УТВЕРЖДАЮ
Проректор по научной и
инновационной деятельности
ФГБОУ ВО «КНИТУ-КАИ»
доктор технических наук, доцент

_____ В.М. Бабушкин

«26» 08 2024 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию Корелова Сергея Викторовича

на тему **«Метод и алгоритм обнаружения спама на основе выделения признаков электронных писем с использованием контентной фильтрации»**,

представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Современный этап развития деловой и управленческой коммуникации характеризуется широким применением технологии электронной почты. Данное обстоятельство неизбежно усложняет задачу обеспечения информационной безопасности различного рода информационных систем органов государственной власти и организаций и предприятий промышленности различных сфер деятельности, в том числе объектов критической информационной инфраструктуры Российской Федерации, функционирование которых жизненно важно для государства.

Вместе с тем несмотря на неоспоримые преимущества, которые дает применение электронной почты, статистика последних лет свидетельствует о ее непрекращающемся использовании злоумышленниками в качестве одного из наиболее распространенных способов для начального проникновения в

информационные системы. Это предполагает решение задачи своевременного обнаружения спамовых писем с целью предотвращения возможных компьютерных инцидентов и негативных последствий, которые могут возникнуть в результате открытия данных писем пользователями и выполнения определенных действий по их содержанию. В то же время, известные алгоритмы выявления спама не в полной мере учитывают содержание сообщений электронной почты, информационная направленность которых для конкретного пользователя может изменяться со временем или в соответствии с решаемой задачей.

С учетом вышеизложенного, тема диссертационной работы Корелова С.В., посвященная разработке и исследованию новых методов и алгоритмов обнаружения спама и идентификации легальных электронных писем на основе классификации их содержания, несомненно, является актуальной.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Диссертационная работа изложена на 181 странице, включает 29 рисунков, 37 таблиц и 6 приложений.

Во введении обоснована актуальность работы, степень разработанности темы исследования, приведены объект и предмет исследования, использованные методы, сформулированы цель и задачи диссертационной работы, положения, выносимые на защиту, представлены научная новизна и практическая значимость результатов научного исследования.

Первая глава посвящена анализу современного состояния исследований в области обнаружения спама и непосредственно проблемы спама. Проанализирована существующая отечественная нормативно-правовая база, затрагивающая вопросы спама. Рассмотрены различные подходы к обнаружению спама и их особенности. На основе результатов проведенного анализа сделан вывод об актуальности проблемы выбора признаков электронных писем, обеспечивающих высокое качество выявления спама и

идентификации легальных сообщений, с учетом персональных информационных потребностей пользователя при классификации сообщений электронной почты. Ее решение предложено осуществить за счет разработки новой модели электронного письма на основе математических моделей текстов и их последующего анализа с использованием метода «генетических карт».

Во второй главе предложена модель электронных писем для обнаружения спама, описаны ее параметры, оказывающие влияние на выделение термов. Приведены результаты вычислительных экспериментов по оценке корректности и применимость разработанной модели, а также неслучайности получаемых с ее применением результатов. Одновременно обоснован выбор значений параметров модели и способов предварительной обработки текстов электронных писем. Также автором представлено место разработанной им модели среди существующих моделей текстов.

В третьей главе приведены разработанные метод и алгоритм классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, основу которых составляет разработанная в предыдущей главе модель электронных писем. Предложено применение весов термов и сокращение размерности признакового пространства. Представлен подход к оценке эффективности разработанного метода. Разработанные автором метод и алгоритм позволяют выбирать способы предобработки, параметры модели и способы классификации, проводить обучение на наборах писем, классификацию писем, вести базу данных термов и сохранять результаты в файл.

В четвертой главе представлена разработанная архитектура исследовательского прототипа подсистемы классификации электронных писем, включающей в себя три взаимодействующих между собой основных модуля, реализующие разработанные модель электронных писем и метод классификации электронных писем. Приведены результаты экспериментальных исследований по классификации писем для обнаружения спама, обосновывающие разработанные в диссертации модель электронного почтового

сообщения и метод 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. Проведено сравнение результатов эксперимента на исследовательском прототипе с результатами аналогичных исследований в области обнаружения спама. Рассмотрены подходы к практическому внедрению разработанной архитектуры подсистемы классификации электронных писем.

В заключении сформулированы основные результаты и выводы, полученные в диссертационной работе, а также предложены возможные направления дальнейших исследований.

Область исследования диссертации соответствует 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».

Согласованность автореферата и диссертации

Текст автореферата полностью отражает содержание диссертации и полученные в ней основные результаты.

Оформление диссертации соответствует ГОСТ Р 7.0.11-2011.

Новизна полученных результатов

1. Новизна предложенной модели электронного письма заключается в применении метода «генетических карт», отличающейся от известных моделей методом выделения значимых последовательностей символов текста (признаков электронных писем на основе их содержания, термов), что позволяет усилить смысловое содержание термов.

2. Новизна разработанного метода классификации электронных писем для обнаружения спама и идентификации легальных электронных писем основывается на использовании разработанной модели электронных писем, что позволяет повысить эффективность обнаружения спама и достоверность идентификации легальных электронных писем, а также снизить количество неклассифицированных писем.

3. Новизна разработанного алгоритма классификации электронных писем на основе методов машинного обучения, заключается в использовании дополнительной процедуры определения «схожести» термов на основе расстояния Левенштейна, обеспечивающей вычисление мер принадлежности классифицируемого электронного письма к классам спама и легальных, что позволяет повысить достоверность идентификации электронных писем.

4. Новизна предложенной архитектуры подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем на основе разработанного алгоритма заключается в реализации в ее составе блока выделения термов и блока нечеткой классификации, реализующие предложенные в работе метод и алгоритм, что позволяет повысить достоверность идентификации легальных электронных писем с учетом меняющихся информационных потребностей конкретного пользователя (персонализации).

Достоверность полученных результатов подтверждается корректной постановкой задач и выбором методов исследования; повторяемостью полученных результатов вычислительных экспериментов, проведенных с использованием известных и широко применяемых в аналогичных

исследованиях наборах писем; практическим применением результатов работы, подтвержденным актами внедрения; обсуждением полученных результатов на научных конференциях; публикацией полученных результатов в рецензируемых научных изданиях.

Публикации

Основные результаты диссертации опубликованы в 19 работах, в том числе: в 4 статьях в научных журналах, включенных в перечень научных изданий ВАК по научной специальности 2.3.6.; в 15 статьях в других изданиях.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость полученных результатов работы заключается в том, что они вносят существенный вклад в решение задачи обнаружения спама. В диссертации разработаны: модель электронного почтового сообщения, учитывающая содержание электронных писем конкретного пользователя (персонализацию), метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, алгоритм классификации электронных писем и архитектура подсистемы классификации электронных писем.

Практическая значимость полученных результатов заключается в разработке программных модулей исследовательского прототипа подсистемы классификации электронных писем. Практическое применение предложенных решений позволяет обеспечить точность классификации электронных писем до 0,995 и полноту их классификации до 0,993, а также снизить количество ошибочно классифицированных и неклассифицированных писем.

Рекомендации по использованию результатов и выводов диссертации

Представленные в диссертации результаты исследования рекомендуются к дальнейшему использованию в компаниях, специализирующихся на разработке средств защиты информации и средств ГосСОПКА, а также компаниях-разработчиках почтовых серверов и почтовых клиентов.

Замечания по работе

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.

Перечисленные замечания не являются принципиальными, не снижают научной и практической значимости представленной работы и не влияют на ее общую положительную оценку.

Заключение

Диссертация Корелова Сергея Викторовича 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 ВАК о порядке присуждения ученых степеней, 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.

Диссертационная работа Корелова С.В. и отзыв обсуждены на заседании кафедры Автоматизированных систем обработки информации и управления Института компьютерных технологий и защиты информации Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ», протокол заседания № 7 от 26 августа 2024 г.

Отзыв составил:
кандидат технических наук, доцент
заведующий кафедрой
Автоматизированных систем обработки
информации и управления
Института компьютерных технологий и
защиты информации
ФГБОУ ВО «КНИТУ-КАИ»

«26» 08 2024 г. Шлеймович Михаил Петрович

Подпись Шлеймовича М.П.
заверяю. Документовед

Кандидатская диссертация защищена
по специальности 05.13.05 - Элементы и устройства вычислительной техники и систем управления

Даю согласие на обработку персональных данных

Адрес организации: 420111, Республика Татарстан, г. Казань, ул. К. Маркса, 10
Рабочий телефон: +7 (843) 231 00 28
Адрес эл. почты: MPShleymovich@kai.ru