

УДК 004.7

## **АНАЛІЗ СУЧАСНИХ МЕТОДІВ ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ**

**Моїсєєнко Р.С.**

*Харківський національний автомобільно-дорожній університет, Харків*

У сучасному світі комп'ютерні мережі є основою функціонування більшості організацій та інфраструктур. Від бізнесу та банківських систем до освітніх та наукових установ – всі покладаються на ефективну і стабільну роботу мереж для передачі даних. З розвитком технологій та зростанням кількості підключених пристроїв, вимоги до мережевої інфраструктури постійно зростають. Це породжує нові виклики у сфері проектування мереж, які стають дедалі складнішими.

З іншого боку, розвиток штучного інтелекту (ШІ) та машинного навчання (ML) приніс революційні зміни у багатьох галузях, включаючи ІТ та телекомунікації. ШІ дозволяє автоматизувати процеси, які раніше вимагали значних людських ресурсів, що робить його надзвичайно ефективним інструментом у проектуванні комп'ютерних мереж. Використання штучного інтелекту може забезпечити створення мереж, що адаптуються до змін, автоматично вирішують проблеми та забезпечують високу продуктивність навіть в умовах інтенсивного трафіку та великої кількості користувачів.

Автоматизоване планування мереж за допомогою штучного інтелекту дозволяє значно скоротити час та людські ресурси, необхідні для розробки мережевої топології. ШІ-системи використовують алгоритми машинного навчання для автоматизації процесів вибору маршрутизації, розподілу ресурсів та створення надійної мережевої інфраструктури. Одним з найяскравіших прикладів таких технологій є система Google B4, яка використовує ШІ для оптимізації глобальної мережі компанії, дозволяючи

ефективно керувати потоками трафіку на глобальному рівні. Такий підхід знижує ризики людських помилок та підвищує стійкість до збоїв, що особливо важливо для великих компаній і організацій [1].

Інтелектуальні алгоритми маршрутизації є важливою складовою оптимізації трафіку в комп'ютерних мережах. Використовуючи ШІ, мережі можуть самостійно аналізувати поточний стан трафіку, знаходити можливі вузькі місця та автоматично визначати найоптимальніші маршрути для передачі даних. Це особливо важливо в умовах великого навантаження на мережу, коли затримки можуть мати критичний вплив на продуктивність систем. Інтелектуальні алгоритми, такі як reinforcement learning (навчання з підкріпленням), дозволяють мережам самонавчатися і постійно покращувати свої рішення щодо маршрутизації [2].

Штучний інтелект грає важливу роль у забезпеченні безпеки комп'ютерних мереж. Використовуючи алгоритми машинного навчання, системи кібербезпеки здатні аналізувати величезні обсяги мережевого трафіку та виявляти аномалії, які можуть свідчити про потенційні загрози, такі як хакерські атаки або витік даних. Однією з ключових переваг використання ШІ в цьому контексті є його здатність виявляти нові, ще невідомі загрози, з якими традиційні методи не можуть впоратися. Наприклад, система може навчатися на основі минулих атак і прогнозувати майбутні загрози, що дозволяє оперативно реагувати на кіберінциденти [3].

Один з найперспективніших напрямів використання ШІ в проектуванні комп'ютерних мереж – це самонавчальні системи. Використовуючи дані про минулу роботу мережі, такі системи здатні автоматично налаштовувати свої параметри для покращення продуктивності та адаптації до змін у навантаженні. Наприклад, система може динамічно змінювати пропускну здатність окремих каналів або розподіляти ресурси між різними мережевими сегментами залежно від потреб у реальному часі. Це дозволяє мережам функціонувати більш ефективно та зменшує потребу у постійному ручному втручанні інженерів [4].

Хоча використання штучного інтелекту має величезний потенціал у сфері проектування комп'ютерних мереж, його впровадження не є безпроблемним. Одна з основних труднощів полягає в необхідності великих обсягів даних для навчання моделей ШІ. Комп'ютерні мережі мають складну структуру, і для створення ефективних алгоритмів ШІ потрібні детальні й точні дані про роботу мережі, що не завжди може бути доступним або легко збирається [5].

Крім того, процес навчання моделей ШІ є складним і тривалим. Висока точність таких моделей вимагає тривалого періоду тренування та тестування, щоб зменшити ймовірність помилок. Це може вимагати значних ресурсів, включаючи потужне обладнання та високооплачуваних фахівців, що є значною перешкодою для невеликих компаній [6].

Ще одним викликом є питання етики та конфіденційності. Використання великих обсягів даних для навчання ШІ може призводити до ризиків витоку інформації або неправильного використання даних. Керування цими аспектами вимагає належної регуляції та контролю за використанням технологій штучного інтелекту в критично важливих мережах [6-8].

Незважаючи на труднощі, перспективи використання штучного інтелекту в мережевих технологіях вражають. По мірі розвитку технологій, таких як Інтернет речей (IoT) та 5G, потреба в автоматизації процесів мережевого управління буде тільки зростати. ШІ дозволяє створювати самонавчальні мережі, які зможуть реагувати на зміни у режимі реального часу, що є критично важливим для інфраструктур з великим навантаженням.

Перспективи також лежать у розширенні масштабованості мережевих рішень за допомогою ШІ. Величезна кількість підключених пристроїв у майбутньому, зокрема з розвитком IoT, вимагатиме від мереж більшої гнучкості та адаптивності, що ШІ здатен забезпечити [7].

Штучний інтелект відкриває нові горизонти у сфері проектування комп'ютерних мереж. Застосування ШІ дозволяє створювати автоматизовані та самонавчальні системи, які можуть адаптуватися до нових умов,

оптимізувати трафік, забезпечувати високий рівень безпеки та знижувати людські помилки. Проте для того, щоб повністю реалізувати потенціал ШІ, необхідно вирішити низку технічних, етичних та регуляторних викликів.

### **Список літератури**

1. Bai, X., Wang, W., & Chen, J. (2020). *Artificial Intelligence in Network Design and Management: A Review*. IEEE Communications Surveys & Tutorials, 22(4), 2864-2895.
2. Krause, F., and Holtkamp, A. (2021). *AI-Driven Network Optimization for Large-Scale Infrastructures*. Journal of Network and Systems Management, 29(2), 547-562.
3. Li, X., & Shen, Z. (2019). *Machine Learning in Cybersecurity: Detecting and Preventing Threats in Network Systems*. ACM Computing Surveys, 51(5), 89-116.
4. Srinivasan, K., & Patel, M. (2020). *Self-Learning Networks: A New Frontier in AI and Networking Technologies*. International Journal of Advanced Computer Science and Applications, 11(3), 112-124.
5. Tang, T., & Lee, S. (2022). *AI and Quantum Computing for Next-Generation Network Design*. IEEE Transactions on Network and Service Management, 19(1), 203-221.
6. Kumar, P., & Ray, P. (2019). *AI-Enhanced Network Design: Towards Efficient and Scalable Solutions for IoT Infrastructures*. Sensors, 19(16), 3453.
7. Gupta, A., & Saxena, N. (2020). *Security and Privacy Challenges in AI-Driven Networks: A Survey*. IEEE Internet of Things Journal, 7(4), 3244-3258.
8. Кононихін О.С., Прачик В.А., Щепетільников С.Ю. Модель вибору мережевого обладнання логістичного підприємства в умовах інтервальної інформації // «Наука і техніка сьогодні» (Серія «Техніка»): журнал. 2024. № 1(29) 2024. С. 718-726