

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 научной специальности 2.3.6. Методы и системы защиты информации,
информационная безопасность

Векторы проведения компьютерных атак постоянно изменяются во времени. Это усложняет их выявление и блокирование средствами защиты. При этом первичная компрометация СВТ пользователей в 80 % случаев осуществляется с использованием методов социальной инженерии, триггером использования которых являются специально подготовленные сообщения электронной почты. Такие сообщения, как правило, направляются массово для охвата более широкого круга лиц (СПАМ). Выявление СПАМ-сообщений и их блокирование является повседневной рутинной задачей подразделений информационной безопасности, решение которой с использованием классических решений (средств антивирусной защиты) не всегда представляется возможным, например, в связи с отсутствием вредоносного файла во вложении к сообщению.

Таким образом, представленное исследование является актуальным и своевременным.

Представленные научные результаты обоснованы теоретически и проверены экспериментально, что показывает высокую степень проработки задачи выявления СПАМ-сообщений. При этом соблюдена методология исследования, предмет исследования опирается на объект исследования, полученные выводы соответствуют поставленной задаче.

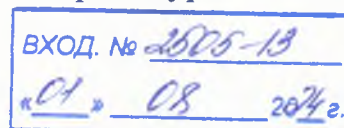
Положительным результатом исследования может быть определена модель СПАМ-сообщения, отражающая особенности таких сообщений в соответствии с объектом исследования. Представленная модель опирается на выделение определенных термов сообщения с использованием метода «генетических карт» и отражает смысл вредоносного контекста СПАМ-сообщений.

Обоснованность и достоверность полученных результатов, их теоретическая значимость и практическая ценность подтверждены результатами экспериментов и публикациями в рецензируемых научных изданиях, входящих в Перечень ВАК.

Однако имеются следующие замечания:

1) представленная архитектура не является составной частью какой-либо существующей системы выявления СПАМ-сообщений и, как следствие, вопрос возможности ее интеграции и практического применения остается открытым;

2) процедура нечеткой классификации, в которой в качестве меры используется функция расстояния Левенштейна, не учитывает транспозиции (перестановки двух соседних символов). Эффективность процедуры может



быть повышена использованием расстояния Дамерау — Левенштейна, нивелирующего наличие опечаток.

При этом замечания не снижают высокой научной ценности и практической значимости выполненного исследования.

С учетом изложенного, считаю, что диссертация Корелова Сергея Викторовича, представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, посвященной решению актуальной задачи обнаружения спама, 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 научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Кандидат технических наук, доцент,
заведующий кафедрой «Информационная безопасность
систем и технологий»

Федерального государственного бюджетного
образовательного учреждения
высшего образования «Пензенский государственный университет»



Зефи́ров Серге́й Льво́вич

Кандидатская диссертация защищена
по специальности 05.12.14 – Сети, узлы связи и распределение информации

Даю согласие на обработку персональных данных

Адрес места основной работы: 440026, г. Пенза, ул. Красная, 40, учебный корпус 4, а. 4-207, каф. ИБСТ
Рабочий телефон: +7 (8412) 20-84-35
Адрес эл. почты: ibst@pnzgu.ru

Личную подпись	<i>С.Л. Зефи́ров</i>
ЗАВЕРЯЮ	
Специалист по кадрам	<i>Татьяна</i>
<i>05.07</i>	<i>2024</i>

