БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ НА ОСНОВІ МОДЕЛЕЙ ВИЯВЛЕННЯ АНОМАЛІЙ

Федюшин О.І., Кавецький М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З кожним днем, комп'ютерні системи та мережі стають все більш важливими для нашого повсякденного життя. Вони забезпечують доступ до інформації, зручність та швидкість взаємодії з іншими людьми та системами. Але разом зі зростанням їх важливості, збільшується також ризик їхнього некоректного функціонування та зловмисного втручання. Тому безпека комп'ютерних систем є дуже важливою.

Одним з підходів до розв'язання цієї проблеми є використання методів машинного навчання на основі виявлення аномалій.

Завдяки цим технологіям, можна виявити відхилення в поведінці комп'ютерної системи або мережі та вчасно вжити необхідні заходи для захисту від потенційних загроз.

Для виявлення загроз комп'ютерним мережам використовують багато методів машинного навчання з вчителем та без нього. Аналіз відповідних робіт показав, що зараз фокус досліджень змістився в бік використання глибоких нейронних мереж для виявлення аномалій [1, 2].

Традиційні методи машинного навчання, як правило, неефективні при обробці великомасштабних даних і нерівномірно розподілених вибірок. Моделі глибокого навчання більш продуктивні при аналізі таких даних.

Отже, оскільки обраним напрямом є моделі глибокого навчання для побудови таких систем потрібно мати багато даних, але це цілком виправдано, бо модель зможе мати більший простір для тренування, що якісно вплине на її точність виявлення аномалій.

Метою доповіді є ознайомлення з потенційними методами забезпечення функціонування комп'ютерних систем та мереж на основі побудови моделі штучного інтелекту для виявлення аномалій.

Результати досліджень показали, що ефективним способом для вирішення завдання є використання моделей глибокого навчання, які приймають дані наперед записаної активності мережі та будують модель, яка найкращим чином може узагальнити всі процеси у комп'ютерній системі та класифікувати активність як нормальну чи шкідливу.

Список літератури

1. Tushkanova, O.; Levshun, D.; Branitskiy, A.; Fedorchenko, E.; Novikova, E.; Kotenko, I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. *Algorithms* 2023, *16*, 85. https://doi.org/10.3390/a16020085

2. Lee, K.-M.; Cho, M.-Y.; Kim, J.-G.; Lee, K.-H. Anomaly Detection Method for Unknown Protocols in a Power Plant ICS Network with Decision Tree. *Appl. Sci.* 2023, *13*, 4203. https://doi.org/10.3390/app13074203