

УДК 004.056

**Програмний засіб формування нечітких еталонів в інформаційній безпеці
методом побудови експоненційної функції**

Автор: О.М. Мильченко, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв

Науковий керівник: М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв

Вступ. Нечіткі системи широко використовуються в інформаційній безпеці використовуються як системи ідентифікації, навігації, управління, систем виявлення уразливостей в початкових кодах тощо, внаслідок зручності врахування числових та якісних факторів, в тому числі визначених експертом на інтуїтивному рівні. Крім того, визначення рівня захисту інформації, його зіставлення із заданим є складною науковою задачею, яка важко піддається структуризації та формалізації, і вимагає для свого рішення глибокого знання предметної області, великого практичного досвіду і навіть інтуїції. Розв'язок цієї задачі, як правило, ґрунтується на знаннях експертів і пов'язаний з високою трудомісткістю процедур аналізу та залежністю кінцевого результату від суб'єктивних факторів. Отже, для ефективного визначення стану безпеки інформації необхідно використовувати спеціальні інтелектуальні засоби, зокрема нечіткі еталони (НЕ).

Метою даної роботи є розробка програмного модуля формування нечітких еталонів методом побудови експоненційної функції для інтегрального програмного засобу формування і обробки нечітких еталонів [1-3].

Для досягнення поставленої мети необхідно розв'язати наступні задачі: проаналізувати сучасні методи формування нечітких еталонів за класичною теорією і особливості формування НЕ методами однозначної нечіткої логіки (ОНЛ) [1]; проаналізувати форми представлення вхідної і вихідної інформації блоку формування нечітких еталонів методом побудови експоненційної функції за класичною теорією та ОНЛ у складі автоматизованої системи формування і обробки нечітких еталонів (АСФОНЕ) [2]; розробити алгоритми визначення функцій належності (ФН) за методом побудови експоненційної функції за класичною теорією та ОНЛ та відповідний програмний модуль, для системи формування і обробки нечітких еталонів в інформаційній безпеці; сформулювати практичні рекомендації щодо використання розробленого програмного засобу.

Метод побудови експоненціальної ФН (ЕФН) заснований на експертних оцінках і може використовуватися як для безпосереднього формування ФН нечіткого числа (НЧ), що приблизно дорівнює деякому чіткому числу, на основі експоненційної функції, так і для формування ФН на основі інтервальних оцінок [3]. В обох випадках завданням експертного опитування є визначення параметрів заздалегідь заданої (експоненційної) функції.

Для побудови ФН числа, що приблизно дорівнює деякому K , можна використовувати функцію:

$$\mu_K(x) = e^{-\alpha(K-x)^2}, \quad (1)$$

де α визначають за виразом $\alpha = -4 \ln(0,5) / \beta^2$;

β - відстань між точками переходу, тобто, точками, в яких функція набуває значення 0,5.

Параметр β , як вказано в [3], визначають за спеціальним алгоритмом і таблиці, побудованої за даними експертного опитування. При розробці програмного модуля параметр β визначався з наступних міркувань: оскільки ФН НЧ за (1) є симетричною відносно вертикальної вісі, що проходить через точку $x=K$, то точки x_{05_1} та x_{05_2} , в яких $\mu(x_{05_1}) = \mu(x_{05_2}) = 0,5$, також розташовуються симетрично цієї вісі при визначенні ФН за класичною теорією. Експертним опитуванням визначають границі носія ФН $x_{\min}, x_{\max}$, такі, що $K = (x_{\max} - x_{\min}) / 2$, та координати точки x_{05_1} . Тоді координати точки x_{05_2} можуть бути визначені за формулою

$$x_{05_2} = x_{\max} - (x_{05_1} - x_{\min}), \quad (2)$$

Відповідно параметр β розраховується за формулою

$$\beta = x_{05_1} - x_{05_2} = x_{05_1} - x_{\max} + (x_{05_1} - x_{\min}) = 2x_{05_1} - (x_{\min} + x_{\max}) \quad (3)$$

Таким чином, для побудови ФН методом експоненційної функції при визначеному носії НМ достатньо задати лише координату x_{05_1} .

Функції належності, які формуються за методом ЕФН, можуть бути нормальними; опуклими; унімодальними або толерантними; безперервними і параметричними, тобто для НЕ у вигляді НЧ задовольняють вимогам ОНЛ [1].

Для формування нелінійних ФН для термів лінгвістичної змінної за класичною теорією ФН будуються незалежно для окремих термів, а за ОНЛ можуть визначатися за двома алгоритмами.

За першим алгоритмом спочатку визначаються ФН тільки для $x_{l-1}^T < x < x_l^T$ (зростаючі ФН) для всіх термів як $a e^{k(x_l - x_{l-1}^T)}$, а потім розраховуються значення ФН для $x_l^T < x < x_{l+1}^T$

$$\mu_{K_l}(x) = \begin{cases} 1 - ae^{k(x_l - x_{l-1}^T)} & \text{якщо } x_{l-1}^T < x_l < x_l^T; \\ ae^{k(x_{l+1}^T - x_l^T)} & \text{якщо } x_l^T < x_l < x_{l+1}^T, \end{cases} \quad (4)$$

де l – номер терму лінгвістичної змінної;

x_{l-1}^T – значення з числової шкали, що відповідає лінгвістичній змінній, при якому досягається максимум ФН попереднього (сусіднього зліва) терму;

x_{l+1}^T – значення з числової шкали, що відповідає лінгвістичній змінній, при якому досягається максимум ФН наступного (сусіднього справа) терму;

x_l^T – значення з числової шкали, що відповідає лінгвістичній змінній, при якому досягається максимум ФН поточного терму.

За другим алгоритмом спочатку визначаються ФН парних термів, а потім для непарних термів розраховуються ФН за формулою

$$\mu_l^H(x) = \begin{cases} 1 - \mu_{l-1}^\Pi(x), & \text{якщо } x_{l-1}^T < x_l < x_l^T; \\ 1 - \mu_{l+1}^\Pi(x), & \text{якщо } x_l^T < x_l < x_{l+1}^T, \end{cases} \quad (5)$$

де $\mu_l^H(x)$ – значення ФН поточного терму;

$\mu_{l-1}^\Pi(x)$ – значення ФН молодшого відносно поточного терму;

$\mu_{l+1}^\Pi(x)$ – значення ФН старшого відносно поточного терму;

Визначення ФН за (4) та (5) реалізується зовнішньою відносно розроблюваного блоку процедурою, тому реалізований алгоритм побудови ФН методом ЕФН має вигляд, наведений на рис.1.

Вихідні дані в АСФОНЕ блоків формування НЕ стандартизовані з метою узагальнення процедур подальшої обробки НЕ. Тому в даному програмному модулі вихідними даними є формула для розрахунку ФН з визначеними в результаті обчислень параметрами α , β для НЧ, що приблизно дорівнює K , а також сформований НЕ у вигляді $A^M = \{x, (\mu_A(x)); x \in X\}$ (рис.2).

Висновки. В результаті аналізу сучасних методів формування нечітких еталонів за класичною теорією і особливостей формування НЕ методами визначено, що метод експоненційної функції в разі представлення НЕ як НЧ може безпосередньо застосовуватися як для побудови ФН за класичною теорією, так і за ОНЛ. У випадку, коли НЕ представлений як лінгвістична змінна, то метод експоненційної функції може за класичною теорією застосовуватися для незалежної побудови ФН окремих термів, а за ОНЛ ФН можуть визначатися за додатковими алгоритмами, які містять як складову блок методу експоненційної функції.



Рисунок 1 – Узагальнений алгоритм визначення ФН методом ЕФН

```

Membership function: m(x)=exp(-0.384815*(9.5-x)^2)
FUZZY STANDARD
< < 6, 0.00896899>; < 7, 0.0902571>; < 8, 0.420701>; < 9, 0.908279>; < 10, 0.908279>; < 11, 0.420701>; < 12, 0.0902571>; < 13, 0.00896899>; >
Membership function by DFL:Membership function by DFL for the junior term:
x[0]=6 m=0.961927
Membership function by DFL for the junior term:
x[1]=7 m=0.840927
Membership function by DFL for the junior term:
x[2]=8 m=0.558274
Membership function by DFL for the junior term:
x[3]=9 m=0.184755
Membership function by DFL for the older term
x[4]=10 m=0
Membership function by DFL for the older term
x[5]=11 m=0.184755
Membership function by DFL for the older term
x[6]=12 m=0.558274
Membership function by DFL for the older term
x[7]=13 m=0.840927
Membership function by DFL for the older term
x[8]=14 m=0.961927

```

Рисунок 2 – Вивод результату

Розроблений програмний блок може використовуватися як окремий модуль, або вбудовуватися в АСФОНЕ чи в прикладні інтелектуальні системи інформаційної безпеки, а також використовуватися в навчальному процесі.

Найбільш доцільним є використання розробки в системах реального часу внаслідок зменшення обсягу оброблюваної інформації і спрощення роботи експертів при побудові ФН за ОНЛ порівняно з КТ.

Список літератури:

1. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1.- Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007.-140 с.
2. Мігунов В.О., Турти М.В. Розробка програмного засобу обробки нечітких еталонів //Матеріали II Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2012/ – С.142-147.
3. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: “МК-Пресс”, 2006. – 320 с.