ОТЗЫВ

на автореферат диссертационной работы АБРАМОВА Максима Викторовича, выполненной на тему: «Методы и алгоритмы анализа защищенности пользователей информационных систем от социоинженерных атак: оценка параметров моделей» и представленной на соискание ученой степени кандидата технических наук по специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Глобальное вовлечение информационного обмена во все сферы жизнедеятельности помимо очевидных достоинств привнесло и существенные недостатки. Одними из них являются угрозы информационной безопасности, проводимые через пользователей методами социальной инженерии. И если область средств противодействие угрозам в случае информационно-технических атак и имеет определенные успехи, то в случае киберсоциальных атак не существует даже удовлетворительных способов оценки защищенности от них, не говоря уже про соответствующие меры противодействия. Моделям и алгоритмам, применимым в интересах анализа защищенности пользователей, имеющих доступ к защищаемой информации, и посвящено диссертационное исследование. С учетом вышеизложенного тему диссертационного исследования следует считать актуальной.

Для повышения оперативности обнаружения угроз социально-инженерных атак автор предлагает производить экспресс-оценку пользователей информационных систем. Для этого используется соответствующая вероятностная модель, параметры которой определяются по активности пользователей в социальных сетях, на страницах сайтов и проч. Согласно автореферата автором разработаны и выносятся на защиту следующие основные научные результаты:

1) Подход к оценке защищённости пользователя с использованием моделей комплекса «критичные документы – информационная система – пользователь», дополненного авторской моделью «злоумышленника»

2) Вероятностная модель и соответствующие методы оценки успеха многоэтапной социально-инженерной атаки

3) Алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальных сетях и частичного восстановления отсутствующей о них информации, а также алгоритмы оценки *выраженности* ряда особенностей пользователей

4) Архитектура комплекса программ для оценки защищённости пользователей от социально-инженерных атак

Все научные результаты обладают новизной, а также имеют теоретическую и практическую значимость.

Общий список работ автора значителен и состоит из 48 публикации, включая 2 монографии, 6 статей в журналах, рецензируемых ВАК РФ, 7 статей в изданиях из системы цитирования Scopus/WoS, 7 свидетельств о государственной регистрации программы для ЭВМ.

Несомненным достоинством работы является то, что соискателю удалось довести ряд полученных научных результатов до программной реализации (прототип комплекса программ для оценки защищенности пользователей).

Автореферат изложен технически грамотным языком. Анализ существа работы, изложенного в материалах автореферата, дает основании считать, что соискателю удалось внести вклад в методологию и технологию оценки защищенности пользователей от социальных атак и противодействия им.

Следует отметить отдельные недостатки по материалам, представленным в автореферате:

1) Содержание глав дается крайне неравномерно: на первую и вторую главы отводится по одному абзацу, тогда как на третью – 6 страниц, а на четвертую – 1 страница.

2) Формулировка третьего основного научного результата содержит в основном практическую значимость, а не его определение или суть. Не раскрыто понятие "выраженности ряда особенностей пользователей", что не позволяют напрямую соотнести алгоритмы автоматизированного поиска аккаунтов сотрудников с областью информационной безопасности и защиты информации.

3) В списке работ, опубликованным автором по теме диссертации, не приведены свидетельства о государственной регистрации программ для ЭВМ, которые служат доказательствами достоверности и авторства основные научных результатов, и которые в соответствии с п.13 «Положения о порядке присуждения ученых степеней» относятся к публикациям в рецензируемых изданиях.

Отмеченные недостатки не влияют на общий достаточно высокий научный уровень и практическую значимость защищаемых научных результатов.

Представленный на отзыв автореферат подтверждает соответствие диссертации на тему «Методы и алгоритмы анализа защищенности пользователей информационных систем от социоинженерных атак: оценка параметров моделей» критериям части II «Положения о порядке присуждения ученых степеней». Диссертация Абрамова М.В. является законченной научно-квалификационной работой, выполненной на актуальную тему, в которой изложены научно обоснованные научные и технические разработки, имеющие существенное значение для совершенствования методологии информационной безопасности и технологии защиты информации, а ее автор заслуживает присвоения ученой степени кандидата технических наук по специальности: 05.13.19 – «Методы и средства защиты информации, информационная безопасность».

Профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета Государственной противопожарной службы МЧС России, доктор технических наук, профессо

уйневич Михаил Викторович

Почтовый адрес: 192242, Санкт-Петербург, ул. Бухарестская, д. 23, корп. 1, кв. 41
Адрес электронной почты: bmv1958@yandex.ru. Тел. +7 (911)-233-17-05

«31» мая 2018 г.

Организация:
Федеральное государственное бюдже
зования "Санкт-Петербургский униве
МЧС России", 196105 Санкт-Петербу