

ОТЗЫВ

на автореферат диссертации Максима Викторовича Абрамова «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».

Информационная безопасность является одной из основных потребностей современного человека, поэтому в настоящее время существует целый ряд разработок, позволяющих снижать риски взлома информационных систем с помощью программно-технических атак. Однако область защиты пользователей информационных систем от социоинженерных атак по-прежнему остается малоисследованной, несмотря на то, что по данным ежегодных отчетов лаборатории Касперского сегодня более 80% социоинженерных атак становятся успешными. В связи с этим тема диссертационной работы М.В. Абрамова является, несомненно, актуальной.

Автором диссертации решается одна из ключевых проблем анализа защищенности пользователей информационных систем от социоинженерных атак - оценка параметров модели пользователя на основе агрегации данных, извлекаемых из контента, публикуемого пользователями в социальных сетях. Абрамовым М.В. разработаны и представлены в диссертации методы и алгоритмы для автоматизированного поиска аккаунтов сотрудников в социальной сети, оценки степени выраженности особенностей их личности, восстановления фрагмента мета-профиля пользователя.

Достаточно оригинальной в моделях комплекса «критичные документы - информационная система-пользователь - злоумышленник» является модель злоумышленника, которая отличается от аналогичных моделей использованием профиля компетенций злоумышленника, причем профиль компетенций представляет собой набор пар «атакующее воздействие - уровень умения злоумышленника использовать данное атакующее воздействие».

Важно также отметить, что в диссертации осуществляется корректный переход от оценок защищённости пользователей информационной системы к защищённости критичных документов.

Однако, судя по тексту автореферата, предложенные вероятностные модели оценки защищённости/поражаемости документов разного уровня критичности от социоинженерных атак не учитывают оценку злоумышленника вероятности того, что пользователь, успешно им атакованный, имеет доступ к подобным документам. Данный аспект открыл бы, на мой взгляд, возможность моделировать атаки злоумышленника с учётом его начальных знаний о соответствующей киберсоциальной системе.

Указанное замечание не влияет на общую положительную оценку диссертации, являющейся законченным научным исследованием, результаты

которого опубликованы в открытой российской и зарубежной научной печати и апробированы на практике. Опубликованные работы в полной мере отражают результаты диссертации.

Считаю, что диссертация и автореферат Абрамова М.В. отвечают всем требованиям действующего Положения ВАК РФ о присуждении ученых степеней, а её автор Абрамов М.В. заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры «Кибернетика» Национального
исследовательского ядерного университета «МИФИ»,
доктор технических наук, профе

Рыбина Г.В.
13.04.2018

Адрес: Москва, Каширское ш., 31, 115409
Телефон/Факс: 8 (495) 788-56-99, доб. 7149
e-mail: galina@nilab.mephi.ru