УДК 004.77
В. Мазур
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ЗАХИСТУ ВІД КІБЕРАТАК НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

UDC 004.77
V. Mazur

AI-BASED METHODS FOR PROTECTION AGAINST CYBERATTACKS

У сучасному цифровому середовищі інформаційна безпека стає все більш важливою через стрімке зростання кількості та складності кіберзагроз. Особливою проблемою є атаки на основі штучного інтелекту (ШІ), які використовують потужні алгоритми машинного навчання, нейронні мережі та інші передові технології для обходу традиційних захисних систем. Ці атаки стають більш витонченими та адаптивними, що ускладнює завдання захисту інформаційних систем [1].

У результаті проведеного дослідження було здійснено глибокий аналіз сучасних методів атак на основі ШІ, таких як генеративні змагальні мережі (GANs), машинне навчання для DDoS-атак та нейронні мережі для обходу CAPTCHA [2]. Було встановлено, що ці інструменти дозволяють зловмисникам створювати реалістичні моделі атак, які можуть обходити традиційні системи захисту, що підвищує загрозу для критичної інфраструктури, корпоративних систем та персональних даних.

Для протидії таким атакам були розроблені ефективні методи захисту, що включають використання систем машинного навчання та глибокого навчання для виявлення аномалій у мережевому трафіку та поведінці користувачів [3]. Зокрема, було запропоновано застосування алгоритмів Random Forest та Support Vector Machines (SVM) для класифікації та виявлення DDoS-атак, а також впровадження генеративних моделей для розпізнавання підроблених фішингових листів та обходу CAPTCHA [4].

Експериментальні дослідження показали, що запропоновані методи забезпечують високу точність виявлення загроз, швидку адаптацію до нових типів атак та зниження кількості хибних спрацьовувань. Наприклад, інтеграція моделей машинного навчання дозволила зменшити ризик простою серверів на 95% та скоротити час реакції на атаки до 30 секунд [5].

Отримані результати дозволили створити гнучкі та ефективні системи захисту, здатні оперативно реагувати на еволюцію кіберзагроз на основі ШІ. Це підвищило загальний рівень безпеки інформаційних систем, забезпечуючи надійний захист від сучасних та майбутніх атак [6]. Таким чином, дослідження продемонструвало важливість використання штучного інтелекту для вдосконалення кіберзахисту та надання ефективних рішень у боротьбі з новими формами кіберзагроз.

Література

1. Аленічев, І.В. Штучний інтелект у кібербезпеці: сучасні підходи, 2015.
2. Бабенко, О.В. Методи захисту інформаційних систем на основі машинного навчання, 2021.
3. Барановський, П.О. Захист від DDoS-атак у мережах на основі штучного інтелекту, 2020.
4. Kim, J., Kim, H., & Kim, J. Deep Neural Networks for Cybersecurity, 2020.
5. Kshetri, N. Artificial Intelligence in Cybersecurity, 2021.
6. Li, W., et al. Network Intrusion Detection Using Machine Learning 2020.