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

Отзыв
на автореферат диссертации Романова Александра Сергеевича
«Методология идентификации автора текстовой информации для решения задач кибербезопасности», представленную на соискание ученой степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Актуальность

А.С. Романов в своей диссертации решает актуальную проблему информационной безопасности – создание методологии идентификации автора текста, включая как естественно-языковые тексты, так и исходный код программ. В условиях распространения деструктивного контента, ложных и вымышленных новостей, неэтичного использования генеративных моделей, проблема атрибуции текстовой информации приобретает не только академическую, но и прикладную значимость в таких областях, как криминалистика, судебная лингвистика, противодействие экстремизму и защита интеллектуальной собственности в цифровом пространстве.

Научная новизна

Автор впервые предложил комплексную методологию идентификации автора текста, включающую:

1. Модель создания текста в киберсреде.
2. Алгоритмы идентификации автора естественного и искусственного текста, основанные на моделях GRU+CNN, CodeBERT, SVM с отбором признаков.
3. Методики, апробированные в том числе на обфусцированных и сгенерированных текстах, учитывающие задачу верификацию при открытом и закрытом множестве кандидатов.
4. Методики идентификации пола, возраста и идеологии с учетом современных социокультурных атрибутов автора.

Обоснованность исследования

Работа строится на обширной теоретической базе (более 300 источников) и включает формализацию понятий среды, авторских признаков, их связи с типами текстов. Применены как классические методы машинного обучения (SVM, RS, GA), так и глубокие нейросетевые архитектуры

(GRU+CNN, BERT, CodeBERT). Приведены результаты экспериментов, проведенных с использованием 10-фолдовой кросс-валидации, анализа значимости различий (*p*-значение, диаграмма Демшара), а также представлены собственные корпуса текстов для всех описанных в диссертации задач (данные из GitHub, социальных сетей, классические художественные тексты). Это подтверждает высокий уровень доказательной базы и достоверности результатов.

Практическая значимость

Среди достоинств работы отмечу высокую степень апробации, публикационную активность (31 публикацию в журналах ВАК и Scopus/WoS), внедрение методик и ПО в деятельность организаций для решения практических задач, охват большого числа проблемных вопросов кибербезопасности (определение автора, пола, возраста, идеологии, выявление деструктивных текстов, заимствований и др.). Структура автореферата логична и последовательна, текст изложен чётко, с соблюдением научного стиля. Также впечатляют предложенные метрики, устойчивость к генеративным атакам, корректность применения терминологии.

Методики внедрены в МВД, ВУЗы, ИТ-компании, войсковую часть. Доказано улучшение точности (на 2–30% по сравнению с аналогами), особенно в сложных случаях, например, анализ образцов, созданных при помощи генерации, заимствования в академических работах, командная разработка.

Замечания и уточнения:

1. В тексте автореферата сказано, что SVM для идентификации автора исходного кода программы обучалась на множестве информативных признаков. Какие признаки входили в это множество и каким образом они отфильтровывались?

2. Почему для апробации методики определения авторства исходных кодов программ был собран собственный набор данных с хостинга GitHub, а не использовались уже существующие открытые датасеты (в тексте упоминается база Google Code Jam)?

3. Методология, представленная на рисунке 3, включает настроение пользователя, однако в автореферате не представлены результаты экспериментов по определению тональности текста.

Указанные недоработки, вероятно, вызваны необходимостью сверхконцентрации материала в автореферате и в самой диссертации отсутствуют. В целом работа производит благоприятное впечатление и заслуживает положительной оценки.

Заключение

Диссертационное исследование Романова А.С. соответствует критериям, установленным в Положении о присуждении ученых степеней, предъявляемым к докторским диссертациям, пп. 9-14. Сформулированные и решенные в ней задачи соответствуют профилю специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность. В работе изложены новые научно обоснованные технические решения, внедрение которых вносит значительный вклад в развитие страны. Считаю, что Романов Александр Сергеевич достоин присуждения ученой степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Я, Сычугов Алкесей Алексеевич, даю свое согласие на обработку персональных данных и на их включение в документы, связанные с работой диссертационного совета.

Директор ИПМКН, заведующей кафедрой «Информационная безопасность», д.т.н., доцент, 05.13.01 «Системный анализ, управление и обработка информации»

Сычугов Алексей Алекеевич

«12» сентября 2025 г.

Наименование организации: ФГБОУ ВО «Тульский государственный университет»

Адрес: г. Тула, пр. Ленина, д. 92

Телефон: 8-(4872)-25-79-50

Сайт: tulsu.ru

Электронная почта: xru2003@list.ru

Подпись Сычугова А.А. заверяю:

Подпись Сычугова А.А.
Специалист по кадровой работе
Докторова
"12" 09 2025