ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ МОДЕЛІ «TRANSFORMER» ДЛЯ ВИЯВЛЕННЯ ВТРУЧАННЯ В КОМП'ЮТЕРНІ МРЕЖІ

Гавриленко С. Ю., Полторацький В. О.
Національний технічний університет "ХПІ", Харків, Україна

Системи виявлення вторгнень в комп'ютерні мережі базуються на використанні методів машинного навчання (МН). Одним із найбільш популярним напрямком МН є методи глибокого навчання.

Моделі глибокого навчання володіють властивістю автоматичного вивчення внутрішньої репрезентації ознак з наданих даних, надаючи їм значущий підхід для розв'язання завдань, які вимагають складних аналізів. В сфері глибокого навчання найсучаснішою архітектурою є Трансформер (Transformer). Трансформер – модель нейронної мережі яка спеціалізується на процесі глибокого навчання з використанням механізму «уваги» до кожного елементу в отриманому наборі вхідних даних. Ця архітектура стала революційним кроком у сфері обробки природної мови (Natural Language Processing, NLP) і застосовується у різних завданнях, таких як машинний переклад, аналіз тональності тексту, генерація тексту та багато інших.

У рамках проведених досліджень були побудовані моделі виявлення вторгнень в комп'ютерні мережі які базуються на методах Vision Transformer (ViT) та Vision Transformer For Small-size Datasets (ViTSD). Запропоновано процедуру перетворення табличних вихідних даних у спеціальний формат зображень, необхідний для роботи моделей.

З метою порівняння ефективності, ті ж дані були також піддані класифікації за допомогою інших алгоритмів, зокрема: Support Vector Machines та K-nearest neighbors. Це дозволило оцінити та порівняти результати різних методів та підходів у задачі класифікації з використанням нейронних мереж та традиційних алгоритмів машинного навчання.

Дослідження показали, що завдяки застосуванню архітектури Трансформер суттєво зросла точність класифікації. Зокрема, показник точності (accuracy) для класифікатора SVM досяг 0,910, у KNN — 0,933, ViT – 0,973 тоді як ViTSD показав найвищу точність 0,987.

Список літератури

1. Ahmad, Zeeshan & Shahid Khan, Adnan & Shiang, Cheah & Ahmad, Farhan. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 32. 10.1002/ett.4150.

2. Vaswani, Ashish & Shazeer, Noam & Parmar, Niki & Uszkoreit, Jakob & Jones, Llion & Gomez, Aidan & Kaiser, Lukasz & Polosukhin, Illia, "Attention is all you need", 2017. NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems.

3. Lee, Seung & Lee, Seunghyun & Song, Byung. "Vision Transformer for Small-Size Datasets". arXiv:2112.13492v1 [cs.CV] 27 Dec 2021