Экз. № 1

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 мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, содержание которого противоречит законодательству Российской Федерации приобретает особую актуальность в связи с активным развитием мобильных устройств. Поэтому задача мониторинга и классификации приложений в потоковом режиме методами машинного обучения, решение которой позволит обеспечить ограничение доступа к подобным сетевым ресурсам является безусловно актуальной.

Целью диссертационного исследования является повышение эффективности классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, на основе анализа сетевого трафика методами машинного обучения в потоковом режиме.

Автором в работе получен ряд новых и оригинальных результатов, среди которых можно выделить следующие:

1) Статистическую модель обнаружения смены концепта при классификации мобильных приложений на основе анализа сетевого трафика, отличающаяся от известных включением АК в качестве базовой модели обнаружения смены концепта, в котором момент наступления смены концепта определяется посредством оценок ошибок восстановления анализируемых приложений и превышения пороговых значений.

2) Новый алгоритм обнаружения смены концепта мобильных приложений в потоковом режиме с обработкой в скользящем окне в режиме накопления с «конечной памятью», как с равномерной, так и неравномерной интенсивностью поступления данных, отличающийся от известных учетом «старения» данных в окне обработки и негауссовским характером изменяющихся параметров классифицируемых приложений.

3) Модифицированный алгоритм Adaptive Random Forest (MARF) со встроенной моделью обнаружения смены концепта, позволяющей обнаруживать смену концепта не только во время обучения, но и во время предсказания, т.к. не использует истинные метки, осуществляет классификацию быстрее чем алгоритмы Random Forest (RF), Hoeffding Adaptive Tree (HAT), K nearest neighbors (RNN), Oza Bagging (OB).

Диссертация соответствует п.15. «Методы и модели выявления и противодействия распространению ложной и вредоносной информации» и п.16. «Принципы и решения

(технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» паспорта специальности 2.3.6.

Достоверность результатов диссертационной работы подтверждается публикациями и широким обсуждением основных положений со специалистами на научных конференциях и семинарах.

Результаты работы отражены в 18 научных публикациях, из них 5 статей опубликованы в ведущих рецензируемых научных журналах, определенных ВАК для изложения основных научных результатов, а также использовались в научно-исследовательских работах и учебном процессе.

По автореферату имеется следующее **замечание**:

1. Недостаточно подробно дано пояснение, какие имеются ограничения при выполнении обучения предлагаемых математических моделей для случая современных целенаправленных атак и приложений (APT атак), имеющих строго уникальный характер.

2. Автореферат содержит упоминание о разработанном программном комплексе, однако описание его архитектуры и функциональных возможностей требует детализации. Например, было бы полезно упомянуть, как осуществляется интеграция компонентов и каким образом обеспечивается её масштабируемость для работы с реальным трафиком.

В целом, судя по автореферату, несмотря на указанное замечание, диссертационная работа Баркова Вячеслава Валерьевича является завершенной научно-квалификационной работой и соответствует требованиям п. 9 «Положения о присуждении ученых степеней», предъявляемых к кандидатским диссертациям, 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, Козачок Александр Васильевич , даю согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

Сотрудник Академии ФСО России
доктор технических наук, доцент
05.13.19 (2.3.6) Методы и системы защиты информации, информационная безопасность

Козачок Александр Васильевич

«14» ноября 2024 г.

Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России)
Тел.: +7(4862) 54-94-99
E-mail: a.kozachok@academ.msk.rsnet.ru
Адрес: Россия, 302020, г. Орёл, ул. Приборостроительная, д. 35

Подпись сотрудника Академии ФСО России доктора технических наук, доцента Козачка Александра Васильевича ЗАВЕРЯЮ.

Руководитель кадрового аппарата Академии ФСО России

А.Б. Семибратов