



УТВЕРЖДАЮ

Ректор ТУСУРа

В.М. Рулевский

«7» _____ 2025 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного автономного образовательного учреждения
высшего образования «Томский государственный университет
систем управления и радиоэлектроники»

Диссертация «Методология идентификации автора текстовой информации для решения задач кибербезопасности» выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР).

В период подготовки диссертации соискатель Романов Александр Сергеевич работал в ТУСУРе, на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) в должности доцента.

В 2007 году окончил ТУСУР с присвоением квалификации «специалист по защите информации» по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».

С 2007 по 2010 годы обучался в аспирантуре Томского государственного университета систем управления и радиоэлектроники.

В 2010 году успешно защитил диссертацию на соискание степени кандидата технических наук на тему «Методика и программный комплекс для идентификации автора неизвестного текста» по специальности 05.13.18 – Математическое моделирование, численные методы и комплексы программ.

Научный консультант – Шелупанов Александр Александрович, д-р техн. наук, профессор, заведующий кафедрой комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Федерального государственного автономного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

По итогам обсуждения принято следующее заключение:

В представленной диссертационной работе Романова А.С. предлагается комплексное решение важной научной проблемы идентификации автора текстовой информации, имеющей важное хозяйственное значение, внедрение которой вносит значительный вклад в развитие кибербезопасности и других областей, основанное на передовых технологиях искусственного интеллекта и машинного обучения.

В работе раскрыта актуальность проблемы, приведен исчерпывающий анализ трудов российских и зарубежных исследователей, произведена оценка степени ее проработанности. Предложена методология идентификации автора текста и модель создания автором текста в киберсреде, учитывающие атрибуты автора и семантические особенности и информативные признаки текста. Предложены методики идентификации автора естественных текстов и исходных кодов программ, в которых применяются классические методы машинного обучения, методы отбора информативных признаков, методы семантической кластеризации и передовые методы глубокого обучения. Предложена методика проверки однородности текста и поиска заимствований. Впервые рассматриваются сложные случаи идентификации автора и атаки на подобные методы. Предложены методики определения запрещенных в РФ текстов

деструктивной и экстремистской направленности и их авторов, определения текстов, созданных представителями ЛГБТ.

Личный вклад автора состоит в разработке методологии идентификации автора текстовой информации, модели создания текста автором в киберсреде, методик идентификации автора естественно-языкового текста, его возраста, пола и гендера, автора исходных кодов программ, деструктивной и экстремистской направленности в текстах и определения автора таких текстов, проверки однородности текста и поиска заимствований. А также в разработке программных продуктов на основе разработанной им методологии, методик, моделей и алгоритмов. Автору принадлежит ключевая роль в получении основных результатов, составляющих научную основу диссертационной работы и выносимых на защиту.

Работы [1, 2, 3, 14, 15, 16, 18] выполнены автором единолично. В работах, написанных в соавторстве, автор формировал концепцию и идею проводимого исследования. В работах [4, 9, 20, 23, 26, 30, 31, 32] соискателем предложены математические модели, методики и программные средства информационных процессов при идентификации автора с учетом особенностей типов естественного текста для решения задач кибербезопасности. В работах [7, 8, 10, 11, 13, 21, 22, 25, 28, 29] соискателем исследуются методики идентификации автора исходных и дизассемблированных кодов, устойчивых к атакам на них. В работах [12, 24, 27] предлагаются подходы для определения возраста, пола и гендера автора текста на основе методов машинного обучения. В работах [5, 6, 17, 19] соискателем предложены алгоритмы и принципы создания программных средств, основанных на анализе текстовой составляющей, для решения задач поиска плагиата и определения деструктивных текстов, нарушающих законодательство РФ. Апробация и тестирование выполнены совместно с сотрудниками ТУ-СУРА, входящими в научную группу автора.

Достоверность научных положений, результатов и основных выводов работы подтверждается использованием корректных методов математической статистики, вычислительного эксперимента и искусственного интеллекта, серией практических экспериментов на представительном и репрезентативном корпусе текстов, а также согласованностью полученных данных с результатами других научных групп и положительным эффектом от внедрения полученных результатов.

Выполненные исследования имеют научную новизну и практическую значимость.

Научная новизна полученных в диссертационной работе результатов заключается в следующем.

1. Впервые предложена комплексная методология идентификации автора текста, учитывающая особенности естественно- и искусственно-языковых текстов и возможные атаки на методы идентификации.

2. Предложена модель создания текста автором в киберсреде, впервые учитывающая семантические особенности и информативные признаки текста на разных уровнях иерархического анализа, специфику среды, атрибуты автора и вид деятельности по созданию текста.

3. Предложена методика идентификации автора естественного текста, отличающаяся использованием комбинации GRU+CNN и SVM с отбором признаков генетическим алгоритмом и методом на основе регуляризации, впервые учитывающая случаи открытой и закрытой атрибуции и текстов, созданных генеративными нейросетями.

4. Предложена методика идентификации автора исходного кода программ, в которой впервые используется классификатор на основе глубокой модели CodeBERT. Методика отличается учетом комплекса сложных случаев идентификации (обфускация, командная разработка, использование стандартов кодирования и искусственно-сгенерированных кодов программ).

5. Предложена методика бинарной и мультиклассовой классификации по возрастным группам на основе текста, отличающаяся использованием модели fastText в сочетании с методами компьютерного зрения для фильтрации обучающих данных.

6. Предложена методика определения текстов деструктивной и экстремистской направленности и определения автора таких текстов, отличающаяся использованием моде-

лей GRU+CNN и BERT, методов семантической кластеризации текста и трансферного обучения, что позволяет выявлять запрещенные законодательством РФ тексты.

7. Разработана новая методика определения пола и гендера автора русскоязычного текста, впервые учитывающая гендеры ЛГБТ и отличающаяся использованием ансамбля: SVM, обученного на признаковом пространстве, сформированного на основе методов семантической кластеризации, сверточной сети, обученной на частотных распределениях триграмм, сглаженных методом Катца, и BERT.

8. Предложена методика проверки однородности текста и поиска заимствований, отличающаяся применением сиамских НС SimNN, обученных с контрастивной и тройной функциями потерь. Методика впервые решает задачу выявления заимствований для случаев открытого множества авторов-кандидатов и использования искусственной генерации текстов.

Теоретическая значимость работы состоит в проработке и систематизации результатов предыдущих исследований, их дополнении и комплексировании с вновь разработанными методиками, моделями и алгоритмами в составе единой методологии идентификации автора текстовой информации.

Практическая значимость результатов исследования заключается в разработке репрезентативных корпусов текстов, которые можно использовать для обучения моделей при решении задач кибербезопасности. А также в разработанных программных продуктах на основе методик идентификации автора естественно- и искусственно-языкового текста, определения текстов деструктивной и экстремистской направленности, определения пола, гендера и возраста автора текста, проверки текста на однородность и поиска заимствований. Полученные решения устойчивы к специфическим видам атак, позволяют сократить временные затраты и повысить точность решаемых задач кибербезопасности и анализа текстовой информации по сравнению с аналогами. Разработанная методология и инструментарий на ее основе может использоваться для защиты интеллектуальной собственности, идентификации автора сообщений в сети Интернет и продленной аутентификации пользователей социальных сетей, выявления признаков пропаганды ЛГБТ и педофилии, определения автора-вирусописателя, определения эмоциональной окраски текста, деструктивных, а также текстов экстремистской направленности, запрещенных законодательством Российской Федерации.

Практическая значимость результатов диссертационной работы подтверждается их внедрением в деятельность АО «Национальный Инновационный Центр», ООО «СИБ», ООО «НТР», ООО «Сибэдж», войсковую часть 51952, ИШИТР ТПУ, ОБК УМВД России по Томской области, на экономическом факультете МГУ имени М.В. Ломоносова, а также в учебный процесс ТУСУРа.

Результаты диссертационного исследования использованы при выполнении государственных заданий, госпрограммы «Приоритет 2030» и хоздоговоров, выполнявшихся в ТУСУРе.

Полнота изложения материалов диссертационной работы в публикациях

По материалам диссертации Романова А.С. опубликовано 93 работы, в том числе 31 публикация в рецензируемых научных изданиях, рекомендуемых для опубликования основных научных результатов диссертаций на соискание ученых степеней кандидата и доктора наук, из них 18 публикаций в рецензируемых журналах из перечня ВАК и 13 публикаций в изданиях, индексируемых Web of Science и/или Scopus, а также 1 монография, 11 свидетельств о регистрации программ для ЭВМ и о регистрации баз данных. Материалы диссертационной работы в публикациях отражены полно.

Публикации в журналах, рекомендованных ВАК:

1. **Романов А.С.** Модель базы данных для хранения текстов и их характеристик / А.С. Романов // Доклады ТУСУР. – 2008. – № 1(17). – С. 70–73.

2. **Романов А.С.** Структура программного комплекса для исследования подходов к идентификации авторства текстов / А.С. Романов // Доклады ТУСУР. – Ч. 1. – 2008. – № 2(18). – С. 106–109.
3. **Романов А.С.** Методика идентификации автора текста на основе аппарата опорных векторов / А.С. Романов // Доклады ТУСУР. – Ч. 2. – 2009. – № 1 (19). – С. 36–42.
4. **Романов А.С.** Обобщенная методика идентификации автора неизвестного текста / А.С. Романов, А.А. Шелупанов, С.С. Бондарчук // Доклады ТУСУР. – Ч. 1. – 2010. – № 1(21). – С. 108–112.
5. **Романов А.С.** Методика проверки однородности текста и выявления плагиата на основе метода опорных векторов и фильтра быстрой корреляции / А.С. Романов, З.И. Резанова, Р.В. Мещеряков // Доклады ТУСУР. – 2014. – № 2(32). – С. 264–269.
6. Созинова И.С. Определение поискового спама с использованием метода опорных векторов / И.С. Созинова, **А.С. Романов**, Р.В. Мещеряков // Труды СПИИРАН. – 2014. – Вып. 36. – С. 78–91.
7. Куртукова А.В. Моделирование архитектуры нейронной сети в задаче идентификации автора исходного кода / А.В. Куртукова, **А.С. Романов** // Доклады ТУСУР. – 2019. – Т. 22, № 3. – С. 37–42.
8. Куртукова А.В. Оценка влияния обфускации на процесс идентификации автора программного кода / А.В. Куртукова, Е.Е. Сваровская, **А.С. Романов** // Доклады ТУСУР. – 2020. – Т. 23, № 2. – С. 50–54.
9. Применение методов машинного обучения и отбора признаков на основе генетического алгоритма в решении задачи определения автора русскоязычного текста для кибербезопасности / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов // Доклады ТУСУР. – 2022. – Т. 25, № 1. – С. 79–85.
10. Идентификация автора исходного кода программы на основе неоднородных данных для решения задач кибербезопасности [Электронный ресурс] / А.В. Куртукова, **А.С. Романов**, А.А. Шелупанов, А.М. Федотова // Моделирование, оптимизация и информационные технологии. – 2022. – № 10(3). – Режим доступа: <https://moitvvt.ru/ru/journal/pdf?id=1227>.
11. Архитектура интеллектуальной системы для идентификации автора исходного кода / А.В. Куртукова, **А.С. Романов**, А.А. Шелупанов, А.М. Федотова // Доклады ТУСУР. – 2022. – Т. 25, № 3. – С. 39–44.
12. Методика определения возраста автора текста на основе метрик удобочитаемости и лексического разнообразия / А.А. Соболев, А.М. Федотова, А.В. Куртукова, **А.С. Романов**, А.А. Шелупанов // Доклады ТУСУР. – 2022. – Т. 25, № 2. – С. 45–52.
13. Куртукова А.В. Разработка методики идентификации авторства бинарных и дизассемблированных кодов программы на основе ансамбля современных методов обработки естественного языка / А.В. Куртукова, **А.С. Романов**, А.А. Шелупанов // Доклады ТУСУР. – 2023. – Т. 26, № 4. – С. 53–60.
14. **Романов А.С.** Методы отбора признаков в задаче определения авторства в контексте кибербезопасности [Электронный ресурс] / А.С. Романов // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12, № 1. – Режим доступа: <https://moitvvt.ru/ru/journal/pdf?id=1489>.
15. **Романов А.С.** Идентификация автора текста для открытого множества кандидатов в контексте кибербезопасности [Электронный ресурс] / А.С. Романов // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12, № 1. – Режим доступа: <https://moitvvt.ru/ru/journal/pdf?id=1510>.
16. **Романов А.С.** Методология идентификации автора текста для решения задач информационной безопасности / А.С. Романов // Вопросы кибербезопасности. – № 3(61). – Москва: НПО «Эшелон», 2024. – С. 120–128.

17. Методика идентификации автора текстовых материалов деструктивной направленности / **А.С. Романов**, А.М. Федотова, А.В. Куртукова, А.А. Шелупанов // Информационные технологии. – 2024. – Т. 30, № 12. – С. 632–640.

18. **Романов А.С.** Методика семантической кластеризации для выявления признаков экстремизма в текстовой информации / А.С. Романов // Доклады ТУСУР. – 2024. – Т. 27, № 4. – С. 141–149.

Публикации, включенные в библиографические базы Web of Science, Scopus:

19. **Романов А.С.** Анализ тональности текстов с использованием методов машинного обучения (Sentiment Analysis of Text Using Machine Learning Techniques) / А.С. Романов, М.И. Васильева, А.В. Куртукова, Р.В. Мещеряков // Proceedings of the R. Piotrowski's Readings in Language Engineering and Applied Linguistics. – Saint Petersburg, Russia, November 27, 2017. – P. 86–95.

20. **Romanov A.** Natural text anonymization using universal transformer with a self-attention / A. Romanov, A. Kurtukova, A. Fedotova, R. Meshcheryakov // Proceedings of the III International Conference on Language Engineering and Applied Linguistics (PRLEAL-2019), Saint Petersburg, Russia. – 2019. – P. 22–37.

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

22. Kurtukova A. De-Anonymization of the Author of the Source Code Using Machine Learning Algorithms / A. Kurtukova, **A. Romanov**, A. Fedotova // Conference Proceedings of 2019 SIBIRCON. – 2019. – P. 0612–0617.

23. Authorship identification of a russian-language text using support vector machine and deep neural networks / **A. Romanov**, A. Kurtukova, A. Fedotova, A. Shelupanov, V. Goncharov // Future Internet. – 2021. – Vol. 13. – Iss. 1. – 3. – 16 p.

24. Determining the Age of the Author of the Text Based on Deep Neural Network Models / **A.S. Romanov**, A.V. Kurtukova, A.A. Sobolev, A.A. Shelupanov, A.M. Fedotova // Information. – 2020. – Vol. 11. – Iss. 12. – 589. – 12 p.

25. Kurtukova A. Source Code Authorship Identification Using Deep Neural Networks / A. Kurtukova, **A. Romanov**, A. Shelupanov // Symmetry. – 2020. – Vol. 12. – Iss. 12. – 2044. – 17 p.

26. Authorship Attribution of Social Media and Literary Russian-Language Texts Using Machine Learning Methods and Feature Selection / A. Fedotova, **A. Romanov**, A. Kurtukova, A. Shelupanov // Future Internet. – 2022. – Vol. 14. – Iss. 4. – 1. – 24 p.

27. **Romanov A.** Age determination of the social media post's author using deep neural networks and facial processing model / A. Romanov, A. Kurtukova, A. Sobolev, A. Fedotova // CEUR Workshop Proceedings. – 2021. – Vol. 2842. – P. 51–59.

28. Complex Cases of Source Code Authorship Identification Using a Hybrid Deep Neural Network / A. Kurtukova, **A. Romanov**, A. Shelupanov, A. Fedotova // Future Internet. – 2022. – Vol. 14. – Iss. 10. – 287. – 20 p.

29. Authorship Identification of Binary and Disassembled Codes Using NLP Methods / **A. Romanov**, A. Kurtukova, A. Fedotova, A. Shelupanov // Information. – 2023. – Vol. 14. – Iss. 7. – 361. – 21 p.

30. Digital Authorship Attribution in Russian-Language Fanfiction and Classical Literature / A. Fedotova, **A. Romanov**, A. Kurtukova, A. Shelupanov // Algorithms. – 2023. – Vol. 16. – Iss. 1. – 13. – 32 p.

31. Semantic Clustering and Transfer Learning in Social Media Texts Authorship Attribution / A. Fedotova, A. Kurtukova, **A. Romanov**, A. Shelupanov // IEEE Access. – 2024. – Vol. 12. – P. 39783–39803.

Свидетельства о регистрации программ ЭВМ и баз данных:

32. Свидетельство о регистрации электронного ресурса №151146 Российская Федерация. Программная система для идентификации автора письменной речи «Авторовед» /

А.С. Романов. Дата регистрации 24.12.2009. Зарегистрировано в Объединенном фонде электронных ресурсов «Наука и образование». Дата выдачи 14.01.2010.

33. Свидетельство о государственной регистрации программы для ЭВМ №2020666001. Программа для тонального анализа текста «Moodorrude» / **А.С. Романов**, М.И. Васильева, Л.С. Шилов, А.В. Куртукова, А.А. Шелупанов. – Заявка №2020665103. Дата поступления 26 ноября 2020. Зарегистрировано в Реестре программ для ЭВМ 03.12.2020.

34. Свидетельство о государственной регистрации программы для ЭВМ №2021681140. Система для идентификации автора исходного кода программы «CoDEtective» / А.В. Куртукова, **А.С. Романов**. – Заявка №2021667210. Дата поступления 26 октября 2021. Зарегистрировано в Реестре программ для ЭВМ 17.12.2021.

35. Свидетельство о государственной регистрации программы для ЭВМ №2022616780. Чат-бот для определения возраста автора текстового сообщения «Age Detector» / **А.С. Романов**, А.А. Соболев, А.М. Федотова, А.В. Куртукова, А.А. Шелупанов. – Заявка №2022616248. Дата поступления 12 апреля 2022. Зарегистрировано в Реестре программ для ЭВМ 15.04.2022.

36. Свидетельство о государственной регистрации программы для ЭВМ №2022667584. Программный комплекс для получения информативных признаков автора текста «PyAuthorship» / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка №2022667003. Дата поступления 19 сентября 2022. Зарегистрировано в Реестре программ для ЭВМ 2.09.2022.

37. Свидетельство о государственной регистрации базы данных №2022622299. База данных естественно и искусственно-языковых текстов для определения авторства / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка №2022622243. Дата поступления 16 сентября 2022. Зарегистрировано в Реестре баз данных 21.09.2023.

38. Свидетельство о государственной регистрации программы для ЭВМ №2023685210. Программный комплекс для идентификации запрещенных законодательством РФ и деструктивных текстов «PyDestructiveDetector» / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка №2023682992. Дата поступления 1 ноября 2023. Зарегистрировано в Реестре программ для ЭВМ 23.11.2023.

39. Свидетельство о государственной регистрации базы данных №2023623911. База данных исходных и дизассемблированных кодов для идентификации авторства программ / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка 2023623657. Дата поступления 01 ноября 2023. Зарегистрировано в Реестре баз данных 13.11.2023.

40. Свидетельство о государственной регистрации базы данных №2024624287. База данных естественных текстов для идентификации пола и гендера автора текста / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка 2024624158. Дата поступления 05 октября 2024. Зарегистрировано в Реестре баз данных 14.10.2024.

41. Свидетельство о государственной регистрации программы для ЭВМ №2024685146. Программный комплекс для сбора данных о поле и гендере автора естественно-языкового текста / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка №2024683353. Дата поступления 10 октября 2024. Зарегистрировано в Реестре программ для ЭВМ 24.10.2024.

42. Свидетельство о государственной регистрации программы для ЭВМ №2025615680. Программный комплекс для определения пола и гендера автора естественно-языкового текста «ProGender» / А.В. Куртукова, **А.С. Романов**, А.М. Федотова, А.А. Шелупанов. – Заявка №2025613057. Дата поступления 20 февраля 2025. Зарегистрировано в Реестре программ для ЭВМ 06.03.2025.

Монографии:

43. **Романов А.С.** Разработка и исследование математических моделей, методик и программных средств информационных процессов при идентификации автора текста / **А.С. Романов**, А.А. Шелупанов, Р.В. Мещеряков // Томск, В-Спектр. – 2011. – 188 с.

Специальность, которой соответствует диссертация

Диссертационная работа Романова А.С. на тему: «Методология идентификации автора текстовой информации для решения задач кибербезопасности» соответствует требованиям «Положения о порядке присуждения ученых степеней», предъявляемым ВАК к диссертационным работам на соискание ученой степени доктора наук, является законченным самостоятельным научным исследованием, имеющим научную ценность. Содержание диссертации соответствует паспорту специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность, а именно п. 1, п. 5, п. 12, п. 13:

– п. 1: Теория и методология обеспечения информационной безопасности и защиты информации;

– п. 5: Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет;

– п. 12: Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа;

– п. 13: Методы и модели выявления и противодействия распространению ложной и вредоносной информации.

Диссертация «Методология идентификации автора текстовой информации для решения задач кибербезопасности» Романова Александра Сергеевича рекомендуется к защите на соискание учёной степени доктора технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

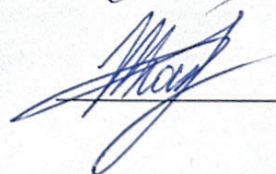
Заключение принято на заседании научно-технического семинара «Интеллектуальные системы моделирования, проектирования и управления» кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Федерального государственного автономного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Присутствовало на заседании 26 чел. Результаты голосования: «за» – 26 чел., «против» – 0, «воздержалось» – 0, протокол № 412 от 07.05 2025 г.

Заместитель председателя семинара,
канд. техн. наук, доцент каф. КИБЭВС,
декан факультета безопасности
ФГАОУ ВО «ТУСУР»

Ученый секретарь семинара, канд. техн.
наук, доцент каф. КИБЭВС

 Е.М. Давыдова

 Е.Ю. Костюченко