УДК 004.896.2:004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.139

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАХИСТІ ТА ПРОТИДІЇ DDOS-АТАКАМ

Павлов О.А.
Науковий керівник – доц. Шаповалова А.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
e-mail: Oleksii.pavlov2@nure.ua.

The article explores the evolving landscape of DDoS attacks within the realm of Artificial Intelligence (AI). Delving into the technological progress, it highlights how AI, particularly Machine Learning, is leveraged by attackers to craft sophisticated and adaptive DDoS strategies. The text emphasizes real-world instances where AI is employed in orchestrating attacks, posing challenges for traditional detection methods. While acknowledging the technical advantages, the article also underscores the challenges of integrating AI into cybersecurity, emphasizing the need for a delicate balance between accuracy and computational resources.

Тенденція розвитку сфери кіберпростору прогресивно зростає з кожним роком. Жертвами DDoS-атак стають критично важливі цілі, здебільшого це – онлайн-банкінг, платіжні шлюзи, урядові портали, оператори зв’язку. З переліченого зрозуміло, що це критично важливі інфраструктури як для звичайного користувача, так і для держави в цілому. Захист подібних цілей є найважливішим та першочерговим. У цій статті ми обговоримо як про важливість захисту від подібних атак, так і можливість інтеграції штучного інтелекту у вже існуючі методи захисту від DDoS-атак, що дасть змогу покращити їх.

Головною метою подібних атак є чітка кінцева ціль – відмова в обслуговуванні. Концепція подібних атак є дуже простою, зловмисники використовують таку кількість трафіку, що б він перевищував роздільну здатність пропускної спроможності цілі. Distributed Denial of Service attack - напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Штучний інтелект дає можливість зловмисникам провести автоматизацію процесів створення та запуску DDoS-атак. Машинне навчання дає змогу атакам виявляти в системі жертви вразливості безпеки та швидко адаптуватись під потрібні методи. Це важливий аспект захисту, оскільки традиційні методи виявлення DDoS-атак стають не ефективними порівняно з сучасними, інтелектуальними атаками з використанням штучного інтелекту.

Вже є випадки, коли штучний інтелект використовувався для реалізації атак. Як приклад, атаки де використовувались ботнети на основі нейронної мережі для імітації поведінки реальних користувачів, вони стають все більш популярними методами атак. Для традиційних методів захисту подібні атаки стають критичними, а їх виявлення та блокування стає набагато складнішим завданням для команд кібербезпеки.

Головна проблематика інтеграції штучного інтелекту, є постійний баланс між швидкістю реагування та точністю дуже великим обсягом даних, які вони обробляють. Більшість сучасних систем штучного інтелекту мають потребу в дуже великих обчислювальних ресурсах, які забезпечити здебільшого складно.

Тенденція розвитку кіберзагроз, з використанням штучного інтелекту та машинного навчання у розробці DDoS-атак стає серйозним викликом для сучасних систем захисту. Порівнюючи технологічні переваги та проблематику інтеграції штучного інтелекту, можна зробити чіткі висновки, сторона безпеки повинна активно інтегрувати штучний інтелект у свої системи для забезпечення ефективної протидії більш новітнім та вдосконаленим атакам.

Системи безпеки, які інтегрують штучний інтелект для захисту від DDoS-атак, зменшують час виявлення атак з годин до хвилин, а іноді цей показник становить секунди.

Дивлячись на тенденції розвитку, можна спрогнозувати, що захист від DDoS-атак буде стрімко проходити інтеграцію зі штучним інтелектом. Розвиток квантових обчислень може дозволити створення нових, надзвичайно швидких алгоритмів для аналізу трафіку та ідентифікації атак, що відбуваються на ранніх етапах та під час самих атак.

Інновації в захисті від DDoS-атак, завдяки використанням штучного інтелекту, відкривають нові горизонти для захисту важливих онлайн ресурсів. Окрім цього, штучний інтелект посиле як чіткість реагування, так і швидкість, що дасть змогу в рази покращити кібербезепку. До всього, штучний інтелект постійно навчається, що в подальшому буде тільки покращувати кібербезпеку на автоматичному рівні.

Список використаних джерел:

1. Dhruba K. B. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance / K. B. Dhruba, K. K. Jugal., 2016. – 312 с. – (1st Edition).

2. Leslie F. Sikos. AI in Cybersecurity (Intelligent Systems Reference Library, 151) / Leslie F. Sikos., 2018. – 222 с. – (1st ed. 2019 Edition).