В диссертационный совет 24.2.385.09 при Федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна»

ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертационную работу Баркова Вячеслава Валерьевича на тему «Классификация противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом режиме», представленную 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, приобретает особую актуальность в связи с активным развитием мобильных устройств. Под противоправным контентом понимается информация, содержание которой противоречит законодательству Российской Федерации. Федеральное законодательство предусматривает порядок ограничения к таким ресурсам в сети Интернет и к соответствующим программным приложениям.

Для решения подобных задач широкое распространение получили методы интеллектуального анализа данных (Data Mining, DM) и машинного обучения (Machine Learning, ML), позволяющие адаптироваться к непрерывно изменяющейся структуре Интернет-ресурсов и учитывающие специфику сетевого трафика. Внедрение таких методов позволяет с достаточно высокой эффективностью производить классификацию, анализ и фильтрацию сетевого трафика мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента.

Отсутствие полной и достоверной информации о структуре фонового трафика значительно снижает качество классификации интересуемых мобильных приложений. Известным методом повышения качества классификации является использование архитектуры искусственных нейронных сетей (ИНС) автокодировщик (АК).

Вышесказанное обусловливает актуальность настоящего исследования, направленного на повышение эффективности классификации трафика мобильных приложений методами машинного обучения в потоковом режиме.

Исследования направлены на повышение эффективности классификации

мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента. 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.

Оценивая выполнение поставленных перед диссертантом задач, следует отметить их широкий научный диапазон, необходимость системного подхода, современного математического аппарата и применения методов машинного обучения. Увлечённость, умение критически оценивать результаты своих исследований – качества, которые проявил диссертант в ходе выполнения работы. Полученные Барковым В.В. результаты свидетельствуют, что он обладает качествами, необходимыми для научной деятельности.

К новым научным результатам диссертационной работы можно отнести:

- Методику отбора значимых атрибутов классификации, обеспечивающую повышение качества классификации, достоверность классификации мобильных приложений, осуществляющих шифрование сетевого трафика, более 90% при ограниченном размере обучающей выборки (300 потоков с 16-58 пакетами в каждом, в зависимости от приложения), в то время как общепринятые подходы предполагают расчет характеристик по данным всего потока. Предложенная методика является инвариантной по отношению к разным типам трафика.
- Алгоритм классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, состоящий из последовательно включенных АК и типовой модели классификации, обеспечивает в условиях априорной неопределенности и неконтролируемого фонового трафика повышение достоверности (accuracy) классификации приложений на 7% по сравнению с известными алгоритмами, не требуя разметки фоновых приложений в случае их внезапного появления.
- Модель обнаружения смены концепта классифицируемых мобильных приложений, отличающаяся от известных включением АК (для каждого приложения), в которой момент смены концепта определяется по ошибкам восстановления анализируемых мобильных приложений и превышению пороговых значений, что повышает точность обнаружения смены концепта в потоковом режиме.

- 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 для равномерной и неравномерной интенсивности поступления данных, отличающийся от известных алгоритмов учетом «старения» данных.
- Модифицированный адаптивный MARF в отличие от стандартного алгоритма ARF, использующего модель обнаружения смены концепта только на этапе обучения и использующего истинные метки класса, позволяет обнаруживать смену концепта на этапе предсказания.

Практическая значимость работы заключается в разработке алгоритмов и реализации программного комплекса для классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, путём анализа сетевого трафика в потоковом режиме в условиях априорной неопределенности состава и числа классифицируемых приложений, в условиях смены концепта. Сформированная 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.

Результаты исследований, посвящённые классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, связаны с научным направлением кафедры «Информационная безопасность» МТУСИ, подтверждаются соответствующими актами внедрения, используются в АО «Лаборатория Касперского» при разработке межсетевых экранов и в учебном процессе МТУСИ в виде программного комплекса для исследования алгоритмов классификации трафика мобильных устройств методами машинного обучения и обучающих лабораторных работах.

В целом, диссертационная работа Баркова В.В. представляет собой целостное исследование, включающее постановку и решение актуальной научной задачи классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, заключающееся в разработке модели классификации мобильных приложений в условиях априорной неопределённости о составе приложений, модели обнаружения смены концепта с использованием автокодировщиков и внедрении её в алгоритм Adaptive Random Forest для классификации

нестационарных потоков в режиме online. Это свидетельствует о зрелости и самостоятельности диссертанта как научного работника.

Останавливаясь на характеристике общественной и научно-педагогической деятельности диссертанта, следует отметить, что Барков В.В. за время работы над диссертацией проявил себя высококвалифицированным специалистом в области информационной безопасности, способным к самостоятельным исследованиям.

Диссертация Баркова Вячеслава Валерьевича полностью соответствует всем требованиям пунктов 9-14 "Положения о присуждении ученых степеней" ВАК Минобрнауки России, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук.

Считаю, что автор диссертации заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» (технические науки).

Научный руководитель:
Заслуженный деятель науки РФ,
доктор технических наук
(05.12.21 – Радиотехнические системы специального назначения, включая технику СВЧ),
профессор,
заведующий кафедрой
«Информационная безопасность»

Шелухин Олег Иванович

Подпись Шелухина Олега Ивановича заверяю.

Ученый секретарь
ученого совета университета

Зотова Татьяна Н

Тел. +7 (495) 957-77-31 (доб. 137)
e-mail: sheluhin52@mail.ru

«16» сентября 2024 г

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»
Адрес: 111024, г. Москва, улица Авиамоторная, 8А
Тел. +7 (495) 957-77-31
e-mail: mtuci@mtuci.ru