В диссертационный совет 24.2.415.04
на базе ФГАОУ ВО ТУСУР
634050, Россия, г. Томск, пр. Ленина, 40

ОТЗЫВ

на автореферат диссертации Куртуковой Анны Владимировны
«Методика и программный комплекс для идентификации автора программного кода», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Программный код в современной цифровой среде выступает не только как основа функционирования систем, но и как ключевой объект анализа при расследовании киберугроз. Актуальность темы диссертационной работы обоснована ростом рисков в области ИБ, требующих анализа больших объемов исходного и бинарного кода, включая атрибуцию авторства вредоносного ПО и выявление инсайдерских утечек. Разработка точных и устойчивых к обфускации методов стилеметрического анализа кода для обеспечения кибербезопасности на всех этапах разработки видится необходимым как для научного, так и для профессионального сообществ. Тема диссертационной работы Куртуковой А.В. является, несомненно, актуальной и представляет высокий научный и практический интерес.

Диссертационное исследование посвящено решению важной научно-технической задачи разработки инструмента, повышающего точность идентификации авторства программного кода. К наиболее значимым научным результатам диссертационной работы, отличающимся **новизной и теоретической значимостью,** следует отнести:

1. Методика идентификации авторства на основе multi-view энкодера формирует новую парадигму анализа за счет унификации различных абстракций в единый вектор с применением контрастивных потерь для межвидового выравнивания. Подход успешно преодолевает ограничения существующих аналогов, демонстрируя высокую эффективность и универсальность как для закрытого, так и для открытого множества авторов.

2. Гибридная архитектура (Inception-v1+BiGRU) для дизассемблированного кода представляет собой оригинальное решение, комбинирующее сверточные (для локальных паттернов) и рекуррентные слои (для контекста) с целью анализа низкоуровневых представлений. Архитектура инвариантна к процессам компиляции и оптимизации, что вносит существенный вклад в теорию извлечения авторских признаков из машинного кода.

3. Метод верификации авторства с адаптивной калибровкой вероятностей впервые решает проблему надежности предсказаний при решении задачи

отнесения кода конкретному автору. Применение сиамской архитектуры в связке с изотонической регрессией позволило достичь точности 0,98 (превосходя аналоги на 0,02), формируя интерпретируемый и практически значимый инструмент для систем информационной безопасности.

4. Сформированный набор данных (255 тыс. образцов, 3811 авторов, 13 языков программирования) включает четыре вида представлений кода и охватывает сложные практические условия: командную разработку, ИИ-генерацию, обфускацию и имитацию стиля. Датасет закладывает фундаментальную базу для развития надежных методов анализа кода.

5. Глубокий анализ деградации моделей при различных трансформациях (обфускация, стандартизация кодирования, оптимизация). Доказано, что предложенные ансамблевые подходы эффективно нивелируют падение точности в условиях целенаправленного противодействия (сохраняя точность до 0,91 при оптимизации и снижая потери качества при обфускации до 11,2%).

Разработанная методика и программный комплекс обладают высокой **практической ценностью** для решения актуальных задач информационной безопасности. Во-первых, система позволяет автоматизировать процесс атрибуции вредоносного ПО и расследования инцидентов безопасности, сокращая время реагирования на угрозы и повышая эффективность работы аналитиков. Во-вторых, методика применима в контексте DevSecOps для контроля целостности кода и выявления аномальных изменений, которые могут свидетельствовать о компрометации учетных записей разработчиков или внедрении недекларированных возможностей. Это способствует снижению рисков инсайдерских угроз и несанкционированных модификаций в цепочке поставок ПО.

Кроме того, разработанное решение находит применение в области защиты интеллектуальной собственности и обеспечения академической добросовестности, позволяя выявлять плагиат в студенческих и исследовательских работах, разрешать авторские споры и объективно оценивать вклад участников проектов.

Результаты диссертационной работы внедрены в процессы компаний ООО «ТомскСофт» и ООО «НТР Томск» в г. Томске, а также в учебный процесс ТУСУРа. Результаты исследования представлены в 7 научных работах в журналах перечня ВАК и 6 в изданиях, индексируемых WoS/Scopus, а также в 1 свидетельстве о регистрации программы для ЭВМ и 2 свидетельствах о регистрации баз данных. Достоверность результатов подтверждается решением задач идентификации авторства с использованием взаимодополняющих методов машинного и глубокого обучения, сопоставлением полученных результатов с данными отечественных и зарубежных исследований, а также апробацией на конференциях и семинарах, включая международные научно-технические конференции и IEEE семинары.

Имеется несколько вопросов и комментариев:

- Система внедрена в учебный процесс ТУСУРа. Как она применяется – для проверки плагиата в студенческих работах? Какова эффективность в этом контексте?
- Для поиска в открытом множестве используется FAISS. Какой тип индекса применяется в рамках исследования?
- Как метод масштабируется на тысячи авторов? Текущие эксперименты ограничены 500 авторами в открытом множестве.

Заключение:

Диссертационная работа Куртуковой А.В. вносит значимый научный и прикладной вклад в область атрибуции программного кода в контексте кибербезопасности. Содержание работы соответствует специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность. Работа соответствует требованиям, установленным пп. 9-14 Положения о присуждении ученых степеней ВАК РФ, предъявляемым к кандидатским диссертациям, и заслуживает положительной оценки, а ее автор, Куртукова Анна Владимировна, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Даю свое согласие на обработку персональных данных.

Директор Института
компьютерных технологий и
информационной безопасности
Южного федерального
университета, доктор
технических наук, доцент,
специальность 05.13.01
Системный анализ,
управление и обработка
информации Веселов Геннадий Евгеньевич

«25» 05 2026 г.

Сведения об организации

Наименование организации: Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» (ФГАОУ ВО «ЮФУ»):

Адрес: 344006, Россия, Ростовская обл., г. Ростов-на-Дону, ул. Большая Садовая, д. 105, корп. 42.

Телефон: +7 (863) 218-40-00

Сайт: https://sfedu.ru

Электронная почта: info@sfedu.ru