АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

Заковоротний О.Ю., Хулап А.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Особливості безпеки інтернету речей та обмеження традиційних методів визначають нагальну потребу в нових технологіях безпеки. Штучний інтелект як новий технологічний напрямок має широку сферу застосування. Машинне навчання може компенсувати недоліки традиційних рішень безпеки в різних аспектах, відповідає характеристикам інтернету речей і надає нові можливості для нього, щоб відповідати новим вимогам безпеки:

- Можливість розпізнавання образів і розрізнення аномальної поведінки.
- Можливість автономного захисту, навчання та вдосконалення.
- Можливість ефективної обробки великих обсягів складних даних.

Згідно з дослідженням [1] є чотири загрози, які необхідно терміново вирішити в безпеці Інтернету речей: автентифікація пристрою, DoS/DDoS-атака, виявлення вторгнень і виявлення шкідливих програм. Традиційним рішенням цих проблем не вистачає здатності обробляти великі набори даних і виникає багато проблем, таких як низька ефективність і низька продуктивність у реальному часі. Більшість із них не можна перенести на інтернет речей. Методи штучного інтелекту, представлені машинним навчанням, можуть використовувати великі обсяги даних інтернету речей для отримання корисної інформації із даних і, таким чином, прогнозувати невідомі події, надаючи нові рішення для цих проблем [2, 3].

Таким чином, для розв'язання усіх цих проблем можуть бути використані нейромережі, навіть нейромережі прямого поширення без зворотних зв'язків. Проблема зводиться до розпізнавання образів та виявлення аномальної поведінки: виявлення нетипового користувача, нетипових дій, нетипових підключень тощо. Але для IoT постає питання обмежених ресурсів (обсяги пам'яті, використання обчислень з плаваючою комою, продуктивність). Це створює наступні проблеми навчання нейромереж, можливості обчислень у реальному часі та інше. Проблема оптимізації виконання нейромереж для виконання у інтернеті речей може бути темою для подальших досліджень.

Література:

1. Abdullahi M., Baashar Y., Alhussian H., Alwadain A., Aziz N., Capretz L.F., Abdulkadir S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. MDPI, 2022. DOI: 10.3390/electronics11020198. URL: https://www.mdpi.com/2079-9292/11/2/198/htm (дата звернення 01.05.2024).

2. Заковоротний О.Ю., Орлова Т.О. Порівняльний аналіз хмарних та туманних середовищ Інтернету речей. Системи управління, навігації та зв'язку, 2023, випуск 2(72). С. 152-154. DOI: 10.26906/SUNZ. 2023.3.152

3. Kuzlu M., Fair C., Guler O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Springler, 2021. DOI: 10.1007/s43926-020-00001-4. URL: https://link.springer.com/article/10.1007/s43926-020-00001-4 (дата звернення 01.05.2024).