УДК 004.056

Р.Муратхан[1], Д.Ж.Сатыбалдина[2]

[1]*Карагандинский государственный университет им. Е.А.Букетова;*
[2]*Евразийский национальный университет им. Л.Н.Гумилева, Астана*
(E-mail: muratkhan_r@enu.kz)

Оценка риска информационной безопасности с помощью теории нечетких множеств

Риск нарушения информационной безопасности современной организации — это многомерное сложное понятие, которое в том числе включает набор взаимосвязанных переменных. Часто значения факторов риска не могут быть точно определены. Поэтому оценка риска информационной безопасности может быть определена как нечеткая проблема. Данная статья описывает методы реализации оценки рисков информационной безопасности в сочетании с теорией нечетких мер.

Ключевые слова: риск, теория нечетких множеств, метод оценки рисков.

Введение. Общепринятым подходом к оценке работоспособности автоматизированных систем (АС) является моделирование, основанное на создании и исследовании моделей, описывающих функционирование этих систем. Применение подобных моделей позволяет проанализировать и оптимизировать процессы сбора, хранения и обработки информации, а также выбрать технологии защиты данных [1]. Математическая модель системы, отражая физическую суть ее процессов функционирования, позволяет адекватно оценить различные характеристики АС. Однако классические методы моделирования требуют подачи на вход модели чётких числовых значений.

Процесс анализа защищенности автоматизированных систем отличается тем, что при оценке рисков информационной безопасности (ИБ) в качестве исходных данных часто используются нечёткие значения в виде экспертных оценок. Это обусловливает необходимость применения нечётких моделей, основное преимущество которых связано с возможностью использования для их разработки значительно меньших объёмов информации о моделируемой системе, по сравнению с традиционными математическими моделями. При этом информация может носить приближённый, нечёткий характер, что является эффективным для такого сложного и неоднозначного процесса, как оценка рисков в автоматизированных системах [2–4].

Целью данной работы является создание модели, позволяющей оценивать риски ИБ в условиях неполных и неоднозначных данных об их составляющих.

1 Выбор типа модели. Для разработки нечеткой модели, пригодной для оценки рисков ИБ, необходимо проанализировать возможности существующих моделей, основанных на теории нечётких множеств.

Под нечётким множеством A, определённым на X, понимается совокупность $A=\left\{\left(x,\mu_A(x)\right)\middle| x\in X\right\}$, где X — область значений, а $\mu_A(x)$ — функция принадлежности, характеризующая степень принадлежности элемента x к нечёткому множеству A. При этом выделяют три случая:

1) $\mu_A(x)=1$ — полная принадлежность элемента x нечёткому множеству A, т.е. $A \in x$;

2) $\mu_A(x)=0$ — отсутствие принадлежности элемента x нечёткому множеству A, т.е. $A \notin x$;

3) $0<\mu_A(x)<1$ — частичная принадлежность элемента x нечёткому множеству A.

Как правило, нечёткие модели разрабатываются для систем нечёткого управления, поэтому типичная структура состоит из 4 блоков [5]:

1) формализация лингвистических переменных;

2) блок фазификации (занимается вычислением степени принадлежности чётких входных параметров модели входным нечётким множествам);

3) блок вывода (основным элементом является база правил – набор логических правил, которые задают причинно-следственные отношения между входными и выходными величинами);

4) блок дефазификации (вычисление чёткого выходного значения на основе результирующей функции принадлежности, которая рассчитывается механизмом вывода в блоке вывода).

Различные типы нечетких моделей отличаются способом реализации указанных блоков.

В настоящее время наиболее часто используемым типом нечёткой модели является модель Мамдани [6]. В рамках метода Мамдани моделируемая система рассматривается как «чёрный ящик», характеризующийся недостаточностью информации о происходящих внутри него физических явлениях. Модель выполняет такое отображение входов (вектор X) в выход Y, которое обеспечивает как можно более точную аппроксимацию реальной системы (например, в смысле средней абсолютной погрешности). Указанное отображение предполагает существование некоторой геометрической поверхности (поверхности отображения) в пространстве, задаваемом декартовым произведением $X \times Y$. Модель Мамдани представляет собой множество правил:

ЕСЛИ (x есть A), ТО (y есть B),

где A, B — нечёткие множества. Каждое правило задаёт в указанном пространстве некоторую нечёткую точку. На основе множества нечётких точек формируется нечёткий график, механизм интерполяции между точками в котором зависит от используемого аппарата нечёткой логики.

Были разработаны и другие типы нечётких моделей, среди которых наиболее важными являются модели Такаги-Сугено-Канга (TSK-модели). От моделей Мамдани модели Такаги-Сугено-Канга отличаются формой правил [7]. В случае TSK-модели правила имеют вид:

ЕСЛИ (x есть A), ТО ($y = f(x)$),

где вместо нечёткого множества заключение каждого правила содержит функцию $f(x)$, которая может быть нелинейной, хотя обычно используются линейные функции вида $y = ax + b$.

Поскольку в модели Такаги-Сугено-Канга получаемое заключение имеет более сложное математическое представление и обладает меньшей обозримостью, чем заключение в модели Мамдани, то для оценки рисков ИБ в большей степени подходит модель Мамдани, так как в данном процессе обозримость общей картины состояния рисков важнее, чем точность значения.

2 Формализация лингвистических переменных. Чтобы использовать модель Мамдани для оценки рисков ИБ, необходимо определить, какие данные следует подавать на вход системы. Из определения риска ИБ следует, что величина риска R есть функция от потенциально возможного ущерба (ценность информации, ресурса или актива) AV, вероятность реализации угрозы ИБ $P(T)$ и мера уязвимости актива к угрозе V

$$R = V * P(T) * AV.$$

Таким образом, входными факторами будут служить экспертные оценки трех нечётких переменных («вероятность реализации угрозы», «ценность актива», «мера уязвимости актива к угрозе»), описанных лингвистическими терм-множествами: {очень низкий, низкий, средний, высокий, очень высокий} (табл. 1).

В результате на выходе системы будет получена оценка уровня риска информационной безопасности, которую можно описать расширенным лингвистическим термом-множеством, например: {пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный, выше среднего, высокий, очень высокий, критический}.

Таблица 1

Уровни шкалы при оценке угроз, ущерба и уязвимостей

Уровни шкалы	Вероятность реализации угрозы ($P(T)$)	Ценность актива (AV)	Мера уязвимости актива к угрозе (V)	Значение
1	2	3	4	5
Очень низкий	Событие практически никогда не происходит	Незначительные потери материальных средств и ресурсов, которые быстро восполняются, или незначительное влияние на репутацию	Уязвимость, которой можно пренебречь	(0; 0; 0,25)
Низкий	Событие случается редко	Более заметные потери материальных активов, более существенное влияние на репутацию или ущемление интересов	Незначительная уязвимость, которую легко устранить	(0; 0,25; 0,5)
Средний	Событие вполне возможно при определённом стечении обстоятельств	Достаточные потери материальных активов или ресурсов или достаточный урон репутации и интересам	Умеренная уязвимость	(0,25; 0,5; 0,75)

1	2	3	4	5
Высокий	Скорее всего, событие произойдёт при организации атаки	Значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности	Серьёзная уязвимость, ликвидация которой возможна, но связана со значительными затратами	(0,5; 0,75; 1)
Очень высокий	Событие, вероятнее всего, произойдёт при организации атаки	Разрушительные последствия и невозможность ведения деятельности	Критическая уязвимость, которая ставит под сомнение возможность её устранения	(0,75;1; 1)

В этом случае шкала измерения уровня информационных рисков будет выглядеть следующим образом (табл. 2).

3 Фазификация. Рассмотрим пример применения модели Мамдани для оценки рисков ИБ. Для автоматизации процесса получения четких значений «риска информационной безопасности» по алгоритму нечеткого вывода Мамдани воспользуемся пакетом Fuzzy Logic Toolbox системы разработки MATLAB. В этом исследовании функции принадлежности лингвистических условий характеризуются треугольными нечеткими числами, поскольку они очень часто используются в приложениях, таких как нечеткие контроллеры, и в организаторском принятии решений, бизнесе и финансах, общественных науках и т.д. [8]. Функции принадлежности четырех нечетких множеств (вероятность ценность актива, реализации угрозы, мера уязвимости актива к угрозе и риск ИБ) приведены соответственно на рисунках 1–4.

Таблица 2

Уровни шкалы риска ИБ

Уровни шкалы	Описание риска	Значение
Пренебрежимо низкий	Риском можно пренебречь	(0; 0; 0,125)
Очень низкий	Необходимо определить, существует ли необходимость в корректирующих действиях или есть возможность принять этот риск	(0; 0,125; 0,25)
Низкий	Уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы	(0,125; 0,25; 0,375)
Ниже среднего	Необходимо разработать и применить план корректирующих действий в течение приемлемого периода времени	(0,25; 0,375; 0,5)
Умеренный	Уровень риска не позволяет стабильно работать, имеется настоятельная необходимость в корректирующих действиях, изменяющих режим работы в сторону уменьшения риска	(0,375; 0,5; 0,625)
Выше среднего	Система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее	(0,5; 0,625; 0,75)
Высокий	Уровень риска такой, что бизнес-процессы находятся в неустойчивом состоянии	(0,625; 0,75; 0,875)
Очень высокий	Необходимо незамедлительно принять меры по уменьшению риска	(0,75; 0,875; 1)
Критический	Уровень риска очень большой и является недопустимым для организации, что требует прекращения эксплуатации системы и принятия радикальных мер по уменьшению риска	(0,875; 1; 1)

Механизм оценивания рисков по существу является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин (т.е. AV, $P(T)$, V) и выходных величин (т.е. R). В простейшем случае это «табличная» логика, в общем — более сложная логика, отражающая реальные взаимосвязи, которые могут быть формализованы с помощью продукционных правил вида «Если ..., то …». В нашем исследовании использованы следующие продукционные правила (рис. 5).

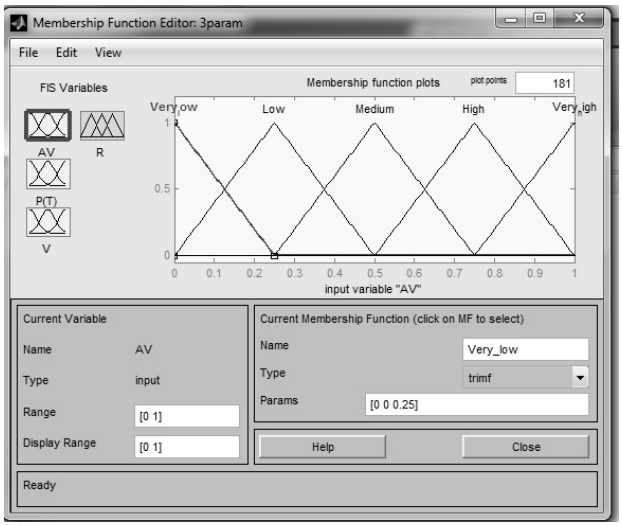

Рисунок 1. Функция принадлежности лингвистической переменной «Ценность актива»

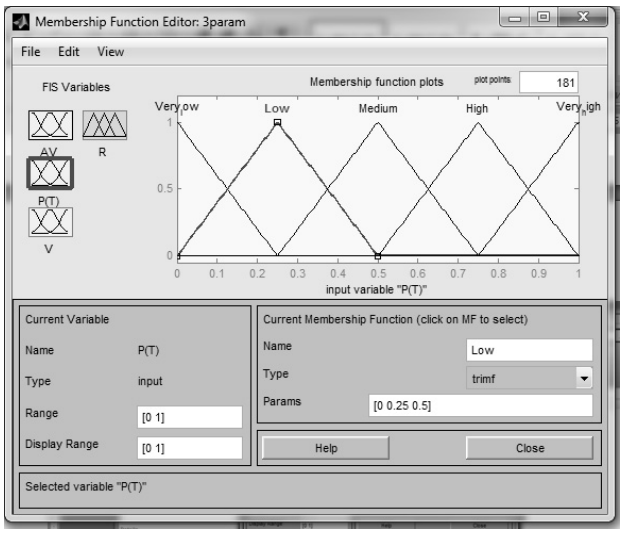

Рисунок 2. Функция принадлежности лингвистической переменной «Вероятность реализации угрозы»

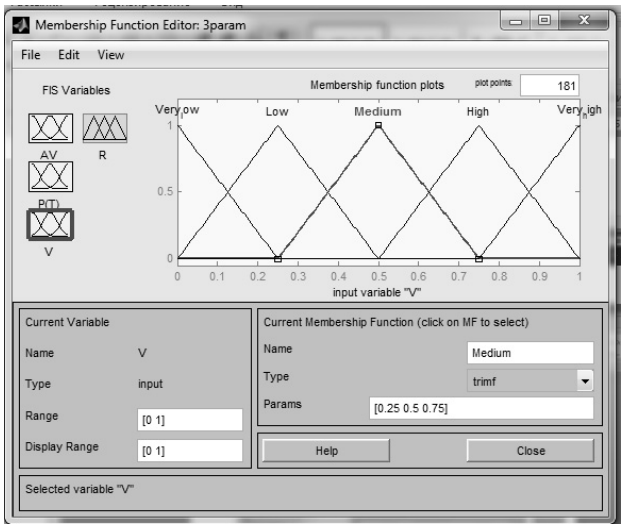

Рисунок 3. Функция принадлежности лингвистической переменной «Мера уязвимости актива к угрозе»

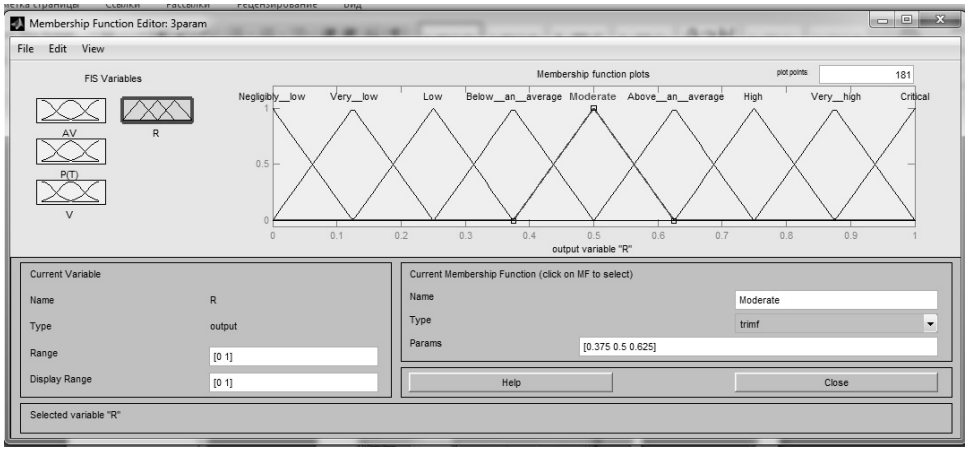

Рисунок 4. Функция принадлежности лингвистической переменной «Риск ИБ»

Рисунок 5. Фрагмент базы знаний (продукционные правила)

4 Дефазификация. Дефазификацией (*defuzzification*) называется процедура преобразования нечеткого множества в четкое число.

В теории нечетких множеств процедура дефазификации аналогична нахождению характеристик положения (математического ожидания, моды, медианы) случайных величин в теории вероятности. Простейшим способом выполнения процедуры дефазификации является выбор четкого числа, соответствующего максимуму функции принадлежности.

Дефазификация нечеткого множества $\tilde{A} = \int\limits_{[\underline{u},\overline{u}]} \mu_A(u)/u$ по методу центра тяжести осуществляется по формуле

$$a = \frac{\int\limits_{\underline{u}}^{\overline{u}} u \cdot \mu_A(u)\, du}{\int\limits_{\underline{u}}^{\overline{u}} \mu_A(u)\, du}.$$

Дефазификация нечеткого множества $\tilde{A} = \int\limits_{[\underline{u},\overline{u}]} \mu_A(u)/u$ по методу медианы состоит в нахождении такого числа a, что

$$\int_{\underline{u}}^{a} \mu_A(u)\, du = \int_{a}^{\overline{u}} \mu_A(u)\, du.$$

Дефазификация нечеткого множества $\tilde{A} = \int_{[\underline{u},\overline{u}]} \mu_A(u)/u$ по методу центра максимумов осуществляется по формуле

$$a = \frac{\int_G u\, du}{\int_G du},$$

где G — множество всех элементов из интервала $[\underline{u},\ \overline{u}]$, имеющих максимальную степень принадлежности нечеткому множеству $\tilde{A}$ [9].

5 Результаты и осуждение. В работе [10] были рассмотрены примеры с тремя входными данными (AV, $P(T)$, V) и рассчитаны по методике Microsoft уровни риска ИБ (R) для одного актива, но с разными уязвимостями (табл. 3).

Таблица 3

Оценка рисков ИБ по методике Microsoft [9]

	Название актива	AV	Описание угрозы	$P(T)$	Описание уязвимости	V	R
	Данные об инвестициях клиента	Средний	Несанкционированный доступ к клиентским данным посредством кражи учетной записи финансового консультанта	Высокий	Кража учетных записей локальной сети из-за несвоевременного обновления антивирусной защиты, конфигурации сети или систем безопасности	Средний	Высокий
	Данные об инвестициях клиента	Средний	Несанкционированный доступ к клиентским данным посредством кражи учетной записи финансового консультанта	Высокий	Кража учетных записей удаленного клиента из-за несвоевременного обновления антивирусной защиты, конфигурации сети или систем безопасности	Высокий	Высокий
	Данные об инвестициях клиента	Низкий	Несанкционированный доступ к клиентским данным посредством кражи учетной записи финансового консультанта	Средний	Кража учетной записи совершается хорошо зарекомендовавшим себя работником, злоупотребившим своим служебным положением	Низкий	Низкий

Далее будет представлены результаты оценки рисков для этих же примеров, но с использованием нечеткой модели.

На рисунке 6 представлены графическая интерпретация алгоритма нечеткого вывода Мамдани треугольными функциями принадлежности для первого примера ($AV = 0.6$, $P(T) = 0.9$, $V = 0.6$) и полученный результат риска ИБ, равный 0,735 (это соответствует лингвистической переменной — высокий риск).

На рисунке 7 представлены графическая интерпретация алгоритма нечеткого вывода Мамдани с трапециевидными функциями принадлежности для рассматриваемого примера угрозы ($AV = 0.6$, $P(T) = 0.9$, $V = 0.6$) и полученный результат риска ИБ, равный 0.71 (это соответствует лингвистической переменной — высокий риск).

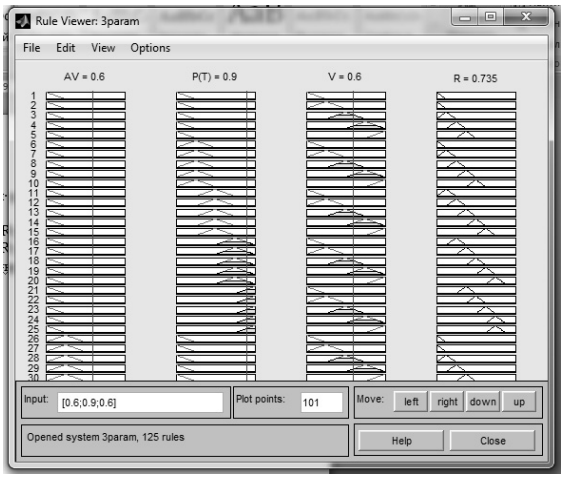

Рисунок 6. Графическая интерпретация алгоритма нечеткого вывода Мамдани с треугольными функциями принадлежности

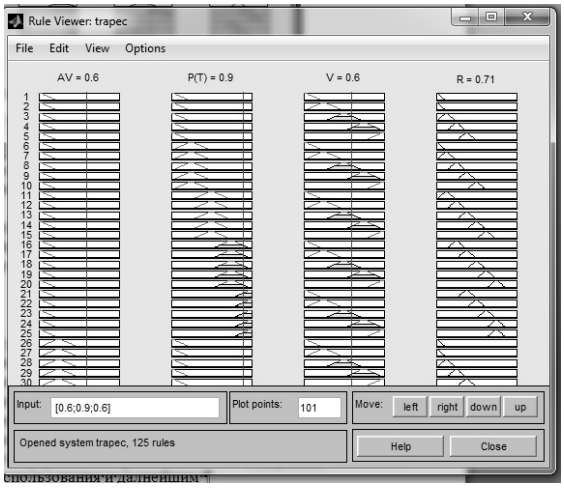

Рисунок 7. Графическая интерпретация алгоритма нечеткого вывода Мамдани с трапециевидными функциями принадлежности

На рисунке 8 представлены графическая интерпретация алгоритма нечеткого вывода Сугено для рассматриваемого примера угрозы ($AV = 0.6$, $P(T) = 0.9$, $V = 0.6$) и полученный результат риска ИБ, равный 0.699 (это соответствует лингвистической переменной — высокий риск).

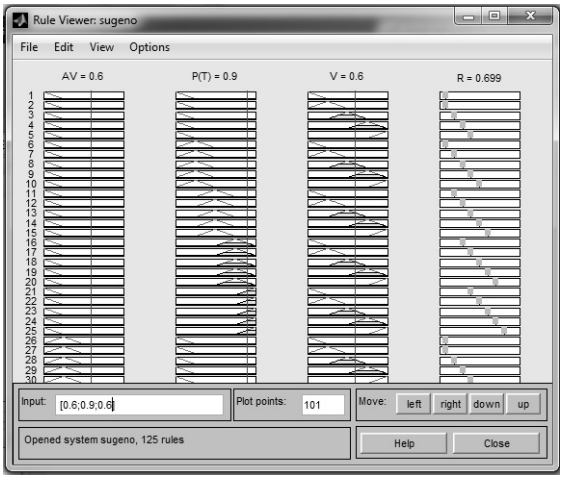

Рисунок 8. Графическая интерпретация алгоритма нечеткого вывода Сугено

Аналогично получены расчетные данные для других случаев из таблицы 3, результаты представлены в таблице 4. Как видно из таблицы 4, уровни риска ИБ, полученные при использовании аппарата нечетких множеств и нечеткой логики, соответствуют уровням риска ИБ, полученным по общепринятой в мировой практике методике Microsoft. Это свидетельствует об адекватности предлагаемой в данной работе нечеткой модели оценки рисков ИБ.

Таблица 4

Сравнительный анализ методов оценки риска ИБ по нечеткой логике

№	В работе [10]	Нечеткий вывод Мамдани		Нечеткий вывод Сугено
		треугольная функция принадлежности	трапециевидная функция принадлежности	
1 случай	Высокий	0,735	0,71	0,699
2 случай	Высокий	0,777	0,81	0,816
3 случай	Низкий	0,271	0,28	0,261

Существующие качественные методики оценки рисков ИБ не обладают достаточной точностью получаемых результатов, а количественные оценки сводятся к вероятностным методикам, которые, в отсутствие статистики инцидентов, не дают достоверных результатов. Модели на основе теории нечетких множеств и нечеткой логики лишены перечисленных выше недостатков и могут быть использованы для обработки оценок экспертов.

Список литературы

1 *Buldakova T.I., Dzalolov A.Sh.* Analysis of Data Processes and Choices of Data-processing and Security Technologies in Situation Centers // Scientific and Technical Information Processing. — 2012. — Vol. 39. — No. 2. — P. 127–132. — [ER]. Access mode: DOI: 10.3103/S0147688212020116.

2 *Zadeh L.A.* Fuzzy sets, Information and Control 8. — 1965. — P. 338–353.

3 *Satybaldina D., Muratkhan R., Kabenov D.* Ontology and Fuzzy Measures Based System for Information Security Risk Assessment. WOSIS — 9th International Workshop on Security in Information Systems. June, 28, July, 1, 2012, Wroclaw, Poland. — P. 77–85.

4 *Балашов П.А., Кислов Р.И., Безгузиков В.П.* Оценка рисков информационной безопасности на основе нечёткой логики // Безопасность компьютерных систем. Конфидент: Информ.-метод. журн. — 2003. — № 6. — С. 60–65.

5 *Ярушкина Н.Г.* Основы теории нечетких и гибридных систем. — М.: Финансы и статистика, 2004. — 320 с.

6 *Mamdani E.H., Assilian S.* An Experiment in Linguistic Synthesis with Fuzzy Logic Controller // Int. J. Man-Machine Studies. — 1975. — Vol. 7. — No. 1. — P. 1–13.

7 *Takagi T., Sugeno M.* Fuzzy identification of systems and its applications to modeling and control // IEEE Transactions on Systems, Man and Cybernetics. — 1985. — Vol. SMC-15. — No. 1. — P. 116–132. — [ER]. Access mode: DOI: 10.1109/TSMC.1985.6313399.

8 *Bojadziev G., Bojadziev M.* Fuzzy Logic for Business, Finance and Management, World Scientific, Singapore, 1997.

9 *Хаптахаева Н.Б., Дамбаева С.В., Аюшеева Н.Н.* Введение в теорию нечетких множеств: Учеб. пособие. Ч. I // Улан-Удэ: Изд-во ВСГТУ, 2004. — 68 с.: ил.

10 *Баранов Д., Конеев И.* Вопросы перехода от качественного к количественному анализу рисков / Депозитариум. — 2008. — № 9 (67). — С. 26–31.

Р.Мұратхан, Д.Ж.Сатыбалдина

Бұлдыр логика теориясы негізінде ақпараттық қауіпсіздіктің тәуекелін бағалау

Қазіргі заманғы кәсіпорындардың ақпараттық қауіпсіздігінің тәуекелі — ол бір-бірімен байланысқан көптеген айнымалылардан тұратын көпөлшемді күрделі түсінік. Көп жағдайда тәуекел факторының мәні дәлме дәл анықталмайды. Сондықтан ақпараттық қауіпсіздіктің тәуекелін бағалауда бұлдыр логиканы пайдалану қажет. Мақалада ақпараттық қауіпсіздіктің тәуекелін бағалау үшін бұлдыр логика теориясын қолдану қарастырылды.

R.Muratkhan, D.Zh.Satybaldina

Assessment of risk of information security by means of the theory of fuzzy sets

Risk of the breach of information security of the modern organization is the multidimensional complex concept which is including set of interconnected variables. Often, the value of risk factors cannot be accurately determined. Therefore, the risk assessment of information security can be defined as a fuzzy problem. This article describes methods of implementation of information security risk assessment in conjunction with the theory of fuzzy measures.

References

1 Buldakova T.I., Dzalolov A.Sh. *Scientific and Technical Information Processing*, 2012, 39, 2, p. 127–132. DOI: 10.3103/S0147688212020116.

2 Zadeh L.A. *Fuzzy sets, Information and Control 8*, 1965, p. 338–353.

3 Satybaldina D., Muratkhan R., Kabenov D. *Ontology and Fuzzy Measures Based System for Information Security Risk Assessment.* WOSIS — 9th International Workshop on Security in Information Systems, June, 28, July, 1, 2012, Wroclaw, Poland, p. 77–85.

4 Balashov P.A., Kislov R.I., Bezguzikov V.P. *Security of computer systems. Confident: Information and methodical magazine*, 2003, 6, p. 60–65.

5 Jarushkina N.G. *Fundamentals of the theory of fuzzy and hybrid systems*, Moscow: Finansy i statistika, 2004, 320 p.

6 Mamdani E.H., Assilian S. *Int. J. Man-Machine Studies*. 1975, 7, 1, p. 1–13.

7 Takagi T., Sugeno M. *IEEE Transactions on Systems, Man and Cybernetics*, 1985, SMC-15, 1, p. 116–132. DOI: 10.1109/TSMC.1985.6313399.

8 Bojadziev G., Bojadziev M. *Fuzzy Logic for Business, Finance, and Management, World Scientific, Singapore*, 1997.

9 Haptahaeva N.B., Dambaeva S.V., Ajusheeva N.N. *Introduction to the theory of fuzzy sets*: Textbook, I, Ulan-Udje: VSGTU publ., 2004, 68 p: il.

10 Baranov D., Koneev I. *Questions transition from qualitative to quantitative risk analysis. Magazine Depositarium*, 9 (67), 2008, p. 26–31.