УДК 004.056:004.94 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.16

О. В. ГЕРАСІНА
кандидат технічних наук, доцент,
доцент кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка»
ORCID: 0000-0002-8196-0657

МОДЕЛЮВАННЯ ТРАФІКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ БЛОЧНО-ОРІЄНТОВАНИХ СТРУКТУР ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

У роботі встановлено, що актуальним завданням є побудова адекватних прогнозуючих моделей мережевого самоподібного трафіку, які б дозволили використовувати їх в системах виявлення вторгнень для детектування мережевих аномалій в режимі реального часу з достатньою ефективністю відносно похибок і достовірності та підвищеною оперативністю. При цьому прогнозування мережевого самоподібного трафіку дозволяє підвищити оперативність виявлення атак. Запропоновано для прогнозування трафіку інформаційно-комунікаційних мереж використовувати інтелектуальні адаптивні фільтри-апроксиматори, які побудовані на основі блочно-орієнтованих моделей Вінера, Гамерштейна та їх комбінацій. Моделювання мережевого трафіку із використанням блочно-орієнтованих структур проводилося в середовищі Matlab на основі експериментальних даних – трафіку, що передається через Інтернет. Як критерій оцінки моделей було використано критерій незміщенності (мінімуму зсуву). Як типи структур розглядались моделі Вінера, Гамерштейна, Гамерштейна-Вінера і авторегресії із додатковим вхідним сигналом. Як базисні функції використовувались вейвнет, нейронні мережі прямого поширення, дерево рішень, лінійні функції, поліном Колмогорова-Габора, обмеження і зона нечутливості. В результаті моделювання було виявлено, що перевагу (у сенсі критерію мінімуму зсуву) мають блочно-орієнтовані моделі Гамерштейна-Вінера з інтелектуальними базисними функціями – сигмоїдальною нейронною мережею і вейвнет. Для інших досліджуваних блочно-орієнтованих моделей перевагу також мають інтелектуальні базисні функції. Адекватність отриманих моделей мережевого самоподібного трафіку експериментальним даним було перевірено та підтверджено за непараметричним критерієм знаків. Подальші дослідження мають бути спрямовані на обґрунтування та дослідження інформативності характеристик і моделей трафіку інформаційно-комунікаційних мереж, а також ефективності критеріїв та методів розпізнавання атак. ***Висновки.*** *Доведена ефективність використання блочно-орієнтованих структур та інтелектуальних базисних функцій шуканих моделей мережевого самоподібного трафіку при розв'язанні задачі його прогнозування.*

Ключові слова: *моделювання, прогнозування, самоподібний трафік, інформаційно-комунікаційна мережа, модель Вінера, модель Гамерштейна, виявлення атак.*

O. V. GERASINA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Security
and Telecommunications
Dnipro University of Technology
ORCID: 0000-0002-8196-0657

MODELING OF INFORMATION AND COMMUNICATION NETWORK TRAFFIC USING BLOCK-ORIENTED STRUCTURES 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. At the same time, predicting network self-similar traffic allows to increase the efficiency of attack detection. It is proposed to use intelligent adaptive approximator filters for predicting information and communication network traffic, which are built on the basis of block-oriented Wiener, Hammerstein models and their combinations. Network traffic modeling using block-oriented structures was carried out in the Matlab environment based on experimental data – traffic transmitted via the Internet. The criterion of unbiasedness (minimum shift) was used as a criterion for evaluating models. The types of structures considered were Wiener, Hammerstein, Hammerstein-Wiener models and autoregression with an additional input signal. Wavenet, forward propagation neural networks, decision tree, linear functions, Kolmogorov-Gabor polynomial, saturation and dead zone were used as basic functions. As a result of the modeling, it was found that the advantage (in the sense of the minimum shift criterion) is given to block-oriented Hammerstein-Wiener models with intelligent basis functions – a sigmoidal neural network and a wavenet. For

other studied block-oriented models, intelligent basis functions are also preferred. The adequacy of the obtained models of network self-similar traffic to experimental data was checked and confirmed by the non-parametric sign criterion. Further research should be aimed at substantiating and studying the informativeness of the characteristics and traffic models of information and communication networks, as well as the effectiveness of the criteria and methods for recognizing attacks. ***Conclusions.*** *The effectiveness of using block-oriented structures and intelligent basis functions of the sought-after models of network self-similar traffic in solving the problem of its prediction is proven.*

Key words: *modeling, prediction, self-similar traffic, information and communication network, Wiener model, Hammerstein model, detection of attacks.*

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

Трафік, що виникає в сучасних ІКМ, є нелінійним стохастичним процесом з властивостями самоподоби, з хаотичною і фрактальною динамікою [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].

У роботі [11] запропоновано методику прогнозування трафіку в ІКМ, яка складається з двох етапів: фрактальний аналіз трафіку та його прогнозування із використанням адаптивних фільтрів-апроксиматорів (АФА). При цьому, на другому етапі здійснюється обґрунтування методів і критерію структурної (глобальної) оптимізації, типу структури моделі, базисних функцій та методів параметричної оптимізації, а також структурна та параметрична оптимізація. Але у роботі [11] відсутнє обґрунтування типу структур моделі та базисних функцій (типу АФА) для подальшого проведення прогнозування мережевого трафіку. Також у роботах [9, 12–14] наведено використання блочно-орієнтованих моделей для вирішення різних завдань, але відсутні роботи, де виконується обґрунтування їх типів.

Таким чином, невирішеною задачею є обґрунтування типу структур та базисних функцій моделей для прогнозування самоподібного трафіку ІКМ для виявлення його аномалій при використанні в СВА.

Формулювання мети дослідження

Дослідження та обґрунтування типів структур та базисних функцій прогнозуючих моделей мережевого самоподібного трафіку для виявлення його аномалій при використанні в системах виявлення та запобігання атак.

Викладення основного матеріалу дослідження

Однією з основних проблем при вирішенні задач ідентифікації та прогнозування складних систем є вибір типів структур моделей. Правильний вибір структури моделі багато у чому визначає успіх побудови адекватної моделі системи. Зазвичай структуру визначають, виходячи з фізичних законів, що реалізуються у системі. Однак, така модель найчастіше має високу розмірність, що ускладнює її практичне використання.

Більш продуктивним є визначення структур моделей складних систем на основі спостережень їх вхідних і вихідних змінних з використанням апроксимацій у вигляді функціональних рядів Вольтера, поліномів Колмогорова-Габора, блочно-орієнтованих моделей тощо [9, 12].

У блочно-орієнтованих моделях мережевий трафік представляється шляхом композиції лінійного динамічного (ЛДБ) і нелінійного статичного (НСБ) блоків, наприклад, у вигляді моделей Вінера, Гамерштейна або їх комбінацій [12, 13].

Модель Вінера містить послідовно з'єднані нелінійний статичний і лінійний динамічний блоки (рис. 1, *а*), а у моделі Гамерштейна, навпаки, нелінійний блок приведений до виходу (рис. 1, *б*). На малюнках ЛДБ – лінії затримки *T*, величини яких (глибини пам'яті) визначаються розмірністю вхідних d_i і вихідних $d_{\hat{Y}}$ змінних, а у якості НСБ можуть використовуватися як традиційні засоби: поліноми Лежандра або Колмогорова-Габора, так і інтелектуальні – нейронні мережі, системи з нечіткою логікою тощо. Входом моделей є вектори спостережень $\{z_i[k]\} \in \hat{Z}[k]$ для моментів часу *k*, а виходом – його прогноз на *n* тактів ($\hat{Y}[k+n]$).

Модель Вінера-Гамерштейна утворюється шляхом об'єднання блоків моделей Вінера і Гамерштейна, для чого вводиться зворотний зв'язок (рис. 2, *а*). Модель Гамерштейна-Вінера утворюється послідовним з'єднанням моделей Гамерштейна і Вінера. При цьому у центрі з'єднання два лінійних динамічних блоки об'єднуються в один (рис. 2, *б*).

Також до блочно-орієнтованих моделей крім моделей Вінера, Гамерштейна та їх комбінацій (див. рис. 1–2) відносяться моделі авторегресії із додатковим вхідним сигналом – ARX-моделі, які описують нелінійні структури, використовуючи паралельну комбінацію нелінійних і лінійних блоків [12].

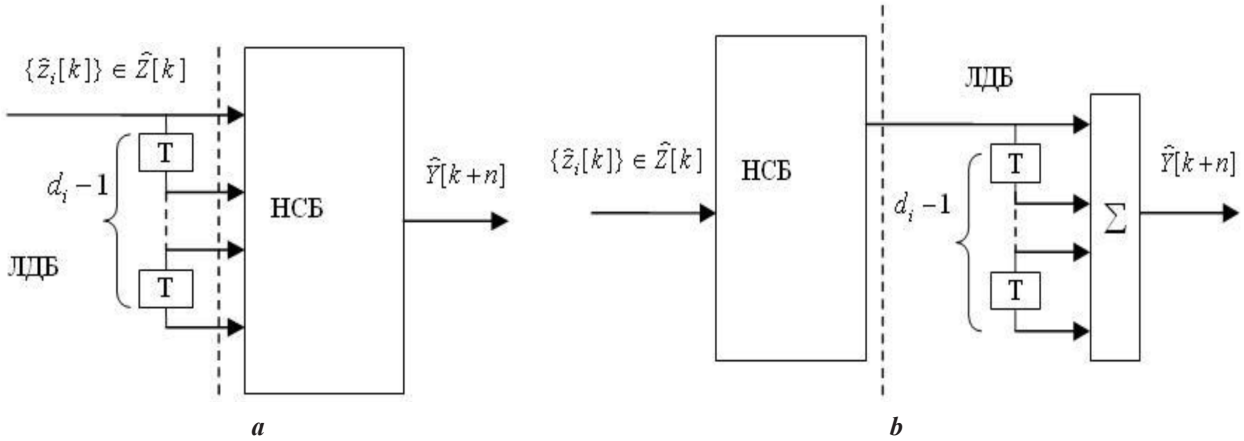


Рис. 1. Структура Вінера (*а*) і Гамерштейна (*б*) моделей мережевого трафіка

Обґрунтування блочно-орієнтованих структур моделей мережевого трафіку є складовою частиною методики інтелектуального прогнозування самоподібного трафіку ІКМ, яка дозволяє підвищити ймовірність визначення вторгнень для СВА за рахунок зниження похибок моделей самоподібного трафіка [11].

Моделювання задачі обґрунтування блочно-орієнтованих структур та базисних функцій моделей мережевого самоподібного трафіка виконувалось за допомогою стандартних та розроблених програм у середовищі Matlab / Simulink [14].

Як експериментальні дані було взято трафік, що передається через мережу Інтернет [15]. 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.

З особливостей цього процесу глибина прогнозу була прийнята 3 такти, а глибина пам'яті – 4.

Як критерій оцінки моделей обрано 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].

$$C_{см} = \frac{\left\| \hat{Y}_A[m+n] - \hat{Y}_B[m+n] \right\|}{\left\| Y^*[m+n] \right\|}. \quad (1)$$

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

Як типи структур розглядались моделі Вінера, Гамерштейна, Гамерштейна-Вінера і ARX. При цьому, як НСБ (базисні функції) для моделі ARX використовувались вейвнет (НМ з функцією активації у вигляді вейвлет), каскадна НМ прямого поширення з трикутною функцією активації прихованого шару, сигмоїдальна НМ (НМ прямого поширення з логістичною сигмоїдальною функцією активації прихованого шару), дерево рішень і лінійна функція, а для моделей Вінера, Гамерштейна і Гамерштейна-Вінера – вейвнет, поліном Колмогорова-Габора, сигмоїдальна НМ, кусково-лінійна функція, обмеження (Saturation – одна з нелінійностей; сигнал на виході блока дорівнює вхідному сигналу доти, поки не досягне заданих порогів обмеження: верхнього або нижнього; після цього сигнал перестає змінюватися) і зона нечутливості (DeadZone – одна з нелінійностей, що являє собою лінійну залежність вихідного сигналу від вхідного скрізь, за винятком області мертвої зони).

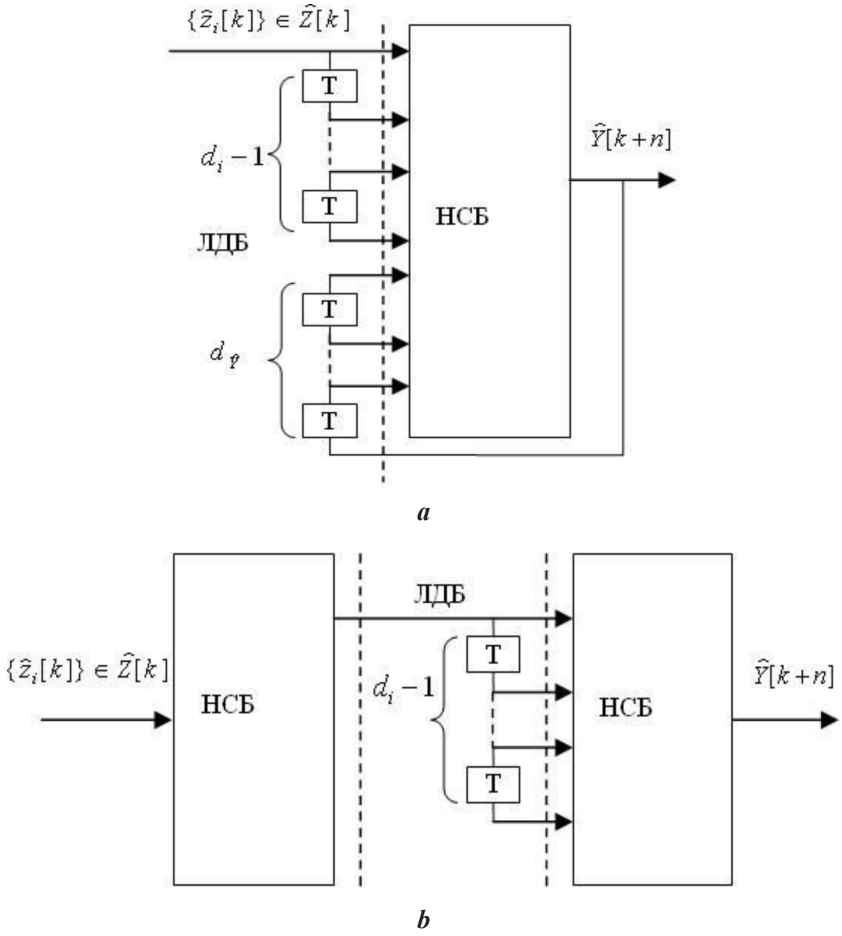


Рис. 2. Структура Вінера-Гамерштейна (*а*) і Гамерштейна-Вінера (*б*) моделей мережевого трафіка

Результати моделювання мережевого трафіку із використанням блочно-орієнтованої структури ARX наведено на рис. 3, *а*. При цьому значення критерію (1) склало 16,13 % для вейвнету, 15,86 % для каскадної НМ прямого поширення, 19,55 % для сигмоїдальної НМ, 20,05 % для дерева рішень і 21,19 % для лінійної функції.

Результати моделювання мережевого трафіку із використанням блочно-орієнтованої структури Гамерштейна-Вінера наведено на рис. 3, *б*. При цьому значення критерію (1) склало 3,70 % для вейвнету, 20,59 % для поліному Колмогорова-Габора, 1,77 % для сигмоїдальної НМ, 4,83 % для кусково-лінійної функції, 5,46 % для обмеження і 4,19 % для зони нечутливості.

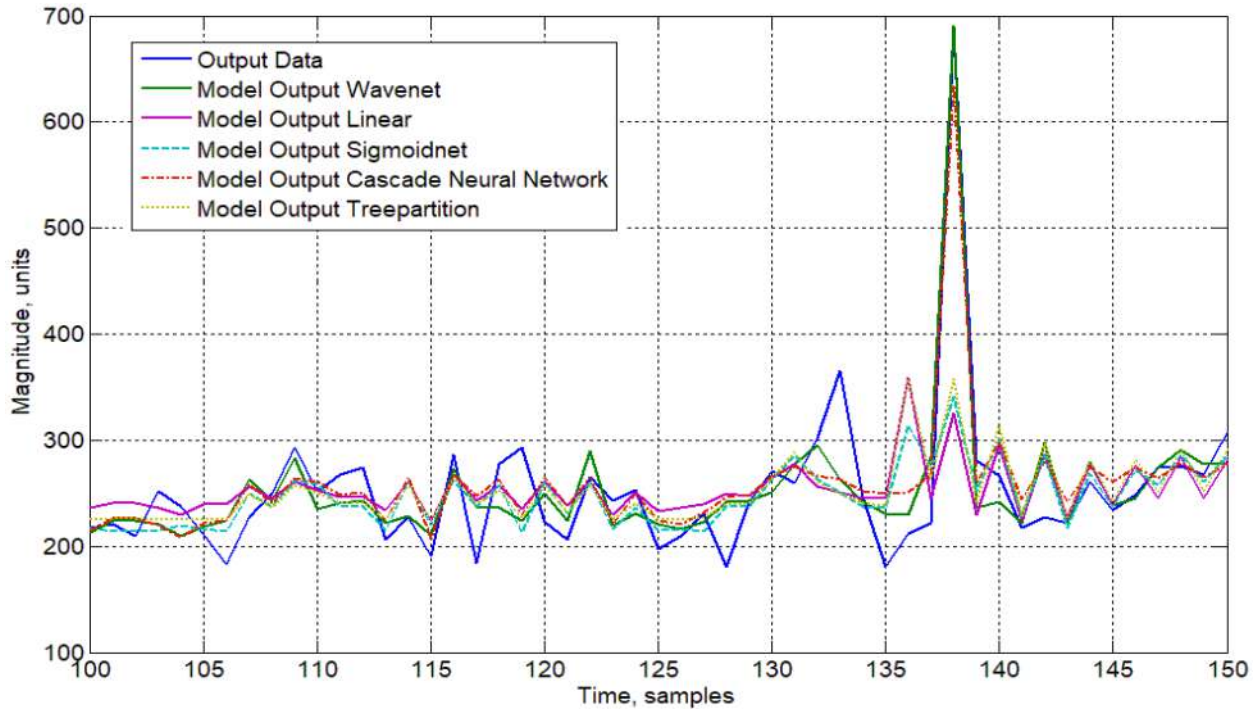
Результати моделювання мережевого трафіку із використанням блочно-орієнтованої структури Вінера наведено на рис. 4, *а*. При цьому значення критерію (1) склало 6,59 % для вейвнету, 8,36 % для поліному Колмогорова-Габора, 3,67 % для сигмоїдальної НМ, 10,73 % для кусково-лінійної функції, 9,22 % для обмеження і 8,36 % для зони нечутливості.

Результати моделювання мережевого трафіку із використанням блочно-орієнтованої структури Гамерштейна наведено на рис. 4, *б*. При цьому значення критерію (1) склало 7,17 % для вейвнету, 8,01 % для поліному Колмогорова-Габора, 7,18 % для сигмоїдальної НМ, 7,35 % для кусково-лінійної функції, 9,48 % для обмеження і 7,21 % для зони нечутливості.

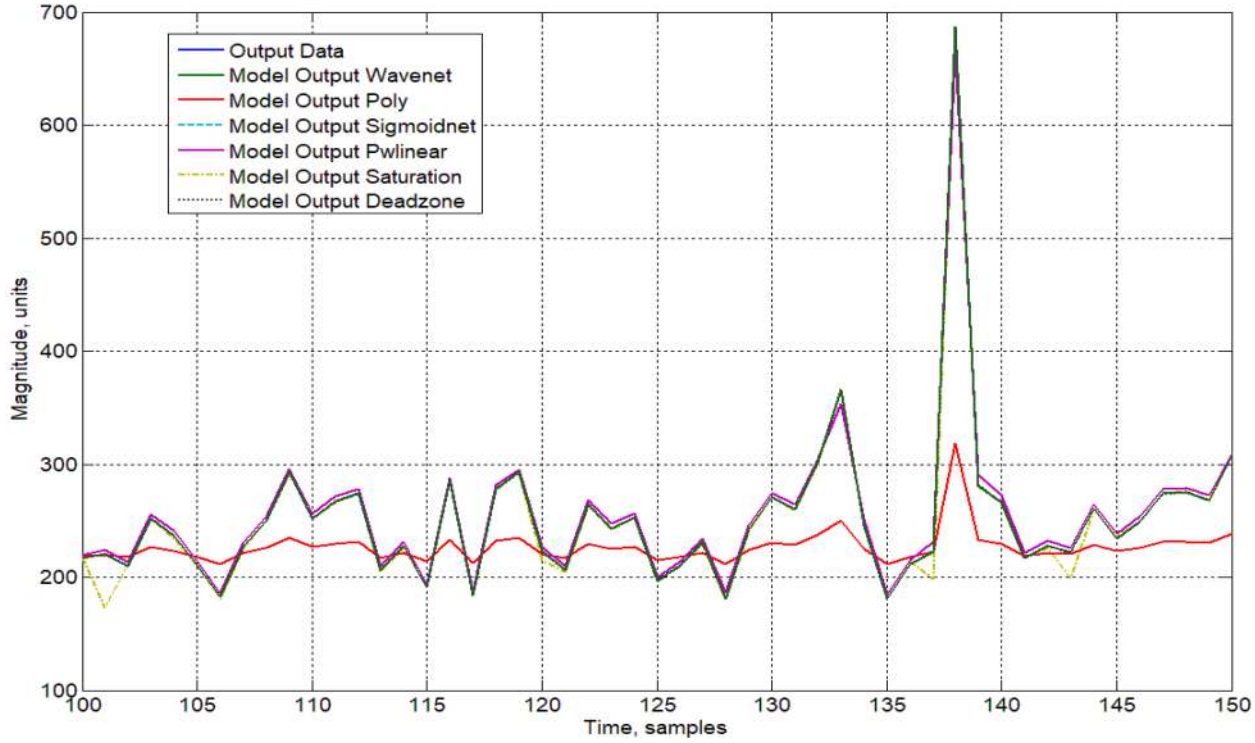
Встановлено (див. рис. 3–4), що перевагу (у сенсі критерію мінімуму зсуву (1)) мають блочно-орієнтовані моделі Гамерштейна-Вінера з інтелектуальними базисними функціями – сигмоїдальною НМ і вейвнет. Для інших моделей перевагу також мають інтелектуальні базисні функції (для Вінера, Гамерштейна – сигмоїдальна НМ і вейвнет, для ARX – сигмоїдальна НМ, каскадна НМ і вейвнет).

Час обчислень на комп'ютері з процесором Pentium IV за моделями Вінера, Гамерштейна і Гамерштейна-Вінера становить 8–11 мс на цикл прогнозу, а по ARX – 0,3 мс, що не вносить часових обмежень на застосування цих моделей для прогнозування трафіка в ІКМ.

Адекватність отриманих моделей мережевого трафіку перевірялася за непараметричним критерієм знаків. Було встановлено, що для рівня значущості 0,01 розроблені моделі адекватні експериментальним реалізаціям.



a



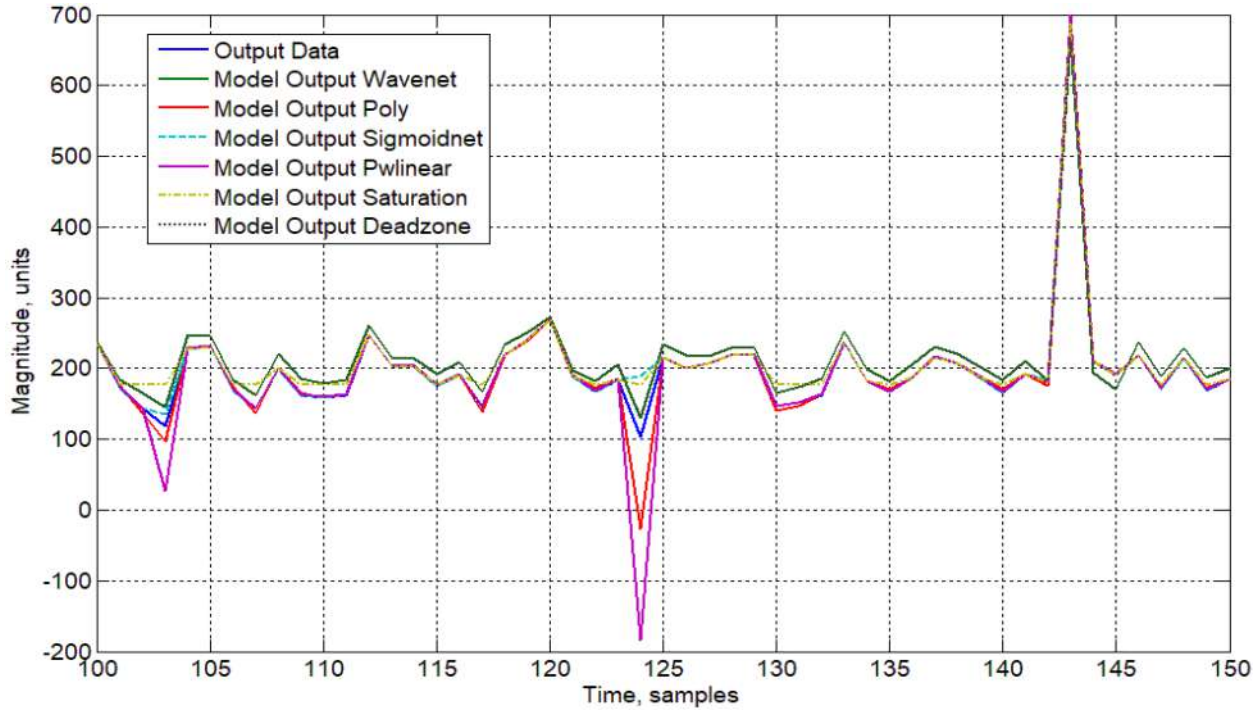
b

Рис. 3. Результати моделювання мережевого трафіку із використанням структури ARX (*а*) і Гамерштейна-Вінера (*б*)

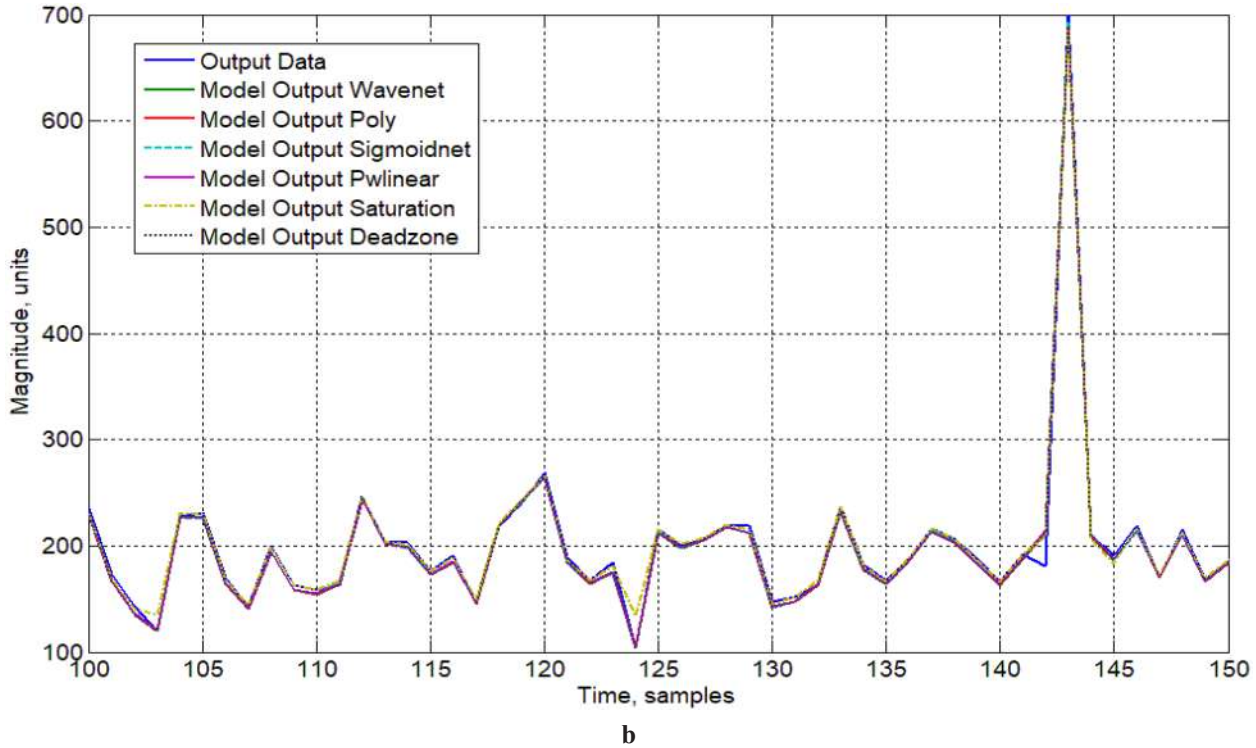
Висновки

Запропоновано для прогнозування самоподібного трафіку в інформаційно-комунікаційних мережах використовувати інтелектуальні адаптивні фільтри-апроксиматори, які побудовані на основі блочно-орієнтованих моделей Вінера, Гамерштейна та їх комбінацій.

Шляхом моделювання на основі експериментальних даних показана ефективність використання блочно-орієнтованих структур та інтелектуальних базисних функцій шуканих моделей мережевого трафіку при розв’язанні



a



b

Рис. 4. Результати моделювання мережевого трафіку із використанням структури Вінера (*а*) і Гамерштейна (*б*)

задачі його прогнозування. Перевірена та підтверджена адекватність отриманих моделей трафіку ІКМ експериментальним даним.

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

Список використаної літератури

1. Толюпа С. Лукова-Чуйко Н., Шестак Я. Засоби виявлення кібернетичних атак на інформаційні системи. *Інфокомунікаційні технології та електронна інженерія*. 2021. № 2 (2). С. 19–31.
2. 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.
3. Толюпа С., Кулько А. Нейро-нечітка система виявлення вторгнень у інформаційну мережу критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (27). С. 233–247.
4. Носенко К. М., Півторак О. І., Ліхоузова Т. А. Огляд систем виявлення атак в мережевому трафіку. *Адаптивні системи автоматичного управління*. 2014. № 1(24). С. 67–75.
5. 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.
6. Лазаренко С. В. Особливості функціонування систем виявлення атак на автоматизовані системи. *Сучасний захист інформації*. 2015. № 1. С. 33–40.
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. Лукова-Чуйко Н. В., Толюпа С. В., Пархоменко І. І. Методи виявлення вторгнень у сучасних системах IDS. *Безпека інформаційних систем і технологій*. 2021. № 1 (5). С. 19–26.
9. Корнієнко В. І., Гусєв О. Ю., Герасіна О. В. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник. 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. *Системи обробки інформації*. 2018. № 1 (152). С. 94–99.
12. Pillonetto G., Chen T., Chiuso A., De Nicolao G., Ljung L. Regularized system identification: Learning dynamic models from data. *Springer Nature*. 2022. 377 p. DOI: 10.1007/978-3-030-95860-2
13. Nikolic S. S. et al. Identification of Nonlinear Systems Using the Hammerstein-Wiener Model with Improved Orthogonal Functions. *Elektronika ir Elektrotechnika*. 2023. № 29 (2). P. 4–11. DOI: 10.5755/j02.eie.33838
14. Dai T., Aljanaideh K., Chen R., Singh R., Stothert A., Ljung L. Deep Learning of Dynamic Systems using System Identification Toolbox. *IFAC PapersOnLine*. 2024. № 58 (15). P. 580–585. DOI: 10.13140/RG.2.2.29127.47527
15. Архів трафіку. URL: http://ita.ee.lbl.gov
16. Ivakhnenko A. G., Madala H. R. Inductive learning algorithms for complex systems modeling. *London, Tokyo: CRC Press*. 1994. 384 p.

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*, no. 2(2), pp. 19–31.
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*, no. 1(2), pp. 31–39.
3. Toliupa, S. & Kulko A. (2025). Neiro-nechitka systema vyiavlennia vtorhnen u informa-tsiinu merezhu krytychnoi infrastruktury [Neuro-fuzzy system for detecting intrusions into the information network of critical infrastructure]. *Kiberbezpeka: osvita, nauka, tekhnika*, no. 3(27), pp. 233–247.
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*, no. 1(24), pp. 67–75.
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*, no. 1(37), pp. 6–15.
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*, no. 1, pp. 33–40.
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*, no. 4, pp. 81–85.
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*, no. 1(5), pp. 19–26.

9. Korniienko V. I., Gusiev O. Yu., & Gerasina 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".

10. Crovella M. E., & Bestravos A. (1997). Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes. *IEEE Transactions on Networking*, no. 5(6), pp. 835–846.

11. Gerasina 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*, no. 1(152), pp. 94–99.

12. Pillonetto G., Chen T., Chiuso A., De Nicolao G., & Ljung L. (2022). Regularized system identification: Learning dynamic models from data. *Springer Nature*. DOI: 10.1007/978-3-030-95860-2

13. Nikolic S. S. et al. (2023). Identification of Nonlinear Systems Using the Hammerstein-Wiener Model with Improved Orthogonal Functions. *Elektronika ir Elektrotechnika*, no. 29 (2), pp. 4–11. DOI: 10.5755/j02.eie.33838

14. Dai T., Aljanaideh K., Chen R., Singh R., Stothert A., & Ljung L. (2024). Deep Learning of Dynamic Systems using System Identification Toolbox. *IFAC PapersOnLine*, no. 58 (15), pp. 580–585. DOI: 10.13140/RG.2.2.29127.47527

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

16. Ivakhnenko A. G., & Madala H. R. (1994). Inductive learning algorithms for complex systems modeling. London, Tokyo: CRC Press.

Дата першого надходження рукопису до видання: 24.09.2025
Дата прийнятого до друку рукопису після рецензування: 20.10.2025
Дата публікації: 28.11.2025