Секція 1

КІБЕРБЕЗПЕКА В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

Ганзера М. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сьогодні стрімкий розвиток штучного інтелекту (ШІ) сильно впливає та змінює багато сфер, особливо технологічну, і кібербезпека також не стала винятком [1]. ШІ може бути як частиною надійного захисту систем, так і стати «мозком» продуманих та фатальних кібератак [2]. Наразі ШІ вже використовується у великих компаніях для аналізу, відстеження та запобігання різного роду атак [3]. Тому з часом, тема пов'язана з використанням ШІ для захисту від кібератак буде тільки набирати більших оборотів та звучати все частіше.

Метою даної роботи є аналіз, як штучний інтелект впливає та буде впливати на сферу кібербезпеки, дослідити потенціал ШІ як інструменту захисту від кібератак або навпаки, як частину атаки [4].

Основні положення. Прогноз, що глобальна кіберзлочинність коштуватиме понад $23 трлн до 2027 року не є втішним, тому співпраця ШІ з кібербезпекою є найоптимальнішим варіантом в даний момент. Кібербезпека на основі ШІ має низку переваг, таких як управління ідентифікацією, що гарантує захист даних і мереж від несанкціонованого доступу, моніторинг у реальному часі, який захищає як локальних, так і віддалених користувачів, а також покращена видимість, яка виявляє прогалини в системі безпеки [3]. Для розуміння того, як ШІ може допомогти у захисті, потрібно знати алгоритми його використання в атаках. Розроблення просунутого шкідливого програмного забезпечення може використовувати алгоритми машинного навчання для створення шкідливого програмного забезпечення, яке самооптимізується на основі реакції середовища, яке намагається заразити, таким чином уникаючи систем, які зазвичай використовуються для його виявлення (антивірусів). Deepfakes: створюють аудіо або відео, які здаються реальними, але не є такими насправді, і можуть використовувати їх для створення дезінформаційних кампаній, погроз, шантажу користувачів і навіть обманювати алгоритми контролю доступу або аутентифікації організацій для доступу до несанкціонованих систем. Але завдяки ШІ можна відстежити нормальну поведінку користувачів і систем у мережі, а також спостерігати за ними, щоб виявляти незвичну активність. Алгоритми

штучного інтелекту також можуть аналізувати програмний код для пошуку потенційних вразливостей для вчасного виявлення та виправлення їх, щоб кіберзлочинці не змогли ними скористатися. Ще однією великою перевагою штучного інтелекту у світі кібербезпеки є можливість автоматизації реагування на інциденти, наприклад, автоматичне блокування підозрілих IP-адрес, що дозволяє швидше відповідати на кіберзагрози. Таким чином, в роботі були розглянуті деякі з переваг ШІ і того, як він може допомогти організаціям зменшити свої ризики та вразливості в більш ефективний і дієвий спосіб.

Висновки. Підсумовуючи, можна сказати, що ШІ безумовно є сильним інструментом, але він сам по собі не є поганим чи хорошим, таким його робить той, хто ним користується. Для того, щоб максимально використовувати можливості ШІ та мінімізувати ризики, необхідно створювати нові методи захисту, підвищувати етичні стандарти та розробляти регуляторні рамки для його використання у кіберпросторі.

Список літератури

1. The impact of AI: Cybersecurity challenges and opportunities. *Pluralsigth.* URL – https://www.pluralsight.com/resources/blog/cybersecurity/ai-impact-cybersecurity#future-of-ai-security (дата звернення: 19.10.2024).
2. Generative AI and Cybersecurity: Strengthening Both Defenses and Threats. *Bain & Company*. URL – https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/ (дата звернення: 19.10.2024).
3. AI Cybersecurity: 18 Companies. *BuiltIn*. URL – https://builtin.com/artificial-intelligence/artificial-intelligence-cybersecurity (дата звернення: 20.10.2024).
4. The Impact and Limitations of Artificial Intelligence in Cybersecurity. *SSRN*. URL – https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317 (дата звернення: 21.10.2024).
5. AI for Cybersecurity A Handbook of Use Cases by Peng Liu, Tao Liu. *Penn State Cyber Security Lab*. URL – https://psucybersecuritylab.github.io/book.pdf (дата звернення: 21.10.2024).

Відомості про авторів

Ганзера Марина Олексіївна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.o.ganzera@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@csn.khai.edu