ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.385.09, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА», МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 10.12.2024 г. № 3

О присуждении Баркову Вячеславу Валерьевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Классификация противоправных и нежелательных мобильных приложений методами машинного обучения в потоковом режиме» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки) принята к защите 08.10.2024 г., (протокол заседания №2) диссертационным советом 24.2.385.09, созданным на базе федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна» Министерства науки и высшего образования Российской Федерации, расположенного по адресу 191186, г. Санкт-Петербург, ул. Большая Морская, д. 18, приказ о создании диссертационного совета № 246/нк от 20.03.2024 г.

Соискатель Барков Вячеслав Валерьевич 3 мая 1990 года рождения, в 2013 году окончил с отличием бакалавриат в федеральном государственном образовательном бюджетном учреждении высшего профессионального образования «Московский технический университет связи и информатики» по направлению подготовки «Информатика и вычислительная техника», в 2015 году

окончил с отличием магистратуру в федеральном государственном образовательном бюджетном учреждении высшего профессионального образования «Московский технический университет связи и информатики» по направлению подготовки «Информатика и вычислительная техника», в 2019 году окончил обучение в аспирантуре Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики» по направлению 11.06.01 «Электроника, радиотехника и системы связи», получил квалификацию «Исследователь. Преподаватель-исследователь». Справка о сдаче кандидатских экзаменов по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки) выдана в 2023 году Ордена Трудового Красного Знамени федеральным государственным бюджетным образовательным учреждением высшего образования «Московский технический университет связи и информатики». С 25.01.2019 г. по настоящее время работает старшим преподавателем кафедры «Информационная безопасность» Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Диссертация выполнена на кафедре «Информационная безопасность» Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Научный руководитель – Шелухин Олег Иванович, заслуженный деятель науки РФ, доктор технических наук, профессор, Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики», кафедра «Информационная безопасность», заведующий кафедрой.

Официальные оппоненты:

Лаврова Дарья Сергеевна, доктор технических наук, доцент, федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», Высшая школа кибербезопасности, Институт компьютерных наук и кибербезопасности, профессор.

Красов Андрей Владимирович, кандидат технических наук, доцент, федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», кафедра «Защищенные системы связи», заведующий кафедрой, доцент.

дали положительные отзывы на диссертацию.

Ведущая организация – федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» Министерства науки и высшего образования Российской Федерации, г. Ростов-на-Дону, в своем положительном отзыве, подписанном заведующим кафедрой информационной безопасности телекоммуникационных систем, Института компьютерных технологий и информационной безопасности Инженерно-технической академии, доктором технических наук, профессором Румянцевым Константином Евгеньевичем и утвержденным первым проректором, доктором химических наук, доцентом Метелицей Анатолием Викторовичем, указала, что 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).

Соискатель имеет 18 опубликованных работ по теме диссертации, из них в рецензируемых научных изданиях, рекомендованных ВАК РФ, опубликовано 5 работ (в т.ч. 2 статьи без соавторов), в изданиях, входящих в международную базу Scopus – 1, свидетельство о регистрации программы для ЭВМ – 1.

Наиболее значимые научные работы по теме диссертации:

1. **Барков, В. В.** Классификации противоправных и нежелательных мобильных приложений с помощью модифицированного алгоритма Adaptive Random Forest в условиях смены концепта // Вестник Санкт-Петербургского государственного университета технологии и дизайна: Серия 1. Естественные и технические науки. 2024. № 2. С. 64–68. Авторский вклад 100%.

2. **Барков, В. В.** Повышение эффективности классификации противоправных и нежелательных мобильных приложений с использованием автокодировщиков // Вестник Санкт-Петербургского государственного университета технологии и дизайна: Серия 1. Естественные и технические науки. 2024. № 1. С. 95–99. Авторский вклад 100%.

3. Шелухин, О. И., **Барков, В. В.**, Маторин, Ф. А. Повышение эффективности классификации противоправных и нежелательных приложений в условиях фонового трафика с помощью автокодировщиков // Вестник Санкт-

Петербургского государственного университета технологии и дизайна: Серия 1. Естественные и технические науки. 2023. № 3. С. 159–165. Авторский вклад 60%.

4. Шелухин, О. И., **Барков, В. В.**, Симонян, А. Г. Обнаружение дрейфа концепта при классификации мобильных приложений с использованием автокодировщиков // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 20–29. Авторский вклад 60%.

5. Шелухин, О. И., **Барков, В. В.**, Полковников, М. В. Сравнительный анализ алгоритмов оценки количества и структуры атрибутов в задачах классификации мобильных приложений // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 90–100. Авторский вклад 50%.

6. Sheluhin, O. I., Erokhin, S. D., Osin, A. V., **Barkov, V. V.** Experimental Studies of Network Traffic of Mobile Devices with Android OS // Systems of Signals Generating and Processing in the Field of on Board Communications. 2019. Авторский вклад 50%. (Scopus).

На диссертацию и автореферат поступили положительные отзывы без замечаний принципиального характера от: доктора технических наук, профессора, начальника научно-образовательного центра «Безопасность интеллектуальных киберфизических систем» института интеллектуальных кибернетических систем федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ» **Дворянкина Сергея Владимировича**; кандидата технических наук, начальника отдела аудита информационной безопасности Департамента информационной безопасности акционерного общества "Финансы, информация, технология" **Васильева Романа Александровича**; кандидата технических наук, генерального директора ООО «Дигитон», **Грудинина Владимира Алексеевича**.

Также поступили положительные отзывы, содержащие следующие вопросы и замечания:

1. от кандидата технических наук, начальника НИО-6 федерального государственного унитарного предприятия «Научно-исследовательский институт «Квант» **Самарина Николая Николаевича: «**1) Как известно, современные

сетевые приложения используют механизмы шифрования, кодирования, маскировки и обфускации на различных уровнях модели OSI, в то же время этот вопрос подробно не рассматривается в автореферате. 2) В связи с тем, что автор рассматривает вопросы предотвращения утечки конфиденциальных данных через метасеть Интернет, в автореферате несколько лаконично рассмотрены отечественные сертифицированные средства контроля защищённости и мониторинга трафика по требованию безопасности информации».

2. от доктора физико-математических наук, доцента, заведующего кафедрой «Информационная безопасность» (ИУ8) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» **Басараба Михаила Алексеевича: «**1) В тексте постоянно подчеркивается направленность на классификацию «противоправных, нежелательных и вредоносных» приложений, в связи с чем неясно, в чем отличие от классификации приложений по другим критериям, и какие принципиальные особенности рассматриваемой предметной области с точки зрения параметров анализируемого трафика и др.; 2) Автор часто использует термин «смена концепта», но не приводится научного определения данного понятия, по-видимому связанному с потерей стационарности процессов, характеризующих трафик; 3) В качестве одного из показателей научной новизны работы заявляется «алгоритм обнаружения смены концепта, … отличающийся от известных алгоритмов учетом «старения» данных», однако далее по тексту эта особенность («старение данных») не раскрывается в явном виде; 4) Автор упоминает строгое понятие «вероятность» применительно к оценке вероятности (эмпирической вероятности или просто частоте) (с.8); при этом снижение «вероятности» ложной классификации оценивается в «разах», в то время как уменьшение «вероятности» правильной классификации – в абсолютных единицах, что несколько затрудняет объективное сравнение двух оценок; 5) Не совсем понятен термин «интенсивность» ошибок 1 рода (с.8)».

3. от доктора технических наук, доцента, заведующего кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» федерального государственного бюджетного образовательного учреждения высшего образования "МИРЭА - Российский технологический университет" **Максимовой Елены Александровны:** «1) При решении задачи построения алгоритмов классификации нежелательных или вредоносных мобильных приложений автор анализирует 5 наиболее значимых атрибутов без учёта IP-адресов (стр. 9). Однако в работе не описано, что они из себя представляют; 2) Из текста автореферата не ясно, каким образом и по каким признакам в работе определяются противоправные и нежелательные мобильные приложения. Не понятно, каким образом автор использует специфичные для каждого из данных видов приложений свойства; 3) На стр.12-13 автореферата обозначено, что «использование МОСК позволяет снизить вероятность ошибки классификации примерно на 5%. … Модели классификации, не использующие МОСК, допускают на 5-7% больше ошибок». Из текста автореферата не понятно каким образом получены данные оценки и не обоснованы обозначенные количественные значения».

4. от доктора технических наук, профессора, профессора кафедры автоматики и процессов управления федерального государственного автономного образовательного учреждения высшего образования "Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина)" **Душина Сергея Евгеньевича:** «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».

5. от доктора технических наук, доцента, сотрудника федерального государственного казенного военного образовательного учреждения высшего образования "Академия федеральной службы охраны Российской Федерации" **Козачка Александра Васильевича:** «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».

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и глубокими знаниями, обобщенными в ряде опубликованных научных работ по направлению диссертационного исследования, способностью определить научную и практическую ценность диссертации, а также их соответствием требованиям, предъявляемым к оппонентам и ведущей организации на основании пунктов 22 и 24 Положения о присуждении ученых степеней.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработана

— модель классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного, вредоносного контента, включающая последовательно включенные искусственную нейронную сеть, автокодировщик и типовую модель классификации, не требующая разметки фоновых приложений, обеспечивающая повышение достоверности классификации по сравнению с известными;

— модель обнаружения смены концепта с накоплением и обработкой в скользящем окне в условиях ограниченной памяти для равномерной и неравномерной интенсивности поступающих данных, учитывающая «старение» данных в окне обработки, с негауссовским характером изменяющихся атрибутов классифицируемых приложений;

предложена методика отбора значимых атрибутов классификации мобильных приложений на основе анализа сетевого трафика, обеспечивающая высокую достоверность классификации, инвариантная по отношению к разным типам сетевого трафика;

доказана применимость разработанной методики классификации и моделей обнаружения смены концепта в алгоритмах потоковой классификации при ограниченном количестве потоков и пакетов в потоке;

введены новый метод и алгоритм обнаружения смены концепта для классификации мобильных приложений на основе разработанных моделей обнаружения;

Теоретическая значимость исследования обоснована тем, что:

доказана эффективность разработанных моделей и алгоритмов классификации и обнаружения смены концепта по сравнению с известными;

применительно к проблематике диссертации результативно использованы методы интеллектуальной обработки данных, включая классические методы машинного обучения и методы глубокого обучения искусственных нейронных сетей, в частности, автокодировщиков;

изложены особенности архитектуры автокодировщиков при решении задач классификации и обнаружения смены концепта анализируемых приложений;

раскрыта зависимость степени сжатия информации, характеризуемой дисперсией численных значений и среднеквадратической ошибкой восстановления атрибутов на выходе автокодировщиков от количества нейронов;

изучены методы классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного или вредоносного контента на основе анализа сетевого трафика в условиях априорной неопределенности;

проведена модернизация алгоритма Adaptive Random Forest (в работе MARF), обеспечивающего возможность использования моделей обнаружения смены концепта на основе анализа статистических характеристик атрибутов,

который не требуют истинных меток и может осуществлять обнаружение смены концепта как на этапе обучения, так и на этапе использования.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработана и внедрена методика классификации мобильных приложений на основе алгоритмов машинного обучения, что подтверждено актами использования в АО «Лаборатория Касперского», свидетельством о регистрации программы для ЭВМ, результатами внедрения в учебный процесс ФГБОУ ВО Московского технического университета связи и информатики;

определены области и перспективы использования предложенных методик и алгоритмов применительно к задачам обеспечения информационной безопасности при учете ограничений размера обучающих выборок и количества сетевых пакетов в потоке при обучении моделей классификации мобильных приложений на основе анализа сетевого трафика;

создана система практических рекомендаций и экспериментальная база данных сетевого трафика для обучения и тестирования моделей классификации для выявления мобильных приложений, осуществляющих распространение противоправного, нежелательного и вредоносного контента;

представлены алгоритмы классификации мобильных приложений с использованием искусственных нейронных сетей и алгоритмов машинного обучения, в том числе в потоковом режиме, в виде разработанного программного комплекса «Система анализа трафика».

Оценка достоверности результатов исследования выявила:

для экспериментальных работ достоверность результатов подтверждается сходимостью данных при имитационном моделировании, с экспериментальными данными, полученными с использованием разработанного программного обеспечения, корректным использованием современного математического аппарата;

теория построена на общепринятых научных представлениях в области машинного обучения и интеллектуальной обработки данных и согласуется с опубликованными экспериментальными данными по теме диссертации;

идея базируется на анализе научно-технической литературы, производственной практике, существующих методов математического моделирования, теории вероятностей, математической статистики, методов машинного обучения, обобщении передового опыта интеллектуальной обработки данных;

использовано сравнение авторских данных и данных, полученных ранее, применительно к классификации неправомерных, нежелательных и вредоносных мобильных приложений методами машинного обучения в потоковом режиме;

установлено качественное и количественное совпадение авторских результатов с результатами, представленными в независимых источниках по тематике диссертации;

использованы современные методы сбора и обработки экспериментального сетевого трафика мобильных устройств, современные технологии защиты информации и вычислительная техника.

Личный вклад соискателя состоит в:

непосредственном участии в разработке методик и алгоритмов классификации противоправных, нежелательных, вредоносных мобильных приложений методами машинного обучения в потоковом режим; в научном анализе и обобщении полученных результатов; в формулировке выводов, а также в подготовке научных публикаций, разработке алгоритмического и программного обеспечения и его апробации в условиях АО «Лаборатории Касперского» и внедрении в учебный процесс ФГБОУ ВО Московского технического университета связи и информатики.

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 всем требованиям ВАК Минобрнауки России, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук. Работа соответствует пп. 9-14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства РФ №842 от 24 сентября 2013 г. (с изменениями и дополнениями), является законченной научно-квалификационной работой, в которой изложены научно обоснованные технические и программные решения интеллектуального анализа данных в области классификации мобильных приложений, осуществляющих распространение противоправного, нежелательного и вредоносного контента, имеющие существенное значение для развития систем обеспечения информационной безопасности страны.

Тема и содержание диссертационной работы соответствует паспорту научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки), пункту 13. Методы и модели выявления и противодействия распространению ложной и вредоносной информации, пункту 15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

В ходе защиты были заданы вопросы и высказаны замечания, на которые соискатель Барков В.В. аргументированно ответил.

Автор работы, Барков Вячеслав Валерьевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

На заседании 10.12.2024 диссертационный совет принял решение присудить Баркову Вячеславу Валерьевичу ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 8 человек, из них 3 доктора наук по научной специальности рассматриваемой диссертации, участвовавших в заседании, из 11 человек, входящих в состав совета, дополнительно введены на разовую защиту 0 человек, проголосовали: за — 8, против — нет, недействительных бюллетеней — нет.

Председатель
диссертационного совета Марковец Алексей Владимирович

Ученый секретарь
диссертационного совета Сиротина Лидия Константиновна
10.12.2024 г.