УДК 004.056:004.94
DOI https://doi.org/10.32782/IT/2022-1-4

Валерій КОРНІЄНКО
доктор технічних наук, професор, завідувач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, korniienko.v.i@nmu.one
***ORCID:** 0000-0002-0800-3359*
***Scopus Author ID:** 56446921900*

Олександра ГЕРАСІНА
кандидат технічних наук, доцент, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, herasina.o.v@nmu.one
***ORCID:** 0000-0002-8196-0657*
***Scopus Author ID:** 55998621600*

Дмитро ТИМОФЄЄВ
старший викладач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, tymofieiev.d.s@nmu.one
***ORCID:** 0000-0002-9718-6678*
***Scopus Author ID:** 55437340600*

Олександр САФАРОВ
кандидат технічних наук, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, safarov.o.o@nmu.one
***ORCID:** 0000-0003-1489-2006*
***Scopus Author ID:** 57191867000*

Юлія КОВАЛЬОВА
кандидат технічних наук, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005, kovalova.yu.v@nmu.one
***ORCID:** 0000-0002-9234-4454*
***Scopus Author ID:** 55320891100*

Бібліографічний опис статті: Корнієнко, В., Герасіна, О., Тимофєєв, Д., Сафаров, О., Ковальова, Ю. (2022). Ідентифікація та прогнозування самоподібного трафіку інформаційно-комунікаційних мереж для систем виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 1, 20–29, doi: https://doi.org/10.32782/IT/2022-1-4

ІДЕНТИФІКАЦІЯ ТА ПРОГНОЗУВАННЯ САМОПОДІБНОГО ТРАФІКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

У роботі визначена актуальність розробки та вдосконалення систем виявлення вторгнень, головним завданням яких є розпізнавання мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі. Ця проблема вирішується шляхом використання засобів моніторингу, здатних аналізувати трафік мережі в режимі реального часу. Для цього сформульовано математичну задачу структурно-параметричної ідентифікації та прогнозування трафіку в інформаційно-комунікаційних мережах. Шляхом моделювання на основі експериментальних даних показана ефективність розв'язання задачі структурно-параметричної ідентифікації трафіка із використанням глобальних методів оптимізації та інтелектуальних базисних функцій. Доведена ефективність використання блочно-орієнтованих структур шуканих моделей та адаптивних нечітких алгоритмів при розв'язанні задачі прогнозування трафіку. Перевірена та підтверджена адекватність отриманих моделей мережевого трафіку експериментальним даним.

Метою роботи *є дослідження та обґрунтування прогнозуючих моделей мережевого самоподібного трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.*

Методологія *вирішення поставленого завдання полягає у комплексному використанні методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку, нечіткої кластеризації), структурних (еволюційних, пошукових) та параметричних (градієнтних, квазіньютоновських) методів оптимізації, статистичних методів обробки модельних та експериментальних даних, адекватних закономірностям сучасного трафіку інформаційно-комунікаційних мереж, що має самоподібний характер.*

Наукова новизна. *Обґрунтовано методику структурно-параметричної ідентифікації і прогнозування самоподібного трафіку інформаційно-комунікаційних мереж, що включає композицію методів глобальної і локальної оптимізації, а також вибір блочно-орієнтованих структур моделей, яка дозволяє підвищити ймовірність визначення вторгнень для систем виявлення атак за рахунок зниження похибок прогнозуючих моделей самоподібного трафіка.*

Висновки. *Сформульована математична задача структурно-параметричної ідентифікації та прогнозування трафіку в інформаційно-комунікаційних мережах.*

Ключові слова: *ідентифікація, прогнозування, самоподібний трафік, інформаційно-комунікаційна мережа, виявлення атак.*

Valerii KORNIIENKO
Doctor of Technical Sciences, Professor, Head of Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, korniienko.v.i@nmu.one
ORCID: *0000-0002-0800-3359*
Scopus Author ID: *56446921900*

Oleksandra GERASINA
Candidate of Technical Sciences, Associate Professor, Associate Professor of Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, herasina.o.v@nmu.one
ORCID: *0000-0002-8196-0657*
Scopus Author ID: *55998621600*

Dmytro TYMOFIEIEV
Senior Lecturer of Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, tymofieiev.d.s@nmu.one
ORCID: *0000-0002-9718-6678*
Scopus Author ID: *55437340600*

Oleksandr SAFAROV
Candidate of Technical Sciences, Associate Professor of Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, safarov.o.o@nmu.one
ORCID: *0000-0003-1489-2006*
Scopus Author ID: *57191867000*

Yuliia KOVALOVA
Candidate of Technical Sciences, Associate Professor of Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, kovalova.yu.v@nmu.one
ORCID: *0000-0002-9234-4454*
Scopus Author ID: *55320891100*

To cite this article: Korniienko, V., Gerasina, O., Tymofieiev, D., Safarov, O., Kovalova, Yu. (2022). Identyfikatsiia ta prohnozuvannia samopodibnoho trafiku informatsiino-komunikatsiinykh merezh dlia system vyiavlennia atak [Identification and prediction of self-similar traffic of information and communication networks for attack detection systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 1, 20–29, doi: https://doi.org/10.32782/IT/2022-1-4

IDENTIFICATION AND PREDICTION OF SELF-SIMILAR TRAFFIC OF INFORMATION AND COMMUNICATION NETWORKS FOR ATTACK DETECTION SYSTEMS

The urgency of development and improvement of intrusion detection systems is determined in the work, the main task of which is to recognize network attacks, attempts of unauthorized access and use of network resources. This problem is solved by using monitoring tools that can analyze real-time network traffic. For this purpose the mathematical problem of structural-parametric identification and forecasting of traffic in information and communication networks is formulated. The efficiency of solving the problem of structural-parametric identification of traffic using global optimization methods and intelligent basic functions is shown by modeling on the basis of experimental data. The efficiency of using block-oriented structures of the required models and adaptive fuzzy algorithms in solving the problem of traffic forecasting is proved. The adequacy of the obtained models of network traffic with experimental data is checked and confirmed.

***The aim** of the work is to study and substantiate predictive models of network self-similar traffic to detect its anomalies when used in systems to detect and prevent attacks.*

***The methodology** of solving this problem is the integrated use of methods of artificial intelligence systems (neural networks, fuzzy inference systems, fuzzy clustering), structural (evolutionary, exploratory) and parametric (gradient, quasi-Newtonian) optimization methods, statistical methods for modeling and experimental data. modern traffic of information and communication networks, which has a self-similar nature.*

***Scientific novelty.** The method of structural-parametric identification and forecasting of self-similar traffic of information and communication networks is substantiated, which includes the composition of global and local optimization methods, as well as the choice of block-oriented model structures, which allows to increase the probability of traffic.*

***Conclusions.** The mathematical problem of structural-parametric identification and forecasting of traffic in information and communication networks is formulated.*

***Key words:** identification, prediction, self-similar traffic, information and communication network, detection of attacks.*

Актуальність проблеми. Розвиток інформаційно-комунікаційних систем і мереж (ІКМ) та інформаційних технологій супроводжується проблемами безпеки мережевих ресурсів.

Одним із рішень актуальної задачі захисту ІКМ від кібератак є розробка та вдосконалення систем виявлення та запобігання атак (СВА) (Лукова-Чуйко, Наконечний, Толюпа, Зюбіна, 2020; Браницкий, Котенко, 2016; Носенко, Півторак, Ліхоузова, 2014), головне завдання яких полягає у виявленні мережевих атак, спроб несанкціонованого доступу і використання ресурсів мережі.

Аналіз останніх досліджень і публікацій. Мета функціонування СВА зводиться до оперативного виявлення вторгнень в ІКМ та запровадження ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів (Довбешко, Толюпа, Шестак, 2019).

Наразі сформувались два напрямки протидії вторгнень: виявлення зловживань та виявлення аномалій (Довбешко, Толюпа, Шестак, 2019; Лазаренко, 2015). При виявленні мережевих аномалій (Браницкий, Котенко, 2016) даними для аналізу є мережевий трафік, представлений як інтенстівность (швидкість) передачі даних або набір мережевих пакетів, в загальному випадку фрагментованих на рівні IP. Дані можуть бути агреговані за певний часовий інтервал і нормалізовані, по ним оцінюються характеристики (набір ознак) трафіку. Створений набір ознак порівнюється з набором характеристик нормальної діяльності об'єкта (користувача або системи) – шаблоном нормальної поведінки. Якщо спостерігається суттєва розбіжність порівнюваних наборів, то фіксується мережева аномалія. В іншому випадку відбувається уточнення шаблону нормального трафіку за допомогою зміни параметрів його настройки з урахуванням поточного спостережуваного профілю мережевої активності. При цьому рішення о стані ІКМ приймається, зазвичай, за статистичними правилами (критеріями) (Браницкий, Котенко, 2016; Довбешко, Толюпа, Шестак, 2019; Лазаренко, 2015; Смирнов, Дрейс, Даниленко, 2014).

Для визначення шаблону нормальної поведінки перспективним є використання моделей захисту на основі розпізнавання аномалій в ІКМ (Гулак, Семко, Складанний, 2015; Бекетова, Ахметов, Корченко, Лахно, 2016; Петров, Корченко, Лахно, 2015; Карачанская, Соседова, 2019), оскільки поточний трафік є реалізацією випадкового процесу, а його адекватна модель – статистично стійка закономірність цього процесу.

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 (Корнієнко,

Гусєв, Герасіна, 2020; Riedi, Crouse, Ribeiro, Baraniuk, 1999).

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 трафіку дозволяє підвищити оперативність виявлення атак.

Таким чином, невирішеною задачею є побудова адекватних прогнозуючих моделей мережевого самоподібного трафіку, які б дозволяли їх використання в СВА для виявлення мережевих аномалій в реальному масштабі часу з достатньою ефективністю відносно похибок і достовірності та підвищеною оперативністю.

Мета статті: дослідження та обґрунтування прогнозуючих моделей мережевого самоподібного трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.

Виклад основного матеріалу.

Задача структурно-параметричної ідентифікації та прогнозування трафіку. Сформулюємо цю задачу таким чином: на підставі експериментальної множини функцій (часових рядів) виходу процесу і його статистичних характеристик в умовах завад визначити структуру (узагальнену функцію Φ) і вектор параметрів a прогнозуючої моделі виду:

$$\hat{Y}[k+n] = \Phi\{Y[k], w[k], \xi[k], a[k], k\}, \quad (1)$$

що достатньо точно (у сенсі деякого критерію) апроксимують процес відносно вхідних і вихідних величин у всьому функціональному просторі. Тут $Y[k], w[k], \xi[k]$ – відповідно, вектори (матриці) виходу процесу, його статистичних характеристик і шуму до поточного часу k з відповідними глибинами пам'яті; n – глибина прогнозу (для компенсації чистого запізнювання і часу на реакцію СВА). Вважаємо, що оцінка стану процесу (1) виконується за допомогою відповідних фільтрів спостереження.

Формування вектора $I_s = \{\Phi, a\}$ оцінки структури Φ (структурна ідентифікація) і параметрів a (параметрична ідентифікація) моделі (1) здійснюється на основі векторів сигналів спостереження шляхом мінімізації прийнятого функціонала:

$$J[I_s] \to \min_{I_s \in S} J \Rightarrow I_s^{opt} = \{\Phi_{opt}, a_{opt}\}, \quad (2)$$

де S – обмеження.

При розв'язанні задачі (2) мають бути визначені (обрані):

– ефективні методи оптимізації;
– зміст критерію (функціонала) J;
– засоби врахування обмежень S;
– тип структури моделі;
– базисні функції.

Для структурної ідентифікації ефективними вважаються зовнішні критерії (функціонали J), що адекватні задачі побудови моделей із мінімальною дисперсією похибки прогнозу, які поділяються на критерії регулярності і критерії незміщенності (мінімуму зсуву) (Корнієнко, Гусєв, Герасіна, 2020).

До критеріїв регулярності відноситься критерій мінімуму відносної похибки покрокового інтегрування:

$$J_{\varepsilon} = \frac{\left\| Y^*[k+n] - \hat{Y}[k+n] \right\|}{\left\| Y^*[k+n] \right\|}, \quad (3)$$

який обчислюється на всій вибірці експериментальних даних N. Він чутливий до рівня шуму у вхідних даних і при збільшенні завад його мінімум зміщується в область простіших моделей.

Стійкіші до завад критерії незміщенності. Наприклад, критерій мінімуму зсуву, заснований на аналізі рішень, має вигляд:

$$J_{см} = \frac{\left\| \hat{Y}_A[k+n] - \hat{Y}_B[k+n] \right\|}{\left\| Y^*[k+n] \right\|}, \quad (4)$$

де $\hat{Y}_A[k+n]$ і $\hat{Y}_B[k+n]$ – виходи моделей, навчених на вибірках A і B, відповідно. Тут обчислення зсуву здійснюється на всій вибірці $N = A + B$.

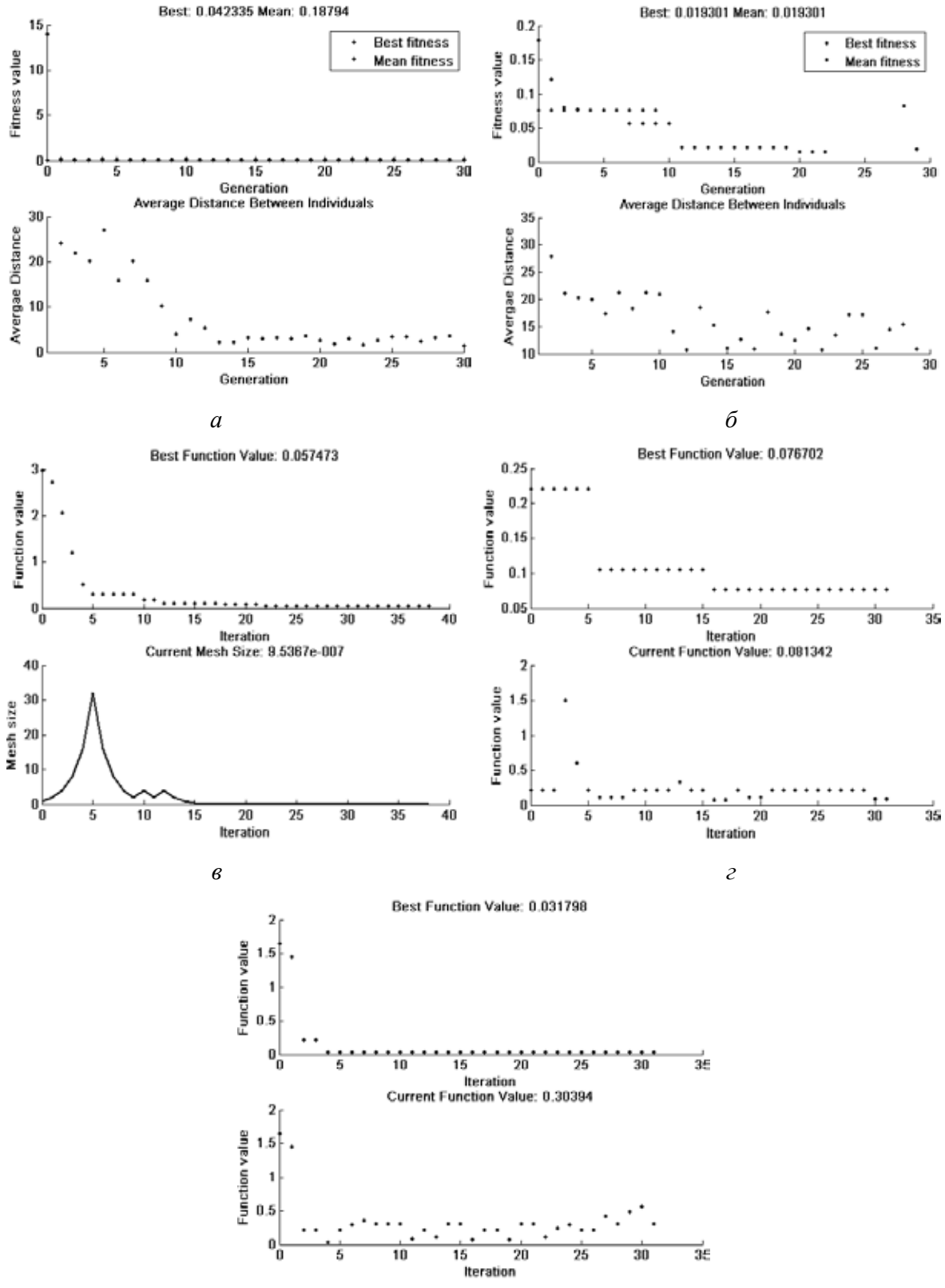
Структурно-параметрична ідентифікація трафіку.

Моделювання розв'язання задачі структурно-параметричної ідентифікації виконувалося на основі експериментальних даних трафіку, що передається через мережу Інтернет (Архів трафіку). 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 1 такт (5 с), а глибина пам'яті за різними входами від 1 до 4. В якості критерію структурної оптимізації обраний критерій зсуву (4). У якості глобальних методів оптимізації застосовувалися: генетичний алгоритм (ГА), ГА з багатокритеріальною оптимізацією (БО), прямий випадковий пошук (ПВП), метод імітації відпалу (МІВ) та метод порогового прийняття (МПП) (Корнієнко, Гусєв, Герасіна, 2020). При цьому використовувалася структура моделей Гаммерштейна-Вінера з базисними функціями у вигляді нейронних мереж (НМ) прямого розповсюдження (ПР), НМ із радіальними базисними функціями (РБФ)

і адаптивної системи нейронечіткого висновку (Anfis) (Корнієнко, Гусєв, Герасіна, 2020).

Результати глобальної оптимізації структури моделі трафіку в ІКМ наведені на рис. 1.



а *б*

в *г*

д

Рис. 1. Результати глобальної оптимізації структури моделі трафіку за допомогою ГА (*а*), БО (*б*), ПВП (*в*), МІВ (*г*) і МПП (*д*)

Метод БО використовував ГА для знаходження оптимальних за Парето рішень, ПВП мав адаптивний крок пошуку і повний пошук навколо поточної ітерації, МІВ та МПП – обмежену область перевідпалу, ГА – одноточкове схрещування, селективний вибір батьків, формування нової популяції з витісненням. Кількість ітерацій для ПВП, МПП і МІВ (для ГА і БО поколінь) обмежувалося на рівні 100, а розмір простору пошуку для ПВП (для ГА і БО розмір популяції, для МПП і МІВ розмір області перевідпалу) – 30.

При глобальній оптимізації варіювалися наступні структурні характеристики моделі:

– тип базисної функції – НМПР, НМ із РБФ і Anfis;

– кількість нейронів в прихованому шарі;

– тип функцій активації та структура прихованого шару;

– тип алгоритму параметричної оптимізації.

В результаті моделювання (див. рис. 1) встановлено, що ГА має найвищу швидкість збіжності (ГА виходить в область оптимальних рішень на перших поколіннях, МПП – в середньому після 5 ітерацій, МІВ – після 15, а БО і ПВП – після 20 ітерацій). Алгоритм МПП виявив найкращу швидкодію (0,6 с на ітерацію при 0,7 с на ітерацію в МІВ, 2,2 с на ітерацію в ПВП, 19,3 с на покоління в ГА і 27,4 с на покоління в БО).

Алгоритм БО виявив найкращу збіжність (значення критерію похибки на перевірочній послідовності (3) склало 0,019 при його використанні, на відміну від 0032 – при МПП, 0,042 – при ГА, 0,057 – при ПВП і 0,077 – при МІО).

Результат параметричної ідентифікації трафіку в ІКМ наведено на рис. 2.

Встановлено, що мінімуму критерію зсуву (5) відповідають базисні функції у вигляді каскадної НМПР. При цьому кількість нейронів в прихованому шарі становить 73, функція активації прихованого шару – конкуруюча з м'яким максимумом, вихідного шару – лінійна, алгоритм навчання НМ – градієнтний спуск з вибором параметра швидкості настроювання.

За міру точності параметричної ідентифікації моделі оптимальної структури використовувався критерій похибки (3), значення якого склало – 0,0311.

Адекватність отриманої інтелектуальної прогнозуючої моделі трафіку перевірялась за непараметричним критерієм знаків. Було встановлено, що для рівня значущості 0,01 розроблена модель з ідентифікованими структурою і параметрами адекватна експериментальним реалізаціям.

Моделювання трафіку із використанням блочно-орієнтованих структур. Глибина прогнозу була прийнята 3 такти, а глибина пам'яті за різними входами від 1 до 4. Як критерій оцінки моделей обрано критерій мінімуму зсуву (4).

Як типи структур розглядались (табл. 1) моделі: Гамерштейна-Вінера; авторегресійна ARX; Вінера і Гамерштейна з базисними функці-

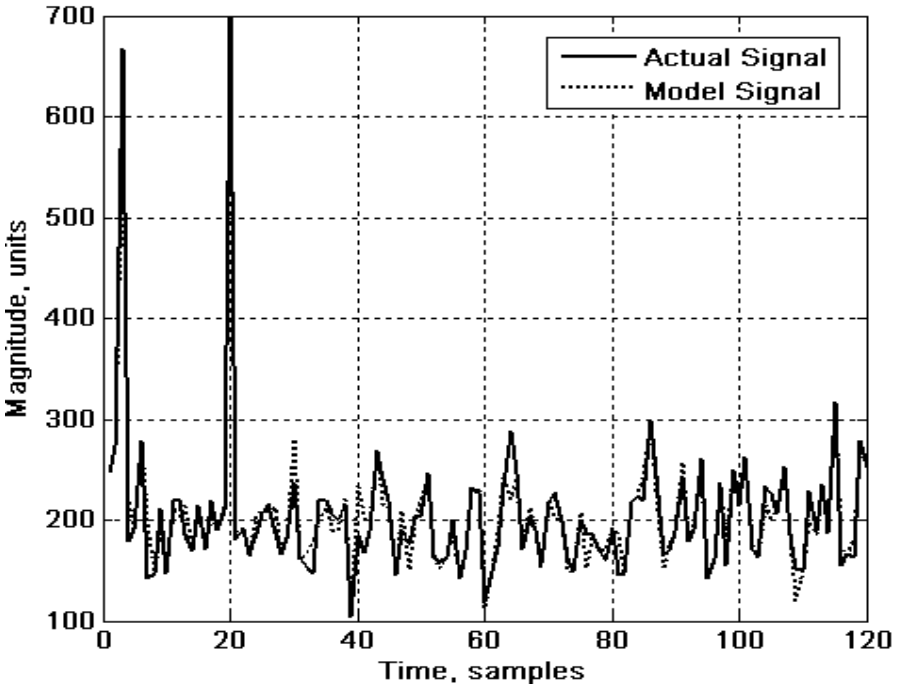
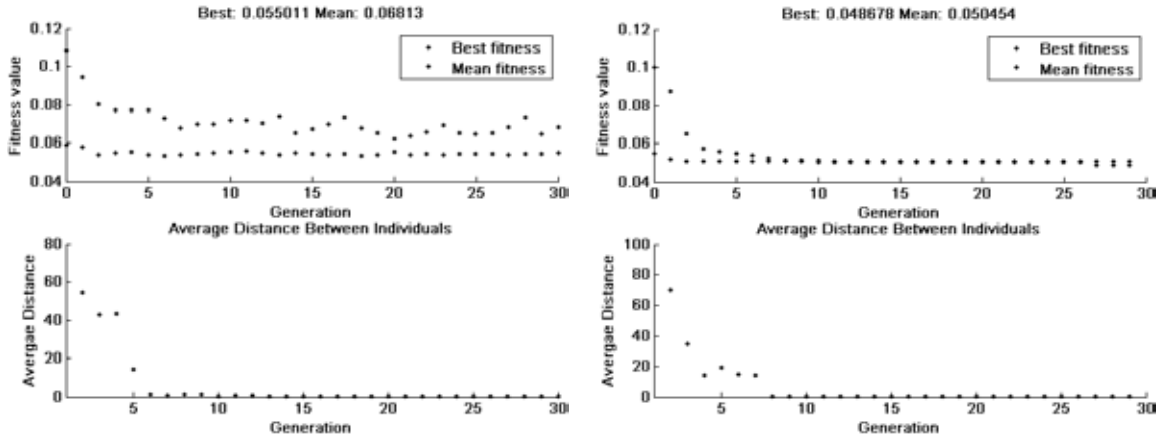
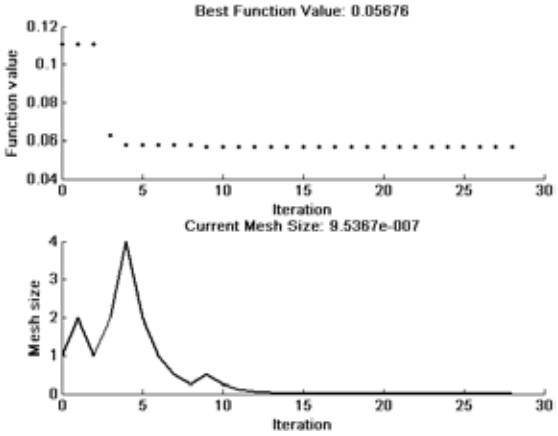


Рис. 2. Результат ідентифікації трафіку

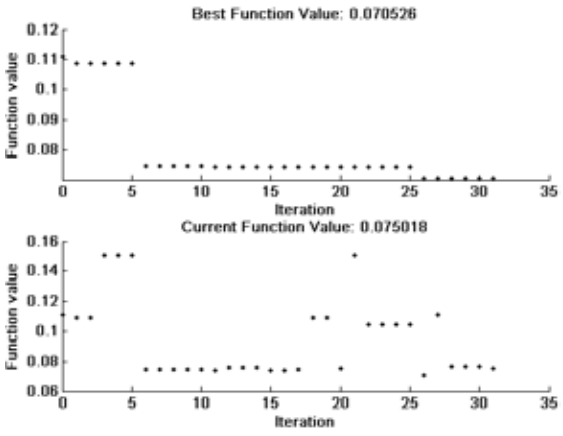


а

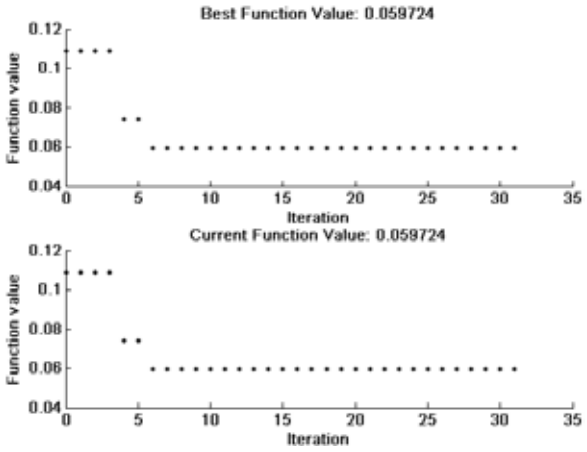
б



в



г



д

Рис. 3. Результати глобальної оптимізації структури і параметрів моделей для прогнозування трафіку за допомогою ГА (*а*), МО (*б*), ПВП (*в*), МІВ (*г*) і МПП (*д*)

Таблиця 1

Похибки незміщенності моделей, відн. од.

Базисна функція	**Тип структури моделі**			
	Гамерштейна-Вінера	ARX	Вінера	Гамерштейна
Каскадна НМПР		0,0619		
Вейвнет	0,0682	0,0679	0,0631	
Поліном Колмогорова-Габора	0,1004			0,1262

ями у вигляді каскадної НМПР; вейвнету і поліному Колмогорова-Габора (Корнієнко, Гусєв, Герасіна, 2020).

Із цієї таблиці видно, що перевагу (у сенсі критерію мінімуму зсуву (4)) мають мережеві базисні функції (каскадна НМПР та вейвнет).

Час обчислень на комп'ютері з процесором Pentium IV за моделями Гамерштейна-Вінера, Вінера і Гамерштейна становить 7-10 мс на цикл прогнозу, а по ARX – 0,2 мс, що не вносить часових обмежень на застосування цих моделей для ідентифікації трафіка в ІКМ.

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

Адаптивне нечітке прогнозування трафіку.

Глибина прогнозу була прийнята у 4 такти, а глибина пам'яті за різними входами від 1 до 4. Результати глобальної оптимізації для знаходження оптимальної структури (типу) і параметрів базисних функцій наведені на рис. 3.

У якості глобальних методів оптимізації застосовувалися ГА, БО, ПВП, МІВ і МПП зі значеннями параметрів настроювання, наведеними вище.

Як критерій параметричної оптимізації використовувався критерій регулярності (3), який вираховується на перевірочної вибірці, а для структурної – критерій зсуву (4).

При глобальної оптимізації варіювалися наступні структурні характеристики:

– тип базисної функції – Anfis, нечіткі апроксиматори з субтрактивною кластеризацією (Genfis2) і кластеризацією с-середніх (Genfis3);

– для Anfis – кількість нейронів в прихованому шарі, його тип функцій належності і тип алгоритму параметричної оптимізації;

– для Genfis2 – діапазон впливу кластерного центру;

– для Genfis3 – алгоритм нечіткої логіки (Мамдані або Сугено) і кількість кластерів, що визначає число правил і функцій належності.

В результаті моделювання встановлено, що ГА має найкращу швидкість збіжності (ГА виходить в область оптимальних рішень на перших поколіннях, БО, МПП і ПВП – в середньому після 10 ітерацій, МІВ – після 25 ітерацій).

Алгоритм МІВ виявив найкращу швидкодію (1,9 с на ітерацію при 3 з на ітерацію в МПП, 7,8 с на ітерацію в ПВП, 17,3 с на покоління в ГА і 21,2 с на покоління в БО). При цьому алгоритм БО виявив найкращу збіжність (значення критерію незміщенності (4) при його використанні склали 0,049, на відміну від 0,055 при ГА, 0,057 при ПВП, 0,06 при МПП і 0,07 при МІВ).

Результат прогнозування трафіку в ІТМ наведено на рис. 4.

Встановлено, що мінімуму критерію регулярності відповідають моделі Genfis2 з діапазоном впливу кластерного центру рівним 0,31. Значення критерію параметричної оптимізації склало 0,0329.

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

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Сформульована математична

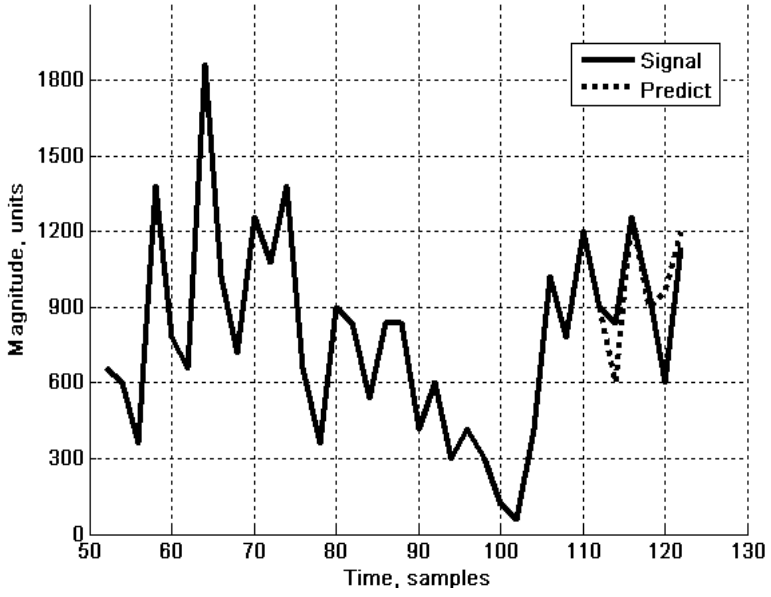


Рис. 4. Результат прогнозування мережевого трафіку

задача структурно-параметричної ідентифікації та прогнозування трафіку в інформаційно-комунікаційних мережах.

Шляхом моделювання на основі експериментальних даних показана ефективність розв'язання задачі структурно-параметричної ідентифікації трафіка із використанням глобальних методів оптимізації та інтелектуальних базисних функцій (нейромереж та систем нечіткого висновку). Доведена ефективність використання блочно-орієнтованих структур шуканих моделей та адаптивних нечітких алгоритмів при розв'язанні задачі прогнозування трафіку.

Перевірена та підтверджена адекватність отриманих моделей мережевого трафіку експериментальним даним.

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

ЛІТЕРАТУРА:

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

2. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН*. 2016. Вып. 2(45). С. 207-244. URL: www.proceedings.spiiras.nw.ru.

3. Носенко К.М., Півторак О.І., Ліхоузова Т.А. Огляд систем виявлення атак в мережевому трафіку. *Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління»*. 2014. № 1(24). С. 67-75.

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

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

6. Смирнов А., Дрейс Ю., Даниленко Д. Имитационная модель NIPDS для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях. *Ukrainian Scientific Journal of Information Security*. 2014. Vol. 20. Issue 1. P. 29-35.

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

8. Бекетова Г., Ахметов Б., Корченко А., Лахно В. Разработка модели интеллектуального распознавания аномалий и кибератак с использованием логических процедур, базирующихся на покрытиях матриц признаков. *Ukrainian Scientific Journal of Information Security*. 2016. Vol. 22. Issue 3. P. 242-254. DOI: 10.18372/2225-5036.22.11096.

9. Петров О., Корченко О., Лахно В. Метод та модель інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту. *Ukrainian Scientific Journal of Information Security*. 2015. Vol. 21. Issue 1. P. 26-34.

10. Карачанская Е.В., Соседова Н.И. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре. *Безопасность информационных технологий*. 2019. С. 98-110. URL: https://bit.mephi.ru/index.php/bit/article/view/1185. Doi: http://dx.doi.org/ 10.26583/bit/2019.1.10.

11. Корнієнко В.І., Гусєв О.Ю., Герасіна О.В. Інтелектуальне моделювання нелінійних динамічних процесів у системах керування, кібербезпеки, телекомунікацій: підручник. *Дніпро*: *НТУ «ДП»*. 2020. 536 с.

12. Riedi R.H., Crouse M.S., Ribeiro V., Baraniuk R.G. A multifractal wavelet model with application to network traffic. *IEEE Transactions on Information Theory*. 1999. Vol. 45. P. 992-1018.

13. Архів трафіку. URL: http://ita.ee.lbl.gov.

REFERENCES:

1. 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. – Security of information systems and technologies*, 1(2), 31-39 [in Ukrainian].

2. Branitskii, A.A., Kotenko, I.V. (2016). Analiz i klassifikaciya metodov obnaruzheniya setevyh atak [Analysis and classification of network attack detection methods]. *Trudy SPIIRAN. – Proceedings of SPIIRAS,* 2(45), 207-244 [in Russian]. URL: www.proceedings.spiiras.nw.ru.

3. Nosenko, K.M., Pivtorak, O.I., Lichouzova, T.A. (2014). Ohliad system vyiavlennia atak v merezhevomu trafiku [Overview of network traffic attack detection systems]. *Mizhvidomchyi naukovo-tekhnichnyi zbirnyk*

«Adaptyvni systemy avtomatychnoho upravlinnia». – *Interdepartmental scientific and technical collection "Adaptive automatic control systems"*, 1(24), 67-75 [in Ukrainian].

4. 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*. – *Modern information protection*, 1(37), 6-15 [in Ukrainian].

5. 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*. – *Modern information protection*, 1, 33-40 [in Ukrainian].

6. Smirnov, A., Dreis, Yu., Danylenko, D. (2014). Imitacionnaya model' NIPDS dlya obnaruzheniya i predotvrashcheniya vtorzhenij v telekommunikacionnyh sistemah i setyah [NIPDS simulation model for intrusion detection and prevention in telecommunications systems and networks]. *Ukrainian Scientific Journal of Information Security*. – *Ukrainian Scientific Journal of Information Security,* 20, 1, 29-35 [in Russian].

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 – Modern information protection*, 4, 81-85 [in Ukrainian].

8. Beketova, G., Ahmetov, B., Korchenko, A., Lahno, V. (2016). Razrabotka modeli intellektual'nogo raspoznavaniya anomalij i kiberatak s ispol'zovaniem logicheskih procedur, baziruyushchihsya na pokrytiyah matric priznakov [Development of a model for intelligent recognition of anomalies and cyberattacks using logical procedures based on coverage of feature matrices]. *Ukrainian Scientific Journal of Information Security. – Ukrainian Scientific Journal of Information Security*, 22, 3, 242-254 [in Russian]. DOI: 10.18372/2225-5036.22.11096.

9. Petrov, O., Korchenko, O., Lakhno, V. (2015). Metod ta model intelektualnoho rozpiznavannia zahroz informatsiino-komunikatsiinomu seredovyshchu transportu [Method and model of intellectual recognition of threats to the information and communication environment of transport]. *Ukrainian Scientific Journal of Information Security. – Ukrainian Scientific Journal of Information Security*, 21, 1, 26-34 [in Ukrainian].

10. Karachanskaya, E.V., Sosedova, N.I. (2019). Metod vyyavleniya anomalij setevogo trafika, osnovannyj na ego samopodobnoj structure [A method for detecting network traffic anomalies based on its self-similar structure]. *Bezopasnost' informacionnyh tekhnologij*. – *Information technology security*, 98-110 [in Russian]. URL: https://bit.mephi.ru/index.php/bit/article/view/1185. DOI: http://dx.doi.org/ 10.26583/bit/2019.1.10.

11. 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»*. – *Dnipro: NTU «DP»*, 536 [in Ukrainian].

12. Riedi, R.H., Crouse, M.S., Ribeiro, V., Baraniuk, R.G. (1999). A multifractal wavelet model with application to network traffic [A multifractal wavelet model with application to network traffic]. *IEEE Transactions on Information Theory*. – *IEEE Transactions on Information Theory*, 45, 992-1018 [in English].

13. Traffic archive [Traffic archive]. URL: http://ita.ee.lbl.gov.