

ОТЗЫВ

на автореферат диссертации Абрамова Максима Викторовича на тему: «Методы и алгоритмы анализа защищенности 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

Рост доступности данных, которые накапливаются в современных информационных системах, влечет рост потребности в научно-обоснованных подходах к их защите. Существенная часть подходов посвящена защите информационных систем от программно-технических атак, хотя атаки через пользователей являются носят более опасный характер. Пользователь может умышленно или неумышленно произвести некоторые действия, которые нанесут серьезный урон информационной безопасности компании. Таким образом, диссертационная работа Абрамова М.В., посвященная разработке методов и алгоритмов анализа защищенности пользователей информационных систем от социоинженерных атак и оценке параметров моделей, является весьма своевременной и выполнена на **актуальную тему**.

Исходя из содержания автореферата, на наш взгляд, отличительные особенности, характеризующие **научную новизну** результатов работы, состоят:

- 1) в усовершенствовании модели комплекса «критичные документы – персонал – злоумышленник», в которой предлагается учитывать также новые модели злоумышленника и профиля компетенций злоумышленника;
- 2) в разработке вероятностной модели и метода оценки успеха многоходовой социоинженерной атаки, учитывающей результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети;
- 3) в разработке архитектуры прототипа комплекса программ для оценки защищенности/поражаемости пользователей информационных сетей.

Практическая значимость результатов диссертации состоит в том, что они позволяют создать инструмент для автоматизированной оценки защищенности/поражаемости пользователей информационных сетей на основании информации, извлекаемой из аккаунтов пользователей в социальных сетях.

Достоверность и обоснованность научных положений, выводов и рекомендаций определяется глубоким анализом исследований в области информационной безопасности и социоинженерных атак, корректностью применения математического аппарата, признанием основных положений диссертации широким кругом специалистов при апробации материалов исследования на научных конференциях, а также внедрением основных научных результатов. Результаты диссертационной работы представлены в

48 публикациях, включая 2 монографии, 7 публикаций в изданиях, индексируемых Scopus/WoS, 6 статей в рецензируемых научных изданиях, рекомендуемых ВАК, получено 7 свидетельств о регистрации программ для ЭВМ.

Вместе с тем, в отношении содержания автореферата можно сделать следующие **замечания**:

- соискатель употребляет термин «многоходовая социоинженерная атака», но не поясняет в тексте автореферата его значение;
- список публикаций можно было сократить до основных работ, где изложены научные результаты, выносимые на защиту, а полный список указать в диссертации, так как на некоторые из них соискатель в автореферате не ссылается.

Приведенные выше замечания носят частный характер и не оказывают влияния на общую положительную оценку диссертационной работы.

Содержание автореферата достаточно полно отражает содержание диссертации и позволяет составить целостное представление о проделанной работе. Тема диссертации, направленность проведенных исследований и полученных результатов соответствует специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

В целом, судя по автореферату, можно сделать **вывод**, что, представленная диссертационная работа «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» является законченным самостоятельным исследованием, обладающим актуальностью и новизной, отвечающим требованиям, предъявляемым к диссертации, изложенным в «Положении о порядке присуждения ученых степеней», а ее автор, Абрамов Максим Викторович, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Зав. кафедрой технологий интроскопии
доктор технических наук

А.В. Федоров

25.05.2018

Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
197101, Санкт-Петербург, Кронверкский пр.
E-mail: od@mail.ifmo.ru
Интернет: <http://www.ifmo.ru/>
тел. (+7812) 232-97-04