ШТУЧНИЙ ІНТЕЛЕКТ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Воронянський Є.[1], Лучик В.[1],

[1]*Харківський національний університет внутрішніх справ*

Штучний інтелект грає важливу роль у протидії кіберзлочинності. Використання штучного інтелекту для боротьби з кіберзлочинністю стає все більш актуальним, оскільки кіберзлочинці стають все більш винахідливими і складними у своїх атаках.

Ось деякі способи, якими штучний інтелект може бути корисним у цьому контексті [1, с.179]:

1. Виявлення загроз. Штучний інтелект може використовуватися для аналізу великих обсягів даних та виявлення потенційних загроз і аномалій в мережі. Він може реагувати на незвичайні активності, які можуть бути зв'язані з кіберзлочинцями.

2. Прогнозування атак. Штучний інтелект може аналізувати попередні атаки і поведінки кіберзлочинців, щоб передбачити майбутні атаки і підготуватися до них.

3. Автоматизована реакція. Штучний інтелект може бути налаштований на автоматичну реакцію на певні типи атак, включаючи блокування доступу до системи, ізолювання компрометованих ресурсів та збільшення рівня безпеки.

4. Моніторинг безпеки. Штучний інтелект може відстежувати безпеку мережі та даних в режимі реального часу, сприяючи вчасному виявленню порушень безпеки.

5. Аналіз логів і великих обсягів даних. Штучний інтелект може використовувати машинне навчання для аналізу логів та даних, щоб виявити аномалії та потенційні загрози, які можуть бути незрозумілі для людей [2].

Оскільки світ стає все більш цифровим, загроза кібератак зростає.

Розвиток технологій дозволяє зловмисникам ставати більш вдосконаленими у своїх методах, включаючи

використання штучного інтелекту для автоматизованих складних атак, які важко виявити і захиститися від них.

Кібератаки на основі штучного інтелекту можуть завдати значно більше шкоди, ніж традиційні кібератаки. Штучний інтелект використовується для автоматизації таких завдань, як пошук вразливостей, здобуття інформації та запуск цілеспрямованих атак. Це значно підвищує швидкість та масштаб атак, дозволяючи хакерам одночасно нападати на кілька цілей. Штучний інтелект також може створювати великі обсяги даних, які використовуються для обходу систем безпеки та проникнення в мережі.

Застосування кібератак на основі штучний інтелект набуває популярності. Останнім часом атаки програм-вимагачів за допомогою штучного інтелекту стали частішими та більш руйнівними. Ці атаки використовують штучний інтелект для швидкого виявлення вразливих систем і розповсюдження шкідливого програмного забезпечення, яке може швидко поширюватися в мережі. Зловмисне програмне забезпечення на основі штучного інтелекту також використовується для незаконного проникнення в мережі, крадіння даних та порушення операцій[3].

Зростаюча загроза кібератак на основі штучного інтелекту змусила уряди та організації приймати додаткові заходи для забезпечення своєї безпеки. Багато організацій впроваджують рішення кібербезпеки на основі штучного інтелекту для виявлення передових загроз і захисту своїх мереж. Крім цього, організації збільшують свої бюджети на кібербезпеку та інвестують у навчання та навчання, щоб допомогти співробітникам розпізнавати потенційні загрози та реагувати на них.

Кібератаки на основі штучного інтелекту становлять значну загрозу для організацій і урядів, і хоча це може здаватися складним завданням, існують заходи, які можна прийняти, щоб зменшити ризик. Інвестування в передові рішення кібербезпеки, навчання співробітників розпізнавати потенційні загрози та збільшення бюджетів на кібербезпеку допоможе організаціям захистити себе від

зростаючої загрози кібератак на основі штучного інтелекту [4].

Роль машинного навчання в протидії кіберзлочинності стає надзвичайно важливою в умовах зростаючої складності цифрових загроз для безпеки. Машинне навчання представляє собою галузь штучного інтелекту, яка дозволяє комп'ютерам самостійно набувати знання на основі аналізу даних та виявлення закономірностей. В контексті боротьби з кіберзлочинністю цю технологію можна використовувати для виявлення зловмисної активності, розпізнавання аномалій та запобігання кібератакам.

Штучний інтелект відіграє ключову роль у протидії зростаючій загрозі кіберзлочинності. З використанням штучного інтелекту ми можемо виявляти та передбачати кібератаки, реагувати на них автоматично та моніторити безпеку в реальному часі. Штучний інтелект дозволяє ефективно виявляти аномалії та потенційні загрози, що є важливим у контексті росту складності кібератак.

Зростаюча загроза кіберзлочинності, особливо з використанням штучного інтелекту, заставляє організації і уряди приймати серйозні заходи для забезпечення своєї кібербезпеки. Інвестування в розвиток та впровадження рішень кібербезпеки на основі штучного інтелекту, а також навчання персоналу стають важливими факторами в захисті від кіберзлочинності.

Загалом, використання штучного інтелекту у сфері кібербезпеки стає необхідністю, оскільки технологічний прогрес веде до зростання загроз у цифровому світі. Штучний інтелект допомагає виявляти, передбачати та запобігати кібератакам, забезпечуючи вищий рівень безпеки для організацій і інфраструктури в цілому.

Список використаних джерел

1. Романчук О. Штучний інтелект в епоху нових медій. *Вісник львівського університету. серія «журналістика»*. 2018. Вип. 44. С. 179–188.

2. Штучний інтелект і запобігання кіберзлочинності: як інтелектуальні системи допомагають виявляти та

запобігати кіберзагрозам. *TS2 SPACE*. URL: https://ts2.space/uk/штучний-інтелект-і-запобігання-кібер/.

3. Концепція розвитку штучного інтелекту в Україні [Електронний ресурс]: Розпорядження Кабінету міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

4. Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса. URL: https://ivpz.kh.ua/wp-content/uploads/2020/12/Матеріали-семінару_Використання-техн-штучного-інтел_5.11.2020.pdf.

5. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. URL: https://dspace.univd.edu.ua/items/2329c5f4-e52e-43d5-8eaf-35758a04ca09.