

ОТЗЫВ

на автореферат диссертации Корелова Сергея Викторовича
на тему «Метод и алгоритм обнаружения спама на основе выделения
признаков электронных писем с использованием контентной фильтрации»,
представленной на соискание ученой степени кандидата технических
наук по специальности 2.3.6. Методы и системы защиты информации,
информационная безопасность

В последние годы наибольшую актуальность в сфере обеспечения информационной безопасности приобрели вопросы обнаружения и предупреждения компьютерных атак. Эти вопросы находятся в центре внимания регулятора этой сферы (ФСБ России), а также компаний – разработчиков программно-аппаратных средств защиты информации и центров ГосСОПКА. Одним из основных способов реализации компьютерных атак являются спамовые фишинговые письма, что подтверждается методическими документами НКЦКИ, в соответствии с которыми спам отнесен к категории компьютерных инцидентов. Таким образом, можно сделать вывод, что тема диссертационной работы Корелова С.В., посвященная повышению эффективности обнаружения спама и достоверности идентификации легальных электронных почтовых сообщений на основе классификации их содержания, является актуальной и востребованной.

К основным результатам работы, обладающим научной новизной, относятся:

- модель электронного почтового сообщения для классификации электронных писем на основе метода «генетических карт»;
- 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;
- 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;
- архитектура подсистемы классификации электронных писем для обнаружения спама и идентификации легальных электронных писем на основе разработанного алгоритма.

Практическая значимость полученных результатов заключается в разработке программных модулей исследовательского прототипа подсистемы классификации электронных писем.

Полученные результаты по своему содержанию соответствуют паспорту научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

ВХОД. № 3058-13
«12» 09 2024

Следует также отметить хороший уровень публикаций автора (автором опубликовано 19 работ, из которых 4 – в журналах из Перечня рецензируемых научных изданий ВАК).

В качестве замечаний по тексту автореферата можно указать следующие:

1. Не представлена функциональная модель классификации электронных писем, что могло бы дать более наглядное представление реализации практического внедрения предложенной архитектуры в существующие решения.

2. В тексте автореферата в контексте проводимых экспериментальных исследований упоминаются только русскоязычные и англоязычные письма. В связи с наличием в реальной переписке русскоязычных писем с англоязычными словами и фразами хотелось бы увидеть оценку эффективности разработанной модели на такого рода письмах.

Тем не менее считаю, что указанные замечания не снижают общей высокой оценки уровня диссертационной работы. Диссертационная работа выполнена на актуальную тему, обладает научной новизной и практической значимостью.

Считаю, что представленная диссертация является завершенной научно-квалификационной работой и 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 специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Кандидат физико-математических наук, доцент,
доцент Института компьютерных наук и технологий
федерального государственного автономного
образовательного учреждения высшего образования
«Пермский государственный
национальный исследовательский университет»

Никитина Елена Юрьевна

03.09.2024

Кандидатская диссертация защищена
по специальности 05.13.11 – Математическое и программное обеспечение
вычислительных машин, комплексов, систем и сетей

Даю согласие на обработку персональных данных

Адрес места основной работы: 614068, г. Пермь, ул. Генкеля, 7, корп. 2

Рабочий телефон: 8 (342) 2-396-164

Адрес эл. почты: neyu@psu.ru

