УДК 004.8

Д. С. Джумела

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ

Вінницький національний технічний університет

Анотація

У цій статті досліджується використання штучного інтелекту у сфері інформаційних технологій, де він відіграє значну роль у контексті швидкого розвитку новітніх технологій. Розглянуто важливість штучного інтелекту та безпеку використання штучного інтелекту у кібербезпеці, а також деякі обмеження, з якими він стикається.

Ключові слова: штучний інтелект, безпека, дані, інформаційні технології, кібербезпека, загрози.

Abstract

This article examines the use of artificial intelligence in the field of information technology, where it plays a significant role in the context of the rapid development of new technologies. Considers the importance of artificial intelligence and the safety of using artificial intelligence in cyber security, as well as some of the limitations it faces.

Keywords: artificial intelligence, security, data, information technology, cyber security, threats.

Вступ

Штучний інтелект – це здатність комп'ютерних систем виконувати завдання, які зазвичай вимагають людського інтелекту. ШІ може аналізувати інформацію, яка була накопичена раніше, та приймати рішення, враховуючи зовнішні фактори [1]. Основним підходом у галузі штучного інтелекту є машинне навчання, його головною метою є розробка алгоритмів, які можуть аналізувати, інтерпретувати та навчатися на основі даних, щоб потім використовувати ці знання для ухвалення обгрунтованих рішень або здійснення прогнозів [2].

Результати дослідження

У сучасному світі штучний інтелект має велике значення для сфери інформаційних технологій, оскільки він може допомагати IT-спеціалістам впоратися зі зростаючою складністю та вимогами сучасних технологічних середовищ [3].

Штучний інтелект відіграє значну роль в IT-сфері, особливо в кібербезпеці. Кібербезпека забезпечує захист мереж, систем і даних від несанкціонованого доступу, атак та збитків. Вона поєднує технології, процеси і поведінку користувачів для зменшення ризиків в кіберпросторі, забезпечуючи конфіденційність, цілісність і доступність інформації та послуг [3,4].

Штучний інтелект може оптимізувати виявлення загроз та розробляти рішення з кібербезпеки, які відповідають до всіх можливих аспектів загроз. Такі системи штучного інтелекту самостійно навчаються та автоматично контролюються, вони здатні застосовувати аналіз у непередбачуваних ситуаціях і приймати рішення на основі власних спостережень [5].

Штучний інтелект може допомогти виявленню та передбаченню загроз наступними способами:

- Автоматизований аналіз великих обсягів даних у реальному часі: штучний інтелект може активно моніторити мережу за наявності загроз, швидко аналізуючи велику кількість структурованих та неструктурованих даних. Це дозволяє автоматизувати процес моніторингу, зменшуючи кількість помилок.

– Виявлення незвичайної активності: використовуючи аналіз змін у мережі, ШІ може встановлювати шаблони та передбачати можливі загрози. Аналітика поведінки виявляє незвичайні дії як у межах, так і поза межами системи.

– Прогнозування результатів векторів атаки: ШІ може використовувати методи машинного навчання для аналізу історичних даних та передбачення майбутніх векторів атаки. Алгоритми штучного інтелекту можуть аналізувати величезні масиви даних і виявляти приховані зв'язки в подіях, які дуже важко виявити людині.

Сучасні системи штучного інтелекту, попри дивовижні успіхи, мають певні обмеження у виконанні складних завдань, які вимагають глибокого розуміння контексту та взаємодії з навколишнім середовищем [6].

Деякі з обмежень штучного інтелекту:

– Системи штучного інтелекту ефективно розв'язують тільки конкретний тип завдань, для якого вони були спеціально розроблені.

– У штучного інтелекту немає такої можливості «перемикати контекст», переключаючись з одного типу завдань на інший, як роблять це люди.

– Для досягнення високої продуктивності системам штучного інтелекту потрібен час на навчання та наявність достатньої кількості якісних даних, перш ніж їх можна буде використовувати за призначенням.

– У разі суттєвих змін у вхідних параметрах системи штучного інтелекту може виникнути необхідність тимчасового припинення роботи системи, для повторного навчання під новими умовами.

Висновок

Штучний інтелект став необхідним елементом сучасного світу технологій, здатним вирішувати складні завдання та суттєво впливати на розвиток інформаційних технологій. Він виступає потужним інструментом для посилення кібербезпеки, адже здатний автоматизувати процеси, вирішувати складні завдання та забезпечувати надійний захист систем [3]. Використовуючи аналіз великих обсягів даних у реальному часі, штучний інтелект виявляє незвичайну активність та прогнозує можливості загрози. Його застосування відкриває нові можливості та досягнення в сучасних технологіях. Однак штучний інтелект також приносить певні ризики та має обмеження у роботі.

У підсумку, штучний інтелект є інструментом для розвитку сучасних технологій та забезпечення кібербезпеки, але його впровадження вимагає ретельного аналізу потенційних ризиків та етичних аспектів для безпечного використання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Фратавчан В.Г., Фратавчан Т.М., Лукашів Т.О., Літвінчук Ю.А., Методи та системи штучного інтелекту: навчальний посібник. Чернівці: ЧНУ, 2023, – 114 с.
2. Гончарук М. У чому відмінності між штучним інтелектом, машинним і глибоким навчанням. 2024. URL: https://lemon.school/blog/v-chem-otlychyya-mezhdu-yskusstvennym-yntellektom-mashynnym-y-glubokym-obuchenyem
3. Марія Ломінська. Як штучний інтелект змінює IT-сферу. 2023. URL: https://blog.ithillel.ua/articles/how-ai-changes-the-it
4. Скарбик П. 10 основних порад із кібербезпеки для співробітників організацій. 2024. URL: https://itechua.com/articles/254888
5. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. Київ. 2024. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/
6. Вишня Г. Штучний інтелект і людина: загрози і можливості. 2021. URL: https://www.radiosvoboda.org/a/shtuchnyi-intelekt-zagrozy-i-mozhlyvisti/31145992.html

Джумела Даяна Стефанівна – студентка групи 1БС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: daianadzhumela@gmail.com

Dzhumela Daiana Stefanivna – student of group 1BS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: daianadzhumela@gmail.com