

О Т З Ы В

на выпускную квалификационную работу бакалавра IV курса
по направлению 02.03.02 «Фундаментальная информатика и информационные технологии»
основной образовательной программы СВ.5003
«Программирование и информационные технологии»

РИТТЕРА Германа Андреевича,

выполненную на тему:

«Обнаружение программ-шифровальщиков на основе статического и динамического анализа с использованием методов машинного обучения»

Выпускная квалификационная работа Риттера Г.А. посвящена такому актуальному направлению в области компьютерной безопасности, как детектирование вредоносного программного обеспечения, которое имеет широкое применение в реальной жизни. Результаты работы могут быть использованы для защиты как личных, так и корпоративных компьютерных систем.

Целью выпускной квалификационной работы Риттера Г.А. являлись разработка методов детектирования программ-шифровальщиков, основанных на агрегации подходов статического и динамического анализа, позволяющих эффективно обнаружить в том числе новые семейства вредоносного ПО без потери времени. Для достижения поставленной цели студентом был проведен обзор существующих методов и решений для распознавания программ-вымогателей. Были описаны ограничения статического анализа для решения данной задачи и динамического анализа. На основе приведенных студентом типичных поведенческих шаблонов программ-вымогателей был составлен список признаков, в дальнейшем используемых моделями для обучения. В работе автором предлагается использование нескольких моделей машинного обучения (SVM и случайный лес) для достижения поставленной цели. Предложенные модели реализуются в рамках популярного фреймворка scikit-learn. Обучение моделей происходит без кросс-валидации на обучающем множестве, а качество обучения оценивается на валидационном множестве с использованием различных метрик качества.

К недостаткам выпускной квалификационной работы Риттера Г.А. следует отнести сжатость изложения материала и отсутствие в сравнительном анализе нейросетевых методов.

Стоит отметить, что все результаты работы получены студентом лично. Автор достаточно хорошо овладел технологиями машинного обучения и инструментами их практической реализации, а отмеченные замечания не влияют на общую положительную оценку работы.

На основании вышеизложенного считаю, что выпускная квалификационная работа Риттера Г.А. на тему «Обнаружение программ-шифровальщиков на основе статического и динамического анализа с использованием методов машинного обучения» выполнена в соответствии с предъявляемыми требованиями и заслуживает оценку «отлично».

Научный руководитель

Заведующий Кафедрой
технологии программирования

доцент, к.т.н.

7 июня 2022 г.



И.С. Блеканов