Системы защиты информации

Оглавление

Глава 6. Математические модели систем и процессов защиты информации

6.1 Общая характеристика проблемы синтеза систем защиты информации для ИС

Оценки параметров СЗИ в условиях высокой степени неопределенности условий ее функционирования должны вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных.

При синтезе оптимальных систем защиты ***исходными*** должны явиться следующие два положения:

- выбор математически продуктивного критерия оптимальности в соответствии с архитектурой системы защиты и технологией обработки информации на объекте;
- четкая математическая формулировка задачи, учитывающая все априорные сведения и позволяющая решить ее в соответствии с принятым критерием.

Итогом решения задачи синтеза оптимальной системы защиты и его конечной целью должны быть четыре содержательных результата:

- архитектура системы защиты;
- количественная оценка качества ее функционирования;
- оценка практической чувствительности разработанных моделей к отклонениям от априорных данных;
- физическая реализуемость синтезируемых систем защиты в современных системах обмена данными (соответствие технологии обработки информации уровню ее защиты).

  Под эффективностью систем защиты информации будем понимать эффективность ее использования в качестве активного средства в операции обеспечения конфиденциальности обработки, хранения и передачи информации.

  При этом, оценка эффективности операции заключается в выработке оценочного суждения относительно пригодности заданного способа действий специалистов по защите информации или приспособленности средств защиты к решению задач.

Введение показателя эффективности требует также определения критерия эффективности как правила, позволяющего сопоставлять стратегии, характеризующемся различной степенью достижения цели, и осуществлять выбор стратегий из множества допустимых.

Теоретические основы построения оптимальных систем защиты исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.

Кроме того отсутствие достаточно общей теории, формирующей методологические основания изучения явлений с неопределенными факторами, делает неприменимыми байесовские методы классической теории статистических решений для синтеза оптимальных систем защиты.

Под методологией оптимизации систем защиты информации будем понимать разработку теории, связывающей их структуру, логическую организацию, методы и средства деятельности с целью формирования функции выбора и выделения подмножества наилучших стратегий.

Оптимальным будет считаться решение, которое в предполагаемых условиях наилучшим образом удовлетворит условиям рассматриваемой задачи. Оптимальность решения достигается за счет наиболее рационального распределения ресурсов, затрачиваемых на решение проблемы защиты.

В процессе создания оптимальной СЗИ неизбежно возникает задача коррекции требований к системе защиты. Трудность ее решения заключается в том, что возникают неопределенности не стохастического характера, определяемые:

- наличием целенаправленного противодействия со стороны противоборствующей системы, способы действий которой неизвестны исследователю;
- недостаточной изученностью некоторых явлений, сопровождавших процесс функционирования систем защиты;
- нечетким представлением цели операции, приводящей к неоднозначной трактовке соответствия реального результата операции требуемому.

Проблемы корректности постановки задач.

Трудность исследования вопросов обеспечения безопасности информационных технологий усугубляется большой неопределенностью условий функционирования ИС.

Поэтому постановка задачи обеспечения защиты информации, как правило, оказывается некорректной, поскольку зачастую формулируется в условиях непредсказуемости поведения системы в нестандартных и, особенно, экстремальных ситуациях. Влияние неопределенности особенно сильно проявляется в трансформируемых, нестабильных, слабо организованных ИС из-за неполноты, несвоевременности, не нормированности и низкой достоверности информации.

В связи с этим задачи обеспечения безопасности информационных технологий , как правило, не обладают свойством единственности решения, эффективность и оптимальность которого определяются степенью учета ограничений, характерных для конкретной ситуации. Для повышения степени корректности постановки задач обеспечения БИТ необходимо повышать знания о ИС в непрерывно изменяющихся условиях ее функционирования.

В связи с этим получение и использование знаний должны осуществляться непосредственно в процессе функционирования системы путем постепенного накопления необходимой информации, анализа и использования ее для эффективного выполнения системой заданной целевой функции в изменяющихся условиях внутренней и внешней среды.

Известные математические модели, используемые для описания структуры, поведения и управления СЗИ, особенно нестабильными, в условиях некорректной постановки задач не дают желаемого результата.

Поэтому необходима разработка новых, ориентированных на специфику процессов защиты информации методов и средств моделирования.

Для получения информации о поведении СЗИ требуется выделить группы параметров и определить времена проверки их значений. При этом рассматриваются особо значимые и важные с точки зрения реализации цели функционирования системы параметры.

Проверка и анализ значений указанных параметров, необходимы для повышения знаний о системе, должны осуществляться таким образом, чтобы обеспечить возможность принятия своевременных и достоверных решений и корректировку поведения системы в процессе функционирования. Таким образом, в СЗИ обязательно должно быть предусмотрено выполнение процедур контроля ее работоспособности и диагностирования состояний.

Принятие решений может в большинстве случаев базируется на экспертных оценках. Однако в условиях неопределенности исходных данных и некорректности постановки задач управления эти оценки могут внести дополнительную некорректность в принимаемое решение, увеличив тем самым исходную неопределенность

Исследование предметной области с целью создания математической модели СЗИ.

Решение проблем моделирования СЗИ требует поэтапного выполнения следующих исследований.

1. Разработка принципов, методов и средств сокращения размерности описания СЗИ, включающая:

- анализ информационной структуры системы и взаимосвязей между решаемыми в ней задачами;
- анализ динамических характеристик решения задач;
- анализ корреляционных зависимостей между параметрами системы, являющимися результатами решения отдельных задач;
- выделение на основе анализа совокупностей задач, результат решения каждой из которых позволяет определить один из контролируемых параметров системы.

В результате разработки должны быть сформулированы требования и рекомендации по рациональной организации структуры СЗИ, декомпозированной по уровням контроля и управления. Это позволит проводить дальнейшие исследования в условиях минимизированной размерности описания системы.

2. Разработка методологии, методов и средств решения задач обеспечения БИТ в условиях неопределенности, включающая:

- исследование вопросов корректности постановки задач при недостаточном понимании конечных результатов и целей решения в резко меняющихся условиях;
- исследование вопросов использования неопределенности (неполноты, низкой достоверности и пр.) исходных данных при решении задач обеспечения БИТ.

Результатом исследований должна явиться разработка методологических основ, методов и средств решения некорректно поставленных задач в условиях неопределенности.

Контроль параметров состояния СЗИ

Разработка идеологии, методов и средств адаптивного контроля параметров и диагностирования состояний системы, включает следующие задачи:

- - формирование динамических зон (нормального функционирования, предупреждения, тревоги, катастрофы), характеризующих различные состояния экономической системы и динамических порогов, разделяющих эти зоны, выделение интегральных динамических векторов индикации состояний системы;
- - разработку идеологии и стратегии выполнения адаптивного (по времени проведения, количеству и номенклатуре контролируемых параметров) контроля векторов индикации, прогнозирования тенденций изменения их значений в процессе функционирования системы;
- - разработку методов и алгоритмов адаптивного одиночного и группового контроля и прогнозирования значений компонентов векторов индикации;
- - разработку методов и алгоритмов распознавания и идентификации принадлежности состояний системы динамическим зонам и порогам на основании анализа текущих и прогнозируемых значений отдельных компонентов и векторов индикации в целом;
- - разработку методов и алгоритмов диагностирования системы на основе анализа результатов идентификации по всем векторам индикации.

Результатом разработки должно быть создание идеологии, математических методов и средств для организации адаптивного контроля и диагностирования состояний СЗИ.

Разработка принципов, методов и средств самоорганизации СЗИ

Разработка принципов, методов и средств самоорганизации СЗИ , включает следующие задачи:

- - конструирование адаптивных моделей для описания структуры и поведения системы, прогнозирование значений ее параметров;
- - конструирование адаптивных моделей для формирования подмножеств контролируемых параметров и диапазонов значений зон их контроля на основе заданных требований к устойчивости функционирования системы;

- - конструирования адаптивных моделей контроля работоспособности и диагностирования нарушений работоспособности системы;
- - самоорганизацию и саморазвитие семейств моделей для описания структуры, поведения, прогнозирования, контроля и диагностирования с учетом обеспечения необходимой устойчивости системы в условиях влияния факторов внутренней и внешней среды.

Результатом исследований должны быть созданные на основе известных и специально разработанных методов и средств адаптивные модели для описания структуры и поведения СЗИ, а также контроля, диагностирования и прогнозирования ее состояний.

Разработка методов и средств поддержки принятия решений

Разработка методов и средств поддержки принятия решений, включает следующие задачи:

- - разработку методов и средств выбора решений из всего множества альтернативных вариантов на основании анализа состояния и поведения системы и с учетом требований управления, реального ресурса, удовлетворяющего этим требованиям, квантифицированных оценок близких и отдаленных последствий выполнения принятых решений;
- - разработку методов и средств декомпозиции принятых решений по уровням управления системы;
- - разработку методов и средств поддержки принятия решений по самоорганизации системы в процессе ее функционирования для совершенствования всех видов перечисленных выше моделей и их семейств.

Исследования базируются на использовании всех полученных ранее результатов и ориентированы на создание банка знаний о системе ЗИ.

Для решения перечисленных и других теоретических и прикладных проблем необходима целенаправленная, выполняемая в рамках государственных программ и на единой концептуальной и методологической основе, организация комплексных исследований проблем обеспечения БИТ.

Конечным результатом исследований должна быть модель СЗИ.

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 защиты информации 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.

Системную классификацию общих моделей в настоящее время произвести практически невозможно, так как ввиду малого числа таких моделей для этого нет достаточных данных. Поэтому классификацию рассматриваемых моделей представим простым перечнем и краткой характеристикой лишь некоторых моделей.

Общая модель процесса защиты информации.

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 системы защиты информации.

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;

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.

Общая характеристика математических методов оценки и обоснования требований к СЗИ

Системы защиты информации, с одной стороны, являются составной частью информационной системы, с другой стороны сами по себе представляют сложную техническую систему. Решение задач анализа и синтеза СЗИ усложняется рядом их особенностей, основными из которых являются:

- 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.

Указанные особенности делают практически невозможным применение традиционных математических методов, в том числе методов математической статистики и теории вероятностей, а также классических методов оптимизации для решения прикладных задач анализа и синтеза СЗИ.

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что при оценке и выборе альтернатив возможно, (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию. Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

Теория нечетких множеств в очередной раз подтвердила одну, известную всем исследователям истину: применяемый формальный аппарат по своим потенциальным возможностям и точности должен быть адекватен смысловому содержанию и точности исходных данных. Математическая статистика и теория вероятностей используют экспериментальные данные, обладающие строго определенной точностью и достоверностью. Теория нечетких множеств имеет дело с “человеческими знаниями”, которые принято называть экспертной информацией.

При написании данной главы поставлена скромная задача:

на основе анализа и использования известной литературы по теории нечетких множеств показать, как можно применить этот современный математический аппарат для решения прикладных задач, связанных с оценкой и выбором вариантов построения систем защиты информации.

Применение теории нечетких множеств для решения этих задач, как правило, иллюстрируется примерами.

6.2 Основные понятия теории нечетких множеств

6.2. 1 Нечеткие множества: определение, свойства, операции

над нечеткими множествами

Данный раздел написан по материалам работ [1, 2, 3, 4], обобщение которых проведено в работе [5].

6.2.1.1. Определение нечеткого множества. Пусть $\boldsymbol{X} = \{x\}$ -универсальное множество, т.е. полное множество, охватывающее всю проблемную область.

Определение 6.2.1. *Нечеткое множество* $\boldsymbol{A} \subseteq \boldsymbol{X}$ представляет собой набор пар $\{(x, \mu^A(x))\}$, где $x \in \boldsymbol{X}$ и $\mu^A: \boldsymbol{X} \longrightarrow [0, 1]$ - 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 $\boldsymbol{A}$.

Если нечеткое множество $\boldsymbol{A}$ определено на конечном универсальном множестве $\boldsymbol{X} = \{x_1, x_2,\ldots,x_n\}$, то его удобно обозначать следующим образом:

$$A = \mu^A(x_1)/x_1 + \mu^A(x_2)/x_2 + \ldots + \mu^A(x_n)/x_n = \sum_{i=1}^{n} \mu^A(x_i)/x_i \qquad (6.2.1)$$

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

Пример 6.2.1. Пусть $\boldsymbol{X}= \{1, 2, ..., 10\}$. Тогда нечеткое множество “большие числа” может быть представлено следующим образом:

$\boldsymbol{A}$ = “большие числа” = 0.2/6 + 0.5/7 + 0,8/8 + 1/9 + 1/10.

Это следует понимать следующим образом: 9 й 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”.

На практике удобно использовать кусочно-линейную аппроксимацию функции принадлежности нечеткого множества, как это показано на рис. 6.2.1, так как требуется только два значения - и $\bar{a}$.

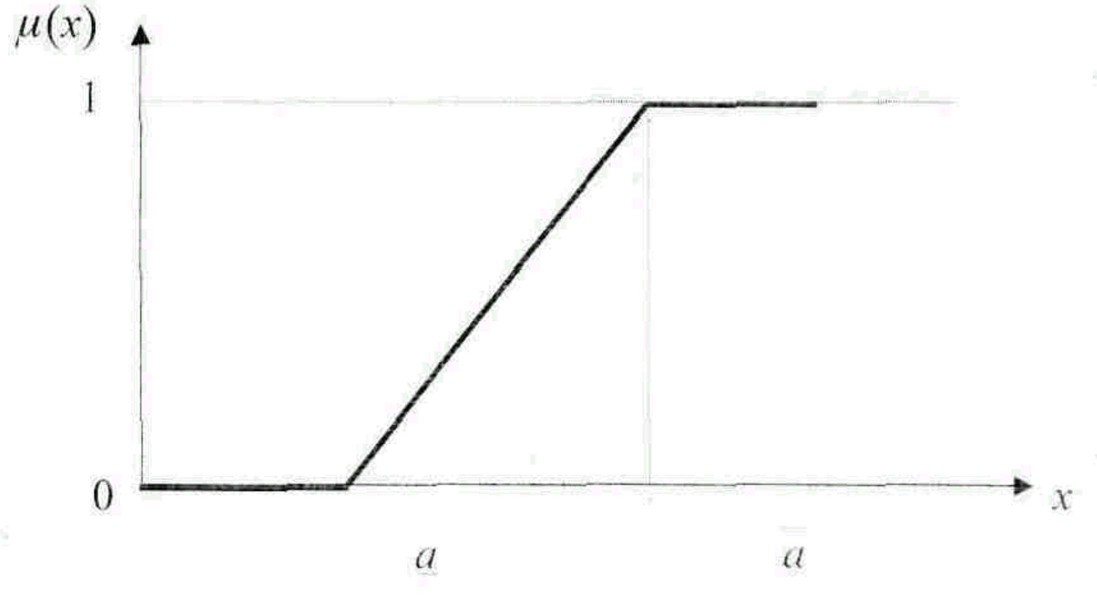

Рис. 6.2.1 Функция принадлежности нечеткого множества.

В случае непрерывного множества $\boldsymbol{X}$ используется следующее обозначение:

$$\min_{S \in M_s} q_1(S) \quad (6.2.2)$$

6.2.1.2. Свойства нечетких множеств.

1. Нечеткое множество $A \subseteq X$ *пустое,* т.е. $A = \varnothing$, если $\mu^{A}(x) = 0$, $\forall x \in \mathbf{X}$.

2. Нечеткие множества A и $B \subseteq X$ *эквивалентны,* т.е. A=B,если

$\mu^{A}(x) = \mu^{B}(x) \;\; \forall x \in \mathbf{X}$..

3. Нечеткое множество $A \subseteq X$ является подмножеством нечеткого множества $B \subseteq X$, т.е. $A \subseteq B$ если $\mu^{A}(x) \le \mu^{B}(x) \;\; \forall x \in \mathbf{X}$.

Пример 6.2.2. Пусть $X = \{1,2,3\}$,

A =0.3/1 + 0.5/2 + 1/3,

B = 0.4/1+0.6/2+1/3.

Тогда $A \subseteq B$.

Кардинальное число (мощность) нечеткого множества *n*

$$A = \mu^{A}(x_1)/x_1 + \mu^{A}(x_2)/x_2 + \ldots + \mu^{A}(x_n)/x_n = \sum_{i=1}^{n} \mu^{A}(x_i)/x_i$$

находится следующим образом:

$$cardA = |A| = \sum_{i=1}^{n} \mu^{A}(x_i) \quad (6.2.3)$$

Пример 6.2.3. Если X={1.,2,3,4} A = 0.1/1 + 0.4/2 + 0.7/3 + 1/4, то card A = 2.2.

6.2.1.3 Операции над нечеткими множествами.

1. *Дополнением* нечеткого множества A называется - нечеткое множество $\rceil A$, функция принадлежности которого равна

$$\mu^{\rceil A}(x) = 1 - \mu^{A}(x), \forall x \in X. \quad (6.2.4)$$

2. *Пересечением* двух нечетких множеств A и $B \in X$ называется нечеткое множество $A \cap B$, функция принадлежности которого равна

$$\mu^{A \cap B}(x) = \mu^{A}(x) \wedge \mu^{B}(x), \forall x \in X \;, (6.2.5)$$

где ^ - знак операции минимума.

3. *Объединением* двух нечетких множеств ***A*** и ***B*** $\in$ ***X*** называется нечеткое множество ***A*** $\cup$ ***B***, функция принадлежности которого равна

$$\mu^{A \cup B}(x) = \mu^{A}(x) \vee \mu^{B}(x), \forall x \in X \quad (6.2.6)$$

где V - знак операции максимума.

Пример 6.2.4 Пусть *X*= {1, 2,..., 10},

A = “малые числа” = 1/1 + 1/2 + 0.8/3 + 0.5/4 + 0.3/5 + 0.1/6;

B = “большие числа” = 0.1/5 + 0.2/6 + 0.5/7 + 0.8/8 +1/9+1/10;

Тогда

$\neg$***A***= *“НЕ* малые числа” = 0.2/3 + 0.5/4 + 0.7/5 + 0.9/6 + 1/7 + 1/8 + +1/9+1/10,

A $\cap$ ***B*** **=** “малые числа” И “большие числа” = 0,1/5 + 0.1/6,

A $\cup$ ***B*** = “малые числа” ИЛИ “большие числа” == 1/1 + 1/2 + 0.8/3 + + 0.5/4 + 0.3/5 + + 0.2/6 + 0.5/7 + 0.8/8 + 1/9 + 1/10.

Приведенные определения операций над нечеткими множествами являются наиболее распространенными.

Определение 6.2.2. α - *срезом (множеством уровня* α*)* нечеткого множества ***A*** $\subseteq$***X***, называется четкое множество ***A***α $\subseteq$***X*** такое, что

$$A_{\alpha} = \{x \in X : \mu^{A}(x) \geq \alpha\}, \forall \alpha \in [0,1]. \quad (6.2.7)$$

Пример 6.2.5. Если ***A*** = 1/1 + 0.8/2+0.5/3+0.1/4, то $A_{0.1}$ = {1,2,3,4}, $A_{0.5}$= {1, 2, 3}, A_{1} ={1}.

Принцип обобщения [1] дает формальный аппарат для переноса операций (арифметических, алгебраических) с обычных множеств на нечеткие.

Пусть функция *f* представляет собой отображение *f:* ***X*** —> ***Y*** и ***A*** есть нечеткое множество в ***X***. В соответствии с принципом обобщения, функция отображает нечеткое множество ***A*** в нечеткое множество **-** ***B*** $\subseteq$ ***Y*** такое, что

$$\mu^{B}(y) = \begin{cases} \sup \mu^{A}(x), f^{-1}(y) \neq \varnothing; \\ y = f(x); \\ 0, f^{-1}(y) = \varnothing. \end{cases} \quad (6.2.8)$$

Пример 6.2.6. Пусть **X**={1,2,3,4}, **Y** ={1,2,3,4,5,6} и y = *x + 2.* Если теперь
A *= 0.1/1 + 0.2/2 + 0.7/3 + 1/4, то* ***B*** *= 0.1/3 + 0.2/4 + 0.7/5 + 1/6.*

6.2.2. Нечеткие отношения

Пусть $X=\{x_1, x_2, \dots, x_n\}$ и $Y=\{y_1, y_2, \dots, y_m\}$.

Определение 6.2.3. *Нечетким отношением* ***R*** называется нечеткое множество, определенное на декартовом произведении $X \times Y$, которому соответствует функция принадлежности $\mu^R: X \times Y \to [0,1]$. Здесь $\mu^R(x, y)$ отражает силу зависимости между $x \in X$ и
$y \in Y$.

Пример 6.2.7. Пусть X = { конь, осел } и Y = { мул, корова }. Нечеткое отношение "подобный" может быть определено следующим образом:

R = "подобный" = 0.8 / (конь, мул) + 0.4 / (конь, корова) + 0.9/(осел, мул) + 0.5/(осел, корова), т.е. конь похож на мула со степенью 0.8, конь похож на корову со степенью 0.4 и т.д.

Определение 6.2.4. Если $R \subseteq X \times Y$ и $S \subseteq Y \times Z$, то *max-min композицией* называется нечеткое множество $R \circ S$, определенное на $X \times Z$, функция принадлежности которого имеет вид

$$\mu^{R \circ S}(x, z) = \sup_{y \in Y} \left[\mu^R(x, y) \wedge \mu^S(y, z) \right] \quad (6.2.9)$$

Max-min композиция позволяет ответить на вопрос, какое нечеткое множество в Y следует поставить в соответствие нечеткому множеству $A' \subseteq X$, если известно, что нечеткое множество $B \subseteq Y$ соответствует нечеткому множеству $A \subseteq X$. Операция нахождения такого соответствия называется *нечетким логическим выводом* и выполняется по следующей формуле:

$$B' = A' \circ R = A' \circ (A \times B), \quad (6.2.10)$$

где R - нечеткое отношение:

$$R = A \times B = \sum_{i=1}^{l} \sum_{j=1}^{m} \left\{ \mu^A(x_i) \wedge \mu^B(y_j) \right\} / (x_i, y_j), \quad (6.2.11)$$

° - max-mm композиция,, в соответствии с которой

$$B' = \sum_{j=1, i=\overline{1,l}}^{m} \vee \left\{ \mu^{A'}(x_i) \wedge \mu^R(x_i, y_j) \right\} / y_j, A, A' \subseteq X, B, B' \subseteq Y. \quad (6.2.12)$$

6.2.3. Нечеткие числа

Введенный принцип обобщения служит для переноса четких отношений в нечеткие. Например, его можно применить для определения нечеткой арифметики.

Определение 6.2.5. *Нечеткое число* это нечеткое множество *A*, определенное на множестве действительных чисел $\Re$, если его функция принадлежности нормальна и выпукла, т. е.

$$\sup_{x \in \Re} \mu^A(x) = 1,$$

$$x \le y \le z \Rightarrow \mu^A(y) \ge \min(\mu^A(x), \mu^A(z)).$$

Примеры нечетких чисел: "около 5", "чуть больше 7". В соответствии с принципом обобщения, арифметические операции над нечеткими числами имеют вид

-сложение $\int$

-вычитание $\mu^{A-B}(z) = \max_{z=x-y} \left\lfloor \mu^A(x) \wedge \mu^B(y) \right\rfloor, \forall x, e, z \in \Re$

- умножение $\mu^{A*B}(z) = \max_{z=x*y} \left\lfloor \mu^A(x) \wedge \mu^B(y) \right\rfloor, \forall x, y, z \in \Re$

-деление $\mu^{A/B}(z) = \max_{z=x/y} \left\lfloor \mu^A(x) \wedge \mu^B(y) \right\rfloor, x, y, z \in \Re.$

К сожалению, использование принципа обобщения для определения арифметических операции над нечеткими числами в общем довольно неэффективно. Поэтому часто предполагается, что нечеткие числа представляются в *LR-форме,* что соответствует описанию левой (left) й правой (right) частей функции.

Нечеткое число ***A*** представляется в *LR-форме,* если

$$\mu^A(x) = \begin{cases} L\left(\dfrac{m-x}{\alpha}\right), \alpha > 0, \forall x \le m \\ R\left(\dfrac{m-x}{\beta}\right), \beta > 0, \forall x \le m \end{cases}, \qquad (6.2.13)$$

где ***L*** и ***R*** - функции, обладающие свойствами

а) L (- x) = L (x);

б) L (0) =1;

в) *L* монотонно убывает на промежутке [0, + ∞].

Здесь m - среднее значение нечеткого числа ***A,*** α - отклонение слева, β - отклонение справа.

Если α = β = 0, то нечеткое число ***A*** переходит в четкое число *m.*

Таким образом, **LR**-форму нечеткого числа ***A*** можно представить в виде тройки ***A***=$\{m_A, \alpha_A, \beta_A\}$. Арифметические операции над нечеткими числами можно определить через операции над соответствующими им тройками

$$A + B = (m_A, \alpha_A, \beta_A) + (m_B, \alpha_B, \beta_B) = (m_A + m_B, \alpha_A + \alpha_B, \beta_A + \beta_B), \qquad (6.2.14)$$

$$A - B = (m_A, \alpha_A, \beta_A) - (m_B, \alpha_B, \beta_B) = (m_A - m_B, \alpha_A - \alpha_B, \beta_A - \beta_B), \quad (6.2.15)$$

$$A \cdot B = (m_A, \alpha_A, \beta_A) \cdot (m_B, \alpha_B, \beta_B) \approx (m_A \cdot m_B, m_A \cdot \alpha_B + m_B \cdot \alpha_A, m_A \cdot \beta_A + m_B \cdot \beta_B), \quad (6.2.16)$$

На практике ***LR***-представление упрощается за счет применения линейных функций, что приводит к треугольным нечетким числам (рис. 6.2.2а), которые имеют функцию принадлежности вида

$$\mu^A(x) = \begin{cases} (x - a^-)/(a - a^-), a^- \le x \le a \\ (a^+ - x)/(a^+ - a), a \le x \le a^+ \end{cases} \quad (6.2.17)$$

Кроме того, получили распространение трапециевидные формы, функций принадлежности (рис. 6.2.2б), которые имеют функций принадлежности вида

$$\mu^A(x) = \begin{cases} (x - a^-)/(\underline{a} - a^-), a^- \le x \le \underline{a} \\ 1, \underline{a} \le x \le \overline{a} \\ (a^+ - x)/(a^+ - \overline{a}), \overline{a} \le x \le a^+ \end{cases}, \quad (6.2.18)$$

Рис. 6.2.2. Треугольная и трапециевидная форма функций принадлежности

6.2.4. Нечеткая и лингвистическая логики

Данный раздел написан в соответствии с работой [б]. Детальное изложение применений нечеткой логики в конкретных практических задачах можно найти в [7,8 и др.].

Нечетким логическим выражением называется формула, в состав которой входят нечеткие предикаты. *Нечетким предикатом* назовем отображение $\boldsymbol{P^F}: \boldsymbol{X^n}$ —>[0, 1], где $\boldsymbol{X}=\{x\}$, *n* - любое натуральное число, принадлежащее отрезку [0, 1]. Число, которое предикат ставит в соответствие конкретному набору $(x_{k_1}, x_{k_2}, \dots, x_{k_n})$, где $k_i \in \overline{1,n}$, будем называть *степенью принадлежности* описываемого данным набором высказывания к множеству истинных высказываний или коротко - *степенью истинности,* Интерпретация степени истинности, как и для функции принадлежности, может быть следующей: степень истинности это вероятность того, что лицо, принимающее решение (ЛПР) назовет высказывание истинным.

Нечеткие логические выражения (или нечеткие формулы) отличаются от обычных наличием в их формулировках лингвистических и нечетких переменных и нечетких отношений (предикатов).

Приведем примеры.

1. Нечеткий предикат примерного равенства ***AE{x,y}***: $x \approx y$, где $x,y \in \boldsymbol{R^1}$.

2. Нечеткий предикат порядка ***GT{C,H): C > H,*** где ***C, H -*** нечеткие числа.

Пусть μ_1 и μ_2 - степени истинности высказываний $\boldsymbol{P_1^F}$ и $\boldsymbol{P_2^F}$ (в которые превращаются нечеткие предикаты $\boldsymbol{P_1^F}$ и $\boldsymbol{P_2^F}$ после подстановки вместо переменных $\left(x_{k_1} - x_{k_n}\right)$ элементов множества ***X***). Тогда степень истинности сложного высказывания, образованного из $\boldsymbol{P_1^F}$ и $\boldsymbol{P_2^F}$ с помощью операций дизъюнкции, конъюнкции и отрицания, может быть определена следующим образом:

$\mu(P_1^F \vee P_2^F) = \oplus(\mu_1, \mu_2);$ (6.2.19)

$\mu(P_1^F \wedge P_2^F) = \otimes(\mu_1, \mu_2);$ (6.2.20)

$\mu(\rceil P_1^F) = 1 - \mu$ (6.2.21)

Здесь операций $\oplus$ и $\otimes$ соответствуют операциям объединения и пересечения нечетких множеств. При минимаксной интерпретации функции принадлежности

$\oplus(\mu_1, \mu_2) = \max\{\mu_1, \mu_2\},$ (6.2.22)

$T : z \to \frac{\alpha z + \beta}{\gamma z + \delta}, \alpha\delta - \beta\gamma \neq 0$ (6.2.23)

Нечеткой называется логика, в которой степень истинности высказываний определяется выражениями (6.2.19)- (6.2.23).

Степень истинности более сложных высказываний можно определить, последовательно сворачивая их с учетом старшинства операций и применяя формулы (6.2.19) - (6.2.21). Задание нечетких предикатов производится путем специального опроса ЛПР или с помощью нечетких алгоритмов. В рамках нечеткой логики обобщен известный метод резолюций.

Рассмотрим условный нечеткий оператор общего вида

*если **У** то **Ф** иначе **Е***, (6.2.24)

где ***У*** - некоторое нечеткое логическое выражение (условие); ***Ф*** и ***Е*** - группы нечетких операторов (в частности, в эти группы могут входить и обычные четкие операторы). Результат выполнения условного оператора (1.24) определим выражением

У (если ***У*** то ***Ф*** иначе ***Е***) = {μ_y / ***V(Ф),*** (1 - μ_y ***)/V(E)***} (6.2.25}

где ***У***(ξ) — результат выполнения оператора ξ ; $\boldsymbol{\mu}_y$ - степень истинности условия ***У***.

Таким образом, результатом выполнения условного нечеткого оператора является нечеткое множество результатов выполнения соответствующих групп нечетких операторов. Содержательно определение (6.2.25) означает, что начинают выполняться обе группы нечетких операторов ***Ф*** и ***Е***, однако каждая группа помечается своей меткой - степенью истинности.

При необходимости однозначного определения группы операторов продолжения можно воспользоваться двумя способами.

1. Задать порог степени истинности $\gamma_0 \in (0, 1)$. Вычислить μ_y.

Тогда

$$У(\textit{если} \quad У \textit{ то } Ф \quad \textit{иначе } E) = \begin{cases} V(Ф), \textit{если} & \mu_y \geq \gamma_0; \\ V(E), \textit{если} & \mu_y < \gamma_0. \end{cases} \quad (6.2.26)$$

Здесь следует обратить внимание на значение $\gamma_0 = 0{,}5$. Оно относится к случаю, когда переход к выполнению группы нечетких операторов ***Ф*** осуществляется, если условие ***У*** более истинно, чем ложно. Увеличение γ_0 свыше 0,5 означает повышение требований к уровню определенности заключения об истинности ***У***.

2. Вычислить μ_y.. Разыграть равномерную распределенную на интервале (0, 1) случайную величину. Пусть полученное значение есть γ_0. Тогда искомый результат определяется выражением (6.2.26). Здесь μ_y рассматривается как вероятность истинности условия ***У***.

В общем случае степень истинности оказывается не числом из отрезка [0, I], а нечетким числом. Логика, в которой степени истинности являются нечеткими числами, называется *лингвистической.* Заметим, что иногда нечеткую логику называют многозначной, а лингвистическую логику - нечеткой.

Лингвистическая степень истинности (ее значения — нечеткие числа) появляется, в частности, при оценке истинности одних нечетких высказываний относительно других. Пусть имеются высказывания ***W:*** $\langle$***X*** есть ***F***$\rangle$ и ***Q:*** $\langle$***X*** есть ***G***$\rangle$, где ***F*** и ***G*** - нечеткие подмножества ***U***. Тогда истинность ***Q*** относительно ***W*** вычисляется как степень соответствия ***G*** и ***F*** [7]

$$T(W, Q) = \bigcup_{\tau \in [0,1]} \mu_T(\tau) / \tau,$$

где

$$\mu_T(\tau) = \sup_{u:\tau = \mu_G(u)} \mu_F(u).$$

Одним из элементов лингвистической логики является правило истинностной модификации утверждения, которое заключается в следующем. Пусть известно, что лингвистическая степень истинности высказывания ***Q:*** $\langle$***X*** есть ***G***$\rangle$ равна ***T***. Тогда справедливо высказывание ***W:*** $\langle$***X*** есть ***F***$\rangle$, где

$$F = \bigcup_{u \in U} \mu_F(u) / u,$$

$$u = \mu_G^{-1}(\tau), \; \mu_F(u) = \mu_T(\mu_G(u)). \quad (6.2.27)$$

В лингвистической логике вводятся операции над лингвистическими истинностями, определяемые на основе формул (6.2.19) - (6.2.23) по принципу обобщения. Операции позволяют вычислять лингвистическую степень истинности составных логических выражений.

Отдельное направление работ в лингвистической логике связано с изучением построения выводов из нечетких посылок, включающих нечеткие кванторы типа “редко”, “очень часто” и т. п. В [8] предложено решение задачи нахождения квантора φ_B по известным кванторам ρ_A и ρ_B в схеме вывода типа modus ponens

$$\frac{\rho_A A;\, A \Rightarrow \rho_B B}{\varphi_B B} \quad (6.2.28)$$

6.3 Обоснование показателя качества СЗИ

Злоумышленник с помощью некоторого источника угроз (ИУ) генерирует совокупность угроз ИС (путь она будет конечной и счетной; $i = 1,\overline{n}$). Каждая í-я угроза характеризуется вероятностью появления $P_{i\,угр}$ и ущербом $\Delta q_i^{угр}$; наносимым информационной системе.

Система защиты информации (СЗИ) выполняют функцию полной или частичной компенсации угроз для ИС. Основной характеристикой средств защиты являются вероятности устранения каждой í-й угрозы $P_{i\,угр}^{устр}$.

За счет функционирования СЗИ обеспечивается уменьшение ущерба W , наносимого ИС воздействием угроз. Обозначим общий предотвращенный ущерб ИС через $\overline{W}$, а предотвращенный ущерб за счет ликвидации воздействия i -и угрозы через $\overline{\Delta q_i}$.

После введенных обозначений сформулируем в общем виде задачу синтеза средств защиты информации в ИС: Необходимо выбрать вариант реализации СЗИ, обеспечивающий максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на СЗИ.

Формальная постановка задачи имеет вид:

$$T^0 = \arg\max \overline{W}(T)$$

найти $T^0 \in T^+$ (6.3.1)

при ограничении $C(T^0) \le C доп$ (6.3.2)

Здесь Ò -некоторый вектор, характеризующий вариант технической реализации СЗИ; $T^+ T^0$ - допустимое и оптимальное значение вектора Т;

Сдоп.- допустимые затраты на СЗИ.

Для решения задачи необходимо прежде всего сформировать показатель качества функционирования СЗИ $\overline{W}$(Т).

Очевидно, предотвращенный ущерб в общем виде выражается соотношением:

$$\overline{W} = F(P_{i\,угр}; \Delta q_i^{угр}; P_{i\,угр}^{устр}; i = 1,\overline{n}) \quad (6.3.3)$$

Предотвращенный ущерб за счет ликвидации воздействия i -й угрозы

$$\overline{\omega_i} = P_{i\,угр} \bullet \Delta q_i^{\,угр} \bullet P_{i\,угр}^{\,устр}; i = \overline{1, n}$$ (6.3.4)

При условии независимости угроз и аддитивности их последствий получаем

$$\overline{W} = \sum_{i=1}^{n} P_{i\,угр} \bullet \Delta q_i^{\,угр} \bullet P_{i\,угр}^{\,устр}$$ (6.3.5)

Остановимся более подробно на сомножителях, входящих в формулу (6.3.5).

Вероятность появления i -й угрозы $P_{i\,угр}$ определяется статистически и соответствует относительной частоте ее появления

$$P_{i\,угр} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda_i},$$ (6.3.6)

где λ_i - частота появления i -й угрозы

Ущерб, приносимый i -й угрозой Δq_i, может определяться в абсолютных единицах: экономических потерях, временных затратах, объеме уничтоженной или “испорченной” информации и т.д.

Однако, практически это сделать весьма затруднительно, особенно на ранних этапах проектирования СЗИ. Поэтому целесообразно вместо абсолютного ущерба использовать относительный ущерб, который по сути дела представляет собой степень опасности i -й угрозы для информационно-управляющей системы. Степень опасности может быть определена экспертным путем в предположении, что все угрозы для ИС составляют полную группу событий [9] , т.е.

$$0 \le \Delta q_i \le 1; \sum_{i=1}^{n} \Delta q_i = 1$$

Наиболее сложным вопросом является определение вероятности устранения i -й угрозы $P_{i\,угр}^{\,устр}$ при проектировании СЗИ. Сделаем естественное допущение, что эта вероятность определяется тем, насколько полно учтены качественные и количественные требования к СЗИ при их проектировании, т.е.

$$P_{i\,угр}^{\,устр} = fi(x_{i1}, .., x_{ij}, .., x_{im}),$$ (6.3.7)

где x_{ij} - степень выполнения j-го требования к СЗИ для устранения i -й угрозы, $i = \overline{1,n}; j = \overline{1,m}$.

Пусть первые “k” требований будут количественными $\left(j=\overline{1,k}\right)$ остальные “m-к“ – качественными $\left(j=\overline{k+1,m}\right)$.

Степень выполнения j -го количественного требования определяется его близостью к требуемому (оптимальному) значению. Для оценки степени выполнения j-го количественного требования к СЗИ удобнее всего использовать его нормированное значение $\overline{x}_{ij}, (j=\overline{1,k}), 0 \le x_{ij} < 1$.

Как показано в [10] , для нормирования удобно использовать функцию вида

$$\overline{x}_{ij} = \frac{x_{ij} - x_{ij}^{нх}}{x_{ij}^{нл} - x_{ij}^{нх}}, \quad (6.3.8)$$

где x_{ij} - текущее значение j-го требования;

$x_{ij}^{нл}, x_{ij}^{нх}$ - наилучшее и наихудшее значения.

С учетом формулы (6.3.8) получаем следующие расчетные соотношения:

при $x_{ij}^{нл} = x_{ij\max}; x_{ij}^{нх} = x_{ij\min}$

$$\overline{x}_{ij} = \frac{x_{ij} - x_{ij\min}}{x_{ij\max} - x_{ij\min}}, \quad (6.3.9)$$

при $x_{ij}^{нл} = x_{ij\min}; x_{ij}^{нх} = x_{ij\max}$

$$\overline{x}_{ij} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}}, \quad (6.3.10)$$

при $x_{ij}^{нл} = x_{ij}opt; x_{ij\,нх} = x_{ij\min}; x_{ij}^{нх} = x_{ij\max}; x_{ij\min} \le x_{ij\,opt} \le x_{ij\max}$

$$\overline{x}_{ij} = \begin{cases} 0 & при \quad x_{ij} > x_{ij\min}; x_{ij} < x_{ij\max} \\ 1 & при \quad x_{ij} = x_{ij\,opt} \\ \dfrac{x_{ij} - x_{ij\min}}{x_{ij\,opt} - x_{ij\min}} & при \quad x_{ij\min} \le x_{ij} \le x_{ij\,opt} \\ \dfrac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\,opt}} & при \quad x_{ij\,opt} \le x_{ij} \le x_{ij\max} \end{cases} \quad (6.3.11)$$

Степень выполнения $j-го$ качественного требования определяется функцией принадлежности к наилучшему значению $\mu(x_{ij})$.

Разложив функцию(6.3.7) в ряд Макларена и ограничившись лишь первыми членами ряда, получим

$$\mathrm{P}_{i\,угр}^{устр} = \mathrm{P}_{i\,угр}^{устр}(0) + \sum_{r=1}^{m} \frac{\partial \mathrm{P}_{i\,угр}^{устр}}{\partial x_{ij}} \bullet x_{ij} \quad (6.3.12)$$

где $\mathrm{P}_{i\,угр}^{устр}(0) = 0$ - вероятность устранения i -й угрозы при невыполнении требований и СЗИ;

$\dfrac{\partial \mathrm{P}_{i\,угр}^{устр}}{\partial x_{ij}} = \alpha_{ij}$ - величина, характеризующая степень влияния $j-го$ требования на вероятность устранения i -й угрозы (важность выполнения j-го требования для устранения i -й угрозы). Очевидно, что $0 \le \alpha_{ij} \le 1; \sum_{j=1}^{m} \alpha_{ij} = 1$ для $i = \overline{1,n}$.

После подстановки в (6.3.12) соответствующих значений получаем

$$\mathrm{P}_{i\,угр}^{устр} = \sum_{j=1}^{k} \alpha_{ij} \cdot \overline{x_{ij}} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}) \quad (6.3.13)$$

Окончательно формула (6.3.5) для оценки величины $\overline{W}$ предотвращенного ущерба принимает вид

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \overline{x_{ij}} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \mu(x_{ij}) \quad (6.3.14)$$

Таким образом, задача синтеза СЗИ в виде (6.3.1), (6.3.2) сводится к оптимальному обоснованию количественных и качественных требований к СЗИ при допустимых затрат и принимает вид:

Найти $\max \overline{W}(x_{ij}; i = \overline{1,n}; j = \overline{1,m}$) (6.3.15)

при ограничении $C(x_{ij}) \le Cдоп; i = \overline{1,n}; j = \overline{1,m}$

В соответствии с формулировкой задачи (6.3.15) основными этапами ее решения являются:

- сбор и обработка экспертной информации о характеристиках угроз: частоте появления i-й угрозы $\overline{\lambda_i}$ и ущербе Δq_i ($i = \overline{1,n}$);

- сбор и обработка экспертной информации для определения важности выполнения j-го требования для устранения i-й угрозы α_{ij} и функции принадлежности μ (x_{ij}), ($i = \overline{1,n}$, $j = \overline{1,m}$);
- оценка стоимости СЗИ для конкретного варианта ее реализации, зависящая от степени выполнения требований C (x_{ij}; $i = \overline{1,n}$; $j = \overline{1,m}$);
- разработка математической модели и алгоритма выбора рационального варианта построения СЗИ (рационального задания требований) в соответствии с постановкой (6.3.15) как задачи нечеткого математического программирования.

В заключение отметим, что при отсутствии информации об угрозах для решения задачи (6.3.15) может быть использован показатель вида

$$\overline{W} = \sum_{i=1}^{n}\sum_{j=1}^{k}\alpha_{ij}\cdot\overline{x_{ij}} + \sum_{i=1}^{n}\sum_{j=k+1}^{m}\alpha_{ij}\cdot\mu(x_{ij}) \qquad (6.3.16)$$

6.4 Методы определения важности требований, предъявляемых к СЗИ

При принятии решения о выборе наилучшего варианта средств защиты информации в соответствии с получением нами критерием (6.3.14) возникает задача определения важности (веса) требований, предъявляемых к параметрам СЗИ.

Наиболее полный обзор методов определения коэффициентов важности приведен в литературе [9]. В современной математической теории измерения различаются два вида измерений: в первичных школах (наименований, порядка, интервалов и т.д.) и в производных шкалах (функций полезности и частот предпочтений). Среди первичных и производных измерений выделяются два подкласса типов измерений.

1 класс - первичные измерения: 1А класс - попарные сравнения; 1Б класс - точечные оценки на шкале; 2 класс - производные измерения: 2А класс - функции ценности; 2Б класс - частоты предпочтений.

Иерархическая классификация методов определения коэффициентов важности требований в соответствии с выше изложенным подходом приведена на рис. 6.4.1.

Используя литературу [9] , проведем краткий анализ приведенных методов.

1 класс. Методы обработки информации в первичных шкалах.

1А .Методы попарного сравнения.

1А.1.Методы анализа матрицы попарного сравнения.

Эта группа методов содержит две подгруппы.

1А.1.1. Методы собственных векторов.

1А.1.1. Методы наименьших квадратов.

1А.1.1. Методы собственных векторов матрицы.

Из этой группы методов наибольшее распространение получили методы УЭЯ [10],Саати [11] и Коггера [12].

а) Метод Уэя.

Метод собственных векторов Уэя основывается на данных матрицы попарных сравнений.

$$A = \|a_{ij}\|, a_{ij} \in \{-1,0,1\}$$

где $a_{ij} = -1$ означает превосходство параметра x_j над параметром x_i, $a_{ij} = 0$ - равноценность x_i и x_j, а $a_{ij} = 1$ -превосходство параметра x_i над x_j.

Ввиду неудобства работы с отрицательными числами матрицу попарных сравнений можно превратить в неотрицательную матрицу

$$A^+ = \|a_{ij}^+\|, a_{ij} \in \{0,1,2\},$$

где числа (0,1,2) имеет вышеозначенный смысл.

Сложив числа по каждой из строк матрицы, будем иметь числовые характеристики важности параметров, а разделив их на общую сумму – получим весовые коэффициенты параметров:

$$\lambda_{ii} = \frac{\sum_{j=1}^{n} a_{ij}^+}{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^+} \quad (6.4.1)$$

Недостатком этой формулы является то, что она не учитывает важность “ничейных”(равноценности x_i и x_j) и “проигрышных” (когда x_j превосходит x_i) сравнений.

Если устранить этот недостаток, то весовыми коэффициентами по сути являются координаты собственного вектора, соответствующего максимальному характеристическому числу матрицы попарных сравнений [11].

б) Метод Саати.

Предположим, что результаты попарного сравнения параметров описываются отношениями их весов, т.е. представимы в виде матрицы А (матрицы Саати).

$$A = \|\lambda_i / \lambda_j\|; i, j \in \overline{1,n}.$$

Справедливо следующее равенство [11],

$(A - nE)\overline{\Lambda} = 0$ (6.4.2)

где E - единичная матрица; $\overline{\Lambda}$ - вектор весов.

Для нахождения вектора весов $\overline{\Lambda}$ необходимо решить уравнение (6.4.2). Поскольку ранг матрицы равен 1, то n – единственное собственное число этой матрицы и, следовательно, уравнение (6.4.2) имеет ненулевое решение. Более того, это единственное решение, обладающее свойством

$$\sum_{i=1}^{n} \lambda_i = \mathbf{1}$$

Это решение и есть искомый вектор относительных весов параметров - вектор Саати.

в) Метод Коггера и Ю.

В этом методе в качестве вектора весов берется решение уравнения

$Д^{-1}\mathrm{T}\overline{\Lambda} = \overline{\Lambda}$, (6.4.3)

где $\mathrm{T} = \left\|t_{ij}\right\|$, $t_{ij} = a_{ij}$ при $j = i$,

$t_{ij} = \mathbf{0}$;

$Д = \left\|d_{ij}\right\|, d_{ij} = n - i + 1$ при $i = j$

$d_{ij} = 0$ при $i \neq j$

Преимуществом метода является то, что он менее трудоемок в вычислительном отношении, чем метод Саати.

А.1.2. Методы наименьших квадратов.

В этом методе весовые коэффициенты определяются путем решения оптимизационного уравнения [13].

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\left(a_{ij} - \frac{\lambda_i}{\lambda_j}\right)^2 \to \min \quad (6.4.4)$$

Для решения этого уравнения используется итеративный алгоритм Марквардта [13].

1.А.2. Ранговые методы.

1.А.2.1. Методы средних рангов.

Как известно из теории квалиметрии [9], для определения весов применяется выражение

$$\lambda_i = \sum_{j=1}^{n} R_{ij}^{1} \Big/ \sum_{i=1}^{n}\sum_{j=1}^{n} R_{ij} \quad (6.4.5)$$

где R_{ij}^{1} - преобразованный ранг параметра i у эксперта j.

Преобразование R_{ij}^{1} состоит в том, что значение 0-параметр с наименьшим рангом; 1 – следующий за ним и т.д.

1.А.2.2. Методы трансформированных рангов

Эта группа методов подразделяется на две подгруппы:

-аппроксимации рангов монотонной функцией (1.А.2.2.1)

-аппроксимации ранжировки параметров системой линейных первенств(1А.2.2.2.).

1А.2.2.1.Методы аппроксимации рангов монотонной функцией.

Эта группа методов базируется на различных преобразованиях (трансформации) рангов значениями монотонно убывающих функций целочисленного аргумента

а) $\lambda_i = \lambda_n + \dfrac{n-i}{n-1}(\lambda_1 - \lambda_n)$, - в работе [14] (6.4.6)

б) $\lambda_i = \dfrac{2\left[m(n+1) - \sum\limits_{k=1}^{n} r_{ik}\right]}{mn(n+1)}$, – в работе [15] (6.4.7)

где R_{ykj}- ранг, присвоенный i -му параметру *k*-м экспертом;

n, m -число параметров СЗИ и экспертов соответственно.

в) $\lambda_i = \dfrac{y(i)}{\sum\limits_{i=1}^{n} y_i}$, где $y_i = \dfrac{i}{2^i - 1}$, - в работе [16] (6.4.8)

1.А.2.2.2. Методы аппроксимации ранжировки линейной системой неравенств.

а) Метод Черчмена-Акофа [17]

В результате попарных сравнений сумм параметров образуется система неравенств, которая определяет многогранник, любая точка внутри которого может быть принята для получения весовых коэффициентов.

б) Метод лексикографии Подиновского [18]

Задаются упорядоченные по важности параметры $(f_1, f_2, \ldots f_n)$ и лексикографическое отношение предпочтения такое, что $X > Y$ тогда и только тогда, когда

1) $f_2(x) \succ f_i(y)$

2) $f_2(x) = f_1(y), f_2(x) \succ f_2(y),$

r) $f_r(x) = f_r(y); r = 1,2,..n-1; f_n(x) \succ f_n(y)$

Для аддитивной функции

$$L(y) = \sum_{r=1}^{n} \lambda_r f_r(y) \quad (6.4.9)$$

в качестве весового коэффициента λ_n выбирается любое положительное число, остальные весовые коэффициенты λ_r, где $r = n-1, n-2,..,2,1$ определяются из неравенств:

$$\lambda_r > \frac{1}{\mu_r} \bullet \sum_{i=r+1}^{n} \lambda_i \mu_i, r = n-1, n-2, \ldots, 2,1 \quad (6.4.10)$$

где $0 < \mu_r < \varepsilon_r = \inf / f_r(x) - f_r(y)$

$x, y \in X$

$\mu \ell > d\ell = \max f_\ell(x) - \min f_\ell(x), x \in X$

Весовые коэффициенты выбираются произвольно в пределах указанных неравенств.

1Б.1. Балльные методы

Для балльных оценок вводится эталонная шкала, т.е. такая шкала, в которой мог бы быть выражен данный признак, если бы вдруг обнаружилось, что он является аддитивным или может быть выражен через другие аддитивные признаки.

Пусть задано конечное множество $A_i = \{x_1, \ldots, x_M\}$, состоящее из M вариантов, представленных комиссией из N экспертов.

Оценка каждого варианта $x_i\,(i = 1,..,N)$ имеет вид $[q_k(x_i), f_k(x_i)]$, где *k* - номер эксперта $(k = 1,..,N)$, причем $q_k(x) \le f_k(x)$. Задача состоит в построении итогового ранжирования вариантов из множества A.

Для решения єтой задачи возможно применение трех групп методов: численные методы обработки интервальных оценок, турнирные методы, аппроксимационные методы [9].

2 класс. Методы обработки и информации в произвольных шкалах.

Этот класс содержит два подкласса.

2А. Методы аппроксимации функции полезности.

2Б. Методы трансформации частот.

Эти подклассы содержат по три группы методов.

2А.1. Методы обобщенного критерия Подиновского.

2А.2. Методы функций ценности.

2А.3. Методы “уклонений”.

2Б.1. Методы трансформации частот предпочтений.

2Б.2. Методы трансформации частот отнесения к классу.

2Б.3. Методы случайных векторов (рандомизации)и, наконец, группы методов 2А.1, 2Б.1. содержит по две подгруппы, представленные на рис.6.4.1.

2А.1.1. Методы аддитивной свертки.

Эти методы можно использовать тогда, когда функция полезности представлена в аддитивной форме:

$$U\left(f_1(x),\ldots,f_n(x)\right)=\sum_{i=1}^{n}\lambda_i U_i\left(f_i(x_i)\right) \quad (6.4.11)$$

Это представление существует, если выполняются аксиомы независимости [9].

2А.1.2.Методы $\max(\min)$свертки.

Эти методы применяются тогда, когда частные параметры логически сворачиваются [19]. Комплексный критерий при этом имеет следующий вид

. $\overline{F}=\max\limits_i\left[\lambda_i f_i(x_i)\right]$ или $\underline{F}=\min\left[f_i(x_i)/\lambda_i\right]$ (6.4.12)

2А.2.1. Методы мультипликативной свертки Кини [20].

Мультипликативная функция полезности существует тогда и только тогда, когда параметры взаимно независимы по полезности

$$U\left(f_1(x),\ldots,f_n(x)\right)=\frac{1}{k}\left\{\prod_{i=1}^{n}\left[1+k\lambda_i U_i\left(f_i(x)\right)\right]-1\right\}, \quad (6.4.13)$$

где к- константа.

2А.2.2. Методы полиаддитивной свертки.

В случае независимости параметров от своего дополнения по отношению интервалов функция ценности имеет вид [20].

$\left(j = \overline{k+1, m}\right)$(6.4.14)

2А.3.1. Методы “уклонения” от идеальной точки.

а) Метод Чарнса - Купера [21].

Все параметры сводятся в обобщенный параметр, имеющий смысл расстояния от рассматриваемой оценки до некоторой идеальной точки $в^* = \left(в_1^*, в_2^*, \ldots в_n^*\right)$.

Чаще всего принимают обобщенный параметр вида

$$\Phi = \sum_{i=1}^{m} \alpha_i \left(f(x_i) - в_i^* \right) \quad (6.4.15)$$

б) Методы нормированной степенной метрики.

Целени в работе [22] используют следующую метрику

$$L_p(x) = \sum_{i=1}^{n} \lambda_i^p \left| \frac{f_i^* - f_i(x)}{f_i^* - f_{i,w}} \right|^{1/p} \quad (6.4.16)$$

где f_i^* -оптимальное значение по i -му параметру;

$f_{i,w}$ -- максимально достижимое значение по i -му параметру.

в) Метод компьютерного уклонения [20].

Компромиссная процедура решения многокритериальной задачи может быть записана в виде:

$$\max_{x \in V} k_i(x) = k_i(x) = k_i^*; i = 1,2,\ldots,S;$$

$$\min_{x \in V} \left[y, k_i^* - k_i(x) \right] \le \frac{y}{\lambda_i} \quad (6.4.17)$$

Весовые коэффициенты определяются равенствами

$$\lambda_i = \frac{1}{k_i^* - k_i}; i = 1,2,..,S:$$

$$k_i^* = \min_i k_i(x) \quad (6.4.18)$$

Критерии оптимальности состоит в минимизации компромисса У.

2А.3.2. Методы “уклонений” от точки равновесия (“статус-кво”). В этих методах применяются различные точки уклонения от точки равновесия.

А) Метод кооперативной теории игр

Метод Сцидаровского [23] использует следующий вид меры уклонения

$$q(x) = \prod_{i=1}^{n} \left[f_i(x) - f_i * \right]^{\alpha_i} \quad (6.4.19)$$

где $f_i *$ - значение i-го параметра в точке равновесия (“статус-кво”).

б) Метод теоретико-игровой [24].

В теоретико-игровой модели компромиссный вариант ищется в виде выпуклой оптимальной комбинации совокупности задач

$$C_i^{\mathrm{T}} \bullet x \to \max;\ i = 1,2....,S;$$
$$\mathrm{A}x \le \mathrm{B};\ x \ge 0;$$
$$x^1 = \sum_{i=1}^{s} \lambda_i \bullet x_i; \quad (6.4.20)$$

при $\sum_{i=1}^{s} \lambda_i = 1,\ \lambda_i \succ 0$

2Б класс. Методы трансформации частот.

2Б.1.Методы трансформации частот предпочтений.

2Б.1.1. Метод Терстоуна [25].

Метод представлен следующим алгоритмом:

Шаг 1. Составляется таблица, характеризующая число случаев, когда параметр x_i определяется как более важный, чем параметр x_j (матрица А).

Шаг 2. Строится матрица Р для выявление процентного числа случаев, когда параметр x_i оказывается более значим, чем x_j (матрица $P = \|p_{ij}\|$, где $p_{ij} = a_{ij}/c, c$ - число экспертов)

Шаг 3.Матрица Z используется для преобразования элементов матрицы P в стандартные измерители различия

$$P_{ij} = G(z_{ij}) = -\int_{-\infty}^{z_{ij}} \frac{1}{\sqrt{2\pi}} \bullet \ell^{-\frac{z^2}{2}} dz \quad (6.4.21)$$

Шаг 4. Рассчитываются

$$z_i = \sum_{j=1}^{n} z_{ij}; \overline{z_i} = \frac{1}{n} \bullet \sum_{i=1}^{n} z_i \quad (6.4.22)$$

Шаг.5. $\overline{z_i}$ преобразуется путем применения таблиц нормального распределения в процент площади нормального распределения, соответствующий значению весового коэффициента.

2Б.1.2.Метод частот предпочтений лица, принимающего решение (ЛПР) [26].

Метод использует формализм Терстоуна и отличается только видом получения исходной информации, т.е. формированием матриц A и P.

2Б.2. Методы трансформации частот принадлежности к классу (слою).

а) Метод Рознера [27].

За счет многократного предъявления параметров эксперту, который опускает их в одну из M –ячеек образуется матрица условных вероятностей $P_i(k)$, где $k = 1,2,\ldots, M; S_i(i = 1,2,..N)$-параметры.

Для определения весов используется соотношение

$$(\lambda_i - \lambda_j)^2 = f(p_i(k), p_j(k)) \quad (6.4.23)$$

Средние шкальные различия между параметрами при суммировании составляют шкалированную величину весов параметров.

2Б.3. Методы случайных векторов (рандомизации) [9].

Веса могут принимать лишь конечное множество возможных значений

$$\lambda_i \in R_N = \left\{0, \frac{1}{N}, \ldots, \frac{N-1}{N}, 1\right\},$$

где N-заданное натуральное число, $N \succ m$.

Общее число L возможных реализаций n-мерного случайного вектора также конечно, $P = (N + m - 1)$.

Считается. что вектор весов подчинен распределению Дирихле $(\lambda_1,\ldots\lambda_m)\in Д(\alpha_1,\ldots,\alpha_m)$, т.е. плотность распределения имеет вид:

$$f(\lambda_1,\ldots,\lambda_m)=\Gamma(\alpha_1,\ldots,\alpha_m)\bullet\prod_{i=1}^{m}p_i^{\alpha_i-1}\Big/\Gamma(\alpha_i) \quad (6.4.24)$$

Для любого $k\le m$ вектор весов сходится по функции распределения к случайной величине $y_1,\ldots,y_k$.

$$(\lambda_1,\ldots,\lambda_k)\to(y_1,\ldots,y_k)$$

такой, что

$$y_1,\ldots,y_k,\left(1-\sum_{i=1}^{k}y_i\right)\in Д(1,\ldots,m-k)$$

При решении практических задач обоснования требований и оценки средств защиты информации возникает естественный вопрос рационального выбора метода определения весовых коэффициентов из числа 19 групп изложенных методов. Неправильный выбор метода приводит, как правило, к недостаточной обоснованности производимых операций над малодостоверными исходными экспертными данными.

Анализ литературы [9, 19 и др.] позволяет определить основные факторы, влияющие на выбор метода оценки весовых коэффициентов. Рассмотрим эти факторы.

1.Физическая сущность параметров и отношение между ними.

Параметры (или в нашем случае требования к СЗИ) определяются исходя из смысла провозглашенной цели. Далее необходимо определить степень взаимосвязей и взаимоотношений между ними, т.е. зависимости или независимости. Характер зависимости или независимости (независимость по полезности, по предпочтению, по безразличию и т.д.) влияет на выбор метода оценки.

2.Сложность проведения экспертизы и трудоемкость получения экспертной информации.

Сложность и трудоемкость экспертизы определяется реальными условиями и возможностями ее проведения.

Как показано в [9], наименьшего времени общения с экспертами требует ранжирование и метод Терстоуна;метод линейной свертки и требует наибольшего времени общения с экспертами (в 12 раз больше, чем ранжирование; в 2 раза больше, чем метод Черчмена-Акофа)и т.д.

3.Степень согласованности мнений экспертов.

Степень согласованности в первую очередь зависит от количества привлекаемых экспертов и уровня их квалификации. В то же время на нее влияет выбранный метод оценки весов. Так, наибольшую согласованность экспертов обеспечивает линейная свертка, наименьшую – непосредственная численная оценка весов [9], при этом ранжирование при всей его простоте позволяет получить весовые коэффициенты достаточно точные и близкие к их значению, полученному методом линейной свертки.

4. Трудоемкость обработки экспертных данных.

Этот фактор не является главным при современном уровне развития вычислительной техники. Однако применение сложных методов обработки экспертной информации может потребовать разработки специальной программы обработки, что повлияет на сроки проведения экспертизы. Очевидно, что наиболее простыми методами с этой точки зрения являются ранговые методы и балльные методы.

Учет выше приведенных факторов позволяет на практике выбрать рациональный вариант оценки весовых коэффициентов.

В заключение рассмотрим пример определения коэффициентов важности требований, предъявляемых к СЗИ, на основе метода парных сравнений (метода Саати). Шкала для оценки относительной важности требований приведена в табл. 6.4.1.

Шкала относительной важности

Таблица 6.4.1

Интенсивность относительной важности	Определение
1	Равная важность сравниваемых требований
3	Умеренное (слабое) превосходство одного над другим
5	Сильное (существенное) превосходство
7	Очевидное превосходство
9	Абсолютное (подавляющее) превосходство
2, 4, 6, 8	Промежуточные решения между двумя соседними оценками

Пусть необходимо определить относительную важность четырех требований (параметров СЗИ). В результате экспертного опроса получена следующая матрица парных сравнений:

$$A = \begin{Vmatrix} 1 & 5 & 6 & 7 \\ 1/5 & 1 & 4 & 6 \\ 1/6 & 1/4 & 1 & 4 \\ 1/7 & 1/6 & 1/4 & 1 \end{Vmatrix}$$

Как следует из соотношения (6.4.2), необходимо решить задачу нахождения собственных значений (A - λ E)· W = 0, где W- собственный вектор, а λ - собственное значение матрицы. Эта неоднородная система имеет нетривиальное решение тогда и только тогда, когда определитель матрицы A - λ E равен нулю. Найдем его

$$\begin{vmatrix} 1-\lambda & 5 & 6 & 7 \\ 1/5 & 1-\lambda & 4 & 6 \\ 1/6 & 1/4 & 1-\lambda & 4 \\ 1/7 & 1/6 & 1/4 & 1-\lambda \end{vmatrix} = \lambda^4 - 4\lambda^3 - 6{,}914\lambda - 2{,}715 = 0$$

Уравнение имеет решение

$\lambda_1 = -0{,}362$; $\lambda_2 = -0{,}140 + 1{,}305i$; $\lambda_3 = -0{,}140 - 1{,}305i$; $\lambda_4 = 4{,}390$.

Следовательно, $\lambda_{max} = 4{,}390$. Найдем соответствующий вектор:

$$\begin{Vmatrix} 1-4{,}390 & 5 & 6 & 7 \\ 1/5 & 1-4{,}390 & 4 & 6 \\ 1/6 & 1/4 & 1-4{,}390 & 4 \\ 1/7 & 1/6 & 1/4 & 1-4{,}390 \end{Vmatrix} \cdot \begin{Vmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{Vmatrix} = 0$$

Введем условие нормировки $a_1 + a_2 + a_3 + a_4 = 1$. Рассмотрим систему

$$\begin{cases} -3{,}390a_1 + 5a_2 + 6a_3 + 7a_4 = 0 \\ 0{,}2a_1 - 3{,}390a_2 + 4a_3 + 6a_4 = 0 \\ 0{,}166a_1 + 0{,}25a_2 - 3{,}390a_3 + 4a_4 = 0 \\ 0{,}142a_1 + 0{,}166a_2 + 0{,}25a_3 - 3{,}390a_4 = 0 \end{cases} \quad (*)$$

Система (*) имеет только нулевое решение. Для нахождения собственного вектора W используется замена одного из уравнений (*) условием нормировки. В результате решения системы получаем собственный вектор весов W = (a_1, a_2, a_3, a_4),
$a_1 = 0{,}619,\ a_2 = 0{,}235,\ a_3 = 0{,}101,\ a_4 = 0{,}045$.

Отметим, что матрица парных сравнений отражает согласованные суждения тогда и только тогда, когда $\lambda_{max} = n$. Кроме того, всегда $\lambda_{max} \geq n$, поэтому $\lambda_{max} - n$ дает меру несогласованности и указывает, когда суждение экспертов следует проверить. В рассмотренном примере при n=4 $\lambda_{max} = 4{,}390$ мера несогласованности равна 0,6390, что является допустимым при принятой шкале (табл. 6.4.1).

Как следует из примера, определение весовых коэффициентов с помощью похождения вектора W матрицы парных сравнений является довольно трудоемкой задачей. Для решения практических задач некоторые авторы [5, 8] предлагают определить весовые коэффициенты путем расчета среднего геометрического из соотношения

$$a_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}};\ i = \overline{1,n}$$, (6.4.25)

где a_{ij} - коэффициенты матрицы парных сравнений.

В нашем примере получаем: $\omega_1 = 0{,}614,\ \omega_2 = 0{,}239,\ \omega_3 = 0{,}103,\ \omega_4 = 0{,}044$.

Ошибки определения весовых коэффициентов в данном примере не превышают 5%, что говорит о возможности применения метода.

6.5 Методы построения функции принадлежности требований к СЗИ заданному уровню качества

Существует значительное количество методов построения по экспертным оценкам функций принадлежности нечеткого множества $\mu^A(x)$. Выделяют две группы методов: прямые и косвенные методы [4].

Прямые методы характеризуются тем, что эксперт непосредственно задает правила определения значений функции принадлежности $\mu^A(x)$, характеризующей элемент x. Эти значения согласуются с его предпочтениями на множестве элементов X следующим образом:

1. для любых $x_1, x_2 \in X$ $\mu^A(x_1)<\mu^A(x_2)$ тогда и только тогда, когда x_2 предпочтительнее x_1, т.е. в большей степени характеризуется свойством А;
2. для любых $x_1, x_2 \in X$ $\mu^A(x_1)=\mu^A(x_2)$ тогда и только тогда, когда x_1 и x_2 безразличны относительно свойства А.

Примерами прямых методов являются непосредственное задание функции принадлежности таблицей, графиком или формулой. Недостатком этой группы методов является большая доля субъективизма.

В косвенных методах значения функции принадлежности выбираются таким образом, чтобы удовлетворить заранее сформулированным условиям. Экспертная информация является только исходной информацией для дальнейшей обработки. Дополнительные условия могут налагаться как на вид получаемой информации, так и на процедуру обработки. Дадим краткую характеристику наиболее часто используемых косвенных методов построения функций принадлежности.

6.5.1 Построение функций принадлежности на основе парных сравнений [4].

Метод основан на обработке матрицы оценок, отражающих мнение эксперта об относительной принадлежности элементов множеству или степени выраженности у них некоторого оцениваемого свойства.

Потребуем, чтобы для всех элементов множества А выполнялось равенство

$$\sum_{i=1}^{n} \mu^A(x_i) = 1 \qquad (6.5.1)$$

Степень принадлежности элементов множеству А будем определять посредством парных сравнений. Для сравнения элементов используются оценки, приведенные в таблице 6.4.1.

Оценку элемента x_i по сравнению с элементом x_j с точки зрения свойства А обозначим через a_{ij}. Для обеспечения согласованности примем $a_{ij} = 1/a_{ji}$. Оценки a_{ij} составляют матрицу $S = \| a_{ij} \|$.

Найдем $W = (w_1,...,w_n)$ – собственный вектор матрицы S, решая уравнение

$$S \cdot W = \lambda \cdot W \text{, (6.5.2)}$$

где λ – собственное значение матрицы S.

Вычисленные значения, составляющие собственный вектор W, принимаются в качестве степени принадлежности элемента x к множеству A: $\mu^A(x_i) = w_i$; $i = \overline{1,n}$. Так как всегда выполняется равенство $S \cdot W = n \cdot W$, то найденные значения тем точнее, чем ближе λ_{max} к n. Отклонение λ_{max} от n может служить мерой согласованности мнений экспертов.

6.5.2 Построение функций принадлежности с использованием статистических данных

Предположим, что наблюдая за объектом в течение некоторого времени, человек n раз фиксирует свое внимание на том, имеет место факт А или нет. Событие, заключающееся в n проверках наличия факта А будем называть оценочным [28]. Пусть в k проверках имел место факт А. Тогда эксперт регистрирует частоту p=k/n появления факта А и оценивает ее с помощью слов “часто”, “редко” и т.п.

На универсальной шкале [0,1] необходимо разместить значения лингвистической переменной: Весьма редко, более – менее редко, более менее часто, весьма часто. Тогда степень принадлежности некоторого значения вычисляется как отношение числа экспериментов, в которых оно встречалось в определенном интервале шкалы, к максимальному для этого значения числу экспериментов по всем интервалам. Метод требует выполнения условия, чтобы в каждый интервал шкалы попадало одинаковое число экспериментов. Если это условие не выполняется, требуется дополнительная обработка экспериментальных данных с помощью так называемой матрицы подсказок [28].

6.5.3 Построение функций принадлежности на основе экспертных оценок [4].

Рассмотрим особенности построения функций принадлежности для приближенных точечных (например, X приблизительно равен 10) и интервальных оценок (вида X находится приблизительно в интервале от 8 до 11). На рис 6.5.1. изображены функции принадлежности множеств, которые соответствуют этим оценкам.

Рис. 6.5.1 Функции принадлежности нечетких множеств соответствующих приближенной точечной оценке

Естественно предположить, что функцию, представленную на рис. 6.5.1б, необходимо строить следующим образом:

если $\alpha \le x \le \beta$, то $\mu_{(\alpha, \beta)}(x) = 1$;

если $x < \alpha$, то $\mu_{(\alpha, \beta)}(x) = \mu_\alpha(x)$;

если $x < \beta$, то $\mu_{(\alpha,\beta)}(x) = \mu_\beta(x)$,

где $\mu_{(\alpha,\beta)}(x)$ – функция принадлежности нечеткому интервалу (α, β);

$\mu_\alpha(x)$ и $\mu_\beta(x)$ – функции принадлежности нечетким множествам чисел, приближенно равных соответственно α и β. Они строятся аналогично функции, график которой приведен на рис. 6.5.1а.

При построении функции принадлежности чисел, приблизительно равных некоторому k, можно использовать функцию [4]

$$\mu_k(x) = e^{-\alpha(k-x)^2}, \quad (6.5.3)$$

где α зависит от требуемой степени нечеткости $\mu_k(x)$, и определяется из выражения

$$\alpha = \frac{4\ln 0{,}5}{\beta^2} \quad (6.5.4)$$

где β - расстояние между точками перехода для $\mu_k(x)$, т.е. точками, в которых функция вида (6.5.3) принимает значение 0,5. На рис. 6.5.1а) эти точки обозначены а и б.

Таким образом, задача построения $\mu_k(x)$ для некоторого числа сводиться к отысканию параметров а и в, чтобы можно было определить β (x), с помощью $\beta(x) - \alpha\ \theta$, используя α, построить $\mu_k(x)$.

6.5.4 Параметрический подход к построению функций принадлежности [29]

Описываемый метод построения функций принадлежности основан на предположении, что эксперт характеризуя лингвистическое значение какого-либо признака, с минимальным напряжением может указать три точки шкалы: А, В, С, из которых В и С – точки, по его мнению, еще (или уже) не принадлежащие описываемому лингвистическому значению, А – точка, определенно принадлежащая ему.

Пусть имеются параметрическое описание термов t и t^I двух значений некоторой лингвистической переменной. Один из термов может представлять собой модификацию (ограничение) другого: $t^I = h(t)$, где h – ограничение на t типа ДОВОЛЬНО, БОЛЕЕ – МЕНЕЕ, НЕ ОЧЕНЬ и т.п. Задача состоит в том, чтобы используя параметры термов t: (z_1, z_2, z_3) и t^I: $(\omega_1, \omega_2, \omega_3)$ описать переход от t к t^I (параметры считаются упорядоченными отношением “меньше”).

Основные виды функций принадлежности приведены на рис.6.5.2.

Рис.6.5.2 Параметрическое задание термов

Очевидно, что S – образную функцию (рис. 6.5.2 б,в) можно рассматривать, как вырожденный случай треугольной функции (рис. 6.5.2 а), в которой один из параметров z_1 или z_2 стремится к бесконечности. Таким образом, задача состоит в том, чтобы описать переход между любыми двумя формами, представленными на рис. 6.5.2.

Для решения этой задачи используется аппарат автоморфных функций. Рассмотрим дробно-линейное отображение прямой на себя вида

$$T: x \to \frac{\alpha x + \beta}{\gamma x + \delta}, \alpha\delta - \beta\gamma \neq 0$$ (6.5.5)

преобразование T^{-1}, обратное T, получается, если уравнение $Z = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}$ разрешить относительно ω:

$$T^{-1}: \omega = \frac{-\delta z + \beta}{\gamma z - \alpha}$$ (6.5.6)

Таким образом, при параметрическом представлении функций принадлежности задача описания перехода от одного терма t: (z_1, z_2, z_3) к другому t^I: $(\omega_1, \omega_2, \omega_3)$ решается непосредственным подсчетом четырех параметров – коэффициентов дробно-линейного преобразования по формулам [4]

$$\begin{aligned}
\alpha &= z_1 z_2(\omega_1 - \omega_2) + z_1 z_3(\omega_3 - \omega_1) + z_2 z_3(\omega_2 - \omega_3);\\
\beta &= \omega_1\omega_2 z_2(z_1 - z_2) + \omega_1\omega_3 z_2(z_3 - z_1) + \omega_2\omega_3 z_1(z_2 - z_3);\\
\gamma &= z_2(\omega_1 - \omega_3) + z_1(\omega_3 - \omega_2) + z_3(\omega_2 - \omega_1);\\
\delta &= \omega_1\omega_2(z_1 - z_2) + \omega_1\omega_3(z_3 - z_1) + \omega_2\omega_3(z_2 - z_3)
\end{aligned}$$ (6.5.7)

Эти же коэффициенты при подстановке в (6.5.6) определяют обратный переход от t^I к t

Рассмотрим теперь переход от терма t треугольной формы к терму t^I с S – образной функцией принадлежности. Для дробно-линейных преобразований этому случаю соответствует переход от одной из крайних заданных точек в положение бесконечно-удаленной точки.

Если $z_1 = \infty$ (переход от рис. 6.5.2,а к рис.6.5.2,в), то параметры дробно-линейного преобразования

$$\begin{aligned}
\alpha &= z_2(\omega_2 - \omega_1) + z_3(\omega_2 - \omega_3);\\
\beta &= \omega_2 z_3(\omega_3 - \omega_1) + \omega_3 z_2(\omega_1 - \omega_2);\\
\gamma &= \omega_2 - \omega_3;\ \delta = \omega_1(\omega_3 - \omega_2)
\end{aligned}$$ (6.5.8)

Если $z_3 = \infty$ (переход от рис. 6.5.2.,а к рис.6.5.2.,б), то

$$\begin{aligned}
\alpha &= z_2(\omega_1 - \omega_3) + z_2(\omega_3 - \omega_2);\\
\beta &= \omega_1 z_2(\omega_2 - \omega_3) + \omega_2 z_1(\omega_3 - \omega_1);\\
\gamma &= \omega_1 - \omega_2;\ \delta = \omega_3(\omega_2 - \omega_1)
\end{aligned}$$ (6.5.9)

Рассмотрим случай, когда функции принадлежности представляются S – образной или просто наклонной кривой. В этом случае имеет место линейное отображение прямой

$$x_i \in R_y = \left[0, \frac{1}{N}, \ldots, \frac{N-1}{N}, 1\right]$$ (6.5.10)

Параметры преобразования (6.5.10)

$$\alpha = \frac{y_1 - y_2}{x_2 - x_1};\ \beta = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \quad (6.5.11)$$

Обратный переход (y → x) осуществляется по формуле

$$x = \frac{1}{\alpha} \cdot y + \left(-\frac{\beta}{\alpha}\right) \quad (6.5.12)$$

6.5.5 Построение функции принадлежности на основе ранговых оценок [5]

Данный метод разработан А.П. Ротштейном и базируется на идее распределения степени принадлежности элементов универсального множества согласно с их рангами.

Будем понимать под рангом элемента $x_{i\in}$ X число $r_s(x_i)$, которое характеризует значимость этого элемента в формировании свойства, которое описывается нечетким термом $\overline{S}$. Допускаем, что выполняется правило: чем больший ранг элемента, тем больше степень принадлежности.

Тогда правило распределения степеней принадлежности можно задать в виде соотношения:

$$\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} = \ldots = \frac{\mu_n}{r_n} \quad (6.5.13)$$

к которому добавляется условие нормирования

Используя соотношение (6.5.13) легко определить степени принадлежности всех элементов универсального множества через степени принадлежности опорного элемента.

Если опорным элементом является элемент $x_1 \in X$ с принадлежностью μ_1, то

$$\mu_2 = \frac{r_2}{r_1} \cdot \mu_1; \mu_3 = \frac{r_3}{r_1} \cdot \mu_1; \ldots; \mu_n = \frac{r_n}{r_1} \cdot \mu_1 \quad (6.5.15)$$

Для опорного элемента $x_2 \in X$ с принадлежностью μ_2, получаем

$$\mu_2 = \frac{r_1}{r_2} \cdot \mu_2; \mu_3 = \frac{r_3}{r_2} \cdot \mu_2; \ldots; \mu_n = \frac{r_n}{r_2} \cdot \mu_2 \quad (6.5.16)$$

Для опорного элемента $x_n \in X$ с принадлежностью μ_n, имеем

$$\mu_1 = \frac{r_1}{r_n} \cdot \mu_n; \mu_2 = \frac{r_2}{r_n} \cdot \mu_n; \ldots; \mu_{n-1} = \frac{r_{n-1}}{r_n} \cdot \mu_n \quad (6.5.17)$$

Учитывая условие нормировки (6.5.14) из соотношений (6.5.15) – (6.5.17) находим:

$$\left.\begin{aligned} &\mu_1 = \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \ldots + \frac{r_n}{r_1}\right)^{-1} \\ &\mu_1 = \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} \ldots + \frac{r_n}{r_2}\right)^{-1} \\ &\ldots\ldots \\ &\mu_n = \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \ldots + 1\right)^{-1} \end{aligned}\right\} \quad (6.5.18)$$

Полученные формулы (6.5.18) дают возможность вычислять степени принадлежности $\mu_S(x_i)$ двумя независимыми путями:

1. по абсолютным оценкам уровней r_i, $i = \overline{1,n}$, которые определяются по 9-ти бальной шкале (1 – наименьший ранг, 9 – наибольший ранг).
2. по относительным оценкам рангов $\frac{r_i}{r_j} = a_{ij}, i, j = \overline{1,n},$

которые образуют матрицу:

$$A = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \frac{r_3}{r_1} & \ldots & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \frac{r_3}{r_2} & \ldots & \frac{r_n}{r_2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \frac{r_3}{r_n} & \ldots & 1 \end{bmatrix} \quad (6.5.19)$$

Эта матрица обладает следующими свойствами:

а) она диагональная, т.е. $a_{ii}=1$ $i = \overline{1,n}$;

б) элементы, которые симметричны относительно главной диагонали, связаны зависимостью: $a_{ij}=1/a_{ji}$;

в) она транзитивна, т.е. $a_{ik} \cdot a_{kj}$, поскольку

$$\frac{r_i}{r_k} \cdot \frac{r_k}{r_j} = \frac{r_i}{r_j}$$

Наличие этих свойств приводит к тому, что при известных элементах одной строки матрицы А легко определить элементы всех других строк. Если известна r-я строка, т.е. элементы a_{kj}, k, $j=\overline{1,n}$, то произвольный элемент a_{ij} находиться так

$$a_{ij} = a_{kj}/a_{ki};i,j=\overline{1,n}.$$

Поскольку матрица (6.5.19) может быть интерпретирована как матрица парных сравнений рангов, то для экспертных оценок элементов этой матрицы можно использовать 9 – ти бальную шкалу Саати: $a_{ij} = r_i/r_j$. Эта шкала приведена ранее, в табл. 6.4.1.

Таким образом, с помощью полученных формул (6.5.18), экспертные значения о рангах элементов или их парные сравнения преобразуются в функцию принадлежности нечеткого терма.

Алгоритм построения функции принадлежности включает в себя следующие операции:

1^0. Задать лингвистическую переменную;

2^0. Определить универсальное множество, на котором задается лингвистическая переменная;

3^0. Задать совокупность нечетких термов $\{S_1, S_2, \ldots, S_m\}$, которые используются для оценки переменной;

4^0. Для каждого терма S_j, $j=\overline{1,m}$ сформировать матрицу (6.5.19);

5^0. Используя формулы (6.5.18) вычислить элементы функций принадлежности для каждого терма.

Нормирование найденных функций осуществляется путем деления на наибольшие степени принадлежности.

Главным преимуществом метода является то, что в отличие от метода парных сравнений, он не требует решения характеристического уравнения. Полученные соотношения дают возможность вычислять функции принадлежности с использованием ранговых оценок, которые достаточно легко получить при экспертном опросе.

Кроме описанных методов построения функций принадлежности, нашедших наиболее широкое практическое применение, имеется еще значительное число методов, описанных в литературе [4] (метод интервальных оценок, метод семантического дифференциала и т.д.).

При выборе метода необходимо учитывать, как правило, сложность получения экспертной информации, особенно организации и проведения экспертизы, достоверность экспертной информации, трудоемкость алгоритма обработки информации при построении функции принадлежности.

В нашем случае функция принадлежности μ ($x_{i,j}$), входящая в формулу (6.3.14) для оценки качества системы защиты информации, характеризует лингвистическую переменную “степень выполнения j-го требования к СЗИ при защите от i-ой угрозы”. В заключение рассмотрим пример построения функции принадлежности μ (x_{ij})=μ (x_i) методом Ротштейна.

Рассмотрим лингвистическую переменную “ качество СЗИ”, характеризуемое степенью выполнения некоторого требования. Эта лингвистическая переменная определена на универсальном множестве вариантов СЗИ: x_i, $i = \overline{1,5}$. Уровень качества СЗИ будем оценивать такими нечеткими термами: Н – низкий; С – средний; В – высокий.

Пусть в результате экспертного опроса сформированы матрицы (6.5.19) для каждого терма. При сравнении вариантов используется табл. 6.4.1.

A_H =

	x_1	x_2	x_3	x_4	x_5
x_1	1	7/9	5/9	3/9	1/9
x_2	9/7	1	5/7	3/7	1/7
x_3	9/5	7/5	1	3/5	1/5
x_4	9/3	7/3	5/3	1	1/3
x_5	9	7	5	3	1

A_B =

	x_1	x_2	x_3	x_4	x_5
x_1	1	3	5	7	9
x_2	1/3	1	5/3	7/3	9/3
x_3	1/5	3/5	1	7/5	9/5
x_4	1/7	3/7	5/7	1	9/7
x_5	1/9	3/9	5/9	7/9	1

A_C =

	x_1	x_2	x_3	x_4	x_5
x_1	1	7/5	9/5	7/5	1
x_2	5/7	1	5/7	1	5/7
x_3	5/9	7/9	1	7/9	5/9
x_4	5/7	1	9/7	1	5/7
x_5	1	7/5	9/5	7/5	1

После обработки этих матриц по формулам (6.5.18) получим функции принадлежности, которые в нормированном виде приведены на рис. 6.5.3.

Рис. 6.5.3 Функции принадлежности нечетких множеств.

6. 6 Методы выбора рационального варианта средств защиты информации на основе экспертной информации

6.6.1 Анализ методов решения задачи выборки рационального варианта СЗИ

Принципиальными особенностями решения задачи выбора рационального варианта СЗИ, определяющими метод ее решения являются:

- многокритериальность задачи выбора;
- не только количественное, но и качественное (нечеткое) описание показателей качества СЗИ, задаваемых в виде требований;
- при нечеткой постановке задачи влияние на выбор метода ее решения экспертной информации, определяющей предпочтение того или иного показателя.

Рассмотрим указанные особенности решения задачи более подробно.

Общая постановка задачи многокритериальной оптимизации имеет следующий вид [8].

Пусть $\overline{X} = |x_1,\dots, x_i,\dots,x_n|$ - вектор оптимизируемых параметров некоторой системы S. Некоторое j-е свойство системы S характеризуется величиной j-го показателя $q_i(\overline{X});\ j = \overline{1,m}$. Тогда система в целом характеризуется вектором показателей $\overline{Q} = |q_1,\dots, q_j,\dots, g_m|$. Задача многокритериальной оптимизации сводится к тому, чтобы из множества M_s вариантов системы S выбрать такой вариант (систему S_0), который обладает наилучшим значением вектора $\overline{Q}$. При этом предполагается. Что понятие “наилучший вектор $\overline{Q}$” предварительно сформулированно математически, т.е. выбран (обоснован) соответствующий критерий предпочтения (отношение предпочтения).

Анализ литературы [] показывает, что все многочисленные методы решения многокритериальных задач можно свести к трем группам методов:

- метод главного показателя;
- метод результирующего показателя;
- лексикографические методы (методы последовательных уступок).

Кратко рассмотрим суть этих методов решения многокритериальных задач.

Метод главного показателя основан на переводе всех показателей качества, кроме какого-либо однородного, называемого главным, в разряд ограничений типа равенств и неравенств. Присвоим главному показателю номер $q_1(S)$. Тогда задача сводится к однокритериальной задаче выбора системы $S\in M_s$, обладающей минимальным значением показателя $q_1(S)$ при наличии ограничений типа равенств и неравенств, т.е. имеет вид

$$\min_{S\in M_s} q_1(S) \quad (6.6.1)$$

при ограничениях

$$q_j(S) = q_{j0};\ j = 2,\dots,l;$$
$$q_k(S) \le q_{k0};\ k = l+1,\dots,p;$$
$$q_r(S) \ge q_{r0};\ r = p+1,\dots,m; \quad (6.6.2)$$

Методу главного показателя присущи следующие недостатки:

1. В большинстве случаев нет достаточных оснований для того, чтобы считать какой-то один и притом вполне определенный показатель качества является главным, а все остальные – второстепенными.
2. Для показателей качества $q_2(S)$, ..., $q_m(S)$, переводимых в разряд ограничений, достаточно трудно установить их допустимые значения.

Метод результирующего показателя качества основанна формировании обобщенного показателя путем интуитивных оценок влияния частных показателей качества q_1, ..., q_m на результирующее качество выполнения системой ее функций. Оценки такого влияния даются группой специалистов – экспертов, имеющих опыт разработки подобных систем.

Наибольшее применение среди результирующих показателей качества получили аддитивный, мультипликативный и минимаксный показатели.

Аддитивный показатель качества представляет собой сумму взвешенных нормированных частных показетелей и имеет вид

$$Q = \sum_{j=1}^{m} \omega_j \overline{q_j}$$, (6.6.3)

где $\overline{q_j}$ - нормированное значение j-го показателя;

ω $_j$ – весовой коэффиициент j-го показателя, имеющий тем большую величину, чем больше он влияет на качество системы; $\sum_{j=1}^{m} \omega_j = 1;\ \omega_j > 0;\ j = \overline{1,m}$.

Обобщенный аддитивный показатель для средств защиты информации приведен в разд....., а методы определения весовых коэффициентов рассмотрены в разд....

Гланым недостатком аддитивного показателя является то, что при его применении может происходить взаимная компенсация частных показателей. Это значит, что уменшение одного из показателей вплоть до нулевого значения может быть компенсировано возрастанием другого показателя. Для ослабления этого недостатка вводятся специальные ограничения на минимальные значения частных показателей, на их веса и другие приемы [].

Мультипликативный показатель качества образуется путем перемножения частных показателей с учетом их весовых коэффициентов и имеет вид

$$Q = \prod_{j=1}^{m} \overline{q_j}^{\omega_j}$$, (6.6.4)

где $\overline{q_j}$ и ω $_j$ имеет тот же смысл, что и в аддитивном показателе.

Наиболее существенное отличие мультипликативного показателя от аддитивного заключается в том, что аддитивный показатель базируется на принципе справедливой абсолютной уступки по отдельным показателям, а мультипликативный – на принципе справедливой относительной уступки []. Суть последнего заключается в том что справедливым считается такой компромисс, когда суммарный уровень относительного снижения одного или нескольких показателей не превышает суммарного уровня относительного увеличения остальных показателей.

Максиминный показатель. В ряде случаев вид результирующей целевой функции достаточно трудно обосновать или применить. В подобных случаях возможным простым путем решения задачи является применение максиминного показателя. Правило выбора оптимальной системы S_0 в этом случае имеет следующий вид

$$\max_{S \in M_s} \min_{1 \le j \le m} \left\{ \overline{q_1}(S), \ldots, \overline{q_j}(S), \ldots, \overline{q_m}(S) \right\}$$, (6.6.5)

если весовые коэффициенты частных показателей отсутствуют;

$$\max_{S \in M,\ 1 \le j \le m} \min \left\{ \overline{q_1}^{\,\omega_1}(S), \ldots, \overline{q_j}^{\,\omega_j}(S), \ldots, \overline{q_m}^{\,\omega_m}(S) \right\}, \quad (6.6.6)$$

если весовые коэффициенты определены.

Максиминный показатель обеспечивает наилучшее (наибольшее) значение наихудшего (наименьшего) из частных показателей качества.

Лексикографический метод.

Предположим, что показатели упорядочены по важности, например, $q_1 (S)>q_2 (S)>...> q_m (S)$.

Суть метода заключается в выделении сначала множества альтернатив с наилучшей оценкой по наиболее важному показателю. Если такая альтернатива единственная, то она считается наилучшей; если их несколько, то из их подмножества выделяются те, которые имеют лучшую оценку по второму показателю и т.д.

Для расширения множества рассматриваемых альтернатив и улучшения качества решения по совокупности показателей может назначаться уступка, в пределах которой альтернативы считаются эквивалентными.

Принципиальной особенностью рассматриваемой задачи выбора рационального варианта СЗИ является преимущественно качественный характер показателей, трактуемых как требования, задаваемые к СЗИ. В связи с этим рассматриваемые методы многокритериальной оптимизации должны формулироваться в нечеткой постановке. В этом случае показатели качества представляют собой функции принадлежности вариантов СЗИ заданному уровню качества.

Как в классической, так и в нечеткой постановке выбор метода решения многокритериальной задачи определяется тем, в каком виде представлена экспертная информация о предпочтении показателей или их важности. Поэтому в заключение этого раздела приведем таблицу, которая позволяет обоснованно выбирать метод нечеткой многокритериальной оптимизации в зависимости от экспертной информации о предпочтении показателей (табл. 6.6.1).

Таблица 6.6.1

Экспертная информация о степени предпочтения или важности показателей	Метод решения многокритериальной задачи
отсутствует	максиминный метод (6.6.5)
показатели упорядочены по важности	лексикографический метод
определены весовые коэффициенты показателей	1. аддитивный показатель (6.6.3) 2. мультипликативный показатель (6.6.4) 3. максиминный показатель (6.6.6)

Используя рекомендации по выбору метода решения, в дальнейшем рассмотрим ряд конкретных методов и примеров решения задачи многокритериальной оптимизаци СЗИ в нечеткой постановке.

6.6.2 Выбор варианта СЗИ при равной важности требований

Пусть имеется множество из m вариантов построения СЗИ

$A = \{a_1, a_2, ..., a_m\}$

Для некоторого требования C (критерия оценки) может быть рассмотрено нечеткое множество

$$C = \{\mu_c(a_1)/a_1; \mu_c(a_2)/a_2; ..., \mu_c(a_m)/a_m\} \quad (6.6.7)$$

где $\mu_c(a_i) \in [0,1]$ - оценка варианта a_i по критерию C, которая характеризует степень соответствия варианта требованию определенному критерием C.

Если имеется n требований: $C_1, C_2, ..., C_n$ $j = \overline{1,n}$, то лучшим считается вариант, удовлетворяющий и требованию C_1, иC_2, ..., иC_n. Тогда правило для выбора наилучшего варианта может быть записано в виде пересечения соответствующих множеств:

$$D = C_1 \cap C_2 \cap ... \cap C_n \quad (6.6.8)$$

Операции пересечения нечеткого множества соответствует операция min, выполняемая над их функциями принадлежности:

$$\mu_D(a_j) = \min_{i=\overline{1,n}} \mu_{c_i}(a_j), j = \overline{1,m} \quad (6.6.9)$$

В качестве лучшего выбирается вариант a^*, имеющий наибольшее значение функции принадлежности

$$\mu_D(a^*) = \max_{j=\overline{1,m}} \mu_D(a_j) \quad (6.6.10)$$

Рассмотрим пример выбора варианта построения СЗИ при равной важности требований.

Для определенности рассмотрим задачу выбора средств защиты применительно к защите процессов и программ. Основными требованиями при выборе являются следующие требования:

- к базе (полнота отражения в законодательных, нормативных и методических документах вопросов, определяющих выбор СЗИ в процессах и программах информационной системы);
- к структуре (степень квалификации сотрудников, ответственных за разработку СЗИ);
- к полноте и обоснованности мероприятий, обеспечивающих разработку СЗИ качественно и в заданные сроки;

- к составу и характеристикам технических средств разработки СЗИ, имеющихся в распоряжении разработчика.

Пусть имеется 3 претендента - исполнителя проекта СЗИ в процессах и программах информационной системы. Претенденты оцениваются по 4 требованиям (критериям), описанным выше: C_1 - база, C_2 - структура, C_3 - меры, C_4 - средства.

В результате экспертной оценки получили следующие данные, характеризующие степень соответствия исполнителей заданным требованиям:

$C_1 = \{0{,}9/a_1; 0{,}7/a_2; 0{,}8/a_3\}$;

$C_2 = \{0{,}8/a_1; 0{,}9/a_2; 0{,}6/a_3\}$;

$C_3 = \{0{,}7/a_1; 0{,}8/a_2; 0{,}9/a_3\}$;

$C_4 = \{0{,}8/a_1; 0{,}6/a_2; 0{,}7/a_3\}$.

В соответствии с правилом выбора получаем:

$D = \{ \min (0{,}9; 0{,}8; 0{,}7; 0{,}8/a_1)$;

$\min (0{,}7; 0{,}9; 0{,}8; 0{,}6/a_2)$;

$\min (0{,}8; 0{,}6; 0{,}9; 0{,}7/a_3)\}=$

$= \{0{,}7/a_1; 0{,}6/a_2; 0{,}6/a_3\}$.

Из правила (6.6.4) следует, что наилучшим является первый исполнитель проекта

$a_1 = \{0{,}9; 0{,}8; 0{,}7; 0{,}8\}$.

6.6.3 Выбор варианта СЗИ при различной важности требований

В случае, если требования С имеют различную важность, каждому из них приписывается число $\alpha_i \geq 0$ (чем важнее требование, тем больше α_i) и общее правило выбора принимает вид [4]

$$D = C_1^{\alpha_1} \cap C_2^{\alpha_2} \cap \ldots \cap C_n^{\alpha_n} \quad (6.6.11)$$

$$\mu^{\neg A}(x) = 1 - \mu^{A}(x), \forall x \in X \quad (6.6.12)$$

Лучший вариант a^* находится из соотношения

$$\mu_D(a^*) = \max_{j=\overline{1,m}} \min_{i=\overline{1,n}} \mu_{C_i}(a_j) \quad (6.6.13)$$

Коэффициенты относительной важности α_i находятся в соответствии с методикой, описанной в разделе 6.4.

Рассмотрим в качестве примера выбор варианта при решении задачи защиты объектов информационной системы с точки зрения выявления потенциальных каналов утечки информации.

Пусть имеется два варианта решения задачи защиты объектов ИС (a_1, a_2). Варианты оцениваются по тем же требованиям: C_1 - база, C_2 - структура, C_3 - меры, C_4 - средства. Важность требований определена: $\alpha_1 = 0{,}15$; $\alpha_2 = 0{,}2$; $\alpha_3 = 0{,}25$; $\alpha_4 = 0{,}4$.

Нечеткие множества, характеризующие альтернативные варианты, имеют вид

$C_1 = \{0{,}9/a_1;\ 0{,}7/a_2\}$;

$C_2 = \{0{,}8/a_1;\ 0{,}9/a_2\}$;

$C_3 = \{0{,}7/a_1;\ 0{,}8/a_2\}$;

$C_4 = \{0{,}8/a_1;\ 0{,}6/a_2\}$.

Модифицируем множества

$C_1^{0,15} = \{0{,}9^{0,15}/a_1;\ 0{,}7^{0,15}/a_2\} = \{0{,}984/a_1;\ 0{,}984/a_2\}$

$C_2^{0,2} = \{0{,}8^{0,2}/a_1;\ 0{,}9^{0,2}/a_2\} = \{0{,}956/a_1;\ 0{,}979/a_2\}$

$C_3^{0,25} = \{0{,}7^{0,25}/a_1;\ 0{,}8^{0,25}/a_2\} = \{0{,}915/a_1;\ 0{,}946/a_2\}$

$C_4^{0,4} = \{0{,}8^{0,4}/a_1;\ 0{,}6^{0,4}/a_2\} = \{0{,}916/a_1;\ 0{,}815/a_2\}$

В соответствии с (6.6.7) получим множество D

$D = \{0{,}916/a_1;\ 0{,}815/a_2\}$

Максимальное значение имеет альтернатива a_1 - ее и выбираем в качестве варианта реализации СЗИ.

6.6.4. Выбор варианта СЗИ по аддитивному критерию

Пусть необходимо упорядочить m вариантов СЗИ a_1, a_2, ..., a_m; оцениваемых по “n” требованиям (критериям) C_1, C_2, ..., C_n. Соответствующую оценку обозначим R_{ij};
$i = \overline{1,m}; j = \overline{1,n}$. относительная важность каждого требования задается коэффициентом W_j
$\sum_{j=1}^{n} W_j = 1$. В этом случае взвешенная оценка i-го варианта вычисляется по формуле

$$R_i = \sum_{j=1}^{n} W_j \cdot R_{ij} \qquad (6.6.14)$$

Пусть оценки вариантов по критериям и коэффициенты относительной важности задаются функциями принадлежности соответственно $\mu_{R_{ij}}(r_{ij})$ и $\mu_{W_j}(\omega_j)$.

Так как в данном случае R_{ij} и W_j являются нечеткими числами, R_i определяется в соответствии с формулой (6.6.14) на основе принципа обобщения [35]. Бинарную операцию * (в данном случае это операция сложения или умножения) можно обобщить на случай нечетких чисел (например, X и Y), задаваемых функциями принадлежности $\mu_X(x)$ и $\mu_Y(y)$ соответственно. Результат обобщенной операции * - нечеткое число Z, определяемое функцией принадлежности

$$\mu_Z(z) = \sup_{z=x*y} \min(\mu_X(x), \mu_Y(y)) \quad (6.6.15)$$

Рассмотрим случай вычисления R_i, когда R_{ij} и W_j заданы функциями принадлежности треугольного типа (рис. 6.6.1).

Рис. 6.6.1 Границы и вершина нечеткого числа

Определим левую x^I и правую x^{II} границы нечеткого числа X, а также его вершину x^*:

$$\forall \delta: \mu(x^I) = 0; \mu(x^I - \delta) = 0; \mu(x^I + \delta) \neq 0;$$
$$\forall \delta: \mu(x^{II}) = 0; \mu(x^{II} - \delta) \neq 0; \mu(x^{II} + \delta) = 0; \mu(x^*) = 1$$

Доказано [6], что нечеткое число Z = X*Y также определяется функцией принадлежности треугольного вида, а границы и вершины находятся следующим образом:

$Z^I = X^I * Y^I$; $Z^{II} = X^{II} * Y^{II}$; $Z^* = X^* * Y^*$ (6.6.16)

После того, как взвешенные оценки R_i получены, необходимо сравнить варианты на их основе. Для этого вводится нечеткое множество I, заданное на множестве индексов вариантов {1, 2, ..., m}. Значение соответствующей функции принадлежности интерпретируется как характеристика степени того, насколько вариант a_i является лучшим. Значением $\mu_I(i)$ выполняется по формуле

$$\mu_I(i) = \sup_{r_1, r_2, \dots, r_m: r_i \geq r_j} \min_{j=1,n} \mu_{R_j}(r_j) \quad (6.6.17)$$

Рассмотрим пример сравнения двух вариантов по двум заданным требованиям (критериям), имеющим оценки, приведенные в табл. 6.6.2.

Таблица 6.6.2

Критериальные оценки для 2-х альтернатив (вариантов)

Критерий	Вариант	
	1	2
1	хорошая	Удовлетворительная
2	Удовлетворительная	хорошая

Первый критерий определен как очень важный, второй - довольно важный. Термы заданы функциями принадлежности, представленными на рис. 6.6.2, 6.6.3.

Рис. 6.6.2 Функции принадлежности Рис. 6.6.3 Функции принадлежности

оценок для двух вариантов коэффициентов важности W_1 W_2

На основании (6.6.16) получаем:

$$R_1^I = R_{11}^I \cdot W_1^I + R_{12}^I \cdot W_2^I = 0{,}6 \cdot 0{,}8 + 0{,}4 \cdot 0 = 0{,}48$$

$$R_1^{II} = R_{11}^{II} \cdot W_1^{II} + R_{12}^{II} \cdot W_2^{II} = 1{,}0 \cdot 1{,}8 + 0{,}8 \cdot 0{,}4 = 1{,}32$$

$$R_1^{*} = R_{11}^{*} \cdot W_1^{*} + R_{12}^{*} \cdot W_2^{*} = 0{,}8 \cdot 1{,}0 + 0{,}6 \cdot 0{,}2 = 0{,}92$$

Аналогично $R_2^I = 0{,}32$; $R_2^{II} = 1{,}2$; $R_2^{*} = 0{,}76$.

Полученные функции принадлежности изображены на рис. 6.6.4. Тогда в соответствии с формулой (6.6.17) $\mu_I(1)=1$; $\mu_I(2)=0{,}76$. Следовательно наилучшим является второй вариант, а степень того, что второй вариант лучше равна 0,76.

Рис. 6.6.4 Функции принадлежности взвешенных оценок R_1 и R_2.

6.6.5 Выбор варианта СЗИ лексикографическим методом

Применение этого метода при нечеткой о показателях качества (требованиях) СЗИ сводится к следующим операциям].

1^0. Упорядочить требования к СЗИ по важности

$$C_1 > C_2 > \ldots > C_j > \ldots > C_n;\ j = \overline{1, n}$$

2^0. С согласия ЛПР для каждого требования назначается величина допустимой уступки ΔC_j $j = \overline{1, n}$ в пределах которой рассматриваемые варианты СЗИ считаются “практически равноценными”.

3^0. Для первого требования C_1 формируется множество “практически равноценных” вариантов, удовлетворяющих условию – множество π_1.

$$\begin{vmatrix} 1-\lambda & 5 & 6 & 7 \\ 1/5 & 1-\lambda & 4 & 6 \\ 1/6 & 1/4 & 1-\lambda & 4 \\ 1/7 & 1/6 & 1/4 & 1-\lambda \end{vmatrix} = \lambda^4 - 4\lambda^3 - 6{,}91\lambda - 2{,}715 = 0$$

4^0. Если π_1 – множество содержит ровно один вариант, то он и считается наилучшим. Если π_1 – множество содержит более одной альтернативы, то переходим к рассмотрению всех вариантов множества π_1 по требованию C_2.

5^0. Для второго требования C_2 формируется π_2- множество вариантов из множества π_1, удовлетворяющих условию

$$\max_{j\in\pi_1} \mu_{C_2}(a_j) - \mu_{C_2}(a_k) \le \Delta C_2$$
$$_{\substack{k\in\pi_1\\ i\ne j}}$$

6^0. Если π_2- множество содержит ровно один вариант, то он и считается наилучшим; если более одного – рассматриваем эти варианты по требованию C_3 и т.д.

7^0. Если все требования последовательно пересмотрены и врезультате получаем π - множество $\pi = \pi_1 \times \pi_2 \times \ldots \times \pi_n$, содержащее более одной альтернативы, то возможно применить два подхода:

- уменшить величину допустимой уступки ΔC_j, начиная с первого по важности требования и повторить все шаги решения;

- представить ЛПР окончательный выбор лучшего варианта.

В заключение рассмотрим пример выбора варианта лексикографическим методом.

Пусть в результате экспертной оценки получили следующие данные, характеризующие степень соответствия СЗИ заданным требованиям:

$$C_1 = \{0{,}9/a_1; 0{,}9/a_2; 0{,}8/a_3; 0{,}6/a_4; 0{,}7/a_5\}$$
$$C_2 = \{0{,}8/a_1; 0{,}9/a_2; 0{,}7/a_3; 0{,}8/a_4; 0{,}9/a_5\}$$
$$C_3 = \{0{,}5/a_1; 0{,}7/a_2; 0{,}8/a_3; 0{,}9/a_4; 0{,}8/a_5\}$$
$$C_4 = \{0{,}6/a_1; 0{,}7/a_2; 0{,}6/a_3; 0{,}7/a_4; 0{,}4/a_5\}$$

1^0. Требования упорядочены по важности следующим образом

$$C_1 > C_2 > C_3 > C_4$$

2^0. Зададимся величиной допустимой уступки

$\Delta C_i = 0{,}1$ для всех $P_{i\ ycp}$.

3^0. Формируем множество π_1 по первому требованию. При максимальном значении $C_1 = 0{,}9$ и $\Delta C_1 = 0{,}1$ в это множество входят варианты $\pi_1 = \{a_1, a_2, a_3\}$.

4^0. Из элементов множества π_1 формируем множество π_2 по второму требованию. При $\max_{j\in\pi_1} C_2 = 0{,}9 \quad u \quad \Delta C_2 = 0{,}1$ множество $\pi_2 = \{a_1, a_2\}$.

5^0. Из элементов множества $\pi = \pi_1 \times \pi_2$ формируем множество π_3 по третьему требованию. При $\max_{j\in\pi_1\times\pi_2} C_3 = 0{,}7 \quad u \quad \Delta C_3 = 0{,}1$ это множество содержит один элемент $\pi_3 = a_2$.

Таким образом, наилучшим вариантом является второй вариант СЗИ.

6.7 Методические рекомендации по проведению экспертизы при оценке средств защиты информации

Методы экспертных оценок - это методы организации работы со специалистами-экспертами и обработки мнений экспертов, выраженных в количественной и/или качественной форме с целью подготовки информации для принятия решений лицами, принимающими решения (ЛПР).

Для проведения экспертизы создают рабочую группу (РГ), которая и организует по поручению ЛПР деятельность экспертов, объединенных (формально или по существу) в экспертную группу (ЭГ).

Организация опроса коллектива экспертов - одна из важнейших проблем, связанных с проведением экспертных оценок. Недооценка этой проблемы при проведении экспертизы ставит под сомнение ценность ее результатов и выражается в поспешном, непродуманном опросе экспертов. Низкое качество собранных таким образом мнений не может быть скомпенсировано применением для обработки современных математических методов.

Можно выделить два основных типа процедур экспертного опроса: 1) процедура с личными контактами между экспертами, 2) многотуровые (итеративные) процедуры без личных контактов с контролируемой обратной связью [34].

К первому типу относится традиционная “дискуссия за круглым столом” называемая также методом комиссий, методы суда, мозговой атаки, отнесенной оценки, процедуры номинальной группы. В ходе дискуссии эксперт имеет возможность неоднократно высказывать суждения, учитывая точки зрения других участников опроса. В традиционной дискуссии фактически действует перманентная и неконтролируемая обратная связь, по которой эксперт получает мнение других экспертов, а также их более общую реакцию. Дискуссия может проводиться и в несколько четко выраженных туров. Достоинства и недостатки метода дискуссии указаны в [34]. Однако незыблемой остается основополагающая черта всех этих процедур - прямые контакты экспертов, что приводит к достаточно сильным проявлениям конформизма со стороны экспертов, присоединяющих свои мнения к мнению более компетентных и авторитетных экспертов даже при наличии противоположной собственной точки зрения [6].

Процедуры второго типа основываются на одном из наиболее разработанных и распространенных в практике экспертных оценок методе “Делфи” [6]. Здесь эксперты изолированы друг от друга, а процедура реализуется за несколько разделенных во времени туров (итераций). На каждом туре эксперт получает по обратной связи информацию о суждениях других членов группы (обезличенно) и пересматривает свои суждения.

Согласно этому методу выделяют следующие этапы проведения экспертизы:

1) формирование экспертной группы;

2) планирование и проведение экспертизы;

3) анализ и интерпретация полученных результатов и подготовка заключения ЛПР.

Рассмотрим более подробно первый этап экспертизы - формирование экспертной группы, так как он является наиболее общим для различных видов экспертиз и как правило не зависит от методов сбора экспертной информации. Он состоит из:

1) определения численного состава экспертной группы;

2) определения коэффициентов авторитета экспертов;

3) подбора экспертов в соответствии с их компетентностью.

Определить необходимый численный состав экспертной группы очень важно. При недостаточном числе экспертов результаты экспертизы не будут надежными. Многочисленную группу квалифицированных экспертов трудно сформировать и трудно организовать ее работу.

Согласно [33], численный состав экспертной группы, вычисляется по формуле:

$k=[\beta\ t_{p,k-1} / \alpha\ ]^2$, (6.7.1)

где k - число экспертов; β - вариация (мера надежности проведенной экспертизы); $t_{p,k-1}$ - коэффициент Стьюдента; α - относительная ширина доверительного интервала.

Вариация определяется как:

$\beta = \sigma / \bar{x}$, (6.7.2)

где σ - среднеквадратический разброс экспертных оценок; $\bar{x}$ - среднее значение оценки.

Относительная ширина доверительного интервала вычисляется из соотношения:

$\alpha = \Delta x / \bar{x}$, (6.7.3)

где Δx - доверительный интервал оценок.

Как видно из (6.7.2) величина вариации определяется по результатам экспертизы, но для этого в свою очередь необходимо знать требуемый состав экспертной группы. Чтобы преодолеть возникшую логическую трудность предлагается следующий подход.

Будем считать, что для статистической обработки допускается лишь такие экспертные оценки, относительное отличие которых от среднего значения по абсолютной величине не превышает $|\Delta x / \bar{x}|$. В пределах интервала ± Δx около $\bar{x}$ отдельные оценки могут располагаться различным образом, от чего будет зависеть величина вариации β . Однако при типичном характере рассеяния отдельных оценок и строгом соблюдении правила о привлечении к экспертизе только квалифицированных специалистов изменение вариации при изменении числа оценок будет не очень значительным. В качестве иллюстрации на рис. 6.7.1 приведены зависимости β в долях $\Delta x / \bar{x}$ от числа k. Кривая *а* построена в предположении, что половина всех оценок превышает среднее значение Δx , а половина оценок на столько же меньше $\bar{x}$. Кривая *б* дает эту зависимость для случая, когда все оценки равномерно рассеяны в интервале от $\bar{x} - \Delta x$ до $\bar{x} + \Delta x$. Кривая *в* построена для случая, когда оценки распределены симметрично относительно $\bar{x}$ по треугольному закону: чем меньше отклонение оценки от среднего значения, тем больше таких оценок.

Рис. 6.7.1 Зависимость β в долях $\Delta x / \bar{x}$ от числа экспертов

Из графиков видно, что с увеличением *k* , во-первых, величина β , изменяется не очень существенно; во-вторых, что особенно важно, величина β монотонно уменьшается с возрастанием *k.* Поэтому. Если на основании предыдущих экспертиз, зададимся некоторой величиной β , соответствующей небольшому *k,* а затем с помощью (6.7.1) вычислим *k,* то можно быть уверенным, что при найденном значении *k* доверительный интервал не превысит выбранной величины [33].

На основании опыта применения метода экспертных оценок для решения различных не формализуемых задач установлено, что результаты экспертизы можно считать удовлетворительными при $\beta \leq 0{,}3$ и хорошими, если $\beta \leq 0{,}2$ [32]. Исходя из этого, при определении численного состава экспертной группы априорное значение вариации следует выбирать в пределах 0,2÷0,3.

Коэффициент Стьюдента $t_{p,k-1}$ определяется по таблицам. Выбрав доверительную вероятность p, для различных *k* находим соответствующие значения $t_{p,k-1}$. Затем для каждой пары *k* и $t_{p,k-1}$ из уравнения (6.7.1) находим β / α и для выбранной p будет получена зависимость $\beta / \alpha = f(k)$, которую можно трактовать как $k = F(\beta / \alpha)$ (рис.6.7.2).

Таким образом, вычислив соотношение β / α и задав доверительную вероятность p из графиков (рис. 6.7.2) находим численный состав экспертной группы *k.*

Рис. 6.7.2 Графики функции $k = F(\beta / \alpha)$ при различных значениях доверительной вероятности P.

Распределение Стьюдента, использованное в формуле (6.7.1) при увеличении *k* сходится к нормальному распределению. Поэтому число экспертов приближенно можно определить с помощью выражения:

$$\beta / \alpha = \sqrt{k} / z(k) \quad (6.7.4)$$

где *z(k)* - значение интеграла вероятности, которое определяется по таблицам. Отличие величины *k,* вычисляемой с помощью (6.7.4) от найденного по формуле (6.7.1) показано в табл. 6.7.1.

Таблица 6.7.1

Относительная погрешность вычисления экспертной группы по (6.7.4)

Число экспертов	Доверительная вероятность	$\Delta k / k$, %

10	0,8	7
10	0,9	10
15	0,8	5
15	0,9	7
20	0,8	4
20	0,9	5

На следующем шаге проведения экспертизы вычисляются коэффициенты авторитета (степень компетентности эксперта) - это число, которое показывает с каким весом включаются в статистическую обработку оценки данного эксперта. Важность правильного определения его величины имеет большое значение, поскольку он прямо влияет как на достоверность результатов экспертизы, так и имеет важное психологическое значение для экспертов.

Существует ряд способов определения коэффициентов авторитета как на основе статистики предыдущих экспертиз [33], так и непосредственно по результатам экспертизы, для которой как раз и требуется знание таких коэффициентов [6]. Однако в этих способах коэффициенты авторитета определяются непосредственно, как некоторые числа из интервала [0,1]. Но так как человеку проще дать сравнительную оценку двум качественным понятиям, чем приписать им меру [34], поэтому более рациональным способом определения таких коэффициентов является их вычисление посредством парного оценивания степени компетентности экспертов. Здесь может возникнуть вопрос о достоверности, полученных таким образом, коэффициентов авторитета. Однако если учесть, что к экспертизе, как правило, привлекаются известные специалисты в соответствующей предметной области, то взаимное сравнение их компетентности дает объективные результаты.

Пусть дана группа экспертов Э = ($э_1$, ..., $э_n$). Согласно [30] субъективные оценки компетентности экспертов из Э в виде отношений предпочтения представляются в виде обратно симметричной матрицы доминирования

$$M = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

где $a_{ii} = 1$; a_{ij} показывает во сколько раз компетентность эксперта $э_i$ превосходит компетентность эксперта $э_j$, а $a_{ji}=1/a_{ij}$. При парных сравнениях используется стандартная 9-ти бальная шкала (табл.3.1).

В качестве меры оценки несогласования субъективных оценок используется так называемое отношение согласованности (ОС), которое определяет степень нарушения свойства транзитивности между оценками:

$$ОС = \frac{ИС}{СС} \quad (6.7.5)$$

где ИС - индекс согласованности; СС - случайная согласованность матрицы того же порядка.

Случайная согласованность матрицы того же порядка это число, которое получилось бы при случайном выборе количественных суждений из шкалы 1/9, 1/8, 1/7,..., 1, 2,..., 9, и образовании обратно симметричной матрицы (табл. 6.7.2).

Таблица 6.7.2

Средние согласованности случайных матриц

Размер матрицы	1	2	3	4	5	6	7	8	9	10
Случайная согласованность	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Индекс согласованности матрицы вычисляется по формуле:

$$ИС = \frac{(\lambda_{\max} - n)}{n - 1} \quad (6.7.6)$$

где n - размерность матрицы, а λ_{max} - наибольшее собственное значение.

Известно, что задача нахождения собственных чисел матрицы М связана с вычислением корней характеристического уравнения

$$\det(M - \lambda E) = 0 \quad (6.7.7)$$

Методы нахождения собственных чисел матрицы М достаточно подробно изложены в разделе 3.

Из опыта проводимых экспертиз величина отношения согласованности должна быть не более 10-15% [33]. Если его величина выходит из этих пределов, то экспертам предлагается проверить свои суждения. При этом процесс "сглаживания" рассогласованности данных, как правило, носит циклический характер. Это процесс можно существенно упростить, если предоставить возможность экспертам уточнить свои оценки на этапе формирования матрицы предпочтений.

При проведении сложных экспертиз СЗИ иногда затруднительно сформировать компетентную группу экспертов силами одного структурного подразделения. В этом случае обращения к экспертам сопряжены с определенными финансовыми издержками. Учитывая это обстоятельство, при формировании экспертной группы можно использовать следующую методику.

Для заданной доверительной вероятности *p* из графиков (рис.6.7.2) находится численный состав возможных кандидатов экспертной группы ($э_1$, $э_2$, ..., $э_n$) и вычисляются их весовые коэффициенты ($\mu_1,\ldots,\mu_n$). Далее , пусть h_1 -условная стоимость обращения к i-му эксперту, а h_0 - граничная суммарная условная стоимость обращения ко всем экспертам.

Введем переменные:

$$x_i = \begin{cases} 1, \textit{если} \quad i-\textit{й} \quad \textit{эксперт} \quad \textit{включен в} \quad \textit{состав} \quad \textit{экспертной} \quad \textit{группы} \\ 0, - \quad \textit{в} \quad \textit{противном} \quad \textit{случае} \end{cases}$$

Тогда задачу формирования экспертной группы, обладающей максимальной компетентностью, можно записать как задачу линейного программирования следующим образом:

$$\sum_{i=1}^{n} \mu_i \cdot x_i \longrightarrow \max \qquad (6.7.8)$$

при ограничениях

$$\sum_{i=1}^{n} h_i \cdot x_i \le h_0, x_i = \begin{cases} 1 \\ 0 \end{cases}, \; i \in \{1,\ldots,n\} \qquad (6.7.9)$$

Для упрощения процедуры сбора и обработки результатов экспертного опроса целесообразно автоматизировать этот процесс с помощью диалоговых средств взаимодействия "эксперт - ЭВМ".

Логическая схема получения экспертной информации с применением диалоговых средств приведена на рис. 6.7.3.

В памяти микроЭВМ содержатся объекты оценки, базовые лингвистические категории, а также лингвистические конструкции организации диалога. Программа последовательно формирует вопросы для экспертов, предлагая базовый набор лингвистических оценок. Эксперт вводит в ЭВМ свои значения оценок, записываемые в память. Введенные оценки обрабатываются и представляются руководителю эксперимента. Увязкой организации диалога и обработки информации управляет программный диспетчер. В конце экспертного опроса оценивается степень согласованности мнений экспертов.

Литература

Поскольку материал этой главы носит действительно научный характер, используемая литература приводиться отдельно:

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

6. Литвак Б.Г. Экспертная информация: методы получения и анализа; М.; Радио и связь, 1982-184с.
7. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений-М; МИР, 1976-165с.
8. Гуткин Л.С. Оптимизация радиоэлектронных устройств по совокупности показателей качества; М.; Радио, 1975-367с.
9. Анохин А.М., Глотов В.А., Павельев В.В., Черкашин А.М. Методы определения коэффициентов важности критериев "Автоматика и телемеханика", №8, 1997, с3-35
10. Wei T.H. The algebraic foundations of ranking theory Theses, Cambridge,1952
11. Saaty Thomas L Eigenweinghtor an logarithmic lease sguares // Eur. J. Oper. res, 1990, V. 48, № 1, p. 156-160.
12. Cogger K.O., Yu P. L. Eigenweight vector and least-distance approximation // J. Optimiz. Theory and Appl, 1985, V. 46, №4, p.483-491.
13. Studler Josef, Weights Search by the Marquardt method // Econ. Math. Obs, 1975, v.21, № 2, h.185-195.
14. Макаров И.М. и др. Выбор принципа построения сетей // АнТ, 1971, №4, с.25-31.
15. Тинтарев Э.М., Трофимов В.М. Аппроксимация коэффициентов важности функциями ранжирования // экономика и мат. методы, 1975, Т.11, №7, с. 17-20.
16. Гмошинский В.Г., Флнорент А.В. Теоретические основы инженерного прогнозирования М.; Наука,1975, 280с.
17. Churchmen C.W., Ackoff R. An approximate Measure of Value // Operations Research, 1954, №2, p. 172-181.
18. Подиновский В.В. Лексикографические задачи линейного программирования// журн. вычисл. матем. и мат. физики 1972, Т.12,№6, с568--571
19. Гермеер Ю.Б. Введение в теорию исследования операций М.; Наука, 1971, 324с.
20. Кини Р.Л. Принятие решений при многих критериях предпочтения и замещения, М; Радио и связь, 1981, 342с.
21. Charsnes A., Cooper W.W. Management models and industrial applications of line programming, N.Y.: Wiley, 1961.
22. Zeleny M. Compromise programming in M.K. Starr and M. Zelleny, Columbia, 1973.
23. Szidarovsky R.I. Use of cooperative games in a multiobjective analysis of maning and enwironment// Proc. and International Conference, Madrid, 1978, p. 11-15.
24. Фарберов Д.С., Алексеев С.Г. Сравнение некоторых методов решения многокритериальных задач линейного программирования // Журнал Высш. математики и мат. физики, 1974, Т.14,№6, с.178-180
25. Thurstone L.L. The measurement of valnes, Chicago, 1959.
26. Глотов В.А. и др. Метод определения коэффициентов относительной важности // Приборы и системы управления 1976, №8, с.17-22
27. Rosner B.S. A new scaling technique for absolute judgement// Psychometrica, 1956, V. 21, №4.
28. Сваровский С.Т. Аппроксимация функций принадлежности значений лингвистической переменной//Математические вопросы анализа данных, Новосибирск, ВЦ СО АН СССР, 1980, с.127-131.
29. Кузьмин В.Б. Параметрическое отношение лингвистических значений переменных и ограничений // Модели выбора альтернатив в нечеткой среде, Рига, 1980, с.75-76
30. Саати Т., Кернс К. Аналитическое планирование, Организация систем М.; Радио и связь, 1991-224с.
31. Демидович Б.Л. Марон И.А. Основы вычислительной математики М; Наука, 1970-663с.
32. Мулен Э. Кооперативное принятие решений: аксиомы и модели- М; Мир , 1991-463с.

33. Брахман Т.Р. Многокритериальность и выбор альтернативы в технике - М; Радио и связь, 1984-287с.
34. Панкова Л. А., ПетровскийА.М., Шнейдерман Н.В. Организация экспертизы и анализ экспертной информации - М; Наука, 1984-214с.