УДК 004.056

АНАЛИЗ МЕТОДОВ И МЕР ПРОТИВОДЕЙСТВИЯ СЕТЕВОЙ СТЕГАНОГРАФИИ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Агарков А.В. (Университет ИТМО), **Федосенко М.Ю.** (Университет ИТМО), **Клишин Д.В.** (Университет ИТМО)

Научный руководитель – кандидат технических наук, доцент Заколдаев Д.А. (Университет ИТМО)

Введение. Среди техник скрытой передачи информации сетевая стеганография является эффективным и незаметным способом доставки скрытой информации. Злоумышленники используют все более изощренные подходы и методы для осуществления сетевой стеганографии. С помощью сетевой стеганографии могут доставляться скрытые сообщения, вредоносное программное обеспечение, изображения и другая полезная нагрузка, позволяющая развивать кампанию кибератаки.

Применение искусственного интеллекта для анализа сетевого трафика на предмет обнаружения сетевой стеганограммы является эффективной и передовой мерой противодействия злоумышленникам для обеспечения защиты конфиденциальных данных от кибератак.

Основная часть. Методы обнаружения сетевой стеганографии, основанные на статическом анализе сетевого трафика, имеют ряд преимуществ, связанных с показателями работы и технической составляющей этих методов. Например, использование искусственного интеллекта и машинного обучения в частности для стегоанализа позволяет обрабатывать большое количество поступающих сетевых данных и находить непредсказуемые шаблоны, позволяющие с высокой вероятностью указать на применение стеганографии.

Основная проблема состоит в выделении аномальных признаков и характеристик, находящихся в разных компонентах пакетов. Для задачи подобной классификации выделают следующие методы: применение случайного леса, метод опорных векторов, Байесовский классификатор, методы глубокого обучения.

- в работе [1] предлагается метод, основанный на применении деревьев решений для обнаружения стеганографических передач;
- в работе [2] рассматриваются методы глубокого обучения, такие как многослойный персептрон (MLP), сверточные нейронные сети (CNN), долговременную кратковременную память (LSTM);
- в работе [3] рассматривается метод обнаружения сетевой стеганографии на базе хранилища с использованием машинного обучения.

Выводы: Проведен обзор исследований по анализу методов и мер противодействия сетевой стеганографии с помощью методов искусственного интеллекта. На основе обзора составлены преимущества и недостатки различных подходов для решения данной проблемы.

Список использованных источников:

1. Piotr Nowakowski,Piotr Zorawski,Krzysztof Cabaj,and WojciechMazurczyk, Detecting Network Covert Channels using Machine Learning, Data Mining and Hierarchical Organisation of Frequent Sets // Warsaw University of Technology, 2021.
2. D.X. Cho, D.T.H. Thuong, N.K. Dung, A Method of Detecting Storage Based Network Steganography Using Machine Learning // Procedia Computer Science, Volume 154, 2019, Pages 543-548.

3. Cho Do Xuan, Lai Van Duong, A New Approach for Network Steganography Detection based on Deep Learning // (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 7, 2021.