ПРОБЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

Заболотня Д.В., здоб. вищої освіти
Державний біотехнологічний університет

В сучасному світі, де технологічний прогрес набуває нестримних обертів, штучний інтелект визначає новий етап розвитку суспільства, кардинально змінюючи підходи до вирішення завдань у різних галузях. Однією з таких галузей є кібербезпека, де машинний інтелект виконує роль у попередженні та боротьбі з кіберзагрозами. Вивчення його впливу на кібербезпеку є важливим завданням, оскільки ці технології стають необхідним інструментом для подолання зростаючих загроз у віртуальному просторі.

Позитивні аспекти використання штучного інтелекту обумовлені його спроможністю революціонізувати підхід до виявлення та протидії кіберзагрозам. Його системи здатні аналізувати великі обсяги данних в режимі реального часу, виявляти потенційні загрози, забезпечуючи цим ефективну реакцію на кібератаки. Однією з ключових переваг машинного інтелекту є швидкість реагування та автоматизовані реакції на кіберзагрози, які дозволяють негайно вживати заходи для запобігання атакам та зменшення часу на відновлення після атак. Його системи здатні стрімко та самостійно виявляти атаки, а також надавати оптимальні варіанти відповіді без значного втручання людини, що є дуже важливо у сучасних умовах, коли час реакції визначає успішність заходів з кібербезпеки. Це, в свою чергу, підвищує загальний рівень безпеки та зменшує ймовірність серйозних втрат внаслідок кібернападів. Важливо також відзначити, що штучний інтелект використовує алгоритми машинного навчання для покращення точності прогнозування нових типів кіберзагроз та вдосконалення систем захисту перед їх можливим виникненням. Це дозволяє забезпечити ефективне попередження атак, що робить рівень кібербезпеки зависоким [1]. Таким чином, маємо суттєво покращену ефективність, адаптивність та передбачуваність заходів захисту. Потужності в автоматизації та оптимізації реакцій на загрози разом із здатністю до навчання та самовдосконалення, роблять щтучний інтелект важливим інструментом для забезпечення високого рівня кібербезпеки в динамічному інформаційному середовищі.

Поглиблюючись у розгляд досяжності високого рівня кібербезпеки неможливо не зазначити деякі негативні аспекти застосування штучного інтелекту, враховуючи можливість зловживання цією технологією. Саме в кібербезпеці використання машинного інтелекту відкриває потенційні ризики, які вимагають уважного вивчення. Перш за все, виникає можливість зловживання штучним інтелектом для створення більш складних та удосконалених кібератак. Кіберзлочинці можуть використовувати ці технології для створення нових загроз, ускладнюючи процес їх виявлення та протидії. Ще однією негативною стороною є можливість вразливості штучного інтелекту до маніпуляцій з боку зловмисників. Якщо хакерам вдасться отримати доступ до

систем, що використовує машинний інтелект, вони можуть змінювати його роботу відповідно до своїх цілей, і це може призвести до непрацездатності системи. Розпізнавання та автоматизація генерації інформації можуть призвести і до широкомасштабного поширення неправдивих новин та впливу на громадську думку. Додатковий аспект стосується етичних питань та соціальних наслідків. Штучний інтелект, який має здатність самостійного розвитку та прийняття рішень, може викликати серйозні виклики у визначенні етичних стандартів та забезпеченні безпеки в його застосуванні в різних сферах, включаючи медицину, фінанси та соціальні служби.

Також, треба зазначити той факт, що штучний інтелект може стати інструментом і для створення потужних кіберзброй та кібератак у воєнних конфліктах. Застосування штучного інтелекту може використовуватися для нападів на критичні інфраструктурні об'єкти, системи зв'язку та електроенергетики, що може призвести до серйозних наслідків для національної безпеки. Додатково небезпека полягає у можливості зловживання системами, для порушення приватності та конфіденційності особистих даних для здійснення масштабного моніторингу та вторгнень у приватне життя громадян. Загалом, можливість використання штучного інтелекту для створення кіберзагроз та порушення безпеки виробляє питання щодо етичних аспектів використання цієї технології. Ретельний контроль, розробка відповідних нормативів та міжнародних угод є важливими аспектами для запобігання можливого негативного використання штучного інтелекту в кібербезпеці [1,2].

Продовжуючи аналіз негативної частини, важливо звернути увагу на питання, яке хвилює значну кількість людей: "Чи може штучний інтелект зашкоджувати людині?". Це питання виходить за межі технічних обговорень і вимагає уваги у контексті етичних, соціальних та правових аспектів, особливо з огляду на можливості автономних систем. Окрім цього, існує потенціал втрати контролю над штучним інтелектом, особливо в разі його самостійного розвитку та прийняття рішень. Це може викликати непередбачувані наслідки та виникнення ситуацій, які суперечать етичним та правовим стандартам [2,3].

У підсумку, слід сказати, що важливо продовжувати розвивати та вдосконалювати нормативну базу, яка б забезпечувала безпеку та відповідальне використання штучного інтелекту в кібербезпеці. Спільна увага до позитивних і негативних аспектів допомагатиме створити більш збалансовану та ефективну стратегію використання штучного інтелекту в цих сферах

Інформаційні джерела:

1. Переваги та недоліки штучного інтелекту. URL: https://www.google.com/url.
2. Сутність і проблематика штучного інтелекту. URL: http://dspace.onua.edu.ua/
3. Штучний інтелект та інформаційні війни. URL: https://tverezo.info/post/168323