Охрімчук В. В. к.т.н., професор
Охрімчук І. А, викладач
Житомирський військовий інститут імені С. П. Корольова

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА СТАН КІБЕРБЕЗПЕКИ

Сучасний розвиток технологій штучного інтелекту (ШІ) відкриває перед людством нові можливості у всіх сферах життя Одним з таких напрямів, де вплив ШІ критично відчутний – це кібербезпека. Сьогодні, коли цифрова інформація стає все більшою частиною нашого життя, забезпечення її захисту від кіберзагроз все більше актуалізується. Тому, ШІ стає ключовим інструментом для виявлення загроз, запобігання кібератакам та управління ризиками. В першу чергу це пов'язане з тим, що він здатен автоматизувати аналіз великих обсягів даних, миттєво реагувати на аномалії та виявляти небезпеки ще на ранніх етапах.

Проте окрім усіх позитивних ефектів від впровадження ШІ в системи інформаційної безпеки виникають додаткові ризики пов'язані з можливістю використання зловмисниками цієї технології для автоматизації атак, створення шкідливого програмного забезпечення, маніпулювання даними, тощо. Тому питання використання ШІ в кібербезпеці є надзвичайно важливим, адже воно межує між забезпеченням додаткового рівня захисту та необхідністю контролювати його потенційні загрози.

Таким чином, для впровадження ШІ в системи інформаційної безпеки необхідно чітко усвідомлювати усі можливі ризики. Таке впровадження можливе тільки за однієї умови: коли виграш від впровадження буде переважати усі наявні та потенційні ризики.

Отже, розглянемо основні можливі переваги від впровадження ШІ в системи інформаційної безпеки.

Виявлення загроз у реальному часі. Системи зі ШІ здатні аналізувати великі обсяги даних і виявляти аномалії, які можуть свідчити про кібератаки. Наприклад, алгоритми машинного навчання можуть фільтрувати небезпечні файли або повідомлення електронної пошти.

Аналіз поведінки користувачів. Алгоритми машинного навчання можуть використовуватися для створення профілів поведінки користувачів і, в подальшому, для виявлення аномальних дії. Цей підхід знижує кількість помилкових спрацьовувань і підвищує точність систем інформаційної безпеки.

Автоматизація реагування на інциденти. Технології ШІ здатні аналізувати ситуацію і автоматично реагувати на загрози. Це зменшує час реагування.

Прогнозування та превентивні заходи. За допомогою алгоритмів ШІ можливе прогнозування потенційних загроз на основі аналізу попередніх кіберінцидентів. Це дозволяє розробляти превентивні заходи для захисту систем.

Незважаючи на значні переваги від впровадження ШІ в системи інформаційної безпеки, в руках зловмисників він може створювати нові виклики та ризики. Зокрема:

Автоматизація кібератак. Зловмисники можуть використовувати ШІ для автоматизації розроблення та здійснення кібератак, які складніше виявляти та блокувати. Наприклад, генеративні алгоритми можуть створювати нові варіанти шкідливого програмного забезпечення, які не виявляються сучасними антивірусними засобами.

Атаки на системи ШІ. Враховуючи значний вплив ШІ на прийняття рішення він може стати ціллю для кібератак. Прикладом такої атаки є так зване "отруєння даних" (*data poisoning*), коли зловмисники навмисно додають спотворені дані у навчальні вибірки щоб змусити алгоритм приймати неправильні рішення.

Соціальна інженерія та фішинг. ШІ здатний створювати фальшиві повідомлення або імітувати поведінку реальних людей (так звані "*deepfake*"), що робить фішинг-атаки ефективнішими та складнішими для виявлення.

Отже, ШІ має значний позитивний вплив на підвищення рівня кібербезпеки, створюючи нові можливості для виявлення загроз, аналізу поведінки та реагування на інциденти. Поряд із тим, потенціал ШІ може бути використаний зловмисниками для удосконалення методів кібератак. Таким чином, щоб мінімізувати ризики кібербезпеці від впровадження ШІ необхідно розробляти нові або удосконалювати наявні технології протидії кіберзагрозам.

Список використаних джерел

1 Охрімчук В. В., Охрімчук І. А. Необхідність інтеграції систем підтримки прийняття рішення в систем и інформаційної безпеки. // Кіберборотьба: розвідка, захист та протидія: тези доповідей II Міжнародної науково-практичної конференції. - Київ: ВІТІ, 2024. С 44.

2 Сукайло І. О., Коршун Н. В. Вплив nlu і генеративного ші на розвиток систем кіберзахист // Кібербезпека: освіта, наука, техніка № 2 (18), 2022. С. 187-196