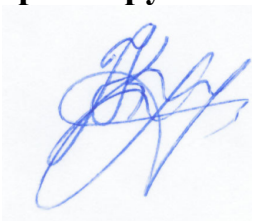
На правах рукописи



Корелов Сергей Викторович

МЕТОД И АЛГОРИТМ ОБНАРУЖЕНИЯ СПАМА НА ОСНОВЕ ВЫДЕЛЕНИЯ ПРИЗНАКОВ ЭЛЕКТРОННЫХ ПИСЕМ С ИСПОЛЬЗОВАНИЕМ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Йошкар-Ола – 2024

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

Научный руководитель: доктор технических наук, профессор, заведующий кафедрой информационной безопасности ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола
Сидоркина Ирина Геннадьевна

Официальные оппоненты:
Коробейников Анатолий Григорьевич, доктор технических наук, профессор, 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
Бурлаков Михаил Евгеньевич, кандидат технических наук, доцент кафедры безопасности информационных систем Федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С. П. Королева»

Ведущая организация: ФГБОУ ВО «Казанский национальный исследовательский технический университет имени А. Н. Туполева-КАИ», г. Казань

Защита диссертации состоится 17.09.2024 года в 10 ч. 00 мин. на заседании диссертационного совета 24.2.479.07 на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу: 450008, г. Уфа, ул. К. Маркса, д. 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский университет науки и технологий» и на сайте https://uust.ru/.

Автореферат разослан « ___ » _____ 20___ г.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время одним из наиболее распространенных способов повседневной и деловой коммуникации, а также управления являются электронные почтовые сообщения. Однако столь высокая популярность электронной почты сопровождается и рядом проблем. Одним из ставших классическим рисков, связанным с ее использованием, является спам – телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя[1].

Доказано, что спам является угрозой безопасности информации, нейтрализация которой является актуальной задачей. В связи с этим исследование, разработка, создание и внедрение новых и совершенствование существующих решений, моделей, алгоритмов, средств, систем и технологий обеспечения безопасности информационных систем, ориентированных на обнаружение (выявление) спама, является актуальной и практически значимой задачей.

При этом особенно актуальным продолжает оставаться вопрос выбора эффективных (с точки зрения качества обнаружения спама и идентификации легальных[2] сообщений) признаков электронных почтовых сообщений для их классификации, учитывающих персональные (пользовательские) особенности (с т. з. информационных потребностей) электронных писем и их содержание применительно к конкретным пользователям. Это требует разработки новых подходов к определению и выделению признаков электронных писем с учетом содержания электронных писем конкретного пользователя и оценки эффективности их применения, что позволит достичь персонализации[3] в обнаружении спама, как одного из ключевых свойств, предъявляемым к системам обнаружения спама, а также повышению его эффективности.

Степень разработанности темы исследования. Исследованиям в области обнаружения спама посвящены работы российских и зарубежных исследователей Б. В. Доброва, А. С. Катасёва, М. П. Малыхиной, Е. М. Мезенцевой, А. П. Никитина, А. Н. Розинкина, М. А. Семеновой, П. Б. Хорева, В. А. Частиковой, Е. Н. Чернопрудовой, I. Androutsopoulos, W. Cohen, S. Delany, H. Drucker, K. Junejo, K. Gee, P. Graham, V. Metsis, G. Robinson, M. Sahami, G. Sakkis, H. Shen и многих других. Ими проведены исследования и предложены теоретические и прикладные подходы к решению вопросов:

- обнаружения спама на основе анализа содержимого электронных писем с составлением их моделей и классификации текстовой информации, содержащейся в электронных письмах, с применением различных методов машинного обучения;
- оценки в различных условиях эффективности применения методов машинного обучения в задаче обнаружения спама;
- отбора признаков, необходимых для классификации электронных писем.

Проведенный автором анализ основных технологий обнаружения спама и признаков электронных писем из категории спама указывает на то, что известные модели электронных писем, как правило, не учитывают содержание легальных писем, что приводит к росту числа ошибок первого и/или второго рода.

---

[1] Постановление Правительства Российской Федерации от 10 сентября 2007 года № 575 «Об утверждении Правил оказания телематических услуг связи».

[2] Здесь и далее под легальным сообщением (сообщением, не относящимся к спаму) понимается электронное сообщение, доставленное абоненту и (или) пользователю с их предварительного согласия и позволяющее определить отправителя этого сообщения, т. е. не подпадающее под определение спама в соответствии с постановлением Правительства Российской Федерации от 10 сентября 2007 года № 575.

[3] Здесь и далее применительно к настоящему диссертационному исследованию под персонализацией понимается ориентированность на персональные (пользовательские) особенности (с т. з. информационных потребностей) электронных писем и их содержание применительно к конкретным пользователям (группе пользователей).

Поэтому разработка модели электронных писем, обеспечивающей выделение признаков электронных писем на основе их содержания, является актуальной задачей и представляет научный и практический интерес.

Объектом исследования в диссертационной работе являются технологии обнаружения спама.

Предметом исследования являются модели электронных писем и алгоритмы обнаружения спама.

Целью диссертационной работы является повышение эффективности обнаружения спама и достоверности идентификации легальных электронных почтовых сообщений на основе классификации их содержания.

Для достижения поставленной цели в работе решались следующие **задачи исследования:**

1. Анализ современного состояния исследований в области обнаружения спама.
2. Разработка модели электронного почтового сообщения, учитывающей содержание электронных писем конкретного пользователя (персонализацию).
3. Разработка метода классификации электронных писем для обнаружения спама и идентификации легальных электронных писем.
4. Разработка алгоритма классификации электронных писем.
5. Разработка архитектуры подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем.

Научная новизна

1. 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.
2. Разработан метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, основанный на положениях задачи классификации текстовых документов, отличающийся использованием разработанной модели электронных писем, применение которого позволяет повысить эффективность обнаружения спама и достоверность идентификации легальных электронных писем, а также снизить количество неклассифицированных писем.
3. Разработан алгоритм классификации электронных писем на основе методов машинного обучения, отличающийся наличием дополнительной процедуры определения «схожести» термов на основе расстояния Левенштейна[4], обеспечивающей вычисление мер принадлежности классифицируемого электронного письма к классам спама и легальных для повышения достоверности идентификации электронных писем, позволяющий осуществить программную реализацию разработанных модели и метода.
4. Разработана архитектура подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем на основе разработанного алгоритма, отличающаяся от известных блоком выделения термов и блоком нечеткой классификации, реализующая предложенные в работе метод и алгоритм, применение которых позволяет повысить достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации).

Теоретическая значимость работы

Теоретическая значимость полученных результатов заключается в том, что в работе предложены новая модель электронного почтового сообщения, учитывающая содержание электронных писем конкретного пользователя (персонализацию), метод классификации

[4] Расстояние Левенштейна – минимальное количество операций удаления, вставки и замены символа, необходимое для преобразования одной строки в другую. Используется наиболее часто для вычисления редакционного расстояния (метрики, измеряющей разность между двумя последовательностями символов), а также для исправления ошибок в слове (в поисковых системах, базах данных, при вводе текста, при автоматическом распознавании отсканированного текста или речи), сравнения текстовых файлов утилитой diff и ей подобными, а также в биоинформатике для сравнения генов, хромосом и белков.

электронных писем для обнаружения спама и идентификации легальных электронных писем, алгоритм классификации электронных писем.

Практическая значимость работы

Практическая значимость полученных результатов заключается в разработке программных модулей исследовательского прототипа подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем. Применение разработанных модели и метода позволяет повысить эффективность обнаружения спама и достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации) с точностью классификации до 0,995 и полнотой классификации до 0,993, а также снизить количество ошибочно классифицированных и неклассифицированных[5] писем.

Методы и методология исследования. Для решения поставленных в работе задач были 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.

Положения, выносимые на защиту

1. Модель электронного почтового сообщения, учитывающая содержание электронных писем конкретного пользователя (персонализацию).
2. Метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем.
3. Алгоритм классификации электронных писем.
4. Архитектура подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем.

Достоверность и обоснованность научных положений и выводов, полученных в диссертационной работе, подтверждается корректной постановкой задач, применением известных технологий и методов, успешно используемых в других прикладных областях, апробацией разработанных модели, метода, алгоритма и программных модулей. Выводы и положения диссертации научно обоснованы и подтверждены положительными оценками на научных конференциях и результатами экспериментальных исследований автора.

Апробация результатов диссертации. Основные положения и результаты диссертации докладывались и обсуждались на научных конференциях: X, XII, XIV, XV, XXIV, XXV и XXVI научных конференциях по радиофизике в Национальном исследовательском Нижегородском государственном университете им. Н. И. Лобачевского (г. Нижний Новгород, 2006, 2008, 2010, 2011, 2020-2023 годы); Международной научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2010» (г. Томск, 2010 год); научно-технической конференции «Автоматизированные системы управления и информационные технологии» АСУИТ-2020 (г. Пермь, 2020 год); XII Международной Интернет-конференции молодых ученых, аспирантов и студентов «Инновационные технологии: теория, инструменты, практика» InnoTech-2020 (г. Пермь, 2020 год); VI Всероссийской молодежной научно-практической конференции с международным участием «Информационные технологии обеспечения комплексной безопасности в цифровом обществе» (19-20 мая 2023 г., г. Уфа); Международном конгрессе по интеллектуальным системам и информационным технологиям (2-9 сентября 2023 г., Россия, Черноморское побережье, Геленджик-Дивноморское).

Результаты диссертационной работы 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).

---

[5] Установлено, что возможна ситуация, при которой класс электронного письма может быть не определен (например, равное количество признаков для обеих категорий писем).

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют следующим пунктам паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»: 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».

Публикация результатов работы. Основные результаты диссертации опубликованы в 19 печатных работах, в том числе в 4 статьях в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, и в 15 статьях в других изданиях.

Структура и объем диссертации. Диссертация включает в себя введение, четыре главы с выводами, заключение, список литературы и приложения. Основной текст работы изложен на 181 странице, содержит 29 рисунков, 37 таблиц, 6 приложений. В список используемой литературы включено 203 наименования, среди которых 89 зарубежных и 114 отечественных публикаций.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность исследуемой темы, определены объект и предмет исследования, цель и задачи исследования, научная новизна, теоретическая и практическая значимость полученных результатов, сформулированы основные положения, выносимые на защиту.

В первой главе проведен анализ современного состояния исследований в области обнаружения спама. Обосновано, что обнаружение спама является не просто желательной, а остронеобходимой и неотъемлемой частью общей системы обеспечения безопасности информационных систем.

По результатам проведенного анализа можно обоснованно предположить, что в настоящее время сложилась достаточно устойчивая и всеобъемлющая система методов, моделей и средств обнаружения спама. В целом можно выделить следующие основные группы методов обнаружения спама:

1. Основанные на черных/белых/серых списках.
2. Основанные на анализе контента (содержания) и его классификации с применением методов машинного обучения.
3. Основанные на контроле массовости рассылок.
4. Основанные на контроле различного рода вложений.

При этом в исследованиях последних лет, посвященных решению задачи обнаружения спама, как правило, используются одни и те же методы классификации или предлагаются их модификации. В то же время большое внимание уделяется вопросу выделения и отбора признаков электронных писем и оценке эффективности обнаружения спама с применением известных методов классификации, но с использованием различных признаков (и/или их сочетаний).

Проведенный анализ и обобщение имеющихся терминологических определений и признаков спама позволили выделить наиболее значимые отличительные особенности спама, представленные на рисунке 1.

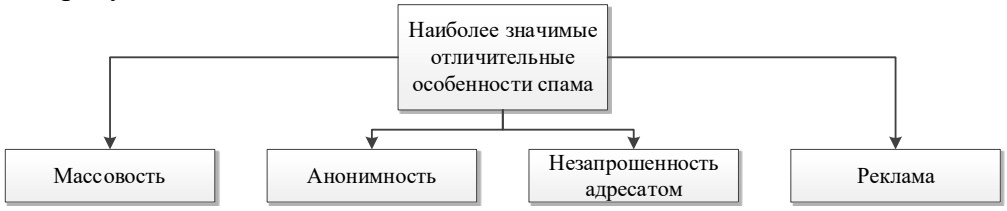


Рисунок 1 – Наиболее значимые отличительные особенности спама

На основе анализа имевшихся в распоряжении массивов англоязычного и русскоязычного спама определены группы и перечень наиболее важных информативных признаков, которые позволяют отнести то или иное электронное письмо к классу спама или легальных. Признаки электронных писем разделены на формальные (формат заголовка, электронные почтовые адреса отправителя и получателя, IP-адреса и т. п.) и лингвистические, отражающие особенности содержания электронного письма.

Проведенный анализ основных технологий обнаружения спама и признаков электронных писем выявил, что отдельные существующие системы обнаружения спама, как правило, не персонифицированы, то есть не учитывают особенности переписки конкретного пользователя, что отрицательно влияет на их точность.

Определена и формализована задача обнаружения спама как задача автоматической классификации электронных писем с использованием их значимых признаков, которую формально можно описать как задачу присвоения булевого значения $\{True, False\}$ каждой паре $\langle el_j,\ c_i\rangle \in EL \times C$,

где EL – множество классифицируемых электронных писем;

$C = \{Spam, Legal\}$ – два класса электронных писем, между которыми их необходимо распределить. $Spam$ – класс спама, $Legal$ – класс легальных электронных писем;

$\{True, False\}$ – булево значение принадлежности электронного письма el_j классу c_i – $True$ или нет – $False$.

Более формально задачу классификации электронных писем на спам и легальные можно представить как построение функции:

$$\tilde{\phi}_{el}: EL \times C \ \rightarrow \ \{True, False\}, \qquad (1)$$

которая описывает процедуру классификации писем.

Таким образом, результаты системного анализа имевшегося в распоряжении англоязычного и русскоязычного спама писем и задачи их обнаружения позволили обосновать при создании модели электронных писем целесообразность применения метода выделения термов, позволяющего усилить их смысловое содержание за счет применения метода «генетических карт». Это позволит учитывать меняющиеся информационные потребности конкретного пользователя и достичь персонализации в обнаружении спама, как одного из ключевых свойств, предъявляемым к системам обнаружения спама, а также повышению эффективности обнаружения спама.

Областью определения модели является текстовое содержание (текст) электронного письма на естественном языке.

Сформированы следующие допущения и ограничения при разработке модели и метода:

1. Электронные письма, составляющие множество, должны быть из реальных переписок (отправлений).

2. Исходное множество писем разбивается на обучающие и тестовые выборки, принадлежность писем к спаму и легальным в которых заранее известна.

3. Автор исследования обладает знаниями, обеспечивающими получение максимальных значений полноты и точности неавтоматизированной классификации электронных писем на спам и легальные.

4. Типовой размер одной информационной единицы (документов в массиве, слов в документе) ограничен объемом памяти ЭВМ.

5. Классы электронных писем являются по своей сути всего лишь символьными метками и не содержат никакой дополнительной информации, позволяющей перечислить и описать признаки именуемых ими классов.

6. Отсутствует какая-либо внешняя (по отношению к электронным письмам) информация, существенная для цели классификации, а значит классификацию электронных писем необходимо осуществлять только по их содержимому.

Необходимо отметить, что поскольку разработанная модель электронных писем по своей сути основана на содержании спама и легальных электронных писем и ориентирована на персональные (пользовательские) особенности (с т. з. информационных потребностей)

электронных писем и их содержание применительно к конкретным пользователям (группе пользователей), ее применение предоставляет возможность формировать набор термов с их маркированием по актуальности для конкретного пользователя (персональные особенности входящего потока электронных писем) и на конкретный момент времени (т. е. учитывать текущий «ландшафт» спама, его целевую направленность с т. з. его содержания).

Вторая глава посвящена разработке модели электронных писем для обнаружения спама. Для ее построения в качестве базового был выбран подход к формированию математических моделей текстов и их анализу с помощью метода «генетических карт». Разработчиком теоретических основ данного метода, а также идеологом теории структурной идентификации и анализа текстовой информации с помощью базовых параметров, является доктор технических наук, профессор К. Г. Кирьянов. Его подход зарекомендовал себя для решения задач идентификации и анализа различных текстов в разных научных областях и ранее не применялся в области обнаружения спама. Ключевой особенностью данного подхода является то, что он оперирует с преобразованными данными, полученными из исходных текстов, преобразованными в числовую последовательность, что позволяет находить границы участков последовательностей символов в текстах.

Введено понятие «терм» электронного письма, специальным образом выделенная значимая последовательность символов текста, соответствующая отдельной последовательности исходных символов текста электронного письма и соотносящаяся с признаками определенного класса электронных писем. Таким образом, термы электронных писем являются элементарными единицами, являющимися отражением отличительных признаков электронных писем.

В машинном обучении важную роль играют непосредственно сами данные, а точнее – их подготовка. На практике электронные письма поступают от разных отправителей и составляются ими с использованием различных почтовых клиентов в различных форматах. При этом они могут содержать различного рода «шумы»: ошибки и искажения различной природы; незначимые с точки зрения содержания слова; символы; неинформативные элементы, например, спецсимволы HTML; скрипты; рекламные вставки и т. п. Такие «шумы» негативно влияют на качество непосредственно самих данных для анализа и могут снизить полноту и точность классификации. Поэтому значимым этапом является предобработка текстов, представляющая собой процесс их очистки и подготовки к классификации.

В работе обосновано, что результаты обнаружения напрямую зависят от выбора способов предобработки в совокупности со значениями параметров разработанной модели. Кроме того, обосновано среди способов предобработки рассматривать только предварительную очистку (предобработку) писем от повторений символов пробелов, табуляции и переносов строк и перевод всех букв в верхний (нижний) регистр.

Теоретические и экспериментальные исследования показали, что применение каких-либо иных способов предобработки целесообразно только при условии их предварительной экспериментальной оценки и постоянной периодической корректировки с течением времени для адаптации метода классификации применительно к индивидуальным особенностям написания электронных писем их автором.

Для описания модели введены следующие условные обозначения:

Ψ_{el} – модель электронного почтового сообщения;

$EL = \{el_i\}$ – множество электронных писем, представленных в виде текстов на естественном языке;

$el = (sym_0, sym_1, \dots, sym_{M-2}, sym_{M-1})$ – электронное письмо, представленное в виде конечной последовательности символов;

$M = |el|$ – длина электронного письма (количество символов в электронном письме);

B – множество десятичных значений байт, соответствующих символам в кодовой таблице, используемой для представления текста в виде числовой последовательности;

b – десятичное значение байта, соответствующего конкретному символу электронного письма в кодовой таблице, используемой для представления текста в виде числовой последовательности;

t_j – терм электронного письма – значимая последовательность исходных символов текста электронного письма;

$T = \{t_j\}$ – множество термов электронного письма;

$l_j = |t_j|$ – длина терма электронного письма (количество символов в терме);

$T^C = \{t_j^C\}$ – множество термов заданного класса электронных писем.

На основе указанного подхода модель электронных писем может быть представлена в виде кортежа:

$$\Psi_{el} = \langle EL, EL\_PrePoc, T\_Proc, T\rangle, \quad (2)$$

где EL_PrePoc – процедура предобработки электронных писем

$$EL\_PrePoc = \{ws\_reps\_del, tabs\_reps\_del, lb\_reps\_del, up\_case\}, \quad (3)$$

где ws_reps_del – процедура удаления повторов пробелов;

$tabs\_reps\_del$ – процедура удаления повторов символов табуляции;

lb_reps_del – процедура удаления повторов переносов строк;

up_case – процедура перевода всех букв в верхний регистр;

T_Proc – процедура выделения термов – значимых последовательностей исходных символов текста электронного письма:

$$T\_Proc = \langle el, Conv\_to\_Dig(el), \mathrm{s},\ H_1\rangle. \quad (4)$$

При этом

$Conv\_to\_Dig(el)$:

$$el = (sym_0, sym_1, \dots, sym_{M-2}, sym_{M-1}) \xrightarrow{q,\Delta t} el' = (b_0, b_1, \dots, b_{M-2}, b_{M-1}), \quad (5)$$

где q – размер кодовой таблицы, используемой для представления текста в виде числовой последовательности;

Δt – шаг выборки символов текста в процедуре преобразования писем в числовую последовательность,

s – числовая последовательность (выборка терма)

$$s = (b_k, b_{k+1}, \dots, b_{k+n-2}, b_{k+n-1}), \quad (6)$$

для которой справедливы условия:

$$\begin{cases} k \in Z, \\ 1 \le k \le (M-n)' \end{cases} \quad (7)$$

H_1 – алгоритм определения границ терма.

Выборка является, по сути, характерной единицей терма, обладающей следующими ключевыми параметрами:

n – длина выборки (N-граммы – последовательности, порождающей терм);

k – начальная позиция выборки в пределах числовой последовательности, представляющей текст электронного письма.

Параметрами модели (2), оказывающими влияние на выделение термов, являются:

q – размер кодовой таблицы, используемой для представления текста в виде числовой последовательности;

Δt – шаг выборки символов текста в процедуре преобразования писем в числовую последовательность;

n – длина выборки (N-граммы – последовательности, порождающей терм).

Необходимо отметить, что все обучаемые модели требуют подходящего для них представления электронных писем, что лежит в области решения задач обработки естественного языка (NLP, аббр. от англ. Natural Language Processing). Широкое распространение по использованию в обработке естественных языков в целом и в решении задач классификации текстов получило представление электронных писем в виде набора слов («bag of words» – мешок слов), появляющихся в спаме или легальных письмах, с их количественными характеристиками. Данное представление просто в реализации, но не учитывает контекст применения слов. Для учета контекста появления тех или иных слов применяются представления в виде n-граммы слов, а также представления в виде векторных вложений («word embedding»), позволяющие учесть связь слов с другими словами в предложении или тексте.

Проводя аналогию между предложенной моделью и описанными подходами, автор приходит к выводу, что по своей сути выборка является n-граммой символов, являющейся отражением отличительного признака электронного письма. При этом модель делает возможным выделение неизменных в пределах нескольких писем участков (именно участков, а не просто последовательностей символов и слов и их последовательностей) с учетом их контекста и позволяет снизить влияние на обнаружение спама таких условий, как, например, начальный символ (слово) письма, «мусорные» символы и слова, грамматические и пунктуационные ошибки и т. п.

Таким образом, предложенная модель является развитием подхода представления «bag of words» и по своей сути представляет собой смешанное представление: частично в виде набора слов и частично в виде векторных вложений, – и может быть использована как соответствующий элемент любого из существующих классификационных пайплайнов в области обнаружения спама. Модель позволяет учитывать информацию на различных уровнях: лексическом (слова и их части) и синтаксическом (словосочетания и их части и предложения и их части, в том числе в контексте частей других частей слов, слов, частей предложений и предложений). Такое представление позволяет избежать недостатков представления «bag of words» с одновременным использовании преимуществ «bag of words» и «word embedding». При этом становится практически невозможным осуществить подбор текста под модель, поскольку использование «легальных» слов и сочетаний в спаме будет нивелировано способом выделения термов.

Сформированная модель электронных писем позволяет осуществить программную реализацию процедуры последовательной разбивки электронных писем на термы. На сформированных наборах англоязычных и русскоязычных писем обоснованы корректность и практическая применимость разработанной модели электронных писем, обоснованы значения ее параметров, оказывающих влияние на выделение термов, а также что модель не зависит от конкретного набора символов и их количества (не зависит от кодировки), т.е. является символонезависимой.

Наилучшие результаты обнаружения спама достигаются при следующих численных значениях ключевых параметров:

- q должно обеспечивать полное символьное разнообразие, т.е. быть равно количеству кодов в соответствующей кодировке;
- $\Delta t = 1$;
- $n = 1$ и $n = 2$.

При этом продемонстрированы неслучайность результатов обнаружения спама с применением разработанной модели и целесообразность применения весовых коэффициентов термов и процедуры сокращения размерности признакового пространства.

В третьей главе разработаны метод и алгоритм классификации электронных писем для обнаружения спама и идентификации легальных электронных писем.

Результаты анализа современных исследований, посвященных задачам классификации текстовых документов, позволили автору сформулировать следующие дополнительные ключевые ограничения и допущения в отношении модели и метода:

- классы электронных писем являются по своей сути всего лишь символьными метками и не содержат никакой дополнительной информации, позволяющей перечислить и описать признаки именуемых ими классов (категорий);
- отсутствует какая-либо внешняя (по отношению к электронным письмам) информация, существенная для цели классификации, а значит классификацию электронных писем необходимо осуществлять только по их содержимому (что полностью соотносится с выбранным подходом к обнаружению спама).

Принятые исходные ключевые ограничения позволяют обеспечить независимость предлагаемых модели электронных писем и метода классификации электронных писем и результатов их применения от любой внешней информации об электронных письмах (например, источник и формат электронных писем, дата их получения, адресат и др.) и использовать исключительно их содержание.

Разработанный метод классификации электронных писем представлен в виде последовательности шести этапов:

1. Предварительная обработка текстов электронных писем EL_PrePoc.

2. Построение признакового пространства (выделение термов) T_Proc.

Данные этапы реализуются через разработанную модель электронных писем Ψ_{el}.

3. Расчет весов термов – процедура ϕ_T^W.

4. Сокращение размерности признакового пространства – процедура ϕ_T^{DR}.

Данные четыре этапа также используются при формировании базы данных термов спама и легальных писем в режиме обучения на обучающем наборе электронных писем $EL^{tr} \subseteq EL$, для каждого электронного письма $el_i^{tr} \in EL^{tr}$ из которого известен его класс $c_k^{tr} \subseteq C$.

5. Определение классов электронных писем (множество $EL = \{el_i\}$) с использованием задаваемого способа классификации – процедура $\tilde{\phi}_{\Psi_{el}}$.

6. Определение классов неклассифицированных на этапе 5 электронных писем с применением подхода к определению «схожести» термов на основе расстояния Левенштейна (нечеткая классификация), которое можно получить путем расчета элементов матрицы D по следующей формуле:

$$D(i,j) = \begin{cases} 0, i = 0, j = 0 \\ i, j = 0, i > 0 \\ j, i = 0, j > 0 \\ min\{ \\ D(i, j-1) + 1 \\ D(i-1, j) + 1, i > 0, j > 0 \\ D(i-1, j-1) + m(S_1[i], S_2[j]) \\ \} \end{cases}, \quad (8)$$

где $d(t_1, t_2) = D(l_1, l_2)$ – редакционное расстояние между термами t_1 и t_2;

i, j – номера строк и столбцов матрицы, где $0 \le i \le l_1, 0 \le j \le l_2$;

$S_1[i], S_2[j]$ – символы термов, соответствующие строкам и столбцам (позициям) i и j;

$m(S_1[i], S_2[j])$ – оператор, $m(S_1[i], S_2[j]) = 1$, если символы $S_1[i]$ и $S_2[j]$ не равны друг другу, и $m(S_1[i], S_2[j]) = 0$ – в противном случае.

По своей сути предложенный метод относится к группе методов, основанных на анализе контента (содержания) и его классификации с применением методов машинного обучения.

В качестве частных показателей эффективности использованы полнота R, оценивающая долю правильной классификации относительно всех объектов определенного класса, точность P, оценивающая долю верной классификации относительно всех объектов, и сводная оценка качества обнаружения классификации – F-мера. Тогда обобщенный показатель эффективности метода классификации электронных писем для обнаружения спама, обеспечивающего точность и полноту обнаружения спама и достоверность идентификации легальных электронных почтовых сообщений, будет иметь следующий вид:

$$Y = \langle R, P, F \rangle \quad (9)$$

Необходимо отметить, что для любого пользователя требуется максимальная полнота обнаружения легальных писем, что выдвигает требования к максимальному значению точности обнаружения спама. Также условием, безусловно, является максимальность F-меры обнаружения спама, демонстрирующая в таких условиях наилучший показатель обнаружения спама при одновременно максимальном значении обнаружения легальных писем. Следовательно, наилучший показатель обнаружения спама и легальных писем одновременно будет достигаться при их максимальных значениях F-меры.

Поскольку возможна ситуация, когда максимальное значение F-меры для спама будет достигаться при использовании одного правила классификатора, а для легальных писем – для другого, то целесообразно оценивать эффективность по единому значению, полученному на основе обоих значений F-мер, например, по их среднему гармоническому:

$$Y = HM(F^{Legal}, F^{Spam}). \quad (10)$$

Предложенный подход к оценке эффективности метода классификации электронных писем позволяет пользователю экспериментальным путем самостоятельно проводить оценку требуемого уровня эффективности путем настройки пороговых значений (критерия эффективности), «настраивая» метод под личные предпочтения. Данный подход позволяет сделать метод обнаружения спама персонализированным.

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 писем для повышения достоверности идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации), а также уменьшение количества неклассифицируемых писем, представлен на рисунке 2.

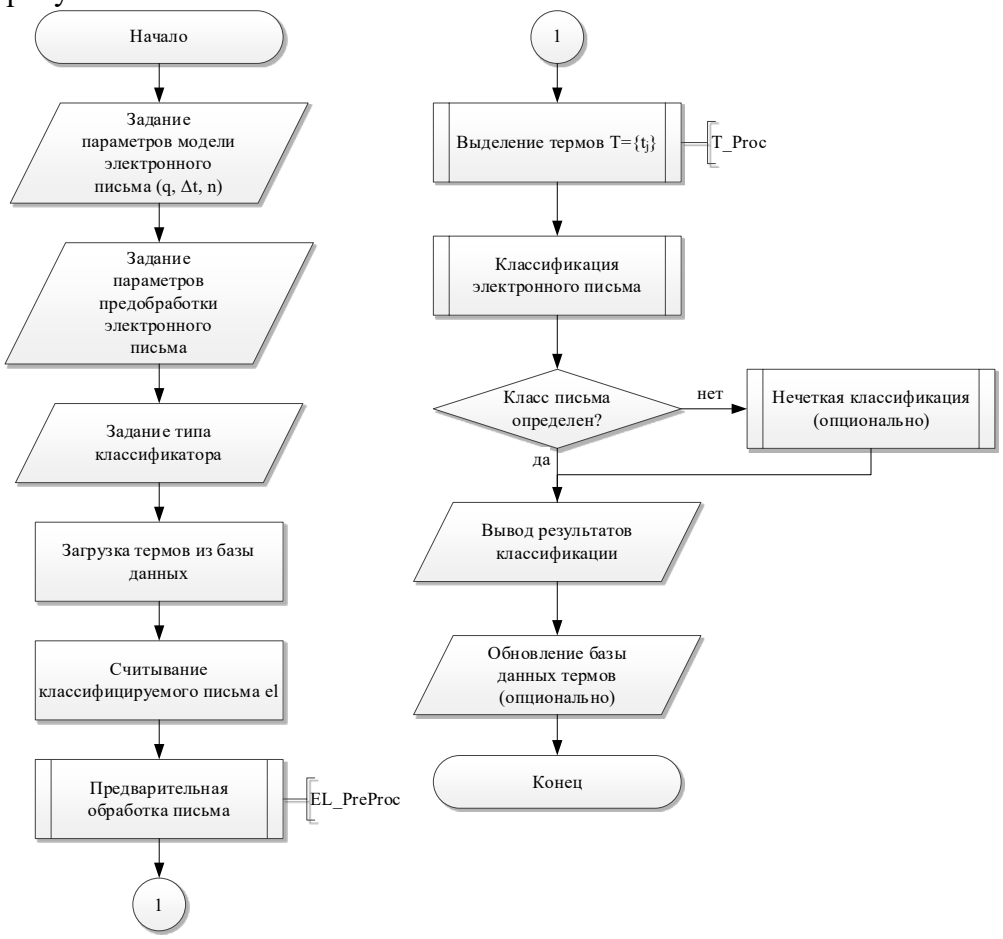


Рисунок 2 – Укрупненный алгоритм классификации электронных писем

Результаты анализа современных исследований, посвященных изучению методов машинного обучения в контексте решения задачи обнаружения спама, позволили автору прийти к следующим выводам:

1. Не существует универсального алгоритма, сочетающего достоинства малой вычислительной сложности и малой ошибки классификации при любых начальных условиях.
2. Малая ошибка отдельных методов достигается за счет существенного увеличения времени обучения и применения слабо формализуемых подходов к настройке их параметров.
3. В зависимости от состава обучающей выборки возможно получение противоречивых результатов в случае применения одного и того же метода.
4. В зависимости от состава обучающей выборки возможно получение соизмеримых ошибок при использовании разных методов. При этом время классификации может заметно отличаться.

Необходимо отметить, что в диссертационном исследовании не рассматривается вопрос обоснования выбора процедур классификации электронных писем, а их использование в

разработанном методе классификации электронных писем обусловлено только демонстрацией его работоспособности в целом и модели электронного почтового сообщения в частности. В связи с этим, а также, принимая во внимание, с одной стороны простоту реализации и обучения, интерпретируемость и устойчивость результатов, а с другой стороны малую ошибку классификации текстовой информации, в настоящем исследовании для оценки применения разработанных модели и метода классификации электронных писем для обнаружения спама и идентификации легальных электронных писем использованы:

- простое решающее правило;
- косинусная мера.

В четвертой главе разработана архитектура подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем (представлена на рисунке 3), отличающаяся от известных блоком выделения термов, реализующим разработанную модель электронного письма, и блоком нечеткой классификации, реализующим дополнительную процедуру определения «схожести» термов, а также проведены экспериментальные исследования, позволившие обосновать практическую применимость и эффективность разработанных модели и метода.

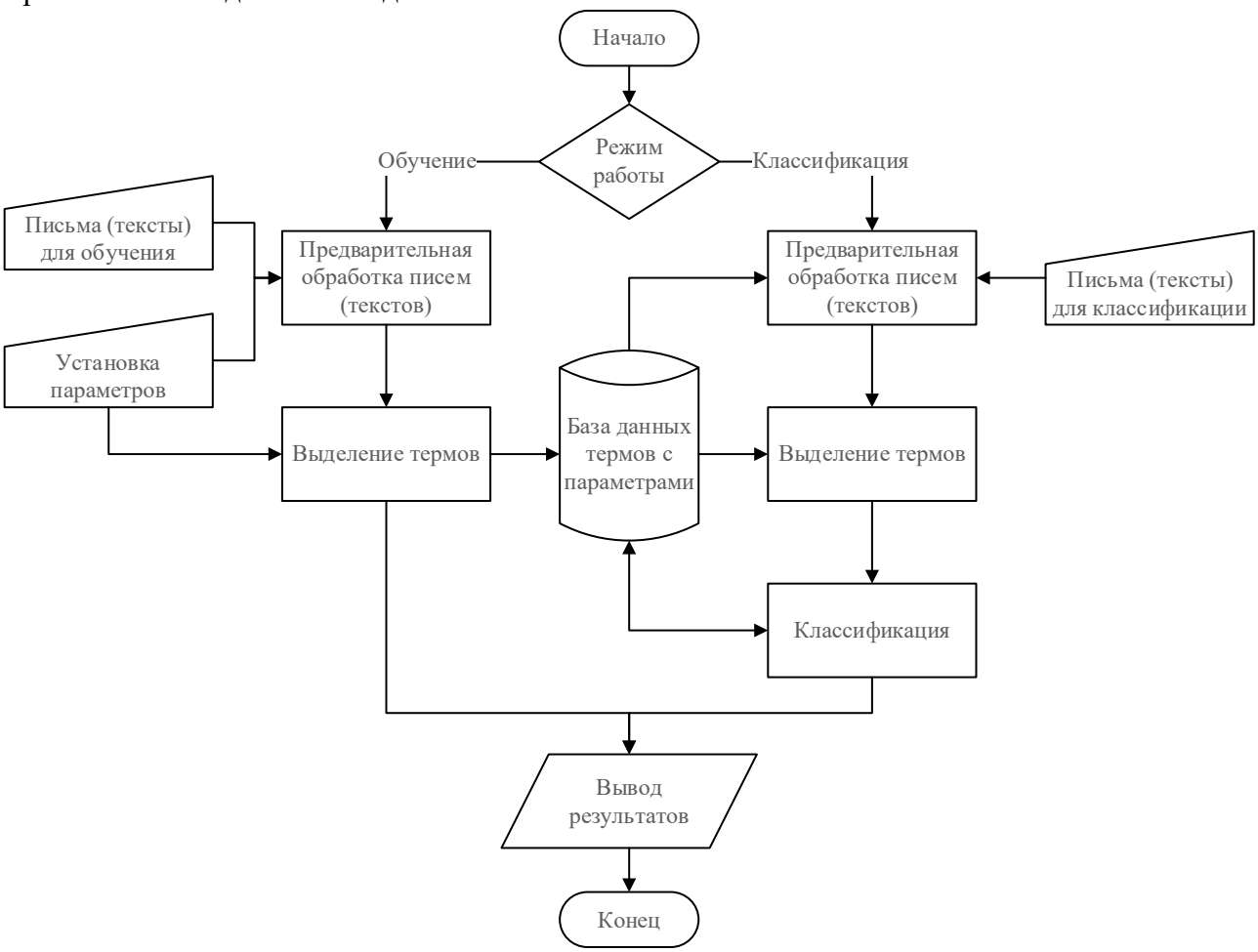


Рисунок 3 – Архитектура подсистемы классификации электронных писем

Практическое внедрение предложенной архитектуры подсистемы может быть реализовано:

- путем интеграции в существующее продуктовое антиспам-решение с позиции его разработчика в виде отдельного, задействуемого для электронного почтового ящика конкретного пользователя модуля;
- в виде дополнения для существующих продуктовых антиспам-решений, поддерживающих подключение дополнений сторонних разработчиков (например, SpamAssasin);
- в виде дополнения для почтовых клиентов.

При этом предложенная подсистема может стать дополнительным рубежом для обнаружения спама с дополнительным набором семантических признаков. Ее использование для почтового сервиса организаций может позволить пользователю простыми манипуляциями именно со своим почтовым ящиком:

- создавать персональную базу данных термов спамовых и легальных писем;
- стать дополнительным рубежом классификации писем, не классифицированных существующими решениями, в том числе ориентированных на персональные (пользовательские) особенности (с т. з. информационных потребностей) применительно к конкретным пользователям.

В программной реализации подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем были использованы метод нисходящего проектирования, который иногда называют функциональной декомпозицией, и метод модульного программирования.

Блок нечеткой классификации задействуется в случае, если классификатор не позволил определить класс электронного письма. В этом случае для определения принадлежности письма к спаму или легальным может быть задействована процедура нечеткой классификации, использующая функцию расстояния Левенштейна. В ходе ее выполнения каждый терм электронного письма последовательно сравнивается с каждым термом базы данных термов легальных писем и спама. Для каждого сравниваемого терма выбираются максимально близкие термы в соответствующих классах. Каждому терму присваивается класс на основании его максимальной близости с одним из термов базы данных. При этом если значение близости терма к термам спама и легальным термам равно, то ему присваивается неопределенный класс. В завершении осуществляется расчет общего количество термов каждого класса, по большему количеству которых принимается решение о принадлежности письма к спаму или легальным письмам. При этом в случае равенства термов обоих классов письмо считается неклассифицированным.

Разработаны программные модули исследовательского прототипа подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, позволяющий решать следующие задачи: классификация электронных писем; настройка предварительной обработки электронных писем, параметров моделей письма и выбора процедур метода классификации; обучение классификатора на спаме и легальных письмах; ведение базы данных термов; ввод и обновление информации в базе данных; формирование файлов с результатами классификации.

При проведении экспериментальных исследований использован метод кросс-валидации. Для проведения эксперимента сформированы поднаборы англоязычных писем набора Enron, состоящие из 4 групп легальных писем общим количеством 13 195 писем и 4 групп спама общим количеством 13 577 писем, количественный состав которых приведен в таблице 1. До настоящего времени набор Enron не утратил своей актуальности и продолжает оставаться одним из самых востребованных и наиболее распространенным в исследованиях в области обнаружения спама. На нем продолжают проводить исследования и эксперименты разные исследователи и исследовательские группы.

Таблица 1 – Набор электронных писем для проведения эксперимента

	Поднабор 14		Поднабор 25		Поднабор 36		Поднабор 53	
	legal1	spam4	legal2	spam5	legal3	spam6	legal5	spam3
Кол-во писем	3 618	4 237	4 189	3 551	3 980	4 337	1 408	1 452

На первом этапе экспериментальных исследований проведены испытания на поднаборах 14, 25, 36 с использованием классификаторов на основе решающего правила и косинусной меры с различными весами термов. Это позволило выбрать веса (для разного типа классификаторов), показавшие наилучшие результаты обнаружения.

На втором этапе экспериментальных исследований проведены испытания на поднаборе 53, состоящем из примерно одинакового количества термов спама и легальных термов, с использованием выбранных на первом этапе весов и с использованием снижения размера

признакового пространства на основе индекса Джини. Оно осуществлялось путем уменьшения количества уникальных термов по задаваемому порогу в виде значения индекса Джини. В результате произведено уменьшение количество уникальных термов примерно до 20% от исходного количества (в среднем с 135 415 до 23 423 при значении индекса Джини равным 0,000003). Пороговое значение выбрано по правилу Парето.

Анализ результатов экспериментальных исследований позволяет сделать следующие выводы:

1. Разработанные модель электронного почтового сообщения и метод классификации электронных писем позволяют эффективно обнаруживать спам и идентифицировать легальные электронные письма.

2. Разработанная модель электронных писем является универсальной с т. з. содержания (текстов) электронных писем. Параметры модели не зависят от обучающего набора электронных писем $EL^{tr} \subseteq EL$ и процедур ϕ_T^W, ϕ_T^{DR}, $\tilde{\phi}_{\Psi_{el}}$.

3. Разработанный метод классификации электронных писем позволяет использовать не только знания о спаме, но и о легальных письмах. Это позволяет повысить не только эффективность обнаружения спама, но и снизить вероятность ошибочной классификации легальных писем. Т. е. метод позволяет «задавать» необходимое качество обнаружения спама с учетом легальных писем.

4. В составленной схеме эксперимента наиболее эффективной процедурой классификации явилось простое решающее правило с единичным весом или мерой $TF - IDF$ в формулировке поисковой системы $INQUERY$:

$$w_{ij} = \beta + (1 - \beta) \cdot tf_{ij} \cdot idf_j. \tag{11}$$

При этом

$$tf_{ij} = \frac{\frac{n_{ij}}{N_T}}{\frac{n_{ij}}{N_T} + 0{,}5 + 1{,}5 \cdot \frac{N_T}{\overline{N_T}}}, \tag{12}$$

$$idf_j = \frac{\log\left(\frac{N_{EL}+0{,}5}{n_j}\right)}{\log(N_{EL}+1)}. \tag{13}$$

где n_{ij} – количество вхождений j-го терма в i-м письме;

N_T – общее число всех термов в заданном письме;

$\overline{N_T}$ – среднее число термов в одном письме (в термах);

N_{EL} – количество всех писем;

n_j – количество писем, в которых встречается j-й терм;

$\beta = 0{,}4$.

Применение процедуры нечеткой классификации продемонстрировало повышение эффективности обнаружения спама и достоверности идентификации легальных электронных писем, а также снижение количества неклассифицированных писем.

На первом этапе получены следующие наилучшие значения (при наилучшем показателе эффективности) с единичным весом и весом в формулировке поисковой системы $INQUERY$:

- для простого решающего правила: точность классификации легальных писем и спама – 0,974/0,966 и 0,995/0,990, полноты классификации легальных писем и спама – 0,993/0,991 и 0,963/0,959 соответственно;

- для косинусной меры: точность классификации легальных писем и спама – 0,979/0,979 и 0,914/0,914, полноты классификации легальных писем и спама – 0,919/0,919 и 0,971/0,971 соответственно.

На втором этапе получены следующие наилучшие значения с единичным весом и весом в формулировке поисковой системы $INQUERY$:

- для простого решающего правила: точность классификации легальных писем и спама – 0,945/0,907 и 0,987/0,967, полноты классификации легальных писем и спама – 0,974/0,968 и 0,924/0,902 соответственно;

- для косинусной меры: точность классификации легальных писем и спама – 0,861/0,861 и 0,996/0,996, полноты классификации легальных писем и спама – 0,996/0,996 и 0,842/0,842 соответственно.

Результаты второго этапа в случае простого решающего правила демонстрируют незначительное ухудшение значений частных показателей качества при примерно пятикратном уменьшении количества термов.

5. Несбалансированность классов обучающей выборки электронных писем влияет на эффективность классификации.

Таким образом, результаты экспериментальных исследований подтверждают достижение поставленной цели диссертационного исследования и свидетельствуют о применимости и эффективности метода с использованием разработанной модели (как степени приспособленности метода для обнаружения спама и идентификации легальных электронных писем как такового).

Дополнительно было проведено сравнение результатов эксперимента на исследовательском прототипе с результатами аналогичных исследований. Проведенный в главе 1 анализ современного состояния исследований в области обнаружения спама позволяет провести сравнение результатов проведенного эксперимента с результатами обнаружения спама с применением различных классификационных пайплайнов на наборе писем Enron без постановки практического эксперимента.

Результаты сравнения представлены в таблице 2.

Таблица 2 – Сравнение результатов эксперимента с результатами аналогичных исследований

Классификатор	P	R	FP_rate	FN_rate	F-мера
Глубокие нейронные сети	n/a	**0,9983**[6]	0,0212	**0,0017**	n/a
J48[7]	0,93	0,933	0,284	0,067[8]	0,93
Опорные вектора	0,898	0,884	0,671	0,116[9]	0,85
Байесовский	0,951	0,931	0,022	0,069[10]	0,936
LazyIBK[11]	0,924	0,892	0,095	0,108[12]	0,901
Случайный лес + AABC[13]	0,762	0,711	n/a	0,289[14]	0,7356
Случайный лес + AACO[15]	0,8427	0,7676	n/a	0,2324[16]	0,8034
Случайный лес + APSO[17]	0,8831	0,8554	n/a	0,1446[18]	0,8690
Решающее правило (ед. вес)	0,995	0,963	**0,005**	0,037	0,979
Решающее правило (вес $INQUERY$)	0,990	0,959	0,01	0,041	0,974
Косинусная мера (ед. вес)	0,914	0,971	0,079	0,029	0,941
Косинусная мера (вес $INQUERY$)	0,914	0,971	0,079	0,029	0,941

Анализ результатов сравнения показывает, что среди сравниваемых предложенные модель и метод по своим показателям в целом по результатам уступают только модифицированному алгоритму на основе глубоких нейронных сетей.

---

[6] Получено расчетным способом.

[7] Реализация на языке Java алгоритма для построения дерева решений C4.5.

[8] Получено расчетным способом.

[9] Получено расчетным способом.

[10] Получено расчетным способом.

[11] Реализация в Weka (свободное программное обеспечение для анализа данных и машинного обучения) k-ближайших соседей.

[12] Получено расчетным способом.

[13] Адаптированный алгоритм пчелиной колонии (AABC, *аббр. от англ.* adapted artificial bee colony).

[14] Получено расчетным способом.

[15] Адаптированный муравьиный алгоритм (AACO, *аббр. от англ.* adapted ant colony optimization).

[16] Получено расчетным способом.

[17] Адаптированный алгоритм роя частиц (APSO, *аббр. от англ.* Adapted particle swarm optimization)

[18] Получено расчетным способом.

В заключении подводятся основные итоги диссертационного исследования, формулируются основные выводы.

В приложениях приведены результаты экспериментальных исследований по обоснованию модели электронных писем и значений ее параметров.

Перспективы дальнейшего исследования. В дальнейшем целесообразно провести исследование эффективности метода классификации в зависимости от различных процедур сокращения размерности признакового пространства, правил классификации электронного письма, а также зависимости выбираемых процедур метода классификации электронных писем от соотношения количества известных термов спама и легальных термов.

В связи с тем, что в реальной практике превалируют несбалансированные обучающие выборки легальных писем и спама, целесообразно провести исследование по выбору техники искусственной модификации наборов и их параметров для выравнивания соотношения классов электронных писем.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ современного состояния исследований в области обнаружения спама, результаты которого позволили выделить наиболее значимые отличительные особенности спама, определить группы и перечень наиболее важных информативных признаков, которые позволяют отнести то или иное электронное письмо к классу спама или легальных, обосновать целесообразность использования при создании модели электронных писем метода выделения термов, позволяющего усилить смысловое содержание термов за счет применения метода «генетических карт».

2. 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.

3. 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.

4. 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.

5. Разработана архитектура подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, отличающаяся от известных блоком выделения термов и блоком нечеткой классификации, реализующая предложенные в работе метод и алгоритм, применение которых позволяет повысить достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации).

6. Разработаны программные модули исследовательского прототипа подсистемы классификации электронных писем и экспериментально продемонстрирована обоснованность разработанных в диссертационном исследовании модели электронного почтового сообщения и метода классификации электронных писем, а также их эффективность со следующими наилучшими результатами (при наилучшем показателе эффективности): точность классификации легальных писем и спама – 0,974/0,966 и 0,995/0,990, полнота классификации легальных писем и спама – 0,992/0,991 и 0,963/0,959 соответственно.

Совокупность результатов диссертационного исследования дает основание утверждать, что достигнута цель работы – повышена эффективность обнаружения спама и достоверность идентификации легальных электронных почтовых сообщений на основе классификации их содержания.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК:

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.

Другие публикации по теме диссертации:

5. Корелов С. В., Крюков А. К., Ротков Л. Ю. Применение метода построения генетической карты текста для идентификации спама // Труды XII научной конференции по радиофизике, посвященной 90-летию со дня рождения М. М. Кобрина (Нижний Новгород, 7 мая 2008 г.) /Под ред. А. В. Якимова, С. М. Грача. Нижний Новгород: Изд-во ТАЛАМ, 2008. С. 277-278.

6. Агаджанов В. В., Корелов С. В., Ротков Л. Ю. Обнаружение спама при помощи аппарата wavelet-преобразований // Труды XII научной конференции по радиофизике, посвященной 90-летию со дня рождения М. М. Кобрина (Нижний Новгород, 7 мая 2008 г.) /Под ред. А. В. Якимова, С. М. Грача. Нижний Новгород: Изд-во ТАЛАМ, 2008. С. 276-277.

7. Корелов С. В., Грачева О. К. Идентификация спама на классах сообщений // Труды XIV научной конференции по радиофизике, посвященной 80-й годовщине со дня рождения Ю. Н. Бабанова (Нижний Новгород, 7 мая 2010 г.) /Под ред. С. М. Грача, А. В. Якимова. Нижний Новгород: ННГУ, 2010. С. 288-289.

8. Корелов С. В., Ротков Л. Ю. Метод генетических карт в задаче идентификации спама // Информационно-измерительные и управляющие системы. 2011. № 3. Т. 9. С. 72-75.

9. Корелов С. В. Обнаружение текстового спама методом генетических карт // Труды XV научной конференции по радиофизике, посвященной 110-й годовщине со дня рождения А. А. Андронова (Нижний Новгород, 1-13 мая 2011 г.) /Под ред. С. М. Грача, А. В. Якимова. Нижний Новгород: ННГУ, 2011. С. 265-267.

10. Корелов С. В., Ротков Л. Ю. Идентификация текстового спама методом генетических карт // Вестник Нижегородского университета им. Н. И. Лобачевского. 2012. № 4 (1). С. 101-104.

11. Корелов С. В., Петров А. М., Ротков Л. Ю., Горбунов А. А. Определение длины выборки в модели электронных писем // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2020. № 4 (36). С. 31-47. DOI:10.15593/2224-9397/2020.4.02.

12. Корелов С. В., Петров А. М., Ротков Л. Ю., Горбунов А. А. К вопросу об определении численного значения параметра в модели электронных писем // Труды XXIV научной конференции по радиофизике, посвященной 75-летию радиофизического факультета (Нижний Новгород, 13 – 31 мая 2020 г.). Нижний Новгород: ННГУ, 2020. С. 471-474.

13. Корелов С. В., Петров А. М., Ротков Л. Ю., Горбунов А. А. К вопросу об определении численного значения параметра модели электронных писем // Материалы всероссийской научно-технической конференции «Автоматизированные системы управления и информационные технологии» (г. Пермь, 9–11 июня 2020 г.). 2020. Т.2. С. 519-525.

14. Корелов С. В., Петров А. М., Ротков Л. Ю., Горбунов А. А. Комбинирование значений параметра модели электронных писем // Материалы XII Международной интернет-конференции молодых ученых, аспирантов, студентов «Инновационные технологии: теория, инструменты, практика» (г. Пермь, 16 ноября – 31 декабря 2020 г.). 2020. С. 448-455.

15. Корелов С. В., Петров А. М., Сидоркина И. Г., Горбунов А. А. Анализ результатов реализации подхода к выделению термов в модели электронных писем на случайность // Труды XXV научной конференции по радиофизике, (Нижний Новгород, 14 – 26 мая 2021 г.). Нижний Новгород: ННГУ, 2021. С. 498-502.

16. Корелов С. В., Петров А. М., Сидоркина И. Г., Ротков Л. Ю. Применение весов термов в задаче обнаружения спама с использованием модели электронных писем // Труды XXVI научной конференции по радиофизике, посвященной 120-летию М. Т. Греховой, (Нижний Новгород, 12 – 27 мая 2022 г.). Нижний Новгород: ННГУ, 2022. С. 522-526.

17. Корелов С. В., Петров А. М., Сидоркина И. Г., Ротков Л. Ю. Подсистема классификации электронных писем на основе модели электронных писем // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 19-20 мая 2023 года) / отв.ред. Д. С. Юнусова – Уфа: РИЦ УУНиТ, 2023. – С. 31-35.

18. Корелов С. В., Петров А. М., Сидоркина И. Г., Ротков Л. Ю. Применение весов термов в задаче обнаружения спама // Труды XXVII научной конференции по радиофизике (Нижний Новгород, 15 – 25 мая 2023 г.). Нижний Новгород: ННГУ, 2023. С. 516-521.

19. Корелов С. В., Петров А. М., Сидоркина И. Г., Ротков Л. Ю. Модель процесса классификации электронных писем и алгоритм его реализации в задаче обнаружения спама // Труды Международного научно-технического конгресса «Интеллектуальные системы и информационные технологии – 2023» («ИС & ИТ-2023», «IS&IT’23»). Научное издание в 2-х т. Т. 2. – Таганрог: Изд-во Ступина С. А., 2023. С. 3-9.

Соискатель  С. В. Корелов