ЗАСТОСУВАННЯ ГЛИБИННОГО НАВЧАННЯ У ВИЯВЛЕННІ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ

Зінченко Є.Ю., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні мережі передають великий обсяг даних і мають високу швидкість обміну та високу комунікаційну складність, що робить виявлення кіберзагроз і несанкціонованих дій складним. Традиційні методи аналізу мережевого трафіку, що засновані на сигнатурному виявленні, не забезпечують достатнього захисту від нових або невідомих типів загроз. Це означає, що для виявлення загроз в сучасних інформаційних мережах необхідно використовувати інтелектуальні методи обробки даних, і глибоке навчання має важливе значення [1].

Метою роботи є вивчення можливостей використання методів глибинного навчання для виявлення аномалій у трафіку мережі, порівняння ефективності різних архітектур нейронних мереж (CNN, RNN і автоенкодерів) і визначення перспективи їх інтеграції у сучасні системи інформаційної безпеки. Багатошарові нейронні мережі є основою глибокого навчання, підмножини машинного навчання. Ці мережі можуть автоматично визначати важливі ознаки в даних і виявити приховані закономірності. Автоенкодери, згорткові (CNN), рекурентні (RNN) та LSTM-архітектури дозволяють ефективно аналізувати неструктуровані потоки мережевого трафіку та класифікувати відхилення, які можуть свідчити про атаки чи аномалії [2, 3]. У дослідженні використовувалися набори даних CICIDS2017 і UNSW-NB15, які містять приклади нормального та шкідливого трафіку. Результати експерименту показали, що моделі глибинного навчання перевершують традиційні методи машинного навчання щодо швидкості та точності виявлення аномалій. Результати підтверджують, що впровадження глибинних моделей у системи SIEM та UEBA є доцільним для підвищення ефективності моніторингу та управління інцидентом інформаційної безпеки в умовах зростаючих обсягів даних, швидкісних характеристик мереж та кіберзагроз [2, 3]. Таким чином, використання глибинного навчання в системах виявлення аномалій підвищує точність, адаптивність і надійність захисту інформаційних мереж, що робить цей напрям одним із ключових у розвитку інтелектуальних систем кібербезпеки.

Список літератури

1. Chawla, S., Chalapathy, R. *Deep Learning for Anomaly Detection: A Survey*. arXiv preprint, 2019. Посилання: https://arxiv.org/abs/1901.03407?

2. The UNSW-NB15 Dataset, The University of New South Wales. Посилання: https://research.unsw.edu.au/projects/unsw-nb15-dataset

3. Moustafa N., Slay J. *UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems*. – MilCIS Conference, 2015. Посилання: https://researchdata.edu.au/the-unsw-nb15-dataset/1957529?