Методы исследования проблем защиты информации

Краткий анализ общих моделей СЗИ

- Основное назначение общих моделей состоит
  - в создании предпосылок для объективной оценки общего состояния ИС с точки зрения меры уязвимости или уровня защищенности информации в ней.
  - Необходимость в таких оценках обычно возникает при анализе общей ситуации с целью выработки стратегических решений при организации защиты информации.
- Общими моделями систем и процессов ЗИ названы такие,
  - которые позволяют определять (оценивать) общие характеристики указанных систем и процессов
  - в отличие от моделей локальных и частных, которые обеспечивают определение (оценки) некоторых локальных или частных характеристик систем или процессов.

Примеры общих моделей СЗИ

- **Общая модель процесса ЗИ**.
  - Данная модель в самом общем виде и для самого общего объекта защиты должна отображать процесс защиты информации как процесс взаимодействия дестабилизирующих факторов, воздействующих на информацию, и средств защиты информации, препятствующих действию этих факторов.
  - Итогом взаимодействия будет тот или иной уровень защищенности информации;
- **Обобщенная модель СЗИ**.
  - Являясь дальнейшим развитием общей модели процесса защиты, обобщенная модель системы защиты должна отображать основные процессы, осуществляемые в ней с целью рационализации процессов защиты.
  - Указанные процессы в самом общем виде могут быть представлены как процессы распределения и использования ресурсов, выделяемых на защиту информации;

Примеры общих моделей СЗИ

- **Модель общей оценки угроз информации**.
  - Основной направленностью этой модели является оценка не просто угроз информации как таковых, а еще и оценка тех потерь, которые могут иметь место при проявлений различных угроз.
  - Модели данного направления важны еще и тем, Что именно на них в наибольшей степени были выявлены те условия, при которых такие оценки могут быть адекватны реальным процессам защиты информации;
- **Модели анализа систем разграничения доступа к ресурсам ИС**.
  - Модели этого класса предназначены для обеспечения решения задач анализа и синтеза систем (механизмов) разграничения доступа к различным видам ресурсов ИС и прежде всего к массивам данных или полям ЗУ.
  - Выделение этих моделей в самостоятельный класс общих моделей обусловлено тем, что механизмы разграничения доступа относятся к числу наиболее существенных компонентов систем защиты информации, от эффективности функционирования которых, в значительной мере зависит общая эффективность защиты информации в ИС.

Сложности решения задач анализа и синтеза СЗИ

- Особенности задач:

  - сложная опосредствованная взаимосвязь показателей качества СЗИ с показателями качества информационной системы;
  - необходимость учета большого числа показателей (требований) СЗИ при оценке и выборе их рационального варианта;
  - преимущественно качественный характер показателей (требований), учитываемых при анализе и синтезе СЗИ;
  - существенная взаимосвязь и взаимозависимость этих показателей (требований), имеющих противоречивый характер;
  - трудность получения исходных данных, необходимых для решения задач анализа и синтеза СЗИ, в особенности на ранних этапах их проектирования.

Общая характеристика мат.методов оценки и обоснования требований к СЗИ

- Практически невозможно применение методов математической статистики и теории вероятностей, а также классических методов оптимизации, так как они используют **экспериментальные данные**, обладающие строго определенной точностью и достоверностью.
- При оценке и выборе альтернатив возможно, (а зачастую просто необходимо) использовать и обрабатывать **качественную** экспертную информацию.
- **Применяемый формальный аппарат по своим потенциальным возможностям и точности должен быть адекватен смысловому содержанию и точности исходных данных.**
- Теория нечетких множеств имеет дело с “человеческими знаниями”, которые принято называть экспертной информацией.
- Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

Определение нечеткого множества

Пусть X = {x} — универсальное множество, т.е. полное множество, охватывающее всю проблемную область.

Нечеткое множество **A** ⊆ **X** представляет собой набор пар $\{(x, \mu^A(x))\}$, где $x \in X$ и $\mu^A : X \to [0, 1]$ — функция принадлежности, которая представляет собой некоторую субъективную меру соответствия элемента нечеткому множеству.

$\mu^A(x)$ может принимать значения от нуля, который обозначает абсолютную не принадлежность, до единицы, которая, наоборот, говорит об абсолютной принадлежности элемента x нечеткому множеству **A**.

Если нечеткое множество **A** определено на конечном универсальном множестве **X** = $\{x_1, x_2, ..., x_n\}$, то его удобно обозначать следующим образом: $\mathbf{A} = \mu^A(x_1)/x_1 + \mu^A(x_2)/x_2 + \ldots + \mu^A(x_n)/x_n = \sum \mu^A(x_i)/x_i$

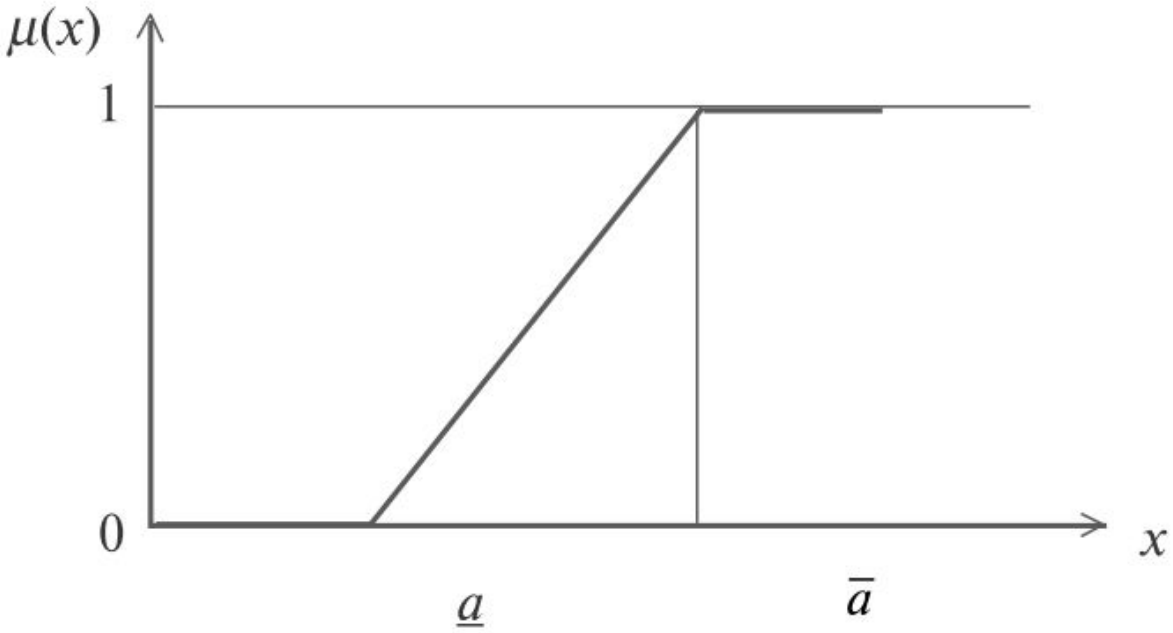
где $\mu^A(x_i)/x_i$ — пара “функция принадлежности/элемент”, называемая синглтоном, а “+” — обозначает совокупность пар.

Пример нечеткого множества

- Пусть X = {1, 2, ..., 10}.
- Тогда нечеткое множество “большие числа” может быть представлено следующим образом:
- A = “большие числа” = 0.2/6 + 0.5/7 + 0,8/8 + 1/9 + 1/10.
- Это следует понимать следующим образом: 9 и 10 с абсолютной уверенностью можно отнести к “большим числам”, 8 — есть “большое число” со степенью 0.8 и т.д. 1,2, ..., 5 абсолютно не являются “большими числами”.

Функция принадлежности нечеткого множества

На практике удобно использовать кусочно-линейную аппроксимацию функции принадлежности нечеткого множества так как требуется только два значения — ~~a~~ и ā



Свойства нечетких множеств

1. Нечеткое множество $A \subseteq X$ пустое, т.е. $A = \varnothing$, если $\mu A(x) = 0, \forall x \in X$.
2. Нечеткие множества A и $B \subseteq X$ эквивалентны, т.е. $A = B$, если $\mu^A(x) = \mu^B(x) \ \forall x \in X$.
3. Нечеткое множество $A \subseteq X$ является подмножеством нечеткого множества $B \subseteq X$, т. е. $A \subseteq B$ если $\mu^A(x) \leq \mu^B(x) \ \forall x \in X$.

Примеры

Пусть X = {1,2,3 },
A = 0.3/1 + 0.5/2 + 1/3, B = 0.4/1+0.6/2+1/3.
Тогда A ⊆ B

Кардинальное число (мощность) нечеткого множества A

$$A = \mu^A(x_1)/x_1 + \mu^A(x_2)/x_2 + \ldots + \mu^A(x_n)/x_n = \sum^n \mu^A(x_i)/x_i$$

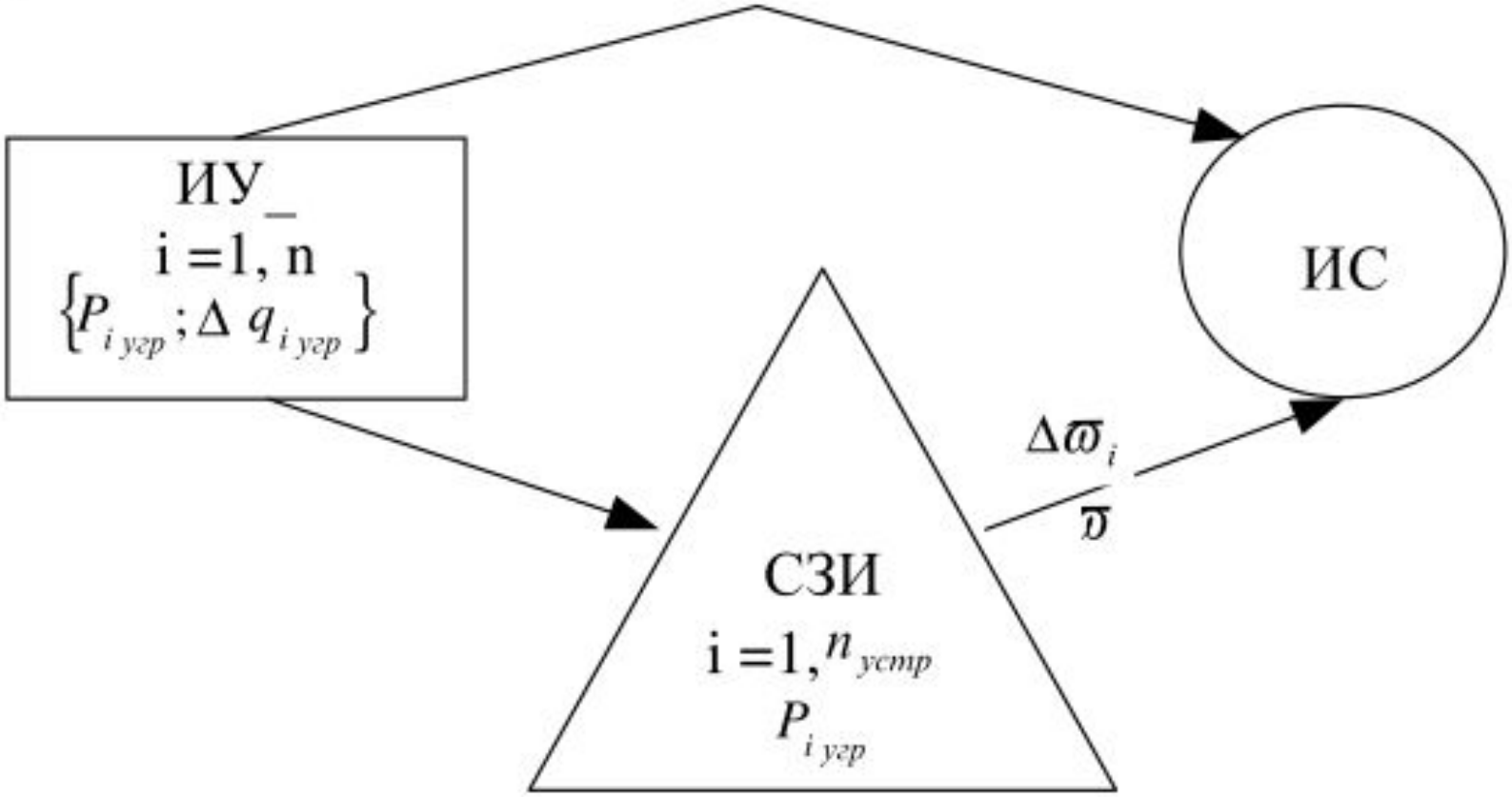
Находится как $$cardA = |A| = \sum_{i=1}^{n} \mu^A(x_i)$$

Если X = {1.,2,3,4} A = 0.1/1 + 0.4/2 + 0.7/3 + 1/4, то
card A = 2.2

Литература по нечетким множествам

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. - К.:000 "ТИД "ДС", 2001. - 688 с.
2. Кофман А. Введение в теорию нечетких множеств М.: Радио и связь, 1982. - 432с.
3. Поспелов Д.А. Нечеткие множества в моделях управления и искусственного интеллекта. "М. :Наука, 1986. - 312с.
4. Борисов А.Н., Алексеев А.В., Меркурьев Г.В. и др. Обработка нечеткой информации в системах принятия решений. - М: Радио и связь, 1989. - 304с.
5. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решения на основе нечетких моделей: примеры использования; Рига “Знание”, 1990. - 184 с.
6. Ротштейн А.П. Интеллектуальные технологии идентификации; Винница: “Универсум-Винница”, 1999. - 320с.

Общая модель процесса защиты информации



Иерархическая классификация методов определения коэффициентов важности критериев

Методы обработки информации в первичных шкалах

- 1А .Методы попарного сравнения.
  - 1А.1.Методы анализа матрицы попарного сравнения.
    - 1А.1.1. Методы собственных векторов.
    - 1А.1.2. Методы наименьших квадратов.
    - 1А.1.3. Методы собственных векторов матрицы.

Методы обработки и информации в произвольных шкалах

- 2А. Методы аппроксимации функции полезности.
  - 2А.1. Методы обобщенного критерия Подиновского.
  - 2А.2. Методы функций ценности.
  - 2А.3. Методы “уклонений”.
- 2Б. Методы трансформации частот.
  - 2Б.1. Методы трансформации частот предпочтений.
  - 2Б.2. Методы трансформации частот отнесения к классу.
  - 2Б.3. Методы случайных векторов

УГРОЗЫ НАРУШЕНИЯ БИ