УДК 004.896

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ВЫЯВЛЕНИЯ ВРЕДОНОСНЫХ ФАЙЛОВ MICROSOFT OFFICE С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЕКТА

Тимашов П.В, **Шестаков И.А.**
Научный руководитель – д.т.н, доцент Бирюков Д.Н.
Военно-космическая академия имени А.Ф.Можайского

В данной работе рассматривается задача повышения защищенности объектов информационной инфраструктуры организаций от вредоносных вложений файлов Microsoft Office. Авторы предлагают новый подход выявления данной угрозы безопасности информации на основе технологий искусственного интеллекта. Также описана структура программного средства и проведение эксперимента для сравнения результативности выявления вредоносных вложений.

Введение. Microsoft Office – самое распространенное прикладное программное обеспечение (ПО) для обработки документов, электронных таблиц и презентаций. Ввиду распространенности данного ПО и повсеместном использовании его файлов, стоит отметить, что злоумышленники используют уязвимости и зловредный код в файлах Microsoft Office для начальных стадий проведения компьютерных атак и проникновения в узлы информационной инфраструктуры.

Основная часть. В рамках исследования решены следующие задачи:
1. Разработана модель угроз вредоносных файлов Microsoft Office. Проведен подробный анализ уязвимостей документов Microsoft Office и представлено описание негативных последствий, источников и способов реализации угроз безопасности информации.
2. Определены признаки вредоносных вложений файлов Microsoft Office (метаданных и VBA).
3. Разработана нейросетевая модель выявления вредоносных файлов Microsoft Office.
4. Проведен эксперимент для сравнения разработанного подхода с современными технологиями машинного обучения (CatBoost, LSTM, Random Forest).

Выводы.
В результате исследования были изучены и проанализированы методы машинного обучения и нейронные сети в рамках задачи повышения защищенности объектов информационной инфраструктуры. Была разработана нейросетевая модель выявления угроз вредоносных файлов Microsoft Office, направленная на улучшение защищенности узлов информационной инфраструктуры. Критерием эффективности модели является высокий показатель точности определения вредоносных файлов.

Тимашов П.В. (автор)

Шестаков И.А. (автор)

Бирюков Д.Н. (научный руководитель)