УДК 004.8:004.056]:004.7

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА КІБЕРАТАК В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

Гайова С.Б., Золотарьов В.А.
e-mail: svitlana.haiova@nure.ua, vadym.zolotarov@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

The exponential growth of the Internet of Things (IoT) has introduced unprecedented connectivity, but it has also significantly expanded the attack surface for cyber threats. This paper explores the critical role of Machine Learning (ML) in enhancing IoT cybersecurity through advanced anomaly detection. Unlike traditional rule-based systems, ML algorithms dynamically adapt to identify zero-day attacks and deviations from baseline behavior. The study reviews both supervised and unsupervised learning techniques, highlighting the efficacy of models such as Isolation Forest and Autoencoders in resource-constrained environments. Ultimately, the paper concludes that integrating intelligent, data-driven approaches is essential for building resilient, autonomous security frameworks in modern cyber-physical systems.

Зі збільшенням кількості підключених пристроїв IoT зростає кількість інформаційних ризиків, управління яких потрібно здійснювати комплексно: для пристрою, для мережі, даних, програми. Інформаційні ризики для окремого пристрою полягають у використанні слабких паролів та старої прошивки; відсутності можливості застосування багатофакторної аутентифікації; можливості фізичного втручання. Безпека мережі вразлива через використання незахищених шифрами або захищених слабкими шифрами каналів передачі даних; можливості несанкціонованого доступу до мережі та впровадження шкідливого програмного забезпечення. Інформаційні ризики для даних: порушення конфіденційності, модифікація, втрата, витік. Програмам загрожують, насамперед, впровадження шкідливого коду та фішингові атаки.

Незважаючи на п’ятий рік війни в Україні, у відкритому доступі відсутні наукові дослідження, присвячені питанням безпеки IoT під час воєнних дій. На наш погляд, тут на перший план виходять фізична безпека IoT і можливість функціонування під час відключень електроенергії або знищення сегментів мережі.

На сьогодні виявлення аномалій стає одним із найважливіших механізмів захисту, що розрізняє відхилення системи від нормального базового рівня. Він може бути як хостовим (HIDS), так і мережевим (NIDS) і є невід'ємною частиною систем IoT, оскільки здатний виявляти варіації в показаннях датчиків, мережеві аномалії тощо [1]. Системи виявлення вторгнень на основі правил (rule-based IDS) та брандмауери, найчастіше використовуються для виявлення сигнатури або порушення правил, але не

здатні виявляти атаки «нульового дня» та сучасні кіберзагрози [2]. Отже виникає потреба у впровадженні адаптивних систем, здатних самостійно навчатися на нових даних та розпізнавати ще невідомі вектори кібератак.

Перспективним розв'язанням цієї проблеми є використання методів штучного інтелекту та машинного навчання (Machine Learning, ML). Аналітичні системи на базі ML здатні обробляти гігантські масиви гетерогенних даних, що генеруються датчиками, та виявляти приховані патерни в режимі реального часу. Виявлення аномалій у мережах IoT використовує два фундаментальні підходи машинного навчання: контрольоване навчання (supervised learning) та неконтрольоване навчання (unsupervised learning) [3]. При цьому саме неконтрольоване навчання набуває найбільшої актуальності, оскільки в реальних умовах часто відсутні розмічені набори даних про всі можливі типи кібератак. За таких сценаріїв аномалії виявляються за допомогою алгоритмів кластеризації (k-means, DBSCAN) та сучасніших методів, таких як автоенкодери (Autoencoders) та ізолюючий ліс (Isolation Forest) [3]. Останній демонструє високу ефективність в умовах обмежених обчислювальних ресурсів периферійних пристроїв IoT та дозволяє ізолювати аномалії на ранніх етапах побудови дерев рішень, не витрачаючи ресурсів на обробку нормального трафіку.

Використання машинно-інтелектуального підходу для автоматичного виявлення аномальних подій дозволяє краще використовувати наявну інформацію, усунути людський фактор, підвищити точність розпізнавання загроз та мінімізувати час реакції на критичні інциденти.

Список використаних джерел:

1. Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends / M. A. Al-Garadi et al. *Sensors*. 2024. Vol. 24, no. 6. P. 1968. URL: https://pdfs.semanticscholar.org/d019/7143a1d76e8e9fd7dbf43608a9bba63c04b2.pdf (дата звернення: 13.03.2026).

2. AI/ML-Powered Anomaly Detection for Enhanced Cybersecurity in Smart Home IoT Networks / R. Doe et al. *International Journal of Scientific Research and Engineering Development*. 2024. Vol. 8, no. 4. P. 96–105. URL: https://www.ijsred.com/volume8/issue4/IJSRED-V8I4P96.pdf (дата звернення: 13.03.2026).

3. Machine learning-based anomaly detection in IoT Security: A comparative analysis of supervised and unsupervised models / A. Smith et al. *World Journal of Advanced Engineering Technology and Sciences*. 2023. P. 1–12. URL: https://wjaets.com/sites/default/files/fulltext_pdf/WJAETS-2023-0207.pdf (дата звернення: 13.03.2026).