ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.415.04,
СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО
АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО
ОБРАЗОВАНИЯ «ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)
МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ
КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело №_____

решение диссертационного совета от 02.07.2026 № 6

О присуждении Куртуковой Анне Владимировне, гражданке Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика и программный комплекс для идентификации автора программного кода», представленная на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность, принята к защите 27 апреля 2026 г. (протокол № 3) диссертационным советом 24.2.415.04, созданным на базе ТУСУРа Минобрнауки России (634050, г. Томск, пр. Ленина, 40). Приказ о создании диссертационного совета № 92/нк от 26 января 2023 г.

Соискатель Куртукова Анна Владимировна, 11.06.1997 года рождения, в 2025 году окончила аспирантуру ТУСУРа. В настоящее время работает преподавателем кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа.

Диссертация выполнена на кафедре КИБЭВС ТУСУРа.

Научный руководитель – член-корреспондент РАН, доктор технических наук, профессор, директор института системной интеграции и безопасности ТУСУРа **Шелупанов Александр Александрович**.

Официальные оппоненты – **Вульфин Алексей Михайлович**, д.т.н., профессор кафедры вычислительной техники и защиты информации Уфим-

ского университета науки и технологий; **Аникин Игорь Вячеславович**, д.т.н., проф., зав. кафедрой систем информационной безопасности Казанского национального исследовательского технического университета им. А.Н. Туполева – дали **положительные отзывы** на диссертацию.

Ведущая организация – **Санкт-Петербургский Федеральный исследовательский центр Российской академии наук** (СПб ФИЦ РАН) в своем **положительном отзыве**, подписанном д.т.н., проф., гл. науч. сотр. лаборатории проблем компьютерной безопасности Саенко И. Б. и д.т.н., проф., директором СПИИРАН Осиповым В. Ю. и утвержденном д.т.н., проф. РАН, директором СПб ФИЦ РАН Ронжиным А. Л., указала, что диссертационная работа Куртуковой А.В. является самостоятельной и законченной научно-квалификационной работой, решающей важную научно-техническую задачу разработки методики, обеспечивающей повышение точности идентификации автора программного кода для решения задач информационной безопасности, и программного комплекса на ее основе, и вносящей значительный вклад в развитие информационной безопасности и методов анализа текстовой информации, а также удовлетворяет пп. 9-14 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства РФ от 24.09.2013 № 842, а ее автор, Куртукова А.В., заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 23 опубликованные работы по теме диссертации. При этом 7 статей опубликованы в рецензируемых научных изданиях из перечня ВАК (из них 2 без соавторов), 6 статей опубликованы в зарубежных научных изданиях, индексируемых Web of Science и/или Scopus (из них 4 – в журналах, входящих в 1-3 квартили Web of Science и/или Scopus). Общий объем – 21 п.л., авторский вклад – 11 п.л. В диссертации отсутствуют недостоверные сведения об опубликованных работах. Наиболее значимые работы по теме диссертации:

1. **Куртукова А.В.** Методика идентификации автора исходного кода программы на основе multi-view-представлений / А. В. Куртукова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2025. – Т. 28, № 3. – С. 59–65.

2. **Куртукова А.В.** Интегрированный подход к идентификации вредоносных программ на основе динамического анализа и глубокого обучения / А. В. Куртукова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2025. – Т. 28, № 1. – С. 108–113.

3. Integrated Technique of Natural Language Texts and Source Codes Authorship Verification in the Academic Environment / A. Romanov, **A. Kurtukova**, A. Fedotova and A. Shelupanov // IEEE Access. – 2025. – Vol. 13. –P. 113274–113290.

4. **Куртукова А.В.** Идентификация автора исходного кода методами машинного обучения / А.В. Куртукова, А.С. Романов // Труды СПИИРАН. – 2019. – № 3(18). – С. 741–765.

На автореферат поступило 14 отзывов от: Белова В.М., д.т.н., проф., проф. кафедры информационной безопасности Сибирского государственного университета геосистем и технологий (г. Новосибирск); Веселова Г.Е., д.т.н., доц., директора Института компьютерных технологий и информационной безопасности Южного федерального университета (г. Ростов-на-Дону); Карташевского В.Г., д.т.н., проф., зав. НИЛ Инфокоммуникационных технологий Поволжского государственного университета телекоммуникаций и информатики (г. Самара); Полякова В.В., д.ф.-м.н., проф., проф. кафедры информационной безопасности и Мансурова А.В., к.т.н., доц., зав. кафедрой информационной безопасности Алтайского государственного университета (г. Барнаул); Остапенко А.Г., д.т.н., проф., зав. кафедрой систем информационной безопасности Воронежского государственного технического университета; Челухина В.А., д.т.н., доц., проф. кафедры Информационной безопасности автоматизированных систем Комсомольского-на-Амуре государственного университета; Носкова С.И., д.т.н., проф., проф. кафедры информационных

систем и защиты информации Иркутского государственного университета путей сообщения; Сухопарова М.Е., д.т.н., доц., зам. директора по научной работе СПбФ АО «НПК «ТРИСТАН»» (г. Санкт-Петербург); Сычугова А.А., д.т.н., доц., директора Института прикладной математики и компьютерных наук, зав. кафедрой информационной безопасности Тульского государственного университета; Федорова М.В., чл.-корр. РАН, д.х.н., проф., и.о. директора Института проблем передачи информации им. А.А. Харкевича (г. Москва); Хашировой Т.Ю., д.т.н., проф., зав. кафедрой компьютерных технологий и информационной безопасности института электроники, робототехники и искусственного интеллекта Кабардино-Балкарского государственного университета им. Х. М. Бербекова (г. Нальчик); Лавровой Д.С., д.т.н., доц., проф. Санкт-Петербургского политехнического университета Петра Великого; Максимовой Е.А., д.т.н., доц., зав. кафедрой безопасности телекоммуникаций Московского технического университета связи и информатики; Шульженко А.Д., к.т.н., доц. кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина). **Все отзывы положительные.**

В качестве критических замечаний указывается: недостаточное описание экспериментальной методологии, в частности, сравнения с другими датасетами, процессов сбора данных для сложных случаев и подбора гиперпараметров; проблема масштабируемости на тысячи авторов; необходимость обоснования выбора методов и архитектур; недостаточность описания алгоритмов нормализации и токенизации.

Выбор официальных оппонентов д.т.н. **Вульфина А.М.** и д.т.н., проф. **Аникина И.В.** обусловлен их компетенциями в областях машинного обучения для решения прикладных задач информационной безопасности, текстового анализа и методов оптимизации.

Вульфин А.М. является автором научных публикаций, посвященных проблемам, непосредственно связанным с тематикой диссертационного исследования соискателя. Компетентность оппонента в вопросах информаци-

онной безопасности и интеллектуального анализа данных позволяет объективно оценить достоверность и новизну разработанных соискателем методов анализа программных артефактов для идентификации и верификации их авторства. За последние 5 лет по теме диссертационного исследования Вульфиным А.М. опубликовано более 15 научных работ по профилю научной специальности 2.3.6 в ведущих рецензируемых научных изданиях.

Аникин И.В. специализируется на разработке математических методов, алгоритмов количественной оценки рисков и интеллектуального анализа защищенности информационных систем в условиях неопределенности. Для темы соискателя критически важен опыт Аникина И.В. в области анализа программного обеспечения, а также исследования нейросетевых моделей для распознавания поведенческих паттернов. Эти компетенции напрямую проецируются на задачи распознавания авторского стиля в исходном и бинарном коде. Аникиным И.В. за последние 5 лет опубликовано более 15 значимых научных работ по профилю научной специальности 2.3.6 в ведущих рецензируемых научных изданиях.

Выбор СПб ФИЦ РАН в качестве ведущей организации обусловлен наличием признанных экспертов в области информационной безопасности и полным соответствием его ключевых компетенций специфике диссертационного исследования. СПб ФИЦ РАН обладает профильной экспертизой благодаря работе лабораторий проблем компьютерной безопасности и интеллектуальных систем, имеет высокий научный авторитет и многолетний опыт исследований в сфере защиты информации и анализа данных. Также сотрудники организации демонстрируют постоянную публикационную активность в ведущих рецензируемых журналах ВАК и Scopus/Web of Science по смежным темам. Наиболее близкими к тематике диссертации являются публикации ученых ведущей организации: Котенко И.В., Саенко И.Б., Израилова К.Е. и некоторых других.

Отзыв подготовлен в лаборатории проблем компьютерной безопасности, известной в области выявления уязвимостей и обеспечения проактивной защиты информации.

Диссертационный совет констатирует, что цель исследования, состоящая в разработке методики, обеспечивающей повышение точности идентификации автора программного кода для решения задач кибербезопасности, и программного комплекса на ее основе, достигнута.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

предложен новый метод верификации автора программного кода, отличающийся применением сиамской нейросетевой архитектуры с контрастивным обучением и адаптивной калибровкой прогностических вероятностей посредством изотонической регрессии;

предложено решение задачи идентификации авторства программного кода, внедрение результатов решения которой вносит значительный вклад в развитие безопасных информационных технологий страны;

разработана новая методика идентификации автора программного кода, отличающаяся использованием multi-view подхода с межвидовым выравниванием через контрастивные потери к получению векторных представлений программного кода, и энкодера для представления дизассемблированного кода на основе авторской гибридной нейронной сети, позволяющая определять автора в случаях открытого и закрытого множества авторов-кандидатов.

Теоретическая значимость исследования обоснована тем, что:

изложены положения, расширяющие базу программных артефактов за счет интеграции различных представлений кода в рамках единого multi-view энкодера, что позволяет выявлять общие закономерности между признаками на разных уровнях анализа кода программы;

применительно к проблематике диссертации эффективно использованы современные методы теории защиты информации, машинного обучения и агрегации различных видов представлений, что обеспечило унифика-

цию решения задач верификации и идентификации в закрытом и открытом множествах авторов-кандидатов, а также статистического анализа для получения достоверных результатов по идентификации автора в различных прикладных сценариях;

изложены новые научные результаты – методика, методы и алгоритмы идентификации и верификации авторства по исходному коду, его абстрактному синтаксическому дереву, дизассемблированному коду и графу потока управления кода, а также для определения APT-группировки, разработавшей вредоносный код;

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

методика и программный комплекс для идентификации автора программного кода **внедрены** в ООО «НТР Томск» с целью автоматизации контроля происхождения кода, повышения безопасности процессов разработки DevSecOps и оптимизации аудита внутренних ИТ-ресурсов;

методика для идентификации автора программного кода и входящие в ее состав методы **внедрены** в учебный процесс факультета безопасности ТУСУРа с целью обучения студентов методам экстракции разноуровневых представлений кода, построения моделей для идентификации авторов вредоносных фрагментов и анализа репозиториев, а также для автоматизации контроля самостоятельности выполнения студенческих работ по программированию;

модули программного комплекса для идентификации автора программного кода **внедрены** в ООО «ТомскСофт» с целью обеспечения непрерывного контроля за использованием исходных кодов коммерческих программных продуктов компании, а также для своевременного отслеживания и предотвращения попыток их несанкционированного применения сотрудниками в личных или противоречащих интересам организации целях;

созданы алгоритмическое и программное обеспечение для экстракции и кодирования программных представлений безопасного программирования с

поддержкой 13 языков программирования, а также репрезентативный набор данных для противодействия угрозам нарушения информационной безопасности, включающим обфускацию, ИИ-генерацию и APT-группировки.

Оценка достоверности результатов исследования выявила:

теория, используемая в диссертационном исследовании, опирается на современные достижения в областях машинного и глубокого обучения, методы математической статистики, а также на передовые подходы к авторской атрибуции как к частному случаю поведенческой биометрии субъектов в задачах обеспечения информационной безопасности;

идея работы базируется на интеграции методов машинного обучения, стилометрии и анализа программных артефактов для идентификации автора в условиях реальных киберугроз, что реализовано посредством объединения четырех разноуровневых представлений программного кода в рамках multi-view архитектуры энкодера с межвидовым выравниванием через контрастивные потери;

установлено, **что** полученные соискателем **результаты согласуются** с результатами исследований в области идентификации авторства программного кода и **не противоречат** известным данным в работах других авторов.

Личный вклад соискателя состоит в самостоятельном проведении всех этапов исследования, включая детальный анализ существующих подходов атрибуции программного кода, формирование набора экспериментальных данных, разработку multi-view методики идентификации автора программного кода и программного комплекса на ее основе. Соискателем лично обоснованы и построены математические модели для методов идентификации авторства в закрытом и открытом множествах авторов-кандидатов, а также разработан метод верификации с адаптивной калибровкой прогностических вероятностей посредством изотонической регрессии. Постановка задач и обсуждение результатов велись совместно с научным руководителем и консультантом, при этом ключевые научные результаты получены соискателем лично.

В ходе защиты высказаны следующие критические замечания: отсутствует информация о перспективах развития темы; недостаточно подробно изложены ограничения разработанных методики и программного комплекса; метод идентификации в открытом множестве и иерархический подход к идентификации авторства не представлены как отдельные обладающие научной новизной результаты.

Соискатель Куртукова А.В. ответила на заданные в ходе заседания вопросы, сформулированные замечания и привела собственную аргументацию: перспективы развития темы состоят в адаптации разработанного инструментария к задаче идентификации авторов-вирусописателей, помимо APT-группировок, а также совершенствовании методов векторизации с целью создания более устойчивых к сложным сценариям представлений; к ограничениям, не упомянутым в тексте диссертации, относится оптимизация кода, направленная на его сжатие, а не на ускорение, а также минимальная длина коммита – 1000 символов; иерархический подход, обеспечивающий высокую точность идентификации авторства в условиях масштабирования, и метод идентификации авторства программного кода в открытом множестве, основанный на метрическом подходе и контрастивном обучении, могли быть вынесены как дополнительные пункты научной новизны при должной формулировке.

Диссертация Куртуковой А.В. на соискание ученой степени кандидата технических наук соответствует паспорту специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность и является законченной научно-квалификационной работой.

На заседании 02 июля 2026 г. диссертационный совет принял следующее заключение: за решение важной научно-технической задачи разработки методики, обеспечивающей повышение точности идентификации автора программного кода для решения задач информационной безопасности, и программного комплекса на ее основе, решение которой вносит значительный вклад в развитие теории и методов защиты информации в области анализа

программных артефактов и противодействия угрозам нарушения информационной безопасности, присудить Куртуковой Анне Владимировне ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве **11** человек, из них **4** доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из **16** человек, входящих в состав совета, проголосовали: за – **11**, против – **0**, недействительных бюллетеней – **0**.

Зам. председателя
диссертационного совета — Заболоцкий Александр Михайлович

Ученый секретарь
диссертационного совета — Костюченко Евгений Юрьевич

03.07.2026