ОТЗЫВ

на автореферат диссертации Максима Викторовича Абрамова на тему «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»

Несанкционированное раскрытие и нелегитимное тиражирование персональных данных, размещенных в персональных аккаунтах, в том числе в социальных сетях, является ущемлением прав соответствующих граждан. В ряде случаев такое раскрытие приводит к репутационным и/или финансовым потерям физических и/или юридических лиц. В связи с этим исследования, направленные на анализ и повышение защищенности персональных данных в сети Интернет, являются своевременными и злободневными.

Исходя из материалов автореферата, соискателем поставлена цель решить на новом математическом и технологическом уровне задачу автоматизированного анализа защищённости групп пользователей информационных систем от фишинг-атак на аккаунты соцсетей. Для этого автором предложены и рассмотрены некоторые математические (в том числе вероятностные) модели, описывающие зависимость успешности социоинженерной атаки от исходных данных, определяемых структурой группы, текущим состоянием сети и активности пользователей.

Исходя из материалов автореферата, научная новизна выполненных исследований состоит в следующем.

1. Предложены усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник». Комплекс является развитием другого ранее разработанного комплекса, ключевой особенностью которого был учёт профиля уязвимостей пользователя. Впервые предложена модель и основанный на ней метод оценки вероятности успеха социоинженерной атаки злоумышленника на пользователя, опирающиеся на профили уязвимостей пользователя и компетенций злоумышленника.

2. Предложены новые вероятностная модель и метод оценки успеха многоходовой социоинженерной атаки, отличающиеся тем, что позволяют учесть результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети.

3. В целях оценки параметров моделей используются данные, извлекаемые из социальных сетей, для чего впервые разработаны методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, основанные на методах машинного обучения.

Анализ материалов автореферата позволил выявить следующие недостатки проведенного исследования:

1. Не обоснован выбор математического аппарата при формировании оценок защищенности/поражаемости пользователей. Вызывает сомнение возможность получения конструктивных оценок предложенными гибридными (нечеткостно-вероятностными) моделями, при этом к настоящему времени в предметной области информационной безопасности имеется развитой и хорошо апробированный математический аппарат исследования переменных, заданных в нечетком базисе.

2. Из автореферата не ясно, учитывались ли погрешности оценки эксперта (при оценке степени компетентности злоумышленника) из-за субъективности, ошибок, некомпетентности или злонамеренности собственно эксперта. Это не позволяет оценить качество итогового решения задачи анализа защищённости данных групп пользователей.

Указанные недостатки несколько снижают степень удовлетворения качеством материалов автореферата, вместе с тем, не оказывают существенного влияния на положительную оценку работы в целом. Автор имеет высокую публикационную активность, материалы статей позволяют более системно оценить результаты проведенных исследований и отражают суть положений, выносимых на защиту.

Исходя из полученных сведений, диссертация представляет собой законченное самостоятельное исследование, обладает актуальностью и новизной, отвечает требованиям, предъявляемым к кандидатским диссертациям в соответствии с Положением о порядке присуждения ученых степеней. М.В. Абрамов имеет ряд публикаций в научных 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» и заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Сотрудник Академ
доктор технически

И.А. Саитов
25.04.2018

Подпись Саитова И

Начальник отдела к

А. И. Дешин

Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации»
302034, г. Орёл, ул. Приборостроительная, д. 35
email: akramovish@mail.ru
Веб-сайт: http://academ.msk.rsnet.ru/
Тел. 8 (4862) 54-97-63