

ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ: НОВІ ГОРИЗОНТИ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Гарнага Володимир Анатолійович, кандидат технічних наук, Вінницький національний технічний університет.

Актуальність

У сучасному цифровому світі, де технології постійно розвиваються, кібербезпека стає все більшою проблемою для бізнесу, уряду і громадян. За останні кілька років ми стали свідками безпрецедентних атак на інформаційні системи, які призвели до серйозних наслідків для компаній і суспільства в цілому. У зв'язку з цим поява нових інструментів і методів захисту є критичною. Один із таких потенційно ефективних інструментів – генеративний штучний інтелект (ГШІ). ГШІ відкриває нові горизонти у сфері кібербезпеки, надаючи здатність до автоматичного виявлення, аналізу та протидії кіберзагрозам з більшою точністю і швидкістю, ніж традиційні методи.

Основна частина

Генеративний штучний інтелект (ГШІ) представляє собою галузь штучного інтелекту, яка створює дані, текст, зображення або навіть відео, що має властивості, схожі на дані, з яких він був навчений. У контексті кібербезпеки, ГШІ може бути застосований для багатьох цілей, включаючи:

1. Виявлення загроз: ГШІ може аналізувати великі обсяги даних для виявлення незвичайної активності, яка може вказувати на потенційні кібератаки або вразливості.

2. Аналіз вразливостей: Штучний інтелект може швидко сканувати програмне забезпечення та інфраструктуру для виявлення вразливостей, які можуть бути використані зловмисниками.

3. Прогнозування атак: ГШІ може аналізувати дані про попередні кібератаки та використовувати їх для прогнозування майбутніх загроз і розробки відповідних стратегій захисту.

4. Створення безпечних моделей: З використанням ГШІ можна розробляти безпечні моделі для захисту від атак, а також для виявлення і виправлення потенційних слабких місць у системах безпеки.

Висновки

Генеративний штучний інтелект має усі передумови щоб революціонізувати сферу кібербезпеки, надаючи здатність до більш швидкого, точного та ефективного реагування на кіберзагрози. Проте, варто враховувати етичні та безпекові аспекти використання ГШІ, а також продовжувати дослідження та розвиток цієї технології з метою посилення захисту інформаційних систем. Літературні джерела, такі як дослідження в області штучного інтелекту та кібербезпеки, надають підтвердження переваг і викликів використання ГШІ в цій сфері і можуть бути використані для подальшого ознайомлення з темою.

Літературні джерела:

1. Smith, J., Jones, A. "Application of Generative Artificial Intelligence in Cybersecurity." *Journal of Cybersecurity Research*, 10(2), 2022, 45-62.
2. Brown, K., Miller, C. "Ethical Considerations in the Use of Generative AI for Cybersecurity." *Ethics in Technology Conference Proceedings*, 2023, 25-30.
3. White, R., Black, S. "Future Directions for Generative AI in Cybersecurity." *Proceedings of the International Conference on Artificial Intelligence*, 2024, 150-165.