УДК 004.056

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ В ЗАДАЧАХ СТЕГАНОАНАЛИЗА И ОБРАБОТКИ ЦИФРОВОГО КОНТЕНТА

Федосенко М.Ю. (ИТМО)
Научный руководитель – доктор технических наук, профессор Беззатеев С.В. (ИТМО)

Введение. В докладе представлены перспективы и особенности применения интеллектуальных технологий в задачах анализа цифрового контента на предмет наличия скрытых вложений вредоносного характера. Актуальность задачи выявления скрытой информации обусловлена увеличением числа атак на информационные ресурсы с применением стеганографии [1], а также несанкционированного использования стеганографических методов в качестве скрытых каналов обмена данными в контексте утечек информации и обмена противоправной информации [2]. Актуальность применения интеллектуальных технологий в данной задачи обусловлена перспективой автоматизации процесса анализа данных в контексте обеспечения информационной безопасности среды их хранения и обработки, а также в рамках реализации приоритетов научно-технологического развития Российской Федерации [3].

Основная часть. Объёмы обрабатываемой в каналах связи цифровой информации растут с каждым годом. В свою очередь, это приводит к развитию методов их хранения и обработки, в том числе со стороны правоохранительных органов и специалистов по информационной безопасности. Например, в 2019 году были приняты поправки № 608767-7 в 149-ФЗ «Об информации, информационных технологиях и о защите информации», позволяющие большие возможности контроля потоков данных [4]. Открывающаяся в следствии этого степень доступности конфиденциальных данных для обработки оператором связи приводит к увеличению количества злонамеренного использования механизмов сокрытия данных, в том числе стеганографических методов. В сообществе специалистов в области ИБ уже известны случаи атак, группировок, программных решений, которые используют стеганографию в атаках [1]. В области информационной безопасности, задача выявления скрытых каналов связи не является новой, однако степень её проработанности, в сравнении с другими угрозами, невелика [2].

В свою очередь, немаловажной является задача по автоматизации методов реагирования на различные виды атак. Подавляющее большинство данных методов реализуются за счёт алгоритмной логики, и представляет собой набор правил и сценариев. Однако, в настоящее время активно развивается подход применения интеллектуальных технологий в задачах защиты информации: выявление сетевых атак на основе аномалий в сетевых протоколах [5], обнаружение мошеннических транзакций за счёт особенностей их проведения [6], поиск сигнатур и активности вредоносного программного обеспечения (ВПО). Применение интеллектуальных технологий в данных задачах показывает хорошие результаты при качественной разработке и отладки моделей принятия решений.

Искусственный интеллект также может быть применён для выявления аномалий в цифровом контенте, которым и являются стегановложения. При всём при этом, с высокой степенью качества способен работать как сильный, так и слабый искусственный интеллект. Представителем сильного искусственного интеллекта являются нейронные сети, применение которых в контексте стеганоанализа целесообразно в универсальных и\или нестандартных (другими словами - новых) случаев сокрытия данных, а также для обнаружения скрытых атак. Применение слабого искусственного, например – машинного обучения, целесообразно для известных случаев сокрытия информации, в заранее известных видах контейнеров, при использовании размеченных наборов данных. Также, при наличии должных механизмов

анализа визуальных и текстовых данных и высокой степени адаптации моделей принятия решений, целесообразно применение технологий компьютерного зрения (Computer Vision) и обработки естественного языка (Natural Language Processing) для выявления частных вложений в частотные области изображений и случаев использования лингвистической стеганографии [7].

Выводы. Разработка методов защиты информации на основе интеллектуальных технологий и моделей принятия решений способны не только дать новые знания в научную отрасль исследований искусственного интеллекта, но и повысить безопасность цифровых данных и сетей связи, в том числе от вредоносных воздействий скрытого характера. Применение искусственного интеллекта в стеганоанализе актуально в контексте реализации приоритета научно-технологического развития Российской Федерации «Переход к передовым технологиям проектирования и создания высокотехнологичной продукции, основанным на применении интеллектуальных производственных решений, роботизированных и высокопроизводительных вычислительных систем, новых материалов и химических соединений, результатов обработки больших объемов данных, технологий машинного обучения и искусственного интеллекта» (Н1) [3].

Список использованных источников:

1. Клишин Д.В., Федосенко М.Ю. Применение стеганографии при осуществлении компьютерных атак на информационную инфраструктуру предприятия // Экономика и качество систем связи -2024. - № 2(32). - С. 158-166.
2. Ахрамеева К.А., Федосенко М.Ю., Герлинг Е.Ю., Юркин Д.В. Анализ средств обмена скрытыми данными злоумышленниками в сети Интернет посредством методов стеганографии // Телекоммуникации - 2020. - № 8. - С. 14-20.
3. Указ Президента Российской Федерации от 28 февраля 2024 г. № 145 "О Стратегии научно-технологического развития Российской Федерации" – URL: https://www.garant.ru/products/ipo/prime/doc/408518353/.
4. Законопроект № 608767-7 «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ» от 14 декабря 2018 г. – URL: https://sozd.duma.gov.ru/bill/608767-7.
5. Федосенко М.Ю., Агарков А.В. Применение сетевой стеганографии злоумышленниками для скрытого обмена информацией и осуществления компьютерных атак // Экономика и качество систем связи -2024. - № 2(32). - С. 149-158.
6. Menshchikov A., Perfilev V., Roenko D., Zykin M., Fedosenko M. Comparative Analysis of Machine Learning Methods Application for Financial Fraud Detection//Proceedings of the 32nd Conference of Open Innovations Association FRUCT, 2022, pp. 178-186.
7. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и её роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы -2023. - № 3(56). - С. 33-57.