Некоторые подходы к оценке информационных рисков с использованием нечётких множеств

Автор: Шевяхов Максим Юрьевич

Содержание

- Информационные риски
- Теория нечётких множеств
- Практическое применение
- Процедура оценки группы рисков
- Пример оценки группы рисков

Информационные риски

Стандарты информационной безопасности (ГОСТ 17799) определяют оценку информационного риска на основании двух показателей:

- Вероятности возникновения риска
- Величины ущерба, приносимого риском

Недостатки:

- Не учитываются затраты на ликвидацию риска
- Не всегда можно дать точное значение какого-либо показателя

Теория нечётких множеств

Основатель теории – Лотфи Заде (Fuzzy Sets// Information and Control. 1965. Vol.8 – P. 338-353)

Теория нечётких множеств

- X – универсальное множество, множество всевозможных значений **x**
- Нечёткое множество $A = \{(x, \mu_A(x)) \mid x \in X; \mu_A(x) \in [0;1]\}$
- $\mu_A(x)$ – функция принадлежности, показывает степень принадлежности элемента x множеству A

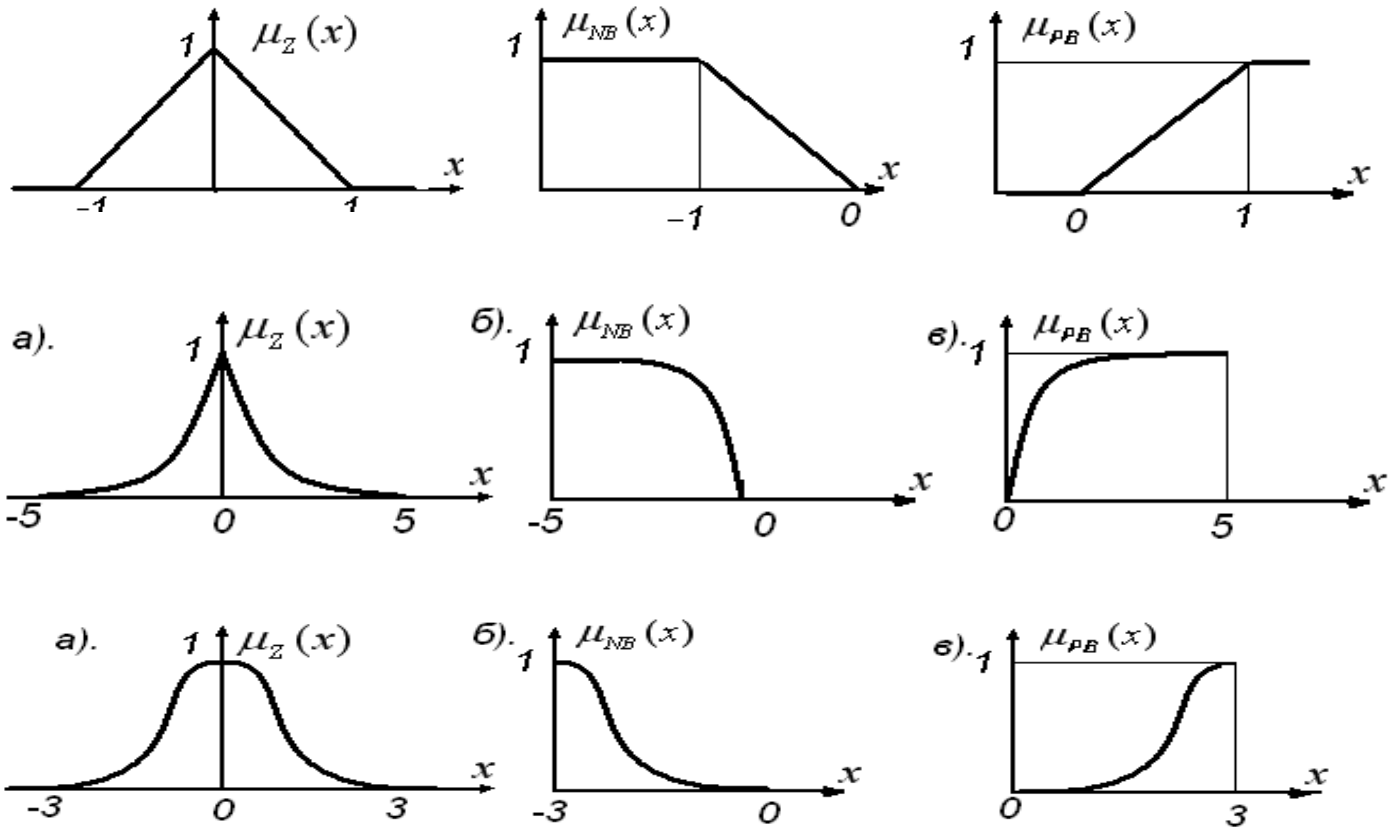
0 – не принадлежит

1 – полностью принадлежит

0,3 – принадлежит на 30%

Теория нечётких множеств

- Частные случаи простейших функций принадлежности:



Теория нечётких множеств

- Лингвистическая переменная – это переменная, значения которой описываются словами или фразами естественного языка.
- Терм-множество – множество допустимых значений лингвистической переменной
- Терм – конкретное значение лингвистической переменной. Выражается нечётким множеством.

Практическое применение

- Стандарт NIST 800-30. Моделирование оценки риска, основанной на вероятности возникновения и возможном ущербе от риска.

IF		THEN	
P	U	DoS	RiskLevel
low	low	1.00	low
low	medium	1.00	low
low	high	1.00	low
medium	low	1.00	low
medium	medium	1.00	medium
medium	high	1.00	medium
high	low	1.00	low
high	medium	1.00	medium
high	high	1.00	high

- Добавление стоимости снижения риска. Новая переменная, показывающая целесообразность снижения риска.

IF		THEN	
U	Z	DoS	doing
low	low	1.00	zero
low	medium	1.00	negative
low	high	1.00	very_negative
medium	low	1.00	positive
medium	medium	1.00	zero
medium	high	1.00	negative
high	low	1.00	very_positive
high	medium	1.00	positive
high	high	1.00	zero

Процедура оценки группы рисков

- Для каждого риска находятся показатели **вероятности возникновения**, **ущерба** и **стоимости снижения** риска в виде качественных оценок
- Для каждого риска получить показатели **уровня риска** и **целесообразности ликвидации** в виде качественных оценок

- Если бюджет СБ ограничен, то в первую очередь работать с теми рисками, *целесообразность снижения* которых наибольшая. Среди этой группы рисков в первую очередь работать с теми рисками, *уровень* которых наибольший

- Если бюджет СБ неограничен или очень велик, то в первую очередь работать с теми рисками, *уровень* которых наибольший. Среди этой группы рисков в первую очередь работать с теми рисками, *целесообразность снижения* которых наибольшая

Оценка группы рисков. Шаг 1

	Вероятность	Ущерб	Стоимость снижения
R1	middle	high	high
R2	middle	middle	middle
R3	high	middle	middle
R4	middle	high	middle
R5	middle	high	high
R6	middle	low	low
R7	middle	middle	high
R8	high	high	low
R9	middle	high	middle
R10	middle	low	high
R11	middle	middle	middle
R12	middle	high	low
R13	middle	middle	middle
R14	high	high	middle
R15	low	high	middle

Оценка группы рисков. Шаг 2

	Уровень риска	Целесообразность устранения
R1	middle	zero
R2	middle	zero
R3	middle	zero
R4	middle	positive
R5	middle	zero
R6	low	zero
R7	middle	negative
R8	high	very_positive
R9	middle	positive
R10	low	very_negative
R11	middle	zero
R12	middle	very_positive
R13	middle	zero
R14	high	positive
R15	low	positive

Оценка группы рисков. Шаг 3

Бюджет неограничен

	Уровень риска	Целесообразность устранения
R8	high	very_positive
R14	high	positive
R12	middle	very_positive
R4	middle	positive
R9	middle	positive
R1	middle	zero
R2	middle	zero
R3	middle	zero
R5	middle	zero
R11	middle	zero
R13	middle	zero
R7	middle	negative
R15	low	positive
R6	low	zero
R10	low	very_negative

Бюджет ограничен

	Уровень риска	Целесообразность устранения
R8	high	very_positive
R12	middle	very_positive
R14	high	positive
R4	middle	positive
R9	middle	positive
R15	low	positive
R1	middle	zero
R2	middle	zero
R3	middle	zero
R5	middle	zero
R11	middle	zero
R13	middle	zero
R6	low	zero
R7	middle	negative
R10	low	very_negative

Спасибо за внимание