УДК 004.8

І. С. Зоря
А. В. Марущак

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ

Вінницький національний технічний університет

Анотація
В даній роботі проведено дослідження щодо прогнозування та боротьби з кіберзагрозами за допомогою штучного інтелекту. Дослідження охоплює аналіз різноманітних аспектів, починаючи від технологій кіберзахисту, впливу штучного інтелекту на кібербезпеку та перспектив розвитку. В роботі наведено переваги та недоліки використання таких систем, що допомагає отримати повний огляд того, як штучний інтелект формує сучасний підхід до кібербезпеки та розглядає його потенційні можливості в цифровому середовищі.
Ключові слова: *штучний інтелект (ШІ); кібербезпека; кіберзагрози; виявлення загроз; реагування на загрози.*

Abstract
In this work, a study was conducted on forecasting and combating cyber threats with the help of artificial intelligence. The study covers analysis of various aspects, ranging from cyber defense technologies, the impact of artificial intelligence on cyber security and development prospects. The paper presents the advantages and disadvantages of using such systems, which helps to get a complete overview of how artificial intelligence is shaping the modern approach to cyber security and considers its potential opportunities in the digital environment.
Keywords: *artificial intelligence (AI); cyber security; cyber threats; threat detection; threat response.*

Вступ

У наш час, в епоху цифрового прогресу, підвищення стійкості інформаційних систем до кіберзагроз є актуальною задачею, що має першочергове значення для користувачів та організацій, які взаємодіють між собою та використовують інформаційні ресурси. Зараз можна спостерігати зростання атак на дані, ресурси та критичну інфраструктуру, включаючи атаки на фінансові ресурси та особисті дані. В умовах постійної еволюції мережевих загроз, розгортання передових технологій стає життєво важливим. У цьому контексті використання штучного інтелекту для виявлення та протидії кіберзагрозам визнається одним з перспективних напрямків. Штучний інтелект володіє здатністю аналізувати та обробляти великі обсяги даних, а також виявляти та уникати ризики, що пов’язані з кіберзагрозами, завдяки своїм можливостям самонавчання. Метою даної роботи є дослідження застосування штучного інтелекту в галузі кібербезпеки та аналіз його ролі у підвищенні захисту від кібератак.

Результати дослідження

У сучасному світі штучний інтелект став не лише інновацією, але й невід'ємною складовою повсякденного життя. Він безперервно трансформує різні сфери, допомагаючи автоматизувати нудні та рутинні завдання, ефективно вирішувати складні проблеми та значно покращувати продуктивність. Але однією з найважливіших областей застосування штучного інтелекту є кібербезпека. Тут його роль набуває критичного значення: алгоритми машинного навчання аналізують величезні обсяги даних, сприяючи виявленню аномалій у мережевому трафіку та ідентифікації потенційно небезпечних

вразливостей. ШІ використовує технології, які можна застосовувати в різних галузях промисловості, таких як фінанси, освіта та охорона здоров'я [1]. Оскільки вищевикладене підтверджує, що зловмисні атаки можуть стати серйозною загрозою, використання методів штучного інтелекту для забезпечення кібербезпеки організацій та підприємств є повністю обґрунтованим. Системи ШІ на базі алгоритмів машинного навчання та лінгвістичних нейромереж широко використовуються для захисту даних у сучасних інструментах [2].

Однією з основних областей застосування штучного інтелекту є виявлення несанкціонованого дослідження інформаційного ресурсу. Системи автоматично виявляють зловмисний код або незвичайний інтернет-трафік і реагують на незвичайну поведінку користувачів. Наприклад, якщо алгоритм виявляє спробу користувача отримати доступ до особистих даних під час нічного часу, це може свідчити про зловмисну активність.

Крім того, алгоритми машинного навчання допомагають у фільтрації спаму. Наприклад, вони використовуються в поштових фільтрах для зменшення кількості фішингових листів, які надходять на електронну пошту користувачів. Це дозволяє попереджати співробітників про підозрілі листи та зменшує ризик відкриття шахрайських повідомлень. Таким чином, використання штучного інтелекту допомагає ефективно боротися з кіберзагрозами і забезпечує високий рівень безпеки в цифровому середовищі.

Традиційні системи ШІ опрацьовують відомі загрози, але нові методи злому з'являються майже щодня [2]. Отже, вміння передбачати зловмисні дії та реагувати на вразливості до їх активізації є надзвичайно важливими в галузі кібербезпеки. Засоби на основі генеративних моделей штучного інтелекту стають ефективним інструментом для цього завдання. Вони не лише здатні виявляти певні патерни, але й генерувати контент, що є перспективним напрямком для розробки як антивірусів, так і комерційних засобів кібербезпеки.

Виявлення порушень цілісності даних набуває важливості, оскільки швидка реакція дозволяє уникнути великих витрат на їх відновлення. Зараз виникає все більше складних кібератак, що збільшує час виявлення та усунення порушень. Автоматизовані системи безпеки та інтелектуальні засоби можуть допомогти організаціям ефективніше контролювати та реагувати на інциденти. Такі системи, як SIEM [3], фільтри спаму та інструменти захищеної автентифікації, використовують методи штучного інтелекту для аналізу та ідентифікації шкідливої активності. Машинне навчання та експертні системи допомагають автоматизувати процеси виявлення та реагування на загрози кібербезпеки. Крім того, застосування нейронних мереж і методів дата майнінгу [4] дозволяє виявляти та прогнозувати атаки, використовуючи великі масиви даних. Інтелектуальні агенти використовуються для захисту від атак типу DoS/DDoS та для розподіленої обробки даних у мережі.

У майбутньому ролі штучного інтелекту в кібербезпеці будуть подвійними. З одного боку, ШІ може використовуватися для посилення систем захисту, сприяючи виявленню та запобіганню атакам більш ефективно. Але з іншого боку, хакери також можуть зловживати ШІ для створення складніших та вдосконалених атак. Нижче детальніше наведено можливості систем генеративного штучного інтелекту в контексті кіберзахисту:

– виявлення аномальної поведінки, полягає у встановленні ознак, за якими дії користувачів вважаються зловмисними для звичайних систем захисту. Коли деякі з цих ознак збігаються, система реєструє вторгнення. У той же момент, штучний інтелект може ідентифікувати параметри, які навіть не враховувалися раніше. Це дозволяє створити більш ефективну предикативну модель;

– автоматичні дії [2]. Вкрай важливо реагувати на загрозу негайно, оскільки її важко виявити. Алгоритми генеративного ШІ можуть зробити це якнайшвидше;

– робота з автоматичними атаками важлива для великих компаній. Зазвичай, вони змушені реагувати на загрози, які реалізуються через комп'ютерні алгоритми, а не одноразово вручну, за допомогою фахівців. Оскільки зловмисні програми постійно змінюються, людина не завжди здатна оперативно виявити та нейтралізувати загрозу;

– боротьба з фальшнегативними та фальшпозитивними сигналами [2]. У галузі корпоративної кібербезпеки система повинна одночасно моніторити різноманітні події, такі як трафік в мережі Інтернет, відвідування веб-сайтів і т. д. В цьому "шумі" легко зробити помилкові висновки щодо того,

чи є певна діяльність нормальною або небезпечною. Це в даний час основна проблема в галузі кібербезпеки.

ШІ має можливість аналізувати великі об'єми даних і потоки інформації в реальному часі, виявляючи автоматично незвичну поведінку або підозрілі активності. Це дозволяє розпізнавати можливі кіберзагрози швидше та ефективніше, ніж їх може виявити людина. Також, ШІ може застосовувати аналіз попередніх даних і поточних загроз для передбачення майбутніх атак [5]. Тому перевагами використання штучного інтелекту в кібербезпеці будуть:

1. Виявлення загроз. Штучний інтелект використовує алгоритми машинного навчання для аналізу та ідентифікації незвичайних патернів, які можуть вказувати на потенційні кіберзагрози. Він може реагувати на нові типи атак, навіть якщо вони не були раніше відомі, завдяки своїм навчальним здібностям.

2. Автоматизована відповідь. Інтелектуальні системи можуть автоматично реагувати на кіберзагрози, здійснюючи швидке блокування або відмову в доступі до підозрілих джерел, навіть без втручання операторів.

3. Прогнозування і попередження. Штучний інтелект може обробляти великі обсяги інформації, включаючи дані про минулі кібератаки, для передбачення майбутніх загроз і прийняття заходів з їх запобігання.

4. Адаптивність. Системи штучного інтелекту можуть навчатися на основі нових даних та аналізувати зміни в структурі атак, щоб адаптувати свої методи виявлення та захисту в реальному часі.

5. Обробка великих обсягів даних. Інтелектуальні системи здатні швидко та ефективно обробляти великі обсяги структурованих та неструктурованих даних, що дозволяє виявляти навіть найскладніші кіберзагрози.

6. Мінімізація помилок. Використання штучного інтелекту допомагає у зменшенні помилок, пов'язаних з людським фактором, так як системи можуть працювати безперервно та не втомлюватися, що дозволяє виявляти загрози більш точно та ефективно.

Штучний інтелект відкриває нові можливості в сфері кібербезпеки, забезпечуючи більшу ефективність захисту та зменшення часу реагування на кіберзагрози. Проте, часто системи штучного інтелекту сприяють хакерам у приховуванні свого місцезнаходження та джерела атаки, ускладнюючи їх виявлення та переслідування для кіберполіції [5]. Таким чином, використання штучного інтелекту в кібербезпеці має і свої недоліки, які потрібно ураховувати та вирішувати для забезпечення ефективного захисту від кіберзагроз. Наведемо декілька недоліків:

1. Неабсолютна точність. ШІ може допускати помилки в аналізі та інтерпретації даних, що може призвести до неправильних висновків про потенційні загрози або інциденти безпеки.

2. Потреба у великих обсягах обробки даних. Деякі алгоритми ШІ вимагають значних обсягів даних для навчання та аналізу, що може створювати складнощі при обробці великої кількості інформації.

3. Залежність від якості даних. Точність та ефективність систем ШІ напряму залежить від якості та доступності вхідних даних. Недостатня якість даних може призвести до неправильних результатів аналізу.

4. Загроза зловживанням. ШІ може бути вразливим до атак, таких як введення неправильних даних або маніпуляція з вихідними результатами, що може призвести до спотворення аналізу та прийняття невірних рішень.

Хоча штучний інтелект має значний потенціал у покращенні кібербезпеки, враховуючи ці недоліки, необхідно уважно розглядати їх впровадження та використання. З метою забезпечення внутрішньої готовності штучного інтелекту, необхідно вжити надійних заходів кібербезпеки для захисту конфіденційності даних і систем штучного інтелекту від кібератак. Ось декілька рекомендацій щодо заходів кібербезпеки:

– захист кінцевих точок, такий як використання антивірусного програмного забезпечення та брандмауерів, може забезпечити безпеку систем і даних ШІ, захищаючи їх від несанкціонованого доступу та кіберзагроз;

– захищений зв'язок, використовуючи безпечні протоколи, такі як SSL/TLS та VPN, допомагає захистити дані під час їх передачі між системами ШІ та іншими кінцевими точками;

– шифрування даних забезпечує захист конфіденційної інформації від несанкціонованого доступу, зашифровуючи дані як у стані спокою, так і під час їх передачі [6];

– контроль та виявлення вразливостей: регулярне тестування на вразливості допомагає виявляти та усувати проблеми в безпеці систем і даних ШІ [6].

Попередні рекомендації представляють лише деякі з можливих заходів кібербезпеки, які можуть бути використані для забезпечення безпеки систем штучного інтелекту. До цього також можна додати важливість постійного моніторингу та аналізу поведінки системи для виявлення аномальних активностей. Важливо пам'ятати, що кібербезпека – це постійний процес, і постійне вдосконалення заходів захисту є ключем до успішної захисту від кіберзагроз.

Висновки

Загальний вплив штучного інтелекту на кібербезпеку є досить вагомим та має як позитивні, так і негативні сторони впливу. Незважаючи на те, що ШІ відкриває нові можливості для ефективного виявлення та захисту від кіберзагроз, він також може стати об'єктом зловживання та представляти загрозу для безпеки. Необхідно постійно вдосконалювати технології та впроваджувати ефективні стратегії співпраці між державними та приватними секторами для ефективного захисту цифрових інфраструктур від кіберзагроз. Таким чином, застосування штучного інтелекту в кібербезпеці є ключовим елементом стратегії захисту у сучасному світі цифрових технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Перегляд Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Open Journal Systems. [Електронний ресурс]. Режим доступу: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2456/2356 (дата звернення: 11.03.2024).

2. Валентина Шимкович. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс. [Електронний ресурс]. Режим доступу: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення: 11.03.2024).

3. Що таке "Інформація про безпеку та управління подіями" (SIEM)? | Gridinsoft. ТОВ "Грідінсофт". [Електронний ресурс]. Режим доступу: https://gridinsoft.ua/siem (дата звернення: 11.03.2024).

4. Що таке data mining (аналіз даних)?. FutureNow. [Електронний ресурс]. Режим доступу: https://futurenow.com.ua/shho-take-data-mining-analiz-danyh/ (дата звернення: 11.03.2024).

5. Штучний інтелект та кібербезпека – стаття від «Cisco, мережна академія » – Education.ua. Освіта в Україні. Усі навчальні заклади – Education.ua. [Електронний ресурс]. Режим доступу: https://www.education.ua/blog/48113/ (дата звернення: 11.03.2024).

6. 4 питання щодо кібербезпеки при розгортанні Штучного інтелекту - BDO. Міжнародна аудиторська компанія BDO - BDO. [Електронний ресурс]. Режим доступу: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/4-cybersecurity-considerations-for-ai-deployment (дата звернення: 11.03.2024).

Марущак Анастасія Віталіївна – студентка групи УБ-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anamar349@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** – ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: iryna.zoria03@gmail.com

Marushchak Anastasiia Vitalyivna – student of group UB-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anamar349@gmail.com

Supervisor: ***Zoria Iryna Serhiivna*** – assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: e-mail: iryna.zoria03@gmail.com