ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Ігнатенко М.Є.,
здобувач вищої освіти факультету менеджменту
Миколаївський національний аграрний університет
Науковий керівник: Полторак А.С.,
д-р екон. наук, професор, завідувач кафедри менеджменту та маркетингу,
Миколаївський національний аграрний університет

Сфера штучного інтелекту використовується у багатьох аспектах нашого життя. Через зростання кількості кіберзлочинів потрібен інструмент, який буде попереджувати або реагувати автоматично на будь-які його прояви. При правильному налаштуванні штучного інтелекту можливо зробити його адаптивним та сприятливим до самонавчання, що допоможе у швидкому запобіганню критичних атак. Таким чином, вищезазначені аспекти підтверджують актуальність досліджуваної проблеми.

Метою роботи є обґрунтування основ та практичних підходів щодо використання штучного інтелекту для автоматизованого виявлення кіберзагроз.

Алгоритми машинного навчання можуть аналізувати великі обсяги даних для виявлення аномалій та підозрілих дій, які можуть свідчити про кібератаки. Вони навчаються на нормальних патернах поведінки мережі та систем, щоб ідентифікувати відхилення [1].

Штучний інтелект дозволяє аналізувати великі обсяги даних та виявляти аномалії, що є критично важливим для запобігання та протидії кіберзагрозам. Завдяки машинному навчанню можливо навчити систему знаходити нові методи кіберзагроз [2].

Інструменти штучного інтелекту дозволяють автоматизувати різні рівні кібербезпеки. Від моніторингу до реакції – штучний інтелект зменшує необхідність ручної обробки повідомлень про загрози, дозволяючи командам безпеки зосередитися на складніших атаках. Крім того, системи на основі ШІ можуть швидко реагувати на загрози, наприклад, ізолювати заражені системи або розгортати контрзаходи, що значно скорочує час на реагування [3].

Технології штучного інтелекту, зокрема обробка природної мови, можуть бути застосовані для автоматизованого аналізу текстових звітів, описів шкідливих програм та інших джерел даних для швидкого виявлення загроз.

Інтеграція моделі штучного інтелекту в системи кібербезпеки дозволяє автоматизувати процеси, які раніше потребували значних людських ресурсів, наприклад, моніторинг подій в системі та виявлення шкідливого програмного забезпечення.

Для ефективного протистояти новим загрозам моделі штучного інтелекту повинні постійно переглядатися та вдосконалювати свої стратегії безпеки. Це включає впровадження нових технологій і методів, які можуть відповідати швидко змінюваному ландшафту кібератак [4].

Різноманіття пристроїв і складність експлуатаційних технологій вимагають розробки спеціалізованих рішень для захисту IIoT-систем від унікальних загроз, але завдяки штучному інтелекту можливо розробити універсальний інструмент для вияву кібератак та загроз, яка буде працювати без людського втручання [5, 6].

Отже, обґрунтовано теоретичні засади та практичні підходи щодо використання штучного інтелекту для автоматизованого виявлення кіберзагроз. Технології штучного інтелекту значно підвищують ефективність виявлення та реагування на кіберзагрози, забезпечуючи своєчасну і точну ідентифікацію аномалій та потенційних атак. Застосування машинного навчання і глибокого навчання дозволяє системам адаптуватися до нових загроз у динамічному кібер середовищі, що є критично важливим для захисту систем. Автоматизація процесів виявлення загроз не лише знижує навантаження на IT-спеціалістів, але й істотно скорочує час реагування на інциденти. Сформовані висновки сприятимуть подальшому розвитку і впровадженню ефективних рішень у сфері кібербезпеки, що відповідають сучасним викликам і вимогам.

Список використаної літератури

1. Кібербезпека та штучний інтелект. *Web Academy Media*. офіц. сайт URL: https://shorturl.at/QZNqX (дата звернення: 15.09.2024).

2. Марущак А. В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. URL: https://shorturl.at/eeLEK (дата звернення: 15.09.2024).

3. AI Tools for Protecting and Preventing Sophisticated Cyber Attacks / ed. by E. Babulak. Hershey. *IGI Global*, 2023. 233 p.

4. Fesokha V. Peculiarities of the confrontation between defensive and offensive artificial intelligence in cyberspace. *International Science Journal of Engineering & Agriculture*. 2024. Vol. 3, no. 4. P. 105–114. URL: https://shorturl.at/w9J5S (date of access: 15.09.2024).

5. Karimipour H., Derakhshan F. AI-Enabled Threat Detection and Security Analysis for Industrial IoT. Springer International Publishing AG, 2021. 250 p.

6. Полторак А.С., Сухорукова А.Л., Бурковська А.І. Кібербезпека в системі трансформації управління бізнес-організацією. Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики : колективна монографія з нагоди 115-річчя Київського національного економічного університету імені Вадима Гетьмана ; за загальною редакцією М. П. Сагайдака, Т. О. Соболєвої. Київ : Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана. КНЕУ, 2021. 378 с. ISBN 978–966–926–399–5 С.158-176.