ПРИМЕНЕНИЕ СИСТЕМЫ MATLAB ДЛЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

С.А. Глушенко,
ассистент кафедры «Информационные системы и прикладная информатика»
ФГБОУ ВПО «Ростовский государственный экономический университет (РИНХ)»

E-mail: www.555.sergey@mail.ru
Адрес: г. Ростов-на-Дону, ул. Большая Садовая, 69

АВ статье обосновывается целесообразность применения нечеткой логики для оценки риска информационной безопасности организации и предлагается нечеткая продукционная модель (НПМ). Проводится реализация процесса нечеткого моделирования базы правил посредством применения специализированного пакета Fuzzy Logic Toolbox программного средства MATLAB. Выполнение нечеткого вывода реализуется на основе алгоритма Мамдани (Mamdani).

Ключевые слова: риск, нечеткое множество, терм-множество, нечеткая продукционная модель, лингвистическая переменная, база правил, функция принадлежности.

1. Введение

Процесс внедрения информационных технологий и средств вычислительной техники в производство и управление современных организаций является эффективным инструментом повышения производительности труда. Однако информационная инфраструктура организаций часто приобретает неструктурированный характер и влечет за собой неконтролируемый рост уязвимостей и риск информационной безопасности (ИБ) организации в целом.

Информационная безопасность организации – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб [1].

В Российской Федерации внешнее регулирование деятельности по обеспечению ИБ осуществляется различными государственными органами, такими как:

- ✧ Комитет Государственной думы по безопасности;
- ✧ Совет безопасности России;
- ✧ Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- ✧ Федеральная служба безопасности Российской Федерации (ФСБ России);
- ✧ Федеральная служба охраны Российской Федерации (ФСО России);

✧ Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

На уровне предприятия для контроля ИБ и осуществления мер по защите информации могут быть организованы:

✦ Служба экономической безопасности;

✦ Служба информационной безопасности;

✦ Служба безопасности персонала.

Деятельность данных служб основана на методических документах государственных органов России (Доктрина информационной безопасности РФ [2], руководящие документы и приказы ФСТЭК (Гостехкомиссии России) и ФСБ) и стандартах ИБ (Международные стандарты, государственные (национальные) стандарты РФ [3], рекомендации по стандартизации, методические указания).

В целях обеспечения информационной безопасности организации строится Система обеспечения информационной безопасности (СОИБ). СОИБ предприятия представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов предприятия от потенциальных угроз. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных документированной полит икой информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих средств и методов защиты информации [3].

Экономический эффект от внедрения СОИБ проявляется в виде снижения величины возможного материального, репутационного и иных видов ущерба, наносимого предприятию, за счет использования мер, направленных на формирование и поддержание режима ИБ.

Определить перечень необходимых мер защиты информации, выбрать стратегию развития информационной структуры организации и поддерживать на должном уровне безопасность организации, возможно только по результатам аудита уязвимостей предприятия и анализа рисков.

В данном случае риск рассматривается как фактор, сущность или элемент, представляющий опасность для ИБ организации, величина которой не определена [6].

Наиболее распространенными методиками оценки риска являются методы, изложенные в специальных рекомендациях 800-30 Национального Института Стандартов и Технологий США (NIST) [7] и разработанный Службой Безопасности Великобритании метод CRAMM [6]. Они охватывают широкий круг вопросов, связанных со стратегией управления рисками и являются хорошей основой для разработки собственной системы управления рисками.

Стоит отметить, что в отечественной нормативной базе ИБ отсутствует ГОСТ по управлению рисками. Российские стандарты ГОСТ ИСО/МЭК 17799 [3] и ГОСТ ИСО/МЭК 27001 [4] являются техническим переводом первой и второй частей соответственно британского стандарта BS 7799 из трех. Согласно российскому стандарту ГОСТ 27001 введенному в 2007 г., система управления ИБ трактуется как часть общей системы управления предприятием и предназначается для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ, а ГОСТ 17799 описывает примеры по среде и системам ИБ, но не отражает вопросов руководства по оценке и управлению рисками. Таким образом, внедрение стандартов ГОСТ 17799 и ГОСТ 27001 в практику подразумевает наличие в организации как минимум двух документов: политики ИБ и методологии оценки рисков ИБ, однако российская нормативная база не содержит описаний формы и содержания для последнего документа [5].

Методики управления рисками NIST и CRAMM для целей анализа предлагают использовать для каждого вида риска вероятность его появления и ущерб негативных последствий от риска. В качестве интегральной оценки риска используется произведение величины вероятности и ущерба. В [6] отмечается, что реально оценить вероятность риска достаточно сложно. В большинстве случаев IT-менеджеры и эксперты, основываясь на собственном опыте и/или имеющихся данных других организаций, проводят оценку в виде словесных формулировок, которые затем связывают с числовыми данными.

Такой «жесткий» механизм получения оценок риска существенно ограничивает возможности всей методики в целом. Например, вероятность риска оценивается как «низкая», «средняя» или «высокая» и этим определениям ставятся в соответствии следующие числовые значения вероятности риска: 17%, 50% и 84%. При этом «низкое» значение риска определяет интервал от 1% до 33% со средним значением 17%, «среднее» – интервал от 34% до 67% со

средним 50% и «высокое» – интервал от 68% до 99% со средним 84%.

Применяемый подход к оценке вероятности риска имеет ряд недостатков. Во-первых, оценки вероятности риска формируются в отдельных точках (17%, 50% и 84%), что не всегда может быть приемлемым. Во-вторых, уверенность эксперта в предлагаемой оценке может быть различной, что не отражается в процедуре оценивания вероятности риска.

Для устранения вышеприведенных недостатков предлагается использовать нечеткие модели [8], применение которых эффективно в следующих случаях:

- имеется недостаточность или неопределенность знаний об исследуемой системе или процессе;
- получение требуемой информации сопряжено с различными трудностями или вообще невозможно;
- основная часть информации получена на основе экспертных данных или эмпирических описаний процессов; параметры и входные данные не являются точными и корректно представленными.

Применение лингвистического подхода, во время оценки состояния системы обеспечения информационной безопасности организации, является общеизвестным. Оценка компонентов СОИБ проводится терминами «средний уровень программно-аппаратной защиты», «высокий уровень организационной защиты», «низкая рыночная ценность информационного ресурса» и др., т.е. IT–менеджерам сложно придать им точную (объективную) количественную оценку и описать с помощью математического языка. При таком подходе целесообразно рассматривать характеристики системы с точки зрения теории нечетких множеств, как лингвистические переменные. Использование методов получения оценок рисков на основе нечеткой логики позволяют использовать как количественные характеристики, которым объективно свойственна неопределенность, так и качественные, субъективные оценки экспертов, выраженные нечеткими понятиями, а также формализовать нечеткие описания с помощью нечетких чисел, множеств, лингвистических переменных и нечетких свидетельств.

Недостатками данного подхода являются субъективность в выборе функций принадлежности и формировании правил нечеткого ввода, а также необходимость специального программного обеспечения и специалистов, умеющих с ним работать.

2. Нечеткая продукционная модель оценки риска

Для моделирования риска информационной безопасности организации, нечеткие модели целесообразно представлять в виде нечетких сетей, элементы и совокупности элементов которых реализуют различные компоненты нечетких моделей и этапы нечеткого вывода.

Нечёткая продукционная модель (НПМ) может быть представлена следующим образом [9]:

$$(i): Q; P; A \Rightarrow B: S; F; N,$$

Q – сфера применения нечеткой продукции;

P – условие активизации ядра нечеткой продукции;

A – условие ядра (антецедент);

B – заключение ядра (консеквент);

S – метод определения количественного значения степени истинности заключения ядра;

F – коэффициент уверенности нечеткой продукции;

N – постусловие продукционного правила.

Нечеткое причинно-следственное отношение между антецедентом и консеквентом задается в виде нечеткой продукции:

ЕСЛИ x есть A, ТО y есть B

X – область определения антецедента;

A – нечеткое множество, определенное на X;

$\mu_A(x) \in [0,1]$ – функция принадлежности нечетного множества A;

Y – область определения консеквента;

B – нечеткое множество, определенное на Y;

$\mu_B(x) \in [0,1]$ – функция принадлежности нечетного множества B.

Если известна функция принадлежности нечетного множества A — $\mu_A(x)$, тогда для нечеткого множества B функция принадлежности определяется по правилу композиции:

$$\mu_B(y) = \sup_{x \in X} \{T(\mu_A(x), \mu_R(x,y))\} \qquad (1)$$

sup – операция определения верхней границы множества элементов;

T – операция Т-нормы.

При моделировании риска информационной безопасности организации, в качестве правила вычисления нечёткой импликации, применяется классическая нечёткая импликация Л. Заде:

$$\mu_R(x,y) = max\left\{min\left[\mu_A(x), \mu_B(y)\right], \left[1-\mu_A(x)\right]\right\} \quad (2)$$

Основными способами нечеткого вывода заключений в НПМ являются прямой и обратный вывод. Прямой вывод основывается на правиле вывода «нечеткий модус поненс» (*fuzzy modus ponens*).

Во время построения нечёткой продукционной модели оценки рисков ИБ организации необходимо сформировать полное пространство предпосылок $X = \{x_i\}, i = \overline{1,n}$ – факторов, являющихся источниками риска, и полное пространство заключений $Y = \{y_j\}, j = \overline{1,m}$ – показателей риска различных областей информационной безопасности организации.

В процессе анализа факторов риска выявлены показатели, которые могут быть источниками риска ИБ организации (*табл. 1*). При задании лингвистических переменных, характеризующих факторы риска, могут использоваться следующие терм–множества, определяющие уровни факторов [10]:

*T*2 = {*Низкий* (*Н*), *Высокий* (*В*)};

*T*3 = {*Низкий* (*Н*), *Средний* (*С*), *Высокий* (*В*)};

*T*4 = {*Очень Низкий* (*ОчН*), *Низкий* (*Н*), *Средний* (*С*), *Высокий* (*В*)};

*T*5 = {*Очень Низкий* (*ОчН*), *Низкий* (*Н*), *Средний* (*С*), *Высокий* (*В*), *Очень Высокий* (*ОчВ*)}.

Таблица 1.

Факторы риска ИБ организации (фрагмент)

Обозначение	Наименование ЛП	Вид терм-множества
x_1	Программно-аппаратный уровень защиты	*T*3. *Н* – удовлетворительная, для обеспечения начально уровня защиты; *С* – достаточна, для базовой информационной защиты; *В* – полностью соответствует уровню конфиденциальности информации
x_2	Уровень организационной защиты	*T*3. *Н* – слабое планирование и отсутствие мониторинга уязвимостей; *С* – планирование и мониторинг уязвимостей проводятся нерегулярно; *В* – своевременное планирование и мониторинг уязвимостей
x_3	Уровень правовой защиты	*T*3. *Н* – обрывочная и неполная документация; *С* – документация имеется, но недостаточно детальная; *В* – документация полная и синхронизированная

В процессе анализа риска выявлены показатели, которые могут характеризовать риски ИБ организации (*табл. 2*). При задании лингвистических переменных, характеризующих показатели риска, используется следующее терм-множество, определяющие показатели риска:

T1 = {Низкая очевидность риска (НОР), Средняя очевидность риска (СОР), Высокая очевидность риска (ВОР)};

T2 = {Очень низкая очевидность риска (ОНОР) Низкая очевидность риска (НОР); Средняя очевидность риска (СОР); Высокая очевидность риска (ВОР), Очень высокая очевидность риска (ОВОР)}.

Таблица 2.

Показатели риска ИБ организации (фрагмент)

Обозначение	Наименование ЛП	Примечание
y_1	Риск снижения эффективности защиты	Характеризует потенциальную возможность снижения/увеличения эффективности защиты, по отношению к требуемой эффективности для конкретного предприятия.
y_2	Риск возникновения потенциальных угроз	Характеризует возможности возникновения потенциальных угроз для предприятия
y_3	Риск материального ущерба	Характеризует возможность возникновения материального ущерба для предприятия при нарушениях параметров информационной безопасности предприятия

Взаимосвязь между факторами (антецедентом) и показателями риска (консеквентом) представляет собой бинарное нечеткое отношение на декартовом произведении соответствующих нечетких множеств. Нечеткое причинно-следственное отношение между антецеденом и консеквентом задается в виде нечеткой продукции [9]. Продукционные правила приведены в т*абл. 3* (фрагмент).

3. Применение пакета Fuzzy Logic Toolbox для построения НПМ

Реализация процесса нечеткого моделирования базы правил проводится посредством применения специализированного пакета *Fuzzy Logic Toolbox* программного средства *MATLAB* [11]. Выполнение нечеткого вывода реализуется на основе алгоритма Мамдани *(Mamdani)*.

Шаг 1. Фазификация — введение нечеткости. На этом шаге необходимо задать функции принадлежности для терм–множеств входных и выходных лингвистических переменных:

ПАЗ в модели соответствует лингвистической переменной «Программно-аппаратный уровень защиты» – x_1;

Таблица 3.

Нечеткие продукционные правила модели (фрагмент)

Обозначение	Антецедент	Консеквент
База правил П1		
П1.1	$(x_1=H \wedge x_2=H \wedge x_3=H) \vee (x_1=C \wedge x_2=H \wedge x_3=H) \vee (x_1=H \wedge x_2=C \wedge x_3=H)$	y_1= Очень ВОР
П1.2	$(x_1=B \wedge x_2=H \wedge x_3=H) \vee (x_1=C \wedge x_2=C \wedge x_3=H) \vee (x_1=H \wedge x_2=B \wedge x_3=H) \vee (x_1=C \wedge x_2=B \wedge x_3=H) \vee (x_1=H \wedge x_2=H \wedge x_3=C) \vee (x_1=H \wedge x_2=C \wedge x_3=C) \vee (x_1=H \wedge x_2=B \wedge x_3=C) \vee (x_1=H \wedge x_2=H \wedge x_3=B)$	y_1= ВОР
П1.3	$(x_1=B \wedge x_2=C \wedge x_3=H) \vee (x_1=B \wedge x_2=B \wedge x_3=H) \vee (x_1=C \wedge x_2=H \wedge x_3=C) \vee (x_1=B \wedge x_2=H \wedge x_3=C) \vee (x_1=C \wedge x_2=C \wedge x_3=C) \vee (x_1=C \wedge x_2=B \wedge x_3=C) \vee (x_1=C \wedge x_2=H \wedge x_3=B) \vee (x_1=H \wedge x_2=C \wedge x_3=B) \vee (x_1=C \wedge x_2=C \wedge x_3=B) \vee (x_1=H \wedge x_2=B \wedge x_3=B)$	y_1= СОР
П1.4	$(x_1=B \wedge x_2=C \wedge x_3=C) \vee (x_1=B \wedge x_2=B \wedge x_3=C) \vee (x_1=B \wedge x_2=H \wedge x_3=B) \vee (x_1=B \wedge x_2=C \wedge x_3=B) \vee (x_1=C \wedge x_2=B \wedge x_3=B)$	y_1= НОР
П1.5	$x_1=B \wedge x2=B \wedge x3=B$	y_1= Очень НОР

ОргЗ в модели соответствует лингвистической переменной «Уровень организационной защиты» – x_2;

ПравЗ в модели соответствует лингвистической переменной «Уровень правовой защиты» – x_3;

РискЗ в модели соответствует лингвистической переменной «Риск снижения эффективности защиты» – y_1.

Для входной переменной *ПАЗ* терм–множество состоит из трех термов T={*Низкий* (*H*), *Средний* (*C*), *Высокий* (*B*)}, которые характеризуют низкий, средний и высокий уровень программно-аппаратной защиты организации. Функции принадлежности для входной переменной *ПАЗ* являются трапециевидными. В общем случае трапециевидная функция принадлежности имеет следующий вид:

$$\mu_T(x,a,b,c,d)=\begin{cases}0, x \le a\\ \dfrac{x-a}{b-a}, a \le x \le b\\ \dfrac{d-x}{d-c}, c \le x \le d\\ 0, d \le x\end{cases}, \qquad (3)$$

где a, b, c, d – числовые параметры, характеризующие нижнее основание трапеции, (a, d) и верхнее (b, c), причем должно выполняться условие $a \le b \le c \ge d$.

С учетом (3) функции принадлежности нечетких терм-множеств лингвистической переменной «Программно–аппаратный уровень защиты» будут иметь следующий вид:

$$\mu_\Delta^H(x;0;0;0{,}15;0{,}45), \mu_\Delta^C(x;0{,}1;0{,}4;0{,}6;0{,}9),$$
$$\mu_\Delta^B(x;0{,}55;0{,}85;1{,}0;1{,}0).$$

На *рис. 1* приведены графики функций принадлежности терм–множеств лингвистической переменной *ПАЗ* – «Программно–аппаратный уровень защиты».

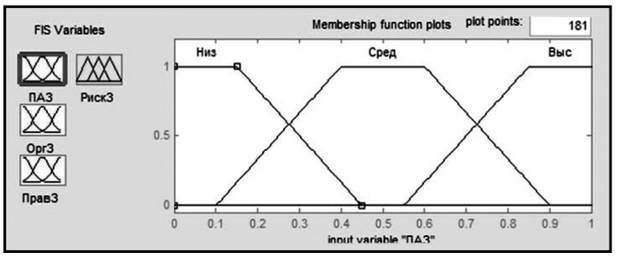

Рис. 1. Функции принадлежности для входной переменной ПАЗ

Для входной переменной *ОргЗ* терм–множество состоит из трех термов T={*H, C, B*}, функции принадлежности которых являются треугольными. В общем случае треугольная функция принадлежности имеет следующий вид:

$$\mu_\Delta(x,a,b,c)=\begin{cases}0, x \le a\\ \dfrac{x-a}{b-a}, a \le x \le b\\ \dfrac{c-x}{c-b}, b \le x \le c\\ 0, c \le x\end{cases}, \qquad (4)$$

где a, b, c — числовые параметры, характеризующие основание треугольника (a, c) и его вершину (b), причем должно выполняться условие $a \le b \le c$.

С учетом (4) функции принадлежности нечетких терм-множеств лингвистической переменной «Уровень организационной защиты» будут иметь следующий вид:

$$\mu_\Delta^H(x;\ 0;\ 0;\ 0{,}4),\ \mu_\Delta^C(x;\ 0{,}1;\ 0{,}5;\ 0{,}9),$$
$$\mu_\Delta^B(x;\ 0{,}6;\ 1,\ 0;\ 1{,}0).$$

На *рис. 2* приведены графики функций принадлежности терм–множеств лингвистической переменной *ОргЗ* – «Уровень организационной защиты».

Для входной переменной *ПравЗ* терм–множество состоит из трех термов T={*H, C, B*}, функции принадлежности которых являются трапециевидными.

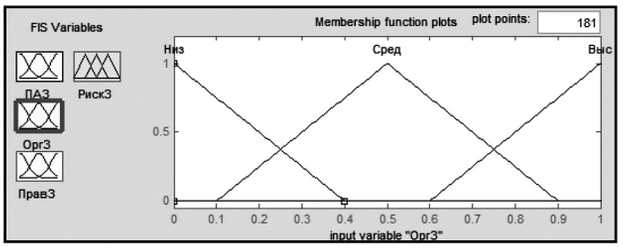

Рис. 2. Функции принадлежности для входной переменной ОргЗ

С учетом (3) функции принадлежности нечетких терм-множеств лингвистической переменной «Уровень правовой защиты» будут иметь следующий вид (*рис. 3*):

$\mu_{\Delta}^{H}(x; 0; 0; 0{,}15; 0{,}45)$, $\mu_{\Delta}^{C}(x; 0{,}05; 0{,}45; 0{,}55; 0{,}95)$, $\mu_{\Delta}^{B}(x; 0{,}55; 0{,}85; 1{,}0; 1{,}0)$.

На *рис. 3* приведены графики функций принадлежности терм–множеств лингвистической переменной *ПравЗ* – «Уровень правовой защиты».

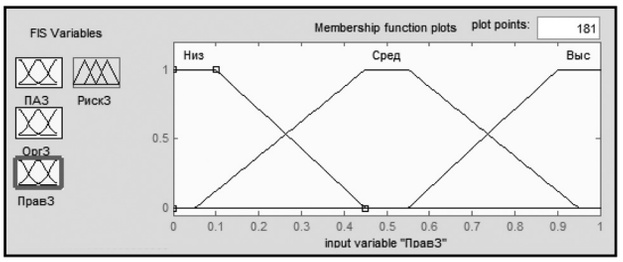

Рис. 3. Функции принадлежности для входной переменной ПравЗ

Для выходной переменной *РискЗ* (лингвистическая переменная «Риск снижения эффективности защиты») терм–множество состоит из пяти термов: *T={Очень низкая очевидность риска (OHOP); Низкая очевидность риска (HOP); Средняя очевидность риска (COP); Высокая очевидность риска (BOP); Очень высокая очевидность риска* (*OBOP*)}. Функции принадлежности лингвистических переменных являются трапециевидными.

С учетом (3) функции принадлежности нечетких терм–множеств лингвистической переменной «Риск снижения эффективности защиты» будут иметь следующий вид:

$\mu_{\Delta}^{OHOP}(x; 0; 0; 0{,}075; 0{,}22)$, $\mu_{\Delta}^{HOP}(x; 0{,}02; 0{,}2; 0{,}3; 0{,}48)$, $\mu_{\Delta}^{COP}(x; 0{,}28; 0{,}45; 0{,}55; 0{,}72)$, $\mu_{\Delta}^{BOP}(x; 0{,}52; 0{,}7; 0{,}8; 0{,}98)$, $\mu_{\Delta}^{OBOP}(x; 0{,}78; 0{,}925; 1{,}0)$.

На *рис. 4* приведены графики функций принадлежности терм–множеств лингвистической переменной *РискЗ* – «Риск снижения эффективности защиты».

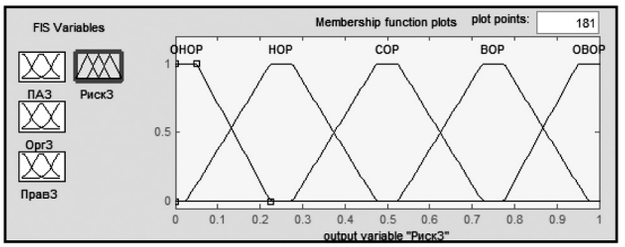

Рис. 4. Функции принадлежности для выходной переменной РискЗ

Шаг 2. Задание нечетких правил. В алгоритме Мамдани база правил должна задаваться в виде структуры с тремя входами и одним выходом (*рис. 5*).

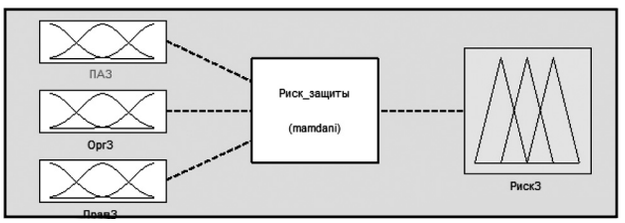

Рис. 5. Структура нечеткой модели для базы правил П1

Правила модели формируются на основе общих закономерностей поведения исследуемой системы и позволяют «вложить» в механизм вывода логическую модель прикладного уровня.

В алгоритме Мамдани для агрегирования степени истинности предпосылок используем *T*-норму и *min*-конъюнкция:

$$T(\mu_A(x), \mu_B(x)) = min(\mu_A(x), \mu_B(x)) \qquad (5)$$

Определение степени истинности заключений по каждому правилу (импликация) основано на операции *min*-активизации:

$$\mu_R(x,y) = min\{\mu_A(x), \mu_B(y)\}. \qquad (6)$$

Шаг 3. Аккумулирование заключения по всем правилам проведено с применением операции *max*-дизъюнкции. При дефазификации использован метод центра тяжести для дискретного множества значений функций принадлежности:

$$y' = \frac{\sum_{r=1}^{Ymax} y_r \mu_{B'}(y_r)}{\sum_{r=1}^{Ymax} \mu_{B'}(y_r)}, \qquad (7)$$

где Y_{max} – число элементов уг в дискретизированной для вычисления «центра тяжести» области *Y*.

Реализуя систему нечеткого вывода на этапе дефазификации, получим оценку приоритета риска. Приоритезация является основной целью анализа рисков и основополагающим фактором в процессе принятия решений по управлению рисками ИБ организации.

4. Использование модели оценки рисков ИБ организации

Предположим, что на основе предварительного обследования получены некоторые оценки уровня программно-аппаратной, организационной и правовой защиты организации, которые введем в окно механизма вывода графического интерфейса *Fuzzy Logic Toolbox.*

При значении классификатора *ПАЗ* = 0,7 значение лингвистической переменой x_1 – «Программно-аппаратный уровень защиты» соответствует терму *Н* – «достаточно, для базовой информационной защиты» с уровнем уверенности $\mu^H x_1 = 0{,}65\mu$. При значении классификатора *ОргЗ* = 0,75 значение лингвистической переменой x_2 — «Уровень организационной защиты» соответствует терму *С* — «планирование и мониторинг уязвимостей проводятся нерегулярно» с уровнем уверенности $\mu^C x_2 = 0{,}7\mu$. При значении классификатора *ПравЗ* = 0,65 значение лингвистической переменой x_3 — «Уровень правовой защиты» соответствует терму *С* – «документация имеется, но недостаточно детальная» с уровнем уверенности $\mu^C x_3 = 1{,}0\mu$.

По заданным исходным условиям активизируются правила 14 и 15. Результирующее значение классификатора выходной переменной *РискЗ* соответствует значению 0,386, что определяет значение лингвистической переменой риска проекта y_1 – «Риск снижения эффективности защиты» равное НОР – «Низкая очевидность риска» с уровнем уверенности $\mu^{HOP} y_1 = 0{,}5\mu$.

Графический интерфейс *Fuzzy Logic Toolbox* позволяет получить график зависимости выходной величины от любой из входных переменных.

На *рис. 6* представлен график «кривой вывода» зависимости выходной переменной *РискЗ* – «Риск снижения эффективности защиты» от входной

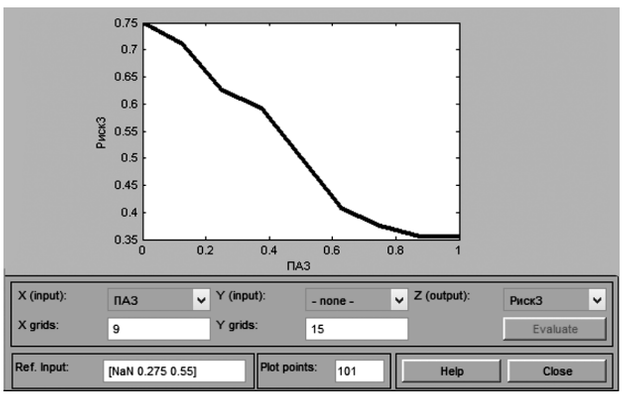

Рис. 6. Зависимость переменной РискЗ от ПАЗ

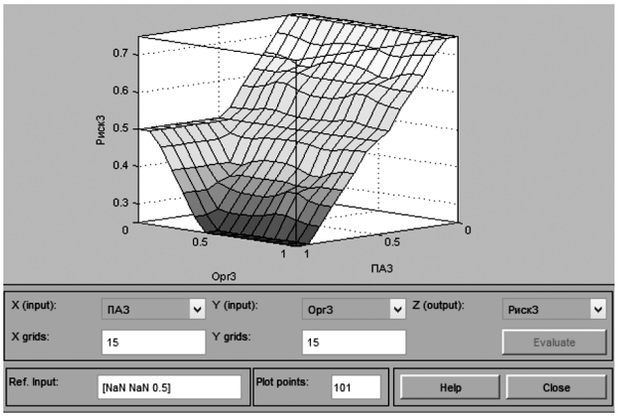

Рис. 7. Поверхность системы нечеткой модели относительно входных переменных ПАЗ и ОргЗ для базы правил П1

переменной *ПАЗ* – «Программно-аппаратный уровень защиты» при фиксированном значении двух других входных переменных для базы правил П1 нечеткой модели.

График показывает обратную зависимость величины риска снижения эффективности защиты организации от уровня программно-аппаратной защиты, а также что значение классификатора выходной переменной *РискЗ* не опускается ниже 0,35, что определяет значение лингвистической переменой риска информационной безопасности организации y_1 равное *НОР* – «Низкая очевидность риска» с уровнем уверенности $\mu^{HOP}_{y1} = 0{,}57\mu$, при значении классификатора *ПАЗ* = 0,85, при котором значение лингвистической переменой x_1 соответствует терму *В* – «полностью соответствует уровню конфиденциальности информации» с уровнем уверенности $\mu^B_{x1} = 0{,}95\mu$ и фиксированных значениях классификатора *ОргЗ* = 0,275, при котором значение лингвистической переменой x_2 соответствует терму *С* — «планирование и мониторинг уязвимостей проводятся нерегулярно» с уровнем уверенности $\mu^C_{x2} = 0{,}5\mu$, и классификатора *ПравЗ* = 0,55, при котором значение лингвистической переменой x_3 соответствует терму *С* – «документация имеется, но недостаточно детальная» с уровнем уверенности $\mu^C_{x3} = 1{,}0\mu$.

На *рис. 7* приведена поверхность зависимости выходной лингвистической переменной от двух входных с фиксированным значением третей переменной для базы правил П1 нечеткой модели.

Графический вид зависимостей выходной лингвистической переменной *РискЗ* – «Риск снижения эффективности защиты» от входных значений переменных *ПАЗ* – «Программно-аппаратный уровень

защиты» и *Орг3* – «Уровень организационной защиты» показывает закономерный рост величины риска снижения эффективности защиты организации при уменьшении уровня программно-аппаратной защиты и уровня организационной защиты.

Интерфейс *Fuzzy Logic Toolbox* обеспечивается возможность контролировать «качество» механизма вывода. Таким образом, гладкие и монотонные графики зависимостей приведенных «поверхностей вывода» и «кривых вывода» свидетельствуют о хорошем «качестве» механизма вывода и о достаточности и непротиворечивости используемых правил вывода.

5. Заключение

Разработанная нечеткая 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.

В НПМ определены 7 входных лингвистических переменных, характеризующих факторы риска, 4 выходных лингвистических переменных, характеризующих риски различных областей ИБ. Модель содержит 4 базы правил и позволяет проводить лингвистический анализ рисков, которые несут потенциальные угрозы и ущерб организации. Используемый в методике механизм получения оценок риска на основе нечеткой логики позволяет получить численное значение риска, лингвистическое описание степени риска, а также уровень уверенности эксперта в возникновении рискового события, которые позволят IT-менеджерам выявить приоритеты рисков (очень высокий, высокий, средний, низкий, очень низкий) и выработать план мероприятий по снижению влияния наиболее опасных угроз на информационную безопасность организации.

Основная сложность механизма получения оценок риска на основе нечеткой логики состоит в построении модели для проведения лингвистического анализа рисков СОИБ, 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 учетом реальных условий политики информационной безопасности организации. ■

Литература

1. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
2. Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ В.В.Путиным 09.09.2000 г., № Пр-1895). – Российская газета, № 187, 28.09.2000 г.
3. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005).
4. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» (ГОСТ Р ИСО/МЭК 27001-2006).
5. Марков А., Цирлов В. Управление рисками – нормативный вакуум информационной безопасности // Открытые системы. СУБД: Журнал для профессионалов в области информационных технологий. – 2007. – №8. – С. 63-67.
6. Симонов С.В. Анализ рисков, управление рисками. – Jet Info, 2003, №2.
7. Risk Management Guide for Information Technology Systems. – NIST, Special Publication 800-30.
8. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. – М.: Горячая линия-Телеком, 2007. .
9. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976.
10. Долженко А.И. Модель анализа риска потребительского качества проектов экономических информационных систем // Вестник Северо-Кавказского государственного технического университета. – 2009. – №1 (18). – С.129-134.
11. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005.