В диссертационный совет на базе
ФГБОУ ВО СПбГУПТД
Д 24.2.385.09
191186, Санкт-Петербург, ул. Большая Морская, д. 18

ОТЗЫВ

на автореферат диссертации Баркова Вячеслава Валерьевича «Классификация противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом режиме», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Задача выявления трафика нежелательных приложений в большом объёме данных стала особенно актуальна из-за развития сетей коммуникации и широкого их распространения. В это же время, для решения задач выявления противоправного контента широкое распространение получили методы интеллектуального анализа данных и машинного обучения, позволяющие адаптироваться к постоянно изменяющейся структуре Интернет-ресурсов и учитывать специфику сетевого трафика. Внедрение таких методов позволяет с высокой эффективностью производить классификацию, анализ и фильтрацию сетевого трафика вредоносных и нежелательных приложений. Однако большинство современных методов обучения плохо адаптированы к постоянно меняющемуся окружению и могут быть подвержены влиянию фоновых процессов, что ведёт к снижению качества распознавания неправомерного контента в потоке данных.

Рассматриваемые в работе Баркова Вячеслава Валерьевича алгоритмы, основанные на новом типе искусственных нейронных сетей – автокодировщиках, способны повысить качество классификации данных в потоковом режиме в изменчивых условиях и с присутствием фоновых потоков. Таким образом, актуальность, теоретическая и практическая значимость результатов диссертационной работы не вызывают сомнений.

Достоверность полученных результатов обеспечена применением современных методов исследования и успешным практическим применением результатов работы. Основные положения диссертации представлялись на международных и всероссийских научных конференциях. Результаты работы отражены в 18 печатных работах, в том числе: 5 – в журналах, входящих в перечень ВАК по специальности 2.3.6, 1 – в научном рецензируемом издании, индексируемом в Scopus; 11 – в материалах конференций и других изданиях, 1 - свидетельство о Государственной регистрации программ для ЭВМ.

В качестве замечаний к автореферату можно отметить следующее:

1. При решении задачи построения алгоритмов классификации нежелательных или вредоносных мобильных приложений автор анализирует 5 наиболее значимых атрибутов без учета IP-адресов (стр. 9). Однако, в работе не описано, что они из себя представляют.
2. Из текста автореферата не ясно, каким образом и по каким признакам в работе определяются противоправные и нежелательные мобильные приложения. Не понятно, каким образом автор использует специфичные для каждого из данных видов приложений свойства.
3. На стр.12-13 автореферата обозначено, что «использование МОСК позволяет снизить вероятность ошибки классификации примерно на 5%. … Модели классификации, не использующие МОСК, допускают на 5-7% больше ошибок». Из текста автореферата не понятно каким образом получены данные оценки и не обоснованы обозначенные количественные значения.

Перечисленные замечания не снижают общей положительной оценки полученных результатов. Считаю, что диссертация Баркова В.В. «Классификация противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом

режиме» является законченной научно-квалификационной работой, соответствует заявленной специальности и удовлетворяет требованиям пунктов 9-14 действующего «Положения о присуждении ученых степеней», предъявляемым в кандидатским диссертациям, а соискатель Барков Вячеслав Валерьевич заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Я, Максимова Елена Александровна, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Заведующий кафедрой
КБ-4 «Интеллектуальные системы
информационной безопасности»
Федерального государственного
бюджетного образовательного
учреждения высшего образования
"МИРЭА - Российский технологический университет",
доктор технических наук, доцент
(специальность докторской диссертации:
2.3.6 Методы и системы
защиты информации,
информационная безопасность) Максимова Елена Александровна

«15» ноября 2024 г.

Адрес: 119454, ЦФО, г. Москва, Проспект Вернадского, д.78, РТУ МИРЭА, кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»
Телефон: +7 961-698-22-79
E-mail: maksimova@mirea.ru

Подпись Максимовой Елены Александровны, заведующего кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» Федерального государственного бюджетного образовательного учреждения высшего образования "МИРЭА - Российский технологический университет", доктора технических наук, доцента заверяю: