УТВЕРЖДАЮ:
Первый проректор
федерального государственного
автономного образовательного
учреждения высшего образования
«Южный федеральный университет»
д.х.н., доцент

Метелица Анатолий Викторович
«7» ноября 2024 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» на диссертацию Баркова Вячеслава Валерьевича «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.

1. Актуальность темы исследования

Задача выявления мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента, приобретает особую актуальность в связи с активным развитием мобильных устройств. 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, нежелательного или вредоносного контента.

Вместе с тем в известных работах, посвященных проблеме классификации приложений на основе анализа сетевого трафика, слабо учитывается требование выявления неизвестного сетевого трафика. При проектировании моделей

классификации приложений он полностью исключается в предположении наличия только известных классов, обучение осуществляется на данных из ограниченного числа классов приложений, а тестирование – с помощью других данных из тех же известных классов. Отсутствие полной и достоверной информации о структуре фонового трафика значительно снижает качество классификации интересуемых мобильных приложений.

Обобщая вышеизложенное, диссертационная работа Баркова Вячеслава Валерьевича, направленная на повышение эффективности классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента, на основе анализа сетевого трафика методами машинного обучения в потоковом режиме в условиях априорной неопределённости является ***актуальной***.

2. Цель, объект и предмет диссертационного исследования

Целью исследования является повышение эффективности классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента, на основе анализа сетевого трафика методами машинного обучения в потоковом режиме. Для достижения поставленной цели диссертантом предложено использовать искусственные нейронные сети (ИНС), в частности, автокодировщики (АК).

Объектом исследования в диссертационной работе является сетевой трафик, генерируемый мобильными приложениями.

Предметом исследования являются методы машинного обучения (ML) для классификация мобильных приложений на основе анализа сетевого трафика в условиях априорной неопределённости числа приложений.

3. Структура диссертации

Структура диссертации логична, даёт возможность последовательно и полно обосновывать выносимые на защиту научные положения. В работе обосновывается актуальность, новизна, теоретическая и практическая значимость, формируются цели и задачи, излагаются основные положения, выносимые на защиту. Даётся классификация мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента.

Диссертация содержит введение, четыре главы, заключение, список использованных источников, содержащий 118 наименования, и пять приложений. Основной текст работы изложен на 107 страницах, проиллюстрирован 25 рисунками и 26 таблицами.

4. Анализ степени обоснованности и достоверность каждого из полученных научных положений, выводов, рекомендаций и заключений, сформулированных в диссертации

Обоснованность первого положения, выносимого диссертантом на защиту, подтверждается обоснованием применения методики отбора рационального числа атрибутов на основе анализа их информативности при фиксировании допустимой вероятности ложной классификации. При этом определены ограничения на структуру анализируемых данных по числу пакетов и потоков, в то время как ***общепринятые*** подходы предполагают расчет характеристик на основе данных всего потока.

Обоснованность второго положения подтверждается новизной предложенного модифицированного алгоритма классификации мобильных приложений в условиях неконтролируемого фонового трафика. Алгоритм отличается от известных алгоритмов каскадным включением нейронной сети с архитектурой АК, и обладающей более высокой эффективностью.

Достоверность результатов подтверждается строгостью применяемого математического аппарата и результатами имитационного моделирования.

Обоснованность третьего положения подтверждается использованием хорошо апробированных моделей обнаружения смены концепта при классификации мобильных приложений на основе анализа сетевого трафика, отличающаяся от известных включением автокодировщика в качестве базовой модели обнаружения смены концепта.

Достоверность результатов подтверждается результатами компьютерного моделирования в среде Python при оценке эффективности предложенных моделей.

Обоснованность четвёртого положения подтверждается новизной предложенного алгоритма обнаружения смены концепта мобильных приложений в потоковом режиме с обработкой в скользящем окне в режиме накопления с «конечной памятью». Алгоритм отличается от известных учетом «старения» данных в окне обработки и негауссовским характером изменяющихся параметров классифицируемых приложений.

Достоверность результатов подтверждается строгостью применяемого математического аппарата, результатами компьютерного моделирования в среде Python при оценке эффективности алгоритма.

Обоснованность пятого положения подтверждается новизной предложенного модифицированного алгоритма Adaptive Random Forest (MARF) со встроенной моделью обнаружения смены концепта, что позволило осуществлять

классификацию анализируемых приложений быстрее, чем известные алгоритмы.

Достоверность результатов подтверждается строгостью применяемого математического аппарата, результатами компьютерного моделирования в среде Python при оценке эффективности алгоритма MARF.

5. Анализ новизны проведённых исследований и полученных результатов

Предложена методика отбора значимых атрибутов классификации мобильных приложений на основе анализа сетевого трафика, обеспечивающая высокую достоверность классификации приложений. Отличительным признаком новизны методики является её инвариантность по отношению к разным типам сетевого трафика.

Предложен алгоритм классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента, состоящий из последовательно включённых автокодировщиков (для каждого приложения) и типовой модели классификации. Отличительным признаком новизны алгоритма является то, что он не требует разметки фоновых приложений в случае их внезапного появления. Алгоритм обеспечивает в условиях априорной неопределенности и неконтролируемого фонового трафика повышение достоверности классификации приложений по сравнению с известными алгоритмами.

Предложена модель обнаружения смены концепта классифицируемых мобильных приложений. Отличительный признак новизны модели состоит в использовании автокодировщика в момент смены концепта, что позволяет повысить точность обнаружения смены концепта в потоковом режиме.

Предложен алгоритм обнаружения смены концепта и классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента в потоковом режиме с накоплением и обработкой в скользящем окне в условиях ограниченной памяти для равномерной и неравномерной интенсивности поступления данных. Отличительным признаком новизны алгоритма является учёт «старения» данных в окне обработки и негауссовским характером изменяющихся параметров классифицируемых приложений.

Предложен модифицированный адаптивный алгоритм Adaptive Random Forest (MARF), обеспечивающий обнаружение смены концепта на этапе предсказания. Отличительный признак новизны алгоритма состоит в использовании предложенной модели обнаружения смены концепта как на этапе

обучения, так и на этапе предсказания.

Перечисленные результаты диссертационного исследований являются новыми и достоверными.

6. Практическая значимость результатов работы

Практическая значимость результатов исследований заключается в том, что разработанные алгоритмы и реализации программного комплекса позволяют в потоковом режиме повысить эффективность и достоверность классификации мобильных приложений, осуществляющих распространение противоправного, вредоносного и нежелательного контента, в условиях смены концепта:

– предложенная методика отбора значимых атрибутов классификации обеспечивает достоверность классификации мобильных приложений на основе анализа сетевого трафика более 90% при ограниченном размере обучающей выборки (300 потоков с 16-58 пакетами в каждом, в зависимости от приложения);

– предложенный алгоритм классификации мобильных приложений обеспечивает в условиях априорной неопределённости и неконтролируемого фонового трафика повышение достоверности классификации приложений на 7% по сравнению с известными алгоритмами и не требует разметки фоновых приложений в случае их внезапного появления.

7. Использование результатов диссертационных исследований

Разработанные в диссертации модели, методики, алгоритмы и рекомендации могут использоваться организациями, обеспечивающими информационную безопасность информационных систем для предотвращения распространения противоправного, нежелательного или вредоносного контента. Сформированная экспериментальная база данных сетевого трафика мобильных приложений 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.

8. Внедрение результатов работы

Практические результаты диссертационных исследований внедрены в АО «Лаборатория Касперского» при разработке межсетевых экранов, а также в учебный процесс МТУСИ, что подтверждается соответствующими актами внедрения.

9. Апробация работы и публикации по диссертации

Основные результаты диссертационных исследований обсуждены и одобрены на конференциях: международная научно-техническая конференция «Телекоммуникационные и вычислительные системы – 2018»; международная конференция «Technology & entrepreneurship in digital society»; научно-техническая конференция РОСИНФОКОМ-2018 «Беспроводная связь и информационная безопасность интернета»; международная научно-техническая конференция «Фундаментальные проблемы радиоэлектронного приборостроения «INTERMATIC-2018»; IX Всероссийская научно-техническая конференция «Безопасные информационные технологи»; международная научно-техническая конференция «Systems of signals generating and processing in the field of on board communications - 2019»; II Всероссийская научная школа-семинар «Современные тенденции развития методов и технологии защиты информации».

Основные положения диссертации опубликованы в 18 научных печатных работах, в том числе: 5 – в научных журналах перечня ВАК; 1 – в научных рецензируемых изданиях по базе Scopus; 11 – в материалах конференций и других изданиях. Получено свидетельство о Государственной регистрации программы для ЭВМ. Среди опубликованных работ одна написана лично диссертантом (12 страниц), 4 – в соавторстве только с научным руководителем. В 12 опубликованных работах среди соавтором одним из двух также является научный руководитель диссертанта.

Исходя из апробации результатов исследований, можно сделать вывод об их качественном обсуждении и апробации.

10. Анализ автореферата диссертации

Автореферат диссертации соответствует основным положениям диссертации и достаточно логично отражает её содержание.

11. Соответствие работы паспорту научной специальности

Диссертация соответствует двум пунктам паспорта специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность (технические науки)»:

п. 13. «Методы и модели выявления и противодействия распространению ложной и вредоносной информации»;

п. 15. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

12. Замечания по диссертации

Замечание 1. Утверждается, что предложенные алгоритмы классификации справляются с потоками, принадлежащими к другим категориям более эффективно, чем те, которые использованы диссертантом для обучения. Однако доказательство в тексте не представлено.

Замечание 2. В главе 2 анализируется конкретная структура автокодировщика с тремя слоями и размерностью внутреннего слоя равной 7. Однако отсутствует обоснование такого выбора размерности внутреннего слоя автокодировщика.

Замечание 3. В предложенном в главе 3 алгоритме обнаружения смены концепта с учётом старения данных, введён параметр λ, характеризующий некий пороговый уровень. Однако никаких соображений о его назначении и о выборе его значения не указано.

Замечание 4. Не ясно, как при проведении эксперимента обеспечивается конфиденциальность проверяемых данных и соблюдается законодательство страны.

Отмеченные недостатки носят частный характер и, в целом, не влияют на высокое качество представленной на отзыв диссертационной работы.

13. Заключение по работе

Несмотря на отмеченные замечания диссертационная работа Баркова Вячеслава Валерьевича может быть оценена положительно.

Диссертационная работа Баркова Вячеслава Валерьевича «Классификация противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом режиме» по актуальности, научной новизне, теоретической и практической значимости соответствует требованиям п. 9-14 «Положения о присуждении ученых степеней» ВАК Минобрнауки России, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, так как является научно-квалификационной работой, в которой изложены научно обоснованные технические и программные решения в области классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного и вредоносного контента, имеющие существенное значение для развития систем обеспечения информационной безопасности страны, использующих методы интеллектуального анализа данных.

Тема и содержание диссертации «Классификация противоправных и нежелательных мобильных приложений методами машинного обучения в

потоковом режиме» полностью соответствует выбранной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)».

Барков Вячеслав Валерьевич заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки).

Диссертационная работа Баркова Вячеслава Валерьевича обсуждена на заседании кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» 30 октября 2024 года (протокол заседания № 7).

Зав. кафедрой информационной безопасности
телекоммуникационных систем,
доктор технических наук (05.12.20 «Оптические
системы локации, связи и обработки информации»),
профессор

Румянцев Константин Евгеньевич[1]

4 ноября 2024 г.

Институт компьютерных технологий и информационной безопасности
Инженерно-технологической академии
Федерального государственного автономного образовательного учреждения
высшего образования «Южный федеральный университет»
347922, Ростовская область, г. Таганрог, ул. Чехова, 2, корпус "И" ИТА ЮФУ, оф. Г-207, Г-211
+7(863) 305-19-90

Федеральное государственное автономное образовательное учреждение высшего образования
«Южный федеральный университет»
344006, Ростовская обл., г. Ростов-на-Дону, ул. Большая Садовая, 105/42
+7(863) 218-40-00 доб. 30039
info@sfedu.ru