Лелета В. Р., здобувачка
Колощук М.С., асистент
Дячук О.Ю., ст. викладач
Державний університет «Житомирська політехніка»

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАСІБ РЕАГУВАННЯ НА МЕРЕЖЕВІ ЗАГРОЗИ

Зростання обсягів даних та складності кіберзагроз вимагає впровадження передових технологій для забезпечення безпеки інформаційних систем. Штучний інтелект (ШІ), завдяки своїм можливостям автоматизації та аналізу великих обсягів даних, стає ключовим інструментом у боротьбі з кіберзагрозами. Використання алгоритмів машинного навчання дозволяє ефективно класифікувати мережевий трафік, виявляти аномалії та реагувати на потенційні загрози в реальному часі.

На сьогоднішній день штучний інтелект стає досить потужним інструментом для різних цілей, зокрема для аналітики трафіку та прогнозування загроз в контексті кібербезпеки. Проте штучний інтелект має дві сторони: він може бути як найбільшою загрозою, так і виступати найефективнішим засобом захисту.

Такий багатогранний інструмент активно можуть використовувати як «червоні» хакери для спрощення та автоматизації цільового фішингу для викрадення особистих даних, виготовлення дипфейків для шахрайства та спрощення розробки шкідливого софту, так і «сині» хакери для виявлення DDoS-атак, фішингових кампаній, несанкціонованих доступів та аналізу великих обсягів логів у реальному часі.

Трафік можна класифікувати за кількома основними ознаками, залежно від його природи та цілей. Легітимний трафік включає запити від реальних користувачів або авторизованих систем, які виконують звичайні операції, такі як перегляд веб-сторінок або покупка товарів. Шкідливий трафік, натомість, містить атаки, направлені на злам або пошкодження системи, зокрема через методи, як DoS, DDoS або фішинг. Що стосується ботнет-трафіку, то це трафік, що генерується зловмисними мережами ботів, які можуть бути використані для розподілених атак або розповсюдження шкідливих програм.

Застосування сучасних алгоритмів машинного навчання для класифікації мережевого трафіку показало високу ефективність нейронних мереж глибокого навчання (94,7% точності), метод опорних векторів продемонстрував баланс точності (91,2%) та швидкодії, а LSTM-архітектура досягла найкращого результату (97,3%) для виявлення часових атак.

Штучний інтелект виявляє аномалії в поведінці мережі через аналіз часових патернів, підозрілих IP-адрес та характерних ознак атак. Комбінований підхід з автоенкодерами та класифікаторами на основі градієнтного бустингу зменшує час реакції на загрози на 67% і знижує частоту помилкових тривог на 42% порівняно з традиційними системами.

Штучний інтелект дозволяє автоматично визначати відхилення від нормальної поведінки у трафіку, що є ключовим у виявленні загроз, таких як DDoS-атаки або спроби несанкціонованого доступу. Автоенкодери та рекурентні нейронні мережі навчаються на нормальному трафіку та виявляють незвичайні патерни, що може сигналізувати про потенційну атаку.

Штучний інтелект є потужним інструментом для підвищення рівня кібербезпеки завдяки здатності автоматизувати процеси аналізу трафіку та реагування на загрози. Використання нейронних мереж та інших алгоритмів машинного навчання дозволяє ефективно адаптуватися до нових типів атак і забезпечувати безперебійну роботу інформаційних систем навіть у складних умовах кіберзагроз. Подальші дослідження можуть бути спрямовані на вдосконалення моделей ШІ для роботи з великими обсягами даних у реальному часі.

Список використаних джерел:

1. Глоба, О. О. Трафік в Інтернеті та його класифікація: практичні аспекти / О. О. Глоба. – Харків : Національний університет радіоелектроніки, 2023. URL: https://pt.nure.ua/wp-content/uploads/2023/12/223_globa_traffic_.pdf
2. Ткачук, М. В. Інтелектуальний аналіз мережевого трафіку для виявлення шкідливих атак / М. В. Ткачук. – Вінниця : Вінницький національний технічний університет, 2022. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3
3. Застосування ШІ у кібербезпеці: роль та переваги / Wezom. URL: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi
4. Штучний інтелект у корпоративній кібербезпеці: роль у захисті даних / BDO. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection
5. Захист від ботнетів / ESET. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/zashchita-ot-botnetov/?srsltid=AfmBOoppW3Y_7jXSFBRjelztS6qKBpa5qMRLKm9Qml0mLrLsTa78qWWg
6. DDoS-атаки: типи атак та рівні моделі OCI / AlexHost. URL: https://alexhost.com/uk/faq/ddos-ataky-typy-atak-ta-rivni-modeli-osi/