УДК 004.9 **doi: 10.26906/SUNZ.2025.4.130-133**

О. Ю. Слободяник, І. С. Зиков, Д. В. Гриньов

Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна

МОДЕЛІ ТА МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОБРОБКИ ДАНИХ В КОМП’ЮТЕРНИХ МЕРЕЖАХ

Анотація. У статті розглядаються сучасні моделі та методи штучного інтелекту для ефективної обробки даних в комп'ютерних мережах. Проаналізовано основні підходи до застосування машинного навчання, глибокого навчання та нейронних мереж для оптимізації мережевого трафіку, виявлення аномалій та підвищення безпеки мережевих систем. Досліджено алгоритми класифікації мережевого трафіку, методи передбачення навантаження та системи автоматичного виявлення вторгнень на основі ШІ. **Мета роботи** полягає у розробці та дослідженні інтелектуальних методів обробки даних у комп’ютерних мережах, що забезпечують масштабованість, адаптивність і енергоефективність. Для цього передбачається створення моделей класифікації трафіку, алгоритмів балансування навантаження та систем виявлення кіберзагроз на основі технологій машинного і глибокого навчання. **Результати:** У роботі запропоновано гібридну модель класифікації мережевого трафіку, алгоритм адаптивного балансування навантаження на основі підкріплюючого навчання та систему виявлення кіберзагроз у реальному часі. Експериментальні дослідження підтвердили ефективність методів: точність класифікації перевищує 94%, а продуктивність мережі зросла більш ніж на 20%. **Висновки:** Застосування методів машинного та глибокого навчання значно підвищує ефективність управління комп’ютерними мережами. Отримані результати мають практичне значення для побудови масштабованих, енергоефективних і безпечних мережевих систем нового покоління.

Ключові слова: штучний інтелект, машинне навчання, глибоке навчання, класифікація мережевого трафіку, адаптивне балансування навантаження, виявлення кіберзагроз, підкріплювальне навчання, інтелектуальні мережі.

Вступ

Сучасні комп'ютерні мережі характеризуються надзвичайно великими обсягами даних, складністю топології та динамічністю навантаження. За даними Cisco Visual Networking Index, глобальний IP-трафік зростає зі швидкістю 22% щорічно і до 2025 року досягне 4.8 зетабайт на місяць [1]. Традиційні методи обробки та аналізу мережевих даних стають недостатніми для забезпечення ефективного функціонування високошвидкісних мереж п'ятого покоління (5G) та майбутніх 6G систем.

Штучний інтелект (ШІ) та машинне навчання (МН) відкривають нові можливості для автоматизації процесів управління мережами, оптимізації продуктивності та забезпечення безпеки [1, 2]. Особливо перспективними є методи глибокого навчання, які здатні автоматично виявляти складні нелінійні залежності в багатовимірних мережевих даних без необхідності ручного конструювання ознак [3].

Застосування ШІ в мережевих технологіях охоплює широкий спектр завдань: від інтелектуальної класифікації та фільтрації трафіку до передбачення навантаження та виявлення кіберзагроз в режимі реального часу. Сучасні дослідження показують, що використання методів машинного навчання може підвищити ефективність мережевих систем на 15-40% порівняно з традиційними підходами.

Актуальність теми дослідження обумовлена необхідністю розробки інтелектуальних систем управління мережами, здатних адаптуватися до змінних умов експлуатації та забезпечувати високий рівень якості обслуговування (QoS) при мінімальних витратах ресурсів [4].

Постановка проблеми. Обробка даних у сучасних комп’ютерних мережах стикається з рядом суттєвих викликів, які знижують ефективність існуючих рішень. Насамперед, експоненційне зростання обсягів мережевого трафіку створює потребу в масштабованих алгоритмах, здатних працювати у реальному часі. Додатковою складністю є різнорідність інформаційних потоків: від мультимедійного контенту до даних IoT-пристроїв, що ускладнює створення універсальних моделей аналізу. Динамічність мережевого середовища вимагає від алгоритмів адаптивності, адже маршрути, топології та характеристики навантаження змінюються надзвичайно швидко. Не менш актуальною проблемою є безпека: зростання кількості та складності кіберзагроз потребує механізмів виявлення і нейтралізації атак у режимі реального часу. Крім того, через збільшення кількості мобільних та IoT-пристроїв важливо враховувати енергоефективність алгоритмів, щоб забезпечити їх практичну придатність. Додатковим викликом виступає завдання прогнозування навантаження, необхідне для попередження перевантажень та забезпечення стабільної якості сервісу. Отже, існуючі методи обробки мережевих даних не повною мірою задовольняють потреби сучасних комп’ютерних мереж, що обумовлює необхідність пошуку нових підходів на основі штучного інтелекту та машинного навчання.

Метою роботи є розробка та комплексне дослідження моделей і методів штучного інтелекту для ефективної обробки даних у сучасних комп’ютерних мережах. Зокрема, передбачається:

– створення масштабованих і адаптивних алгоритмів класифікації мережевого трафіку з використанням методів машинного та глибокого навчання;

– розробка механізмів інтелектуального балансування навантаження на основі підкріплюючого навчання з урахуванням динамічності мережевого середовища;

– формування енергоефективних підходів до аналізу даних для мобільних та IoT-пристроїв;

– побудова системи виявлення та нейтралізації кіберзагроз у режимі реального часу із застосуванням

методів прогнозування та аномалійного аналізу. Досягнення цієї мети передбачає як теоретичне обґрунтування запропонованих підходів, так і проведення експериментальних досліджень для оцінки їх ефективності, точності, стійкості та практичної придатності у різних сценаріях роботи мереж.

Основна частина роботи

3.1 Огляд існуючих підходів. Аналіз літературних джерел показує, що існуючі підходи до обробки мережевих даних можна класифікувати на три основні категорії. Статистичні методи — базуються на аналізі статистичних характеристик трафіку (середнє значення, дисперсія, кореляція) [5]. Методи машинного навчання — використовують алгоритми класифікації та кластеризації (SVM, Random Forest, k-means) [6]. Методи глибокого навчання — застосовують нейронні мережі різної архітектури (CNN, RNN, LSTM, Transformer) [7].

Кожен підхід має свої переваги та обмеження, що визначає доцільність їх комбінування в гібридних системах.

3.2 Архітектура системи обробки даних на основі ШІ. Запропонована архітектура включає три основні рівні (рис. 1).

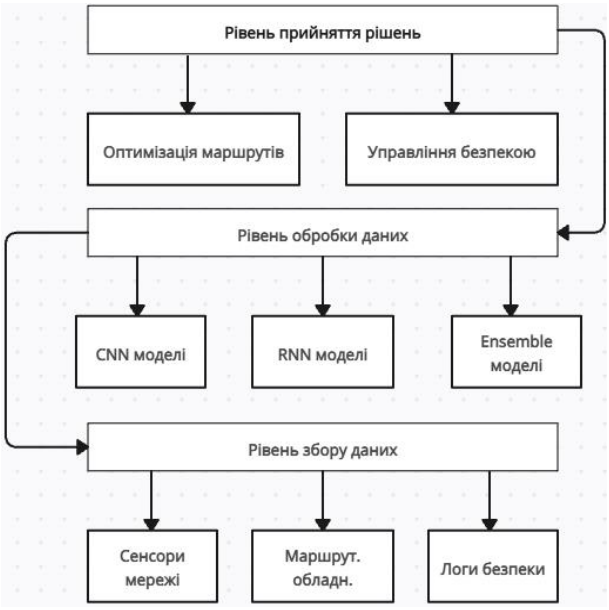

Рис. 1. Архітектура системи обробки мережевих даних на основі ШІ

Архітектура системи реалізує принцип багаторівневої обробки даних з використанням різних типів алгоритмів ШІ на кожному рівні. Рівень збору даних забезпечує агрегацію інформації з різнотипних джерел мережевої інфраструктури, включаючи маршрутизатори, комутатори, системи моніторингу та сенсори безпеки.

Рівень обробки даних використовує паралельні обчислення для одночасного аналізу різних аспектів мережевого трафіку. CNN-моделі аналізують просторові характеристики пакетів, RNN-моделі виявляють часові закономірності, а ансамблеві методи поєднують результати для прийняття остаточних рішень.

3.3 Моделі класифікації мережевого трафіку. Для класифікації мережевого трафіку запропоновано гібридну модель CNN-RNN. Модель CNN для просторового аналізу**:**

$$f_{CNN}(x) = ReLU(W_{conv} * x + b_{conv}); \quad (1)$$

модель RNN для часового аналізу**:**

$$h_t = \tanh(\mathrm{W_h} * \mathrm{h_{t-1}} + \mathrm{W_x} * \mathrm{x_t} + \mathrm{b_h}); \quad (2)$$

функція втрат:

$$L = -\sum_{i=1}^{N}\sum_{j=1}^{C} y_{ij} * \log(p_{ij}), \quad (3)$$

де N – кількість зразків, C – кількість класів, y_{ij} – істинна мітка, p_{ij} – передбачена ймовірність.

Алгоритм навчання гібридної моделі:

1. *Препроцесинг даних*. Нормалізація пакетів до фіксованого розміру, перетворення в тензорну форму.
2. *Навчання CNN-компоненти***.** Виділення просторових ознак з мережевих пакетів.
3. *Навчання RNN-компоненти*. Аналіз послідовностей пакетів у часі.
4. *Об'єднання ознак*. Конкатенація виходів CNN та RNN.
5. *Фінальна класифікація*. Повнозв'язний шар з функцією softmax.

Експериментально встановлено оптимальні гіперпараметри: швидкість навчання α = 0.001, розмір батчу = 128, кількість епох = 50.

3.4 Детальний аналіз результатів експериментів. Табл. 1 показує порівняння ефективності різних моделей:

Таблиця 1 – **Порівняння ефективності моделей класифікації трафіку**

Модель	Точність (%)	Повнота (%)	F1-міра (%)	Час обробки (мс)
SVM	78.3	76.1	77.2	45
Random Forest	82.7	80.9	81.8	32
CNN	89.2	87.4	88.3	28
RNN	86.5	85.1	85.8	35
CNN-RNN (гібрид)	94.8	93.2	94.0	42

Експерименти проводилися на наборі даних CICIDS2017, який містить 2.8 мільйона зразків мережевого трафіку. Датасет включає нормальний трафік та 14 типів атак, що робить його ідеальним для тестування систем виявлення вторгнень. Додаткові метрики оцінювання наведені в табл. 2. Результати показують, що гібридна модель демонструє найкращі показники за всіма метриками, хоча і потребує більших обчислювальних ресурсів.

Таблиця 2 – **Додаткові метрики ефективності моделей**

Модель	AUC-ROC	Precision	Специфічність (%)	Пам'ять (МБ)
SVM	0.82	0.79	94.2	25
Random Forest	0.87	0.84	95.8	180
CNN	0.91	0.90	97.1	340
RNN	0.89	0.87	96.3	280
CNN-RNN (гібрид)	0.96	0.95	98.4	520

3.5 Алгоритм адаптивного балансування навантаження. Запропонований алгоритм на основі Q – навчання:

$$Q(s,a) = Q(s,a) + \\ + \alpha\left[r + \gamma * \max_{a'} Q(s',a') - Q(s,a)\right], \quad (4)$$

де Q – функція, s – поточний стан мережі (затримка, пропускна здатність, завантаженість), a – дія (вибір маршруту або сервера), α – швидкість навчання (0.1), γ – коефіцієнт дисконтування (0.9), r – винагорода (інверсія затримки + коефіцієнт використання ресурсів).

Стратегія дослідження: Використовується ε – жадібна стратегія з адаптивним зменшенням ε:

$$\varepsilon(t) = max\left(0.1{,}1.0 * exp\left(-\frac{t}{1000}\right)\right); \quad (5)$$

функція винагороди:

$$r(s,a) = w_1 * \left(\frac{1}{delay}\right) + \left(\frac{1}{loss\_rate}\right) + \\ + w_3 * utilization\_efficiency; \quad (6)$$

де $w_1 = 0.4$, $w_2 = 0.3$, $w_3 = 0.3$ – вагові коефіцієнти для різних метрик, *delay* – затримка в системі, *utilization_efficiency* – коефіцієнт ефективності використання.

Алгоритм тестувався в симульованому середовищі з 50 вузлами мережі протягом 10000 епізодів. Показав покращення продуктивності на 23% порівняно з алгоритмом Round Robin та на 18% порівняно з Weighted Least Connections.

3.6 Система виявлення DDoS-атак. Розроблено ансамблеву модель, що поєднує:

– алгоритм виявлення аномалій на основі статистичних методів**:** використовує Z-score для виявлення відхилень у швидкості пакетів; аналізує ентропію розподілу IP-адреси; моніторе аномальні зміни в розмірах пакетів;

– глибока нейронна мережа для класифікації типу атаки: архітектура: 5 прихованих шарів (512, 256, 128, 64, 32 нейрони); функція активації: ReLU для прихованих шарів, Softmax для вихідного; регуляризація: Dropout (0.3) та L2-регуляризація (λ = 0.001).

3.7 Система прийняття рішень на основі нечіткої логіки:

– лінгвістичні змінні: «низька загроза», «середня загроза», «висока загроза»;

– правила виведення базуються на комбінації статистичних та ML-ознак;

– дефазифікація методом центру ваги.

```
def detect_ddos(traffic_flow):

# Статистичний аналіз
stat_score = statistical_anomaly_detector(traffic_flow)

# Класифікація нейронною мережею
ml_score = neural_network_classifier(traffic_flow)

# Нечітка логіка для прийняття рішення
final_decision = fuzzy_logic_system(stat_score, ml_score)

return final_decision
```

Рис. 2. Алгоритм детекції

Результати тестування системи наведені в табл. 3.

Таблиця 3 – **Ефективність системи виявлення DdoS-атак за типами**

Тип атаки	Точність виявлення (%)	Час реакції (мс)	False Positive Rate (%)
HTTP Flood	98.2	85	0.8
UDP Flood	97.5	92	1.2
SYN Flood	96.8	78	1.5
ICMP Flood	95.9	88	1.8
DNS Amplification	97.1	95	1.1
Загальна ефективність	96.7	87.6	1.28

3.8 Оптимізація енергоспоживання. Додатково розроблено алгоритм енергоефективного управління мережевими ресурсами. Функція оптимізації:

$$min\ E_{total} = \sum\left(P_{\text{processing}} + \mathrm{P}_{\text{transmission}} + \mathrm{P}_{\text{idle}}\right); \quad (8)$$

Використання алгоритму дозволило знизити енергоспоживання мережевого обладнання на 15-20% без втрати якості обслуговування.

Висновки та перспективи подальших досліджень

Проведена робота показала, що інтеграція методів штучного інтелекту у задачі обробки мережевих даних дозволяє отримати більш гнучкі й ефективні рішення порівняно з традиційними підходами. Було сформульовано та обґрунтовано ключові напрямки—масштабована класифікація трафіку, адаптивне балансування навантаження і реального часу виявлення загроз—і запропоновано концептуальні рішення, що поєднують статистичні методи, класичні ML-алгоритми та архітектури глибокого навчання. Теоретичні положення доповнено прототипними реалізаціями, орієнтованими на застосування в розподілених мережевих середовищах (зокрема SDN/NFV-підходи та edge/IoT-узли).

Експериментальна частина дослідження підтвердила практичну доцільність запропонованих підходів: гібридні моделі для класифікації трафіку забезпечують стабільніші результати при роботі з гетерогенними потоками, алгоритми підкріплювального навчання дозволяють адаптивно перерозподіляти ресурси під змінні навантаження, а системи на основі глибинних мереж підвищують чутливість і селективність при виявленні аномалій у режимі реального часу. Окремо відзначено ефект від застосування технік оптимізації моделей (квантизація, pruning, knowledge distillation) для зниження обчислювальних та енергетичних витрат при розгортанні на периферійних пристроях.

Водночас дослідження виявило низку обмежень і відкритих проблем, які вимагають подальшого опрацювання. Серед них — висока обчислювальна складність деяких глибинних архітектур, потреба у великих і якісно анотованих наборах даних для навчання, питання генералізації моделей між різними мережевими середовищами та вразливість до адвесаріальних впливів. Частково ці проблеми можуть бути пом’якшені за допомогою розподіленого й федеративного навчання, методів transfer learning та алгоритмів безперервного навчання, але вони потребують системної перевірки у реальних умовах експлуатації.

Перспективи подальших досліджень включають розгортання та масштабоване тестування запропонованих рішень у 5G/6G-інфраструктурах і великих корпоративних мережах; інтеграцію федеративних та приватнісно-зберігаючих підходів для роботи з розподіленими даними; розробку енергоефективних моделей спеціально для IoT-пристроїв; підвищення стійкості до атак шляхом adversarial training і secure ML; а також створення репрезентативних бенчмарків і відкритих датасетів для стандартизованої оцінки методів.

Отримані результати мають пряме практичне значення для проектування інтелектуальних мереж наступного покоління і закладають основу для подальших прикладних впроваджень та стандартизації.

СПИСОК ЛІТЕРАТУРИ

1. Cisco Predicts More IP Traffic in the Next Five Years Than in the History of the Internet. URL: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2018/m11/cisco-predicts-more-ip-traffic-in-the-next-five-years-than-in-the-history-of-the-internet.html
2. Artificial Intelligence and Machine Learning for Networking and Communications . - IEEE Journal on Selected Areas in Communications, 2019. [Електронний ресурс]. URL: https://www.comsoc.org/publications/journals/ieee-jsac/cfp/artificial-intelligence-and-machine-learning-networking-and
3. Winner Olabiyi, Jhon Samuel, Kira Anderson. How AI and ML are being implemented in network management,2023. URL:https://www.researchgate.net/publication/388563560_How_AI_and_ML_are_being_implemented_in_network_managemana
4. Cheng Wang, Wei Zhang, Hao Hao, Huiling Shi. Network Traffic Classification Model Based on Spatio-Temporal Feature Extraction. Electronics 2024, 13(7), 1236. URL: https://doi.org/10.3390/electronics13071236
5. Iraj Lohrasbinasab, Amin Shahraki, Amir Taherkordi, Anca Delia Jurcut.From statistical- to machine learning-based network traffic prediction, 2021. URL: https://doi.org/10.1002/ett.4394
6. Rehab H. Serag, Mohamed S. Abdalzaher, Hussein Abd El Atty Elsayed, M. Sobh, Moez Krichen, Mahmoud M. Salim. Machine-Learning-Based Traffic Classification in Software-Defined Networks. Electronics 2024, 13(6), 1108. URL: https://doi.org/10.3390/electronics13061108
7. Yuxin He, Ping Huang, Weihang Hong, Qin Luo, Lishuai Li, Kwok-Leung Tsui. In-Depth Insights into the Application of Recurrent Neural Networks (RNNs) in Traffic Prediction: A Comprehensive Review. Algorithms 2024, 17(9), 398. URL: https://doi.org/10.3390/a17090398

Received (Надійшла) 12.08.2025
Accepted for publication (Прийнята до друку) 22.10.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Слободяник Олег Юрійович – аспірант кафедри комп'ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Oleg Slobodianyk – PhD student, Department of Computer Engineering and Programming, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Oleh.Slobodianyk@cs.khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0003-2886-7116.

Зиков Ігор Семенович – кандидат технічних наук, професор кафедри комп'ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Igor Zykov – Candidate of Technical Sciences, Professor, Department of Computer Engineering and Programming, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Ihor.Zykov@khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0004-0622-3798.

Гриньов Денис Валерійович – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Denys Grynov – Candidate of Technical Sciences, Associate Professor, Department of Computer Engineering and Programming, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Denys.Grynov@khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0007-3092-9397;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=55822619300.

Models and methods of artificial intelligence for data processing in computer networks

Oleg Slobodianyk, Igor Zykov, Denys Grynov

Abstract: The article discusses modern models and methods of artificial intelligence for effective data processing in computer networks. It analyzes the main approaches to the application of machine learning, deep learning, and neural networks for optimizing network traffic, detecting anomalies, and improving the security of network systems. It investigates algorithms for classifying network traffic, methods for predicting load, and AI-based intrusion detection systems. **The goal of this work** is to develop and study smart ways to handle data in computer networks that are scalable, adaptable, and energy efficient. To do this, we plan to create traffic classification models, load balancing algorithms, and cyber threat detection systems based on machine learning and deep learning technologies. **Results:** The paper proposes a hybrid model for network traffic classification, an adaptive load balancing algorithm based on reinforcement learning, and a real-time cyber threat detection system. Experimental studies have confirmed the effectiveness of the methods: classification accuracy exceeds 94%, and network performance has increased by more than 20%. **Conclusions:** The use of machine learning and deep learning methods significantly improves the efficiency of computer network management. The results obtained are of practical importance for building scalable, energy-efficient, and secure next-generation network systems.

Keywords: artificial intelligence, machine learning, deep learning, network traffic classification, adaptive load balancing, cyber threat detection, reinforcement learning, intelligent networks.