Отзыв

официального оппонента на диссертационную работу

Куртуковой Анны Владимировны

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

Актуальность темы диссертации

Диссертационная работа Куртуковой Анны Владимировны посвящена разработке методики и программного комплекса для идентификации автора программного кода, что представляет собой своевременное и актуальное исследование в области информационной безопасности. Актуальность работы обусловлена рядом факторов. Во-первых, инсайдерские угрозы составляют значительную долю всех инцидентов информационной безопасности, а атаки на цепочки поставок программного обеспечения демонстрируют экспоненциальный рост. Идентификация авторства кода становится критически важным инструментом для расследования инцидентов, атрибуции вредоносного ПО и выявления несанкционированных модификаций в критической информационной инфраструктуре. Во-вторых, существующие подходы к идентификации авторства демонстрируют значительные ограничения. Традиционные методы, опирающиеся на поверхностные признаки, чувствительны к обфускации, рефакторингу и стандартизации кода, а современные подходы на основе глубокого обучения, хотя и показывают высокие результаты на контролируемых наборах данных, часто деградируют при работе с реальными сложными сценариями: командной разработкой, применением строгих стандартов кодирования, использованием генеративных моделей для создания кода. В-третьих, требования нормативных документов ФСТЭК России, в частности, приказы № 239 и № 117, предусматривают необходимость обеспечения доверия к ПО, контроля целостности и управляемости жизненного цикла программных средств. Разработанная соискателем методика соответствует этим требованиям,

предоставляя инструментарий для повышения прослеживаемости происхождения кода и установления доверия к его источнику.

Анализ содержания диссертации

Общий объем диссертационного исследования составляет 178 страниц печатного текста. Работа включает введение, пять глав, заключение, список литературы и 2 приложения. Библиография включает 114 русскоязычных и англоязычных источника.

Полученные соискателем результаты изложены последовательно и логично.

Во **введении** приводятся обоснование актуальности проблемы атрибуции программного кода, формулируются цели и задачи работы. Здесь же приводятся основные защищаемые положения и ключевые результаты, а также дается оценка их научной новизны и перспектив практического применения.

Первая глава посвящена обзору работ по теме диссертационного исследования. В главе рассмотрены исследования ученых и научных групп, внесших существенный вклад в развитие методов идентификации авторства программного кода: Романова А., Богомолова Е., Стремоухова Д., Богдановой А., Burrows S., Frantzeskou E., Caliskan A., Abuhamad M., Rosenblum N., Choi S., Alrabaee S., Álvarez-Fidalgo D., Wang N., Ilyas M. и др. На основе анализа выделяются актуальные задачи кибербезопасности, связанные с атрибуцией программного кода, и подчеркивается необходимость совершенствования существующих подходов для учета особенностей современных практик разработки ПО и потенциальных атак на методы атрибуции программного кода.

Во **второй главе** приводятся подробное описание разработанного соискателем набора данных для решения исследовательских и прикладных задач кибербезопасности в области атрибуции программного кода, а также критерии отбора репозиториев и алгоритмы сбора данных, охватывающих различные сценарии разработки ПО. Следует отметить, что авторский набор данных зарегистрирован в Роспатенте РФ, что подтверждается соответствующими свидетельствами о регистрации БД.

Третья глава посвящена методике идентификации авторства программного кода на основе multi-view представлений и контрастивного обучения, а также методам, направленным на решение задач идентификации и верификации авторства программного кода: идентификации в закрытом множестве, подразумевающей выбор наиболее подходящего варианта из строго ограниченного списка известных авторов; идентификации в открытом множестве, предполагающей сопоставление с базой данных, которое допускает, что код может принадлежать неизвестному, и позволяет воздержаться от принятия решения об авторстве; верификации авторства с калибровкой прогностических вероятностей, подразумевающей подтверждение или опровержение гипотезы о том, что программный код был написан конкретным автором-программистом.

В **четвертой главе** представлены результаты серии экспериментов по решению задач идентификации и верификации авторства программного кода в различных простых и сложных сценариях, а также в случаях атак на методы атрибуции программного кода. Методика демонстрирует высокую эффективность, позволяя достигнуть 0,97 по *F1* в случае закрытого множества из 50 авторов, 0,64 – в случае открытого множества и 0,97 – при верификации автора-программиста. Отдельный эксперимент посвящен оценке качества иерархического подхода, позволяющего сохранять высокое качество идентификации при масштабировании методики на большие множества авторов-программистов. Для множества из 500 авторов-кандидатов при применении данного подхода *F1* варьируется от 0,94 до 0,97 в зависимости от языка программирования.

Пятая глава описывает реализацию разработанной соискателем методики в виде масштабируемого программного комплекса с модульной архитектурой, включающей пять подсистем. Соискатель детализирует технологический стек, архитектурные решения и динамическую модель функционирования разработанного ПО. Программный комплекс зарегистрирован в Роспатенте РФ, внедрен и апробирован в трех организациях, в частности, в двух компаниях-разработчиках ПО и в образовательном учреждении ТУСУР, что подтверждено

соответствующими свидетельством о регистрации программы для ЭВМ и актами внедрения.

Заключение содержит ключевые результаты, полученные в процессе выполнения диссертационного исследования. Поставленные соискателем задачи выполнены в полном объеме, обозначенная цель достигнута.

Научная новизна диссертации

Диссертационная работа отличается высокой научной новизной. Соискателем разработана комплексная методика идентификации авторства программного кода, отличающаяся интеграцией четырех взаимодополняющих представлений через multi-view энкодер с межвидовым контрастивным выравниванием, предложен метод верификации авторства программного кода, отличающийся применением сиамской нейросетевой архитектурой в сочетании с адаптивной калибровкой прогностических вероятностей посредством изотонической регрессии, а также реализовано алгоритмическое обеспечение, отличающееся возможностью экстракции и кодирования четырех видов представлений программного кода и позволяющее верифицировать и идентифицировать автора программного кода в целях решения задач кибербезопасности.

Теоретическая значимость полученных результатов

Теоретическая ценность представленного исследования заключается в пересмотре классических подходов к анализу программных артефактов. Соискатель обосновывает необходимость комплексного рассмотрения кода на разных уровнях, доказывая, что индивидуальный почерк программиста остается инвариантным даже при частичной модификации программы. Работа демонстрирует проявление авторства не только в стилистике, но и в глубоких семантических и структурных паттернах. Полученные результаты расширяют теоретическую базу защиты информации в сфере анализа программных артефактов и служат фундаментом для создания адаптивных систем идентификации авторства, сохраняющих эффективность в постоянно изменяющейся программной среде.

Практическая значимость полученных результатов

1. Создан масштабный исследовательский набор данных, содержащий 255 тысяч образцов кода от 3811 разработчиков. Уникальность набора заключается в сочетании четырех типов представлений кода и моделировании реальных условий современной программной разработки.

2. Предложен метод идентификации автора программного кода в закрытом множестве, достигающий средней точности 0,97 для 13 различных языков программирования в простых случаях и 0,93 в случаях атак на методы идентификации автора программного кода.

3. Реализован метод идентификации автора программного кода в открытом множестве, демонстрирующий метрики 0,68 по *F1*-макро и 0,85 по *F1*-макро по топ-10 для выборки из 500 авторов. Использование ансамбля представлений кода позволило улучшить результат на 12-18% относительно одиночных представлений.

4. Разработан способ верификации авторства программного кода, применяющий адаптивную калибровку прогностических вероятностей на основе изотонической регрессии и достигающий точности 0,98 (на 0,02 выше аналогов).

5. Создано программное обеспечение, позволяющее извлекать и кодировать четыре вида представлений программного кода, идентифицировать и верифицировать автора программного кода в простых и сложных случаях, включая обфускацию, оптимизацию и командную разработку.

Обоснованность и достоверность научных положений, выводов и рекомендаций

Обоснованность и достоверность полученных результатов сомнений не вызывают. В своем исследовании соискатель грамотно оперирует инструментами машинного обучения и методами математической статистики. Экспериментальные серии проведены на разнообразном, объемном и сбалансированном наборе данных, охватывающим различные простые и сложные сценарии программной разработки. Для оценки эффективности разработанных методов соискатель использует стандартные метрики качества, а также проводит сопоставление полученных

результатов с работами других ученых и научных коллективов, занимающихся исследованиями в области анализа программных артефактов.

Основные итоги исследования отражены в 7 статьях в журналах ВАК и в 6 публикациях в изданиях, индексируемых Web of Science /Scopus, также получено 1 свидетельство о регистрации программы для ЭВМ и 2 – о регистрации БД.

Замечания и вопросы по диссертации

При общей положительной оценке актуальности темы, научной новизны и практической значимости диссертационной работы следует отметить ряд замечаний, требующих пояснения или уточнения.

1. Чем обоснована привязка первых двух положений, выносимых на защиту, именно к пункту 13 паспорта специальности 2.3.6, а не к пунктам 3, 16 и 17, которые непосредственно связаны с идентификацией угроз, расследованием инцидентов и безопасной разработкой ПО?

2. Экспериментальный протокол недостаточно подробно описан с точки зрения исключения утечек данных между обучающей, валидационной и тестовой выборками. Под утечкой данных понимается ситуация, при которой связанные или производные версии одного и того же объекта попадают одновременно в обучение и тестирование, что приводит к завышению метрик качества. В работе используются обфускация, оптимизация, искусственная генерация и имитация стиля, однако не раскрыто, исключалось ли попадание исходного файла и его трансформированных вариантов в разные подгруппы при перекрестной проверке. Для рассматриваемой задачи это принципиально важно, поскольку модель может выучить признаки конкретного проекта, файла, задачи или трансформации, а не устойчивые признаки авторского стиля.

3. Требует уточнения воспроизводимость экспериментов с кодом, сгенерированным и преобразованным большими языковыми моделями. Большая языковая модель представляет собой нейросетевую модель, обученную на больших корпусах текстовых и программных данных и способную генерировать программный код по текстовому запросу. В автореферате указано использование GPT-3, GPT-4 и DeepSeek для генерации кода и имитации авторского стиля, однако

не приведены точные версии моделей, даты генерации, параметры temperature, top-p, ограничения на длину ответа, число промптов и процедура проверки синтаксической и семантической корректности полученных программ. Без этих сведений воспроизводимость данного блока экспериментов существенно ограничена.

4. Каков итоговый объем сформированного набора данных: 255004 исходных образца или большее значение с учетом аугментаций? Необходимо пояснить итоговое количество примеров по категориям: исходные коды, обфусцированные образцы, искусственно сгенерированные образцы, образцы имитации стиля, APT-образцы и промежуточные представления.

5. Каким образом выбирался порог принятия решения в открытом множестве и в задаче верификации? Использовалась ли для выбора порога независимая валидационная выборка, не пересекающаяся с тестовой?

6. В тексте имеются отдельные логические и редакционные неточности, которые необходимо устранить до окончательного представления работы. В частности, формулировка о том, что при оптимизации полный ансамбль «падает с 0,93 до 0,96», логически некорректна, поскольку указанное изменение является ростом, а не падением. Также встречаются терминологические и орфографические ошибки, в том числе «соотствтенно», «искусственной-генерации», «программного в простом случае», а также неоднородное употребление терминов «точность», «F1», «F1-макро» и «эффективность».

Отмеченные недостатки не затрагивают сущности научных положений, выносимых на защиту, и не влияют на общую оценку работы, которая, несомненно, положительна.

Заключение

Диссертационная работа Куртуковой А.В. представляет собой законченную научно-квалификационную работу, отличающуюся научной новизной и практической значимостью. Соискателем сформулирована и решена важная научно-техническая задача, несущая ценность для областей кибербезопасности и компьютерной лингвистики. Решение поставленной задачи имеет научную и

практическую ценность для построения эффективных систем защиты информации. Результаты работы достаточно полно представлены в публикациях автора. Автореферат полностью соответствует содержанию диссертации. Тема диссертационной работы соответствует пунктам 5 и 13 паспорта специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Диссертация Куртуковой Анны Владимировны удовлетворяет всем требованиям пп. 9-14 «Положения о порядке присуждения ученых степеней» ВАК РФ, утвержденного постановлением Правительства РФ от 24.09.13 №842 (редакция от 16.10.2024), предъявляемых к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Я, Вульфин Алексей Михайлович, даю свое согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета, и их дальнейшую обработку.

Официальный оппонент,
доктор технических наук, профессор кафедры вычислительной техники и защиты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий»
450076, Республика Башкортостан, г.о. город Уфа, г. Уфа, ул. Заки Валиди, д. 32
Тел. 8(347)272-63-70
e-mail: vulfin.am@ugatu.su

Алексей Михайлович Вульфин

«21» 05 2026

Подпись Вульфина А.М.
Удостоверяю «21» 05 2026 г.
Начальник общего отдела УУНиТ Ахметова Ф.Ф.

Диссертация на соискание ученой степени доктора технических наук защищена в 2022 году по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность