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

Диссертационная работа Куртуковой Анны Владимировны посвящена актуальной научно-технической задаче — разработке методики и программного комплекса для идентификации автора программного кода. Значимость темы определяется современными вызовами информационной безопасности: усложнением цепочек поставок программного обеспечения, рисками инсайдерской деятельности, несанкционированного изменения кода, внедрения недекларированных возможностей, а также необходимостью защиты интеллектуальной собственности и выявления плагиата.

Научная новизна исследования состоит в разработке методики идентификации автора программного кода, основанной на multi-view подходе и объединяющей несколько представлений кода: исходный код, абстрактное синтаксическое дерево, дизассемблированный код и граф потока управления. Существенным результатом является метод верификации автора программного кода с применением сиамской нейросетевой архитектуры, контрастивного обучения и адаптивной калибровки прогностических вероятностей. Использованные методы машинного и глубокого обучения, математической статистики и вычислительного эксперимента соответствуют поставленным задачам.

Практическая значимость работы подтверждается созданием набора данных, включающего 255 тыс. образцов программного кода 3811 авторов, поддержкой 13 языков программирования и разработкой программного комплекса для идентификации и верификации авторства. Важным достоинством является проверка методики в сложных сценариях: при обфускации, оптимизации, следовании стандартам кодирования, командной разработке, имитации авторского стиля и использовании ИИ-сгенерированного кода. Достигнутые результаты — точность до 0,97 при идентификации автора в закрытом множестве и до 0,98 при верификации — подтверждают высокий научный и прикладной уровень исследования.

Автореферат изложен логично и последовательно: в нем представлены актуальность, цель, задачи, научная новизна, практическая значимость, положения, выносимые на защиту, и результаты апробации. Положительно следует отметить наличие количественных оценок, графиков и таблиц, позволяющих судить об эффективности предложенной методики. Автором проведен содержательный анализ отечественных и зарубежных исследований и выявлены ограничения существующих подходов, включая чувствительность к обфускации и ориентацию на закрытое множество авторов.

К основным достоинствам диссертации следует отнести актуальность поставленной задачи, комплексность предложенного подхода, учет закрытого и открытого множества авторов, разработку метода верификации, формирование крупного экспериментального набора данных и наличие программной реализации. Работа имеет выраженную практическую направленность и может быть востребована в задачах информационной безопасности, цифровой криминалистики и экспертизы программного обеспечения.

При общем положительном впечатлении от автореферата можно высказать отдельные замечания рекомендательного характера. Целесообразно было бы подробнее раскрыть вопрос воспроизводимости экспериментов, включая параметры обучения моделей и особенности разбиения данных, а также более развернуто показать сценарии интеграции программного комплекса в реальные процессы DevSecOps, системы контроля версий и инструменты цифровой криминалистики. С учетом быстрого развития генеративных моделей искусственного интеллекта полезно было бы подробнее обозначить пределы устойчивости методики к новым способам имитации авторского стиля. Указанные замечания не снижают общего высокого впечатления от работы.

Автореферат диссертации Куртуковой Анны Владимировны производит положительное впечатление. Судя по представленному автореферату, цель исследования достигнута, поставленные задачи решены, научная новизна и практическая значимость обоснованы, а положения, выносимые на защиту, подтверждены результатами экспериментальной апробации. Диссертационная работа соответствует основным требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее содержание соответствует специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность; автор диссертации заслуживает присуждения ученой степени кандидата технических наук.

И.о. директора ИППИ РАН,
член-корреспондент РАН М.В. Федоров

22.05.2026

Федеральное государственное бюджетное учреждение науки Институт проблем передачи информации им. А.А. Харкевича Российской академии наук (ИППИ РАН). 127051, г. Москва, Большой Каретный переулок, д. 19, стр. 1. Тел.: +7 (495) 650-42-25, e-mail: director@iitp.ru.