DOI 10.34185/1562-9945-5-161-2025-01
УДК 004.056:004.94

О.В. Герасіна

НЕЙРО-НЕЧІТКЕ ПРОГНОЗУВАННЯ САМОПОДІБНОГО ТРАФІКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

Анотація. Запропоновано для прогнозування самоподібного трафіку інформаційно-комунікаційних мереж використовувати адаптивні фільтри-апроксиматори у вигляді адаптивних систем нечіткого висновку на основі алгоритмів Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя. Шляхом моделювання на основі експериментальних даних показана ефективність розв'язання задачі прогнозування мережевого трафіка із використанням глобальних методів оптимізації та нейро-нечітких фільтрів. Підтверджена адекватність отриманих результатів.
Ключові слова: виявлення атак, інформаційно-комунікаційна мережа, прогнозування, самоподібний трафік, адаптивна мережа нечіткого висновку, глобальна оптимізація.

Постановка проблеми. Стрімкий розвиток інформаційних технологій та інформаційно-комунікаційних систем і мереж (ІКМ) викликає ряд безпрецедентних загроз зі сторони окремих осіб, організацій або країн, які прагнуть дестабілізувати суспільне життя, втручаючись в роботу критично важливих об'єктів інфраструктури. Тому актуальним рішенням зазначеної проблеми є використання засобів моніторингу, здатних аналізувати трафік мережі в режимі реального часу. До таких засобів відносяться системи виявлення та запобігання атак (СВА) [1-4].

Аналіз останніх досліджень і публікацій. Основним завданням СВА є оперативне виявлення вторгнень та запровадження ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів [1-4].

Сучасні СВА прийнято розділяти на два типи: спрямовані на пошук зловживань та на виявлення аномалій у системі. Виявлення зловживань ґрунтується на формуванні шаблонів вторгнень, що не є ефективним при детектуванні невідомих атак. Для реєстрації невідомих атак в ІКМ використовують системи виявлення аномалій, в яких певні дії, що є відмінними від поведінки в нормальному стані, ідентифікуються як аномальні. При виявленні мережевих аномалій даними для аналізу є мережевий трафік. Створений набір ознак (характеристики трафіку) порівнюється з набором ознак нормальної діяльності системи або конкретних користувачів, і якщо спостерігається суттєва розбіжність, фіксується мережева аномалія. При цьому, набір ознак нормальної діяльності системи або конкретних користувачів, СВА на основі аномалій повинні накопичити перед поча-

тком використання, і постійно оновлювати його із урахуванням поточного спостережуваного профілю мережевої активності [5-8].

Трафік в ІКМ є нелінійним стохастичним процесом з властивостями самоподоби та з хаотичною і фрактальною динамікою. Крім того, встановлено, що агрегований трафік від різних джерел на малих часових масштабах проявляє мультифрактальний характер [9, 10].

Оцінка характеристик мережевого трафіку необхідна для побудови його адекватної моделі, що дозволяє сформувати еталонну модель (шаблон) «нормального» трафіку і за нею виявляти аномалії трафіку в СВА. При цьому прогнозування мережевого трафіку, яке дозволяє підвищити оперативність виявлення атак, доцільно проводити із використанням адаптивних фільтрів-апроксиматорів (АФА), побудованих на основі систем штучного інтелекту (нейронних мереж (НМ), систем з нечіткою логікою) [9].

Для усунення недоліків НМ і систем з нечіткою логікою запропоновані гібридні мережі, в яких висновки робляться на основі апарату нечіткої логіки, а відповідні функції належності підлаштовуються із використанням алгоритмів навчання НМ. Такі системи не тільки використовують апріорну інформацію, але й можуть набувати нових знань, а для користувача є логічно прозорими [3, 9, 11-15].

У роботі [11] запропоновано методику прогнозування трафіку в ІКМ, яка дозволяє підвищити ймовірність визначення вторгнень для СВА за рахунок зниження похибок інтелектуальних прогнозуючих моделей самоподібного трафіка. При цьому, у роботі [11] досліджується один тип АФА на основі гібридної мережі для прогнозування мережевого трафіку. У роботах [3, 9, 12-14] наведено використання гібридних мереж для вирішення різних завдань, але відсутні роботи, де виконується дослідження використання різних типів гібридних мереж із налаштуванням їх параметрів оптимізаційними методами.

Таким чином, невирішеною задачею є обґрунтування типу нейро-нечіткого АФА для прогнозування самоподібного трафіку ІКМ для виявлення його аномалій в реальному масштабі часу при використанні в СВА.

Мета роботи – дослідження гібридних нейро-нечітких мереж для прогнозування самоподібного трафіку ІКМ, із налаштуванням їх параметрів за допомогою методів глобальної оптимізації, які б дозволяли їх використання в СВА для виявлення мережевих аномалій.

Викладення основного матеріалу дослідження. Прогнозування на основі гібридних нейро-нечітких мереж. Гібридна нейро-нечітка мережа – це мережа з чіткими сигналами, вагами і активаційною функцією, але з об'єднанням сигналів і ваг з використанням *t*-норми, *t*-конорми або деяких інших безперервних операцій. Входи, виходи і ваги гібридної мережі – речові числа, що належать відрізку [0,1] [9].

До гібридних мереж належить Anfis (Adaptive Neuro Fuzzy Inference System) – адаптивна мережа нечіткого висновку. Такі мережі дозволяють вхідним сигналам за допомогою нечітких перетворень (алгоритмів Сугено-Такагі, Такагі-Сугено-Канга, Ванга-Менделя) та апроксимації зіставити вихідний сигнал.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Алгоритм Сугено-Такагі використовує наступну модель нечіткого правила [3, 9]:

R_r: ЯКЩО x_1 це A_{1r}, … І x_n це A_{nr}, ТО $y=f(X)$,

де $x_1, x_2, \ldots, x_n$ – входи мережі; y – вихід мережі; $f(X)$ – деяка чітка функція (наприклад, поліном першого порядку); A_{ir} – нечіткий терм з функцією належності $\mu_r(x_i)$, що застосовується для лінгвістичної оцінки змінної x_i у правилі r ($r=\overline{1,m}$, $i=\overline{1,n}$).

Мережа Anfis на основі алгоритму Сугено-Такаги є п'ятишаровою штучною НМ прямого розповсюдження сигналу. Призначення шарів наступне: перший шар – терми вхідних змінних; другий – антецеденти (посилки) нечітких правил; третій – нормалізація ступенів виконання правил; четвертий шар – укладення правил; п'ятий – агрегування результату, отриманого за різними правилами.

Входи мережі в окремий шар не виділяються. Структуру мережі Anfis на основі алгоритму Сугено-Такаги представлено на рис. 1.

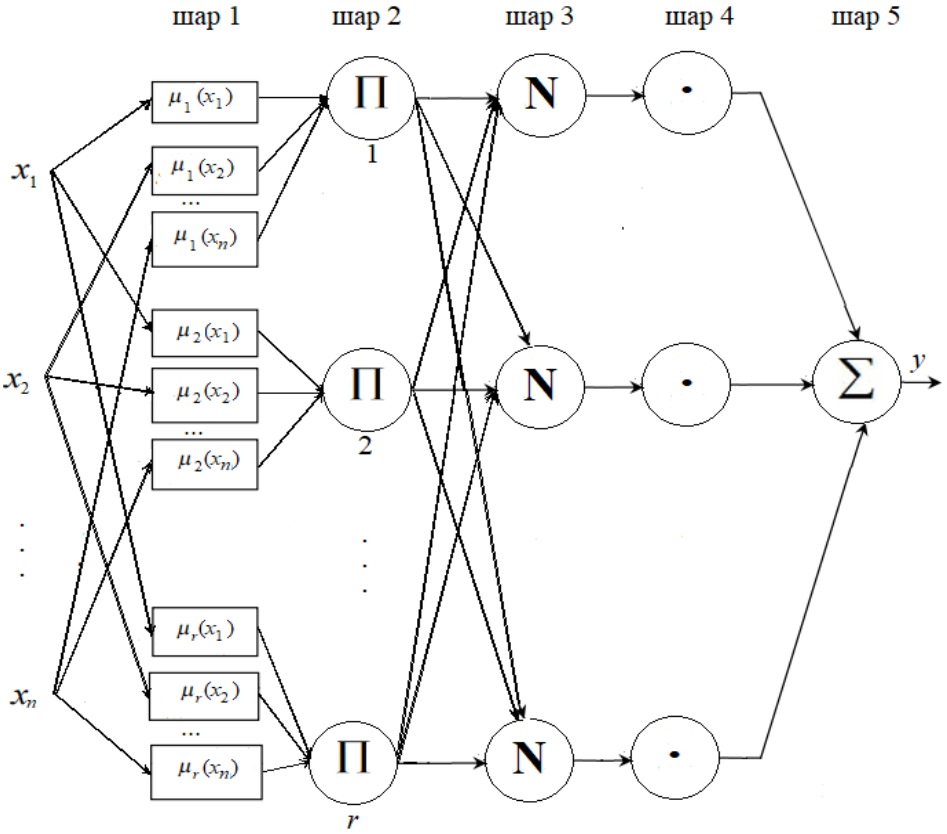


Рисунок 1 - Структура адаптивної мережі нечіткого висновку на основі алгоритму Сугено-Такагі

Шар 1. Кожен вузол першого шару представляє один терм з функцією належності. Входи мережі $x_1, x_2, \ldots, x_n$ з'єднані тільки зі своїми термами. Кількість вузлів цього шару дорівнює сумі потужностей терм-множин вхідних змінних. Виходом вузла є ступінь належності значення вхідної змінної відповідного нечіткого терму:

$$\mu_r(x_i)=\frac{1}{1+\left|\frac{x_i-c}{a}\right|^{2b}} \qquad (1)$$

де *a, b* і *c* – параметри функції належності, які налаштовуються.

Шар 2. Кількість вузлів цього шару дорівнює *m*. Кожен вузол шару відповідає одному нечіткому правилу. Вузол другого шару з'єднаний з тими вузлами першого шару, які формують антецеденти відповідного правила. Отже, кожен вузол цього шару може приймати від 1 до *n* вхідних сигналів. Виходом вузла τ_r ($r = \overline{1,m}$) є ступінь виконання правила, яка розраховується як добуток вхідних сигналів.

Шар 3. Кількість вузлів цього шару також дорівнює *m*. Кожен вузол розраховує відносну ступінь виконання нечіткого правила:

$$\tau_r^* = \frac{\tau_r}{\sum\limits_{j=1,m} \tau_j}. \qquad (2)$$

Шар 4. Кількість вузлів цього шару також дорівнює *m*. Кожен вузол з'єднаний з одним вузлом третього шару, а також із усіма входами мережі (на рис. 1 зв'язки зі входами не показані). Вузол четвертого шару розраховує внесок одного нечіткого правила у вихід мережі:

$$y_r = \tau_r^* (b_{0,r} + b_{1,r} x_1 + ... + b_{n,r} x_n), \qquad (3)$$

де $b_{q,r}$ – коефіцієнти у висновку *r*-правила ($r = \overline{1,m}$, $q = \overline{0,n}$).

Шар 5. Єдиний вузол цього шару підсумовує вклади усіх правил:

$$y = y_1 + \ldots + y_r + \ldots + y_m. \qquad (4)$$

Типові процедури навчання НМ можуть бути застосовані для налаштування мережі Anfis на основі алгоритму Сугено-Такагі, оскільки в ній використовуються тільки функції, які диференціюються. Зазвичай застосовується комбінація градієнтного спуску у вигляді алгоритму зворотного поширення похибки і методу найменших квадратів. Алгоритм зворотного поширення похибки налаштовує параметри антецедентів правил, тобто функцій належності. Метод найменших квадратів оцінює коефіцієнти висновків правил, оскільки вони лінійно пов'язані із виходом мережі.

Кожна ітерація процедури налаштування виконується у два етапи. На першому етапі на входи подається навчальна вибірка й по розбіжності між бажаною і дійсною поведінкою мережі ітераційним методом найменших квадратів знаходяться оптимальні параметри вузлів шару 4. На другому етапі залишкова розбіжність передається з виходу мережі на входи і методом зворотного поширення похибки модифікуються параметри вузлів шару 1. При цьому знайдені на першому етапі коефіцієнти висновків правил не змінюються. Ітераційна процедура налаштування триває доки розбіжність перевищує заздалегідь встановлене значення. Для налаштування функцій належності поряд з методом зворотного поширення похибки можуть використовуватись й інші алгоритми оптимізації (метод Левенберга-Марквардта та інші).

Алгоритм Такагі-Сугено-Канга використовує наступну модель нечіткого правила [12, 13]:

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

$П_i$: ЯКЩО x_1 це A_{i1}, І … І x_j це A_{ij} І … І x_m це A_{im} ТО $y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j$,

де i=1,…m; j=1,…n; A_{ij} – значення лінгвістичної змінної x_j для правила $П_i$ з функцією належності Гауса:

$$\mu_{A_{ij}}(x_j) = \exp\left(-0{,}5\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right), \tag{5}$$

де x_j – входи мережі; a_{ij}, b_{ij} – параметри функції належності, що налаштовуються.

Функціональна залежність для отримання вихідної змінної величини після дефазифікації, що здійснюється методом центроїду, має вигляд:

$$y' = \frac{\sum_{i}^{n}\left(\left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j\right)\prod_{j}^{m} \mu_{A_{ij}}\left(x'_j\right)\right)}{\sum_{i=1}^{n}\prod_{j}^{m} \mu_{A_{ij}}\left(x'_j\right)} = \frac{\sum_{i}^{n}\left(\left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j\right)\right)\prod_{j=1}^{m} \exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}}\right)^2\right]}{\sum_{i=1}^{n}\prod_{j}^{m} \exp\left[-\left(\frac{x'_j - a_{ij}}{b_{ij}}\right)^2\right]} \tag{6}$$

Вираз (6) лежить в основі мережі Anfis із застосуванням алгоритму Такагі-Сугено-Канга, яка включає п'ять шарів (рис. 2).

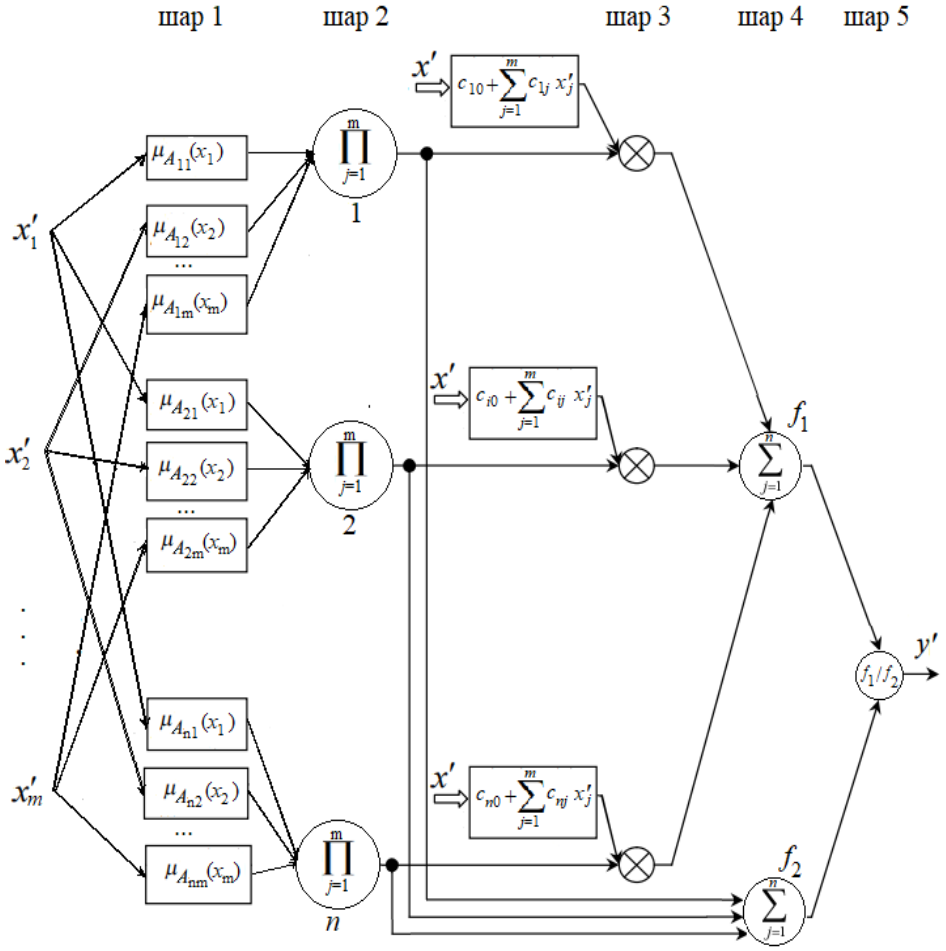


Рисунок 2 - Структура адаптивної мережі нечіткого висновку на основі алгоритму Такагі-Сугено-Канга

Шар 1. Складається з елементів, які виконують фазифікацію вхідних чітких змінних x'_j (j=1,…,n). Елементи цього шару обчислюють значення ступенів належності гаусівських функцій належності $\mu_{A_{ij}}\left[x'_j\right]$, з параметрами a_{ij} і b_{ij}, які підлягають адаптації в процесі навчання мережі.

Шар 2. Число елементів цього шару дорівнює кількості правил в базі. Виконує нечітку імплікацію (нечіткий добуток) ступенів належності відповідних правил.

Шар 3. У цьому шарі розраховується значення функцій вихідного сигналу $\left(c_{j0}+\sum_{j=1}^{m} c_{ij}x'_j\right)$, які множаться на вагові коефіцієнти, що отримані попереднім шаром. При чому параметри c_{i0} та c_{ij} , які визначають функції висновків правил, підлягають адаптації в процесі навчання мережі.

Шар 4. Містить два елементи-суматори. Перший елемент агрегує висновки правил попереднього шару, другий – проводить допоміжні обчислення для подальшої дефазифікації.

Шар 5. Складається з єдиного нормалізуючого елемента, який виконує дефазифікацію результату.

В мережі Anfis на основі алгоритму Такагі-Сугено-Канга процес навчання відбувається в два етапи. Спочатку шляхом розв'язання системи лінійних рівнянь розраховуються параметри c_{i0} та c_{ij} лінійних функцій із висновків правил за умови фіксованих значень параметрів a_{ij} та b_{ij}. На другому етапі визначені параметри c_{ij} фіксуються та розраховуються фактичні вихідні сигнали мережі для всіх прикладів, після чого уточнюються нелінійні параметри a_{ij} і b_{ij} гаусівських функцій належності фазифікатора (наприклад, за алгоритмом Уідроу-Хоффа). Далі процес адаптації параметрів запускається знову доти, доки настане повторюваність результатів. Цей алгоритм називають гібридним, його особливість полягає у розподілі етапів процесу навчання. Також дана мережа може бути навчена із використанням алгоритму зворотного поширення похибки.

Мережу Anfis на основі алгоритму Ванга-Менделя можна розглядати як окремий випадок попередньої мережі. У мережі Такагі-Сугено-Канга результатом є поліном $c_{i0}+\sum_{j=1}^{m} c_{ij}x_j$, тоді як у мережі Ванга-Менделя вихідна змінна є константною c_i, яку можна розглядати як поліном нульового порядку.

Мережа Anfis із застосуванням алгоритму Ванга-Менделя заснована на нечітких правилах [14, 15]:

D_i: ЯКЩО x_1 це A_{i1}, І … І x_j це A_{ij}, І … І x_m це A_{im} ТО y=$B_{i/}$,

де i=1,…m; j=1,…n.

Нечіткий висновок для даної моделі має наступний вигляд:

$$\mu_{B'_i}(y)=\mu_{B_i}[y]\prod_{j=1}^{m}\mu_{A_{ij}}\left(x'_j\right) \qquad (7)$$

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Оскільки акумулювання активізованих висновків правил не проводиться, методом дефазифікації є метод середнього центру, а функції належності всіх нечітких множин є функціями Гауса, то вихідна змінна визначається наступним чином:

$$y' = \frac{\sum_{i=1}^{n}\left(\arg\max_{y}\left(\exp\left[-\frac{y-c_i}{d_i}\right]\right)\right)\prod_{j=1}^{m}\exp\left[-\frac{x'_j-a_{ij}}{b_{ij}}\right]}{\sum_{i=1}^{n}\prod_{j=1}^{m}\exp\left[-\frac{x'_j-a_{ij}}{b_{ij}}\right]} = \frac{\sum_{i=1}^{n}c_i\prod_{j=1}^{m}\exp\left[-\frac{x'_j-a_{ij}}{b_{ij}}\right]}{\sum_{i=1}^{n}\prod_{j=1}^{m}\exp\left[-\frac{x'_j-a_{ij}}{b_{ij}}\right]}, \quad (8)$$

де c_i, d_i – відповідно, центри та ширина гаусівських функцій, що представляють функції належності нечітких множин B_i висновків правил; a_{ij}, b_{ij} – відповідно центри і ширина гаусівських функцій, що є функціями належності нечітких множин A_{ij} предпосилок правил.

На рис. 3 представлена структура мережі Anfis на основі алгоритму Ванга-Менделя, елементи шарів якої реалізують відповідні компоненти виразу (8).

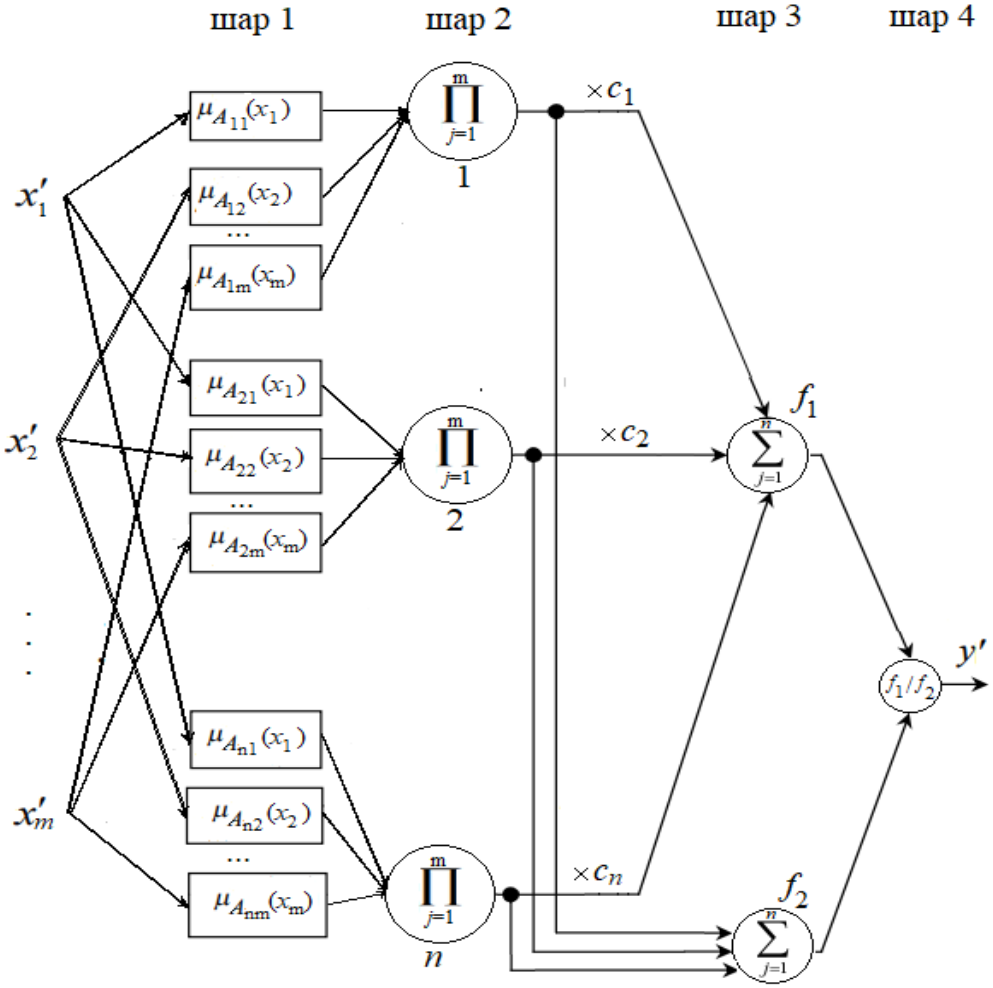


Рисунок 3 - Структура адаптивної мережі нечіткого висновку на основі алгоритму Ванга-Менделя

Шар 1. Складається з елементів, які виконують фазифікацію вхідних чітких змінних x'_j (j=1,…,n) та обчислюють значення гаусівських функцій належності $\mu_{A_j}\left[x'_j\right]$.

Шар 2. Число елементів цього шару дорівнює кількості правил в базі. Здійснює агрегування ступенів належності передумов відповідних правил.

Шар 3. Перший елемент цього шару служить для активізації висновків правил (c_i) відповідно до значень агрегованих у попередньому шарі ступенів належності передумов правил. Другий елемент проводить допоміжні обчислення для подальшої дефазифікації.

Шар 4. Складається з одного елемента, який виконує дефазифікацію результату.

Алгоритм навчання мережі Anfis на основі алгоритму Ванга-Менделя відбувається в два етапи. На першому етапі при фіксованих значеннях параметрів першого шару (a_{ij} і b_{ij}) налаштовуються лінійні параметри елементів третього шару c_i. Ця процедура ітераційно повторюється і вважається завершеною якщо значення функції похибки за кожним прикладом навчальної вибірки не перебільшує деякого встановленого порога, або оцінка середньої сумарної похибки нечіткої продукційної моделі із урахуванням всіх прикладів навчальної вибірки не перебільшує деякого порога, або похибка застабілізувалась на певному значенні. На другому етапі налаштовуються параметри нелінійної функції належності в елементах першого шару a_{ij} та b_{ij}. Це також ітераційна процедура, умови завершення якої аналогічні умовам завершення першого етапу. У разі невиконання першої чи другої умов завершення процес ітераційно повторюється, починаючи з коригування c_i доки мережа не буде коректно навчена. Також замість вищенаведеного адаптивного алгоритму, мережа Ванга-Менделя може бути навчена за допомогою алгоритму найскорішого спуску з моментами.

Оскільки задача обґрунтування типу нейро-нечіткого АФА із налаштуванням його параметрів є полімодальною, то це вимагає використання методів глобальної оптимізації, серед яких найбільш ефективними є пошукові методи. У них алгоритм пошуку оптимального рішення пов'язує наступні один за одним рішення $\Psi_s(j+1) = F[\Psi_s(j)]$, де F – алгоритм пошуку, який показує які операції слід зробити на кроці j при рішенні $\Psi_s(j)$, щоб отримати нове рішення $\Psi_s(j+1) \succ \Psi_s(j)$. Тут знак переваги $\succ$ при мінімізації функціоналу має сенс:

$$C[\Psi_s(j+1)] < C[\Psi_s(j)]. \qquad (9)$$

В алгоритмах прямого випадкового пошуку (ПВП) задаються напрямки пошуку і визначаються значення функціоналу C в точках $\Psi_s(j) \pm \gamma\varsigma$. Рішення полягає у виборі кроку в напрямку зменшення цього функціоналу:

$$\Psi_s(j+1) = \Psi_s(j) - \omega\varsigma\{C[\Psi_s(j) + \gamma\varsigma] - C[\Psi_s(j) - \gamma\varsigma]\}, \qquad (10)$$

де $\omega, \varsigma, \gamma$ – параметри, що визначають сфери прийняття рішення (ω), збору інформації (γ) та одиничний випадковий напрям (ς). У загальному випадку параметри в (10) можуть змінюватися (адаптуватися) до процедури пошуку і виду гіперповерхні прийнятого функціоналу.

Розвитком методу ПВП є метод імітації відпалу (МІВ), який відображає поведінку розплавленого матеріалу при затвердінні із застосуванням процедури керованого охолодження (відпалу). У процесі відпалу кристалізація розплаву супроводжується глоба-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

льним зменшенням його енергії, однак допускається її зростання на деякий час. Завдяки цьому можливий вихід з пасток локальних мінімумів енергії, що виникають при реалізації процесу. В алгоритмах МІВ задаються напрямки пошуку і визначаються значення функціоналу C в точках $\Psi_s(j) \pm \upsilon\tau$. Рішення полягає у виборі кроку в напрямку зменшення цього функціоналу:

$$\Psi_s(j+1) = \Psi_s(j) - \omega\upsilon\{C[\Psi_s(j) + \upsilon\tau] - C[\Psi_s(j) - \upsilon\tau]\}, \quad (11)$$

де ω, υ, τ – параметри, що визначають сфери прийняття рішення (ω), зміну поточного рішення (υ) і зменшення температури (τ).

Багатокритеріальна оптимізація (БО) заснована на знаходженні рішення, одночасно оптимізуючого більш ніж одну функцію. У цьому випадку шукається певний компроміс, в ролі якого виступає рішення, оптимальне в сенсі Парето. При БО, що використовує генетичні алгоритми (ГА) вибирається не одна хромосома, що представляє собою оптимальне рішення в звичайному сенсі, а безліч хромосом, оптимальних в сенсі Парето. Користувач має можливість вибрати оптимальне рішення з цієї безлічі:

$$k \cdot \Psi_s(j+1) = k \cdot (\Psi_s(j) + \delta\Psi_s(j)), \quad (12)$$

де $k \geq 2$ – число розглянутих критеріїв.

Моделювання процесу прогнозування мережевого трафіку було проведено в середовищі Matlab / Simulink за допомогою стандартних та розроблених програм.

Як експериментальні дані було взято трафік, що передається через мережу Інтернет [17]. Дані являють собою залежність розміру Ethernet кадрів в байтах від часу. Для їх нормування по часової осі була проведена процедура агрегації з кроком 5 с.

Глибина прогнозу була прийнята у 4 такти, а глибина пам'яті за різними входами від 1 до 4.

Як глобальні методи оптимізації застосовувались БО, ПВП і МІВ. Метод БО використовував ГА для знаходження безлічі оптимальних за Парето рішень. ПВП мав адаптивний крок пошуку та повний пошук навколо поточної ітерації, МІВ – обмежену область перевідпалу. Кількість ітерацій для ПВП і МІВ (для БО поколінь) обмежувалося на рівні 100, а розмір простору пошуку для ПВП (для БО розмір популяції, для МІВ розмір області перевідпалу) – 30.

Як критерій глобальної оптимізації використовувався критерій незміщенності (мінімуму зсуву), який не чутливий до рівня шуму у вхідних даних і при збільшенні завад їх мінімум не зміщується в область простіших моделей [16]:

$$C_{зм} = \frac{\left\| \hat{Y}_A[m+n] - \hat{Y}_B[m+n] \right\|}{\left\| Y^*[m+n] \right\|}, \quad (13)$$

де $\hat{Y}_A[m+n]$ і $\hat{Y}_B[m+n]$ – виходи моделей, які навчені на вибірках *A* і *B*, відповідно.

Як критерій параметричної оптимізації використовувався критерій регулярності, що обчислюється на перевірочній вибірці [16]:

$$C_{рег} = \frac{\left\| Y_B^*[m+n] - \hat{Y}_B[m+n] \right\|}{\left\| Y_B^*[m+n] \right\|}, \quad (14)$$

де *m* – глибина пам'яті, *n* – глибина прогнозу.

Для побудови АФА використовувалась структура Гамерштейна-Вінера [11].

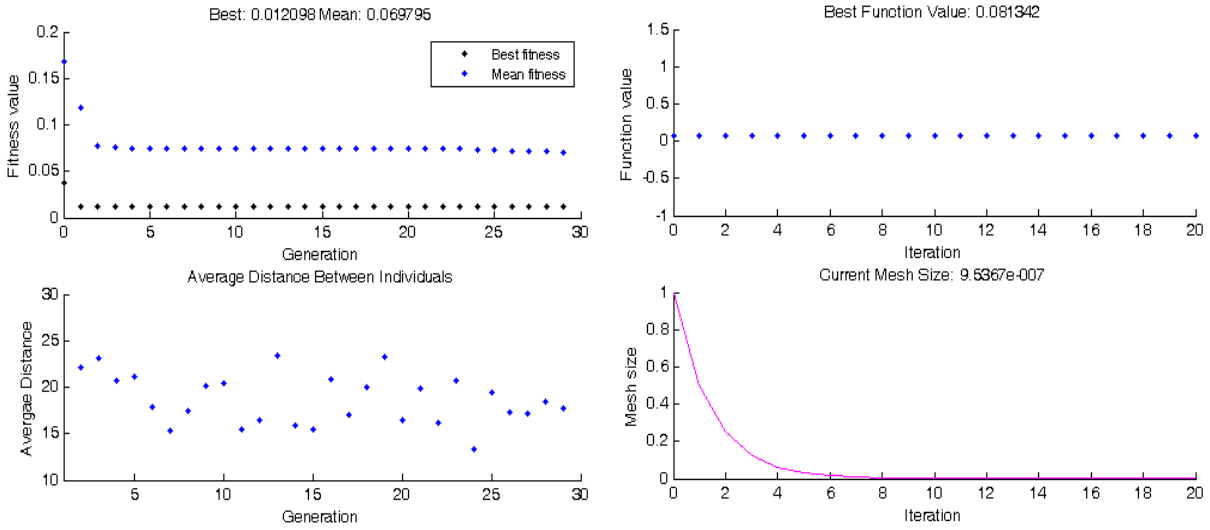
При глобальній оптимізації варіювалися наступні параметри АФА:

- тип АФА (базисної функції) – Anfis на основі алгоритму Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя;

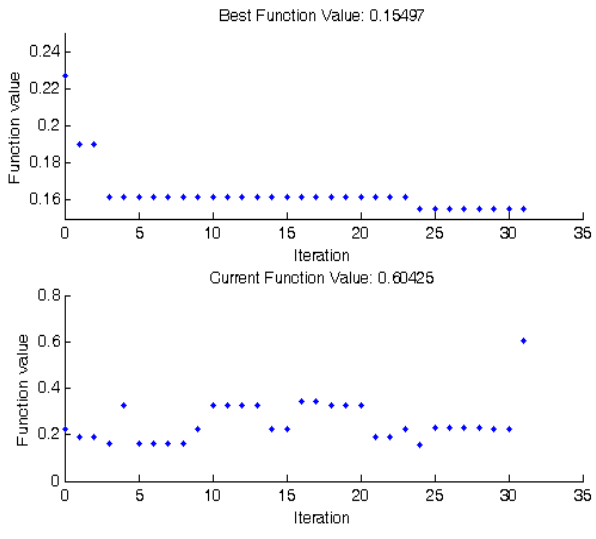
- метод параметричної оптимізації (функція навчання мереж Anfis).

Результати глобальної оптимізації для знаходження оптимальної структури (типу) та параметрів АФА Anfis наведені на рис. 4.

В результаті моделювання (див. рис. 4) встановлено, що ПВП і БО мають найкращу швидкість збіжності (ПВП виходить в область оптимальних рішень на перших ітераціях, БО – на перших поколіннях, МІВ – після 20 ітерацій). Алгоритм МІВ виявив найкращу швидкодію (2,3 с на ітерацію при 8,2 с на ітерацію в ПВП і 20,9 с на покоління в БО). При цьому алгоритм БО виявив найкращу збіжність (значення критерію (13) при його використанні склали 0,0121, на відміну від 0,0813 при ПВП і 0,155 при МІВ).



а б



в

Рисунок 4 - Результати глобальної оптимізації структури та параметрів АФА для прогнозування трафіку за допомогою: а – БО, б – ПВП, в – МІВ

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Результат прогнозування мережевого трафіку наведено на рис. 5.

Встановлено, що мінімуму критерію регулярності відповідають АФА Anfis на основі алгоритму Такагі-Сугено-Канга, яка навчена гібридним алгоритмом. Значення критерію параметричної оптимізації (14) склало 0,0457.

Адекватність отриманих моделей мережевого трафіку експериментальним даним була перевірена і підтверджена за непараметричним критерієм знаків з рівнем значущості 0,01.

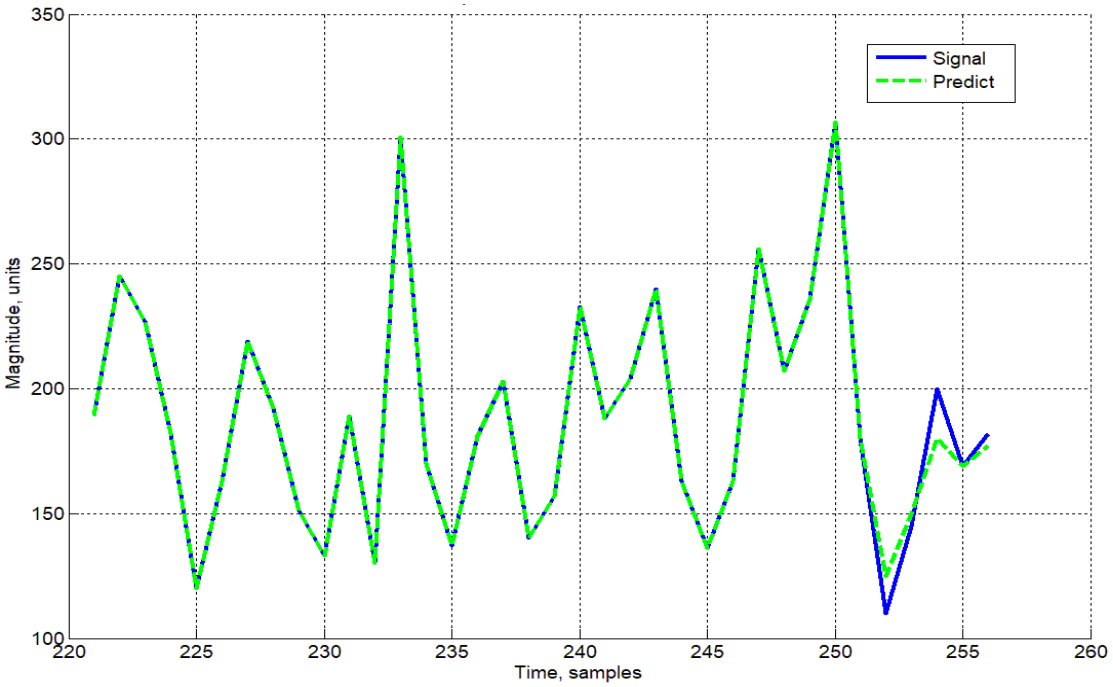


Рисунок 5 - Результат прогнозування мережевого трафіку

Висновки. Запропоновано для прогнозування самоподібного трафіку в інформаційно-комунікаційних мережах використовувати нейро-нечіткі адаптивні фільтри-апроксиматори у вигляді мереж Anfis на основі алгоритмів Сугено-Такагі, Такагі-Сугено-Канга та Ванга-Менделя. Для оптимізації цих фільтрів під реальні процеси виконана ідентифікація їх параметрів за критерієм точності на навчальній і перевірочній послідовностях.

Шляхом моделювання на основі експериментальних даних показана ефективність розв’язання задачі прогнозування мережевого трафіка із використанням глобальних методів оптимізації та інтелектуальних базисних функцій (адаптивних мереж нечіткого висновку). Перевірена та підтверджена адекватність отриманих моделей самоподібного трафіку експериментальним даним.

Подальші дослідження мають бути спрямовані на обґрунтування та дослідження інформативності характеристик і моделей мережевого трафіку та ефективності критеріїв та методів розпізнавання атак.

ЛІТЕРАТУРА

1. Толюпа С. Засоби виявлення кібернетичних атак на інформаційні системи / С. Толюпа, Н. Лукова-Чуйко, Я. Шестак // Інфокомунікаційні технології та електронна інженерія. – 2021. – № 2(2). – С. 19–31.

2. Проблеми захисту критично важливих об’єктів інфраструктури / Н. Лукова-Чуйко, В. Наконечний, С. Толюпа, Р. Зюбіна // Безпека інформаційних систем і технологій. – 2020. – № 1(2). – С. 31-39.

3. Толюпа С. Нейро-нечітка система виявлення вторгнень у інформаційну мережу критичної інфраструктури / С. Толюпа, А. Кулько // Кібербезпека: освіта, наука, техніка. – 2025. – 3(27). – С. 233-247.

4. Носенко К.М. Огляд систем виявлення атак в мережевому трафіку / К.М. Носенко, О.І. Півторак, Т.А. Ліхоузова // Адаптивні системи автоматичного управління. – 2014. – № 1(24). – С. 67-75.

5. Довбешко С.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак / С.В. Довбешко, С.В. Толюпа, Я.В. Шестак // Сучасний захист інформації. – 2019. – №1(37). – С. 6-15.

6. Лазаренко С.В. Особливості функціонування систем виявлення атак на автоматизовані системи / С.В. Лазаренко // Сучасний захист інформації. – 2015. – №1. – С. 33-40.

7. Гулак Г.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережевих аномалій. / Г.М. Гулак, В.В. Семко, П.М. Складанний // Сучасний захист інформації. – 2015. – №4. – С. 81-85.

8. Лукова-Чуйко Н.В. Методи виявлення вторгнень у сучасних системах IDS / Н.В. Лукова-Чуйко, С.В. Толюпа, І.І. Пархоменко // Безпека інформаційних систем і технологій. – 2021. – № 1(5). – С. 19-26.

9. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с.

10. Crovella M.E., Bestravos A. Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes. IEEE Transactions on Networking. 1997. Vol. 5. № 6. P. 835-846.

11. Герасіна О.В. Методика інтелектуальної ідентифікації та прогнозування трафіку в інформаційних телекомунікаційних мережах / О.В. Герасіна // Системи обробки інформації. – 2018. – № 1(152). – С. 94-99.

12. Modelling Intelligent System for the Estimation of Technical State of Construction Structures / S. Terenchuk, A. Pashko, B. Yeremenko, S. Kartavykh, N. Ershova // Eastern-European Journal of Enterprise Technologies. – 2018. – 3(2 (93)). – P.47-53.

13. Кондратенко Н.Р. Основи нейронних мереж. Теорія та практика / Н.Р. Кондратенко, С.М. Куземко. - Вінниця: ВНТУ, 2006. – 104 с.

14. Vladov S. A neuro-fuzzy expert system for the control and diagnostics of helicopters aircraft engines technical state. / S. Vladov, Y. Shmelov, M. Petchenko // ICT in Education, Re-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

search and Industrial Applications. Integration, Harmonization and Knowledge Transfer: Proceedings of the 17th International Conference. – 2021. – P. 40-52.
15. Wang L.X. Generating fuzzy rules by learning from examples / L.X. Wang, J.M. Mendel // IEEE Transactions on systems, man, and cybernetics. – 1992. – Vol. 22 (6). – P. 1414-1427.
16. Ivakhnenko A.G. Inductive learning algorithms for complex systems modeling / A.G. Ivakhnenko, H.R. Madala – London, Tokyo: CRC Press, 1994. – 384 p.
17. Traffic Archive. [Електронний ресурс] – Режим доступу: http://ita.ee.lbl.gov.

REFERENCES

1. Toliupa, S., Lukova-Chuiko, N., & Shestak, Ya. (2021). Zasoby vyiavlennia kibernetychnykh atak na informatsiini systemy [Means of detecting cyber attacks on information systems]. Infokomunikatsiini tekhnolohii ta elektronna inzheneriia, 2(2), 19–31 [in Ukrainian].
2. Lukova-Chuiko, N., Nakonechnyi, V., Toliupa, S., & Ziubina, R. (2020). Problemy zachystu krytychno vazhlyvych ob`iektiv infrastruktury [Problems of protection of critical infrastructure facilities]. Bezpeka informatsiinykh system i tekhnolohii, 1(2), 31-39 [in Ukrainian].
3. Toliupa, S., & Kulko, A. (2025). Neiro-nechitka systema vyiavlennia vtorhnen u informatsiinu merezhu krytychnoi infrastruktury [Neuro-fuzzy system for detecting intrusions into the information network of critical infrastructure]. Kiberbezpeka: osvita, nauka, tekhnika, 3(27), 233-247 [in Ukrainian].
4. Nosenko, K.M., Pivtorak, O.I., & Lichouzova, T.A. (2014). Ohliad system vyiavlennia atak v merezhevomu trafiku [Overview of network traffic attack detection systems]. Adaptyvni systemy avtomatychnoho upravlinnia, 1(24), 67-75 [in Ukrainian].
5. Dovbeshko, S.V., Toliupa, S.V., & Shestak, Ya.V. (2019). Zastosuvannia metodiv intelektualnoho analizu danykh dlia pobudovy system vyiavlennia atak [Application of data mining methods to build attack detection systems]. Suchasnyi zakhyst informatsii, 1(37), 6-15 [in Ukrainian].
6. Lazarenko, S.V. (2015). Osoblyvosti funktsionuvannia system vyiavlennia atak na avtomatyzovani systemy [Features of functioning of systems of detection of attacks on automated systems]. Suchasnyi zakhyst informatsii, 1, 33-40 [in Ukrainian].
7. Hulak, H.M., Semko, V.V., & Skladannyi, P.M. (2015). Model systemy vyiavlennia vtorhnen z vykorystanniam dvostupenevoho kryteriiu vyiavlennia merezhevykh anomalii [Model of the system for detecting intrusion based on the two-stage criterion for detecting fencing anomalies]. Suchasnyi zakhyst informatsii, 4, 81-85 [in Ukrainian].
8. Lukova-Chuiko, N.V., Toliupa, S.V., & Parkhomenko, I.I. (2021). Metody vyiavlennia vtorhnen u suchasnykh systemakh IDS [Intrusion detection methods in modern IDS systems]. Bezpeka informatsiinykh system i tekhnolohii, 1(5), 19-26 [in Ukrainian].
9. Korniienko, V.I., Husiev, O.Yu., & Herasina, O.V. (2020). Intelektualne modeliuvannia neliniinykh dynamichnykh protsesiv u systemakh keruvannia, kiberbezpeky, telekomunikatsii: pidruchnyk [Intelligent modeling of nonlinear dynamic processes in control systems, cybersecurity, telecommunications: a textbook]. Dnipro: NTU «DP», 536 [in Ukrainian].
10. Crovella, M.E., & Bestravos, A. (1997). Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes. IEEE Transactions on Networking, 5(6), 835-846 [in English].

11. Herasina, O.V. (2018). Metodyka intelektualnoi identyfikatsii ta prohnozuvannia trafiku v informatsiinykh telekomunikatsiinykh merezhakh [Methodology of intelligent identification and traffic forecasting in information telecommunication networks]. Systemy obrobky informatsii, 1(152), 94-99 [in Ukrainian].
12. Terenchuk, S., Pashko, A., Yeremenko, B., Kartavykh, S., & Ershova, N. (2018). Modelling Intelligent System for the Estimation of Technical State of Construction Structures. Eastern-European Journal of Enterprise Technologies, 3(2 (93)), 47-53 [in English].
13. Kondratenko, N.R., & Kuzemko, S.M. (2006). Osnovy neironnykh merezh. Teoriia ta praktyka [Fundamentals of Neural Networks. Theory and Practice]. Vinnytsia: VNTU, 104 [in Ukrainian].
14. Vladov, S., Shmelov, Y., & Petchenko, M. (2021). A neuro-fuzzy expert system for the control and diagnostics of helicopters aircraft engines technical state. ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer: Proceedings of the 17th International Conference, 40-52 [in English].
15. Wang, L.X., & Mendel, J.M. (1992). Generating fuzzy rules by learning from examples. IEEE Transactions on systems, man, and cybernetics, 22 (6), 1414-1427 [in English].
16. Ivakhnenko, A.G., & Madala, H.R. (1994). Inductive learning algorithms for complex systems modeling. London, Tokyo: CRC Press, 384 [in English].
17. Traffic Archive. [Electronic resource] – Access mode: http://ita.ee.lbl.gov.

Received 11.08.2025.
Accepted 13.08.2025.

Neural-fuzzy prediction of self-similar traffic of information and communication networks for attack detection systems

It was established that the current task is to build adequate predictive models of network self-similar traffic, which would allow their use in IDS for detecting network anomalies in real time with sufficient efficiency in terms of errors and reliability and increased efficiency. It is proposed to use adaptive filter-approximators in the form of adaptive fuzzy inference systems based on the Sugeno-Takagi, Takagi-Sugeno-Kang and Wang-Mendel algorithms for predicting self-similar traffic of information and communication networks. Since the problem of substantiating the type of neuro-fuzzy AFA with setting its parameters is polymodal, this requires the use of global optimization methods. The modeling of the network traffic forecasting process was carried out in the Matlab environment based on experimental data - traffic transmitted over the Internet. Multi-criteria optimization, direct random search and simulated annealing method were used as global optimization methods. The criterion of non-displacement (minimum shift) was used as the criterion of global optimization, and the criterion of parametric optimization was the regularity criterion, which was calculated on the test sample. As a result of the modeling, it was found that direct random search and multi-criteria optimization have the best convergence speed, the simulated annealing method showed the best performance, and the multi-criteria optimization algorithm showed the best convergence. It was also established that the minimum regularity criterion is met by the Anfis AFA based on the Takagi-Sugeno-Kanga algorithm, which is trained by a hybrid algorithm. Adequacy of the received traffic models of information and communication networks with experimental

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

data was checked and confirmed by the non-parametric criterion of signs. Further research should be aimed at substantiating and investigating the informativeness of the characteristics and models of self-similar network traffic and the effectiveness of the criteria and methods for recognizing attacks.

Key words: attack detection, information and communication network, prediction, self-similar traffic, adaptive fuzzy inference network, global optimization.

Герасіна Олександра Володимирівна – доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», к.т.н., доцент, ORCID: https://orcid.org/0000-0002-8196-0657

Gerasina Oleksandra – Associate Professor of Department of Information Security and Telecommunications, Dnipro University of Technology, Candidate of Technical Sciences, Associate Professor, ORCID: https://orcid.org/0000-0002-8196-0657