

## ШТУЧНИЙ ІНТЕЛЕКТ В КІБЕРАТАКАХ

Ніконенко Д.В., В'юхін Д.О.

Харківський національний університет радіоелектроніки Харків, Україна

**Метою доповіді** є опис потенційних загроз, які штучний інтелект може становити для кібербезпеки. У галузі кібербезпеки штучний інтелект набирає все більшої популярності, оскільки його можна використовувати для створення нових методів виявлення та протидії кібератакам.

Через те, що штучний інтелект швидко навчається на великих обсягах даних, можна розробляти нові методи атак. Швидкість обробки даних можна використовувати для аналізу великих наборів даних щоб адаптуватись під поведінку користувачів, це допоможе знайти шаблони, які можуть бути використані для розробки фішингових атак та зробити ці програми важчими для виявлення антивірусним програмним забезпеченням [1]. Наприклад, можна зробити програму, яка може шифрувати файли користувача та вимагати викупу.

Штучний інтелект можна використовувати для автоматизації кібератак [2-4]. Це може призвести до збільшення їх частоти та масштабу. Наприклад, коли буде автоматизовано робитись часті масові атаки на цілі, які не мають достатньої захисту, можна буде легко отримати якісь цінні данні, витративши на це менше ресурсів.

Також, його можна використовувати для атаки на критичну інфраструктуру, наприклад, на енергосистеми або транспортну систему. Це може призвести до значних економічних збитків і навіть до людських жертв.

Проведений аналіз показав, що використання штучного інтелекту для реалізації кібератак є потенційною загрозою. Організації повинні бути готові до цієї загрози та розробляти заходи для протидії новим загрозам. Ці заходи можуть включати в себе:

- впровадження систем виявлення кібератак;
- розробку політик та процедур безпеки;
- підвищення обізнаності співробітників про кіберзагрози.

### Список літератури

1. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. DOI: 10.31673/2409-7292.2020.04061
2. Mathew A., Amudha P. and Sivakumari S. Deep Learning Techniques: An Overview. In book: Advanced Machine Learning Technologies and Applications. January 2021. [https://www.researchgate.net/publication/341652370\\_Deep\\_Learning\\_Techniques\\_An\\_Overview](https://www.researchgate.net/publication/341652370_Deep_Learning_Techniques_An_Overview).
3. Al Musawi, Ahmad. (2018). Introduction to Machine Learning. [https://www.researchgate.net/publication/323108787\\_Introduction\\_to\\_Machine\\_Learning](https://www.researchgate.net/publication/323108787_Introduction_to_Machine_Learning).
4. Dipankar Dasgupta, Zahid Akhtar, Sajib Sen. Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling & Simulation. September 2020.