для предприятия, корпорации, государства и мира. Разобравшись, как на основе этих архетипов вести ИМ, можно применить эти знания на предприятии и в государстве. Новые информационные технологии начала третьего тысячелетия сделали возможным эффективное массовое производство, внедрение и применение на практике архетипов ИМ. При этом почти с математической точностью можно добиваться изменения индивидуального и коллективного сознания.

Литература

1. *Цыганов В.В., Бородин В.А., Шишкин Г.Б.* Интеллектуальное предприятие: механизмы овладения капиталом и властью (теория и практика управления эволюцией организации). М.: Университетская книга, 2004.

2. *Цыганов В.В., Бухарин С.Н.* Информационные войны в бизнесе и политике. Теория и методология. М.: Академический проект, 2007.

3. *Бухарин С.Н., Цыганов В.В.* Методы и технологии информационных войн. М.: Академический проект, 2007.

The concept of the information management

***Vladimir Viktorovich Tsyganov**, Dr.Sci., Institute of Control Sciences them. VA Trapeznikov*

***Vladimir Grigor'evich Gorbunov**, Dr.Sci, Federal State Unitary Enterprise Experimental Factory of Scientific Engineering Russian Academy of Sciences*

This paper presents the results of researches of adaptive and learning mechanisms of the information management functioning. Scientists and societal leaders increasingly agree that the information management is irretrievably changing the human environment. Action to control human impact on the information management is an imperative prerequisite to achieving social stability. Accelerating information management due to stress have been associated with emerging conflicts. Traditional dogmas, whether ethnic, religious or political, must be re-thought in this changing context if information society is to avoid collapse.

***Keywords:** Information management, information warfare, the mechanism archetypes*

УДК 004.056.5:002

МЕТОДИКА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕЧЁТКОЙ ЛОГИКИ НА БАЗЕ ИНСТРУМЕНТАРИЯ MATLAB

***Елена Константиновна Баранова**, доц. кафедры информационной безопасности,*
e-mail: ekbaranova@hse.ru,
Национальный исследовательский университет «Высшая школа экономики»,
https://www.hse.ru,
***Александр Михайлович Гусев**, лаборатория специальных работ,*
e-mail:sanekgysev@mail.ru,
ЗАО НПЦ Фирма «НЕЛК»,
http://www.nelk.ru

Анализируются проблемы, возникающие при анализе рисков информационной безопасности в организациях малого и среднего бизнеса. Для повышения эффективности применяемых в настоящее время методик анализа и оценки рисков предлагается использовать нечёткую логику. Предлагаемая методика дает возможность оценивать риски информационной безопасности с использованием нечёткой логики на базе инструментария MATLAB и позволяет наглядно представить состояние системы защиты информации, а также комплексно оценить возможные угрозы безопасности и получить оценки информационных рисков.

Ключевые слова: информационная безопасность; нечёткая логика; риски информационной безопасности; защита информации


Е.К. Баранова

Использование информационных технологий в бизнес-процессах современных организаций является эффективным инструментом повышения производительности труда. Однако информационная система организаций зачастую имеет неструктурированный характер, что влечёт за собой рост уязвимостей и риска нарушения информационной безопасности (ИБ). В России в последние годы принят ряд стандартов, регламентирующих деятельность в области информационной безопасности – это семейство ГОСТ Р ИСО/МЭК 27000, основанное и соответствующее семейству международных стандартов на системы управления информационной безопасностью ISO/IEC 27000. Эти стандарты определяют требования к системам управления информационной безопасностью, управлению рисками, метрики и измерения, а также руководство по внедрению. Однако, темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Российской Федерации, отсюда возникает необходимость в решении следующих вопросов: в соответствии с какими критериями и показателями производить оценку эффективности системы защиты информации, как обеспечить оценку и мониторинг информационных рисков в организациях, особенно, малого и среднего бизнеса.


А.М. Гусев

Современные методики управления рисками для анализа каждого вида риска используют вероятность реализации угроз и ущерб от негативных последствий, но реально оценить вероятность реализации угроз и степень наносимого ущерба затруднительно. В большинстве случаев эксперты в области ИБ, основываясь на собственном опыте, проводят оценку в виде словесных формулировок, которые затем связывают с числовыми значениями. Такой механизм получения оценок рисков ограничивает возможности методики в целом, так как уверенность в предлагаемой экспертом оценке может носить дискуссионный характер.

Для устранения недостатков методик анализа и оценки рисков ИБ предлагается использовать нечёткую логику, применение которой эффективно следующих случаях:

–недостаточность знаний об исследуемой системе;

–невозможность получения требуемого объёма информации;

–информация основана на экспертных данных, входные данные некорректно представлены или не являются достаточно точными.

Экспертам в области информационной безопасности сложно дать точную количественную оценку компонентам системы обеспечения ИБ организации, таким, например, как «низкий уровень организационной защиты», «средний уровень программно-аппаратной защиты», «высокая очевидность риска» и т.д. Поэтому необходимо рассматривать эти компоненты с точки зрения нечётких множеств и лингвистических переменных. Используя нечёткую логику для оценки рисков ИБ, можно получить как качественные (выраженные в виде нечётких понятий), так и количественные характеристики.

Для создания методики оценки рисков необходимо разработать экспертную систему, которая была бы реализована в виде системы нечёткого вывода и позволяла определять величину риска на основе субъективных оценок всех уровней информационной безопасности. Для моделирования экспертной системы использовался программный инструментарий *MATLAB* – высокоуровневый язык и интерактивная среда для программирования численных расчётов и визуализации результатов, а также *Fuzzy*

Logic Toolbox – пакет расширения *MATLAB*, содержащий инструменты для проектирования систем нечёткой логики.

В качестве входных переменных используются определённые экспертным путём уровни информационной безопасности, представленные в таблице 1.

Таблица 1

Обозначение	Наименование	Вид терм-множества
X1	Программно-аппаратный уровень защиты (ПаЗ)	Н – удовлетворительная для обеспечения начального уровня защиты; С – достаточная для базовой информационной защиты; В – высокий уровень обеспечения ИБ.
X2	Уровень организационно-правовой защиты (ОргЗ)	Н – удовлетворительная для обеспечения начального уровня защиты; С – достаточная для базовой информационной защиты; В – высокий уровень обеспечения ИБ.
X3	Уровень иженерно-технической защиты (ИнжЗ)	Н – удовлетворительная для обеспечения начального уровня защиты; С – достаточная для базовой информационной защиты; В – высокий уровень обеспечения ИБ.

В качестве выходных лингвистических переменных будем принимать:

Y1 – риск нарушения конфиденциальности информации;

Y2 – риск нарушения целостности информации;

Y3 – риск нарушения доступности информации.

После определения входных и выходных переменных введена система нечёткого вывода в интерактивном режиме, для этого использовался редактор систем нечёткого вывода *FIS* (рисунок 1).

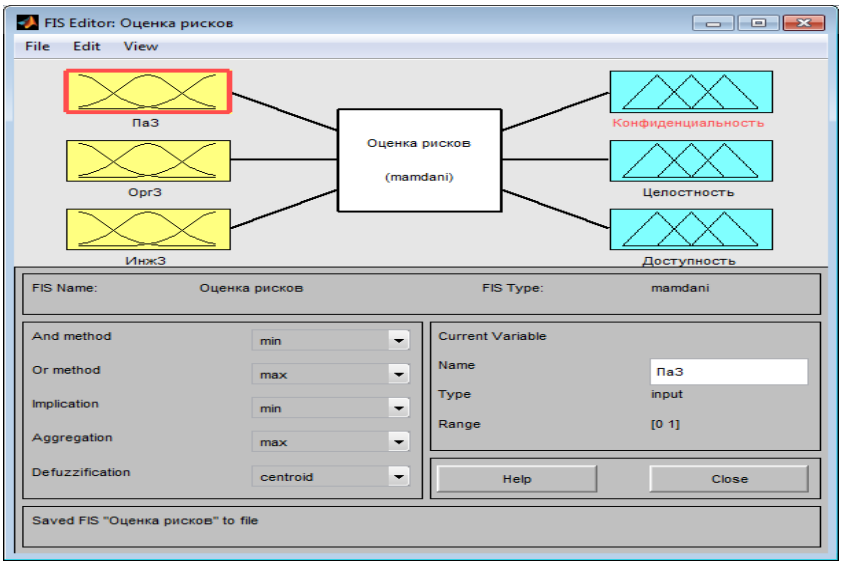

Рисунок 1 – Редактор систем нечёткого вывода

Входные переменные:
Input1 – ПаЗ;
Input2 – ОргЗ;
Input3 – ИнжЗ.

Выходные переменные:
Output1– конфиденциальность (Y1);
Output2 – целостность (Y2);
Output3 – доступность (Y3).

Далее определяются термы и их функции принадлежности для входных и выходных переменных системы нечёткого вывода. Для этого следует воспользоваться редактором функций принадлежности (рисунок 2).

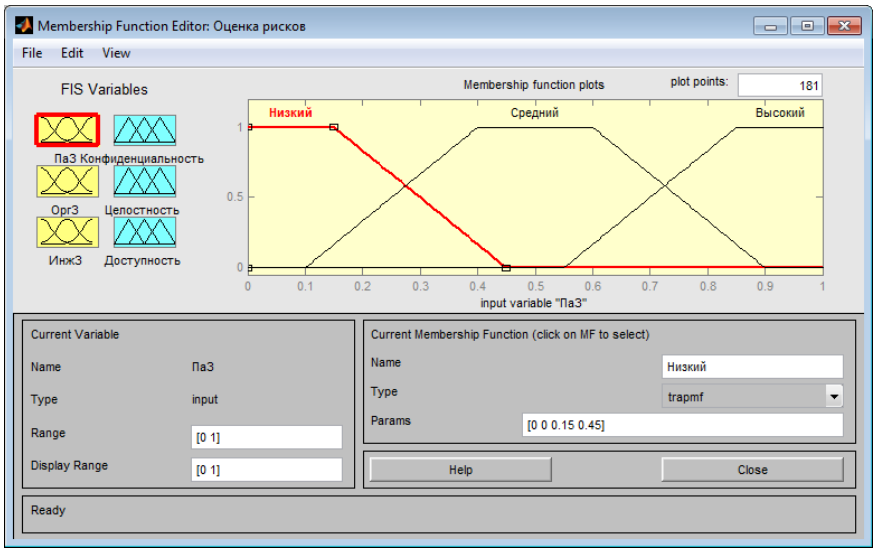

Рисунок 2 – Редактор функций принадлежности

В работе используется трапецеидальная и треугольная форма для задания функции принадлежности.

Для задания трапецеидальной функции принадлежности необходима четвёрка чисел *(a, b, c, d)*, ее значение в точке *x* вычисляется согласно выражению:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ 1-\dfrac{x-c}{d-c}, c\le x\le d\\ 0\end{cases}$$ в остальных случаях

При *(b – a) = (d – c)* трапецеидальная функция принадлежности принимает симметричный вид.

Треугольная функция принадлежности определяется тройкой чисел *(a,b,c)*, и ее значение в точке *x* вычисляется согласно выражению:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1-\dfrac{x-b}{c-b}, b\le x\le c\\ 0\end{cases}$$ в остальных случаях

При *(b – a) = (c – b)* имеем случай симметричной треугольной функции принадлежности, которая может быть однозначно задана двумя параметрами из тройки *(a,b,c)*.

Для входных переменных ПаЗ и ИнжЗ, параметры каждого из термов будут определены следующим образом (функции принадлежности принимаем как трапецеидальные): для терма «низкий» зададим параметры [0 0 0,15 0,45], для терма «средний» [0,1 0,4 0,6 0,9], для терма «высокий» [0,55 0,85 1 1] (рисунок 3).

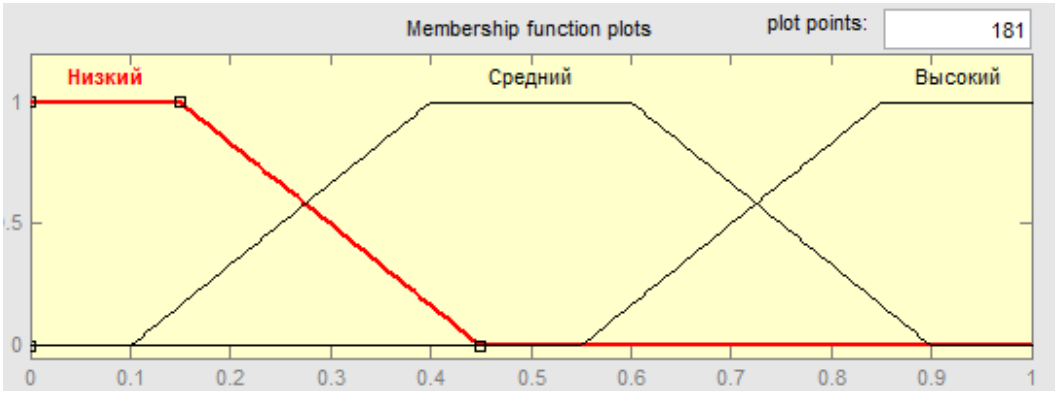

Рисунок 3 – Параметры входных переменных Паз и ИнжЗ

Для входной переменной ОргЗ, функции принадлежности являются треугольными (рисунок 4).

Низкий – [0 0 0,4];

Средний – [0,1 0,5 0,9];

Высокий – [0,6 1 1].

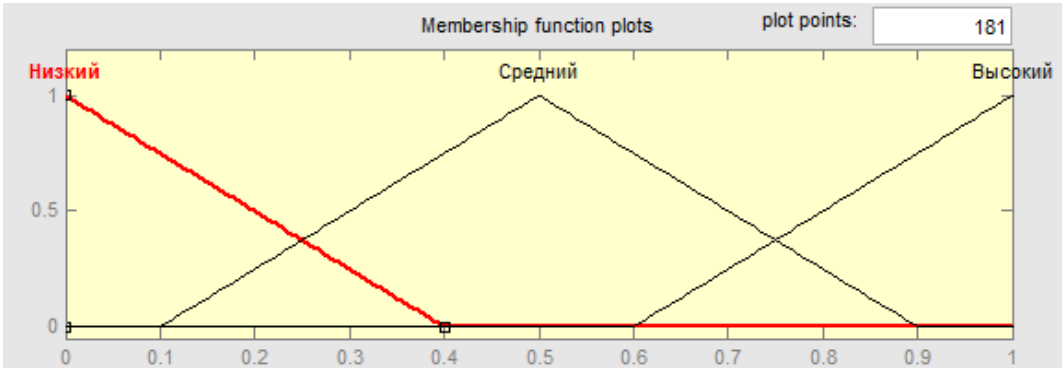

Рисунок 4 – Параметры входной переменной ОргЗ

На следующем этапе определяются терм-множества для выходных переменных.

Для выходных переменных: «конфиденциальность, целостность, доступность», параметры термов будут следующими (рисунок 5).

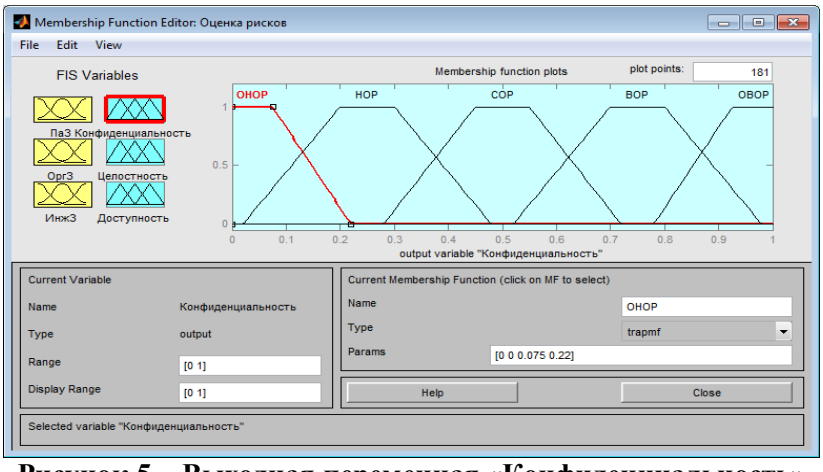

Рисунок 5 – Выходная переменная «Конфиденциальность»

Где *T* = {Очень низкая очевидность риска (OHOP); Низкая очевидность риска (HOP); Средняя очевидность риска (COP); Высокая очевидность риска (BOP); Очень высокая очевидность риска (OBOP)}.

OHOP – [0 0 0,075 0,22];

HOP – [0,02 0,2 0,3 0,48];

COP – [0,28 0,45 0,55 0,72];

ВОР – [0,52 0,7 0,8 0,98];
ОВОР – [0,78 0,925 1 1].

Далее необходимо определить правила нечёткого вывода для методики оценки и анализа рисков (экспертной системы). Эти правила представляют собой алгоритм, оценки рисков.

Чтобы понять, каким образом уровни программно-аппаратной, организационно-правовой и инженерно-технической защиты влияют на выходные переменные – нарушение конфиденциальности, целостности, доступности, составляем матрицу (Таблица 2).

Таблица 2

Уровни влияния на возникновение рисков

Уровень/Риск	**К**	**Ц**	**Д**
ПаЗ	3	1	2
ОргЗ	1	2	3
ИнжЗ	2	3	1

В матрице определены уровни влияния на возникновение рисков. Например, на конфиденциальность информации в организации наибольшее влияние оказывает уровень программно-аппаратной защиты, поэтому на пересечении первой строки и первого столбца матрицы выставляется значение 3 (высокий). Далее все остальные уровни ранжируются по тому же принципу. Каждый из термов будет соответствовать значению из матрицы:

1 – низкий;
2 – средний;
3 – высокий.

Для лучшего восприятия, приведём пример. Если уровень ПаЗ = низкий (н), ОргЗ = средний (с), а уровень ИнжЗ = высокий (в), то риск нарушения конфиденциальности (к) – средний, целостности (ц) – низкий, доступности (д) – средний. Это было рассчитано следующим образом: из матрицы следует, что на конфиденциальность наибольшее влияние имеет уровень ПаЗ, затем – ИнжЗ, так как уровень ПаЗ в данном примере низкий, а уровень ИнжЗ высокий, то риск нарушения конфиденциальности средний (н+в) = с, для остальных рисков расчёт происходит аналогичным образом. Необходимо также ввести правило: (с+в)=с, (в+с)=в.

База правил нечёткого вывода, построенная на основе ранее приведённой матрицы, приведена на рисунке 6.

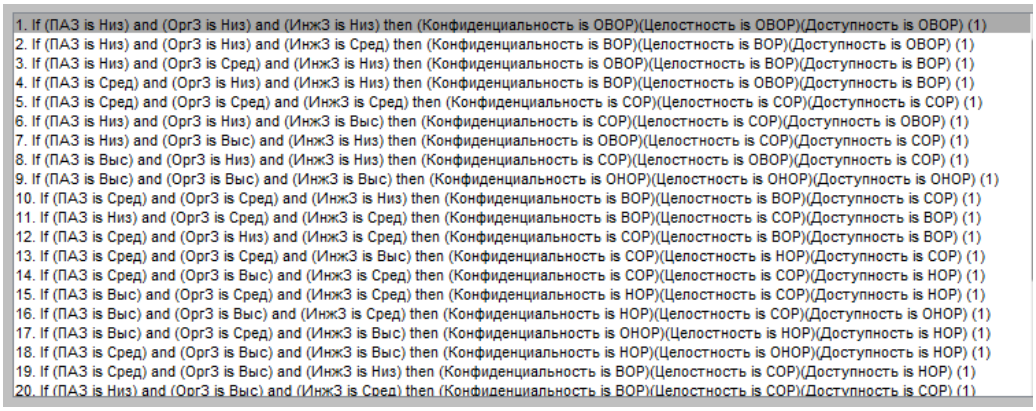

Рисунок 6 – Правила нечёткого вывода

Предположим, что на основе экспертных данных были получены оценки программно-аппаратной, инженерно-технической и организационной защиты, которые будем вводить в окно механизма вывода графического интерфейса *Fuzzy Logic Toolbox* (рисунок 7).

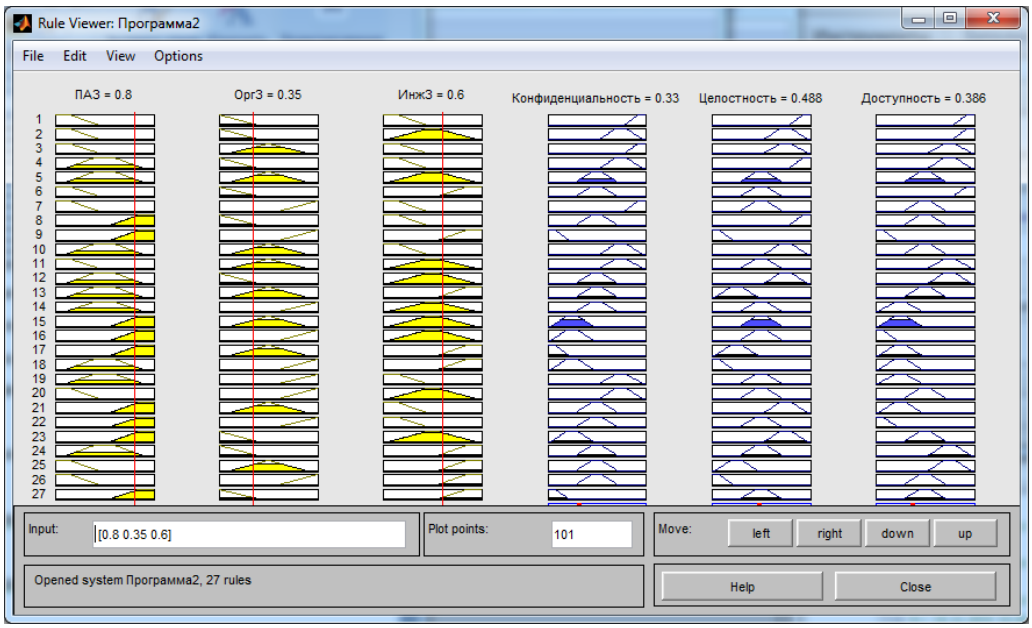

Рисунок 7 – Окно вывода

ПаЗ = 0,8, что соответствует терму «высокий уровень обеспечения ИБ»;

ОргЗ = 0,35, что соответствует «удовлетворительная для обеспечения начального уровня защиты»;

ИнжЗ = 0,6, что соответствует терму «достаточная для базовой информационной защиты».

Из рисунка 7 видно, что при введённых значениях входных переменных, выходные переменные принимают значения:

Конфиденциальность = 0,33, что соответствует терму «низкая очевидность риска».

Целостность = 0,488, что соответствует терму «средняя очевидность риска».

Доступность = 0,386, что соответствует терму «низкая очевидность риска».

Графический интерфейс программного инструментария позволяет получить график зависимости выходной величины от любой из входных переменных.

На рисунке 8 представлен график зависимости выходной переменной «Целостность» от входной переменной ОргЗ.

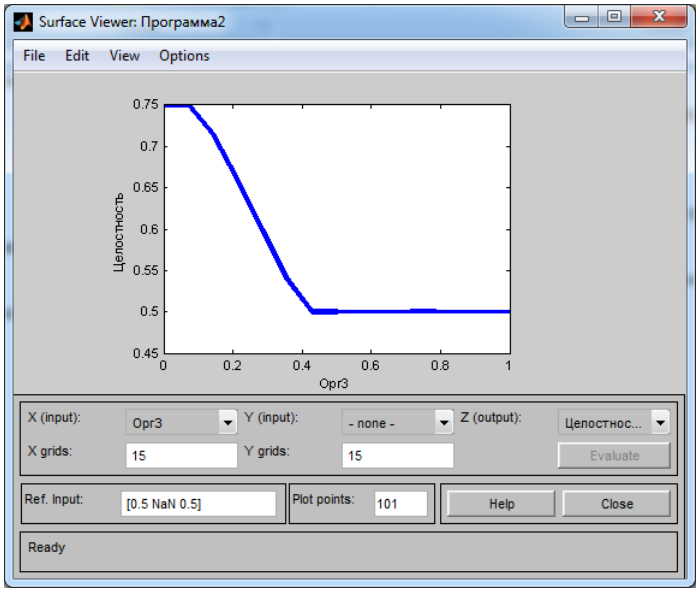

Рисунок 8 – Зависимость переменной «Целостность» от ОргЗ

График показывает обратную зависимость величины риска нарушения целостности от уровня организационной защиты.

На рисунке 9 приведена полученная поверхность зависимости выходной лингвистической переменной от двух входных с фиксированным значением третей переменной для базы правил нечёткой модели.

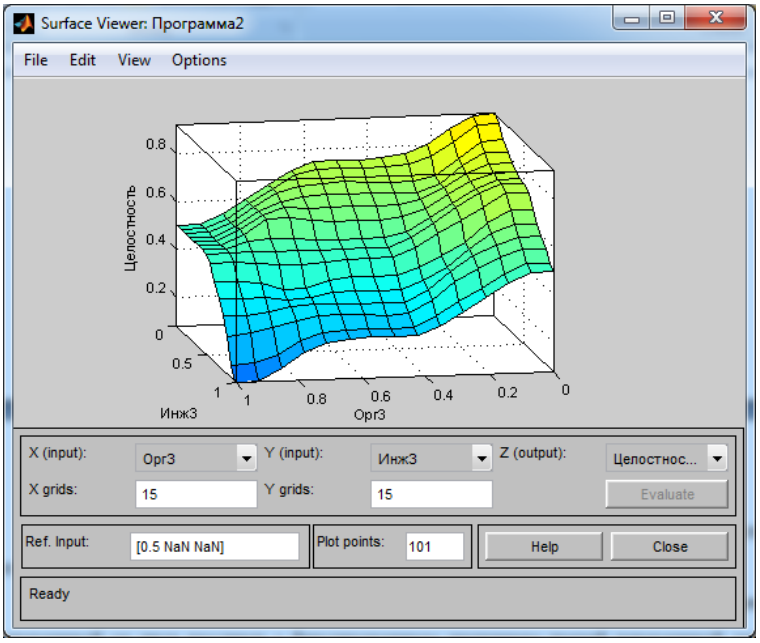

Рисунок 9 − Поверхность системы нечёткой модели

Заключение

Предлагаемая методика даёт возможность оценивать риски информационной безопасности с использованием нечёткой логики на базе инструментария *MATLAB* и позволяет наглядно представить состояние системы защиты информации, а также комплексно оценить возможные угрозы безопасности и получить оценки информационных рисков.

Разработанная методика может быть рекомендована в качестве демонстрационного учебного материала для бакалавров в курсах «Информационная безопасность» и «Управление информационной безопасностью», а также может использоваться в организациях малого и среднего бизнеса для базового анализа рисков информационной безопасности и послужить для оценки эффективности системы защиты информации в организации.

Созданная в ходе разработки методики база правил может быть изменена в зависимости от приоритетов каждого из уровней защиты. Также для её построения могут использоваться различные методы принятия решений.

Разработанная нечёткая продукционная модель позволяет существенно расширить возможности существующих методик, снять ограничения на число учитываемых входных переменных и интегрировать как качественные, так и количественные подходы к оценке рисков. Используемые в методике механизмы оценки риска на основе нечёткой логики позволяют получить лингвистическое описание степени риска, что позволяет IT-менеджерам выявить приоритеты рисков (очень низкая очевидность риска; низкая очевидность риска; средняя очевидность риска; высокая очевидность риска; очень высокая очевидность риска) и выбрать план мероприятий по снижению уровня наиболее опасных угроз информационной безопасности организации.

Основная сложность механизма получения оценок риска на основе нечёткой логики состоит в построении модели для проведения лингвистического анализа рисков системы обеспечения информационной безопасности, однако данный механизм является эффективным инструментом, когда другие подходы к оценке риска неприменимы. Он обладает широкими возможностями и позволяет адаптировать его к имеющимся на

предприятии моделям управления рисками, а также модифицировать с учётом реальных условий политики информационной безопасности организации.

Литература

1. *Баранова Е.К.* Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности. Проблемы информационной безопасности. Компьютерные системы / под ред. проф. Зегжды П.Д. СПб.: Институт информационных технологий и управления. 2014. № 4. С. 160–168.

2. *Баранова Е.К., Зубровский Г.Б.* Управление инцидентами информационной безопасности. Проблемы информационной безопасности; труды I Международной научно-практической конференции «Проблемы информационной безопасности». Гурзуф, Крымский федеральный университет им. В.И. Вернадского, 26–28 февраля 2015 г. С. 27-33.

3. *Баранова Е.К., Бабаш А.В.* Информационная безопасность и защита информации. М.: РИОР; ИНФРА-М, 2014.

4. *Леоненков А.В.* Нечёткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ – СПб., 2005.

5. *Штовба С.Д.* Проектирование нечётких систем средствами MATLAB. М.: Горячая линия – Телеком, 2011.

The method of information security risk analysisusing fuzzy logic based tools MATLAB

***Elena Konstantinovna Baranova**, Associate professor of the Information Security Department, Higher School of Economics National Research University*

***Aleksandr Mihaylovich Gusev**, Laboratory of special worksSPC Firm NELK*

Analyzes the problems arising in the analysis of information security risks in organizations small and medium businesses. To improve the efficiency of the currently used methods of analysis and risk assessment is proposed to use fuzzy logic. The proposed method allows to evaluate the information security risks using fuzzy logic based tools MATLAB and allows to visualize the state of the system of information protection, as well as to comprehensively assess potential threats to security and get the information risk assessment.

Keywords: information security: fuzzy logic; risks of information security; data protection.

УДК 001.51, 001.2, 001.19

КАРТИНА МИРА КАК КОГНИТИВНАЯ ПАРАДИГМА

***Игорь Владимирович Соловьёв**, д-р техн. наук,*
проф., проректор по НИР,
e-mail: i.v.soloviev54@mail.ru,
Московский государственный университет информационных технологий, радиотехники и электроники,
https://www.mirea.ru

Статья анализирует формирование научной картины мира как сложной модели познания. Показан когнитивный фактор как важный компонент познания и формирования картины мира. Статья раскрывает содержание персонифицированной картины мира. Статья раскрывает содержание научной картины мира. Статья показывает отношение между персонифицированной и научной картинами мира. Определен когнитивный фактор как инструмент явного и неявного познания и формирования картины мира.

Ключевые слова: знание, познание, картина мира, когнитивные факторы, персонифицированная картина мира, научная картина мира