

МОЖЛИВОСТІ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ АТАК НА МУЛЬТИСЕРВІСНІ МЕРЕЖІ

Порошенко А.І., Коваленко А.А., Буслов П.В.

Харківський національний університет радіоелектроніки, Харків, Україна

Застосування нейронних мереж у кібератаках на мультисервісні мережі наразі не є значущою загрозою для захисту даних, проте ця тенденція заслуговує на увагу. Технології штучного інтелекту, зокрема нейронні мережі, поступово інтегруються в методи кібератак, що може ускладнити виявлення та запобігання злочинним діям. Сучасні нейронні мережі, володіючи здатністю обробляти та аналізувати великі обсяги даних, можуть використовуватися для автоматизації атак та генерації підробленого мережевого трафіку, що може ускладнити передачу даних у мережі [1]. Вивчення механізмів, за допомогою яких нейронні мережі можуть імітувати легітимну поведінку, дозволить розробити ефективніші системи виявлення аномалій та захисту.

Метою доповіді є дослідження можливого використання нейронних мереж та штучного інтелекту для атак на мультисервісні мережі з метою удосконалення механізмів виявлення аномалій та захисту.

В доповіді наводяться результати аналізу потенційних загроз та сценаріїв використання нейронних мереж у кібератаках. Нейронні мережі можуть використовуватися для аналізу та оптимізації DDoS-атак, створення трафіку, який виглядає легітимним для систем IDS/IPS, а також для атак на алгоритми шифрування, атак на якість обслуговування мережі та аналізу поведінкових патернів користувачів у мультисервісних мережах. Наведені дані показують, що інтеграція штучного інтелекту в методи атак може значно підвищити їхню ефективність, що вимагає вдосконалення існуючих систем безпеки. Незважаючи на те, що спостерігається зростання популярності способів захисту мультисервісних мереж на основі використання нейронних мереж та штучного інтелекту [2], завжди з'являються нові засоби атак, тому лише постійний моніторинг та інновації можуть забезпечити надійний захист у цій безперервній боротьбі.

Список літератури

1. Poroshenko, A. and Kovalenko, A. (2023) "Audio signal transmission method in network-based audio analytics system", *INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES*, (4 (26), pp. 58–67. doi: 10.30837/ITSSI.2023.26.058
2. V. Bhatia, S. Choudhary and K. R. Ramkumar, "A Comparative Study on Various Intrusion Detection Techniques Using Machine Learning and Neural Network," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2020, pp. 232-236, doi: 10.1109/ICRITO48877.2020.9198008.