И. А. Мазан
(*ГрГУ им. Я. Купалы, Гродно*)

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ

Сегодня безопасность в массе своей реактивна. Мы боремся с тем, что уже кого-то задело, заразило, вывело из строя, украло деньги. И эффективность системы защиты зависит от того, насколько быстро мы будем узнавать об атаках, с которыми кто-то уже столкнулся [1]. Следовательно, это вызывает потребность в новых методах обнаружения угроз. Традиционные подходы, основанные на поиске сигнатур файлов, перестают быть эффективными так, как современные вирусы имеют способность мутировать, изменяться в процессе жизнедеятельности. На смену приходит автоматизация анализа файлов для поиска подозрительных файлов.

В работе рассматривается задача обнаружения вредоносных программ с использованием моделей машинного обучения. Требуется по известным признакам определить является ли рассматриваемая программа вредоносной. Исследуемый набор данных построен с использованием библиотек Python и содержит доброкачественные и вредоносные данные из PE-файлов [2].

В работе был проведен анализ обучающей выборки, произведена обработка обучающих данных, обучение нескольких моделей вы-

явления вредоносных программ: решающее дерево, случайный лес, градиентный бустинг. Также были применены методы для снижения размерности и обработки данных. В результате проделанных исследований для всех моделей получена высокая точность предсказаний, на уровне 92-96%. Однако, существует целый класс атак, направленных как на наборы данных, так и на сами алгоритмы обучения. Следовательно, в будущем необходимо искать решение и этих проблем.

Литература

1 Машинное обучение и информационная безопасность [Электронный ресурс]. – 2018. – Режим доступа: https://www.it-world.ru/cionews/security/141988.html. – Дата доступа: 17.02.2021.

2 Benign and malicious PE Files Dataset for malware detection [Электронный ресурс]. – 2019. – Режим доступа: https://www.kaggle.com/amauricio/pe-files-malwares. – Дата доступа: 17.02.2021.