ISSN 1814-1196
Научный вестник НГТУ
том 65, № 4, 2016, с. 121–134

http://journals.nstu.ru/vestnik
Science Bulletin of the NSTU
Vol. 65, No. 4, 2016, pp. 121–134

УДК 004.934.2

Анализ рисков информационной безопасности с использованием системы нечеткого вывода*

И.В. СИБИКИНА

414056, РФ, г. Астрахань, ул. Татищева, 16, Астраханский государственный технический университет, кандидат технических наук, доцент. E-mail: isibikina@bk.ru

В статье представлены этапы построения системы нечеткого вывода при анализе рисков информационной безопасности. Обоснованы необходимость и возможность использования нечеткого моделирования при реализации политики безопасности предприятия или организации. Отмечена сложность задачи оценки рисков информационной безопасности в связи с отсутствием общепринятых подходов и методик для оценки рисков. Проанализированы достоинства и недостатки существующих методик анализа рисков информационной безопасности. Описаны процедуры сбора и обработки экспертной информации, необходимой для построения системы нечеткого вывода

Предложена методика построения лингвистических шкал, в основу которой положен метод статистического эксперимента. Авторами построены функции принадлежности нечетких переменных «степень риска», «степень ущерба», «уровень угрозы» на основе экспертных данных, необходимые при построении нечеткой модели. Представлен расчетный пример определения функций принадлежности для одной из нечетких переменных. Автором сформированы продукционные правила для системы нечеткого вывода. Предложенные процедуры и методы были реализованы в виде системы нечеткого вывода в среде MatLab. Приведены этапы построения и анализ адекватности нечеткой модели. Представлен графический интерфейс редактора переменных, редактора правил, поверхности нечеткого вывода модели, разработанные в среде MatLab. Полученная модель позволяет установить зависимость значений выходной переменной «степень риска» от значений входных переменных «уровень угрозы», «степень ущерба» и «степень уязвимости». Результаты моделирования автоматически меняются при изменении параметров входных переменных, что позволяет использовать данную модель при изменяющихся внешних условиях. Результаты могут быть использованы для решения задач управления информационной безопасностью.

Ключевые слова: анализ рисков информационной безопасности, управление информационной безопасностью, обработка экспертных данных, нечеткое моделирование, функции принадлежности, продукционные правила, система нечеткого вывода, модель оценки рисков

DOI: 10.17212/1814-1196-2016-4-121-134

* *Статья получена 23 ноября 2016 г.*

ВВЕДЕНИЕ

Для создания системы информационной безопасности требуется решение задач, которые направлены на обработку, хранение и защиту формализованной информации. В этом случае можно сформировать и при помощи методов теории информации рассчитать довольно точные параметры, отражающие степень защищенности объекта или системы. Однако для комплексной оценки степени защищенности нередко приходится применять экспертные методы оценивания тех параметров, которые невозможно рассчитать при помощи теоретико-информационного подхода. Предпосылкой для применения нечетких моделей является наличие неопределенности, обусловленной отсутствием информации либо сложностью системы, и наличие информации качественного характера о системе [1].

Деятельность практически любой организации сопряжена с необходимостью применения современных технологий сбора, обработки и хранения информации. В связи с этим неизбежны возникновения угроз информационной безопасности (ИБ), которые необходимо своевременно устранять во избежание потери целостности, конфиденциальности и доступности информации и нанесения ущерба деятельности организации. Одним из важнейших этапов в процессе управления информационной безопасностью является этап анализа и оценки рисков ИБ.

Оценка рисков информационной безопасности в задаче управления ИБ на сегодняшний момент – одна из сложных и актуальных задач. Сложность заключается в том, что отсутствуют общепринятые подходы и методики для оценки рисков [2–7]. Факторы риска (угроза, уязвимость, ущерб) анализируются с помощью эвристических методов, в результате чего могут получиться данные, отличные друг от друга, если экспертиза проводилась различными экспертами [2]. Кроме этого, процедура оценки рисков является трудоемкой задачей. Проводить анализ вручную, применяя офисные инструменты, задача практически невыполнимая в связи с большими объемами обрабатываемой информации и вероятностью получить ошибочный результат. Поэтому необходимо применять совокупность методов анализа и обработки информации, позволяющих оценить риски информационной безопасности и на основе полученных данных осуществлять управление информационной безопасностью.

Управление информационной безопасностью объекта может быть реализовано при помощи систем нечеткого вывода в совокупности с экспертными методами оценивания. В данной работе будет рассмотрена реализация анализа рисков информационной безопасности в виде нечеткого моделирования в среде MatLab с использованием метода статистического эксперимента для построения функций принадлежности нечетких переменных.

ПОСТАНОВКА ЗАДАЧИ

Для создания системы информационной безопасности требуется решение задач, которые направлены на обработку, хранение и защиту формализованной информации. В этом случае можно сформировать и при помощи методов теории информации рассчитать довольно точные параметры, отражающие степень защищенности объекта или системы. Однако для комплексной

оценки степени защищенности нередко приходится применять экспертные методы оценивания тех параметров, которые невозможно рассчитать при помощи теоретико-информационного подхода.

Формирование системы информационной безопасности объекта, требует решения ряда задач, связанных с формализованной информацией – информацией взаимодействия в форме документов или обменных сигналов технических систем. В этих случаях вполне применимы методы математической теории информации и удается сформировать весьма точные значения параметров, характеризующих защищенность системы. Однако для полной оценки защищенности эти параметры приходится сопоставлять с оценками для не поддающейся непосредственному доступу информации воздействия. Например, можно достаточно достоверно оценить вероятность восстановления отдельного слова в перехваченном речевом сообщении, однако далее необходимо установить, какую вероятность считать допустимой. Получить такую оценку можно только экспертным путем. Применять методы теории информации в этом случае неэффективно, так как результат полностью определяется исходными допущениями, формируемыми фактически произвольно. Для различных ситуаций, различного содержания фраз, различного словарного состава экспертные оценки могут дать результаты, отличающиеся на порядок. Предпосылкой для применения нечетких моделей является наличие неопределенности, обусловленной отсутствием информации либо сложностью системы, и наличие информации качественного характера о системе [2].

К преимуществам нечетких систем следует отнести их универсальность. Согласно исследованию [8], любая непрерывная функция может быть представлена нечеткой моделью с любой заданной точностью. Особые качества систем с нечеткой логикой позволяют синтезировать модель объекта на основании эвристической информации, полученной от эксперта или в результате эксперимента. Вместе с тем нечетким системам присущи такие недостатки, как отсутствие алгоритмов синтеза устойчивых моделей и низкая скорость работы последних при большом числе управляющих правил [2, 9, 10].

ОСНОВНЫЕ ЭТАПЫ ПОСТРОЕНИЯ НЕЧЕТКОЙ МОДЕЛИ

Построение нечеткой модели основано на формализации характеристик системы управления информационной безопасностью в терминах лингвистических переменных. Основными понятиями систем управления являются алгоритмы управления, входные и выходные переменные. Именно они рассматриваются как лингвистические переменные при формировании базы правил в системах нечеткого вывода [10].

В настоящее время предложено несколько алгоритмов нечеткого вывода: Мамдани, Цукамото, Ларсена, Сугено. Упрощенный алгоритм нечеткого вывода формально может быть определен следующим образом.

1. Формирование базы правил нечеткого вывода.
2. Фаззификация входных переменных.
3. Агрегирование подусловий в нечетких правилах продукций.

4. Активизация подзаключений в нечетких правилах продукций.

5. Аккумуляция заключений в нечетких правилах продукций.

6. Дефаззификация выходных переменных.

Цель создания нечеткой модели управления информационной безопасностью заключается в том, чтобы на основе текущего состояния объекта защиты определить значения управляющих переменных, реализация которых обеспечит необходимый уровень защиты.

В классической теории управления базовая модель основана на представлении объекта и процесса в виде некоторых систем. Объект управления характеризуется конечным множеством входных и выходных переменных. Входные переменные формируются с помощью конечного множества датчиков. На выходе системы управления формируется множество выходных (управляющих) переменных. Значения управляющих переменных поступают на вход объекта управления и формируют адекватное управляющее воздействие.

В случае если строится модель нечеткого управления, то классическая система управления заменяется системой нечеткого управления [10]. В качестве данной системы используется система нечеткого вывода с реализацией всех необходимых этапов (рис. 1). Процесс нечеткого вывода формируется на основе одного из алгоритмов нечеткого вывода.

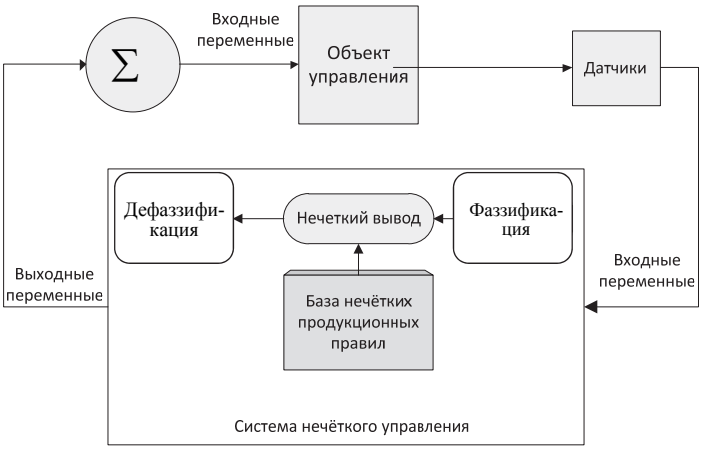

Рис. 1. Схема процесса нечеткого управления

ПОСТРОЕНИЕ ЛИНГВИСТИЧЕСКИХ ШКАЛ ДЛЯ ПЕРЕМЕННЫХ НЕЧЕТКОЙ МОДЕЛИ

Для построения системы нечеткого вывода служит система MatLab, обладающая достаточно широким функционалом. Для оценки рисков необходимо задать входные переменные, которыми являются факторы риска: угроза, ущерб и уязвимость. Выходной переменной является степень риска.

Однако, прежде чем приступать к построению нечеткой модели, необходимо построить функции принадлежностей для каждой из нечетких переменных. Входные переменные имеют значения в интервале от 0 до 1. Чем ближе значение каждой из переменных к единице, тем более высока степень воздей-

ствия фактора риска на систему безопасности. Для построения функций принадлежности предлагаем использовать метод построения лингвистических шкал [11, 12].

Построение нечеткой лингвистической шкалы для каждой из нечетких переменных осуществляется в два этапа:

1) определение множества значений лингвистической переменной β_i;

2) размещение значений лингвистической переменной на универсальной шкале от 0 до 1.

На первом этапе речь идет о построении синтаксического правила, порождающего названия значений лингвистической переменной. Процедура выполняется на эвристическом уровне. При этом число термов должно быть не очень большим во избежание затруднений у экспертов при формировании предпочтений при выборе конкретного значения лингвистической переменной. С другой стороны, это число не должно быть слишком малым, чтобы не загрублять чувствительность оценок эксперта [11, 12].

Далее выбираются названия термов. Должно выполняться требование – однозначное толкование этих названий большинством экспертов.

Определим входные лингвистические переменные: β_1 – уровень угрозы, β_2 – степень ущерба, β_3 – степень уязвимости.

Определим терм-множества для входных переменных:

- для переменной β_1 терм-множество имеет вид

$$T_1 = \{\textit{низкий},\ \textit{средний}, \textit{высокий}\};$$

- для переменной β_2 терм-множество имеет вид

$$T_2 = \{\textit{незначительный},\ \textit{достаточный}, \textit{значительный}\};$$

- для переменной β_3 терм-множество имеет вид

$$T_3 = \{\textit{незначительный},\ \textit{умереннай}, \textit{серьезный}\}.$$

На втором этапе построения нечеткой лингвистической шкалы задается семантическое правило, сопоставляющее название лингвистической переменной с ее смыслом, т. е. строится функция принадлежности термов множества.

Одним из способов построения функций принадлежности является способ статистического эксперимента [8]. Предположим, что эксперту необходимо оценить в значениях лингвистической переменной «степень угрозы» , угроза принимает значения ΔВ , где В – максимально возможная угроза, ΔВ лежит в интервале [0; В]. Разделим интервал на *N* отрезков.

Группе экспертов в случайном порядке предъявляются числа из каждого отрезка, интерпретируемые как точечные значения степени угрозы. Эксперт на основе индивидуальных представлений относит предъявленное значение к определенным термам из множества Т. В ходе эксперимента формируется эмпирическая таблица (табл. 1) , каждый элемент которой a_{ij} есть суммарное количество отнесения случайного числа из отрезка j к i-му терму.

Таблица 1

Результаты статистического эксперимента

Значение лингвистической переменной «степень угрозы»	Интервал					
	1	2	…	j	…	N
Низкий	a_{11}	a_{12}	…	a_{1j}	…	a_{1N}
Средний	a_{21}	a_{22}	…	a_{2j}	…	a_{2N}
Высокий	a_{31}	a_{32}	…	a_{3j}	…	a_{3N}

Очевидно, что если в каждый интервал попадает одинаковые число экспериментов, то степень принадлежности некоторого значения может быть вычислена как отношение числа экспериментов, в котором оно встречалось в определенном интервале шкалы, к максимальному для этого значения числу экспериментов по всем интервалам [12–15]. Однако на практике это условие может и не соблюдаться (например, эксперт затрудняется отнести оцениваемое значение к какому-либо интервалу).

Заметим, что естественными свойствами функции принадлежности являются наличие одного максимума и гладкие, затухающие до нуля фронты. Поэтому до обработки из эмпирической таблицы должны быть удалены явно ошибочные данные. Критерием удаления служит наличие нескольких нулей в строке вокруг этого элемента.

Тогда значение функции принадлежности по эмпирической матрице может быть рассчитано по следующему алгоритму [10].

Формируется вспомогательная матрица

$$R_{1\times N} = \left\{ r_1, r_2, ..., r_j, ..., r_n \right\}, \tag{1}$$

где N – количество интервалов разбиения максимально возможного изменения,

$$r_j = \sum_{i=1}^{n} a_{ij} , \tag{2}$$

где n – число термов.

Из вспомогательной матрицы выбирается максимальный элемент

$$r_{\max} = \max_{j=1,...,N} r_j . \tag{3}$$

Все элементы эмпирической таблицы преобразуются по формуле

$$c_{ij} = \frac{a_{ij} r_{\max}}{r_j}, \; i = \overline{1,n}, \; j = \overline{1,N} , \tag{4}$$

Для столбцов, где $r_j = 0$, применяется линейная аппроксимация

$$c_{ij} = \frac{c_{i(j-1)} + c_{i(j+1)}}{2},\ i = \overline{1,n},\ j = \overline{1,N}. \quad (5)$$

По строкам эмпирической таблицы выделяются максимальные элементы

$$c_{\max} = \max_{j=1,\ldots,N} c_{ij},\ i = \overline{1,n}. \quad (6)$$

Значения функции принадлежности вычисляются по формуле

$$\gamma_{ij} = \frac{c_{ij}}{c_{i\max}}. \quad (7)$$

Таким образом, в результате обработки данных статистического эксперимента имеем n дискретных нечетких множеств.

Дискретные функции принадлежности могут быть интерполированы непрерывными функциями вида $\varphi_j(\mathrm{B})$. Тогда семантическое правило запишется в следующем виде:

$$\text{низкий} = {}^{\Delta}\left\{\left\langle \Delta \mathrm{B}_j,\ \psi_1(\Delta \mathrm{B} \middle| \psi_1(\Delta \mathrm{B}_j) = \gamma_{1j} \right\rangle\right\},$$

$$\text{средний} = {}^{\Delta}\left\{\left\langle \Delta \mathrm{B}_j,\ \psi_2(\Delta \mathrm{B} \middle| \psi_1(\Delta \mathrm{B}_j) = \gamma_{2j} \right\rangle\right\},$$

$$\text{высокий} = {}^{\Delta}\left\{\left\langle \Delta \mathrm{B}_j,\ \psi_3(\Delta \mathrm{B} \middle| \psi_3(\Delta \mathrm{B}_j) = \gamma_{3j} \right\rangle\right\}.$$

РЕАЛИЗАЦИЯ ПРОЦЕДУРЫ ПОСТРОЕНИЯ ЛИНГВИСТИЧЕСКОЙ ШКАЛЫ

Интервал изменения $\beta \in [0,1]$. Экспертами принято решение разбить интервал на 10 отрезков. Результаты статистического эксперимента для определения функции принадлежности переменной «степень угрозы» представлены в табл. 2.

Таблица 2

Результаты экспертизы

Значение лингвистической переменной «степень угрозы»	Интервал									
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Низкий	10	9	8	1	1	0	0	0	0	0
Средний	0	1	2	9	8	8	0	0	0	0
Высокий	0	0	0	0	1	2	10	10	10	10

Далее, согласно представленой методике табл. 2 преобразована и получена табл. 3.

Таблица 3

Преобразованная матрица

Значение	Интервал									
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Низкий	10	9	8	2	1	0	0	0	0	0
Средний	0	1	2	8	8	8	6	1	0	0
Высокий	0	0	0	0	1	2	4	9	10	10

Результирующая матрица представлена в табл. 4.

Таблица 4

Функция принадлежности переменной «степень угрозы»

Значение	Интервал									
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Низкий	1	0,9	0,8	0,3	0,1	0	0	0	0	0
Средний	0	0,125	0,25	0,875	1	1	0,75	0,125	0	0
Высокий	0	0	0	0	0,1	0,2	0,4	0,9	1	1

Согласно данным табл. 4 построим функции принадлежности нечеткой переменной «степень угрозы» (рис. 2).

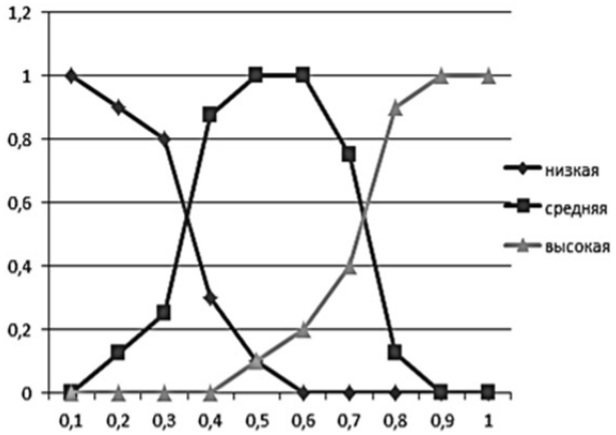

Рис. 2. График функций принадлежности переменной «степень угрозы»

Аналогично строятся функции принадлежности для входных переменных «степень ущерба» и «степень уязвимости».

В результате применения метода статистического эксперимента для обработки экспертных данных получаем лингвистические шкалы для нечетких переменных, которые можно использовать при построении системы нечеткого вывода в MatLab.

Таблица 5

Значения нечетких переменных

Значение терма	Значение переменной β_1	Значение терма для переменной β_2	Значение переменной β_2	Значение терма для переменной β_3	Значение переменной β_3
Низкий	[0; 0,35]	Незначительный	[0; 0,3]	Незначительный	[0; 0,35]
Средний	[0,35; 0,75]	Достаточный	[0,3; 0,6]	Умеренный	[0,35; 0,7]
Высокий	[0,75; 1]	Значительный	[0,6; 1]	Серьезный	[0,7; 1]

РЕАЛИЗАЦИЯ НЕЧЕТКОЙ МОДЕЛИ. ОЦЕНКА СТЕПЕНИ РИСКА В MATLAB

Разработка нечеткой экспертной системы, реализованная в виде системы нечеткого вывода, которая на основе оценок экспертов степени угроз уровня ущерба и уровня уязвимостей позволит определять степень риска.

Графический интерфейс редактора функций принадлежности после задания входной переменной «степень угрозы» показан на рис. 3. Значения терм-множеств данной входной переменной заданы согласно полученным лингвистическим шкалам.

Аналогично происходит задание переменных «степень ущерба», «степень уязвимости».

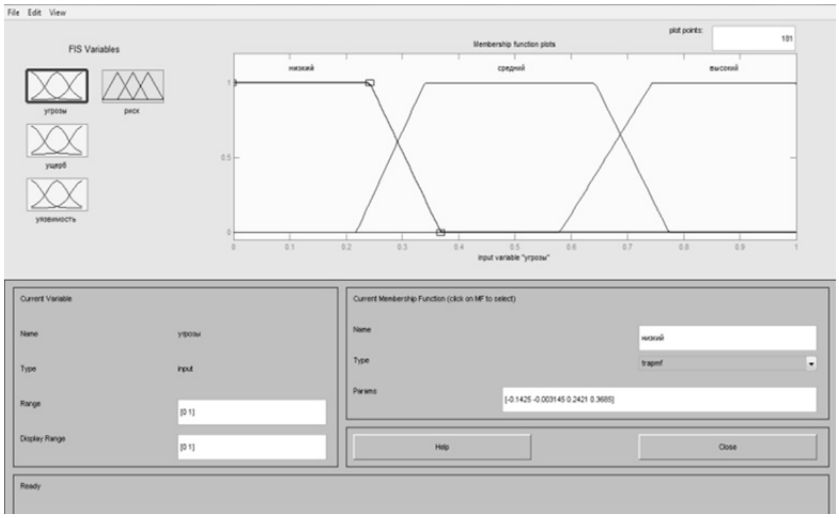

Рис. 3. Редактор переменных

Далее происходит задание правил для системы нечеткого вывода. Вид графического интерфейса редактора правил после задания всех правил изображен на рис. 4.

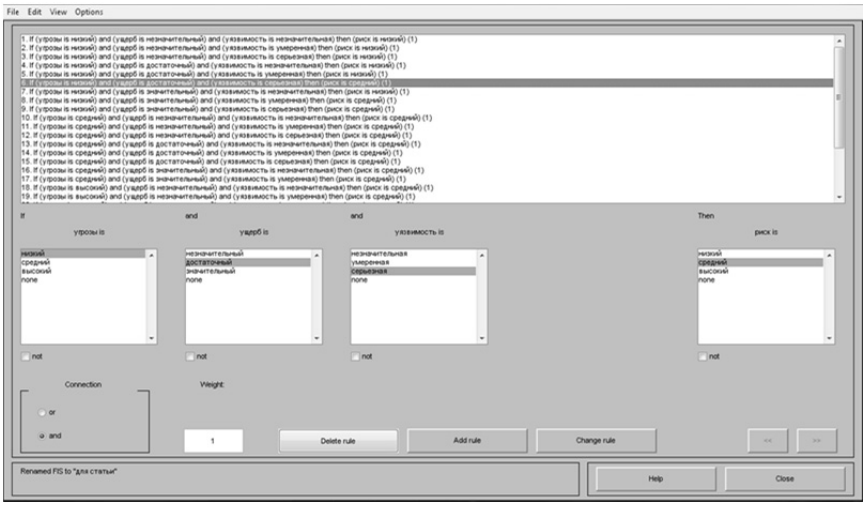

Рис. 4. Редактор правил

Теперь можно выполнить оценку построенной системы нечеткого вывода для задачи оценки рисков информационной безопасности. Для этого откроем окно просмотра (рис. 5) и введем значения входных переменных для частного случая: уровень угрозы = 0,549; степень ущерба = 0,91; степень уязвимости = 0,512. Процедура нечеткого вывода, реализованная в системе MatLab для разработанной нечеткой модели, выдает результат 0,866, что подтверждает ее адекватность, в рамках рассматриваемой модели.

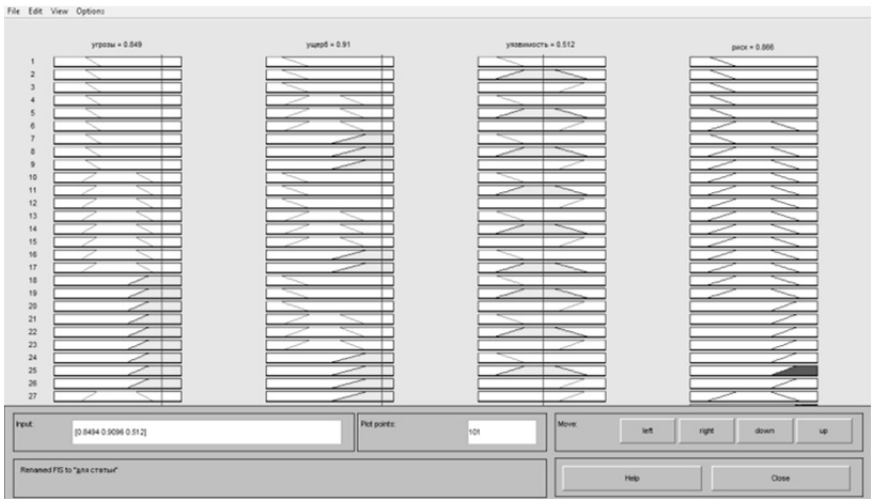

Рис. 5. Редактор просмотра правил

Процесс исследования и анализа разработанной нечеткой модели состоит из тестового выполнения нечетких выводов для различных значений входных переменных и оценки полученных результатов с целью внесения необходимых корректировок в случае несогласованности отдельных результатов.

Общий анализ разработанной модели позволяет получить поверхность нечеткого вывода (рис. 6).

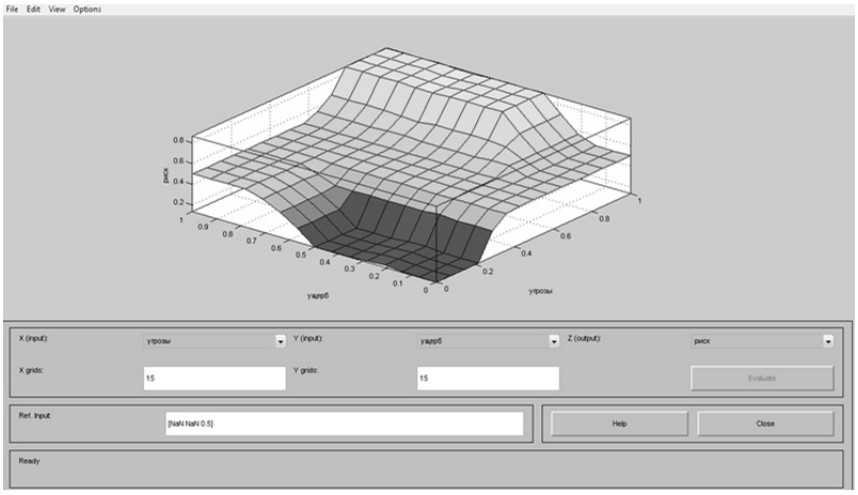

Рис. 6. Поверхность нечеткого вывода

Данная поверхность нечеткого вывода позволяет установить зависимость значений выходной переменной «степень риска» от значений входных переменных «уровень угрозы», «степень ущерба» и «степень уязвимости».

ЗАКЛЮЧЕНИЕ

Рассмотренная методика построения функций принадлежности на основе экспертных данных и моделирование нечеткой системы анализа рисков информационной безопасности является одним из этапов решения задачи управления информационной безопасностью. Процедура построения лингвистических шкал позволяет получить функции принадлежности для нечетких переменных. Нечеткая экспертная система, реализованная в среде MatLab, определяет значения выходной переменной в зависимости от входных данных. MatLab позволяет оценить адекватность построенной модели. Представленные методы и процедуры могут быть использованы при решении практических задач.

СПИСОК ЛИТЕРАТУРЫ

1. *Зайченко Ю.П.* Нечеткие модели и методы в интеллектуальных системах: учебник для вузов. – Киев: Слово, 2008. – 344 с.

2. *Булдакова Т.И., Миков Д.А.* Реализация методики оценки рисков информационной безопасности в среде Matlab // Вопросы кибербезопасности. – 2015. – № 4 (12) – С. 53–61.

3. *Космачева И.М., Сибикина И.В., Галимова Л.В.* Алгоритм оценки риска нарушения информационных сервисов в организации // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2015. – № 2. – С. 58–64.

4. *Выборнова О.Н.* Онтологическая модель процесса оценки рисков // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2015. – № 2. – С. 97–102.

5. *Давидюк Н.В., Белов С.В.* Формирование начальной популяции в процедуре генетического поиска варианта эффективного расположения средств обнаружения на объекте защиты // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2010. – № 1. – С. 114–118.

6. *Сибикина И.В., Космачева И.М., Давидюк Н.В.* Мониторинг качества подготовки выпускников ВУЗа при осуществлении компетентностного подхода // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2013. – № 1. – С. 208–214.

7. *Ажмухамедов И.М.* Динамическая нечеткая когнитивная модель оценки уровня безопасности информационных активов ВУЗа // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2012. – № 2. – С. 137–142.

8. *Усков А.А.* Принципы построения систем управления с нечеткой логикой // Приборы и системы. Управление, контроль, диагностика. – 2004. – № 6. – С. 7–13.

9. *Sivanandam S.N., Sumathi S., Deepa S.N.* Introduction to fuzzy logic using Matlab. – Berlin: Springer, 2007. – 430 p.

10. *Леоненков А.В.* Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 716 с.

11. *Сибикина И.В., Квятковская И.Ю.* Построение лингвистических шкал в целях выявления важных дисциплин, формирующих компетенцию // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2012. – № 2. – С. 182–186.

12. *Сибикина И.В., Квятковская И.Ю.* Теоретические основы разработки информационных систем и ресурсов на основе модели компетенции для автоматизированных систем управления вузом. – Астрахань: АГТУ, 2016. – 100 с.

13. *Космачева И.М., Яковлева Е.П.* Подсистема управления доступом в информационных системах вуза // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2016. – № 2. – С. 25–34.

14. *Белов С.В., Мельников А.В.* Процедура оценки показателей злоумышленного проникновения в составе автоматизированной системы контроля физической безопасности объекта защиты // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2014. – № 2. – С. 28–37.

15. *Белов С.В., Досмухамедов Б.Р.* Оценка степени злоумышленного интереса к различным компонентам объекта защиты // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2013. – № 1. – С. 14–20.

Сибикина Ирина Вячеславовна, кандидат технических наук, доцент кафедры информационной безопасности Астраханского государственного технического университета. Основное направление научных исследований: управление в социально-экономических системах, информационная безопасность. Имеет более 30 публикаций, в том числе 1 монография. E-mail: isibikina@bk.ru.

Analysis of information security risks by using a fuzzy inference system [*]

I.V. SIBIKINA

Astrakhan State Technical University, 16 Tatishchev Street, Astrakhan, Russian Federation, PhD (Eng.), associate professor. E-mail: isibikina@bk.ru

Stages of creating a fuzzy inference system while analyzing information security risks are described in the article. A need and a possibility to use fuzzy modeling while implementing a security policy at an enterprise or organization is proved. The complexity of the task of evaluating information security risks due to the lack of standard techniques and approaches to risk evaluation is considered. Merits and demerits of the existing techniques of information security risk analysis are studied. Procedures of collecting and processing expert information necessary for creating a fuzzy inference system are described. A technique for building linguistic scales

[*] *Received 23 November 2016.*

based on the statistical experiment method is proposed. The author constructed membership functions of fuzzy variables such as "a risk degree", "a damage level" and "a threat level" based on expert data necessary in building a fuzzy model. An example of calculating membership functions for one of the fuzzy variables is provided. The author developed rules for generating a fuzzy inference system. The proposed procedures and methods were implemented in the form of a fuzzy inference system in the Matlab environment. Stages of creating and analyzing the adequacy of the fuzzy model are described. A graphic interface of the variable editor, rule editor, and surfaces of the fuzzy inference model developed in the Matlab environment is provided. The proposed model makes it possible to reveal the dependence of values of such an output variable as "a risk degree" on the values of such input variables as "a threat level", "a damage level" and "a vulnerability level". The results of simulation automatically change when parameters of input variables change, which allows using this model under changing external conditions. The results can be used for solving problems of information security management.

Keywords: analysis of information security risks, information security management, processing of expert data, fuzzy modeling, membership function, production rules, fuzzy inference system, risk assessment model

DOI: 10.17212/1814-1196-2016-4-121-134

REFERENCES

1. Zaichenko Yu.P. *Nechetkie modeli i metody v intellektual'nykh sistemakh* [Indistinct models and methods in intellectual systems]. Kiev, Slovo Publ., 2008. 344 p.

2. Buldakova T.I., Mikov D.A. Realizatsiya metodiki otsenki riskov informatsionnoi bezopasnosti v srede Matlab [Realization of a technique of assessment of risks of information security in the environment of Matlab]. *Voprosy kiberbezopasnosti – Cybersecurity Issues*, 2015, no. 4 (12), pp. 53–61.

3. Kosmacheva I.M., Sibikina I.V., Galimova L.V. Algoritm otsenki riska narusheniya informatsionnykh servisov v organizatsii [Algorithm of assessment of risk of violation of information services in the organization]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2015, no. 2, pp. 58–64.

4. Vybornova O.N. Ontologicheskaya model' protsessa otsenki riskov [Ontologic model of process of assessment of risks]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2015, no. 2, pp. 97–102.

5. Davidyuk N.V., Belov S.V. Formirovanie nachal'noi populyatsii v protsedure geneticheskogo poiska varianta effektivnogo raspolozheniya sredstv obnaruzheniya na ob"ekte zashchity [Forming of initial population in the procedure of genetic search of option of an effective arrangement of sensors on subject to protection]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2010, no. 1, pp. 114–118.

6. Sibikina I.V., Kosmacheva I.M., Davidyuk N.V. Monitoring kachestva podgotovki vypusknikov VUZa pri osushchestvlenii kompetentnostnogo podkhoda [Forming of initial population in the procedure of genetic search of option of an effective arrangement of sensors on subject to protection]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2013, no. 1, pp. 208–214.

7. Azhmukhamedov I.M. Dinamicheskaya nechetkaya kognitivnaya model' otsenki urovnya bezopasnosti informatsionnykh aktivov VUZa [Dynamic indistinct cognitive model of assessment of level of safety of data assets of higher education institution]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2012, no. 2, pp. 137–142.

8. Uskov A.A. Printsipy postroeniya sistem upravleniya s nechetkoi logikoi [The principles of creation of control systems with fuzzy logic]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika – Instruments and Systems: Monitoring, Control, and Diagnostics*, 2004, no. 6, pp. 7–13.

9. Sivanandam S.N., Sumathi S., Deepa S.N. *Introduction to fuzzy logic using Matlab*. Berlin, Springer, 2007. 430 p.

10. Leonenkov A.V. *Nechetkoe modelirovanie v srede MATLAB i fuzzyTECH* [Indistinct modeling in the environment of MATLAB and fuzzyTECH]. St. Petersburg, BHV-Petersburg Publ., 2005. 716 p.

11. Sibikina I.V., Kvyatkovskaya I.Yu. Postroenie lingvisticheskikh shkal v tselyakh vyyavleniya vazhnykh distsiplin, formiruyushchikh kompetentsiyu [Creation of linguistic scales for identification of the important disciplines forming competence]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2012, no. 2, pp. 182–186.

12. Sibikina I.V., Kvyatkovskaya I.Yu. *Teoreticheskie osnovy razrabotki informatsionnykh sistem i resursov na osnove modeli kompetentsii dlya avtomatizirovannykh sistem upravleniya vuzom* [Theoretical bases of development of information systems and resources on the basis of competence model for automated control systems for higher education institution]. Astrakhan', ASTU Publ., 2016. 100 p.

13. Kosmacheva I.M., Yakovleva E.P. Podsistema upravleniya dostupom v informatsionnykh sistemakh vuza [The subsystem access control in information systems of the University]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2016, no. 2, pp. 25–34.

14. Belov S.V., Mel'nikov A.V. Protsedura otsenki pokazatelei zloumyshlennogo proniknoveniya v sostave avtomatizirovannoi sistemy kontrolya fizicheskoi bezopasnosti ob"ekta zashchity [Procedure of evaluation of indicators of malicious penetration in the automated monitoring system of physical security of the protected object]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2014, no. 2, pp. 28–37.

15. Belov S.V., Dosmukhamedov B.R. Otsenka stepeni zloumyshlennogo interesa k razlichnym komponentam ob"ekta zashchity [Assessment of the level of malicious interest in the various components of the protected object]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika – Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*, 2013, no. 1, pp. 14–20.