УДК 004.8

А. Р. Магденко
І. О. Бучацький
І. О. Бондаренко

ШТУЧНИЙ ІНТЕЛЕКТ: НОВА ЗБРОЯ У РУКАХ КІБЕРЗЛОЧИНЦІВ ТА ШАХРАЇВ

Вінницький національний технічний університет

Анотація

У даному дослідженні розглянуто роль штучного інтелекту в кібербезпеці. Завдяки своїй здатності аналізувати великі обсяги даних, виявляти вразливості в системах безпеки та прогнозувати потенційні кіберзагрози штучний інтелект стає одним із ключових інструментів у боротьбі із кіберзагрозами та захисті від кібератак.

Ключові слова: штучний інтелект, кібербезпека, загрози, хакери, машинне навчання, алгоритми машинного навчання, аналіз даних

Abstract

In this study, the role of artificial intelligence in cybersecurity has been examined. Thanks to its ability to analyze large volumes of data, identify vulnerabilities in security systems, and forecast potential cyber threats, artificial intelligence becomes one of the key tools in combating cyber threats and protecting against cyberattacks.

Keywords: artificial intelligence, cybersecurity, threats, hackers, machine learning, machine learning algorithms, data analysis

Вступ

У сучасному цифровому світі загрози в сфері кібербезпеки розвиваються дуже стрімко. Через зростаючу складність кібератак, організації все частіше звертаються до інструментів штучного інтелекту (ШІ) для зміцнення своєї оборони та захисту активів. Інструменти ШІ для кібербезпеки використовують алгоритми машинного навчання та прогностичний аналіз для виявлення загроз, реагування на інциденти та захисту конфіденційних даних в реальному часі [1].

Штучний інтелект стає дедалі популярнішою темою розмов, коли йдеться про технології в наш час, особливо з публічним випуском таких інструментів, як ChatGPT. І хоча ШІ має законні та корисні застосування, деякі його негативні аспекти затьмарюють позитивний потенціал. Однією з великих проблем, коли мова йде про використання ШІ, є те, як його використовують хакери та шахраї для зловмисних цілей.

Результати дослідження

Сучасні системи штучного інтелекту (ШІ) використовуються для машинного навчання, що передбачає навчання на основі великих обсягів даних. Ці дані використовуються для створення моделей, які дозволяють системам ШІ аналізувати нові дані та робити висновки або приймати рішення, покращувати свою продуктивність без явного програмування. Тренування моделі за допомогою великої кількості даних дозволяє їй розпізнавати шаблони в цих даних, а потім робити прогнози або класифікації. Модель "навчається", налаштовуючи свої параметри на основі зворотного зв'язку і порівнюючи свої прогнози з фактичними результатами. Процес навчання включає аналіз і використання великих обсягів даних, щоб ідентифікувати закономірності та шаблони. Ці дані можуть бути збережені у вигляді навчальних наборів даних, які будуть використовуватися для тренування моделей ШІ. Коли модель навчання завершується, вона може бути використана для прогнозування або прийняття рішень на основі нових даних. Це дозволяє системам ШІ реагувати на нові ситуації та робити висновки навіть без чітко визначених правил чи інструкцій.

Отже, завдяки цьому процесу навчання системи машинного навчання стають більш точними та ефективними у вирішенні конкретних завдань, таких як розпізнавання зображень, розпізнавання мови та аналіз даних [1].

Штучний інтелект стає все більш помітним у сферах виявлення шахрайства та кібербезпеки, пропонуючи інноваційні рішення для боротьби з новими загрозами в сучасному цифровому ландшафті. Від фінансових установ до платформ електронної комерції – організації з різних секторів використовують технології на основі штучного інтелекту для посилення заходів із запобігання шахрайству та кібербезпеки.

Увага хакерів та шахраїв до ШІ викликана можливістю отримати доступ до цінної інформації та потенційною загрозою, яку вони можуть представляти для систем безпеки. Зловживання штучним інтелектом зловмисниками та шахраями для злочинних цілей є серйозною проблемою. Наведемо приклади деяких з найпоширеніших методів:

– Використання ШІ для автоматизації процесів злому або атак на комп'ютерні системи може робити такі атаки швидшими, ефективнішими та складними для їх виявлення.

– Створення переконливих повідомлень електронної пошти або текстових повідомлень за допомогою ШІ може допомогти зловмисникам в імітації відомих осіб або організацій з метою обману і викрадення даних.

– Використання ШІ для створення переконливих фейкових профілів у соціальних мережах або чат-ботів, що імітують людську поведінку, для ведення обману та маніпуляції користувачами з метою отримання конфіденційної або фінансової інформації.

– Генерація за допомогою ШІ відео та аудіо дипфейків, що дозволяють здійснювати підробки, що призводить до крадіжки особистих даних або маніпуляції громадською думкою.

– Алгоритми ШІ допомагають хакерам виявляти вразливості, використовувати слабкі місця та вилучати цінні дані з скомпрометованих систем у безпрецедентному масштабі.

– За допомогою штучного інтелекту хакери можуть прискорювати процес злому паролів, використовуючи техніки машинного навчання для аналізу шаблонів і передбачення ймовірних комбінацій [1].

– Використання ШІ для аналізу великого обсягу біометричних даних та створення імітацій голосових команд авторизованих користувачів і відбитків пальців, які можуть бути використані для несанкціонованого доступу до системи [2].

На протидію хакерам у кібербезпеці також активно використовуються ШІ. На сьогоднішній день є чимало інструментів із штучним інтелектом для захисту інформації.

Кібербезпека дійсно може отримати значну користь від використання штучного інтелекту. Там, де традиційні системи безпеки можуть бути обмеженими у швидкості та ефективності, методи ШІ можуть підвищити їхню загальну ефективність і забезпечити кращий захист від постійно зростаючої кількості складних кіберзагроз.

ШІ може виявляти підозрілу активність та незвичайні патерни, які можуть бути важко виявити традиційними методами. Використання алгоритмів глибокого навчання дозволяє системам ШІ виявляти аномальні патерни, навіть якщо вони раніше не були відомі. Це може допомогти вчасно виявляти та запобігати кібератакам та іншим загрозам:

– Використання ШІ системами виявлення вторгнень та аномалій для аналізу трафіку в мережі та виявлення аномальної активності, що може свідчити про потенційні кібератаки або інциденти безпеки.

– Для прогнозування загроз штучний інтелект використовується для аналізу великих обсягів даних з метою прогнозування потенційних кіберзагроз та виявлення вразливостей у системах безпеки.

– В системах виявлення загроз ШІ може автоматично реагувати на кібератаки шляхом блокування систем, або їх ізоляцією, також використовується для виявлення та видалення шкідливого програмного забезпечення, відновлення нормального функціонування мережі або системи [3].

Використання ШІ у кібербезпеці дозволяє ефективно виявляти, аналізувати та відповідати на кіберзагрози в реальному часі, що допомагає підтримувати безпеку інформаційних систем та захищати конфіденційні дані від зловмисників.

Висновки

Хакери та шахраї активно використовують штучний інтелект (ШІ) для вдосконалення своїх атак. Вони використовують алгоритми ШІ для автоматизації атак, збільшуючи швидкість, масштаб та складність нападів. Інструменти на основі ШІ дозволяють аналізувати великі обсяги даних для створення персоналізованих фішингових листів, повідомлень та чат-ботів, що робить їх шахрайство

більш ефективним. Також він прискорює процес злому паролів та обходить біометричні системи, створюючи вражаючі копії відбитків пальців та голосу.

Інструменти кібербезпеки на основі штучного інтелекту, хоч і складні, проте є корисними для кожної комп'ютерної системи та мережі. Вони відіграють важливу роль у протидії кіберзлочинам, реагуючи на будь-які ризики та мінімізуючи загрози безпеці. Автоматизований процес безпеки створений для розрізнення між загрозливою інформацією та корисними даними.

Інтеграція інструментів ШІ у комп'ютерні системи допомагатиме знизити ризики кіберзагроз та кіберзлочинів.

Важливо розуміти, що не зважаючи на те, що штучний інтелект надає зловмисникам нові можливості для реалізації складних атак, які можуть призвести до серйозних наслідків для інформаційної безпеки та конфіденційності даних, важливо визнати й потенційну користь ШІ, що допомагає забезпечити більш ефективний захист від кібератак та зменшити загрози безпеки [4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. How Hackers and Scammers Use AI (Artificial Intelligence) - Cyber-Seniors Inc. *Cyber-Seniors Inc.* URL: https://cyberseniors.org/uncategorized/how-hackers-and-scammers-use-ai-artificial-intelligence/ (дата звернення: 09.05.2024).

2. How Do Hackers Use AI? - New. New. URL: https://oxen.tech/blog/how-do-hackers-use-ai-omaha-ne/ (дата звернення: 10.05.2024).

3 Artificial Intelligence (AI) Cybersecurity | IBM. *IBM in Deutschland, Österreich und der Schweiz*. URL: https://www.ibm.com/ai-cybersecurity?utm_medium=OSocial&utm_source=Youtube&utm_content=RSRWW&utm_id=YT-101-AI-and-Cybersecurity (дата звернення: 11.05.2024).

4 Top 7 AI Tools for Cybersecurity in 2024. URL: https://www.geeksforgeeks.org/ai-tools-for-cybersecurity/?ref=ml_lbp (дата звернення: 12.05.2024).

Магденко Анастасія Романівна – студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: anastasiiamahdenko@gmail.com

Бучацький Ілля Олександрович – студент групи 2КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: illiabu2005@gmail.com

Бондаренко Ірина Олексіївна **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Magdenko Anastasija R. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anastasiiamahdenko@gmail.com

Buchazkij Illja O.- student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: illiabu2005@gmail.com

Bondarenko Iryna O. **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua