ОТЗЫВ

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

Проблема анализа защищенности пользователей информационных систем от социоинженерных атак является актуальной для области информационной безопасности. В настоящее время предложено множество различных методов и алгоритмов анализа защищенности программно-технической составляющей информационных систем, но угрозы, исходящие или реализуемые через пользователей информационных систем, чаще всего остаются без внимания. Существующие системы защиты конфиденциальной информации от социоинженерных воздействий в качестве методов обеспечения безопасности используют разграничение прав доступа пользователей, а также мониторинг поведения пользователя в системе с целью отслеживания нестандартных действий. Другими словами, не предлагается никаких методов анализа защищенности пользователей с целью разработки превентивных мер, обеспечивающих снижение вероятности успеха социоинженерной атаки. Таким образом, тема диссертационной работы Абрамова М.В. «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» вне сомнения является актуальной.

Целью диссертационного исследования, сформулированной в автореферате, является 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. Она включает в себя следующие подзадачи: (1) разработать подход к оценке защищённости пользователя с использованием усовершенствованных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник», а также метод и вероятностную модель оценки защищённости пользователя, опирающиеся на профиль компетенций злоумышленника и профиль уязвимостей пользователей; (2) разработать вероятностную модель и опирающиеся на неё методы оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети; (3) построить 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; (4) разработать архитектуру прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализовать в указанном комплексе предложенные выше алгоритмы.

В результате исследования были получены важные научные результаты: предложена формализация моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник», на основе моделей профиля уязвимостей пользователя и компетенций злоумышленника, входящих в модели пользователя и злоумышленника соответственно, были разработаны метод и вероятностная модель оценки защищённости пользователя. Соискатель формализовал задачу оценки вероятности многоходовой социоинженерной атаки таким образом, что для её решения стало возможно использовать адаптированную модель Белла–Тревино. Кроме того, были разработаны методы и алгоритмы для оценки параметров моделей, в частности модели пользователя, посредством агрегации сведений из социальных сетей. Отличительной особенностью является разработанный комплекс программ, позволяющий моделировать комплекс «критичные документы – информационная система – пользователи – злоумышленник» для последующего проведения вычислительных экспериментов.

Практическая ценность полученных в рамках диссертационного исследования результатов заключается в том, что впервые был предложен подход, позволяющий проводить экспресс-оценку защищённости пользователей информационных систем от социоинженерных атак, что способствует своевременному принятию мер, способствующих повышению уровня защищённости системы.

Можно сделать следующее замечание по автореферату: соискатель резонно предлагает использовать t-норму как основу для совместного учета степени выраженности уязвимости пользователя и уровня владения атакующим воздействием при формировании оценки успеха социоинженерного атакующего воздействия, не указав, однако, на основе каких ожидаемых свойств оценки такой выбор сделан и не обсудив более широкий класс вариантов, где перестановка аргументов может привести к несовпадающим результатам. Кроме того, t-нормы активно используются в нечеткой логике и в теории копул, рассмотрение связи с которыми могло бы привести к содержательным для рассматриваемой в диссертации предметной области ассоциациям.

Автореферат диссертации свидетельствует о том, что она является законченным самостоятельным исследованием, обладает актуальностью и новизной, отвечает требованиям, предъявляемым к кандидатским диссертациям, содержащимся в действующем Положении о присуждении ученых степеней. Абрамов М.В. имеет 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» и несомненно заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Декан факультета прикладной математики и кибернетики Тверского государственного университета, доктор физико-математических наук, профессор

А.В. Язенин
13.04.2018

Контактная информация:
Адрес: Садовый переулок, д. 35, к. 231, г.Тверь, 170002
Телефон/Факс: (4822) 58-54-10
email: Alexander.Yazenin@tversu.ru
Веб-сайт: http://pmk.tversu.ru/general/employ