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

Использование в современных компьютерных сетях большего количества разнообразных сетевых сервисов и приложений, различного аппаратного и программного обеспечения приводит к лавинному росту разнородного по объему и характеру сетевого трафика, в том числе, связанным с мобильными приложениями, осуществляющими распространение противоправного, нежелательного или вредоносного контента. Решение задачи точной идентификации и классификации подобных приложений и протоколов приобретает особую актуальность в связи с широким распространением мобильных устройств. Учитывая то, что сетевой трафик несет информацию о пользователе и его предпочтениях, решение этой задачи приобретает дополнительный экономический и социальный эффект. Исходя из вышеизложенного следует, что исследования в области классификации противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом режиме проводимые в диссертационной работе, являются весьма актуальными.

Основные задачи, решаемые в диссертационной работе, следующие:

1) разработка нового алгоритма классификации на основе использования искусственных нейронных сетей в виде автокодировщика;
2) разработка модели обнаружения «смены концепта» в наблюдаемых атрибутах при классификации мобильных приложений,

осуществляющих распространение противоправного, нежелательного или вредоносного контента, на основе анализа сетевого трафика;

3) разработка алгоритмов классификации мобильных приложений на основе анализа сетевого трафика в потоковом режиме с «конечной» и «бесконечной» памятью на базе созданных репрезентативных выборок;
4) разработка программного комплекса для автоматизированной классификации мобильных приложений с помощью анализа сетевого трафика.

Представленные в автореферате результаты соответствуют поставленным задачам, достоверны, содержат научную новизну и являются практически значимыми. Результаты диссертации в достаточной степени апробированы на конференциях различного уровня и представлены в публикациях. Достоверность полученных результатов подтверждается результатами моделирования, публикациями в журналах из списка ВАК РФ, а практическая значимость – актами внедрения разработанного программного обеспечения в АО «Лаборатория Касперского», внедрением результатов в образовательный процесс МТУСИ.

Автореферат написан грамотным, доступным языком. Вместе с тем, необходимо отметить следующие замечания к автореферату:

1) в тексте постоянно подчеркивается направленность на классификацию «противоправных, нежелательных и вредоносных» приложений, в связи с чем неясно, в чем отличие от классификации приложений по другим критериям, и какие принципиальные особенности рассматриваемой предметной области с точки зрения параметров анализируемого трафика и др.;
2) автор часто использует термин «смена концепта», но не приводится научного определения данного понятия, по-видимому связанному с потерей стационарности процессов, характеризующих трафик;
3) в качестве одного из показателей научной новизны работы заявляется «алгоритм обнаружения смены концепта,... отличающийся от известных алгоритмов учетом «старения» данных», однако далее по тексту эта особенность («старение данных») не раскрывается в явном виде;

4) автор упоминает строгое понятие «вероятность» применительно к оценке вероятности (эмпирической вероятности или просто частоте) (с. 8); при этом снижение «вероятности» ложной классификации оценивается в «разах», в то время как уменьшение «вероятности» правильной классификации – в абсолютных единицах, что несколько затрудняет объективное сравнение двух оценок;
5) не совсем понятен термин «интенсивность» ошибок I рода (с. 8).

Несмотря на указанные недостатки, судя по автореферату, можно считать, что диссертация выполнена на высоком научном уровне и соответствует специальности 2.3.6, отвечает требованиям ВАК РФ, а ее автор, Барков Вячеслав Валерьевич, заслуживает присвоения ему ученой степени кандидата технических наук по специальности 2.3.6 - методы и системы защиты информации, информационная безопасность.

Я, Басараб Михаил Алексеевич, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Доктор физико-математических наук (01.04.03 – радиофизика), доцент (05.13.19 – методы и системы защиты информации, информационная безопасность), заведующий кафедрой информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»

Басараб Михаил Алексеевич

«8» ноября 2024 г.

ФГБОУ ВО МГТУ им. Н.Э. Баумана
105005, г. Москва, ул. 2-я Бауманская, д. 5, корп. 1
+7 (499) 263-69-36
basarab@bmstu.ru
https://bmstu.ru

подпись оппонента заверяю: