в населенном пункте	1) Очень неудобное; 2) Создает значительные трудности для защиты; 3) Создает определенные трудности для защиты; 4) Удобное
	Расположение на территории объекта	1) Хаотичное; 2) Разбросанное; 3) Распределенное; 4) Компактное
	Обустроенность	1) Очень плохая; 2) Плохая; 3) Средняя; 4) Хорошая
Технология обработки информации	Масштаб обработки	1) Очень большой; 2) Большой; 3) Средний; 4) Незначительный
	Стабильность информации	1) Отсутствует; 2) Частично стабильная; 3) Достаточно упорядоченная; 4) Регулярная
	Доступность информации	1) Общедоступная; 2) С незначительными ограничениями на доступ; 3) С существенными ограничениями на доступ; 4) С полным регулируемым доступом
	Структурированность информации	1) Полностью отсутствует; 2) Частичная; 3) Достаточно высокая; 4) Полная
Организация работы с информацией	Общая постановка дела	1) Очень плохая; 2) Плохая; 3) Средняя; 4) Хорошая
	Укомплектованность кадрами	1) Очень слабая; 2) Слабая; 3) Средняя; 4) Полная
	Уровень подготовки и воспитания кадров	1) Очень низкий; 2) Низкий; 3) Средний; 4) Высокий
	Уровень дисциплины	1) Очень низкий; 2) Низкий; 3) Средний; 4) Высокий
Использование	Предоставление удаленного	1) Отсутствует; 2) Ограниченное; 3) Неограниченное

ИКТ	доступа к своим ИТ-системам	
	Использование интернета для мониторинга рынка	1) Очень низкое; 2) Низкое; 3) Среднее; 4) Высокое
	Использование интернета для взаимодействия с органами власти	1) Очень низкое; 2) Низкое; 3) Среднее; 4) Высокое
	Использование интернета для получения цифровых продуктов	1) Очень низкое; 2) Низкое; 3) Среднее; 4) Высокое
	Использование интернета для осуществления банковских и финансовых операций	1) Очень низкое; 2) Низкое; 3) Среднее; 4) Высокое
	Использование интернета для профессионального образования и подготовки работников	1) Очень низкое; 2) Низкое; 3) Среднее; 4) Высокое
	Наличие Web-сайта	1) Отсутствует; 2) Плохо оформленный; 3) Удовлетворительный; 4) Совершенный
	Доля онлайновых закупок в общем объеме закупок предприятий	1) Очень большая; 2) Большая; 3) Средняя; 4) Незначительная
	Доля онлайновых продаж в обороте предприятий	1) Очень большая; 2) Большая; 3) Средняя; 4) Незначительная

Перечисленные в табл. 1 факторы будем считать лингвистическими переменными, каждая из которых в качестве своего значения принимает одно из указанных термов. Как показали расчёты, общее число различных вариантов потенциально возможных условий защиты превышает астрономическое число $1.7 \cdot 10^{10}$. В привычном смысле представленная классификация факторов (концептов) сопряжена с решением комбинаторной задачи весьма большой размерности и с высоким уровнем неопределенности. Поэтому, исходя из этой классификации рассмотрим задачу определения уровня ИБ на основе нечёткого когнитивного моделирования.

На рис. 2 представлена нечёткая когнитивная карта, охватывающая все концепты из перечня классов, оговоренных в табл. 1. Здесь основным ядром является замкнутый контур $A \rightarrow B \rightarrow C \rightarrow D \rightarrow E \rightarrow F \rightarrow A$, в котором каждое «звено», являясь узловым, представляет собой концепт (или терм), описываемый в виде соответствующего нечёткого множества. Остальные факторы: B_k (k=1÷13), C_i (i=1÷3), D_j (j=1÷4) и E_r (r=1÷4), являются исходными, т.е. нечёткими входными характеристиками предлагаемой нечёткой когнитивной модели для оценки ИБ.

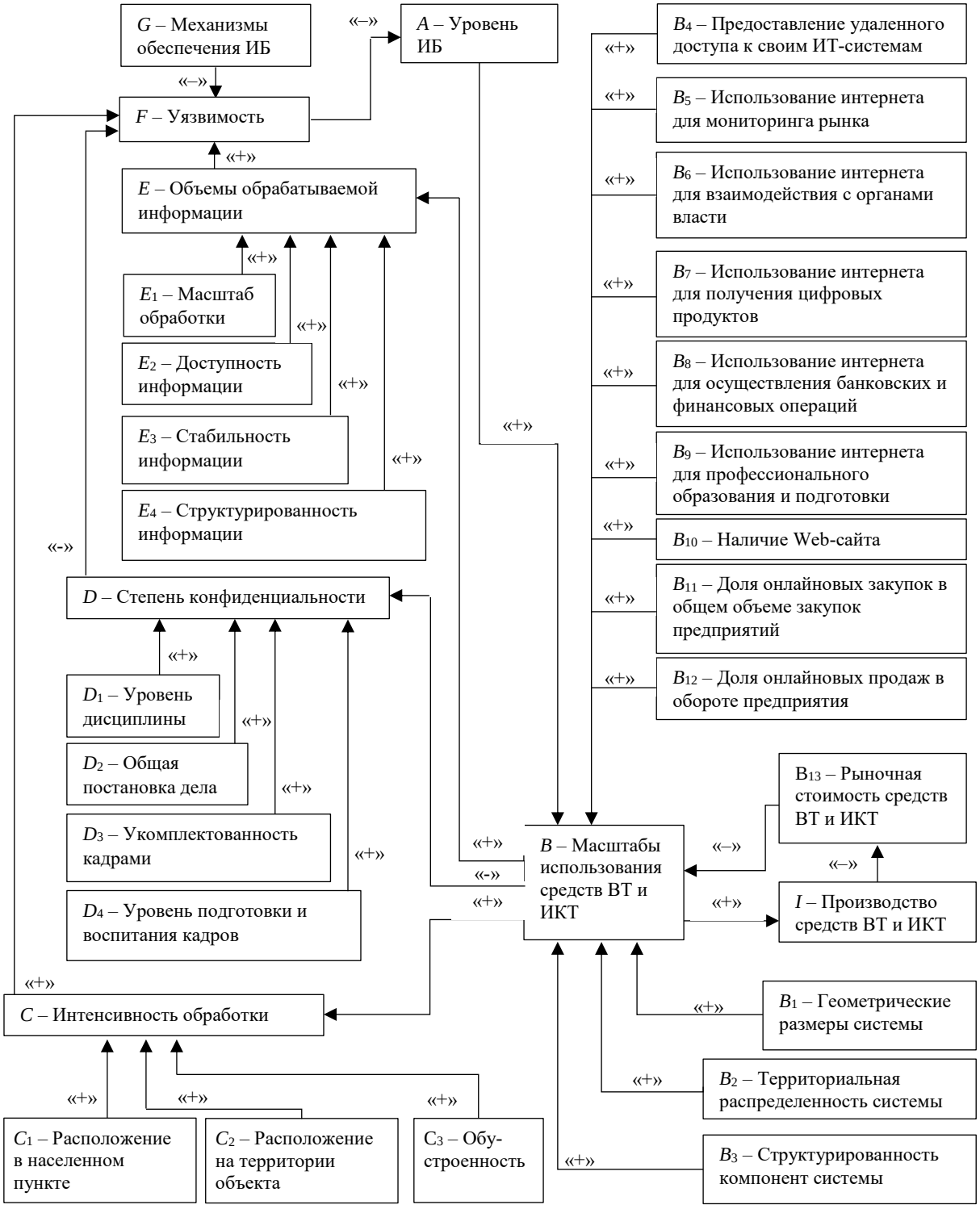

Рис. 2. Нечёткая когнитивная карта для анализа ИБ

Используя указанные в табл. 1 термы входных и выходных лингвистических переменных, все причинно-следственные связи, фигурально обозначенные на рис. 2, можно реализовать посредством тривиальных импликативных правил в нотации пакета MATLAB.

Однако для построения составных и композиционной моделей за основу возьмём нижеследующие высказывания, которые, как нам кажется, более адекватно отражают искомые причинно-следственные связи.

***Уровень масштабов использования средств ВТ и ИКТ*:**

a_1: «Если геометрические размеры системы небольшие, для получения цифровых продуктов предприятие интернет не использует, а также не использует интернет для осуществления своих банковских и финансовых операций, тогда масштабы использования средств ВТ и ИКТ на данном предприятии слишком малые»;

a_2: «Если в дополнение к предыдущим условиям предприятие использует интернет для мониторинга рынка и для взаимодействия с органами власти, тогда масштабы использования средств ВТ и ИКТ на данном предприятии все же очень малые»;

a_3: «Если геометрические размеры системы небольшие, но при этом предприятие использует интернет для получения цифровых продуктов, для осуществления своих банковских и финансовых операций, для профессионального образования и подготовки своих работников, имеет свой web-сайт, а также имеет возможность приобретать средства ВТ и ИКТ по низким рыночным ценам, тогда масштабы использования средств ВТ и ИКТ на данном предприятии являются более чем малыми»;

a_4: «Если предприятие использует интернет для получения цифровых продуктов, для осуществления своих банковских и финансовых операций, для профессионального образования и подготовки своих работников, имеет свой web-сайт, а также имеет возможность приобретать средства ВТ и ИКТ по низким рыночным ценам, тогда масштабы использования средств ВТ и ИКТ на данном предприятии являются все ещё малыми»;

a_5: «Если в дополнение к условиям, оговоренным в e_4, предприятие использует интернет для взаимодействия с органами власти, а также доля его онлайновых закупок в общем объеме закупок существенная и доля онлайновых продаж в обороте предприятия значительная, тогда масштабы использования средств ВТ и ИКТ на данном предприятии большие»;

a_6: «Если к тому же предприятие использует интернет для мониторинга рынка, тогда масштабы использования средств ВТ и ИКТ на данном предприятии более чем большие»;

a_7: «Если структурированность компонент системы предприятия полная, предприятие предоставляет возможность удаленного доступа к своим ИТ-системам, использует интернет для мониторинга рынка, для взаимодействия с органами власти, для получения цифровых продуктов, для осуществления банковских и финансовых операций, для профессионального образования и подготовки своих работников, имеет свой web-сайт, доля его онлайновых закупок в общем объеме закупок существенная и доля онлайновых продаж в обороте предприятия значительная, а также предприятие имеет возможность приобретать средства ВТ и ИКТ по низким рыночным ценам, тогда масштабы использования средств ВТ и ИКТ на данном предприятии очень большие»;

a_8: «Если в дополнение к условиям, оговоренным в e_7, геометрические размеры системы предприятия и её территориальная распределенность очень большие, тогда масштабы использования средств ВТ и ИКТ на данном предприятии являются слишком большими».

Анализ приведенных импликативных высказываний позволяет определить входные характеристики (критерии) в виде термов лингвистических переменных B_k (k=1÷13) и одну выходную лингвистическую переменную B – масштабы использования средств ВТ и ИКТ.

Используемые в высказываниях $a_1 \div a_8$ значения переменной B зададим в виде нечётких подмножеств универсального дискретного множества U={0; 0.1; 0.2; …; 1} следующим образом [13, 14]:

- L=БОЛЬШИЕ: $\mu_L(u)=u$, $u\in U$;
- ML=БОЛЕЕ ЧЕМ БОЛЬШИЕ: $\mu_{ML}(u)=\sqrt{u}$, $u\in U$;
- VL=ОЧЕНЬ БОЛЬШИЕ: $\mu_{VL}(u)=u^2$, $u\in U$;
- TL=СЛИШКОМ БОЛЬШИЕ, $\mu_{TL}(u)=\begin{cases}1, u=1,\\ 0, u<1,\end{cases}$ $u\in U$;
- S=МАЛЫЕ: $\mu_S(u)=1-u$, $u\in U$;
- MS=БОЛЕЕ ЧЕМ МАЛЫЕ: $\mu_{MS}(u)=\sqrt{1-u}$, $u\in U$;
- VS=ОЧЕНЬ МАЛЫЕ: $\mu_{VS}(u)=(1-u)^2$, $u\in U$;
- TS=СЛИШКОМ МАЛЫЕ, $\mu_{TS}(u)=\begin{cases}0, u=1,\\ 1, u<1,\end{cases}$ $u\in U$.

С учетом этих формализмов и термов входных лингвистических переменных B_k (k=1÷13), запишем высказывания a_1÷a_8 виде следующих нечётких импликативных правил:

a_1: «Если B_1=НЕБОЛЬШИЕ и B_7=НЕ ИСПОЛЬЗУЕТ и B_8=НЕ ИСПОЛЬЗУЕТ, тогда B=TS»;

a_2: «Если B_1=НЕБОЛЬШИЕ и B_5=ИСПОЛЬЗУЕТ и B_6=ИСПОЛЬЗУЕТ B_7=НЕ ИСПОЛЬЗУЕТ и B_8=НЕ ИСПОЛЬЗУЕТ, тогда B=VS»;

a_3: «Если B_1=НЕБОЛЬШИЕ и B_7=ИСПОЛЬЗУЕТ и B_8=ИСПОЛЬЗУЕТ и B_9=ИСПОЛЬЗУЕТ и B_{10}=ИМЕЕТ и B_{13}=ПРИЕМЛЕМЫЕ, тогда B=MS»;

a_4: «Если B_7=ИСПОЛЬЗУЕТ и B_8=ИСПОЛЬЗУЕТ и B_9=ИСПОЛЬЗУЕТ и B_{10}=ИМЕЕТ и B_{13}=ПРИЕМЛЕМЫЕ, тогда B=S»;

a_5: «Если B_6=ИСПОЛЬЗУЕТ и B_7=ИСПОЛЬЗУЕТ и B_8=ИСПОЛЬЗУЕТ и B_9=ИСПОЛЬЗУЕТ и B_{10}=ИМЕЕТ и B_{11}=СУЩЕСТВЕННАЯ и B_{12}=ЗНАЧИТЕЛЬНАЯ и B_{13}=ПРИЕМЛЕМЫЕ, тогда B=L»;

a_6: «Если B_5=ИСПОЛЬЗУЕТ и B_6=ИСПОЛЬЗУЕТ и B_7=ИСПОЛЬЗУЕТ и B_8=ИСПОЛЬЗУЕТ и B_9=ИСПОЛЬЗУЕТ и B_{10}=ИМЕЕТ и B_{11}=СУЩЕСТВЕННАЯ и B_{12}=ЗНАЧИТЕЛЬНАЯ и B_{13}=ПРИЕМЛЕМЫЕ, тогда B=ML»;

a_7: «Если B_3=ПОЛНАЯ и B_4=ИСПОЛЬЗУЕТ и B_5=ИСПОЛЬЗУЕТ и B_6=ИСПОЛЬЗУЕТ и B_7=ИСПОЛЬЗУЕТ и B_8=ИСПОЛЬЗУЕТ и B_9=ИСПОЛЬЗУЕТ и B_{10}=ИМЕЕТ и B_{11}=СУЩЕСТВЕННАЯ и B_{12}=ЗНАЧИТЕЛЬНАЯ и B_{13}=ПРИЕМЛЕМЫЕ, тогда B=VL»;

a_8: «Если B_1=БОЛЬШИЕ и B_4=БОЛЬШАЯ и B_3=ПОЛНАЯ и B_4=ИСПОЛЬЗУЕТ и B_5=ИСПОЛЬЗУЕТ и B_6=ИСПОЛЬЗУЕТ и B_7=ИСПОЛЬЗУЕТ и B_8=ИСПОЛЬЗУЕТ и B_9=ИСПОЛЬЗУЕТ и B_{10}=ИМЕЕТ и B_{11}=СУЩЕСТВЕННАЯ и B_{12}=ЗНАЧИТЕЛЬНАЯ и B_{13}=ПРИЕМЛЕМЫЕ, тогда B=TL».

Интенсивность обработки:

b_1: «Если масштабы использования средств ВТ и ИКТ на предприятии большие, тогда интенсивность обработки информации высокая»;

b_2: «Если в дополнение к предыдущему условию расположение корпоративной системы в населенном пункте удобное, тогда интенсивность обработки информации более чем высокая»;

b_3: «Если масштабы использования средств ВТ и ИКТ на предприятии большие, расположение корпоративной системы в населенном пункте удобное и расположение на территории объекта компактное, тогда интенсивность обработки информации очень высокая»;

b_4: «Если дополнительно к условиям, оговоренным в b_3, обустроенность на предприятии хорошая, тогда интенсивность обработки информации черезчур высокая»;

b_5: «Если масштабы использования средств ВТ и ИКТ на предприятии небольшие, но при этом расположение корпоративной системы в населенном пункте удобное, расположение на территории объекта компактное, а обустроенность на предприятии хорошая, тогда интенсивность обработки информации все равно высокая»;

b_6: «Если масштабы использования средств ВТ и ИКТ на предприятии небольшие и обустроенность на предприятии плохая, тогда интенсивность обработки информации невысокая».

В данном случае входными характеристиками (критериями) являются термы лингвистических переменных B, C_1, C_2 и C_3, а выходной – лингвистическая переменная C – интенсивность обработки информации. Используемые в высказываниях $b_1 \div b_6$ значения переменной C зададим в виде нечётких подмножеств универсального дискретного множества $U=\{0; 0.1; 0.2; \ldots; 1\}$:

- H=ВЫСОКАЯ: $\mu_H(u)=u$, $u \in U$;
- MH=БОЛЕЕ ЧЕМ ВЫСОКАЯ: $\mu_{MH}(u)=\sqrt{u}$, $u \in U$;
- VH=ОЧЕНЬ ВЫСОКАЯ: $\mu_{VH}(u)=u^2$, $u \in U$;
- TH=ЧЕРЕСЧУР ВЫСОКАЯ, $\mu_{TH}(u)=\begin{cases}1, u=1,\\ 0, u<1,\end{cases}$ $u \in U$;
- L=НИЗКАЯ: $\mu_L(u)=1-u$, $u \in U$.

С учётом введенных формализмов и обозначенных термов входных лингвистических переменных B, C_1, C_2 и C_3, запишем высказывания $b_1 \div b_6$ в виде следующих нечётких импликативных правил:

b_1: «Если B=БОЛЬШИЕ, тогда С=ВЫСОКАЯ»;

b_2: «Если B=БОЛЬШИЕ и C_1=УДОБНОЕ, тогда C=БОЛЕЕ ЧЕМ ВЫСОКАЯ»;

b_3: «Если B=БОЛЬШИЕ и C_1=УДОБНОЕ и C_2=КОМПАКТНОЕ, тогда C=ОЧЕНЬ ВЫСОКАЯ»;

b_4: «Если B=БОЛЬШИЕ и C_1=УДОБНОЕ и C_2=КОМПАКТНОЕ и C_3=ХОРОШАЯ, тогда C=ЧЕРЕСЧУР ВЫСОКАЯ»;

b_5: «Если B=НЕБОЛЬШИЕ и C_1=УДОБНОЕ и C_2=КОМПАКТНОЕ и C_3=ХОРОШАЯ, тогда C=ВЫСОКАЯ»;

b_6: «Если B=НЕБОЛЬШИЕ и C_3=ПЛОХАЯ, тогда C=НЕВЫСОКАЯ».

Степень конфиденциальности:

c_1: «Если уровень дисциплины на предприятии высокий и общая постановка дела хорошая, тогда степень конфиденциальности высокая»;

c_2: «Если в дополнение к предыдущему условию укомплектованность кадрами полная, тогда степень конфиденциальности более чем высокая»;

c_3: «Если масштабы использования средств ВТ и ИКТ на предприятии небольшие, уровень дисциплины высокий, общая постановка дела хорошая и укомплектованность кадрами полная, тогда степень конфиденциальности очень высокая»;

c_4: «Если дополнительно к условиям, оговоренным в c_3, уровень подготовки и воспитания кадров высокий, тогда степень конфиденциальности на предприятии чересчур высокая»;

c_5: «Если масштабы использования средств ВТ и ИКТ на предприятии большие, уровень дисциплины высокий, общая постановка дела хорошая и уровень подготовки и воспитания кадров высокий, тогда степень конфиденциальности высокая»;

c_6: «Если масштабы использования средств ВТ и ИКТ на предприятии большие, общая постановка дела плохая и уровень подготовки и воспитания кадров низкий, тогда степень конфиденциальности невысокая».

Здесь критериями оценки являются термы лингвистических переменных B, D_1, D_2, D_3 и D_4, а выходной – лингвистическая переменная D – степень конфиденциальности. Используемые в высказываниях $c_1 \div c_6$ значения переменной D зададим аналогично предыдущему случаю в виде нечётких подмножеств универсального дискретного множества

U={0; 0.1; 0.2; …; 1}. Тогда перечисленные высказывания $c_1 \div c_6$ запишем в виде соответствующих импликативных правил:

c_1: «Если D_1=ВЫСОКИЙ и D_2=ХОРОШАЯ, тогда D=ВЫСОКАЯ»;

c_2: «Если D_1=ВЫСОКИЙ и D_2=ХОРОШАЯ и D_3=полная, тогда D=БОЛЕЕ ЧЕМ ВЫСОКАЯ»;

c_3: «Если B=НЕБОЛЬШИЕ и D_1=ВЫСОКИЙ и D_2=ХОРОШАЯ и D_3=полная, тогда D=ОЧЕНЬ ВЫСОКАЯ»;

c_4: «Если B=НЕБОЛЬШИЕ и D_1=ВЫСОКИЙ и D_2=ХОРОШАЯ и D_3=полная и D_4=ВЫСОКИЙ, тогда D=ЧЕРЕСЧУР ВЫСОКАЯ»;

c_5: «Если B=БОЛЬШИЕ и D_1=ВЫСОКИЙ и D_2=ХОРОШАЯ и D_4=ВЫСОКИЙ, тогда D=ВЫСОКАЯ»;

c_6: «Если B=БОЛЬШИЕ и D_2=ПЛОХАЯ и D_4=НИЗКИЙ, тогда D=НЕВЫСОКАЯ».

Объёмы обрабатываемой информации:

d_1: «Если масштабы использования средств ВТ и ИКТ на предприятии большие и имеет место полный регулируемый доступ к информации, тогда объёмы обрабатываемой информации высокие»;

d_2: «Если в дополнение к предыдущему условию структурированность информации полная, тогда объёмы обрабатываемой информации более чем высокие»;

d_3: «Если масштабы использования средств ВТ и ИКТ на предприятии большие, имеет место полный регулируемый доступ к информации, стабильность информации регулярная, а структурированность информации полная, тогда объёмы обрабатываемой информации очень высокие»;

d_4: «Если дополнительно к условиям, оговоренным в d_3, масштаб обработки информации большой, тогда объёмы обрабатываемой информации чересчур высокие»;

d_5: «Если масштабы использования средств ВТ и ИКТ на предприятии большие, масштаб обработки информации большой, имеет место полный регулируемый доступ к информации, но при этом стабильность информации отсутствует, тогда объёмы обрабатываемой информации все же остаются высокими»;

d_6: «Если масштабы использования средств ВТ и ИКТ на предприятии небольшие и имеют место существенные ограничения на доступ к информации, тогда объёмы обрабатываемой информации невысокие».

Входными характеристиками (или критериями оценки) являются термы лингвистических переменных B, E_1, E_2, E_3 и E_4, а выходной – лингвистическая переменная E – объёмы обрабатываемой информации. Используемые в высказываниях $d_1 \div d_6$ термы лингвистической переменной E зададим аналогично предыдущему случаю в виде нечётких подмножеств универсального дискретного множества U={0; 0.1; 0.2; …; 1}. Тогда высказывания $d_1 \div d_6$ будут иметь следующий вид:

d_1: «Если B=БОЛЬШИЕ и E_2=ПОЛНЫЙ, тогда E=ВЫСОКИЕ»;

d_2: «Если B=БОЛЬШИЕ и E_2=ПОЛНЫЙ и E_4=ПОЛНАЯ, тогда E=БОЛЕЕ ЧЕМ ВЫСОКИЕ»;

d_3: «Если B=БОЛЬШИЕ и E_2=ПОЛНЫЙ и E_3=РЕГУЛЯРНАЯ и E_4=ПОЛНАЯ, тогда E=ОЧЕНЬ ВЫСОКИЕ»;

d_4: «Если B=БОЛЬШИЕ и E_1=БОЛЬШОЙ и E_2=ПОЛНЫЙ и E_3=РЕГУЛЯРНАЯ и E_4=ПОЛНАЯ, тогда E=ЧЕРЕСЧУР ВЫСОКИЕ»;

d_5: «Если B=БОЛЬШИЕ и E_1=БОЛЬШОЙ и E_2=ПОЛНЫЙ и E_3=ОТСУТСТВУЕТ, тогда E=ВЫСОКИЕ»;

d_6: «Если B=БОЛЬШИЕ и E_2=СУЩЕСТВЕННО ОГРАНИЧЕННЫЙ, тогда E=НЕВЫСОКИЕ».

Таким образом, сформулировав типовые нечёткие модели для оценки источников уязвимости системы, мы можем сравнительно легко сформировать полный набор лингвистических переменных и правил для построения системы нечеткого вывода,

оценивающую уровень уязвимости системы. Для удобства все переменные сведены в табл. 2, а система правил в символьной форме представлена ниже.

Табл. 2

Переменные системы нечеткого вывода для оценки уровня уязвимости системы

Входные переменные	x_1	Имя переменной	Интенсивность обработки информации
		Терм-множество	{НЕВЫСОКАЯ, ВЫСОКАЯ, БОЛЕЕ ЧЕМ ВЫСОКАЯ, ОЧЕНЬ ВЫСОКАЯ, ЧЕРЕСЧУР ВЫСОКАЯ}
		Пределы значений	[0, 1]
	x_2	Имя переменной	Степень конфиденциальности информации
		Терм-множество	{НЕВЫСОКАЯ, ВЫСОКАЯ, БОЛЕЕ ЧЕМ ВЫСОКАЯ, ОЧЕНЬ ВЫСОКАЯ, ЧЕРЕСЧУР ВЫСОКАЯ}
		Пределы значений	[0, 1]
	x_3	Имя переменной	Объёмы обрабатываемой информации
		Терм-множество	{НЕВЫСОКИЕ, ВЫСОКИЕ, БОЛЕЕ ЧЕМ ВЫСОКИЕ, ОЧЕНЬ ВЫСОКИЕ, ЧЕРЕСЧУР ВЫСОКИЕ}
		Пределы значений	[0, 1]
Выходная переменная y		Имя переменной	Уязвимость системы
		Терм-множество	{НИЗКАЯ, ПОНИЖЕННАЯ, СРЕДНЯЯ, ПОВЫШЕННАЯ, ВЫСОКАЯ}
		Пределы значений	[0, 1]

- Если x_1=НЕВЫСОКАЯ и x_2=ЧЕРЕСЧУР ВЫСОКАЯ и x_3=НЕВЫСОКИЕ, тогда y=НИЗКАЯ;
- Если x_1=ВЫСОКАЯ и x_2=ОЧЕНЬ ВЫСОКАЯ и x_3=ВЫСОКИЕ, тогда y=ПОНИЖЕННАЯ;
- Если x_1=БОЛЕЕ ЧЕМ ВЫСОКАЯ и x_2=БОЛЕЕ ЧЕМ ВЫСОКАЯ и x_3=БОЛЕЕ ЧЕМ ВЫСОКИЕ, тогда y=СРЕДНЯЯ;
- Если x_1=ОЧЕНЬ ВЫСОКАЯ и x_2=ВЫСОКАЯ и x_3=ОЧЕНЬ ВЫСОКИЕ, тогда y=ПОВЫШЕННАЯ;
- Если x_1=ЧЕРЕСЧУР ВЫСОКАЯ и x_2=НЕВЫСОКАЯ и x_3=ЧЕРЕСЧУР ВЫСОКИЕ, тогда y=ВЫСОКАЯ.

Приведенные правила можно легко реализовать в нотации пакета MATLAB, использовав при этом, например, «колоколообразные» функции принадлежности для описания термов входных и выходных лингвистических переменных (рис. 3).

Рис. 3. Реализация правил для оценки уязвимости системы в нотации MATLAB

После задания всех переменных, функций принадлежности и правил нечеткой базы знаний можно провести анализ работы построенной системы. Для этого удобно

воспользоваться графической интерпретацией пакета MATLAB в виде поверхностей принадлежности, приведенных на рис. 4.

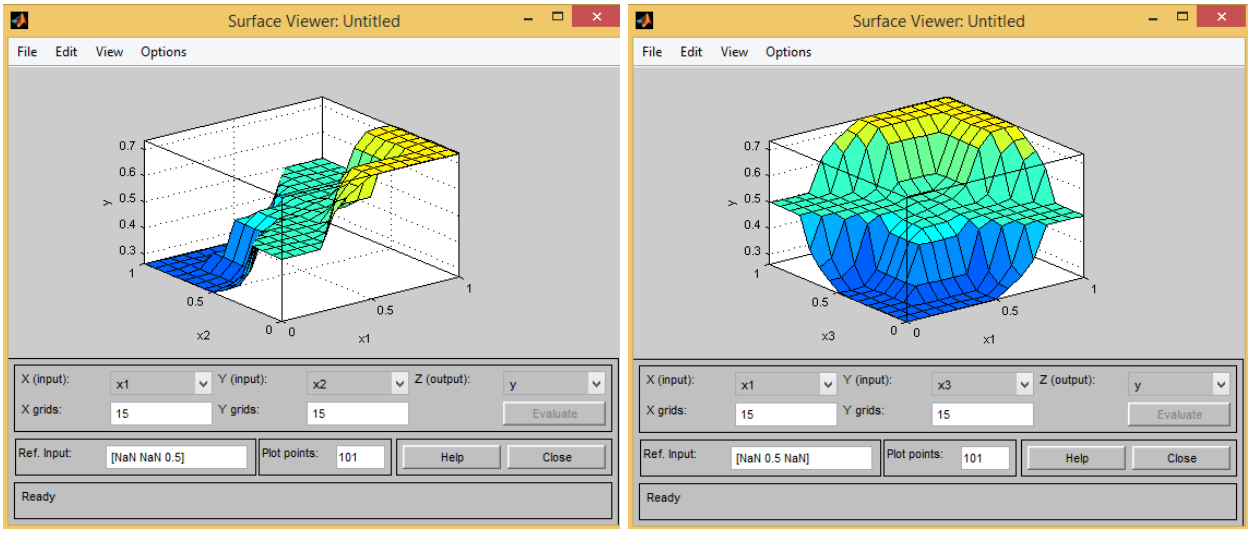

Рис. 4. Зависимость степени уязвимости системы от факторов влияния

Общая уязвимость информационной системы не превышает значения 0.908 при наихудшем сценарии уровня конфиденциальности и, соответственно, не ниже 0.0917 при ее наилучшем сценарии. Кроме того, система весьма «чувствительна» к небольшим изменениям в величинах факторов влияния: увеличивается с ростом интенсивности обработки информации и резко возрастает при превышении объёмов обрабатываемой информации эквивалентной величине 0.73.

Существующую корреляцию между уязвимостью системы и уровнем ИБ можно легко построить, использовав для этого подходящую модель регрессии или аппроксимируя ее посредством feedforward нейронной сети с одним «скрытым» слоем.

5. Выводы. Для окончательного формирования систем нечёткого вывода, реализуемых на базе импликативных правил: $a_1 \div d_8$, $b_1 \div b_6$, $c_1 \div c_6$, $d_1 \div d_6$, необходимо отобразить введенные входные лингвистические переменные на множество соответствующих им действительных чисел путём задания соответствующих функций принадлежности. В частности, можно оценивать преимущество одного элемента чёткого множества над другим по отношению к свойству заданного нечёткого множества при помощи 9-балльной шкалы Саати [15] или, что еще лучше, реализовать системы нечёткого вывода в нейросетевом логическом базисе [16]. Но эти процедуры потребуют выполнения достаточно трудоёмкого и затратного по времени скрупулёзного статистического анализа, что приведет к значительным издержкам.

Данную задачу можно существенно упростить, если выбрать несколько и/или более альтернатив (в нашем случае предприятий) для оценки их ИБ, например, условно: u_1, u_2, …, u_n, и строить нечёткие множества по опорному вектору (u_1, u_2, …, u_n) с помощью, скажем, гауссовских функций принадлежности: $\mu(x)=\exp[-(x-x_0)^2/\sigma^2]$, где x_0 – середина, а σ^2 плотность распределения соседних значений. Тогда оценки ИБ предприятий можно проводить в комплексе по единой шкале ранжирования.

Предлагаемые в статье типовые модели нуждаются в структурном и параметрическом обучении с тем, чтобы претендовать на необходимую степень адекватности поставленной задаче. Более того, не факт, что предложенная на рис. 2 когнитивная карта вобрала в себя абсолютное большинство факторов, влияющих на уровень информационной безопасности. Но предлагаемый подход именно тем и хорош, что является в определенном смысле гибким

по отношению к возможным дополнениям и/или уточнениям, которые могут быть предъявлены экспертами и/или заказчиками. Тем не менее, даже в предложенном «несовершенном» варианте модель, не выдавая абсолютных значений для оценки уровней ИБ, способна реагировать на возможные изменения в концептах когнитивной карты и стать основой для анализа ИБ.

Литература

1. Zadeh L.A. Outline of a New Approach to the Analysis of Complex Systems and Decision Processes. – IEEE Trans., Syst., Man., Cybern., vol. SMC-3. 1973, Jan., p. 28-44.
2. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: 2-е изд. – М.: Издательско-торговая корпорация «Дашков К°», 2005. – 336 с.
3. Курило А. П., Зефиров С. Л., Голованов В. Б. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
4. Домарев В.В. Безопасность информационных технологий. Системный подход. – Киев, Изд-во «Диасофт», 2004, 992 с.
5. Максимов В.И., Корноушенко Е.К. Аналитические основы применения когнитивного подхода при решении слабо структурированных задач // Труды ИПУ РАН. - М.: 1999. – Т. 2. – с. 95-109.
6. Коврига С.В. Методические и аналитические основы когнитивного подхода к SWOT-анализу // Проблемы управления, 2005, №5. − с. 58–63.
7. Корноушенко Е.К., Максимов В.И. Управление процессами в слабоформализованных средах при стабилизации графовых моделей среды // Труды ИПУ РАН: Сб. науч. Тр. – М.: ИПУ РАН, 1999. – Т.2. – с. 82–94.
8. Прангишвили И.В. О методах эффективного управления сложными системами // Тр. 5-ой междунар. конф. “Когнитивный анализ и управление развитием ситуаций” (CASC’2005) / ИПУ РАН. − М.: 2005. – с. 7–15.
9. Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями). Авдеева З.К. и др. Доступно на http://www.mtas.ru/Library/uploads/1168452488.pdf (дата обращения: 26.09.2015)
10. Ажмухамедов И.М. Концептуальная модель управления комплексной безопасностью системы // Вестник АГТУ. Серия: «Управление, вычислительная техника и информатика» 1/2010 г., с. 62-66
11. Решение задач обеспечения информационной безопасности на основе системного анализа и нечёткого когнитивного моделирования. Ажмухамедов И.М. Доступно на http://arxiv.org/ftp/arxiv/papers/1204/1204.3245.pdf (дата обращения: 30.09.2015)
12. Kosko B. Fuzzy cognitive maps //International Journal of Man-Machine Studies, 1986.–Vol. 1, p. 65–75.
13. Рзаев Р.Р. Интеллектуальный анализ данных в системах поддержки принятия решений. Verlag: LAP Lambert Academic Publishing GmbH & Co, 2013, 130 с.
14. Рзаев Р.Р., Джамалов З.Р., Мехтиев Т., Гасанов В. Моделирование временных рядов на основе нечёткого анализа позиционно-бинарных составляющих исторических данных. Нечёткие системы и мягкие вычисления, Т. 10, №1, 2015, с. 35-73.
15. Ротштейн, А. П. Нечеткий многокритериальный выбор альтернатив: метод наихудшего случая // Известия РАН. Теория и системы управления. – 2009. – N 3. – с. 51-55.
16. Lin C. T., George Lee C. S. Supervised and Unsupervised Learning with Fuzzy Similarity for Neural Network-based Fuzzy Logic Control Systems. Fuzzy sets, Neural Networks, and Soft Computing. Edited by R.R. Yager and L.A. Zadeh. N.-Y.: Van Nostrand Reinhold, 1994, p. 85–125.

UOT 519.712.3

E.T. Əliyev, V.İ. Həsənov, Z.R. Camalov, A.K. Xudadova

İnformasiya təhlükəsizliyinin kompleks qiymətləndirilməsi üçün qeyri-səlis koqnitiv model

Müəssisələrdə informasiya təhlükəsizlik səviyyəsinin qiymətləndirilməsi üçün nümunəvi qeyri-səlis koqnitiv model işlənilmiş və təsvir edilmişdir. İnformasiya təhlükəsizliyinə təsir göstərən faktorların kifayət qədər geniş spektorunu əhatə edən koqnitiv xəritə əsas kimi götürülmüşdür. Burada faktorlar arasında mövcud olan səbəb-nəticə növlü əlaqələr qeyri-səlis implikativ qaydaların məhtudlaşdırılmış toplusu şəklində təsvir edilmişdir.

Açar sözlər: qeyri-səlis koqnitiv model, koqnitiv xəritə, informasiya təhlükəsizliyi, qeyri-səlis çıxarılış sistemi

Transaction of Azerbaijan National Academy of Sciences, Series of Physical-Technical and Mathematical Sciences: Informatics and Control Problems, Vol. XXXV, No.6, 2015
www.icp.az/2015/6-08.pdf

E.T. Aliyev, V.I. Hasanov, Z.R. Jamalov, A.K. Hudadova

Fuzzy cognitive model for a comprehensive assessment of information security

The authors develop and describe a typical fuzzy cognitive model to assess the level of information security in enterprises. The model is based on the cognitive map, which covers quite a large range of factors of influence on information security, the causal relationship between them is represented in the form of a limited set of fuzzy implicative rules.

Keywords: fuzzy cognitive model, cognitive map, information security, fuzzy inference system

Институт Систем Управления НАН Азербайджана

Представлено 19.10.15