УДК 510.635:004.891(045)

Н.А. Товстуха
Національна академія Служби безпеки України, Київ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ: ЗА ТА ПРОТИ

Штучний інтелект (ШІ) з кожним днем стає актуальним в інформаційній безпеці. На сьогодні близько 50% підприємств вже використовують комбінацію ШІ та інструментів машинного навчання, а понад 90% організацій планують запровадити такі інструменти в майбутньому. І це не дивно, адже такі системи можна використовувати починаючи від перевірки на вразливість і закінчуючи захистом даних, а в поєднанні з досвідченим, у сфері кібербезпеки, фахівцем, стає надзвичайно ефективним.

Так чому ж ШІ викликав до себе такий інтерес з боку фахівців з кібербезпеки? Бо система має ряд переваг, таких як:

1. Виявлення загроз. Найбільша проблема, з якою постійно зустрічаються фахівці з кібербезпеки – величезний обсяг даних, в якому звичайні системи забезпечення не можуть виявити значну кількість нових вірусів. Штучний інтелект, здатен швидко аналізувати шаблони в базах даних, щоб виявити аномальну поведінку чи ідентифікувати загрози.

2. Автоматизація. ШІ розгортають для того, щоб автоматизувати та оптимізувати аспекти кібербезпеки. Тобто, це дозволяє фахівцям зосередити увагу на розслідуванні та ліквідуванні складних загроз, тоді як ШІ виконує монотонні базові завдання.

3. Самонавчання. Одна з переваг технології ШІ є здатність вчитися та вдосконалюватися. Маючи дані минулих атак, алгоритми машинного навчання ідентифікують закономірність, а потім розробляють нові та покращені методи виявлення. Тому хакерам буде важче перехитрити ШІ.

4. Виявлення внутрішніх загроз. Ці загрози ще більш небезпечні, тому що їх складно виявити, оскільки залучені особи мають законний доступ до даної мережі. Але системи на базі штучного інтелекту можуть аналізувати поведінку користувачів і таким чином визначати характерні риси, що вказують на внутрішню загрозу.

5. Передбачення загроз. Аналізуючи великі обсяги даних, ШІ

може передбачити загрози, її масштаб, а також як і де найімовірніше буде взлом. Цю інформацію потім можна використовувати для розробки ефективних методів стратегії кібербезпеки.

6. Рішення безпеки кінцевих точок, що базуються на штучному інтелекті, використовують алгоритми машинного навчання для виявлення небезпечної поведінки та раніше невідомих загроз. Цей підхід ефективніший, ніж традиційні методи, оскільки дозволяє ідентифікувати небезпеку, яка за іншими обставинами була б непоміченою.

Але не дивлячись на ряд переваг, система має суттєві недоліки:

1. Нездатність працювати автономно. Оскільки вони ще не в стані повністю замінити людські рішення, залишаються задачі, які вимагають втручання людини.

2. Проблема з приватністю. Аналіз великого обсягу даних може призвести до того, що як приватні, так і суспільна інформація буде аналізована ШІ, що зможе призвести до втрати конфіденційності інформації.

3. Відсутність контролю. Найбільш поширеною проблемою є побоювання з приводу того, що ШІ може вийти з під людського контролю через унікальний непередбачуваний характер, до якого не можливо застосувати правові рамки

4. Етнічні проблеми. На цей час ШІ не має морального кодексу, отже рішення, які приймаються замість людини, не обов'язково будуть такими ж, якби такі рішення приймала людина.

Отже, ШІ – це дуже перспективний інструмент у сфері кібербезпеки, який потребує подальшого вдосконалення, та контролю зі сторони людей.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Artificial Intelligence in Cybersecurity, Nadine Wirkuttis and Hadas Klein, p. 103-119*
2. *https://cybersecurityforme.com/artificial-intelligence-for-cybersecurity/*
3. *https://www.cybertalk.org/2023/03/27/how-artificial-intelligence-is-revolutionizing-cyber-security/*