

ФЕДЕРАЛЬНОЕ АГЕНТСТВО НАУЧНЫХ ОРГАНИЗАЦИЙ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ  
САНКТ-ПЕТЕРБУРГСКИЙ ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОС-  
СИЙСКОЙ АКАДЕМИИ НАУК  
(СПИИРАН)

199178 Санкт-Петербург, 14 линия, д.39. Тел.:(812)328-3311 Факс: (812) 328-4450;  
E-mail:spiiiran@iias.spb.su; http://www.spiiras.nw.ru  
ОКПО 04683303, ОГРН 1027800514411 ИНН/КПП 7801003920/780101001

---

## ОТЗЫВ

научного руководителя о диссертационной работе

Максима Викторовича Абрамова *Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей*, представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность

Максим Викторович Абрамов, 1990 года рождения, в 2013 году окончил математико-механический факультет Санкт-Петербургского государственного университета по специальности «Прикладная информатика (в сфере международных отношений)». С 2013 года по настоящее время работает в лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук. Свою исследовательскую работу, посвященную анализу защищенности пользователей информационных систем от социоинженерных атак, М.В. Абрамов начал на четвертом курсе специалитета на кафедре информатики математико-механического факультета СПбГУ и продолжает ее на протяжении более пяти лет. За это время им были подготовлены и представлены доклады на научных конференциях и опубликован ряд статей в ведущих рецензируемых российских и зарубежных научных изданиях.

Диссертационная работа М.В. Абрамова подготовлена в ходе научных исследований, проводимых в лаборатории теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук и на кафедре информатики математико-механического факультета Феде-

рального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет».

Основными результатами, полученными соискателем, являются

- подход к оценке защищённости пользователя с использованием усовершенствованных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» и основанная на нём вероятностная модель оценки защищённости пользователя, опирающаяся на профиль компетенций злоумышленника и профиль уязвимостей пользователей;
- вероятностная модель оценки успеха многоходовой социоинженерной атаки, учитывающая результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети;
- алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, автоматизированной оценки выраженности ряда особенностей пользователей на основании данных, содержащихся в контенте, публикуемом пользователями социальных сетей, восстановления фрагмента мета-профиля пользователя информационной системы (а именно, родной город, город проживания, год рождения), построенные на основе агрегации доступных сведений;
- программная реализация предложенных в диссертационном исследовании алгоритмов в прототипе комплекса программ для оценки защищённости/поражаемости пользователей информационных систем.

Высокая степень достоверности результатов, полученных в ходе диссертационной работы, обеспечивается посредством глубокого анализа исследований по тематике информационной безопасности и социоинженерных атак, корректного применения математических методов, подтверждается согласованностью результатов, их успешной апробацией на международных и российских научных конференциях, внедрениями, а также публикацией итогов исследований в ведущих рецензируемых изданиях.

В диссертации Абрамов М.В. представил результаты работ, которые выполнялись им в 2013–2018 гг. в рамках нескольких научно-исследовательских проектов, объединённых общей целью повышения оперативности обнаружения угроз социоинженерных атак, за счёт автоматизации экспресс-оценки защищённости/поражаемости пользователей информационной системы от социоинженерных

атак, учитывающей результаты агрегации сведений из социальных сетей и других источников, для оценки параметров моделей указанных пользователей и связей между ними.

Среди публикаций соискателя есть 2 монографии, 7 работ из списка WoS/Scopus, 6 работ (из которых одна единоличная) в изданиях из «Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук», 40 докладов и тезисов на научных конференциях (из которых 9 единоличных). Следует отметить аспект, дополнительно характеризующий завершенность и применимость теоретических разработок соискателя, — полученные теоретические результаты легли в основу разработки ряда программ (7 свидетельств о государственной регистрации в Роспатенте), которые формируют комплекс, использующийся в вычислительных экспериментах, а также — на практике.

М.В. Абрамов успешно сочетает научную работу (в т.ч. над кандидатской диссертацией) вместе преподавание на кафедре информатики Санкт-Петербургского государственного университета. Ежегодно им читаются курсы и проводятся практические занятия по дисциплинам «Частотные методы анализа информации», «Прикладные технологии анализа и моделирования социальных сетей», «Модели и архитектуры программ и знаний», «Системы управления контентом», «Основы обработки и интеллектуального анализа данных», «Разработка комплексов программ», «Теория байесовских сетей». Под его руководством выполняются студенческие выпускные квалификационные работы.

Характеризуя М.В. Абрамова, как научного работника, отмечаю его высокую квалификацию, трудолюбие, способность к самостоятельной творческой деятельности и анализу, а также — к самостоятельной постановке новых исследовательских задач, глубокую эрудицию в вопросах проведения междисциплинарных исследований на стыке информатики, математики, психологии, социологии.

Кандидатская диссертация Абрамова М.В. является завершенной научной работой, выполненной на высоком теоретическом уровне, и имеющей практическое применение, о чем свидетельствуют 3 акта о ее внедрении в государственной организации и коммерческих предприятиях.

Результаты диссертационного исследований имеют высокую научную значимость для решения проблемы анализа защищённости/поражаемости пользователей информационных систем от социоинженерных атак. Считаю, что диссертационная работа Максима Викторовича Абрамова является завершённой научно-квалификационной работой и соответствует требованиям действующей редакции «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, в том числе — всем критериям, перечисленным в Разделе II указанного положения, включая изложенные в п.9 (второй абзац), и может быть представлена на диссертационном совете Д.002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по научной специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность.

Научный руководитель — заведующий лабораторией теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), д.физ.-мат.н., доцент

А.Л. Тулупьев

14 марта 2018 г.

Рабочий адрес: 199178, Санкт-Петербург, ВО 14 линия, дом 39

Тел. (812)328-01-03

E-mail: alt@iias.spb.su, alexander.tulupyev@gmail.com

*Личную подпись руки Александра Львовича ТУЛУПЬЕВА, заведующего лабораторией теоретических и междисциплинарных проблем информатики и автоматизации СПИИРАН, доктора физико-математических наук, доцента, удостоверяю.*

Ученый секретарь СПИИРАН,

к.воен.н., доцент

Е.П. Силла

14 марта 2018 г.