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

В диссертации Баркова В.В. рассмотрена актуальная задача классификация противоправных и нежелательных мобильных приложений методами машинного обучения, имеющая важное прикладное значение. В работе рассмотрены вопросы блокирования доступа к нелегальной, экстремистской, антисоциальной информации, предотвращения утечки конфиденциальной информации через Интернет и др.

Известные в настоящее время традиционные методы классификации сетевого трафика основаны как на номерах портов, так и на информационной нагрузке, связаны с прямым изучением сетевых пакетов. При наличии полного и помеченного тренировочного набора данных, целесообразно строить классификатор, используя технологии машинного обучения (ML - Machine Learning) и интеллектуального анализа данных (Data Mining), оказавшиеся наиболее эффективными. Создание «идеального» классификатора невозможно, пока не будут решены проблемы, присущие данной области: отсутствие общего, репрезентативного набора исходных данных, который мог бы стать стандартным для исследований в данной области.

Внедрение в практику предложенных в работе подходов, позволит производить классификацию, анализ и фильтрацию сетевого трафика вредоносных и нежелательных приложений с более высокой эффективностью в соответствии с предложенными показателями, по сравнению с другими методами классификации сетевого трафика, такими как Deep Packet Inspection (DPI) или анализ номеров портов. Все это подтверждает актуальность настоящего исследования по эффективной классификации IP-трафика на основе метода машинного обучения.

Можно отметить, что соискателем в работе получен ряд новых и оригинальных результатов.

- Впервые создан ***алгоритм классификации*** мобильных

приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, состоящий из последовательно включенных АК и типовой модели классификации, ***не требующий разметки фоновых приложений*** в случае их внезапного появления.

- Впервые ***разработан алгоритм обнаружения смены концепта*** и классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента в потоковом режиме с накоплением и обработкой в скользящем окне в условиях ограниченной памяти, ***отличающийся от известных алгоритмов учетом «старения» данных.***

К практической значимости результатов, полученных в работе, следует отнести следующие.

- Сформирована экспериментальная база данных сетевого трафика мобильных приложений, которая может быть использована в системах обнаружения вторжений, для блокировки мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, в том числе приложений, использующих шифрование сетевого трафика;
- Разработано программно-аппаратное обеспечение, реализующее алгоритмы классификации в потоковом режиме.

Основные положения диссертации докладывались и обсуждались на многих научно- технических конференциях. Результаты работы отражены в 18 научных публикациях, из них 5 статей опубликованы в ведущих рецензируемых научных журналах, рекомендованных ВАК для изложения основных научных результатов, а также использовались в научно-исследовательских работах и учебном процессе.

В качестве замечаний к автореферату можно отметить следующее:

1. В автореферате не уделено должного внимания вопросу выбора длины обучающих последовательностей при обучении автокодировщиков?
2. Из автореферата осталось не ясным, из каких соображений осуществлялся выбор количества внутренних слоев автокодировщиков и количество нейронов в них.

Указанные недостатки носят непринципиальный характер и не снижают ценности представленной работы.

В целом, диссертационная работа Баркова В.В выполнена на достаточно высоком научном уровне, содержит признаки фундаментальности выполненных исследований, характеризуется новизной и достоверностью, теоретической и практической значимостью. Результаты диссертации опубликованы и апробированы.

Таким образом, на основе содержания автореферата можно сделать вывод, что диссертационная работа удовлетворяет требованиям «Положения

о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 г. №842 (в редакции Постановления Правительства Российской Федерации от 26 сентября 2022 года № 1690), предъявляемым к кандидатским диссертациям. Соискатель Барков Вячеслав Валерьевич заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

Д.т.н., профессор,
профессор кафедры автоматики и
процессов управления
СПбГЭТУ «ЛЭТИ» Душин Сергей Евгеньевич

Я, Душин Сергей Евгеньевич, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

a. Душин Сергей Евгеньевич;
b Доктор технических наук, специальность 05.13.01 Управление в технических системах, профессор;
СПбГЭТУ «ЛЭТИ», профессор;
c ул. Профессора Попова, дом 5 литера Ф, Санкт-Петербург, Россия, 197022, +7 812 234-46-51
info@etu.ru

« 6 » ноября 2024г.

Подпись профессора Душина Сергея Евгеньевича, удостоверяю.