УДК 004.056.5

канд. техн. наук Самойлов І. В. ORCID: 0000-0002-8251-9257 (ІСЗЗІ КПІ)
д-р техн. наук Чевардін В. Є. ORCID: 0000-0002-1070-4568 (ВІТІ)
канд. техн. наук Конотопець М. М. ORCID: 0000-0002-6963-1877 (ІСЗЗІ КПІ)
канд. техн. наук Сторчак А. С. ORCID: 0000-0002-5267-3122 (ІСЗЗІ КПІ)

ПОСЛІДОВНИЙ МЕТОД НАСТРОЙКИ НЕЧІТКИХ ВІДНОШЕНЬ ІНТЕРВАЛЬНОГО ТИПУ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

На сьогодні актуальною науково-технічною проблемою є створення систем оцінки захищеності інформаційних систем від загроз, які можуть опрацьовувати нечітку інформацію. Дані систем дозволяють визначати, які дії ефективні для мінімізації та попередження загроз. Нечітка модель будується на основі композиційного правила виведення Заде, в якому носієм інформації є матриця нечітких відношень „загрози – збитки", що зв'язує вектор мір значимості загроз і вектор мір значимості збитків. При проєктуванні подібних систем на базі нечітких відношень необхідно визначати множину її параметрів (Ω_I – множина параметрів, які визначають модель системи на базі нечітких відношень I типу, та Ω_{II} – множина параметрів, які визначають модель системи на базі нечітких відношень II типу). На сьогоднішній день для настройки нечітких систем інтервального типу використовується незалежний метод, який передбачає визначення множини Ω_{II} з „нуля", не використовуючи результати настройки множини параметрів Ω_I, що призводить до збільшення часу настройки.

У статті запропоновано послідовний метод настройки нечітких відношень інтервального типу, який передбачає спочатку визначення множини параметрів нечітких відношень I типу за допомогою генетико-нейронного алгоритму, а потім на їх базі настройку тільки додаткових параметрів, що дозволяє зменшити середній час настройки нечіткої моделі та оцінити вплив невизначеності на точність оцінки.

Ключові слова: *нейро-нечітка мережа, нейронна мережа, невизначеність, нечіткі відношення, нечіткі множини, інтервальна функція належності, загрози, збитки.*

I. Samoylov, V. Chevardin, N. Konotopets, A. Storchak. A sequential method of tuning interval-type fuzzy relations for assessing the security of information systems.

Today, an urgent scientific and technical problem is the creation of systems for assessing the security of information systems from threats that can process fuzzy information. These systems allow you to determine what actions are effective to minimize and prevent threats. The fuzzy model is built on the basis of the Zadeh compositional inference rule, in which the information carrier is the matrix of fuzzy "threat-damage" relations connecting the vector of measures of the significance of threats and the vector of measures of significance of damage. When designing such systems based on fuzzy relations, it is necessary to determine a set of its parameters (Ω_I - a set of parameters that determine a system model based on fuzzy relations of type I and Ω_{II} - a set of parameters that define a system model based on fuzzy relations of type II). To date, for tuning interval-type fuzzy systems, an independent method is used, which assumes the determination of the set Ω_{II} from "zero", without using the results of tuning the set of parameters Ω_I, which leads to an increase in the setup time.

The article proposes a sequential method for adjusting fuzzy relations of interval type, which firstly provides for the determination of a set of parameters of fuzzy relations of type I using a genetic-neural algorithm, and then, on their basis, adjustment of only additional parameters, which makes it possible to reduce the average tuning time of a fuzzy model and assess the effect of uncertainty on the accuracy of the assessment.

Keywords: *neural-fuzzy network, neural network, uncertainty, fuzzy relations, fuzzy sets, interval membership function, threats, losses.*

Постановка завдання. На сьогодні актуальною науково-технічною проблемою є створення систем оцінки захищеності інформаційних систем від загроз, які можуть опрацьовувати нечітку інформацію. Дані систем дозволяють визначати, які дії ефективні для мінімізації та попередження загроз. На основі аналізу захищеності можна прогнозувати можливий збиток від реалізації загрози, його оцінку та рекомендувати необхідні дії. У базах знань таких систем міститься не тільки кількісна інформація, що характеризує стан інформаційної системи, а й якісна інформація, яка являє собою експертні оцінки. Для формалізації експертної інформації при моделюванні причинно-наслідкових зв'язків зручно використовувати теорію нечітких множин [1; 2]. Нечітка модель будується на основі композиційного правила виведення Заде [3], в якому носієм інформації є матриця нечітких відношень „загрози – збитки", що зв'язує вектор мір значимості загроз і вектор мір значимості збитків.

Аналіз останніх публікацій. При проєктуванні систем оцінки захищеності інформаційних систем від загроз виникає проблема моделювання і мінімізація наслідків невизначеності.

В роботах [4–6] розглядаються методичні аспекти побудови нечітких систем, що здатні оперувати з різними типами невизначеності. В нечітких системах I типу використовуються точні функції належності, коли ступінь належності є чітким числом, тобто невизначеність, щодо значень слів, повністю ігнорується. В нечітких системах II типу з'являється можливість моделювати невизначеність, пов'язану зі значенням слів за рахунок введення інтервальних функцій належності. Останні дозволяють оперувати з різними видами невизначеності, що виникають в реальних системах оцінки захищеності інформаційних систем.

У загальному випадку, при проєктуванні подібних систем на базі нечітких відношень, необхідно визначити множину її параметрів. Нехай: Ω_{I} – множина параметрів, які визначають модель системи на базі нечітких відношень I типу (параметри функцій належності вхідних (вихідних) змінних до нечітких термів загроз (збитків) та параметри концентрації функцій належності нечітких множин збитків); Ω_{II} – множина параметрів, які визначають модель системи на базі нечітких відношень II типу (параметри нижніх і верхніх функцій належності вхідних (вихідних) змінних до нечітких термів загроз (збитків) та параметри концентрації нижніх і верхніх функцій належності нечітких множин збитків, що задають інтервали значень нечітких відношень). Між множинами Ω_{I} та Ω_{II} згідно з [4] виконується співвідношення: $\Omega_{\text{I}} \subset \Omega_{\text{II}}$, тобто при проєктуванні систем II типу використовуються додаткові параметри Ω'. Для настройки нечітких систем II типу в роботі [4] використовується *незалежний метод*, який передбачає визначення множини Ω_{II} з „нуля", не використовуючи результати настройки множини параметрів Ω_{I} нечіткої системи I типу, що призводить до збільшення часу настройки.

Мета роботи. Запропонувати *послідовний метод* настройки, який передбачає спочатку визначення множини параметрів Ω_{I}, а потім на їх базі настройку тільки додаткових параметрів Ω', що дозволить зменшити середній час настройки нечіткої моделі та оцінити вплив невизначеності на точність оцінки захищеності інформаційних систем.

Виклад основного матеріалу. Нехай навчальна вибірка задана у вигляді M пар експериментальних даних:

$$\left\langle \hat{X}_p, \hat{Y}_p \right\rangle, \; p = \overline{1, M},$$

де $\hat{X}_p = \left(\hat{x}_1^p, \hat{x}_2^p, \ldots, \hat{x}_n^p\right)$ – вектор значень вхідних змінних в експерименті номер p;

$\hat{Y}_p = \left(\hat{y}_1^p, \hat{y}_2^p, \ldots, \hat{y}_m^p\right)$ – вектор значень вихідних змінних в експерименті номер p.

Припустимо, що $\tilde{s}_j, \; j = \overline{1, \; m}$ – деякий збиток, який розглядається як нечітка множина II типу. Нечітка множина, за допомогою якої формалізується терм $\tilde{s}_j$, являє собою сукупність пар: $\tilde{S}_j = \left\{ \frac{\mu_1^{\tilde{s}_j}}{d_1}, \frac{\mu_2^{\tilde{s}_j}}{d_2}, \ldots, \frac{\mu_n^{\tilde{s}_j}}{d_n} \right\}$, де $\{d_1, \; d_2, \; \ldots, \; d_n\} = D$ – універсальна множина загроз, на якій задається нечітка множина $\tilde{s}_j$; $\mu_i^{\tilde{s}_j}$ – вторинна функція належності елемента $d_i \in D, \; i = \overline{1, \; n}$ нечіткій множині $\tilde{s}_j$ [7].

Нехай $\underline{Q} = \left(\underline{q}_1, \underline{q}_2, \ldots, \underline{q}_m\right)$ і $\overline{Q} = \left(\overline{q}_1, \overline{q}_2, \ldots, \overline{q}_m\right)$ – вектори параметрів концентрації нижніх і верхніх функцій належності збитків $\tilde{s}_j$ такі, що матриця нечітких відношень має вигляд:

$$R = \begin{bmatrix} \left[\underline{r}_{11}^{\underline{q}_1}, \overline{r}_{11}^{\overline{q}_1}\right] & \left[\underline{r}_{12}^{\underline{q}_2}, \overline{r}_{12}^{\overline{q}_2}\right] & \ldots & \left[\underline{r}_{1m}^{\underline{q}_m}, \overline{r}_{1m}^{\overline{q}_m}\right] \\ \left[\underline{r}_{21}^{\underline{q}_1}, \overline{r}_{21}^{\overline{q}_1}\right] & \left[\underline{r}_{22}^{\underline{q}_2}, \overline{r}_{22}^{\overline{q}_2}\right] & \ldots & \left[\underline{r}_{2m}^{\underline{q}_m}, \overline{r}_{2m}^{\overline{q}_m}\right] \\ \ldots & \ldots & \ldots & \ldots \\ \left[\underline{r}_{n1}^{\underline{q}_1}, \overline{r}_{n1}^{\overline{q}_1}\right] & \left[\underline{r}_{n2}^{\underline{q}_2}, \overline{r}_{n2}^{\overline{q}_2}\right] & \ldots & \left[\underline{r}_{nm}^{\underline{q}_m}, \overline{r}_{nm}^{\overline{q}_m}\right] \end{bmatrix}. \qquad (1)$$

З урахуванням матриці (1) співвідношення, яке визначає залежність „загрози – збитки" для нечіткої системи діагностики ІІ типу, можна записати в такому вигляді:

$$Y = f\left(X,\ C_X,\ P_{\tilde{D}},\ Q_{\tilde{R}},\ P_{\tilde{S}}\right), \tag{2}$$

де X – множина вхідних змінних;

Y – множина вихідних змінних;

$P_{\tilde{D}} = \left(\underline{G}_{\tilde{D}},\ \overline{G}_{\tilde{D}},\ C_{\tilde{D}}\right)$ – вектори параметрів нижніх і верхніх функцій належності вхідних змінних до нечітких термів загроз;

$P_{\tilde{S}} = \left(\underline{G}_{\tilde{S}},\ \overline{G}_{\tilde{S}},\ C_{\tilde{S}}\right)$ – вектори параметрів нижніх і верхніх функцій належності вихідних змінних до нечітких термів збитків;

C_X – вектор параметрів концентрації функцій належності, що моделюють неточність вхідних змінних.

Задача настройки нечітких відношень інтервального типу може бути сформульована так: необхідно підібрати такі вектори параметрів нижніх і верхніх функцій належності вхідних (вихідних) змінних та параметрів концентрації нижніх і верхніх функцій належності збитків, а при наявності неточних вхідних даних і вектори параметрів концентрації функцій належності, що моделюють цю неточність, які забезпечують мінімальну відстань між теоретичними і експериментальними виходами об'єкта:

$$\sum_{p=1}^{M}\left[\sum_{j=1}^{m}\left[f_j\left(\hat{X}_p,\ C_X,\ P_{\tilde{D}},\ Q_{\tilde{R}},\ P_{\tilde{S}}\right) - \hat{y}_j^p\right]^2\right] = \min_{C_X, P_{\tilde{D}}, Q_{\tilde{R}}, P_{\tilde{S}}}. \tag{3}$$

В роботі для настройки нечітких відношень інтервального типу пропонується використовувати послідовний метод, суть якого полягає в тому, що настройка таких нечітких відношень здійснюється не з нуля, а використовується результат настройки нечітких відношень І типу. В даному випадку на другому етапі пропонується використовувати нейро-мережевий метод [8; 9]. Етапи настройки приведені в табл. 1, перші три рядки якої відповідають генетико-нейронному етапу настройки нечітких відношень І типу [10]. На другому етапі при розв'язанні задачі оптимізації (3) до вектора параметрів додаються вектори нижніх та верхніх границь координат максимуму функцій належності $\underline{G}_{\tilde{D}}$, $\overline{G}_{\tilde{D}}$, $\underline{G}_{\tilde{S}}$, $\overline{G}_{\tilde{S}}$ та нижніх і верхніх границь параметрів концентрації $\underline{Q}_R$, $\overline{Q}_R$. Параметри концентрації функцій належності $C_{\tilde{D}}$ та $C_{\tilde{S}}$ залишаються без змін. У випадку наявності вхідних даних з відомим середнім відхиленням до вектора змінних, що настроюються, додаються вектори параметрів концентрації функцій належності, що моделюють неточність вхідних даних C_X.

Таблиця 1

Етапи настройки нечітких відношень інтервального типу

Модель		Параметри настройки			Кількість параметрів настройки	Метод
		Вхідні змінні	Вихідні змінні	Нечіткі відношення		
Точні ФН	Точні вхідні дані	G_D	G_S	Q_R	$n + m$	Генетичний алгоритм
		$G_D,\ C_D$	$G_S,\ C_S$	Q_R	$2n + 3m$	Нейронна мережа
	Неточні вхідні дані	$G_D,\ C_D,\ C_X$	$G_S,\ C_S$	Q_R	$3n + 3m$	
ФН інтервального типу	Точні вхідні дані	$\underline{G}_{\tilde{D}}, \overline{G}_{\tilde{D}}, C_{\tilde{D}}$	$\underline{G}_{\tilde{S}},\ \overline{G}_{\tilde{S}}, C_{\tilde{S}}$	$\underline{Q}_R,\ \overline{Q}_R$	$4n + 4m$	
	Неточні вхідні дані	$\underline{G}_{\tilde{D}}, \overline{G}_{\tilde{D}}, C_{\tilde{D}}, C_X$	$\underline{G}_{\tilde{S}},\ \overline{G}_{\tilde{S}}, C_{\tilde{S}}$	$\underline{Q}_R,\ \overline{Q}_R$	$5n + 4m$	

На рис. 1 представлена структура інтервальної нейро-нечіткої мережі, а зміст вузлів показаний в табл. 2.

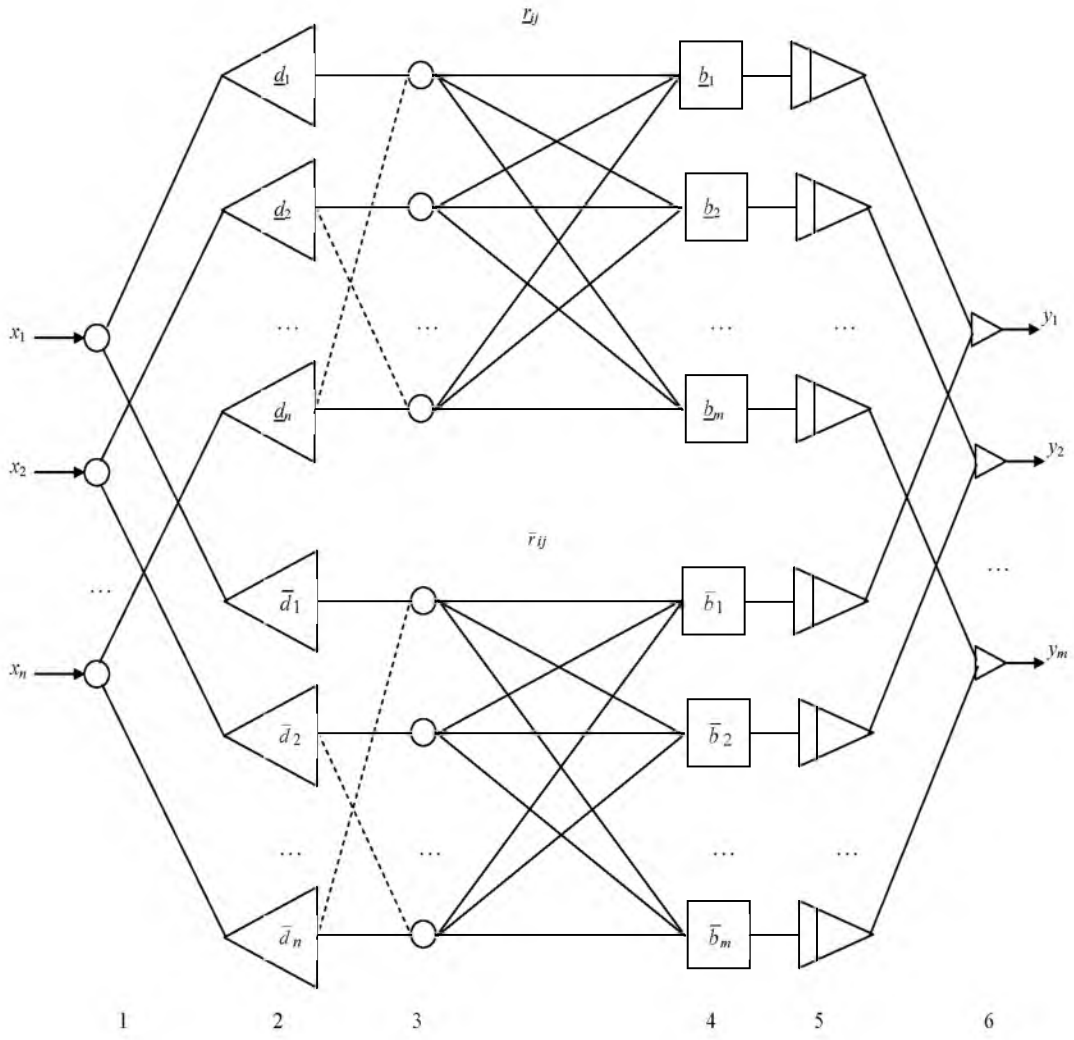


Рис. 1. Структура інтервальної нейро-нечіткої мережі

З рисунка видно, що інтервальна нейро-нечітка мережа складається з нижнього і верхнього фрагментів, що використовують нижні і верхні функції належності вхідних змінних та нижні і верхні границі нечітких відношень відповідно. Нейро-нечітка модель на рис. 1 отримана шляхом імплантації матриць нечітких відношень в нейронну мережу таким чином, що вагами дуг, які підлягають настроюванню, є нижні і верхні границі нечітких відношень. Представлена нейро-нечітка мережа має шість шарів: шар 1 – входи об'єкта; шар 2 (3) – нечіткі терми загроз $\mu^{\tilde{d}_i}$, $i=\overline{1,n}$, або їх комбінація; шар 4 – нечіткі терми збитків $\mu^{\tilde{s}_j}$, $j=\overline{1,m}$; шар 5 – операція пониження типу, тобто перехід від нечіткої множини II типу до нечіткої множини I типу; шар 6 – операція дефазифікації, тобто перетворення результатів нечіткого логічного виведення в чітке число.

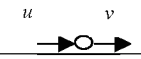
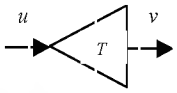
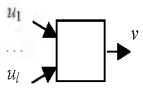
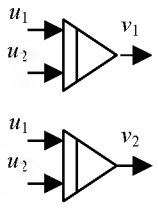
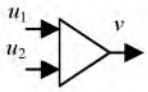
Число вузлів в шарах 2, 3, 4, 5 нейро-нечіткої мережі подвоюється, оскільки інтервальна нейро-нечітка мережа складається з двох частин, що відповідають верхній і нижній мережам I типу і визначають верхню та нижню границі ступеня належності вихідної нечіткої множини.

Дуги графа на рис. 1 зважені таким чином: нижніми і верхніми функціями належності входів до нечітких термів загроз – дуги між 2-м і 3-м шарами; нижнім і верхнім границями нечітких відношень – дуги між 3-м і 4-м шарами; нижніми і верхніми функціями належності виходів до нечітких термів збитків – дуги між 4-м і 5-м шарами. Ваги дуг між іншими шарами дорівнюють одиниці.

Суть настройки нейро-нечіткої мережі інтервального типу полягає в підборі таких ваг дуг (параметрів нижніх і верхніх функцій належності вхідних (вихідних) змінних, параметрів концентрації нижніх і верхніх нечітких множин збитків), які мінімізують різницю між теоретичними і експериментальними виходами об'єкта.

Таблиця 2

Елементи інтервальної нейро-нечіткої мережі

Вузол	Назва	Функція	
	Вхід	$v = u$	
	Нечіткий терм загрози	$v = \mu^T(u)$ $v = \sup[\min(\mu^*(u), \mu^T(u))]$	
	Нечіткий терм збитку	$v = \mu^{s_j} \max\limits_{i=\overline{1,n}}(u_i)$	
	Пониження типу	для лівої границі	для правої границі
		$v_1 = \dfrac{\sum\limits_{k=1}^{N} y_j^k h_k^l}{\sum\limits_{k=1}^{L(X)} u_1 + \sum\limits_{k=L(X)+1}^{N} u_2}$ $h_k^l = \begin{cases} u_2, & \text{ÿêùî } k \le L(X) \\ u_1, & \text{ÿêùî } k > L(X) \end{cases}$	$v_2 = \dfrac{\sum\limits_{k=1}^{N} y_j^k h_k^r}{\sum\limits_{k=1}^{R(X)} u_1 + \sum\limits_{k=R(X)+1}^{N} u_2}$ $h_k^r = \begin{cases} u_2, & \text{ÿêùî } k \le R(X) \\ u_1, & \text{ÿêùî } k > R(X) \end{cases}$
	Дефазифі-кація	$v = \dfrac{u_1 + u_2}{2}$	

Розглянемо задачу оптимізації (3). В цьому випадку для настройки параметрів моделі F використовується система рекурентних співвідношень:

$$\underline{q}_j(t+1) = \underline{q}_j(t) - \eta_q \frac{\partial E_t}{\partial \underline{q}_j(t)}; \qquad \overline{q}_j(t+1) = \overline{q}_j(t) - \eta_q \frac{\partial E_t}{\partial \overline{q}_j(t)};$$

$$\underline{g}^{\tilde{d}_i}(t+1) = \underline{g}^{\tilde{d}_i}(t) - \eta_g \frac{\partial E_t}{\partial \underline{g}^{\tilde{d}_i}(t)}; \qquad \overline{g}^{\tilde{d}_i}(t+1) = \overline{g}^{\tilde{d}_i}(t) - \eta_g \frac{\partial E_t}{\partial \overline{g}^{\tilde{d}_i}(t)};$$

$$c^{\tilde{d}_i}(t+1) = c^{\tilde{d}_i}(t) - \eta_c \frac{\partial E_t}{\partial c^{\tilde{d}_i}(t)};$$

$$\underline{g}^{s_j}(t+1) = \underline{g}^{s_j}(t) - \eta_g \frac{\partial E_t}{\partial \underline{g}^{s_j}(t)}; \qquad \overline{g}^{s_j}(t+1) = \overline{g}^{s_j}(t) - \eta_g \frac{\partial E_t}{\partial \overline{g}^{s_j}(t)};$$

$$c^{s_j}(t+1) = c^{s_j}(t) - \eta_c \frac{\partial E_t}{\partial c^{s_j}(t)}, \tag{4}$$

які мінімізують критерій

$$E_t = \frac{1}{2}\left(f_j(t) - \hat{y}_j(t)\right)^2,$$

де $f_j(t)$, $\hat{y}_j(t)$ – теоретичний і експериментальний виходи об'єкта оцінки на t-ому кроці настройки;

$\underline{q}_j(t)$, $\overline{q}_j(t)$ – нижнє і верхнє значення параметра концентрації функції належності збитку на t-ому кроці настройки;

$\underline{g}^{\tilde{d}_i}(t)$, $\overline{g}^{\tilde{d}_i}(t)$, $c^{\tilde{d}_i}(t)$ – параметри функцій належності вхідних змінних до нечітких термів загроз на t-ому кроці настройки;

$\underline{g}^{\tilde{s}_j}(t)$, $\overline{g}^{\tilde{s}_j}(t)$, $c^{\tilde{s}_j}(t)$ – параметри функцій належності вихідних змінних до нечітких термів збитків на t-ому кроці настройки;

η_g, η_c, η_w – параметри настройки.

Якщо враховувати неточність вхідних даних, то до системи рекурентних співвідношень (4) слід додати співвідношення: $c_i^*(t+1) = c_i^*(t) - \eta_c \frac{\partial E_t}{\partial c_i^*(t)}$, де $c_i^*(t)$ – параметр концентрації функцій належності вхідних змінних на t-ому кроці настройки.

Аналогічно правилу „back-propagation", алгоритм навчання нейро-нечіткої мережі інтервального типу складається з двох фаз. На першій фазі обчислюються модельні значення виходів об'єкта оцінки (f_1, f_2, …, f_m), що відповідають заданій архітектурі мережі. На другій фазі обчислюється значення нев'язки (E_t) і перераховуються ваги міжнейронних зв'язків (4).

Висновки. Таким чином, для настройки нечітких відношень інтервального типу пропонується використовувати послідовний метод, який передбачає спочатку визначення множини параметрів нечітких відношень I типу за допомогою генетико-нейронного алгоритму, а потім на їх базі настройку тільки додаткових параметрів, що дозволяє зменшити середній час настройки нечіткої моделі та оцінити вплив невизначеності на точність оцінки. Результати експериментів доводять, що використання інтервальних нечітких відношень і функцій належності II типу дозволяють мінімізувати наслідки невизначеності через неточні навчальні вибірки.

Напрямом подальших досліджень є удосконалення послідовного методу настройки нечіткої моделі за рахунок вибору іншої системи нечітких термів, що описують загрози і збитки, що можливо дозволить зменшити середній час настройки та оцінити вплив невизначеності на точність оцінки.

ЛІТЕРАТУРА

1. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. Винница: УНІВЕРСУМ-Вінниця, 1999. 320 с.

2. Минаев Ю. Н., Филимонова О. Ю. Методы и алгоритмы решения задач идентификации и прогнозирования в условиях неопределенности в нейросетевом логическом базисе. Москва: Горячая линия – Телеком, 2003.

3. Заде Л. Понятие лингвистической переменной и её применение к принятию приближенных решений. Москва: Мир, 1976. 167 с.

4. Mendel J. Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Direction. Prentice Hall PTR, USA. 2001. 520 p.

5. Mordeson J. N. Fuzzy Mathematics in Medicine. 2009. 257 p.

6. Exact analytical inversion of interval type-2 TSK fuzzy logic systems with closed form inference methods // Applied Soft Computing, 37. 2015. P. 60–70.

7. Герасимов Б. М., Самойлов І. В. Алгоритм побудови матриці нечітких відношень для системи діагностування комп'ютерних мереж // Сучасні інформаційні технології у сфері безпеки та оборони: науково-практичний журнал Національної Академії оборони України. 2008. № 1. С. 8–11.

8. Ротштейн А. П., Митюшкин Ю. И. Нейро-лингвистическая идентификация нелинейных зависимостей // Кибернетика и системный анализ. 2000. № 2. С. 37–44.

9. Rotshtein, A. Rakytyanska, H. Fuzzy Evidence in Identification, Forecasting and Diagnosis, Springer, Berlin: Heidelberg, 2012. 314 p.

10. Ротштейн А. П., Ракитянская А. Б. Идентификация нелинейных зависимостей нечеткими базами знаний с генетико-нейронной настройкой // Известия РАН. Теория и системы управления. 2005. № 1. С. 110–117.