**ОТЗЫВ**

**официального оппонента**

кандидата технических наук, доцента Бурлакова Михаила Евгеньевича

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**

В настоящее время в качестве одного из способов коммуникации широкое распространение получила электронная почта. Также без нее невозможно получение некоторых видов услуг. Вместе с тем ее высокая популярность сопровождается и рядом проблем, одной из которых является спам. При этом электронные письма являются одним из наиболее распространенных способов начального этапа проникновения злоумышленников в информационные системы различных организаций, а количество блокируемых спамовых писем различными почтовыми сервисами в квартал измеряются миллиардами единиц. 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 литературы и приложений, выполнена на 181 странице, содержит 29 рисунков, 37 таблиц и 6 приложений. Список используемой литературы содержит 203

наименования. Приложения включают копии актов внедрения, а также дополнительный материал.

**Во введении** обоснована актуальность темы исследования, степень ее разработанности, указаны объект и предмет исследования, использованные методы, цель и задачи диссертации, положения, выносимые на защиту, научная новизна и значимость полученных результатов, сведения об их апробации.

**В первой главе** приведен анализ проблемы спама. Рассмотрена существующая нормативная база, проведен анализ и обобщение имеющихся терминологических определений и признаков спама, выделены основные группы технологий и методов обнаружения спама, а также определены группы и перечень наиболее важных информативных признаков писем, позволяющие отнести их к классу спама или легальных.

Отмечены преимущества применения методов машинного обучения (Байесовский классификатор, деревья решений, метод опорных векторов, $k$-ближайших соседей, искусственные иммунные системы, нейросетевые классификаторы) для решения задачи обнаружения спама. Проведен анализ современного состояния исследований в области обнаружения спама. Разработку модели электронного письма предложено осуществлять на базе математических моделей текстов и их последующего анализа с использованием «генетических карт».

**Во второй главе** представлена модель электронных писем для обнаружения спама, описаны ее параметры, оказывающие влияние на выделение термов. В основе предложенного подхода к построению модели используется метод «генетических карт». Приведены результаты вычислительных экспериментов, подтверждающих корректность и применимость модели, обосновывающих выбор значений ее параметров, а также способов предобработки электронных писем. В данной главе также обсуждена возможность использования предложенной модели как элемент любого из существующих классификационных пайплайнов в области обнаружения спама.

**В третьей главе** представлены результаты разработки метода и алгоритма классификации электронных писем для обнаружения спама и идентификации легальных электронных писем. Они основаны на разработанной в предыдущей главе модели электронных писем, а также содержат дополнительную процедуру определения «схожести» термов на основе расстояния Левенштейна. В данной главе описаны используемые подходы к вычислению весов термов и сокращению размерности признакового пространства. Также в данной главе предложен подход к оценке эффективности (качества) разработанного метода.

**В четвертой главе** представлена архитектура исследовательского прототипа подсистемы классификации электронных писем для обнаружения спама и идентификации легальных писем, включающего в себя три взаимодействующих между собой основных модуля, реализующие разработанные модель электронных писем и метод классификации электронных писем. В данной главе также приведены результаты экспериментальных исследований по классификации писем для обнаружения спама и проведено сравнение результатов эксперимента на исследовательском прототипе с результатами аналогичных исследований. Результаты экспериментов подтверждают обоснованность разработанных модели электронного почтового сообщения и метода классификации электронных писем, а также высокую эффективность их применения для решения задач обнаружения спама. Также в главе предложены подходы к практическому внедрению разработанной архитектуры подсистемы классификации электронных писем.

**В заключении** представлены выводы и полученные результаты.

**В приложениях** приведены акты внедрения результатов диссертационной работы и дополнительные результаты проведенных исследований.

**Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации,** является высокой, что обеспечивается корректной постановкой цели и задач исследования, выбором

методов проведения вычислительных экспериментов и решения поставленных задач, непротиворечивостью и повторяемостью полученных результатов.

Достоверность и новизна полученных результатов подтверждается сравнением полученных результатов с результатами других авторов, апробацией предложенных решений при решении ряда прикладных задач, публикацией основных результатов исследования в ведущих рецензируемых журналах, их обсуждением на представительных всероссийских и международных научно-практических конференциях.

Полученные результаты опубликованы в 19 работах, из них 4 – в журналах, включенных в перечень изданий ВАК по научной специальности 2.3.6.; 15 – в прочих изданиях.

Автореферат достаточно полно отражает содержание диссертации и существо полученных в ней результатов.

**Научная новизна работы** заключается в следующем:

1. Новизна предложенной автором модели электронного почтового сообщения для классификации электронных писем базируется на применении метода «генетических карт», отличающаяся 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, основанный на положениях задачи классификации текстовых документов, заключается в 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 наличии 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).

**Теоретическая и практическая значимость полученных автором результатов**

Теоретическая значимость работы обусловлена тем, что в ней разработаны научно обоснованные положения, составляющие основу решения задачи обнаружения спама: разработана модель электронного почтового сообщения, учитывающая содержание электронных писем конкретного пользователя (персонализацию), предложены метод классификации электронных писем для обнаружения спама и идентификации легальных электронных писем, а также алгоритм классификации электронных писем.

Практическая значимость полученных результатов подтверждена разработкой программных модулей исследовательского прототипа подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем. Результаты проведенных вычислительных экспериментов показали высокую эффективность предложенных решений при обнаружении спама и идентификации легальных писем с точностью классификации до 0,995 и полнотой классификации до 0,993. Результаты работы

внедрены в ряде организаций, что подтверждается соответствующими актами внедрения.

**Соответствие паспорту специальности**

Диссертация 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».

**Замечания по работе**

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.

В целом, указанные замечания не снижают высокой научной ценности и практической значимости выполненного исследования.

**Заключение**

Диссертация Корелова Сергея Викторовича, представленная на соискание ученой степени кандидата технических наук, обладает внутренним единством, научной новизной, теоретической и практической значимостью, она является законченной научно-квалификационной работой, посвященной решению актуальной задачи обнаружения спама, и соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней. С учетом вышеизложенного считаю, что автор диссертации 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:
кандидат технических наук, доцент,
доцент кафедры безопасности
информационных систем
Федерального государственного автономного
образовательного учреждения высшего
образования «Самарский национальный
исследовательский университет
имени академика С. П. Королева»

Бурлаков Михаил Евгеньевич

Кандидатская диссертация защищена
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Даю согласие на обработку персональных данных

Адрес места основной работы: 443086, г. Самара, Московское шоссе, д. 34
Рабочий телефон: +7 846 337 99 41
Адрес эл. почты: burlakov@ssau.ru

Подпись Бурлакова М.Е. удостоверяю.
Начальник отдела сопровождения деятельности ученых советов Самарского университета
Бояркина У.В.
«04» 09 2024 г.