ОТЗЫВ

официального оппонента

доктора технических наук, профессора Коробейникова Анатолия Григорьевича

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

Область исследования, выбранная соискателем, занимает весомое место при решении задач обеспечения безопасности информации информационных систем и ресурсов. Значимость указанной предметной области связано прежде всего с одним из основных векторов компрометации информационных систем организаций.

Актуальность выбранной предметной области подтверждается нормативными документами Национального координационного центра по компьютерным инцидентам и Банка России, в соответствии с которыми спам отнесен к категории компьютерных инцидентов.

Исследования в данной области в значительной степени направлены на отбор признаков сообщений электронной почты, позволяющих повысить эффективность выявления спамовых сообщений с использованием различных выбранных методов машинного обучения.

В связи с вышеизложенным, тема диссертационной работы Корелова С.В., посвященная разработке метода и алгоритма обнаружения спама на основе выделения признаков электронных писем с использованием контентной

фильтрации, является актуальной, решение этой задачи, несомненно, имеет научную и практическую ценность.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложений. Основной текст работы изложен на 181 странице, содержит 29 рисунков, 37 таблиц, 6 приложений. В список используемой литературы включено 203 наименования источников. В приложениях содержатся копии актов внедрения и дополнительные материалы по результатам исследований.

Во введении обоснована актуальность работы, степень разработанности темы исследования, представлены объект и предмет исследования, сформулированы цель и задачи диссертационной работы, научная новизна и практическая значимость результатов диссертации.

В первой главе приведен анализ существующей нормативно-правовой базы в области спама, проведен анализ и обобщение имеющихся определений и признаков спама. На основании проведенного анализа основных технологий обнаружения спама и признаков электронных писем сделан вывод о целесообразности применения при построении модели электронного письма метода выделения термов, позволяющего усилить их смысловое содержание. 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.

Во второй главе определен базовый подход для разработки модели электронного почтового сообщения для классификации электронных писем и непосредственно разработана модель электронных писем, описаны и обоснованы ее параметры. Приведены полученные автором результаты экспериментов, связанных с выбором и обоснованием значений параметров. Также обоснованы способы предобработки электронных писем, позволяющие

повысить эффективность применения разработанной модели в задаче обнаружения спама. Предложено формирование набора термов с их маркированием по актуальности для конкретного пользователя (персональные особенности входящего потока электронных писем) и на конкретный момент времени.

В третьей главе предложены метод и алгоритм классификации электронных писем для обнаружения спама и идентификации легальных электронных писем. Вместе с тем описаны используемые подходы к вычислению весов термов и сокращению размерности признакового пространства, являющиеся этапами разработанного метода. Также в данной главе предложен обобщенный показатель эффективности метода классификации электронных писем для обнаружения спама, обеспечивающего точность и полноту обнаружения спама и достоверность идентификации легальных электронных почтовых сообщений.

В четвертой главе разработан исследовательский прототип подсистемы классификации электронных писем для обнаружения спама и идентификации легальных писем, реализующей предложенные автором модель электронных писем, метод и алгоритм классификации, применение которой позволяет учитывать персональные (пользовательские) особенности (с т. з. информационных потребностей) электронных писем и их содержание применительно к конкретным пользователям (группе пользователей), что обеспечивает персонализацию процесса обнаружения спама.

Результаты приведенных в данной главе экспериментов обосновывают применимость разработанных модели письма и метода классификации электронных писем.

В заключении приведены основные выводы и результаты проведенных исследований.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Обоснованность научных положений и выводов, представленных в диссертационном исследовании, подтверждается опубликованными по материалам исследований работами, включающими в себя 4 статьи в профильных научных журналах по специальности 2.3.6., входящих в Перечень рецензируемых научных изданий, рекомендованных ВАК и 15 статьях в других изданиях.

Диссертация содержит достаточное для понимания результатов проведенных исследований количество иллюстративного материала и таблиц.

Автореферат отражает содержание диссертации и представленные в работе основные выводы и результаты. Полученные результаты соответствуют заявленным автором пунктам паспорта специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Достоверность и новизна полученных результатов подтверждаются корректной постановкой задач и выбором методов исследования; анализом выполненных исследовательских работ в данной предметной области; результатами сравнительного анализа полученных результатов с результатами аналогичных исследований; апробацией полученных результатов на научно-практических конференциях.

Научная новизна работы

В качестве результатов диссертационного исследования, обладающих научной новизной, можно отметить следующие:

1. 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. 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. 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 разработанных модели и метода.

4. 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 и практическая значимость полученных автором результатов

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.

Практическая значимость полученных результатов заключается в разработке программных модулей исследовательского прототипа подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем. Применение предложенных модели и метода с учетом меняющихся информационных потребностей конкретного пользователя (персонализации), а также снизить количество ошибочно классифицированных и неклассифицированных писем. Данные выводы подтверждаются применением результатов работы в ряде организаций.

Замечания по работе

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.

Вместе с тем отмеченные недостатки не носят принципиального характера и не снижают значимости и общей положительной оценки представленной работы.

Заключение

Диссертация Корелова С.В., представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, в которой решена задача повышения эффективности обнаружения спама

и достоверности идентификации легальных электронных почтовых сообщений на основе классификации их содержания, результаты которой обладают научной новизной и практической ценностью.

Считаю, что диссертация соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, а ее автор Корелов Сергей Викторович заслуживает присуждения ему ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
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

Коробейников Анатолий Григорьевич

01.08.2024

Докторская диссертация защищена
по специальности 05.13.12 – Системы автоматизации проектирования (по отраслям)

Даю согласие на обработку персональных данных

Адрес места основной работы: 199034, г. Санкт-Петербург, Менделеевская линия, д. 1
Рабочий телефон: +7 812 323 28 07
Адрес эл. почты: korobeynikov_a_g@mail.ru