

# БЕЗОПАСНОСТЬ ИНФОРМАЦИИ CRYPTOSAFETY INFORMATION

УДК 004.64

С. А. Глушенко, аспирант, e-mail: www.555.sergey@mail.ru,  
А. И. Долженко, д-р эконом. наук, доц., проф., e-mail: doljenkoalex@gmail.ru,  
Ростовский государственный экономический университет, г. Ростов-на-Дону

## Система поддержки принятия решений нечеткого моделирования рисков информационной безопасности организации

*Обосновывается целесообразность применения нечеткой логики для оценки риска информационной безопасности организации, а также предъявляются функциональные требования к системе поддержки принятия решений управления рисками. Проводится реализация процесса нечеткого моделирования базы правил посредством разработанной СППР ModelingFuzzySet. 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, система поддержки принятия решений

### Введение

Процесс внедрения информационных технологий и средств вычислительной техники в производство и управление современных организаций является эффективным инструментом повышения производительности труда. Однако существующие и проектируемые информационные инфраструктуры организаций и предприятий часто приобретают неструктурированный характер, что способствует неконтролируемому росту уязвимостей и риску информационной безопасности в целом.

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

В целях обеспечения ИБ 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 политикой информационной безопасности. Меры защиты программно-технического уровня реализуются с помощью соответствующих средств и методов защиты информации [2].

Экономический эффект от внедрения СОИБ проявляется в виде снижения возможного матери-

ального, 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 работе [3] рассматривается риск как фактор, сущность или элемент, представляющий опасность для ИБ организации, величина которой не определена.

Недостатками существующих подходов к анализу и управлению рисками является отсутствие методологической основы для интегрального анализа качественных и количественных факторов рисков [4].

Для устранения вышеперечисленных недостатков предлагается использовать нечеткие модели, которые являются эффективным инструментом, в тех случаях, когда [5]:

- 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.

Данные доводы обуславливают целесообразность применения нечетких моделей [5, 6] при оценке состояния системы обеспечения информационной безопасности организации, которые позволяют использовать общеизвестный лингвистический подход. Оценка компонентов СОИБ проводится терминами *средний уровень программно-аппаратной защиты, высокий уровень организационной защиты, низкая рыночная ценность информационного ресурса* и др., т. е. в тех случаях, когда ИТ-менеджерам сложно придать им точную (объективную) количественную оценку и описать с помощью математического языка. При таком подходе характеристики системы целесообразно рассматривать с точки зрения теории нечетких множеств как лингвистические переменные. Применение методов получения оценок рисков на основе нечеткой логики позволяет 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 [7].

В работах [8, 9] описана нечеткая производственная модель (НПМ), которая позволяет снять ограничения на число учитываемых входных переменных и интегрировать как качественные, так и количественные подходы к оценке рисков. В НПМ определены семь входных лингвистических переменных, характеризующих факторы риска, и четыре выходных лингвистических переменных, характеризующих риски различных областей ИБ. Модель содержит четыре базы правил и позволяет проводить лингвистический анализ рисков, которые несут потенциальные угрозы и ущерб организации, а также выявлять приоритеты рисков (очень высокий, высокий, средний, низкий, очень низкий), которые важны для ИТ-менеджмента информационной структуры предприятия.

На рис. 1 приведена диаграмма вариантов использования (Use Cases), которая охватывает функциональные требования к СППР управления рисками информационной безопасности организации, поддерживающей нечеткие модели.

Лицо принимающее решение (ЛПР), ИТ-менеджер, задействует вариант использования (ВИ) "Формирование модели анализа" при оценке риска, который включает ВИ "Ввод факторов риска" и "Формирование базы правил". Далее посылается сообщение на выполнение ВИ "Задание цели анализа". Цель анализа определяет необходимые входные факторы риска и базу правил, которые должен ввести ИТ-менеджер. База правил и база фактов (рабочая область) определяют возможность выполнения ВИ "Инициировать нечеткий вывод", который вычисляет функцию принадлежности лингвистической переменной, характеризующей показатель риска. Вариант использования "Выполнить оценку риска" выполняется по сигналу от ИТ-менеджера и использует ВИ "Инициировать нечеткий вывод".

На рис. 2 приведена общая схема взаимодействия компонентов СППР.

Система электронной обработки данных (СЭОД) имеет большой набор источников данных, включая внешние источники, об объекте управления, который приводится к единому формату и согласовыва-

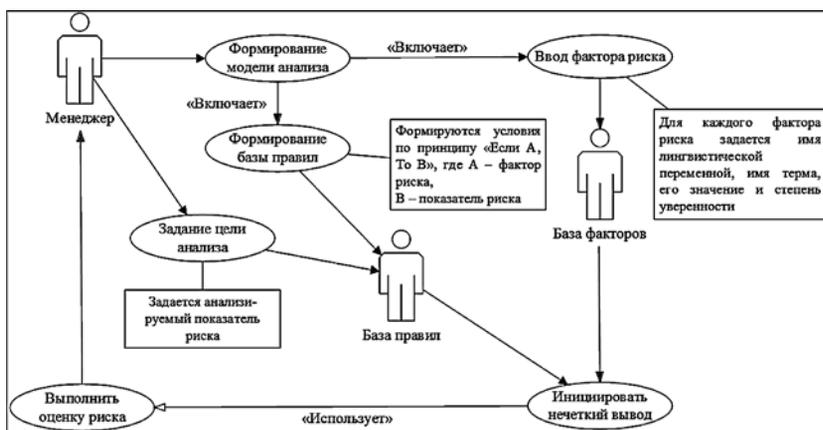


Рис. 1. Диаграмма Use Cases

### Постановка задачи для инструментария управления рисками

Автоматизация процесса анализа рисков посредством применения систем поддержки принятия решений (СППР) повышает эффективность работы ИТ-менеджера. Однако существующие программные пакеты анализа и оценки рисков не обладают возможностями построения нечетких производственных сетей и интегрального анализа качественных и количественных факторов риска [3].



Рис. 2. Схема компонентов СППР

Обозначение лингвистических переменных

Обозначение в модели	Наименование лингвистической переменной
ЛП01	Программно-аппаратный уровень защиты
ЛП02	Уровень организационной защиты
ЛП03	Уровень правовой защиты
ЛП04	Риск снижения эффективности защиты
ЛП05	Мотивация источника угроз
ЛП06	Возможности источника угроз
ЛП07	Риск возникновения потенциальных угроз
ЛП08	Рыночная ценность информационного ресурса
ЛП09	Объем данных в информационном ресурсе организации
ЛП10	Риск материального ущерба
ЛП11	Риск ИБ организации

ется до минимально требуемого уровня обобщения для расчета поставленной задачи с помощью математических моделей в подсистеме данных СППР.

Подсистема моделей включает собрание математических и аналитических моделей, которые применяются для моделирования и анализа поставленной задачи.

Система управления интерфейсом обеспечивает простое взаимодействие между пользователем, подсистемой данных и моделями, а также обеспечивает проведение анализа и моделирования проблемы для помощи в принятии управленческих решений [11].

В работе [5] описывается процесс нечеткого моделирования базы правил НПМ оценки рисков ИБ организации посредством применения специализированного пакета Fuzzy Logic Toolbox программного средства MATLAB и реализацией нечеткого вывода на основе алгоритма Мамдани (Mamdani) [12].

Используемый пакет является достаточно универсальным, однако для реализации нечеткой продукционной сети, ориентированной на оценку рисков ИБ, не обеспечивает требуемой функциональности, так как имеет ограничения по числу входных переменных для баз правил и характеризуется ограниченными возможностями по организации проведения интерактивного имитационного эксперимента при оценке рисков по схеме "Если...То...".

Таким образом, вышеприведенные ограничения программных пакетов побудили выполнить собственную разработку системы поддержки принятия решений анализа рисков на базе нечетких продукционных сетей, которая позволит получить как качественные, так и количественные оценки.

### Применение разработанной СППР для построения НПМ

Для реализации процесса нечеткого моделирования рисков ИБ организации посредством разработанной СППР ModelingFuzzySet [13] IT-менеджеру необходимо выполнить следующие действия.

**Шаг 1.** Сформировать нечеткую продукционную модель оценки рисков с помощью дизайнера модели. Формирование модели предполагает задание лингвистических переменных (ЛПхх), формализующих факторы и показатели рисков ИБ, а также базы нечетких продукционных правил (БПхх). IT-менеджер может использовать предложенную НПМ (рис. 3, см. третью сторону обложки), либо провести модификацию модели, определяя факторы и показатели риска, актуальные для конкретной организации, а также изменить правила нечеткого вывода.

Обозначения лингвистических переменных, используемых в сформированной НПМ, представлены в табл. 1.

**Шаг 2. Фазификация** — введение нечеткости. На этом шаге необходимо задать функции принадлежности для терм-множеств входных и выходных

лингвистических переменных. Программное средство ModelingFuzzySet обеспечивает формирование функций принадлежности терм-множеств различных видов: треугольные, трапециевидные, Z-, S- и П-образные.

Для входной переменной ЛП01 терм-множество состоит из трех термов  $T = \{\text{Низкий (Н)}, \text{Средний (С)}, \text{Высокий (В)}\}$ , которые характеризуют низкий, средний и высокий уровни программно-аппаратной защиты организации. Функции принадлежности для входной переменной ЛП01 являются трапециевидными. В общем случае трапециевидная функция принадлежности имеет следующий вид:

$$\mu_T(x, a, b, c, d) = \begin{cases} 0, & x \leq a; \\ \frac{x-a}{b-a}, & a \leq x \leq b; \\ 1, & b \leq x \leq c; \\ \frac{d-x}{d-c}, & c \leq x \leq d; \\ 0, & d \leq x, \end{cases} \quad (1)$$

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

С учетом формулы (1) функции принадлежности нечетких терм-множеств лингвистической переменной "Программно-аппаратный уровень защиты" будут иметь следующий вид:

$$\begin{aligned} \mu_{\Delta}^{\text{Н}}(x; 0; 0; 0,15; 0,4), \quad \mu_{\Delta}^{\text{С}}(x; 0,2; 0,4; 0,6; 0,8), \\ \mu_{\Delta}^{\text{В}}(x; 0,6; 0,85; 1,0; 1,0). \end{aligned}$$

На рис. 4 (см. третью сторону обложки) приведены графики функций принадлежности терм-множеств лингвистической переменной ЛП01 — "Программно-аппаратный уровень защиты".

Для входной переменной ЛПО2 терм-множество состоит из трех термов  $T = \{H, C, B\}$ , функции принадлежности которых являются треугольными. В общем случае треугольная функция принадлежности имеет следующий вид:

$$\mu_{\Delta}(x, a, b, c) = \begin{cases} 0, & x \leq a; \\ \frac{x-a}{b-a}, & a \leq x \leq b; \\ \frac{c-x}{c-b}, & b \leq x \leq c; \\ 0, & c \leq x, \end{cases}$$

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

С учетом формулы (2) функции принадлежности нечетких терм-множеств лингвистической переменной "Уровень организационной защиты" будут иметь следующий вид:

$$\mu_{\Delta}^H(x; 0; 0; 0,4), \mu_{\Delta}^C(x; 0,2; 0,5; 0,8), \\ \mu_{\Delta}^B(x; 0,6; 1,0; 1,0).$$

На рис. 5 (см. третью сторону обложки) приведены графики функций принадлежности терм-множеств лингвистической переменной ЛПО2 — "Уровень организационной защиты".

Для входной переменной ЛПО3 терм-множество состоит из трех термов  $T = \{H, C, B\}$ , функции принадлежности которых являются трапециевидными.

С учетом формулы (1) функции принадлежности нечетких терм-множеств лингвистической переменной "Уровень правовой 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. 6 (см. четвертую сторону обложки) приведены графики функций принадлежности терм-множеств лингвистической переменной ЛПО3 — "Уровень правовой защиты".

Для выходной переменной ЛПО4 (лингвистическая переменная "Риск снижения эффективности защиты") терм-множество состоит из пяти термов:  $T = \{\text{Очень низкая очевидность риска (ОНОР)}; \text{Низкая очевидность риска (НОР)}; \text{Средняя очевидность риска (СОР)}; \text{Высокая очевидность риска (ВОР)}; \text{Очень высокая очевидность риска (ОВОР)}\}$ . Функции принадлежности лингвистических переменных являются трапециевидными.

С учетом формулы (1) функции принадлежности нечетких терм-множеств лингвистической пе-

ременной "Риск снижения эффективности защиты" будут иметь следующий вид:

$$\mu_{\Delta}^{\text{ОНОР}}(x; 0; 0; 0,1; 0,25), \\ \mu_{\Delta}^{\text{НОР}}(x; 0,1; 0,25; 0,35; 0,5), \\ \mu_{\Delta}^{\text{СОР}}(x; 0,3; 0,45; 0,55; 0,7), \\ \mu_{\Delta}^{\text{ВОР}}(x; 0,5; 0,65; 0,75; 0,9), \\ \mu_{\Delta}^{\text{ОВОР}}(x; 0,75; 0,9; 1,0; 1,0).$$

На рис. 7 (см. четвертую сторону обложки) приведены графики функций принадлежности терм-множеств лингвистической переменной ЛПО4 — "Риск снижения эффективности защиты".

Аналогичным образом задаются функции принадлежности для других лингвистических переменных.

**Шаг 3. Задание нечетких правил.** Правила модели формируются на основе общих закономерностей поведения исследуемой системы и позволяют "вложить" в механизм вывода логическую модель прикладного уровня. С учетом ограничений алгоритма Мамдани модифицируем базу правил БПО1 в вид, приведенный на рис. 8 (см. четвертую сторону обложки). Также в процессе формирования нечетких правил модели ИТ-менеджер задает уровень влияния показателя риска на систему информационной безопасности организации, который используется для оценки возможного ущерба при возникновении данного рискованного события.

В алгоритме Мамдани для агрегирования степени истинности предпосылок используем  $T$ -норму и  $\min$ -конъюнкцию:

$$T(\mu_A(x), \mu_B(x)) = \min(\mu_A(x), \mu_B(x)).$$

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

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

**Шаг 4.** Аккумуляция заключения по всем правилам проведено с применением операции  $\max$ -дизъюнкции. При дефазификации использован метод центра тяжести для дискретного множества значений функций принадлежности:

$$y' = \frac{r=1}{Y_{\max}} \frac{\sum_{r=1}^{Y_{\max}} y_r \mu_{B'}(y_r)}{\sum_{r=1}^{Y_{\max}} \mu_{B'}(y_r)},$$

где  $Y_{\max}$  — число элементов  $y_r$  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.

### Использование модели оценки рисков ИБ организации

В процессе идентификации рисков ИТ-менеджерами были определены уровни программно-аппаратной, организационной и правовой защиты

Рис. 9. Форма ввода значения лингвистической переменной ЛП01

Рис. 10. Форма ввода значения лингвистической переменной ЛП02

Рис. 11. Форма ввода значения лингвистической переменной ЛП03

паратной, организационной и правовой защиты организации. Данная информация будет использоваться для моделирования показателя риска "Снижение эффективности защиты" в разработанной СППР ModelingFuzzySet.

Значение входной лингвистической переменной ЛП01 — "Программно-аппаратный уровень защиты" соответствует терму В — "полностью соответствует уровню конфиденциальности информации" с уровнем уверенности  $\mu_{ЛП01}^В = 0,7\mu$  (рис. 9).

Значение входной лингвистической переменной ЛП02 — "Уровень организационной защиты" соответствует терму Н — "слабое планирование и отсутствие мониторинга уязвимостей" с уровнем уверенности  $\mu_{ЛП02}^Н = 0,8\mu$  (рис. 10).

Значение входной лингвистической переменной ЛП03 — "Уровень правовой защиты" соответствует терму С — "документация имеется, но недостаточно детальная" с уровнем уверенности  $\mu_{ЛП03}^С = 0,7\mu$  (рис. 11).

По заданным исходным условиям активизируется правило 12 (см. рис. 8), которое определяет значение выходной лингвистической переменной ЛП04 — "Риск снижения эффективности защиты", равное СОР — "Средняя очевидность риска" с уровнем уверенности  $\mu_{ЛП04}^{СОР} = 0,7\mu$  и значением показателя риска 50 (рис. 12). Реализация нечеткого вывода определяется на основе алгоритма Мамдани (Mamdani) [14].

Используя результаты моделирования, ИТ-менеджер может определить сумму возможного ущерба по табл. 2.

Таким образом, снижение эффективности защиты предприятия может привести к возможному ущербу в размере \$500 тыс.

Для получения интегральной оценки риска ИБ организации необходимо провести моделирование всех выходных лингвистических переменных первого уровня, затем программное средство рассчитает значение выходной лингвистической переменной ЛП11 — "Риск ИБ организации", используя полученные ранее оценки в качестве входных данных. Результаты нечеткого моделирования выход-

Таблица 2

#### Шкала оценки последствий возникновения риска

Ранг показателя риска	Значение показателя риска				
	0...20	21...40	41...60	61...80	81...100
1	\$100	\$300	\$500	\$700	\$900
2	\$1 тыс.	\$3 тыс.	\$5 тыс.	\$7 тыс.	\$9 тыс.
3	\$10 тыс.	\$30 тыс.	\$50 тыс.	\$70 тыс.	\$90 тыс.
4	\$100 тыс.	\$300 тыс.	\$500 тыс.	\$700 тыс.	\$900 тыс.
5	\$1 млн	\$3 млн	\$5 млн	\$7 млн	\$10 млн



Рис. 12. Результат нечеткого моделирования ЛП04

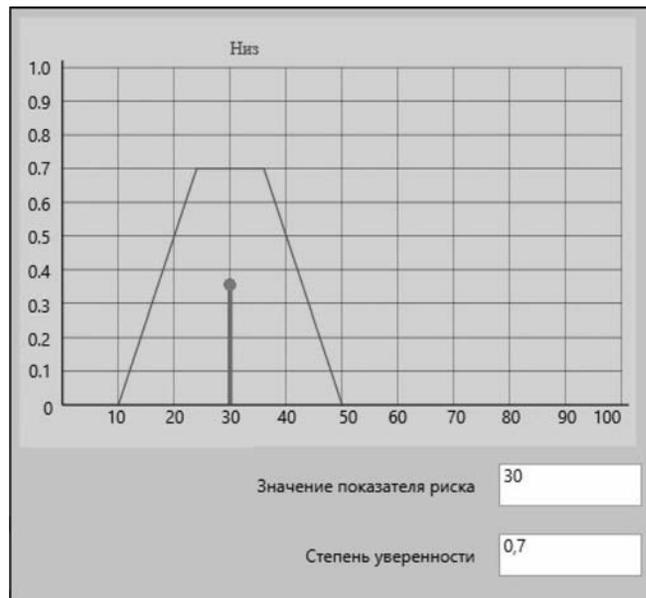


Рис. 13. Результат нечеткого моделирования интегральной ЛП11

ной лингвистической переменной ЛП07 — "Риск возникновения потенциальных угроз" показали  $\text{НОР}$  — "Высокая очевидность риска" с уровнем уверенности  $\mu_{\text{ЛП07}} = 0,8\mu$  и значением показателя риска 70. Результаты нечеткого моделирования выходной лингвистической переменной ЛП10 — "Риск материального ущерба" показали  $\text{НОР}$  — "Низкая очевидность риска" с уровнем уверенности  $\mu_{\text{ЛП10}}^{\text{НОР}} = 1,0\mu$  и значением показателя риска 30. Результаты нечеткого моделирования интегральной выходной лингвистической переменной ЛП11 — "Риск ИБ организации" показали  $\text{НОР}$  — "Низкая очевидность риска" с уровнем уверенности  $\mu_{\text{ЛП11}}^{\text{НОР}} = 0,7\mu$  и значением показателя риска 30 (рис. 13).

Таким образом, оценка показывает, что уровень риска ИБ организации позволяет работать ИТ-менеджерам в нормальном режиме, но имеются предпосылки нарушения системы обеспечения информационной безопасности (СОИБ). Поэтому необходимо разработать и применить план по поиску и устранению уязвимостей СОИБ, иначе ущерб организации может составить около \$3 млн.

### Заключение

Разработанная система поддержки принятия решений позволяет строить многоуровневые нечеткие производственные модели оценки рисков, а используемый механизм нечеткого вывода позволяет получить числовое значение риска, лингвистическое описание степени риска, а также степень уверенности эксперта в возникновении рисковом со-

бытия. Полученные данные помогают ИТ-менеджерам выявить приоритеты рисков (очень высокий, высокий, средний, низкий, очень низкий) и выработать план мероприятий по снижению влияния наиболее опасных угроз на ИБ организации.

Механизм получения оценок риска на основе нечеткой логики 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.

### Список литературы

1. **Рекомендации** по стандартизации "Информационные технологии. Основные термины и определения в области технической защиты информации" (Р 50.1.053—2005).
2. **Национальный стандарт РФ** "Информационная технология. Практические правила управления информационной безопасностью" (ГОСТ Р ИСО/МЭК 17799—2005).
3. **Симонов С. В.** Анализ рисков, управление рисками // Информационный бюллетень "Jet Info". 1999. № 1 (68).
4. **Долженко А. И., Глушенко С. А.** Анализ предпосылок создания СППР управления рисками проектов информационных систем // Информационные системы, экономика, управление трудом и производством. Ученые записки. Вып. 12. Ростов-на-Дону: РГЭУ (РИНХ). 2011. № 12.
5. **Борисов В. В., Круглов А. С. и Федулов А. С.** Нечеткие модели и сети. М.: Горячая линия — Телеком, 2007. 284 с.
6. **Заде Л. А.** Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: Мир, 1976. 168 с.
7. **Долженко А. И.** Модель анализа риска потребительского качества проектов экономических информационных систем // Вестник Северо-Кавказского государственного технического университета. 2009. № 1 (18). С. 129—134.
8. **Глушенко С. А.** Нечеткая производственная модель оценки рисков информационной безопасности организации // Вопросы экономики и права: Сборник статей аспирантов и соиска-

телей ученой степени кандидата наук. Ростов-на-Дону: РГЭУ (РИНХ), 2013.

9. **Глушенко С. А.** Применение системы matlab для оценки рисков информационной безопасности организации // БИЗНЕС-ИНФОРМАТИКА. 2013. № 4 (24).

10. **Глушенко С. А.** Анализ функциональной полноты программных систем управления рисками // Вестник РГЭУ (РИНХ). 2012. № 2 (38).

11. **Трахтенгерц Э. А.** Компьютерная поддержка принятия решений: научно-практическое изд. Сер. "Информатизация России на пороге XXI века". М.: СИНТЕГ, 1998. 376 с.

12. **Леоненков А. В.** Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2005. 736 с.

13. **Долженко А. И.** Система моделирования производственной нечеткой сети (ПРОНЕС) № 2010612952 / Долженко А. И., Глушенко С. А., Калугян К. Х., Лозина Е. Н., Чередниченко А. С. Свидетельство о государственной регистрации программы для ЭВМ. М., 25.05.2010 г.

14. **Анисимова Г. Б., Долженко А. И.** Система оценки риска потребительского качества проектов информационных систем // Вестник ИНЖЭКОНА. Сер. "Экономика". 2010. № 1 (36). С. 179—191.

**S. A. Glushenko**, Graduate Student, e-mail: www.555.sergey@mail.ru,  
**A. I. Dolzenko**, Professor, e-mail: doljenkoalex@gmail.ru,  
Rostov State Economic University (RINE), Russia, Rostov-on-Don

## Decision Support Fuzzy Modeling System of Information Security Risks

*The article explains the importance of the application of risk analysis in the management system of information security (IS) and explains the usefulness of fuzzy logic to evaluate the risk. Application of fuzzy models allows to take into account both quantitative and qualitative characteristics, as well as represent fuzzy description using fuzzy sets and linguistic variables.*

*In the article, the problem statement for risk management tools to support fuzzy models and expediency proprietary decision support system (DSS) risk analysis. The following describes the process of implementing the fuzzy rule base modeling developed by DSS ModelingFuzzySet. Mechanism for obtaining risk assessments based on the algorithm of Mamdani allows obtaining the numerical value of the risk, the linguistic description of the risk and the degree of confidence in expert risk event occurs.*

*IT-managers used the simulation results to identify priority risks (very high, high, medium, low, very low) and allowed to develop effective action plan to reduce the impact of the most dangerous threats to the information security organization.*

**Keywords:** risk, fuzzy set, term set, fuzzy production model, the linguistic variable, rule base, the membership function, decision support system

### References

1. **Рекомендации** по стандартизации "Информационные технологии. Основные термины и определения в области технической зашхиты информации" (R 50.1.053—2005).

2. **Национальный** стандарт RF "Информационная технология. Практические правила управления информационной безопасностью" (GOST R ISO/MJEK 17799—2005).

3. **Simonov S. V.** Анализ рисков, управление рисками. *Информационный бюллетень "Jet Info"*. 1999. N. 1 (68).

4. **Dolzenko A. I., Glushenko S. A.** Анализ предпосылок создания СПР управления рисками проектов информационных систем. *Информационные системы, экономика, управление трудом и производством. Ученые записки*. Вып. 12. Ростов-на-Дону: РГЭУ (РИНХ), 2011. N. 12.

5. **Borisov V. V., Kruglov A. S. i Fedulov A. S.** *Нечеткие модели и сети*. М.: Горькая линия-Телеком, 2007. 284 п.

6. **Zade L. A.** *Понятие лингвистической переменной и его применение к принятию приближенных решений*. М.: Мир, 1976. 168 п.

7. **Dolzenko A. I.** Модель анализа риска потребителя качества проектов экономических информационных систем. *Вестник Северо-Кавказского государственного технического университета*. 2009. N. 1 (18). P. 129—134.

8. **Glushenko S. A.** Nечetkaja produkcioнная model' ocenki riskov informacionnoj bezopasnosti organizacii. *Voprosy jekonomiki i prava: Sbornik statej aspirantov i soiskatelej uchenoj stepeni kandidata nauk*. Ростов-на-Дону: РГЭУ(РИНХ), 2013.

9. **Glushenko S. A.** Primenenie sistemy matlab dlja ocenki riskov informacionnoj bezopasnosti organizacii. *BIZNES—INFORMATIKA*. 2013. N. 4 (24).

10. **Glushenko S. A.** Analiz funkcional'noj polnoty programnyh sistem upravlenija riskami. *Vestnik RGEU (RINH)*. 2012. N. 2 (38).

11. **Trahtengerc Je. A.** *Komp'yuternaja podderzhka prinjatija reshenij: Nauchno-prakticheskoe izd. Ser. "Informatizacija Rossii na poroge XXI veka"*. М.: SINTEG, 1998. 376 п.

12. **Leonenkov A. V.** *Nечetkoe modelirovanie v srede MATLAB i fuzzyTECH*. SPb.: BHV-Peterburg, 2005. 736 п.

13. **Dolzenko A. I.** *Sistema modelirovanija produkcioнной nechetkoj seti (PRONES)* — № 2010612952. Dolzenko A. I., Glushenko S. A., Kalugjan, K. H., Lozina, E. N., Cherednichenko A. S. Svidetel'stvo O gosudarstvennoj registracii programmy dlja JeVM. М., 25.05.2010 g.

14. **Anisimova G. B., Dolzenko A. I.** Sistema ocenki riska potrebitel'skogo kachestva proektov informacionnyh sistem. *Vestnik INZhEKONA*. Ser. "Jekonomika". 2010. N. 1 (36). P. 179—191.