

УДК 004.05(081)

Програмний модуль вибору методу формування нечітких еталонів в інформаційній безпеці автоматизованої системи формування і обробки нечітких еталонів

***Автор:** Ю.О. Горбунов, 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. Головним критерієм якості систем захисту інформації є відповідність міцності захисту інформації заданому діапазону значень, причому багато впливових факторів мають нечіткий характер і підлягають обробці методами нечіткої логіки. Нечіткі системи використовуються в інформаційній безпеці 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. Одним з напрямів використання нечітких знань є обробка даних за допомогою нечітких еталонів (НЕ) [1-4]. Розв'язок таких задач, як правило, пов'язаний з високою трудомісткістю процедур аналізу нечітких даних та залежністю кінцевого результату від суб'єктивних факторів. Крім того, робота з НЕ передбачає в більшості випадків наявність бібліотеки еталонів і повторюваність типових процедур обробки даних, і тому ефективно може виконуватися тільки в автоматизованому режимі.

Метою даної роботи є розробка програмного модуля формування нечітких еталонів за сукупністю методів для інтегрального програмного засобу формування і обробки нечітких еталонів.

Основна частина. Для досягнення поставленої мети були розв'язані наступні задачі: проведено аналіз сучасних методів формування і обробки НЕ; розроблені алгоритми обробки НЕ за певними методами і програмний блок обробки НЕ за сукупністю методів.

Основою вибору методу формування нечітких еталонів в інформаційній безпеці автоматизованої системи формування і обробки нечітких еталонів (АСФОНЕ) [1] є класифікація методів формування НЕ, яка може здійснюватися за чотирма ознаками:

1. За типом НЕ:

а) нечітке число (НЧ) – визначається як $\langle a, U, A \rangle$, де a – найменування змінної, $U=\{u\}$ – область визначення змінної (набір можливих значень u), $A=\{\langle \mu_A(u)|u \rangle\}$ – нечітка множина, що описує обмеження на можливі значення змінної a (семантику). Нечітка змінна – це теж саме, що і нечітке число, тільки з додаванням імені, яким формалізується поняття, що описується цим числом;

б) лінгвістична змінна (ЛЗ) – множина нечітких змінних. Характеризується терм-множиною (множиною всіх можливих значень лінгвістичної змінної). Терм, що є елементом терм-множини формалізується нечіткою множиною за допомогою функції належності;

в) правило – П1: якщо $x \in A1$ і $y \in B1$, то $z \in C1$.

2. За теоретичними основами формування НЕ:

а) класична теорія [2]; функції належності визначаються експертом у вигляді математичних, табличних, графічних залежностей на рівні інтуїції з врахуванням їх взаємного впливу без обмежень на значення амплітуди, форму і розташування на універсумі. Лінгвістична змінна описується як $\langle A, T, U, G, M \rangle$, де A – ім'я змінної; T – терм-множина $T=\{t_i\}$, кожен елемент якої задається нечіткою множиною на універсальній множині U ; G – синтаксичні правила (часто у вигляді граматики), що породжують назву термів; M – семантичні правила, що задають функції приналежності нечітких термів, породжених синтаксичними правилами з G . Нечітка множина t_i – це множина пар (x_j, μ_j) , де x_j – число з універсуму, а μ_j – функція належності (міра впевненості експерта) елемента x_j нечіткій множині t_i ;

б) однозначна нечітка логіка (ОНЛ) [3]: функції належності мають форму, задану параметрично, максимум функції належності поточного терму дорівнює 1 і припадає на мінімум (0) функції належності попереднього терму, додатково задаються граничні точки. Експерт визначає граничні точки і точки максимумів функцій належності. Нечітка множина t_i -це множина пар $(x_j, f(x))$, де x_j – число з універсуму, для якого $\mu_j = 1$, $f(x)$ – монотонна функція.

3. За методами формування функцій належності (ФН): метод опитування; числовий метод; метод лінгвістичних термів; метод кількісного парного порівняння; метод порівняння з визначенням квадратного кореня; метод порівняння із знаходженням результату ділення; метод парного порівняння найменших квадратів; метод парних порівнянь на рангових оцінках; метод призначення параметрів; метод коригування параметрів; метод побудови експоненціальної функції; метод прямого і зворотного оцінювання; метод інтервальних оцінок; метод рівневих множин.

4. За властивостями ФН нечітких чисел

а) нормальність: субнормальні, нормальні;

б) модальність: унімодальні, толерантні, полімодальні;

в) опуклість: опуклі, неопуклі;

г) безперервність: неперервні, дискретні;

д) параметричність: параметричні, непараметричні.

Методи обробки нечітких еталонів можуть бути поділені на дві групи операцій:

1. Операції з одиничними НМ:

- а) визначення властивостей НМ;
- б) нормалізація НМ;
- в) визначення α - рівнів НМ;
- г) визначення центра тяжіння НМ;
- д) розклад НМ по α - рівням.

2. Операції з множиною НМ:

- а) операції нечіткої арифметики:

- б) порівняння нечітких чисел на основі функції впорядкування або узагальненої відстані

Хеммінга, або методом впорядкування чи методом центра тяжіння.

Проведений аналіз дозволив визначити задачі формування та обробки НЕ за сукупністю методів в АСФОНЕ:

1. Формування НЕ обраним методом:

- а) вибір теоретичних основ побудови НЕ (замовник еталону (ЗЕ) або зважена експертна оцінка);

- б) вибір методу формування НЕ (ЗЕ або зважена експертна оцінка);

- в) визначення кількості експертів (ЗЕ);

- г) визначення вагових коефіцієнтів експертів (ЗЕ або зважена експертна оцінка);

- д) визначення питання, що підлягає експертній оцінці;

- е) отримання експертних даних:

- завдання питання до експерта;
- виведення питання до експерта;
- отримання числових або лінгвістичних даних від експерта;
- зважування експертних оцінок числових або лінгвістичних даних.

2. Обробка НЕ

- а) вибір типу обробки одиничної ФН або групи ФН;

- б) вибір процедури обробки одиничної ФН або групи ФН;

- в) визначення властивостей ФН.

3. Відображення результату дії пп.1,2

4. Збереження еталону у бібліотеці

5. Вилучення еталону з бібліотеки.

Вхідними даними для побудови ФН в АСФОНЕ прийнято теоретичні основи побудови НЕ, які обмежують спектр доступних методів побудови ФН; тип НЕ, метод визначення ФН, який

обирається зваженою експертною оцінкою з доступних за теоретичними основами методів; характеристики носія НМ.

Теоретичні основи побудови НЕ визначаються у відповідності до вимог щодо наявності чи відсутності зон толерантності, вимог щодо $\sum_{j=1}^N \mu_j(x_i) = 1$. Додатковою вимогою може бути відсутність зон невизначеності між носіями НМ, що відповідають термам ЛЗ. Ця вимога є обов'язковою але недостатньою для вибору ОНЛ в якості теоретичної основи побудови НЕ у вигляді лінгвістичної змінної.

Тип НЕобирається зваженою експертною оцінкою з міркувань відповідності предмету оцінювання.

Метод визначення ФНобирається відповідно до вимог щодо бажаних властивостей ФН, оскільки кожен метод забезпечує певні властивості ФН. Зваженою експертною оцінкою визначається набір бажаних властивостей ФН і автоматично перевіряється його непротиворічність. Методи визначення ФН, що забезпечують визначений набір властивостей отримують мітку доступності. Далі експерти оцінюють доступні методи і автоматично визначається метод з максимальною сумарною зваженою експертною оцінкою.

Характеристики носія НМ (тип координат, граничні точки, кількість точок та їх розташування на носії НМ) визначаються зваженою експертною оцінкою для всіх методів формування ФН.

Вхідними даними для обробки НЕ в АСФОНЕ процедурами порівняння і відображення НЕ прийнято характеристики носія НМ (тип координат, граничні точки, кількість точок та їх розташування на носії НМ) та ФН нечіткого числа або терму ЛЗ у вигляді $A^M = \{x, \mu_A(x)\}$ НМ. Для визначення властивостей НЕ вхідними даними є метод формування НЕ, який визначає досяжну множину властивостей, і ФН у вигляді НМ для уточнення властивостей по додатковим алгоритмам для окремих методів, які дозволяють отримати ФН з протирічними властивостями (наприклад, унімодальні – полімодальні).

На рис.1. наведено узагальнений алгоритм, який застосовується для вирішення наступних задач: вибору теоретичних основ побудови НЕ; вибору методу формування НЕ; вибору типу координат числової шкали; вибору типу НЕ як одиничної ФН або групи ФН/ вибору процедури обробки одиничної ФН або групи ФН; збереження еталону у бібліотеці; вилучення еталону з бібліотеки.

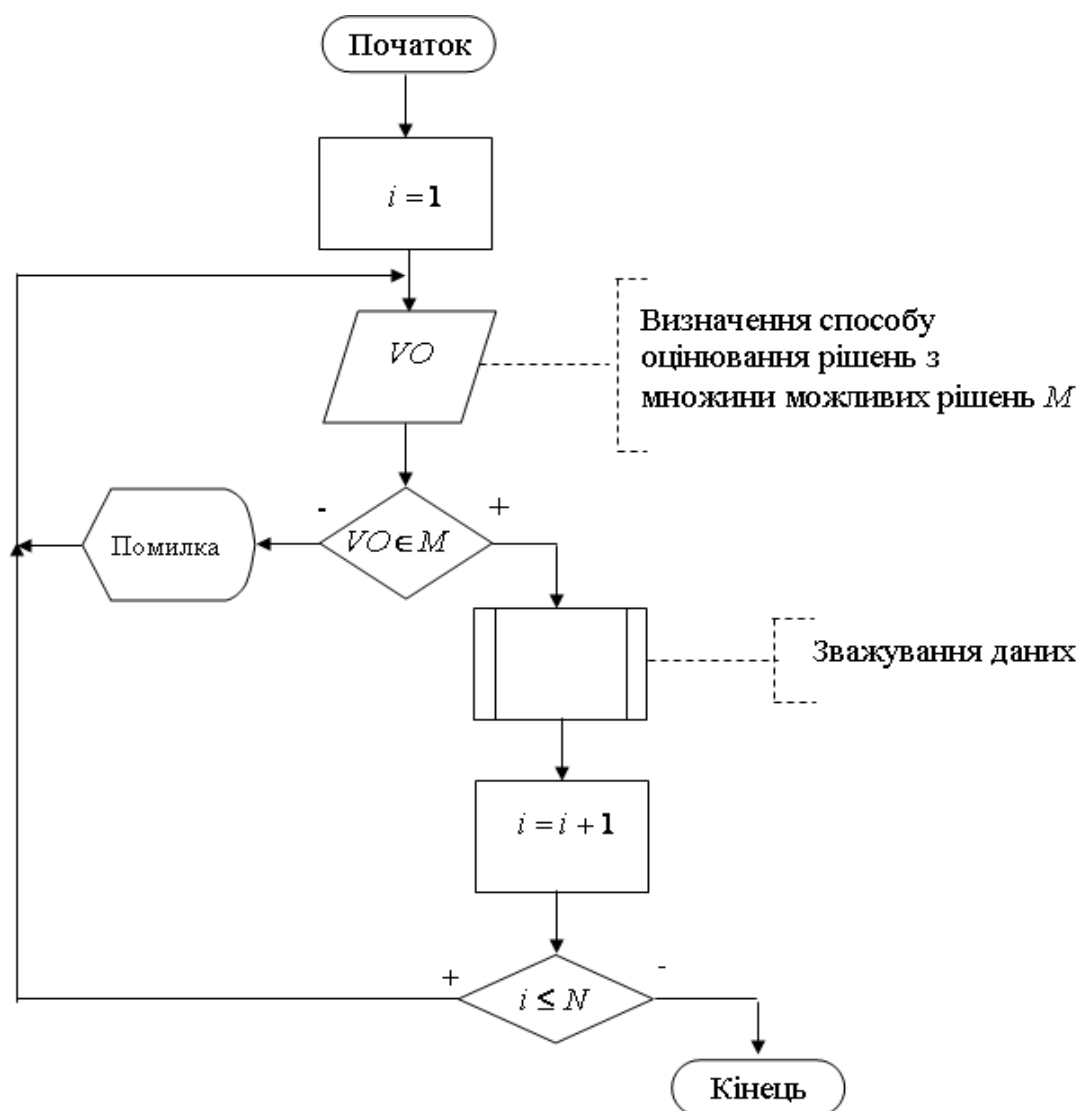


Рисунок 1 – Узагальнений алгоритм

На рис.2 наведено результати спрацювання розробленого програмного модуля при виборі методу формування НЕ.

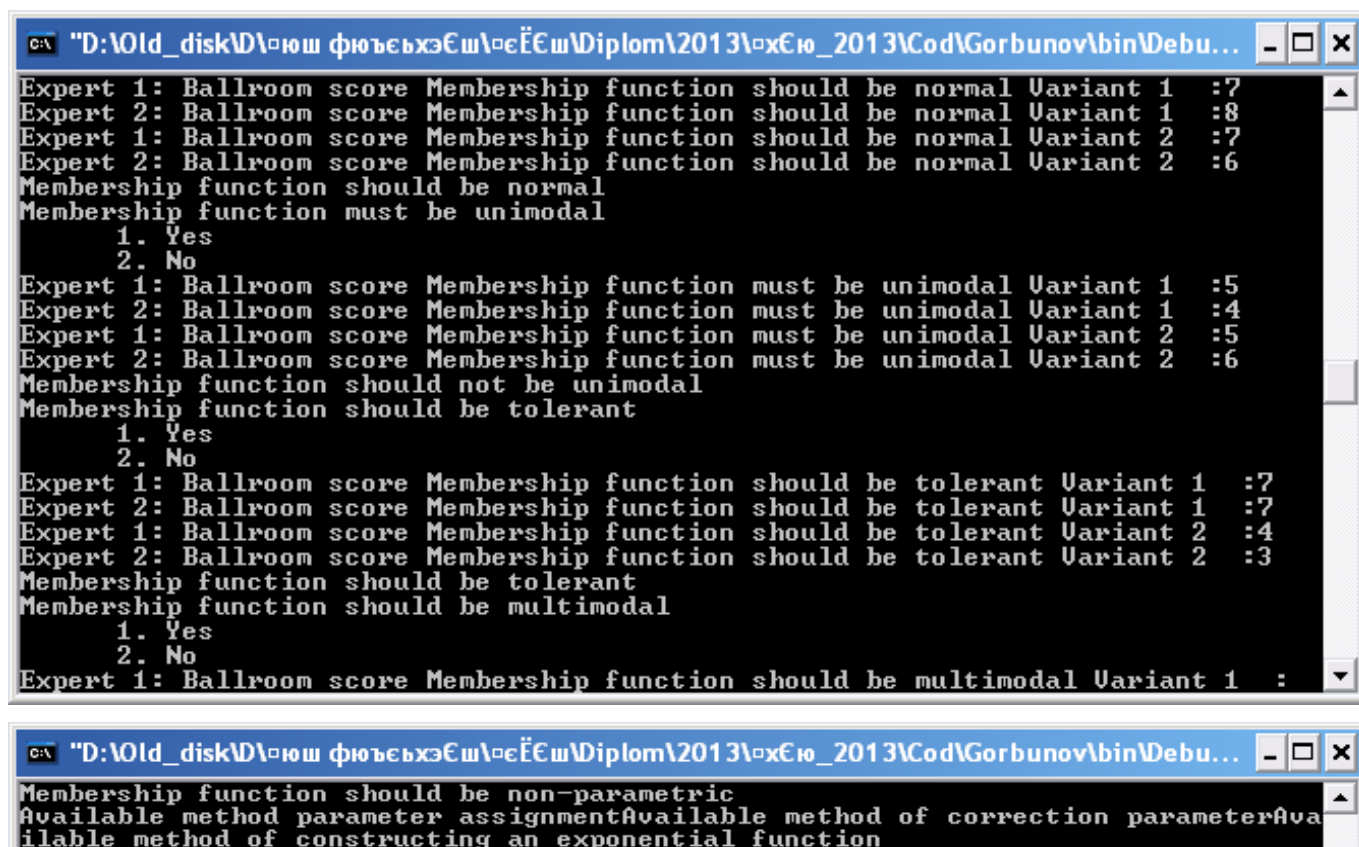
Висновки.

1. В роботі на основі проведеного аналізу особливостей побудови інтелектуальних систем з використанням НЕ; сучасних методів обробки НЕ, форм їх представлення була розроблена структура блоку формування НЕ за сукупністю методів для роботи у складі автоматизованої системи формування і обробки НЕ.

2. Розроблено програмний модуль формування нечітких еталонів.

3. Визначено галузі застосування розробленого програмного модуля в інформаційній безпеці:

– навчальний процес підготовки фахівців галузі знань 1701 «Інформаційна безпека» в рамках курсів «Методи системного аналізу», «Теорія статистичних рішень і ситуаційного аналізу», «Розпізнавання образів в системах захисту інформації»;



```

C:\ "D:\Old_disk\Діюш фюьєьхэЄш\оєЁЄш\Diplom\2013\оxЄю_2013\Cod\Gorbunov\bin\Debu...
Expert 1: Ballroom score Membership function should be normal Variant 1 :7
Expert 2: Ballroom score Membership function should be normal Variant 1 :8
Expert 1: Ballroom score Membership function should be normal Variant 2 :7
Expert 2: Ballroom score Membership function should be normal Variant 2 :6
Membership function should be normal
Membership function must be unimodal
1. Yes
2. No
Expert 1: Ballroom score Membership function must be unimodal Variant 1 :5
Expert 2: Ballroom score Membership function must be unimodal Variant 1 :4
Expert 1: Ballroom score Membership function must be unimodal Variant 2 :5
Expert 2: Ballroom score Membership function must be unimodal Variant 2 :6
Membership function should not be unimodal
Membership function should be tolerant
1. Yes
2. No
Expert 1: Ballroom score Membership function should be tolerant Variant 1 :7
Expert 2: Ballroom score Membership function should be tolerant Variant 1 :7
Expert 1: Ballroom score Membership function should be tolerant Variant 2 :4
Expert 2: Ballroom score Membership function should be tolerant Variant 2 :3
Membership function should be tolerant
Membership function should be multimodal
1. Yes
2. No
Expert 1: Ballroom score Membership function should be multimodal Variant 1 :
Membership function should be non-parametric
Available method parameter assignment Available method of correction parameter Ava
ilable method of constructing an exponential function
  
```

Рисунок 2 – Результати опитування експертів щодо бажаних властивостей ФН
і висновки щодо доступних методів формування ФН

– біометричні криптографічні системи, системи комп'ютерного зору, системи аналізу фаз процесу роботи програмного забезпечення.

Розроблений програмний модуль може використовуватися в біометричних криптографічних системах для біометричної автентифікації і системах на основі fuzzy extractors, в системах «комп'ютерного зору» для пошуку еталону на зображенні; в автоматизованих системах аналізу програмного забезпечення для виявлення аномальної (відмінної від еталонної) поведінки програмного забезпечення на різних фазах роботи.

Список літератури:

1. В.О. Мігунов В.О. Програмна обробка нечітких еталонів // Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2011. – С.97-101.
2. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.
3. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1.- Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007.-140 с.

4. Биометрические криптографические системы и их применение [Электронный ресурс]/ О.В. Куликова, О.П.Цветочкин // EUROCRYPT. – 2005. – №11. – с.53-57. – Режим доступа: www.pvti.ru/data/file/bit/bit_3_2009_10.pdf.