УДК 004.896

ДАМАСКІН В.О.

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ: ПОТЕНЦІЙНІСТЬ ТА ВИКЛИКИ

Вінницький національний технічний університет

Анотація

У цій статті досліджено використання штучного інтелекту (ШІ) у сфері кібербезпеки, зокрема його потенційність та виклики. Розглянуто різні аспекти застосування ШІ, включаючи системи виявлення загроз, кіберзахист, прогностичний аналіз, та відновлення після кібератак.

Ключові слова: штучний інтелект, кібербезпека, виявлення загроз, кіберзахист, прогностичний аналіз, відновлення після кібератак.

Abstract

This article explores the use of artificial intelligence (AI) in cybersecurity, including its focus and challenges. Various aspects of AI applications are considered, including threat detection systems, cyber defense, predictive analytics, and cyber attack recovery.

Keywords: Artificial Intelligence, cyber security, emergence of threats, cyber protection, prognostic analysis, investigation after cyber attacks.

Вступ

Розвиток технологій штучного інтелекту (ШІ) привертає все більше уваги до його потенціалу в багатьох сферах, включаючи кібербезпеку. Сучасні системи ШІ відкривають нові можливості для виявлення, аналізу та протидії кіберзагрозам, що стає особливо актуальним у світлі зростаючих обсягів цифрових атак та кіберпреступності. Проте разом із зростанням потенціалу ШІ у кібербезпеці виникають і нові виклики, пов'язані з етичними, правовими та технічними аспектами його застосування. У даному дослідженні ми спробуємо проаналізувати потенціал та виклики використання штучного інтелекту у сфері кібербезпеки. Ми розглянемо різні аспекти застосування ШІ, включаючи системи виявлення загроз, кіберзахист, прогностичний аналіз, та відновлення після кібератак. Крім того, ми звернемо увагу на етичні та правові аспекти використання ШІ у кібербезпеці та важливість розробки відповідних стандартів та регулювання для забезпечення безпеки та конфіденційності даних у цифрову епоху.На основі цього аналізу, ми сподіваємося зрозуміти, як штучний інтелект може використовуватися для посилення кібербезпеки, а також ідентифікувати важливі виклики, які потребують уваги та вирішення з боку дослідників, практиків та законодавців.

Потенціал ШІ в кібербезпеці

Перш за все, варто розглянути потенціал систем штучного інтелекту у сфері кібербезпеці. Системи виявлення загроз, основані на ШІ, можуть аналізувати великі обсяги даних та виявляти аномальну активність, що допомагає попереджати кібератаки та запобігати їх наслідкам. Наприклад, алгоритми машинного навчання можуть виявляти незвичайні патерни в поведінці користувачів або аномальний трафік в мережі, що вказує на можливі загрози. Крім того, штучний інтелект може бути використаний для автоматизації процесів кіберзахисту, наприклад, за допомогою систем, що аналізують та блокують атаки у режимі реального часу. Автоматизовані системи можуть швидко реагувати на нові загрози та адаптуватися до них, що дозволяє забезпечити високий рівень захисту мережі.

Виклики використання ШІ у кібербезпеці

З інноваціями у сфері штучного інтелекту (ШІ) у кібербезпеці постають нові виклики. Етичні та правові аспекти використання ШІ потребують уважного розгляду, оскільки деякі застосування можуть порушувати приватність та права людини. Наприклад, системи моніторингу можуть неповідомлено збирати та аналізувати особисті дані користувачів, порушуючи їх права на конфіденційність. Крім того, системи ШІ можуть бути вразливі до атак та зловживань кіберзлочинців. Атаки можуть використовувати слабкості у алгоритмах машинного навчання або системах автоматизованого кіберзахисту для отримання несанкціонованого доступу до системи або проведення кібератак.

Висновок

У світлі зростаючої складності кіберзагроз та швидкого розвитку технологій ШІ, розуміння їхнього потенціалу та викликів стає надзвичайно важливим. Використання штучного інтелекту у кібербезпеці може значно полегшити виявлення та протидію кіберзагрозам, проте потребує ретельного аналізу етичних, правових та технічних аспектів. Для ефективного використання ШІ у кібербезпеці необхідно розробляти та впроваджувати стандарти безпеки, а також надавати відповідну підготовку та навчання фахівцям у галузі кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. [Електронний ресурс] ─ Режим доступу : https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/
2) Штучний інтелект та кібербезпека .[Електронний ресурс] ─ Режим доступу : https://www.education.ua/blog/48113/

ДАМАСКІН Володимир Олександрович — студент групи 1БС-22Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email:vovadamaskin4@gmail.com

DAMASKIN Volodymyr Oleksandrovych — student of group 1BS-22b, Faculti of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.