

Возможности применения нейронных сетей для анализа текстов на предмет стеганографии и возможные угрозы информационной безопасности

**Сивков Д.И. (ИТМО) Агарков А.В. (ИТМО), Федосенко М.Ю. (ИТМО)
Научный руководитель – к.т.н., доцент ФБИТ, Воробьева А.А. (ИТМО)**

Введение. В последнее время повышается интерес к стеганографическим методам защиты информации. В отличие от криптографических методов, где конфиденциальность информации обеспечивается с помощью ее преобразования, в стеганографии скрывается сам факт существования конфиденциальной информации при ее передаче, обработке или хранении. Лингвистическая стеганография, использующая тексты в качестве контейнера для скрытых сообщений, становится все более сложной и трудной в обнаружении.

Методы машинное обучения могут помочь в обнаружении скрытой информации в тексте и далее будут рассмотрены различные виды нейронных сетей, их применение для задач стегоанализа, а также типы атак на эти систем [1].

Основная часть. Будут рассмотрены такие виды нейронных сетей, как CNN, RNN, LSTM, GRU для лингвистического стегоанализа:

- 1) Сверточные нейронные сети “CNN” - применяются для анализа текстов на предмет стеганографии благодаря их способности обрабатывать последовательности слов и выявлять закономерности в использовании языка [2].
- 2) Рекуррентные нейронные сети “RNN”, в том числе долгая краткосрочная память “LSTM“ и Управляемые рекуррентные блоки “GRU” будут эффективны в обработке последовательностей данных, таких как тексты, для обнаружения аномалий в структуре или содержании, что может указывать на наличие стеганографии [3].

Также будут рассмотрены популярные атаки на системы стегоанализа. [4]

Выводы. Нейронные сети представляют хороший инструмент для обнаружения лингвистической стеганографии, способный анализировать текст на глубоком уровне, а также важно учитывать возможные на него потенциальные угрозы информационной безопасности.

Список использованных источников:

- 1) Liang M., Hu X. Recurrent convolutional neural network for object recognition //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2015. – С. 3367-3375.
- 2) Bao Y. J. et al. Text Steganalysis with Attentional LSTM-CNN //2020 5th International Conference on Computer and Communication Systems (ICCCS). – IEEE, 2020. – С. 138-142.
- 3) Sundermeyer M., Schlüter R., Ney H. LSTM neural networks for language modeling //Thirteenth annual conference of the international speech communication association. – 2012.
- 4) Chang C. Y., Clark S. Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method //Computational linguistics. – 2014. – Т. 40. – No. 2. – С. 403-448.

Сивков Д.И.

Агарков А.В.

Федосенко М.Ю.

Воробьева А.А.