УДК: 004.056.5

Н. В. Медведев, И. И. Троицкий, В. Л. Цирлов

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ АППАРАТА ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ ПРИ АНАЛИЗЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрены вопросы применения аппарата нечетких множеств для проведения анализа риска. Предложены выражения для расчета показателей уязвимостей.

Email: vz@cnpo.ru

Ключевые слова: уязвимость, анализ риска, оценка риска, информационная безопасность.

В основе всех организационно-технических мероприятий в области информационной безопасности лежит процедура анализа рисков. Современные стандарты в этой области ориентированы на качественные способы анализа риска, главным образом по причине невозможности получения вероятностных оценок ряда классов угроз [1–9]. Однако отсутствие достоверных количественных показателей затрудняет автоматизацию процессов управления информационной безопасностью [2].

В данной работе предлагается подход, позволяющий получить простые количественные оценки анализа риска, основанные на аппарате теории нечетких множеств [12].

Анализ риска информационной безопасности обычно включает следующие этапы:

– идентификацию активов,
– определение требований по информационной безопасности,
– идентификацию угроз и уязвимостей,
– оценку угроз и уязвимостей,
– оценку риска и обработку риска.

Рассмотрим основные этапы анализа риска.

1. Идентификация активов. С использованием экспертно-документального метода путем анализа эксплуатационной документации на автоматизированных системах (АС) перечисляются материальные и нематериальные активы организации. В результате идентификации материальных и нематериальных активов, подлежащих защите в АС, должено быть сформировано множество активов $A = \left\{a_1, a_2, ..., a_{n_A}\right\}$.

2. Идентификация угроз. Для каждого из идентифицированных активов $a_\alpha \in A, \alpha = \overline{1, n_A}$ из n_α угроз формируется множество $T_{a_\alpha} = \left\{t_1, t_2, ..., t_{n_\alpha}\right\}$.

Каждую из угроз $t \in T_{a_\alpha}$ характеризуют следующие параметры:

– источник угрозы TP_1;
– предполагаемый способ реализации угрозы TP_2;
– активы, TP_3, которые являются целью нападения;
– нарушаемые свойства TP_4 безопасности активов;
– возможные последствия TP_5 реализации угрозы.

Описание параметров последовательно проводится для всего множества угроз $T = \left\{T_1, T_2, ..., T_{n_A}\right\}$.

3. Идентификация уязвимостей. Множество уязвимостей $V = \left\{V_1, V_2, ..., V_{n_V}\right\}$ формируется как подмножество $V \subseteq T$. На данном этапе отбрасываются заведомо нереализуемые угрозы, а также угрозы, выходящие за рамки политики информационной безопасности организации [1, 11].

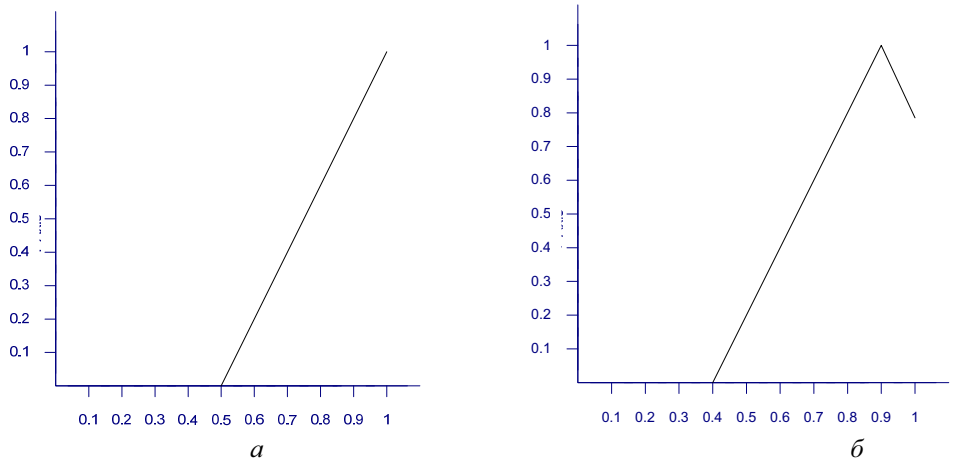
4. Оценка уязвимостей. Исходными данными для проведения анализа являются множества $V = \left\{V_1, V_2, ..., V_{n_V}\right\}$ и $(TP_i)_j$, $i = \overline{1,5}$, $j = \overline{1,n_V}$.

Для оценки критериев и весов критериев уязвимостей используются две лингвистические переменные:

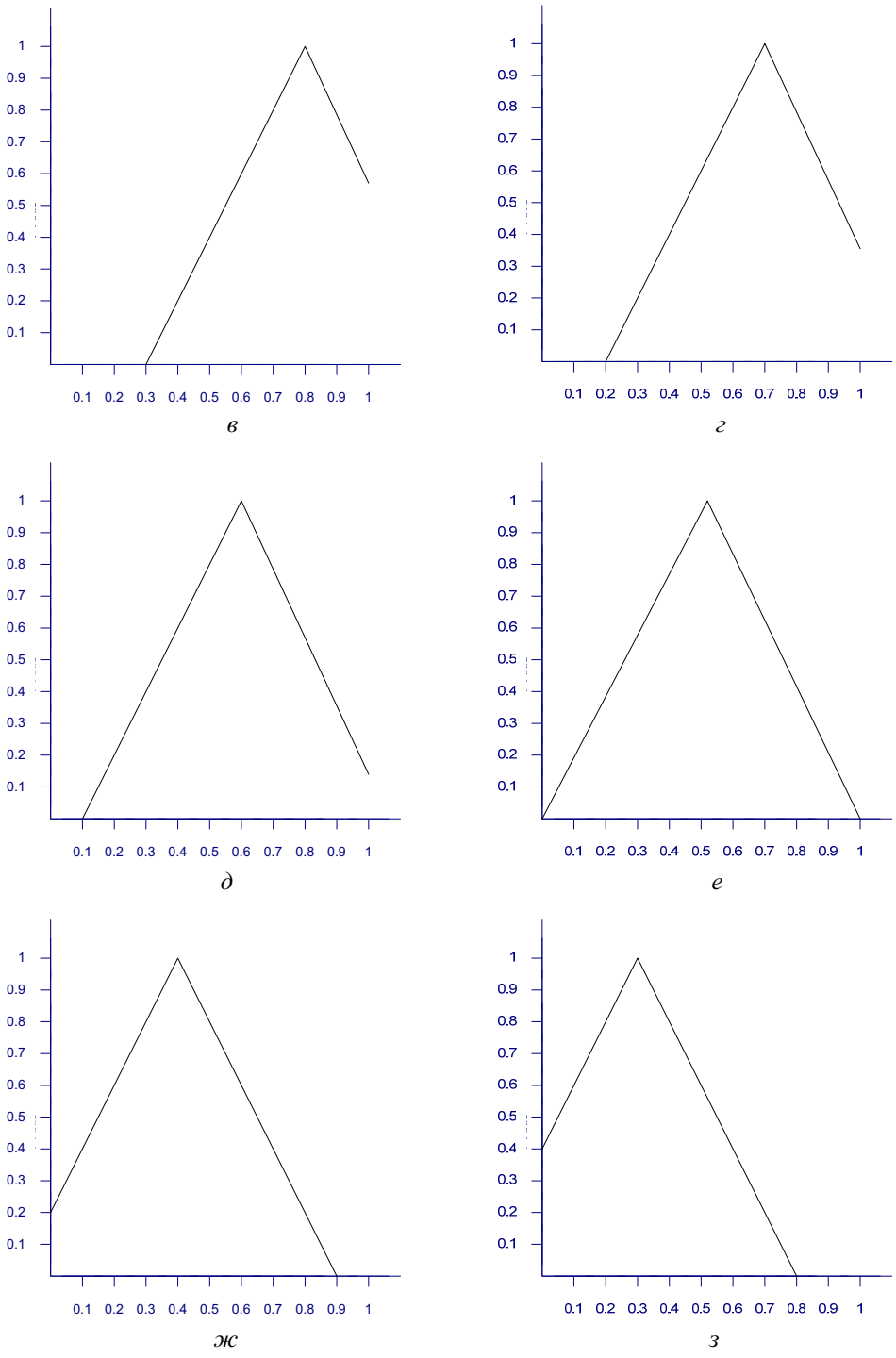
– X_1 = <ОЦЕНКА КРИТЕРИЯ УЯЗВИМОСТИ>;
– X_2 = <ВЕС КРИТЕРИЯ УЯЗВИМОСТИ>

с терм-множеством $T = T_{X_1} = T_{X_2} = < T_1, T_2, ..., T_{11} > =$ <ОЧЕНЬ ВЫСОКИЙ, ВЫСОКИЙ, ДОВОЛЬНО ВЫСОКИЙ, ОТНОСИТЕЛЬНО ВЫСОКИЙ, ВЫШЕ СРЕДНЕГО, СРЕДНИЙ, ОТНОСИТЕЛЬНО НИЗКИЙ, ДОВОЛЬНО НИЗКИЙ, НИЗКИЙ, ОЧЕНЬ НИЗКИЙ, ПРАКТИЧЕСКИ ОТСУТСТВУЕТ>.

Функции принадлежности лингвистических термов приведены на рисунке.



Функции принадлежности лингвистических термов (начало):
а — <ОЧЕНЬ ВЫСОКИЙ> (описание 0,5, 1,0, 1,5); *б* — <ВЫСОКИЙ> (0,4, 0,3, 1,4)



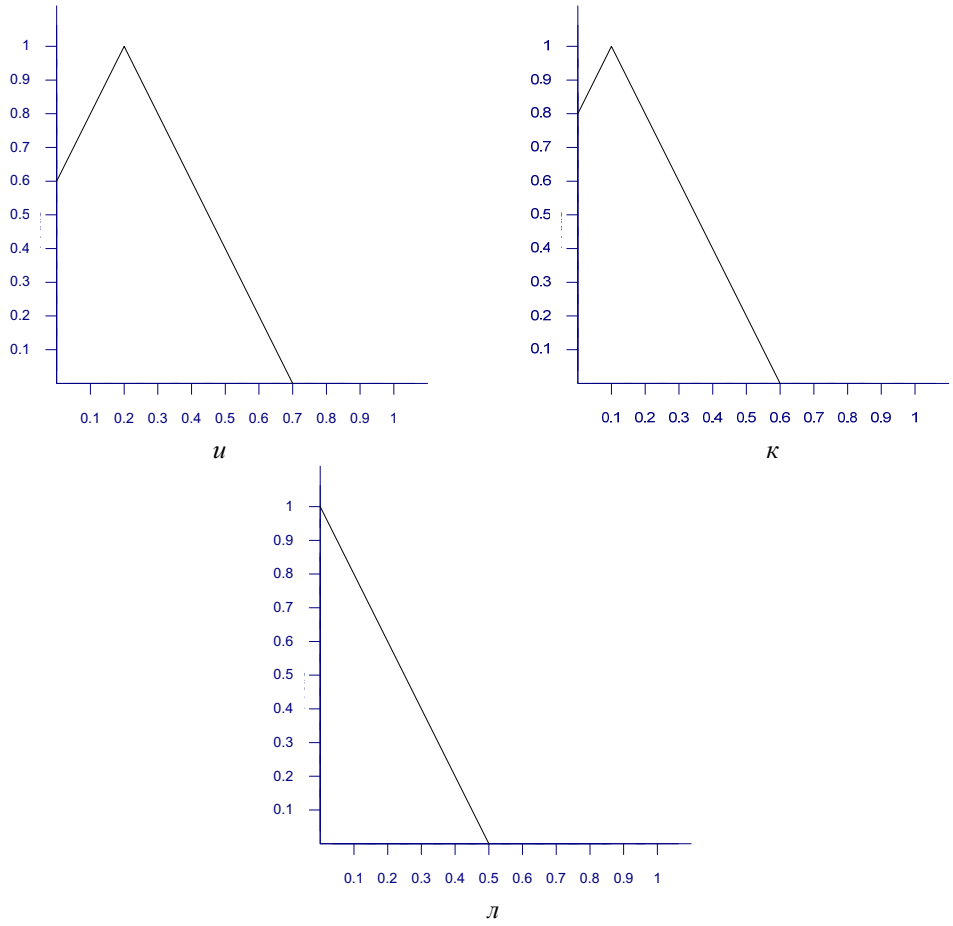
в *г*

д *е*

ж *з*

Функции принадлежности лингвистических термов (продолжение):

в — <ДОВОЛЬНО ВЫСОКИЙ> (0,3, 0,8, 1,3); *г* — <ОТНОСИТЕЛЬНО ВЫСОКИЙ> (0,2, 0,7, 1,2); *д* — <ВЫШЕ СРЕДНЕГО> (0,1, 1,6, 1,1); *е* — <СРЕДНИЙ> (0, 0,5, 1,0); *ж* — <ОТНОСИТЕЛЬНО НИЗКИЙ>; *з* — <ДОВОЛЬНО НИЗКИЙ> (–0,2, 0,3, 0,8)



Функции принадлежности лингвистических термов (окончание):
и — <НИЗКИЙ> (–0,3, 0,2, 0,7); *к* — <ОЧЕНЬ НИЗКИЙ> (–0,4, 0,1, 0,6); *л* — <ПРАКТИЧЕСКИ ОТСУТСТВУЕТ> (–0,5, 0, 0,5)

Каждая из уязвимостей $v_i \in V$ оценивается в рамках группового принятия решений с привлечением n_E экспертов по трем критериям: возможность нарушения конфиденциальности K_1; целостности K_2; доступности K_3 информации.

Оценка критерия K_i уязвимости $v_i \in V$ осуществляется экспертом E_j, $j = \overline{1, n_E}$, в качественной форме с помощью значения лингвистической переменной X, отображаемого в нечеткое число $r_{v_{iK_i}}^{E_j}$, $v_i = \overline{1, n_V}$, $E_j = \overline{1, n_E}$.

Оценка веса критерия K_i осуществляется экспертом в качественной форме с помощью значения лингвистической переменной X, отображаемого в нечеткое число $w_{K_i}^{E_j}$, $j = \overline{1, n_E}$.

Агрегирование весов $w_{K_i}^{E_j}$, и оценок $r_{v_i}^{E_j}$ осуществляется с использованием следующих соотношений:

$$w_{K_i} = \frac{w_{K_i}^1 + \ldots + w_{K_i}^{n_E}}{n_E}; \quad r_{v_{iK_i}} = \frac{r_{vK_i}^1 + \ldots + r_{v_{iK_i}}^{n_E}}{n_E}. \tag{1}$$

Нормировка весов осуществляется с использованием соотношения

$$\underline{w}_{K_i} = \frac{w_{K_i}}{w_{K_1} + w_{K_2} + w_{K_3}}, \quad K_i = \{K_1, K_2, K_3\}. \tag{2}$$

Комплексная оценка уязвимости v_i вычисляется по формуле

$$R_{v_i} = \underline{w}_{K_1} r_{v_{iK_1}} + \underline{w}_{K_2} r_{v_{iK_2}} + \underline{w}_{K_3} r_{v_{iK_3}}. \tag{3}$$

Для ранжирования уязвимостей определяется расстояние Хемминга между $R_{v_i} \forall\, v_i \in V$ и нечетким числом <ПРАКТИЧЕСКИ ОТСУТСТВУЕТ>, и полученные величины упорядочиваются в порядке возрастания.

Результатом оценки уязвимостей является перечень уязвимостей программного обеспечения АС, упорядоченный в порядке возрастания комплексного показателя, характеризующего возможность реализации угроз конфиденциальности, целостности и доступности информации.

Политикой информационной безопасности организации устанавливается максимально допустимый уровень $\overline{R_{vi}}$ комплексной оценки. Для всех уязвимостей, комплексная оценка которых $R_{vi} > \overline{R_{vi}}$, требуется принятие управленческих решений и в дальнейшем повторное проведение анализа.

Предлагаемый подход показал достаточно высокую эффективность при аудите систем менеджмента информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Марков А. С., Миронов С. В., Цирлов В. Л. Разработка политики безопасности организации в свете новейшей нормативной базы // Защита информации. Конфидент. 2004. – № 2. – С. 20–28.
2. Марков А. С., Цирлов В. Л. Управление рисками — нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. – № 8. – С. 63–67.
3. Марков А. С., Цирлов В. Л. BS 7799-3:2006 и состояние отечественной нормативной базы по управлению рисками информационной безопасности // Материалы Конференции по стандартизации информационных технологий и интероперабельности SITOP-2007 (Москва, 2–3 октября 2007 г.). 2007. – С. 60–67.

4. BS 7799-3:2006. Information security management systems. P. 3: Guidelines for information security risk management. London: BSI, 2006. – 57 p.
5. ISO/IEC 13335-1:2004. Concepts and models for information and communications technology security management. Berlin: ISO Secretariat, 2004. – 32 p.
6. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management. Berlin: ISO Secretariat, 2005. – 104 p.
7. ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements. Berlin: ISO Secretariat, 2005. – 48 p.
8. ISO/IEC TR 13335-3:1998. Information technology — Guidelines for the management of IT Security – P. 3: Techniques for the management of IT security. Berlin: ISO Secretariat, 2004. – 26 p.
9. Risk Management Guide for Information technology Systems. Washington: NIST, 2002. – 55 p.
10. Chen S.-M. Evaluating weapon systems using ranking fuzzy numbers // Fuzzy Sets and Systems. 1999. – Vol. 107(1). – P. 25–35.
11. Медведев Н. В., Квасов П. М., Цирлов В. Л. Стандарты и политика информационной безопасности автоматизированных систем // Вестник Московского государственного технического университета им. Н.Э. Баумана. Сер. Приборостроение. 2010. – № 1. – С. 103–111.

Статья поступила в редакцию 19.10.2011