***Михайліченко О.В., аспірант***
*Національний університет «Полтавська політехніка ім. Юрія Кондратюка»*

**ЗАПОБІГАННЯ КІБЕРАТАКАМ ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖ**

Сучасні телекомунікаційні мережі стикаються з дедалі витонченішими кібератаками, які можуть загрожувати як безпеці даних і конфіденційності користувачів, так і стабільності зв'язку. У світлі стрімкого зростання обсягів даних та швидкої еволюції новітніх технологій виникає гостра необхідність у впровадженні комплексних підходів до кібербезпеки. Згідно з даними Cybersecurity Ventures, до 2025 року глобальні економічні втрати від кіберзлочинів можуть досягти неймовірних $10,5 трлн на рік.

Одним із ключових інструментів у боротьбі з кіберзагрозами є нейронні мережі, здатні обробляти величезні обсяги інформації в реальному часі. Завдяки цій технології системи безпеки можуть ефективніше адаптуватися до нових типів атак, підвищуючи точність виявлення шкідливих дій. Особливо це важливо в умовах ускладнення атак, спрямованих на Інтернет речей (IoT) та хмарні платформи. [1]

З огляду на критичність кіберзагроз, лише у 2022 році середні витрати на ліквідацію наслідків витоку даних досягли 4,35 мільйона доларів, причому найбільша частка припала на DDoS-атаки. Ще однією небезпечною сферою використання шкідливих технологій штучного інтелекту є злам паролів або обхід двофакторної аутентифікації. [3]

Разом із цим існують численні успішні приклади використання нейронних мереж для захисту інформаційних систем - інтеграція в антивірусні програми. Завдяки впровадженню методів машинного навчання такі системи здатні виявляти не лише відомі шкідливі програми, а й зовсім нові загрози, які ще не внесені до відповідних баз даних. [1]

Для реалізації детекції кібератак у розподілених системах із застосуванням штучного інтелекту виконують аналіз різноманітних параметрів систем виявлення атак (IDS). До таких параметрів можуть належати характеристики пакетів даних, що включають заголовки, протоколи, методи кодування, тимчасові мітки передачі, інформацію про відправника та отримувача. Розглянуто запропоновану модель, яку автори визначають як багатоядерний алгоритм k-середніх із неповним ядром (MKKM-IC).

Ефективність запропонованого підходу була перевірена на трьох наборах даних: NSL-KDD, UNSW та AWID. Серед визначених загроз виділяють DDoS-атаки, ін'єкції даних, несанкціоноване заволодіння адміністративним доступом та імітаційні дії. Результати експериментального порівняння точності (precision) виявлення кібератак показали, що найвищу ефективність продемонстрували моделі MKKM-IC і Змішана Модель Гаусса (GMM), досягнувши точності в діапазоні 71–88 %. У той же час найнижчі показники були зафіксовані для алгоритму пікових щільностей і k-середніх, які мали точність в межах 55–72 %. [2]

Для організацій, які бажають відповідати найвищим стандартам у сфері інформаційної безпеки у відношенні до нейромереж, стандарти ISO 27001 та ISO 27701 залишаються основними орієнтирами. [1]

Сучасні популярні інструменти для роботи з розподіленими системами включають вбудовані засоби для виявлення кібератак. Пропозиції таких компаній, як Oracle, AWS, Azure, DigitalOcean, Cisco та IBM, демонструють як подібність функцій, так і унікальні відмінності. Cisco зосереджується на мережевій безпеці, Oracle акцентує увагу на безпеці баз даних, тоді як IBM пропонує рішення, що базуються на аналізі та обробці даних із використанням штучного інтелекту. Azure та AWS пропонують широкий спектр різноманітних служб для покращення захищеності системи.

Аналізуючи існуючі рішеня від провідних компаній у сфері кібербезпеки, включаючи Cisco, Oracle, AWS, Azure та IBM. Зроблено висновок про важливість інтеграції методів штучного інтелекту для забезпечення адаптивного та проактивного захисту інформаційних систем.

**Список використаних джерел:**

1. Вплив нейронних мереж на розвиток кібербезпеки в умовах регуляторних змін. *THE INFLUENCE OF NEURAL NETWORKS ON THE DEVELOPMENT OF CYBER SECURITY IN THE CONDITIONS OF REGULATORY CHANGES*. 2024. Т. 30. С. 261–267. URL: https://doi.org/10.18372/2225-5036.30.19238.

2.ЧЕРЕВКО К. О. ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ЗЛОЧИННОСТІ. *Вісник Кримінологічної асоціації України*. 2023. Т. 28, № 1. С. 124–133. URL: https://doi.org/10.32631/vca.2023.1.10 .

3. Volokyta A., Melenchukov M. NEURAL NETWORKS IN DETECTING ATTACKS ON DISTRIBUTED SYSTEMS. *TECHNICAL SCIENCES AND TECHNOLOGIES*. 2024. No. 1(35). P. 135–145. URL: https://doi.org/10.25140/2411-5363-2024-1(35)-135-145.