ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.479.07 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 17.09.2024 № 6

О присуждении Корелову Сергею Викторовичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Метод и алгоритм обнаружения спама на основе выделения признаков электронных писем с использованием контентной фильтрации» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 02.07.2024 г., протокол № 4 диссертационным советом 24.2.479.07 на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, созданного приказом Министерства образования и науки Российской Федерации от 24.03.2023 г. № 542/нк (с изменениями приказами от 18.12.2023 г. № 2368/нк и от 11.06.2024 г. № 581/нк).

Соискатель **Корелов Сергей Викторович,** 12 марта 1980 года рождения. является военнослужащим в/ч 43753.

В 2001 г. окончил Академию Федерального агентства правительственной связи и информации при Президенте Российской Федерации по специальности 220200 «Автоматизированные системы обработки информации и управления».

В 2024 году соискатель окончил аспирантуру ФГБОУ ВО «Поволжский государственный технологический университет» по направлению 10.06.01 «Информационная безопасность», направленность «Методы и системы защиты информации, информационная безопасность».

Справки со сведениями о сдаче кандидатских экзаменов выданы: в 2021 г. ФГБОУ ВО «Национальный исследовательский университет им. Н.И. Лобачевского» (кандидатский экзамен по английскому языку), в 2021 г. ФГБОУ ВО «Национальный исследовательский университет им. Н.И. Лобачевского» (кандидатский экзамен по истории и философии науки) и в 2023 г. ФГБОУ ВО «Поволжский государственный технологический университет» (кандидатский экзамен по специальности 05.13.19 Методы и системы защиты информации, информации).

Диссертация выполнена на кафедре информационной безопасности ФГБОУ ВО «Поволжский государственный технологический университет».

Научный руководитель – доктор технических наук, профессор Сидоркина Ирина Геннадьевна, ФГБОУ ВО «Поволжский государственный технологический университет», заведующая кафедрой информационной безопасности.

Официальные оппоненты:

1. Доктор технических наук, профессор Коробейников Анатолий Григорьевич, заместитель директора по науке «Санкт-Петербургского филиала Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук»;

2. Кандидат технических наук, доцент Бурлаков Михаил Евгеньевич, доцент кафедры безопасности информационных систем ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С. П. Королева»

дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ», г. Казань,

в своем положительном отзыве, подписанном заведующим кафедрой Автоматизированных систем обработки информации и управления Института компьютерных технологий и защиты информации, кандидатом технических наук, доцентом Шлеймовичем Михаилом Петровичем, утвержденном проректором по научной и инновационной деятельности, доктором технических наук, доцентом Бабушкиным Виталием Михайловичем, указала, что диссертация Корелова Сергея Викторовича, представленная на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований решена задача повышения эффективности обнаружения спама и достоверности идентификации легальных электронных почтовых сообщений на основе классификации их содержания, результаты которой обладают научной новизной, теоретической и практической ценностью.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (в редакции от 25.04.2024 г.), а ее автор, Корелов Сергей Викторович, заслуживает присуждения ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 29 опубликованных работ, в том числе по теме диссертации 19 работ, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 15 статей в других изданиях. 1 публикация выполнена соискателем единолично, остальные – при непосредственном участии и ведущей роли соискателя.

Общий объем публикаций – 11,44 п.л., авторский вклад – 9,91 п.л.

Наиболее значимые работы по теме диссертации:

1. Корелов С. В., Ротков Л. Ю., Рябов А. А. Вероятностный метод идентификации спама // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1 (21), часть 1. С. 150-152.

2. Корелов С. В., Петров А. М., Ротков Л. Ю., Горбунов А. А. Модель электронных писем в задаче обнаружения спама // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. 2020. № 2 (46). С. 44-54. DOI:10.25686/2306-2819.2020.2.44.

3. Корелов С. В., Петров А. М., Ротков Л. Ю., Горбунов А. А. Предобработка текстов электронных писем в задаче обнаружения спама // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 80-90. DOI:10.31854/1813-324X-2020-6-4-80-90.

4. Корелов С. В., Петров А. М., Сидоркина И. Г., Ротков Л. Ю., Горбунов А. А. Выбор размера кодовой таблицы в модели электронных писем // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. 2021. № 3 (51). С. 49-62. DOI:10.25686/2306-2819.2021.3.49.

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации; соискатель ссылается на авторов и источники заимствования.

На диссертацию и автореферат поступили положительные отзывы, в которых содержатся ряд замечаний:

- ведущей организации ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ». *Замечания*: **1.** В первой главе можно было более подробно рассмотреть виды спамовых писем. **2.** Недостаточно подробно освещены вопросы генетической информации и кодирования у биологических организмов, положенные в основу использованного метода «генетических карт». **3.** Не указано, в каком формате представлена база данных термов. **4.** В явном виде не указаны требуемые вычислительные ресурсы, необходимые для реализации предложенного в работе исследовательского прототипа подсистемы классификации электронных писем. **5.** Не указан язык программирования, на котором реализованы разработанные программные модули исследовательского прототипа. **6.** Не указано, существует ли

возможность добавления в базу данных термов спамовых и легальных писем не на этапе ее начального обучения, а непосредственно в процессе эксплуатации. **7.** В тексте диссертационной работы не упомянуто, существует ли возможность в случае ошибочной классификации письма скорректировать базу данных термов во избежание дальнейшего неправильного отнесения писем к классам спамовых или легальных;

- **официального оппонента** доктора технических наук, профессора Коробейникова Анатолия Григорьевича, заместителя директора по науке «Санкт-Петербургского филиала Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук». *Замечания*: **1.** В работе приводятся результаты экспериментов по классификации электронных писем из корпуса Enron. Для полноты исследования можно было бы для экспериментальных исследований использовать более свежие наборы писем. **2.** В работе не представлен вопрос выбора расстояния Левенштейна в качестве меры принадлежности классифицируемого электронного письма к классам спама и легальных. **3.** Не получил должного освещения вопрос сравнения полученных результатов с результатами обнаружения спама с использованием продуктовых пакетов. **4.** Из текста работы не ясно, каким образом должна осуществляться актуализация базы данных термов с учетом их маркирования по актуальности для конкретного пользователя и на конкретный момент времени;

- **официального оппонента** кандидата технических наук, доцента Бурлакова Михаила Евгеньевича, доцента кафедры безопасности информационных систем ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С. П. Королева». *Замечания*: **1.** В первой главе можно было более подробно остановиться на существующих зарубежных нормативных документах и актах в области борьбы со спамом в информационном пространстве. **2.** Из текста работы не вполне ясно, какие существуют ограничения на реализацию и применение предложенного алгоритма и программных модулей (аппаратная и программная платформа, требуемые вычислительные ресурсы и др.). **3.** Из текста

работы не прозрачен вывод, каким образом должно осуществляться оповещение и реагирование на выявленные спамовые письма для возможности дальнейшей интеграции в специализированные системы.

Получено 16 положительных отзывов на автореферат:

1. ФГБОУ ВО «Чувашский государственный университет имени И. Н. Ульянова», профессор кафедры математического и аппаратного обеспечения информационных систем, **д.т.н., доцент Галанина Наталия Андреевна**. *Замечания*: В целях лучшей интерпретации результатов желательно было бы в тексте автореферата привести не только значения выбранных частных показателей эффективности, но и первичные значения матрицы ошибок.

2. ФГБОУ ВО «Пензенский государственный университет», заведующий кафедрой «Информационная безопасность систем и технологий», **к.т.н., доцент Зефиров Сергей Львович**. *Замечания*: **1.** Представленная архитектура не является составной частью какой-либо существующей системы выявления СПАМ-сообщений и, как следствие, вопрос возможности ее интеграции и практического применения остается открытым. **2.** Процедура нечеткой классификации, в которой в качестве меры используется функция расстояния Левенштейна, не учитывает транспозиции (перестановки двух соседних символов). Эффективность процедуры может быть повышена использованием расстояния Дамерау-Левенштейна, нивелирующего наличие опечаток.

3. ФГБОУ ВО «Вятский государственный университет», профессор кафедры радиоэлектронных средств, **д.т.н., доцент Трубин Игорь Сергеевич**. *Замечание*: В описанной процедуре нечеткой классификации решение об отнесении письма к спаму принимается исходя из преобладания количества термов одного из двух классов. Принадлежность терма классу определяется наиболее близким в смысле расстояния Левенштейна термом в базе данных. При этом процедура не учитывает значения расстояний до ближайших термов из базы, что, возможно, несет потенциал для повышения эффективности алгоритма.

4. Институт искусственного интеллекта ФГБОУ ВО «МИРЭА – Российский технологический университет», заведующий базовой кафедрой № 252 –

информационной безопасности, **к.т.н., старший научный сотрудник, член-корреспондент Академии криптографии Российской Федерации, член-корреспондент Академии Инженерных наук им. А. М. Прохорова Российской Федерации Корольков Андрей Вячеславович**. *Замечания*: **1.** Предложенная архитектура подсистемы классификации электронных писем в автореферате представлена в достаточно общем виде. Вместе с тем, можно было бы увеличить степень ее детализации для более полного и наглядного представления о работе разработанных модели и метода. **2.** В целях наглядного представления приведенного на стр. 13 возможного практического внедрения предложенной архитектуры подсистемы классификации электронных писем целесообразно было бы указать блоки (точки) взаимодействия с внешними антиспам-решениями или почтовыми клиентами. **3.** Не ясно, были ли проведены оценки вычислительных ресурсов, требуемых для реализации предложенных автором решений, и времени, затрачиваемого на классификацию писем.

5. РУНЦ «Безопасность» ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», директор РУНЦ «Безопасность» МГТУ им. Н. Э. Баумана, **д.т.н., профессор Сычев Михаил Павлович**. *Замечания*: **1.** В автореферате указано, что результаты обнаружения спама с применением разработанной модели неслучайны. При этом не отражено, на основании чего сделан такой вывод. **2.** При проведении эксперимента для снижения размера признакового пространства использован индекс Джини. При этом вопрос его выбора не получил должного освещения.

6. ФГБОУ ВО «Марийский государственный университет», заведующий кафедрой прикладной математики и информатики, **д.т.н., доцент Петропавловский Михаил Вячеславович**. *Замечания*: **1.** В автореферате упоминается об обосновании выбора отдельных способов предобработки для соответствующей предобработки; при этом в тексте не нашло отражение описание множества рассмотренных способов, среди которых осуществлен выбор представленных в составе процедуры способов. **2.** Из текста автореферата неясно,

учитывает ли разработанная модель писем структуру их содержания; возможно, это несет потенциал для повышения эффективности классификации писем.

7. ФГБОУ ВО «Ульяновский государственный университет», доцент кафедры информационной безопасности и теории управления, **к.т.н., доцент Иванцов Андрей Михайлович**. *Замечание*: В целях лучшей интерпретации результатов и обоснования вывода № 5 в тексте автореферата можно было бы привести количественные данные по термам спамовых и легальных писем в наборах, участвовавших в экспериментальных исследованиях.

8. ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники», **д.т.н., профессор Шелупанов Александр Александрович**. *Замечания*: **1.** Определение легального сообщения, приведенное в сноске 2 в тексте автореферата, видится заужающим обусловленный практикой смысл этого понятия: не все легальные сообщения подразумевают предварительное согласие пользователя на их доставку. **2.** В описании результатов второй главы в тексте автореферата утверждается, что наличие «шумов» (спецсимволов HTML, скриптов, рекламных вставок) негативно влияет на качество данных для анализа и может снизить полноту и точность классификации. При этом, на наш взгляд, указанные шумы могут сами служить сильным классифицирующим признаком.

9.ФГАОУ ВО «Южный федеральный университет», **д.т.н., профессор Курейчик Владимир Викторович**. *Замечания*: **1.** Не вполне ясно, может ли предлагаемое решение использоваться в качестве основного, а не только путем интеграции в существующие решения или в виде дополнительного модуля. **2.** В тексте говорится о возможном практическом внедрении предложенной архитектуры путем интеграции в существующие решения или в виде дополнений для них. Вместе с тем, можно было бы одновременно предложить и возможные механизмы взаимодействия с ними.

10. ФГБОУ ВО «Самарский государственный технический университет», **к.т.н., доцент Карпова Надежда Евгеньевна**. *Замечания*: **1.** Новые письма ведут к увеличению размера базы данных термов, что неизбежно ведет к проблеме исчерпания свободного дискового пространства и роста вычислительных затрат.

Из автореферата неясно, каким образом планируется решать данную проблему. **2.** В автореферате не описаны детали применения в экспериментальных исследованиях метода кросс-валидации.

11. ФГБОУ ВО «Российский государственный гуманитарный университет», **к.и.н., доцент Шевцова Галина Александровна**. *Замечания*: **1.** Недостаточно описан предложенный алгоритм классификации электронных писем для обнаружения спама и идентификации легальных электронных писем. **2.** Недостаточно описана программная реализация исследовательского прототипа подсистемы классификации электронных писем. **3.** Указано, что при проведении экспериментальных исследований использован метод кросс-валидации. Вместе с тем, в автореферате не нашло отражение значение параметра данного метода (количество частей, на которые разбиваются массивы писем для тестирования), а также порядок его применения в эксперименте.

12. ФГАОУ ВО «Пермский национальный исследовательский политехнический университет», **к.т.н., доцент Шабуров Андрей Сергеевич**. *Замечания*: **1.** Неясно, какие способы предобработки текстов были рассмотрены автором, а также на основании каких критериев произведен отбор выбранных им способов. **2.** Неясно, чем обоснован выбор простой метрики Левенштейна для поиска схожих контекстов содержимого сообщений электронной почты.

13. ФГАОУ ВО «Пермский государственный национальный исследовательский университет», **к.ф.-м.н., доцент Никитина Елена Юрьевна**. *Замечания*: **1.** Не представлена функциональная модель классификации электронных писем, что могло бы дать более наглядное представление реализации практического внедрения предложенной архитектуры в существующие решения. **2.** В тексте автореферата в контексте проводимых экспериментальных исследований упоминаются только русскоязычные и англоязычные письма. В связи с наличием в реальной переписке русскоязычных писем с англоязычными словами и фразами хотелось бы увидеть оценку эффективности разработанной модели на такого рода письмах.

14. ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», **д.т.н., доцент Милославская Наталья Георгиевна**. **1.** Можно было более подробно остановиться на вопросе выбора простого решающего правила и косинусной меры в качестве правила классификации. **2.** Не вполне ясны допущения и ограничения на разрабатываемые модель и метод. **3.** В автореферате не нашли отражение вопросы выбора расстояния Левенштейна в качестве меры близости и индекса Джини в качестве меры сокращения размерности признакового пространства.

15. ФГАОУ ВО Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), **к.т.н., доцент Горячев Александр Вадимович**. **1.** Можно было бы указать требования к квалификации пользователя (администратора), требуемой для развертывания и сопровождения разработанных автором решений при их практической реализации в предложенных формах. **2.** Возможно, следовало бы привести дополнительные данные, отражающие возможный эффект от применения предложенных автором решений.

16. ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники», **д.т.н., доцент Душкин Александр Викторович**. **1.** Приведенные в тексте автореферата и сноске 2 определения спамовых и легальных писем основываются исключительно на отечественной нормативно- правовой базе. В связи с имеющимися различиями нормативных баз различных стран и в целях возможного учета опыта в этой области, обобщения и унификации данных понятий, целесообразно было бы рассмотреть зарубежные нормативные правовые акты, регулирующие отношения в этой области. **2.** Для повышения наглядности программной реализации исследовательского прототипа можно было бы представить описание структуры базы данных термов, ее таблиц и их полей в какой-либо нотации. **3.** Из автореферата неясно, на каком уровне (хост, клиент и т. д.) может быть использована разработанная автором подсистема классификации электронных писем для обнаружения спама и идентификации электронных писем.

Выбор официальных оппонентов и ведущей организации обосновывается их достижениями в данной отрасли наук, наличием публикаций в соответствующей сфере исследования и способностью определить научную и практическую ценность диссертации. Ведущая организация и оппоненты не имеют совместных проектов и публикаций с соискателем.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **разработана** модель электронного почтового сообщения для классификации электронных писем на основе метода «генетических карт», отличающаяся от известных моделей методом выделения значимых последовательностей символов текста (признаков электронных писем на основе их содержания, термов), позволяющим усилить смысловое содержание термов;

- **разработан** метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, отличающийся от известных использованием разработанной модели электронных писем, применение которого позволяет повысить эффективность обнаружения спама и достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации), а также снизить количество неклассифицированных писем;

- **разработан** алгоритм классификации электронных писем, отличающийся от известных наличием дополнительной процедуры определения «схожести» термов на основе расстояния Левенштейна, обеспечивающей вычисление мер принадлежности классифицируемого электронного письма к классам спама и легальных, применение которого позволяет повысить достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации), а также уменьшить количество неклассифицируемых писем;

- **разработан** исследовательский прототип подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, отличающийся от известных блоком выделения термов и

блоком нечеткой классификации, реализующий предложенные в работе метод и алгоритм, применение которых позволяет повысить достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации);

- экспериментально **доказана** обоснованность и эффективность использования разработанных модели электронного почтового сообщения и метода классификации электронных писем для обнаружения спама и идентификации легальных электронных писем на основе реальных спамовых и легальных писем.

Теоретическая значимость исследования обоснована тем, что:

- **применительно к проблематике диссертации** результативно (то есть с получением обладающих новизной результатов) **использованы** методы интеллектуального анализа данных и защиты информации, теория систем и системного анализа, теория принятия решений, теория эксперимента, методы контент-анализа, методы машинного обучения, методы теории вероятностей и математической статистики, методы объектно-ориентированного анализа и проектирования;

- **изложены** аргументы и факты, подтверждающие актуальность подхода к выделению термов электронного письма и разработки модели, метода и алгоритма, отличительным признаком которых является применение метода «генетических карт», методов машинного обучения и блока нечеткой классификации для обнаружения спама и идентификации легальных электронных писем, что позволяет усилить смысловое содержание термов и повысить эффективность обнаружения спама и достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации);

- **раскрыты** несовершенство исследованных средств обнаружения спама и невозможность с их помощью адекватно реагировать на постоянно изменяющиеся способы составления спамовых писем; кроме того, показано отсутствие универсального описания спама в связи с наличием вариативного изменения

информационных потребностей конкретного пользователя, влияющего на классификацию спамовых электронных писем;

- **изучены** наиболее значимые отличительные особенности спама, обуславливающие выбор подхода к обнаружению спама на основе классификации содержания электронных писем с целью повышения эффективности обнаружения спама и достоверности идентификации легальных электронных почтовых сообщений.

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

- **внедрены** в ООО «Омега Софт» (г. Йошкар-Ола), ООО «ТРЭВЕЛ ЛАЙН СИСТЕМС» (г. Йошкар-Ола) и в учебный процесс кафедры информационной безопасности ФГБОУ ВО «Поволжский государственный технологический университет» (г. Йошкар-Ола) результаты диссертационной работы, в том числе:

1) алгоритм классификации электронных писем на основе методов машинного обучения, отличающийся наличием дополнительной процедуры определения «схожести» термов на основе расстояния Левенштейна, обеспечивающей вычисление мер принадлежности классифицируемого электронного письма к классам спама и легальных для повышения достоверности идентификации электронных писем, позволяющий осуществить программную реализацию метода в виде плагина;

2) исследовательский прототип подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем на основе алгоритма, отличающийся от известных блоком выделения термов и блоком нечеткой классификации, реализующая метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, отличающийся использованием модели электронного почтового сообщения для классификации электронных писем на основе метода «генетических карт»;

3) модель электронного почтового сообщения для классификации электронных писем на основе метода «генетических карт»;

4) метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, отличающийся использованием модели электронного почтового сообщения для классификации электронных писем на основе метода «генетических карт»;

- **определены** возможные пути практического внедрения предложенной архитектуры подсистемы классификации электронных писем для решения задачи обнаружения спама, в том числе в практической деятельности разработчиков средств для обнаружения спама;

- **создан** исследовательский прототип подсистемы классификации электронных писем, позволяющий строить признаковое пространство (выделять термы) электронных писем, проводить их классификацию (обнаруживать спама и идентифицировать легальные электронные письма) и позволивший обосновать практическую применимость и эффективность разработанной модели и метода;

- **представлены** предложения по дальнейшему развитию полученных результатов, связанные с совершенствованием предложенного метода классификации с целью повышения его эффективности в условиях применения различных процедур сокращения размерности признакового пространства и правил классификации электронного письма, а также с выбором техники искусственной модификации наборов писем и их параметров для выравнивания соотношения классов электронных писем.

Оценка достоверности результатов исследования выявила:

- **для экспериментальных работ** в процессе работы исследовательского прототипа подсистемы классификации электронных писем использовались персональные компьютеры и открытые наборы обучающих данных (датасеты);

- **теория** базируется на использовании известных положений, подходов и принципов технологий классификации текстов, методов машинного обучения и результатах вычислительных экспериментов, а также на известных, проверяемых и апробированных данных, фактах и согласуется с опубликованными ранее работами и экспериментальными данными других авторов по теме диссертации;

- **идея базируется** на подходе к формированию математических моделей текстов и их анализу с помощью позволяющего специфическим образом находить границы участков последовательностей символов в текстах метода «генетических карт»;

- **использовано** сравнение полученных с помощью предложенных модели и метода результатов с результатами обнаружения спама с применением различных рассмотренных в диссертации классификационных пайплайнов;

- **установлено**, что предложенные модель и метод по своим показателям в целом по результатам уступают только модифицированному алгоритму на основе глубоких нейронных сетей при достижении точности классификации легальных писем и спама – 0,974/0,966 и 0,995/0,990 и полноты классификации легальных писем и спама – 0,992/0,991 и 0,963/0,959 соответственно;

- **использованы** современные методы интеллектуального анализа данных и защиты информации, теория систем и системного анализа, теория принятия решений, теория эксперимента, методы контент-анализа, методы машинного обучения, методы теории вероятностей и математической статистики, методы объектно-ориентированного анализа и проектирования, а также выборочные совокупности электронных писем с обоснованием их выбора.

Личный вклад соискателя состоит в: анализе текущего уровня исследований в области обнаружения спама и непосредственно проблемы спама, существующей отечественной нормативно-правовой базы по проблеме спама и исследовании различных подходов к обнаружению спама и их особенностей; разработке модели электронного почтового сообщения на основе метода «генетических карт», учитывающей содержание электронных писем конкретного пользователя (персонализацию); разработке метода классификации электронных писем для обнаружения спама и идентификации легальных электронных писем; разработке алгоритма классификации электронных писем; разработке исследовательского прототипа подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем; планировании и проведении экспериментов, выполненных автором лично, а также в обработке, анализе и

интерпретации результатов экспериментов, подготовке научных статей и материалов докладов на российских и международных научных конференциях.

Диссертационный совет пришел к выводу о том, что в диссертации:

- соблюдены установленные Положением о порядке присуждения ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени кандидата технических наук;

- отсутствуют недостоверные сведения об опубликованных соискателем ученых степеней работах, в которых изложены основные научные результаты диссертации;

- соискатель ссылается на авторов и источники заимствования;

- оригинальность диссертационной работы составляет 85,34 %.

Диссертационная работа Корелова Сергея Викторовича «Метод и алгоритм обнаружения спама на основе выделения признаков электронных писем с использованием контентной фильтрации» соответствует п. 9 Положения о порядке присуждения ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 г. № 842 (в редакции от 25.01.2024 г.), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность по пунктам: п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»; п. 5 «Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»; п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности»

Таким образом, диссертация Корелова С. В. является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения научной задачи повышения эффективности обнаружения

спама и достоверности идентификации легальных электронных почтовых сообщений на основе классификации их содержания, имеющей важное значение для развития соответствующей отрасли знаний, связанной с совершенствованием средств защиты информации и обеспечением информационной безопасности.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. На слайде 9 указано, что при формализации задачи обнаружения спама как задачи классификации используется бинарная логика, в тоже время при обсуждении результатов эксперимента показано, что часть почтовых сообщений может быть не классифицирована.

Соискатель Корелов С.В. согласился с замечаниями и привел собственную аргументацию:

1. В ходе применение разработанной модели и метода в особых случаях возникают ситуации, при которых почтовое сообщение не может быть классифицировано ни как спам, ни как легитимное письмо. К этим случаям относятся: одновременное отсутствие термов анализируемого почтового сообщения в базах спамовых и легитимным термов, либо равное количество термов, относящихся к спаму или легитимным сообщениям. Для этих случаев введен третий класс – неизвестные сообщения. По результатам экспериментальных исследований добавлен блок нечеткой классификации.

На заседании 17.09.2024 г. диссертационный совет принял решение:

- за решение научной задачи повышения эффективности обнаружения спама и достоверности идентификации легальных электронных почтовых сообщений на основе классификации их содержания, имеющей важное значение для развития отрасли знаний, связанной с совершенствованием средств защиты информации и обеспечением информационной безопасности, присудить Корелову Сергею Викторовичу ученую степень кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 8 докторов наук по специальности защищаемой диссертации,

участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 14, против – 0, воздержались – 2.

Председатель
диссертационного совета
д-р техн. наук, профессор Султанов Альберт Ханович

Ученый секретарь
диссертационного совета
д-р техн. наук Вульфин Алексей Михайлович

17 сентября 2024 года