В разі виходу з ладу каналу зв'язку між керованим вузлом МПД та ЦСУ або при виникненні порушення доступності керованого обладнання з інших причин персонал центра керування втрачає контроль над цим обладнанням. Для запобігання таким ситуаціям доцільно використовувати системи управління типу Out-of-band.

Система управління типу Out-of-band дозволяє персоналу оператора мережі отримувати віддалений доступ до системних консолей (портів RS-232, AUX тощо) критичного обладнання вузлів МПД через виділені канали зв'язку, які призначені виключно для цілей керування. Крім підвищення надійності мережі та ефективності її експлуатації такий підхід дозволяє збільшити захищеність інформаційних ресурсів підсистем керування МПД від НСД, оскільки технологічна інформація керування фізично відокремлена від інформації абонентів.

Проаналізувавши особливості захисту від несанкціонованого доступу інформаційних ресурсів глобальних мультисервісних мереж національного рівня, можна зробити висновок, що внаслідок широкого застосування персоналом операторів МПД віддаленого керування обладнанням вузлів цих мереж можуть бути реалізовані специфічні загрози технологічній інформації керування, яка обробляється та зберігається в системах управління, в керованих об'єктах та циркулює в каналах зв'язку. Для запобігання порушенням конфіденційності, цілісності та (або) доступності інформації через реалізацію цих загроз необхідно у повній мірі використовувати можливості штатних систем ТЗІ обладнання вузів мережі, можливості позаштатного обладнання, а також тісно інтегрувати ці засоби у єдину підсистему керування безпекою. Особливу увагу слід звернути на коректність роботи механізмів розподілу прав доступу до систем управління. При передачі технологічної інформації між контрольованим обладнанням вузлів мережі та програмно-апаратними засобами ЦСУ впродовж сесії віддаленого керування необхідно використовувати захищені канали зв'язку. В особливих випадках для підвищення надійності мережі та збільшення захищеності інформаційних ресурсів підсистем керування МПД від НСД слід використовувати системи керування типу Out-of-band.

ЛІТЕРАТУРА

1. Компьютерные сети. Принципы, технологии, протоколы. *Олифер В.Г., Олифер Н.А.* – СПб: Питер, 2001. – 672 с.: ил.

2. Атака на Internet – 3-е изд., стер. *Медведовский И.Д., Семьянов П.В., Леонов Д.Г.* – М.: ДМК, 2000. – 336 с.: ил.

3. *Stephen L. Packard, Archie D. Andrews*, "Remote System Administration", ATI IPT Special Report, April 2000, <http://ips.aticorp.org>.

Надійшла 10.07.2002

УДК 004.56.021.2: 510.22 (045)

А.Г. Корченко, к.т.н., В.В. Душеба, к.т.н., В.А. Рындюк, Е.В. Пацира

ИССЛЕДОВАНИЕ МЕТОДОВ ОБРАБОТКИ ТОЛЕРАНТНЫХ НЕЧЕТКИХ ЧИСЕЛ ДЛЯ ПРИМЕНЕНИЯ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Определение состояния безопасности информационной системы в настоящее время является одним из наиболее распространенных классов задач, в которых немаловажное место уделяется проблеммам принятия решений. На практике часто принятие решений

происходит в таких условиях, когда исходные данные являются неполными, размытыми, либо представленными в лингвистической форме. Для обработки информации подобного рода применяют аппарат теории нечетких множеств [1], используя который можно построить модели систем, решающих вышеуказанную задачу.

Часто различные размытые понятия, отображаемые при помощи нечетких множеств, легко интерпретировать с помощью нечетких чисел (НЧ).

В ряде работ при построении моделей и систем защиты информации [2-9] были использованы методы и модели теории нечетких множеств, однако в них не содержится обоснование применения того или иного способа реализации нечетких арифметических операций (НАО).

Для выполнения НАО в зарубежной и отечественной литературе описано ряд методов, которые в основном базируются на принципе обобщения, предложенном Л.А. Заде [1].

В данной работе проведено исследование методов, которые, в отличие от других известных [10], могут обрабатывать толерантные НЧ. К ним относятся - максминная композиция (ММК), метод выполнения монотонных операций (ММО), метод аналитического выполнения арифметических операций (МАО), матрично-диагональный метод (МДМ), модифицированный (МПО) и α-уровневый принципы обобщения (АУПО), а также метод обработки параметрических НЧ (МПЧ). Основные результаты обработки НЧ перечисленными методами проиллюстрированы на конкретных примерах и представлены в данной статье.

Основываясь на принципе обобщения, ММК [1] реализуется двумя процедурами, в первой из которых осуществляются преобразования по формуле [11]:

$$\underset{\sim}{Z} = \underset{\sim}{X} \mathbin{\tilde{*}} \underset{\sim}{Y} = \bigcup_{i=1}^{n} \{\mu_X(x_i)/x_i\} \mathbin{\tilde{*}} \bigcup_{j=1}^{m} \{\mu_Y(y_j)/y_j\} = \bigcup_{i=1}^{n}\bigcup_{j=1}^{m} \{(\mu_X(x_i) \wedge \mu_Y(y_j))/(x_i * y_j)\}, \quad (1)$$

(где $\underset{\sim}{X}$ и $\underset{\sim}{Y}$ - НЧ, содержащие соответственно n и m компонентов, а знаками $*$ и $\tilde{*}$ обозначены одна из арифметических операций +, -, ·, : и одна из НАО $\tilde{+}, \tilde{-}, \tilde{\cdot}, \tilde{:}$ соответственно), а во второй - осуществляется поглощение нескольких компонентов $\mu_Z(z_k)/z_k$, $k = \overline{1,r}$, (r – количество компонентов с равными носителями) одним - $\mu_Z(z_s)/z_s$: $\mu_Z(z_s) = \max(\mu_Z(z_k))$.

Данный метод, наряду с толерантными, может обрабатывать также полимодальные и унимодальные, нормальные и субнормальные, выпуклые и невыпуклые, дискретные, непрерывные (дискретизированные), непараметрические НЧ, т.е. осуществляет преобразование почти всех широко используемых классов чисел [12]. Здесь под дискретизацией понимается процесс, когда НЧ приводят к дискретному виду, используя при этом α-уровни (с переменным или постоянным шагом) либо локальные максимумы. Дискретизировать НЧ можно также по их носителям или любым произвольным образом.

Пример 1. Выполним по формуле (1) нечеткое умножение ($\tilde{*} \Rightarrow \tilde{\cdot}$) двух НЧ, которые, согласно классификации [12], можно определить как нормальные выпуклые унимодальные дискретные непараметрические: $\underset{\sim}{X} = \underset{\sim}{3} = \{0.6/2,\ 1/3,\ 0.8/4\}$ и $\underset{\sim}{Y} = \underset{\sim}{5} = \{0.5/3,\ 1/5,\ 0.7/6\}$.

Процедура 1. $\underset{\sim}{15} = \underset{\sim}{3} \tilde{\cdot} \underset{\sim}{5} = \{0.5/6,\ 0.6/10,\ 0.6/12,\ 0.5/9,\ 1/15,\ 0.7/18,\ 0.5/12,\ 0.8/20,\ 0.7/24\} = \{0.5/6,\ 0.5/9,\ 0.6/10,\ 0.6/12,\ 0.5/12,\ 1/15,\ 0.7/18,\ 0.8/20,\ 0.7/24\}$.

Процедура 2. $\underset{\sim}{15} = \{0.5/6,\ 0.5/9,\ 0.6/10,\ 0.6/12,\ 1/15,\ 0.7/18,\ 0.8/20,\ 0.7/24\}$.

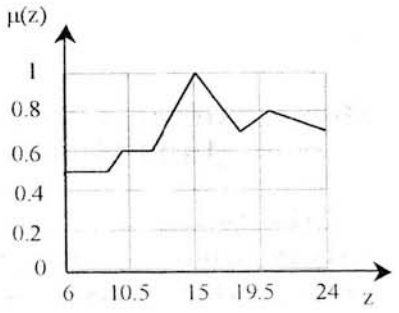


Рис. 1

Графическая интерпретация результата операции проиллюстрирована на рис. 1, где здесь и в последующих дискретных НЧ, для наглядности их носители соединены ломаной.

Данный метод позволяет сформировать результат, содержащий полное множество компонентов НЧ (относительно формулы (1)), расположенных между граничными значениями в диапазоне носителей $D_н$. Так, в примере 1 результирующее НЧ содержит восемь компонентов, а $D_н \in [6, 24]$. Этот метод, по отношению к известным методам своего подмножества [10], является самым точным, поскольку полностью отображает образованную нечеткую величину. Основным недостатком ММК является рост при многократных операциях с НЧ количества компонентов, который при компьютерной обработке может привести к быстрому переполнению оперативной памяти и значительному увеличению времени выполнения указанных НАО.

МДМ [13] предназначен для дискретизированных по α-уровням НЧ. При этом могут быть исключены элементы, которые являются локальными максимумами и входят в полное множество компонент НЧ, образуемых при ММК. Отметим, как ограничение в методе, что исходные НЧ в МДМ должны иметь одинаковое количество компонентов.

Данный метод предполагает построение матрицы. В ней две исходные функции принадлежности (ФП) размещаются соответственно в левом столбце и верхней строке матрицы (см. табл. 1). В результате операции получим матрицу, каждый элемент которой представляет собой результат выполнения одной из арифметических операций над соответствующими элементами строки и столбца $z_{ij} = x_i \textcircled{*} y_j$, а в качестве ФП взята минимальная из ФП компонентов, участвующих в операции, т.е. $\mu_Z(z_{ij}) = \min(\mu_X(x_i), \mu_Y(y_j))$.

Авторами отмечено, что решения для результирующей ФП располагаются в зависимости от вида НАО на одной из диагоналей матрицы: для сложения и умножения на левой диагонали, а для вычитания и деления - на правой.

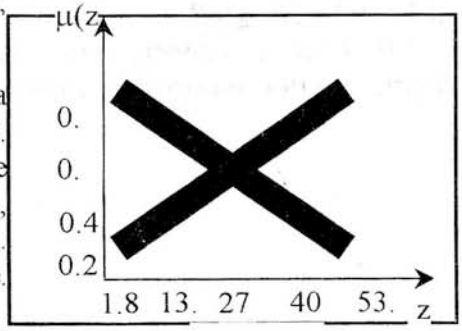
Пример 2. Выполним умножение двух НЧ $\underset{\sim}{X}$ и $\underset{\sim}{Y}$, заданных в примере 1, используя для реализации НАО МДМ. Для этого предварительно преобразуем исходные НЧ, дискретизировав их по α-уровням [14]. Пусть $\alpha = 0.2$ и шаг дискретизации равен 0.2. Тогда: $\underset{\sim}{X} = \underset{\sim}{3} =$ {0.2/1, 0.4/1.5, 0.6/2, 0.8/2.5, 1/3, 0.8/4, 0.6/5, 0.4/6, 0.2/7} и $\underset{\sim}{Y} = \underset{\sim}{5} =$ {0.2/1.8, 0.4/2.6, 0.6/3.4, 0.8/4.2, 1/5, 0.8/5.67, 0.6/6.33, 0.4/7, 0.2/7.67}.

В табл. 1 представлена матрица, на левой диагонали которой показан результат операции умножения полужирным шрифтом, а ФП - полужирным курсивом:

Таблица 1

Y / X	.2	.8	.4	.6	.6	.4	.8	.2			.8	.67	.6	.33	.4		.2	.67
.2	**.2**		.2		.2		.2		.2		.2		.2		.2		.2	
		.8		.6		.4		.2				.67		.33				.67
.4	.2		**.4**		.4		.4		.4		.4		.4		.4		.2	
.5		.7		**.9**		.1		.3		.5		.5		.5		0.5		1.5
.6	.2		.4		**.6**		.6		.6		.6		.6		.4		.2	
		.6		.2		**.8**		.4		0		1.3		2.7		4		5.3
.8	.2		.4		.6		**.8**		.8		.8		.6		.4		.2	
.5		.5		.5		.5		**0.5**		2.5		4.2		5.8		7.5		9.2
	.2		.4		.6		.8				.8		.6		.4		.2	
		.4		.8		0.2		2.6		**5**		7		8.9		1		3
.8	.2		.4		.6		.8		.8		**.8**		.6		.4		.2	
		.2		0.4		3.6		6.8		0		**2.7**		5.3		8		0.7
.6	.2		.4		.6		.6		.6		.6		**.6**		.4		.2	
				3		7		1		5		8.4		**1.7**		5		8.4
.4	.2		.4		.4		.4		.4		.4		.4		**.4**		.2	
		0.8		5.6		0.4		5.2		0		4		7.9		**2**		6
.2	.2		.2		.2		.2		.2		.2		.2		.2		**.2**	
		2.6		8.2		3.8		9.4		5		9.7		4.3		9		**3.7**

$\underset{\sim}{3} \tilde{-} \underset{\sim}{5} =$ {0.2/ 1.8, 0.4/3.9, 0.6/6.8, 0.8/10.5, 1/15, 0.8/22.7, 0.6/31.7, 0.4/42, 0.2/53.7} = $\underset{\sim}{15}$.



Графическая интерпретация результата приведена на рис. 2. Для всех операций алгебраическое решение, т.е. такое, которое при подстановке в исходное уравнение позволяют обеспечить равенство левой и правой части, лежит на левой диагонали, а на правой диагонали - т.н. поточечное решение операций деления или вычитания: т.е. действие $\underset{\sim}{X} \tilde{-} \underset{\sim}{Y}$ заменяется на $\underset{\sim}{X} + (-\underset{\sim}{Y})$, а $\underset{\sim}{X} \tilde{:} \underset{\sim}{Y}$ - на $\underset{\sim}{X} \tilde{\cdot} (1/\underset{\sim}{Y})$.

Используя классификацию НЧ [12], можно сказать, что МДМ также может применяться для нормальных и субнормальных, выпуклых, унимодальных и толерантных, дискретных и непрерывных (дискретизированных), непараметрических НЧ.

При более внимательном изучении метода было определено, что все выполняемые матричные операции, с получением аналогичного результата, могут быть заменены операциями над носителями НЧ одного α-уровня, т.е. выполнением прямого произведения. Данный метод можно реализовать более просто, использовав следующие формулы: для операций сложения и умножения

$$\underset{\sim}{Z} = \underset{\sim}{X} \overset{\sim}{*} \underset{\sim}{Y} = \bigcup_{i=j=1}^{n} \mu_Z(z_{ij}) = \bigcup_{i=j=1}^{n} \{(\mu_X(x_i) \wedge \mu_Y(y_j))/(x_i * y_j)\}, \qquad (2)$$

для вычитания и деления

$$\underset{\sim}{Z} = \underset{\sim}{X} \overset{\sim}{*} \underset{\sim}{Y} = \bigcup_{i=1}^{n} \bigcup_{j=n}^{1} \mu_Z(z_{ij} = \bigcup_{i=1}^{n} \bigcup_{j=n}^{1} \{(\mu_X(x_i) \wedge \mu_Y(y_j))/(x_i \overset{\sim}{*} y_j)\}, \qquad (3)$$

где n - количество компонентов НЧ. Применение этих формул сэкономит компьютерные ресурсы (оперативную память и время) и ускорит получение результата, т.к. при выполнении матричных операций производится n^2 вычислений для нахождения итоговых компонент, а при использовании формул (2) или (3) количество вычислений равно n.

В МДМ авторы также не показали, каким образом получать носители НЧ при заданных α-уровнях в случаях, когда на этих уровнях данное число не определено. Тогда, вероятно, данный метод либо не пригоден для выполнения НАО, либо должны быть разработаны методы экстраполяции для определенных видов НЧ. В работе [13] авторами также не указаны ограничения на получение алгебраических решений (на левой диагонали) операций деления и вычитания при действиях с выпуклыми НЧ. Так, например, проведенные исследования операции вычитания показали, что для получения выпуклого НЧ у уменьшаемого интервалы соответствующих α-уровней должны быть больше, чем у вычитаемого.

В работе [15] описан ММО (возрастающих или убывающих) над непрерывными НЧ. При этом бинарная операция $\overset{\sim}{*}$ на R называется возрастающей, если $(x_1 > y_1, x_2 > y_2) \Rightarrow x_1 \overset{\sim}{*} x_2 > y_1 \overset{\sim}{*} y_2$, и убывающей, если $(x_1 > y_1, x_2 > y_2) \Rightarrow x_1 \overset{\sim}{*} x_2 < y_1 \overset{\sim}{*} y_2$.

В ММО любое непрерывное НЧ раскладывают на выпуклые, возможно ненормализованные нечеткие подмножества с ФП, являющимися строго возрастающими, строго убывающими, или постоянными. Кроме того, НЧ должно быть дискретизировано по конечному числу уровней α_i, $i = \overline{1,k}$ (α_1=0, α_k=1). С каждым i-тым уровнем связано множество

$$X_i = \{x_{i1}, x_{i2}, ..., x_{iJ}\},\ x_{ij} \in R,\ \mu(x_{ij}) = \alpha_i;\ j = \overline{1,J},$$

т.е. в общем виде НЧ представляется как

$$\underset{\sim}{X} = \{\alpha_1 / x_{11}; \alpha_2 / x_{21}; ...; \alpha_k / x_{k1}; ...; \alpha_2 / x_{22}; \alpha_1 / x_{12}\},$$

а результат обобщенной операции $\overset{\sim}{*}$ над НЧ $\underset{\sim}{X}$ и $\underset{\sim}{Y}$, представленными в виде

$$\underset{\sim}{X} = \{\alpha_1 / x_{11}; \alpha_2 / x_{21};\ \alpha_1 / x_{12}\} \text{ и } \underset{\sim}{Y} = \{\alpha_1 / y_{11}; \alpha_2 / y_{21};\ \alpha_1 / y_{12}\},$$

будет число $\underset{\sim}{Z} = \underset{\sim}{X} \overset{\sim}{*} \underset{\sim}{Y} = \{\alpha_1 / (x_{11} \overset{\sim}{*} y_{11});\ \alpha_2 / (x_{21} \overset{\sim}{*} y_{21});\ \alpha_1 / (x_{12} \overset{\sim}{*} y_{12})\}$

Как видим, операции выполняются над абсциссами точек, расположенных на одном уровне и участках одинаковой монотонности соответствующих ФП. Объединение соответствующих частей и составляет конечный результат.

Анализ метода показал, что сложение и умножение осуществляется аналогично МДМ для получения алгебраических решений (на левой диагонали). Соответственно и результаты умножения НЧ из примера 1, полученные ММО, будут идентичны результатам МДМ (см. рис. 2). Деление и вычитание (как операции не являющиеся возрастающими либо убывающими [15]) рекомендуется выполнять с использованием операции изменения знака и получения обратного значения, т.е. за 2 шага, в то время как в МДМ такой же результат получается за 1 шаг - на правой диагонали. В результате сравнения этих методов определено, что МДМ более приемлем для выполнения операций вычитания и деления с α-уровневыми НЧ.

Здесь и в последующих случаях будем полагать, что, если метод определен для работы с непрерывными исходными НЧ, но обрабатывает их не в аналитическом виде, а предусматривает дискретизацию этих чисел, то он будет определен как работающий с дискретными (будь то дискретизированные по α-уровням, либо каким-нибудь другим образом НЧ (см. табл. 2)).

Используя известную классификацию [12], можно теперь определить, что ММО применим для нормальных и субнормальных, выпуклых и невыпуклых, унимодальных, непрерывных дискретизированных, параметрических и непараметрических НЧ, но по описанию метода не ясно, можно ли его использовать для полимодальных НЧ.

В работе [14] предлагаются АУПО и МПО, которые описаны исключительно для толерантных НЧ. Исходная математическая модель в этих методах представляется в виде функции, аргументами которой являются, по аналогии с МДМ и ММО, α-уровневые НЧ.

Рассмотрим АУПО. Так, если задана функция от нечетких аргументов $\underset{\sim}{y}= f(\underset{\sim}{x}_1, \underset{\sim}{x}_2, \ldots, \underset{\sim}{x}_n)$, в которой НЧ представлены в виде разложения по α-уровневым множествам: $\underset{\sim}{y} = \bigcup_{\alpha\in[0,1]}\left(\underline{y}_\alpha, \overline{y}_\alpha\right)$, $\underset{\sim}{x}_i = \bigcup_{\alpha\in[0,1]}\left(\underline{x}_{i\alpha}, \overline{x}_{i\alpha}\right)$, $(i=\overline{1,n})$, то для любого α-уровня значение функции вычисляется по формулам:

$$\underline{y}_\alpha = \inf\left(f\left(x^*_{1\alpha}, x^*_{2\alpha}, \ldots, x^*_{n\alpha}\right)\right), \quad \overline{y}_\alpha = \sup\left(f\left(x^*_{1\alpha}, x^*_{2\alpha}, \ldots, x^*_{n\alpha}\right)\right), \tag{4}$$

где $x^*_{i\alpha} \in [\underline{x}_{i\alpha}, \overline{x}_{i\alpha}], (i=\overline{1,n})$.

Пример 3. Найдем значение функции $\underset{\sim}{y} = \underset{\sim}{x}_1 + \underset{\sim}{x}_2$, где $\underset{\sim}{x}_1 = (1_0, 5_0)\cup(2_1, 4_1)$ и $\underset{\sim}{x}_2 = (6_0, 12_0)\cup(8_1, 10_1)$.

Согласно (7) значение функции $\underset{\sim}{y}$ для нулевого и первого α-уровней будут составлять:

$\underline{y}_0 = \inf$ (1+6, 1+12, 5+6, 5+12) = 7, $\underline{y}_1 = \inf$ (2+8, 2+10, 4+8, 4+10) = 10,

$\overline{y}_0 = \sup$ (1+6, 1+12, 5+6, 5+12) = 17, $\overline{y}_1 = \sup$ (2+8, 2+10, 4+8, 4+10) = 14.

Таким образом, получим $\underset{\sim}{y} = (7_0, 17_0)\cup(10_1, 14_1)$.

Исходные НЧ и результаты вычислений представлены на рис. 3.

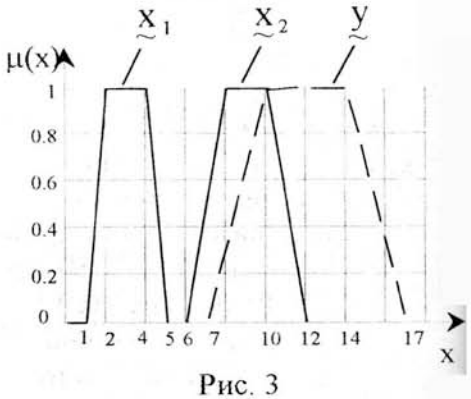


Рис. 3

Согласно описаниям метода [14] и классификации НЧ [12], отметим, что АУПО может быть использован для нормальных, выпуклых, толерантных, дискретных, непараметрических НЧ.

Анализируя АУПО, отметим, что здесь для получения результата потребуется выполнить больше операций, чем в ММО, а итоговые НЧ у них будут идентичны.

В МПО исходная функция $y= f(x_1, x_2, \dots, x_n)$ должна удовлетворять следующим условиям:

- область изменения любого аргумента непрерывна;

- на области определения функция дифференцируема;

- множество аргументов $X=\{x_1, x_2, \dots, x_n\}$ можно представить объединением не более, чем трех подмножеств $X = X_1 \cup X_2 \cup X_3$, причем

$$X_1 \cap X_2 = X_3 \cap X_2 = X_1 \cap X_3 = \varnothing;\ X_1 = \left\{ x_r : \frac{dy}{dx_r} \geq 0 \right\}\ (r = \overline{1, p_1});$$

$$X_2 = \left\{ x_s : \frac{dy}{dx_s} \leq 0 \right\}\ (s = \overline{1, p_2});$$

$$X_3 = \left\{ x_t :\ \operatorname{sign}\left(\frac{dy}{dx_t} \right) = h_t(x_r, x_s) \right\}\ (t = \overline{1, p_3};\ p_1 + p_2 + p_3 = n).$$

Здесь $\frac{dy}{dx_t} = g_t(x_r, x_s)$ - знакопеременная функция и для всех $x_t \in X_3$ знак производной $\frac{dy}{dx_t}$ не зависит от x_t, т.е. $\operatorname{sign}\left(\frac{dy}{dx_t} \right) \neq h(x_t)$.

Если $y = f(x_1, x_2, \dots, x_n)$ - функция от n переменных и ее аргументы x_i - НЧ вида

$$\underset{\sim}{X}_i = \bigcup_{\alpha \in [0,1]} \left(\underline{x}_{i\alpha}, \overline{x}_{i\alpha} \right),\ (i = \overline{1, n}),$$

то нечетким обобщением $\underset{\sim}{y} = f(\underset{\sim}{X}_1, \underset{\sim}{X}_2, \dots, \underset{\sim}{X}_n)$ будет названо число

$$\underset{\sim}{y} = \bigcup_{\alpha\in[0,1]} \left\{ f\left(\underline{x}_{r_\alpha}, \bar{x}_{s_\alpha}, x^{I}_{t_\alpha}\right), f\left(\bar{x}_{r_\alpha}, \underline{x}_{s_\alpha}, x^{II}_{t_\alpha}\right) \right\}, \qquad (5)$$

где $x^{I}_{t_\alpha} = \begin{cases} \underline{x}_{t_\alpha}, \text{ при } g_t\left(\underline{x}_r, \bar{x}_s\right) \geq 0 \\ \bar{x}_{t_\alpha}, \text{ при } g_t\left(\underline{x}_r, \bar{x}_s\right) < 0; \end{cases}$ $x^{II}_{t_\alpha} = \begin{cases} \bar{x}_{t_\alpha}, \text{ при } g_t\left(\bar{x}_r, \underline{x}_s\right) \geq 0 \\ \underline{x}_{t_\alpha}, \text{ при } g_t\left(\bar{x}_r, \underline{x}_s\right) < 0. \end{cases}$

Пример 4. Пусть исходная модель представлена в виде функции $y = x_1 + x_2$ и определена на области $x_1 \in [1, 5]$, $x_2 \in [6, 12]$. Требуется получить нечеткий аналог этой модели и определить $\underset{\sim}{y}$ при $\underset{\sim}{x}_1 = (1, 5)_0 \cup (2, 4)_1$, $\underset{\sim}{x}_2 = (6, 12)_0 \cup (8, 10)_1$.

Процедура 1. Найдем частные производные: $\frac{dy}{dx_1} = 1, \frac{dy}{dx_2} = 1$.

Процедура 2. Определим знаки частных производных:

$\frac{dy}{dx_1} > 0$ и $\frac{dy}{dx_2} > 0$ на всей области определения.

Процедура 3. Запишем нечеткую математическую модель $\underset{\sim}{y} = \underset{\sim}{x}_1 + \underset{\sim}{x}_2$ согласно (5) в виде $\underset{\sim}{y} = \bigcup_{\alpha\in[0,1]} \left\{ f\left(\underline{x}_{1_\alpha}, \underline{x}_{2_\alpha}\right), f\left(\bar{x}_{1_\alpha}, \bar{x}_{2_\alpha}\right) \right.$

Процедура 4. Определим значение функции $\underset{\sim}{y} = \underset{\sim}{x}_1 + \underset{\sim}{x}_2$ при заданных в условии задачи аргументах:

$\underline{y}_0 = 1+6 = 7$, $\underline{y}_1 = 2+8 = 10$, $\bar{y}_0 = 5+12 = 17$, $\bar{y}_1 = 4+10 = 14$.

Итак, получим $\underset{\sim}{y} = (7, 17)_0 \cup (10, 14)_1$.

МПО, в отличие от АУПО, более громоздкий метод, но при АУПО в операции нахождения значения одной компоненты участвуют значения переменных всех компонент на данном α-уровне, а при МПО - только соответствующее граничное значение каждого из аргументов на определенном уровне. Результаты же МПО будут идентичны АУПО (см. рис. 3).

Согласно описанию метода [14] и классификации НЧ [12], МПО можно применять для нормальных, выпуклых, толерантных, непрерывных (дискретизированных), параметрических НЧ.

МПЧ, обрабатывающий НЧ в L-R представлении [12, 13, 16], является методом быстрого приближенного вычисления результата НАО, отличающийся тем, что при выполнении арифметических операций используются только числовые параметры НЧ, а вид самих L-R функций важен лишь при выполнении некоторых специфических операций и часто используется только при получении окончательного ответа. К тому же, результат сложения и вычитания L-R НЧ есть L-R число, а результат умножения и деления будет НЧ лишь приблизительно [16].

Пусть унимодальные НЧ L-R типа $\underset{\sim}{X}$ и $\underset{\sim}{Y}$ характеризуется видом функций L и R, а также тремя параметрами $\underset{\sim}{X} = (m, \alpha, \beta)_{LR}$, $\underset{\sim}{Y} = (n, \gamma, \delta)_{LR}$, где m и n средние значения (мода) НЧ $\underset{\sim}{X}$ и $\underset{\sim}{Y}$; α, γ, а также β, δ - левые и правые коэффициенты нечеткости $\underset{\sim}{X}$ и $\underset{\sim}{Y}$ соответственно. Арифметические операции для таких чисел записываются как:

$$(m, \alpha, \beta)_{LR} + (n, \gamma, \delta)_{LR} = (m + n, \alpha + \gamma, \beta + \delta)_{LR};$$

$$-(m, \alpha, \beta)_{LR} = (-m, \alpha, \beta)_{LR};$$

$$(m, \alpha, \beta)_{LR} - (n, \gamma, \delta)_{LR} = (m - n, \alpha + \delta, \beta + \gamma)_{LR};$$

$$(m, \alpha, \beta)_{LR} \cdot (n, \gamma, \delta)_{LR} \approx (mn, \alpha n + \gamma m, \beta n + \delta m)_{LR}, \text{ при } \underset{\sim}{X} > 0, \underset{\sim}{Y} > 0;$$

$$(m, \alpha, \beta)_{LR} \cdot (n, \gamma, \delta)_{LR} \approx (mn, \gamma m - \beta n, \delta m - \alpha n)_{LR}, \text{ при } \underset{\sim}{X} > 0, \underset{\sim}{Y} < 0;$$

$$(m, \alpha, \beta)_{LR} \cdot (n, \gamma, \delta)_{LR} \approx (mn, \alpha n - \delta m, \beta n - \gamma m)_{LR}, \text{ при } \underset{\sim}{X} < 0, \underset{\sim}{Y} > 0;$$

$$(m, \alpha, \beta)_{LR} \cdot (n, \gamma, \delta)_{LR} \approx (mn, -\beta n - \delta m, -\alpha n - \gamma m)_{LR}, \text{ при } \underset{\sim}{X} < 0, \underset{\sim}{Y} < 0;$$

$$(m, \alpha, \beta)_{LR}^{-1} \approx \left(\frac{1}{m}, \frac{\beta}{m^2}, \frac{\alpha}{m^2}\right)_{LR}, \text{ при } \underset{\sim}{X} > 0;$$

$$(m, \alpha, \beta)_{LR} : (n, \gamma, \delta)_{LR} \approx \left(\frac{m}{n}, \frac{\delta m + \alpha n}{n^2}, \frac{\gamma m + \beta n}{n^2}\right)_{LR}, \text{ при } \underset{\sim}{X} > 0, \underset{\sim}{Y} > 0.$$

Как видим, формулы для операций умножения и деления зависят от знаков операндов $\underset{\sim}{X}$ и $\underset{\sim}{Y}$, при этом носители этих операндов не должны содержать ноль. Данный метод может применяться [12] для нормальных, выпуклых, унимодальных и толерантных, непрерывных, параметрических НЧ.

В работе [15] предложен довольно громоздкий МАО для непрерывных НЧ $\underset{\sim}{X}$ и $\underset{\sim}{Y}$ с известными областями определения $V_X = \{x\}$ и $V_Y = \{y\}$, где V_X, $V_Y \subset R$, а также заданной в аналитическом виде ФП. Областью определения НЧ $\underset{\sim}{Z}$ будет являться

$$V_Z = [\min(x^{\circ} * y^{\circ}, x^{\circ} * y^{*}, x^{*} * y^{\circ}, x^{*} * y^{*}), \quad (6)$$
$$\max(x^{\circ} * y^{\circ}, x^{\circ} * y^{*}, x^{*} * y^{\circ}, x^{*} * y^{*})] = [z^{\circ}, z^{*}],$$

где $x^{\circ} = \min_{x \in V_X} x$, $x^{*} = \max_{x \in V_X} x$, $y^{\circ} = \min_{y \in V_Y} y$, $y^{*} = \max_{y \in V_Y} y$, $z^{\circ} = \min_{z \in V_Z} z$, $z^{*} = \max_{z \in V_Z} z$.

Если $z \in V_Z$, то для любого $x \in V_X'$

$$V_X' = [\max(\min(z \circ y^{\circ}, z \circ y^{*}), x^{\circ}), \min(\max(z \circ y^{\circ}, z \circ y^{*}), x^{*})] \quad (7)$$

можно найти $y \in V_Y^{'}$:

$$V_Y^{'} = [\max(\min(z \circ x^{o}, z \circ x^{*}), y^{o}),\ \min(\max(z \circ x^{o}, z \circ x^{*}), y^{*})], \qquad (8)$$

такой, что $z = x * y$, $x = z \circ y$, $y = z \circ x$, где $\circ$ - обратная операция по отношению к $*$. При этом значение ФП определяется следующим образом:

$$\mu_Z(z) = \begin{cases} \max\limits_{x \in V_x^{'}} (\mu_X(x) \mu_X(x) = \mu_Y(z \circ x)), \text{если } \exists x : \mu_X(x) = \mu_Y(z \circ x); \\ \min(\max\limits_{x \in V_x} \mu_X(x), \max\limits_{y \in V_y} \mu_Y(y), \text{если } \forall x : \mu_X(x) \neq \mu_Y(z \circ x). \end{cases} \qquad (9)$$

Пример 5. Используя МАО, выполним умножение НЧ из примера 1, предварительно экстраполировав их с целью удовлетвореня исходным условиям метода. Для этого представим $\underset{\sim}{X}$ и $\underset{\sim}{Y}$ в виде непрерывных треугольных НЧ и, воспользовавшись правилом подобных треугольников, получим $\underset{\sim}{X} = \underset{\sim}{3} = \{0/0.5,\ 1/3,\ 0/8\}$ и $\underset{\sim}{3} = \underset{\sim}{5} = \{0/1,\ 1/5,\ 0/8.3\}$. Вычисление производится в несколько этапов.

1. Найдем область определения возможного решения по формуле (6):

$V_Z = [\min(0.5 \cdot 1,\ 0.5 \cdot 8.3,\ 8 \cdot 1,\ 8 \cdot 8.3),\ \max(0.5 \cdot 1,\ 0.5 \cdot 8.3,\ 8 \cdot 1,\ 8 \cdot 8.3)] = [0.5,\ 66.4]$

2. Выберем из данной области такое z, для которого необходимо определить значение ФП. Пусть z = 6.8.

3. Далее по формулам (11) и (12) найдем области определения $V_X^{'}$ и $V_Y^{'}$, в которых находятся такие x и y, что их сумма равна данному z:

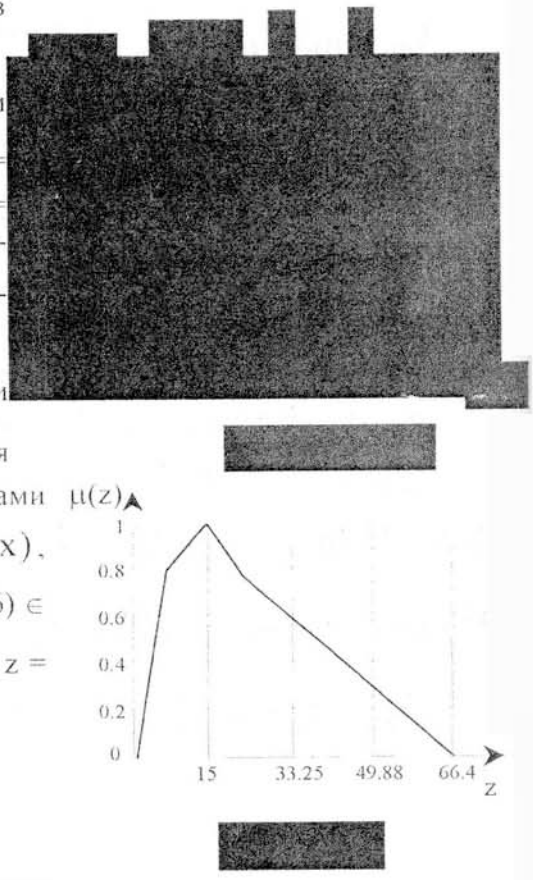
$V_X^{'} = [\max(\min(6.8:1, 6.8:8.3), 0.5),\ \min(\max(6.8:1,\ 6.8:8.3), 8)] = [0.82,\ 6.8]$,

$V_Y^{'} = [\max(\min(6.8:0.5, 6.8:8), 1),\ \min(\max(6.8:0.5, 6.8:8), 8.3)] = [1,\ 8.3]$.

4. Определим ФП в граничных точках $V_Y^{'}$ - в данном случае они известны (по условию).

5. Для построения ФП $\mu_Y(z:x)$ отобразим $V_Y^{'}$ на $V_X^{'}$, причем x = z : y. Так, при y = 1 x = 6.8 : 1 = 6.8, при y = 8.3 x = 6.8 : 8.3 = 0.82, при y = 5 x = 6.8 : 5 = 1.36. Значения функции сохраняются при соответствующих y. Получим точки графика ФП $\mu_Y(z:x) \in$ {(0/0.82), (1/1.36), (0/6.8)} (см. рис. 4).

6. Найдем точки пересечения ФП $\mu_Y(z:x)$ и $\mu_X(x)$ на области $V_X^{'}$. Их, очевидно, будет две. Первая получится при пересечении линий, образованных точками (0/0.5), (1/3) $\in \mu_X(x)$ и (0/0.82), (1/1.36) $\in \mu_Y(z:x)$, вторая - точками (0/0.5), (1/3) $\in \mu_X(x)$ и (0/6.8), (1/1.36) $\in \mu_Y(z:x)$. Согласно (9), определяет значение μ_z при z = 6.8 та из точек, у которой больше значение ФП.



Итак, для нахождения координат второй точки пересечения, в методе используется уравнение прямой, проходящей через две точки. После составления системы уравнений из полученных прямых (y = 0.4x - 0.2; y = 1.248 - 0.183x) и ее решения, определим, что x= 2.483, а y=$\mu_X(x)$=0.81, т.е., в соответствии с (9), при z = 6.8 $\mu_z(z)$= 0.81. Для точек z = 15 и z = 22.7 ФП будут соответственно иметь значения 1 и 0.77.

Графически результат представлен на рис. 5

МАО описан для кусочно-линейных ФП НЧ, а по классификации НЧ [12], можно определить, что он предназначен для нормальных и субнормальных, выпуклых, унимодальных и толерантных, непрерывных, параметрических НЧ.

Он, как и МНЧ, предназначен для НЧ с известными границами, здесь также как и в МНЧ, ФП итогового НЧ находится в зависимости от величины его носителей. Однако МАО более трудоемкий. Так, в примере 5 значение ФП для данного носителя было определено за 6 этапов, в то время как в МНЧ эта операция была выполнена с использованием одной формулы. К тому же, авторы не показали, как данный метод может применяться для выполнения вычитания и деления, поскольку формула (8) пригодна лишь для операций сложения и умножения.

Итак, согласно проведенным исследованиям, ММК, по сравнению с МДМ обладает более высокой информативностью, обеспечивая сохранение всего диапазона НЧ, полученного в результате выполнения НАО. Однако, в отличие от ММК, МДМ (по условию) обеспечивает постоянное число компонентов результата, зависящее от величины задаваемого α - уровня и его шага. Постоянное число компонент результата обеспечивают также ММО, МПО, АУПО и МПЧ.

Проанализировав вышеизложенное, можно сделать следующие выводы: если при решении вышеуказанных задач в области защиты информации нужна достаточно высокая информативность результата, то для выполнения НАО лучше использовать метод ММК, если можно обойтись более грубыми результатами, то лучше использовать МДМ, либо ММО, (с учетом всех вышеуказанных ограничений), при необходимости жесткой экономии ресурсов лучше выбрать МПЧ, а если должна присутствовать альтернатива при выборе количества компонентов итогового НЧ, то МАО. Некоторые из этих методов, согласно табл. 2, могут работать и с унимодальными НЧ. Отметим, однако, что ни в одном из рассмотренных методов авторами не определено, пригоден ли этот метод для обработки чисел разных классов или только одного, например, может ли быть одно из НЧ, участвующих в операции унимодальным, а другое - толерантным и т.п.

Также были проведены исследования выполнения законов коммутативности (К), ассоциативности (А), дистрибутивности (Д) при реализации НАО указанными методами для различных типов чисел. Их результаты занесены в табл. 2, где использованы следующие сокращения: 1(0) - выполнимость (невыполнимость) критерия, ОКК - одинаковое количество компонент в исходных НЧ, ИР - сохранение информативности результата, ЭР - существенная экономия аппаратных и программных ресурсов по отношению к ММК, НД(α) - необходимость приведения НЧ к α-уровневому виду, НУЭ - не описаны условия экстраполяции НЧ, РКК - возможность регулирования количества компонент при формировании итогового НЧ, УНО - необходимость учета выявленных недостатков и ограничений.

Таблица 2

Метод	Вид нечетких чисел									Выполняемые операции				Свойства	НЧ с ОКК	Подмножество ММК	Примечания
	Нормальные	Субнормальные	Выпуклые	Невыпуклые	Унимодальные	Полимодальные	Дискретные	Непрерывные	**Параметрические**	+	-	*	/				
ММК	1	1	1	1	1	1	1	0	0	1	1	1	1	КА	0	1	Самый точный, ИР
МДМ	1	1	1	0	1	0	1	0	0	1	1	1	1	КАД	1	1	НД(α), НУЭ, РКК, УНО
ММО	1	1	1	1	1	0	0	0	0	1	1	1	1	КА	1	0	НД(α), ЭР
МПО	1	0	1	0	0	0	0	0	0	1	1	1	1	КАД	1	1	НД(α), РКК, УНО, ЭР
АУПО	1	0	1	0	0	0	1	0	0	1	1	1	1	КАД	1	1	НД(α), РКК, ЭР
МПЧ	1	0	1	0	1	0	0	1	1	1	1	1	1	КАД	1	0	ЭР
МАО	1	1	1	0	1	0	0	1	1	1	0	1	0	---	0	0	ИР, НУЭ, РКК, УНО

СПИСОК ЛИТЕРАТУРЫ:

1. *Заде Л.А.* Понятие лингвистической переменной и его применение к принятию приближенных решений. - М.: Мир, 1976. - 166 с.
2. *Корченко А.Г., Черныш Л.Г.* Организация моделей систем оценки уровня защищенности с использованием нечетких множеств // Моделювання та інформаційні технології: Зб. наук. пр. ІПМЕ НАН України. Випуск 1. – Львів: Вид-во "Світ". – 1999. - С. 66 – 73.
3. Корченко А.Г., Черныш Л.Г. Оценка безопасности компьютерных систем на базе методов и моделей нечетких множеств // Защита информации: Сб. науч. тр. – К: КМУГА. – 1998. – С. 14-18.
4. Корченко А.Г., Черныш Л.Г. Методология синтеза систем оценки уровня безопасности информации в компьютерных системах // Збірник наукових праць ІПМЕ НАН України. Випуск 8.- Львів: НВМ ПТ УАД.- 1999.- С.72 - 77.
5. Корченко А.Г., Черныш Л.Г., Морозов А.С. Исследование методов и средств определения состояния безопасности информации в компьютерных системах // Збірник наукових праць УДМТУ.- Миколаїв: УДМТУ, 2000.- № 3 (369). – С. 152 –161.
6. Корченко А.Г., Щербина В.П., Черныш Л.Г. Логико-лингвистический подход в задачах оценки уровня безопасности информации в компьютерных системах // Збірник наукових праць ІПМЕ НАН України. Випуск 10.- Львів: НВМ ПТ УАД.- 2000.- С. 41 - 46.
7. Корченко А.Г., Щербина В.П., Черныш Л.Г. Система оценки уровня безопасности информации в компьютерных системах. Моделювання та інформаційні технології: // Збірник наукових праць ІПМЕ НАН України. Випуск 4. - Львів: НВМ ПТ УАД.- 1999.- С. 72 - 77.
8. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ (МГТУ), 1997. – 537 с.
9. Стенг Д., Мун С. Секреты безопасности сетей. - К.: Диалектика, 1995. – 544 с.

10. Корченко А.Г., Рындюк В.А., Мелешко Е.А., Пацира Е.В. Исследование нечетких операций для применения в системах защиты информации // Матеріали V Міжнародн. науково-практичної конф. "Безпека інформації в інформаційно-телекомунікаційних системах".- К.: Видавництво "Інтерлінк", НДЦ "ТЕЗІС" НТУУ "КПІ", 2002. - С. 56.

11. Корченко А.Г. Методы и аппаратные средства реализации нечетких операций // Автоматизированные системы обработки информации: Сб. науч. трудов. – К.: КМУГА, 1996. – С. 17-25.

12. Корченко А.Г., Рындюк В.А., Пацира Е.В. Классификация нечетких чисел для рационального применения в методах и моделях систем защиты информации // Матеріали V Міжнародн. науково-практичної конф. "Безпека інформації в інформаційно-телекомунікаційних системах".- К.: Видавництво "Інтерлінк", НДЦ "ТЕЗІС" НТУУ "КПІ", 2002. - С. 57.

13. Алтунин А.Е., Семухин М.В. Модели и алгоритмы принятия решений в нечетких условиях: Монография. Тюмень: Издательство Тюменского государственного университета, 2000. 352 с.

14. Ротштейн А.П., Штовба С.Д. Нечеткая надежность алгоритмических процессов. – Винница: Континент – ПРИМ, 1997. – 142 с.

15. Борисов А.Н., Крумберг О.А., И.П. Федоров. Принятие решений на основе нечетких моделей. Примеры использования. Рига: Зинатне, 1990 г.

16. Борисов А.Н., Алексеев А.В., Меркурьева Г.В. и др. Обработка нечеткой информации в системах принятия решений.. - М.: Радио и связь, 1989. – 304 с.

Поступила 20.07.2002
После доработки 11.09.2002

УДК 621.391:519.2

Алексейчук А. Н.

ОПТИМАЛЬНОЕ СЛУЧАЙНОЕ КОДИРОВАНИЕ РАВНОВЕРОЯТНЫХ СООБЩЕНИЙ В Q-ИЧНОМ СИММЕТРИЧНОМ КАНАЛЕ СВЯЗИ

Настоящая статья является непосредственным продолжением работ автора [1, 2], посвященных исследованию вероятностных характеристик систем передачи дискретной информации со случайным кодированием в канале связи с аддитивным шумом, распределенным на конечной абелевой группе. Ранее теоретико-информационные свойства и способы построения таких систем для случая двоичного симметричного канала (ДСК) изучались в [3 – 11] и ряде других работ.

Далее в статье свободно используются терминология и обозначения, введенные в [2]. Рассматриваемая нами математическая модель системы передачи информации со случайным кодированием представляет собой вероятностно-криптографическую систему (ВКС) $\mathfrak{R} = (S, \sigma, W)$, состоящую из источника (S, P_S), где S – конечное множество P_S – равномерное распределение вероятностей (РВ) на S, отображения σ: $Y \to S$ и стохастической матрицы (канала) $W = \left\| W\left(\frac{y}{x}\right) \right\|_{x,y \in Y}$, удовлетворяющих следующим условиям:

(а) S и Y – конечные абелевы группы;

(б) σ – равновероятная функция из Y в S,

$$|\sigma^{-1}(s)| = |Y|\,|S|^{-1},\ s \in S; \qquad (1)$$