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 противоправного контента, нежелательных и вредоносных приложений в сетевом трафике, генерируемом в том числе мобильными устройствами приобретает особую актуальность.

Для сотовых операторов информация об использовании тех или иных приложений пользователями сети необходима для составления статистики по наиболее часто используемым. Это обеспечивает не только мониторинг состояния сети и выявление сбоев, но и при необходимости ограничение доступа к сетевым ресурсам, которые с точки зрения информационной безопасности могут нанести вред

Для точной классификации в работе используется набор трафика нежелательных или вредоносных мобильных приложений, полученные с помощью разработанного программного комплекса программного комплекса (ПК) «для автоматизации процесса классификации мобильных приложений с помощью анализа сетевого трафика. ПК включает сервер баз данных, сервер приложений, Web-приложение и клиентское программное обеспечение (ПО) для мобильных устройств под управлением ОС Android. Рассмотрены нежелательные и вредоносные мобильные приложения, использующие шифрование сетевого трафика при передаче по сети, а также данные, содержащие смешанный трафик снятые в разное время и в разных точках сети.

Актуальность темы диссертации Баркова В. В. обусловлена ограниченностью традиционных методов, привела к альтернативным подходам точной и эффективной классификации противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом режиме.

Целью диссертационной работы Баркова В. В. является повышение эффективности классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента, на основе анализа сетевого трафика методами машинного обучения в потоковом режиме.

В работе предложен новый оригинальный подход обработки нежелательных приложений в режиме реального времени на основе модели обнаружения смены концепта (МОСК). Показано, что он может осуществляться не только на этапах обучения и тестирования, но и на этапе предсказания. Обнаружение смены концепта заключается в определении приложений, статистические характеристики которых значительно изменяются во времени, приводя к снижению качества классификации.

Реализация предложенного в работе алгоритма обнаружения смены концепта реализована на языке программирования Python. Показано, что использование МОСК позволяют снизить значительно снизить вероятность ошибки классификации.

Практическая ценность работы подтверждена разработкой специализированного программного обеспечения, реализующего методы машинной обучения в реальном масштабе времени для АО «Лаборатория Касперского» при разработке межсетевых экранов, а также в учебном процессе МТУСИ .

Достоверность полученных в диссертации научных результатов подтверждена результатами экспериментальных измерений анализируемых приложений, вычислительным экспериментом, а также широким обсуждением работы, апробацией ее основных научных положений на международных и всероссийских научно-технических конференциях.

К недостаткам автореферата можно отнести следующее :

Из автореферата осталось до конца непонятно, как алгоритмы классификации, рассмотренные в диссертационной работе, позволяют учесть изменение статистических характеристик вредоносного контента в потоковом режиме.

Указанное замечание не снижает общей положительной оценки диссертационной работы Баркова В. В.

Изложенное в автореферате позволяет сделать вывод, что представленная к защите диссертационной работа является завершенной научно-квалификационной работой, которая по своей актуальности, научной новизне и практической значимости соответствует требованиям «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям.

Диссертация соответствует специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, а ее автор Барков В. В. заслуживает присуждения ему ученой степени кандидата технических наук.

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

Грудинин Владимир Алексеевич
Кандидат технических наук
Специальность 05.12.04 - Радиотехника, в том числе системы и устройства телевидения
ООО «Дигитон», генеральный директор
Юридический адрес: 194156 Санкт-Петербург, Светлановский пр. д. 2 пом. 100
Фактический адрес: Ленинградская Область Приозерский район, п. Сосново,
ул.Механизаторов,д.11 оф.3,3

Телефон +7 901 3701241
Электронный адрес: grudinin@itmo.ru

Грудинин Владимир Алексеевич

«8» ноября 2024г.