Раздел III
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ (ПО ОТРАСЛЯМ), ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И РЕСУРСЫ

III. DATA MEASURING AND CONTROL SYSTEMS (BY BRANCHES), INFORMATION PROCESSES AND RESOURCES

УДК 004.056.53

О ЛОКАЛИЗАЦИИ УТЕЧКИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ С ПРИМЕНЕНИЕМ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

Е.К. Герасимова

ГООУ СПО «Оленегорский горнопромышленный колледж», г. Оленегорск, Мурманская область

Ключевые слова и фразы: лингвистическая переменная; математические модели; методы принятия решений; многокритериальная задача; оптимальные системы защиты информации; нечеткие множества; экспертная информация; утечка информации.

Аннотация: На основе анализа теории нечетких множеств показано как можно применить этот современный математический аппарат для решения прикладных задач, связанных с оценкой и выбором вариантов построения системы защиты информации (СЗИ). Поставлены и решены задачи выбора наилучшего варианта построения СЗИ применительно к защите процессов передачи информации при равной и различной важности требований (критериев) выбора с использованием экспертной информации. Рассчитана вероятность утечки информации при локализации на одном из узлов компьютерной сети.

Построение и исследование математических моделей процессов передачи и обработки информации на базе математического аппарата является одним из методов оптимизации информационной системы (ИС). Это позволяет отражать зависимость функционирования от различных внешних факторов, разрабатывать методики организации информационного обмена.

Теоретические основы построения оптимальных систем защиты информации исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства. Кроме того, отсутствие достаточно общей теории, формирующей методологические основы изучения явлений с неопределенными факторами, делает неприменимыми методы классической теории статистических решений для синтеза оптимальных систем защиты.

Под методологией оптимизации систем защиты информации понимаются разработки теории, связывающей их структуру, логическую организацию, методы

и средства деятельности с целью формирования функции выбора и выделения подмножества наилучших стратегий. Эффективность систем защиты информации – это эффективность ее использования в качестве активного средства в операции обеспечения конфиденциальности обработки, хранения и передачи информации.

Критерий эффективности определяется как правило, позволяющее сопоставлять стратегии, характеризующиеся различной степенью достижения цели, и осуществлять выбор стратегий из множества допустимых. 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 [2].

В связи с этим наиболее важными задачами представляются следующие:

– построение и исследование математических моделей информационных систем, учитывающих различные варианты программных и аппаратных средств, средств связи, требуемые объем и скорость передачи информации;

– исследование влияния различных факторов на функционирование систем и сетей связи, их анализ и синтез;

– создание на основе моделей эффективных протоколов обмена, позволяющих уменьшить расходы на организацию взаимодействия;

– оптимизация средств передачи информации в условиях различных характеристик оборудования и каналов связи;

– формулировка критериев адаптации ИС, позволяющих оптимизировать параметры информационного обмена;

– разработка моделей процесса защиты информации в ИС при передаче данных;

– выбор варианта реализации системы защиты информации, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на СЗИ.

Таким образом, практическая ценность решения задачи оптимизации может состоять в разработке многофункциональных моделей и методик построения многопользовательских систем, учитывающих программно-аппаратные средства связи и основные характеристики каналов связи, и в решении проблемы создания надежных, недорогих, многофункциональных информационных средств в системах с оптимальными характеристиками взаимодействия компонентов ИС между собой.

Системы защиты информации, с одной стороны, являются составной частью информационной системы, с другой стороны, – сами по себе представляют

сложную техническую систему. Системную классификацию общих моделей СЗИ в настоящее время произвести практически невозможно, так как ввиду малого числа таких моделей (общая модель процесса защиты информации, модель общей оценки угроз информации, модели анализа систем разграничения доступа к ресурсам ИС, и т.д.) для этого нет достаточных данных. 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.

Решение задач анализа и синтеза СЗИ усложняется рядом их особенностей (необходимость учета большого числа показателей (требований) СЗИ при оценке и выборе их рационального варианта; преимущественно качественный характер показателей (требований); существенная взаимосвязь и взаимозависимость этих показателей (требований), имеющих противоречивый характер; и др.), которые 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.

Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

Теория нечетких множеств подтверждает, что 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 [3].

Пусть $X = \{x\}$ – полное множество, охватывающее всю проблемную область.

Нечеткое множество $A \subseteq X$ представляет собой набор пар $\{(x, \mu^A(x))\}$, где $x \in X$ и $\mu^A : X \to [0,1]$ – функция принадлежности, которая представляет собой некоторую субъективную меру соответствия элемента нечеткому множеству, $\mu^A(x)$ может принимать значения от нуля, который обозначает абсолютную не принадлежность, до единицы, которая, наоборот, говорит об абсолютной принадлежности элемента *x* нечеткому множеству *A*.

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

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

где $\mu^A(x_i)/x_i$ – пара «функция принадлежности / элемент», называемая синглтоном, а «+» обозначает совокупность пар [1].

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.

Общая постановка задачи многокритериальной оптимизации имеет следующий вид.

Пусть $\overline{X} = [x_1, ..., x_i, ..., x_n]$ – вектор оптимизируемых параметров некоторой системы *S*. Некоторое *j*-е свойство системы *S* характеризуется величиной *j*-го показателя $q_j(\overline{X}), j = \overline{1, m}$. Тогда система в целом характеризуется вектором показателей $\overline{Q} = [q_1, ..., q_j, ..., q_m]$. 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 сформулировано математически, то есть выбран (обоснован) соответствующий критерий предпочтения (отношение предпочтения) [3].

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).

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 [2].

Пусть имеется множество из *m* вариантов построения СЗИ $A = \{a_1, ..., a_m\}$. Для некоторого требования *C* (критерия оценки) может быть рассмотрено нечет-

кое множество $C = \{\mu_c(a_1)/a_1, \mu_c(a_2)/a_2, ..., \mu_c(a_m)/a_m\}$, 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: $C_1, C_2, ..., C_j, ..., C_n, j = \overline{1,n}$, то лучшим считается вариант, удовлетворяющий и требованию C_1, и C_2, ..., и C_n. Тогда правило для выбора наилучшего варианта может быть записано в виде пересечения соответствующих множеств:

$$D = C_1 \cap C_2 \cap ... \cap C_n .$$

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

$$\mu_D(a_j) = \min_{i=\overline{1,n}} \mu_{ci}(a_j), j = \overline{1,m} .$$

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

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

Рассмотрим процесс передачи информации и выберем СЗИ применительно к защите процессов передачи информации.

Зададим схему функционирования ИС с помощью связного графа $G = (V, E)$ (рис. 1), определенного на множестве вершин-узлов $V = \{v_1, ..., v_n\}$ и множестве ребер-линий связи $E = \{e_1, ..., e_k\}$ произвольной сети.

Предположим, что на одном из узлов v_y сети происходит утечка информации, и определим вероятность $P(C)$ прохождения информации через этот узел. Событие C заключается в попадании информации в узел v_y при передаче из узла v_1 в v_n.

1. Пусть существует единственный маршрут из узла v_1 в v_n. Тогда

– $P(C) = 1$, если v_y принадлежит множеству $\{(\mathrm{v}_1, \mathrm{v}_2), ..., (\mathrm{v}_{n-1}, \mathrm{v}_n)\}$;

– $P(C) = 0$, если v_y не принадлежит множеству $\{(\mathrm{v}_1, \mathrm{v}_2), ..., (\mathrm{v}_{n-1}, \mathrm{v}_n)\}$;

2. Пусть существует m маршрутов из узла v_1 в v_n, тогда

– $P(C) = S/m$, если S – количество маршрутов через узел v_y;

– $P(C) = 0$, если ни один маршрут не проходит через v_y.

Количество маршрутов S через узел v_y в зависимости от количества промежуточных узлов i в маршрутах передачи информации определяется как

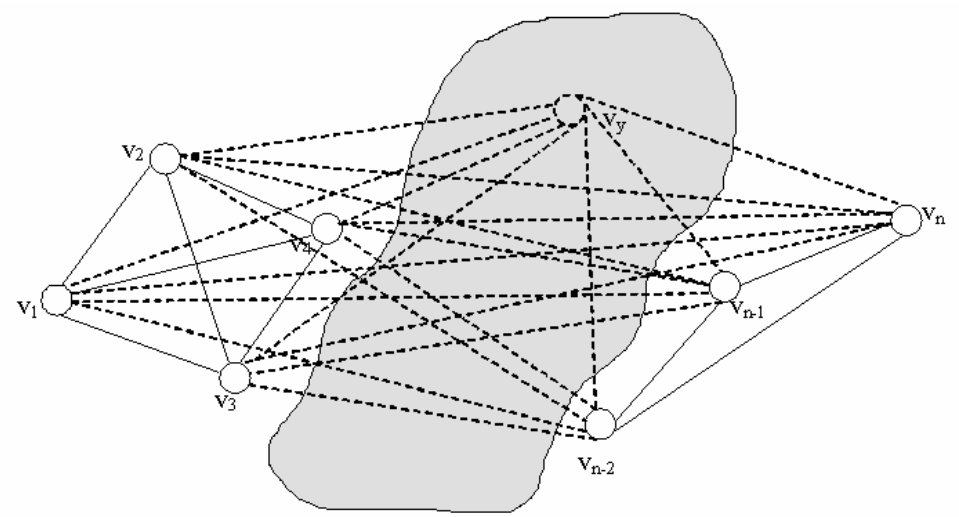

Рис. 1. Связный граф

$$S = \sum_{i=1}^{n-2} i \frac{(n-3)!}{(n-2-i)!},$$

общее количество всевозможных маршрутов

$$m = \sum_{i=1}^{n-2} \frac{(n-2)!}{(n-1-i)!}.$$

Следовательно,

$$P(C) = \frac{\sum_{i=1}^{n-2} i \frac{(n-3)!}{(n-2-i)!}}{\sum_{i=1}^{n-2} \frac{(n-2)!}{(n-1-i)!}}.$$

С увеличением количества промежуточных узлов в маршрутах из v_1 в v_n возрастает вероятность попадания информации на узел v_y и утечки информации.

Пусть имеется 3 варианта построения СЗИ применительно к защите процессов передачи информации: $A = \{a_1, a_2, a_3\}$.

При равной важности требований (критериев) выбора варианта основными положим следующее:

C_1 – обеспечение максимальной скорости передачи информации;

C_2 – оптимальный маршрут передачи информации;

C_3 – надежная защита от несанкционированного доступа;

C_4 – стойкий к атакам криптографический алгоритм;

C_5 – эффективные меры предотвращения утечки информации.

Пусть в результате экспертной оценки получили следующие данные (нечеткие множества), характеризующие степень соответствия варианта заданным требованиям:

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

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

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

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

$$C_5 = \{0{,}9 / a_1,\ 0{,}8 / a_2,\ 0{,}7 / a_3\}.$$

В соответствии с правилом выбора получаем:

$$D = \{\min(0{,}9;\ 0{,}8;\ 0{,}7;\ 0{,}8;\ 0{,}9) / a_1, \min(0{,}7;\ 0{,}9;\ 0{,}8;\ 0{,}6;\ 0{,}8) / a_2,$$
$$\min(0{,}8;\ 0{,}6;\ 0{,}9;\ 0{,}7;\ 0{,}7) / a_3\} = \{0{,}7 / a_1;\ 0{,}6 / a_2;\ 0{,}6 / a_3\}.$$

Из правила для выбора наилучшего варианта следует, что наилучшим является первый

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

В случае, если требования C имеют различную важность, каждому из них приписывается число $\alpha_i \geq 0$ (коэффициенты относительной важности). Чем важнее требование, тем больше α_i и общее правило выбора принимает вид

$$D = C_1^{\alpha_1} \cap C_2^{\alpha_2} \cap \ldots \cap C_n^{\alpha_n}.$$

Лучший вариант a^* находится из соотношения

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

Пусть важность требований определена как $\alpha_1 = 0{,}15$, $\alpha_2 = 0{,}2$, $\alpha_3 = 0{,}25$, $\alpha_4 = 0{,}3$, $\alpha_5 = 0{,}1$. Модифицируем нечеткие множества:

$$C_1^{0,15} = \{0{,}9^{0,15} / a_1,\ 0{,}7^{0,15} / a_2,\ 0{,}8^{0,15} / a_3\} = \{0{,}984 / a_1,\ 0{,}948 / a_2,\ 0{,}967 / a_3\};$$

$$C_2^{0,2} = \{0,8^{0,2} / a_1,\ 0,9^{0,2} / a_2,\ 0,6^{0,2} / a_3\} = \{0,956 / a_1,\ 0,979 / a_2,\ 0,903 / a_3\};$$

$$C_3^{0,25} = \{0,7^{0,25} / a_1,\ 0,8^{0,25} / a_2,\ 0,9^{0,25} / a_3\} = \{0,915 / a_1,\ 0,946 / a_2,\ 0,974 / a_3\};$$

$$C_4^{0,3} = \{0,8^{0,3} / a_1,\ 0,6^{0,3} / a_2,\ 0,7^{0,3} / a_3\} = \{0,935 / a_1,\ 0,856 / a_2,\ 0,899 / a_3\};$$

$$C_5^{0,1} = \{0,9^{0,1} / a_1,\ 0,8^{0,1} / a_2,\ 0,7^{0,1} / a_3\} = \{0,990 / a_1,\ 0,978 / a_2,\ 0,965 / a_3\}.$$

В соответствии с правилом выбора

$$D = \{0,915 / a_1,\ 0,856 / a_2,\ 0,899 / a_3\}$$

максимальное значение имеет альтернатива a_1 – ее и выбираем в качестве варианта реализации СЗИ.

Список литературы

1. Беллман, Р. Принятие решений в расплывчатых условиях / Р. Беллман, Л. Заде. – М. : Мир, 1976. – 215 с.

2. Домарев, В.А. Энциклопедия безопасности информационных технологий. Методология создания систем защиты информации / В.А. Домарев. – Киев : ООО «ТИД «ДС», 2001. – 688 с.

3. Заде, Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – М. : Мир, 1976. – 165 с.

4. Кофман А. Введение в теорию нечетких множеств / А. Кофман. – М. : Радио и связь, 1982. – 432 с.

5. Борисов, А.Н. Принятие решения на основе нечетких моделей: примеры использования / А.Н. Борисов, О.А. Крумберг, И.П. Федоров. – Рига : Знание, 1990. – 184 с.

ABOUT LOCALIZATION OF INFORMATION LEAKAGE IN COMPUTER NETWORKS WITH APPLICATION OF THE THEORY OF NOT PRECISE SETS

E.K. Gerasimova

Key words and phrases: a linguistic variable; information leakage; mathematical models; methods of decision-making; not precise sets; optimum systems of protection of the information; the expert information.

Abstract: On the basis of the analysis of the theory of not precise sets it is shown, how it is possible to apply this modern mathematical device to the decision of the applied problems connected with an estimation and a choice of variants of construction of system of protection of the information (SPI). Are put and solved problems of a choice of the best variant of construction SPI with reference to protection of processes of transfer of the information at equal and various importance of requirements (criteria) of a choice with use of the expert information. The probability of information leakage is calculated at localization on one of units of a computer network.