УДК **004.056: 004.7**

МЕТОД ВИЯВЛЕННЯ АНОМАЛЬНОЇ МЕРЕЖЕВОЇ ПОВЕДІНКИ IoT-ПРИСТРОЇВ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Верясов О.А.
e-mail: oleksii.veriasov.cpe@nure.ua
Науковий керівник – к.т.н., доц. Кириченко І.В.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна

The growth of IoT devices has increased network attack surfaces and exposed the limitations of signature-based intrusion detection systems. This study explores machine learning methods for anomaly detection in IoT traffic using behavioural network features extracted from benign and malicious datasets. The findings show that models such as Isolation Forest effectively detect abnormal activity and are suitable for real-time monitoring applications.

Стрімкий розвиток технологій Інтернету речей (IoT) призводить до значного збільшення кількості підключених до мережі пристроїв. За оцінками аналітичних агентств, кількість IoT-пристроїв у світі щороку зростає, що призводить до розширення потенційної поверхні атак у комп'ютерних мережах. Багато IoT-пристроїв мають обмежені обчислювальні ресурси, використовують спрощені механізми автентифікації та часто не отримують регулярних оновлень безпеки. Це робить їх вразливими до різних типів кіберзагроз, зокрема ботнет-атак, DDoS-атак, сканування портів та несанкціонованого доступу [1].

Традиційні системи виявлення вторгнень здебільшого використовують сигнатурні методи аналізу мережевого трафіку. Основним недоліком такого підходу є неможливість виявлення нових або модифікованих атак, для яких відсутні відповідні сигнатури. У зв'язку з цим актуальним напрямом досліджень є використання методів машинного навчання для аналізу поведінки мережевого трафіку та виявлення аномалій [2].

Метою роботи є аналіз та оцінка ефективності застосування методів машинного навчання для виявлення аномальної мережевої поведінки IoT-пристроїв. У межах аналізу було розглянуто особливості мережевого трафіку IoT-систем та проведено аналіз відкритих датасетів мережевої активності.

Перед застосуванням алгоритмів машинного навчання було виконано попередню обробку даних, яка включала очищення даних, нормалізацію значень ознак та формування набору поведінкових характеристик мережевого трафіку. Для аналізу мережевої поведінки IoT-пристроїв використовуються характеристики трафіку такі, як тривалість з'єднання, кількість переданих байтів, кількість пакетів, інтенсивність мережевої активності. Нехай вектор ознак мережевого з'єднання визначається

як $X=(x_1, x_2, \dots, x_n)$, де x_1– окрема характеристика мережевого трафіку. Для оцінювання поведінки пристрою може бути використана регресійна модель $y=\beta_0+\beta_1 \cdot x_1+\beta_2 \cdot x_2+ \dots +\beta_n \cdot x_n+\varepsilon$, де y – прогнозована характеристика мережевої активності, β_i – коефіцієнти моделі, ε – випадкова похибка. Отримана модель дозволяє оцінювати нормальну поведінку мережевого трафіку та визначати відхилення від очікуваних значень. Значні відхилення можуть свідчити про аномальну активність або потенційну атаку.

Окрім регресійного аналізу, для виявлення аномалій були розглянуті алгоритми машинного навчання, що використовуються для задач детекції нетипової поведінки. До таких алгоритмів належать Isolation Forest, One-Class SVM та автоенкодери [3]. Дані алгоритми дозволяють виявляти аномальні мережеві з'єднання без необхідності попереднього маркування всіх типів атак.

Застосування методів машинного навчання дозволяє формувати поведінкові моделі роботи IoT-пристроїв і автоматично визначати відхилення від нормальної активності.

Такий підхід є більш адаптивним у порівнянні з класичними сигнатурними методами, оскільки він здатний виявляти нові типи атак та нетипову поведінку мережевих пристроїв [2], і може бути використаний для побудови систем моніторингу мережевої безпеки, що працюють у режимі реального часу та забезпечують підвищений рівень захисту IoT-інфраструктури.

Подальші дослідження можуть бути спрямовані на застосування глибоких нейронних мереж для аналізу часових характеристик мережевого трафіку та інтеграцію у системи моніторингу безпеки IoT-мереж.

Список використаних джерел:

1. Sicari S., Rizzardi A., Griego L. A. Coen-Porisini A. Security, privacy and trust in Internet of Things Computer Networks 2015 DOI: 10.1016/j.comnet.2014.11.008.

2. Buczak A.L.,Guven E. A survey of data mining and machine learning methods for cyber security instrusion detection. IEEE Communications Surveys 2016. DOI: 10.1109/COMST.2015.2494502.

3. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys 2009. 74 pages, URL: http://dl/acm.org/doi/epdf/10.1145/1541882 (дата звернення: 12.02.2026).

4. Liu F. T., Ting K.M., Zhou Z.-H. Isolation forest. IEEE ICDM. 2008 DOI: 10.1109/ICDM.2008.17.