

ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Абрамова Максима Викторовича на тему: «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей», научный руководитель – д.ф.-м.н., доцент, заведующий лабораторией теоретических и междисциплинарных проблем информатики Тулупьев А.Л.

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Молдовян Н.А. (председатель), д.т.н., проф. Котенко И.В., д.т.н., проф. Молдовян А.А. после ознакомления с кандидатской диссертацией Абрамова Максима Викторовича на тему: «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» сделала вывод о том, что диссертационная работа Абрамова М.В. посвящена решению актуальной научной задачи: построению оценок защищённости/поражаемости пользователей и критичных документов информационных систем от социоинженерных атак, учитывающих результаты агрегации данных, извлекаемых из контента, публикуемого пользователями в социальных сетях, и иных источников.

Цель исследования заключается в повышении 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.

Практическую значимость исследования составляют разработанные в диссертации комплексный подход, методы и алгоритмы, которые обеспечивают решение актуальной научно-технической задачи, направленной на автоматизацию экспресс-оценки защищённости/поражаемости пользователей информационной системы от социоинженерных атак, и вносят значительный вклад в развитие моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник», используемых для имитации социоинженерных атак и оценки защищённости пользователей. Результаты исследования внедрены в государственном учреждении и коммерческих предприятиях.

Разработанные в диссертации методы, модели, алгоритмы и реализация создают основу для оценок защищённости/поражаемости пользователей информационной системы на основании информации, извлекаемой из их аккаунтов в социальных сетях. Предложенные подходы позволяют производить анализ возможных траекторий распространения многоходовых социоинженерных атак, а также рассчитывать вероятности реализации каждой такой траектории, что в свою очередь способствует расширению числа учитываемых факторов, влияющих на оценку защищённости пользователей информационной системы, и позволяет искать постановки задач бэктрекинга атак в одной из удачных для такого поиска решений форм.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются посредством глубокого анализа исследований по тематике информационной безопасности и социоинженерных атак, корректного применения математических методов, подтверждается согласованностью полученных результатов, их успешной апробацией на международных и российских научных конференциях, внедрениями, а также публикацией итогов исследований в ведущих рецензируемых изданиях.

Материалы и основные результаты кандидатской диссертации Абрамова М.В. удовлетворяют паспорту специальности: 05.13.19 – «Методы и системы защиты

информации, информационная безопасность», по которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

Основные научные результаты диссертации удовлетворяют требованиям, предусмотренным пунктами 11 и 13 Положения о присуждении ученых степеней: по материалам диссертационной работы сделано 48 публикаций и приравненных к ним научных работ по теме диссертации, из них — 2 монографии, 7 публикаций в изданиях, индексируемых Scopus/WoS, 6 статей 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» (в журналах «Информатизация и связь», «Компьютерные инструменты в образовании», «Нечёткие системы и мягкие вычисления», «Информационно-управляющие системы», «Автоматизация процессов управления», «Научно-технический вестник информационных технологий механики и оптики»), 40 докладов и тезисов на научных конференциях (из которых 9 единоличных), получены 7 свидетельств о регистрации программ для ЭВМ (РОСПАТЕНТ).

Диссертация Абрамова М.В. в целом соответствует п. 9 (абзац 2) Положения о присуждении учёных степеней.

Недостовверные сведения о работах, в которых изложены основные научные результаты диссертации, опубликованных соискателем ученой степени, отсутствуют.

Текст диссертации, представленной в диссертационный совет, идентичен тексту диссертации, размещенной на сайте СПИИРАН.

Объем оригинального текста диссертационной работы составляет не менее 90%; цитирования оформлены корректно. Требования, установленные пунктом 14 Положения о присуждении ученых степеней, соблюдены: заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем ученой степени в соавторстве, без ссылок на соавторов, не выявлено.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Абрамова М.В. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н. Овчарова В.А., к.т.н., доц. Красова А.В.
3. В качестве ведущей организации утвердить Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».
4. Разрешить Абрамову М.В. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «07» июня 2018 г.

Члены комиссии:

д.т.н., проф. Молдовян Н.А.

д.т.н., проф. Котенко И.В.

д.т.н., проф. Молдовян А.А.