ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»; 634050, г. Томск, пр. Ленина, 40; тел.: (3822) 51–05–30; эл. почта: office@tusur.ru.

ОТЗЫВ

на автореферат диссертации Абрамова Максима Викторовича «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».

Диссертационная работа Абрамова М.В. посвящена автоматизации анализа защищённости пользователей информационных систем от социоинженерных атак. Основной целью данного исследования является повышение оперативности обнаружения угроз социоинженерных атак за счёт автоматизации экспресс-оценки защищённости/поражаемости пользователей информационной системы. Созданное в рамках диссертационной работы математическое, методическое и алгоритмическое обеспечение вносит вклад в развитие подходов к обеспечению внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и к оценке защищенности информации и информационной безопасности объекта. Поэтому диссертационная работа Абрамова М.В., направленная на обеспечение процесса принятия решений по поддержанию и повышению степени защищённости от социоинженерных атак персонала информационных систем, безусловно, является актуальной.

Научная новизна диссертационной работы Абрамова М.В. определяется следующими основными результатами: предложенными усовершенствованными моделями комплекса «критичные документы – информационная система – пользователь – злоумышленник»; вероятностной моделью и методом оценки успеха многоходовой социоинженерной атаки; разработанными алгоритмами поиска и автоматизированной обработки аккаунтов пользователей в социальной сети.

Материалы диссертационной работы отражены в 48 публикациях, в том числе в 2 монографиях в соавторстве и в 6 статьях, опубликованных в рецензируемых журналах, рекомендованных ВАК.

По содержанию автореферата возникли следующие замечания.

1. Неясно, каким образом в предлагаемых моделях (модель критичных документов, модель хостов информационной системы и т.д.) учитывается временная динамика информационной системы. В частности, множество

пользователей, имеющих доступ к *i*-му документу определенного уровня, может быть различным в разные моменты времени.

2. Автор указывает, что количество ресурса, которым обладает злоумышленник, рассматривается не как непрерывная величина, а как величина, которая допускает «квантование». Однако непонятно, каким образом следует квантовать такой ресурс злоумышленника как его личностные особенности (стр. 8 автореферата).

3. В автореферате не определено неоднократно упоминаемое понятие многоходовой социоинженерной атаки.

Высказанные замечания не уменьшают значимости проведенного Абрамовым М.В. исследования. Диссертация по объему и научной новизне является законченной научно-квалификационной работой и удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность», а ее автор Абрамов Максим Викторович заслуживает присуждения ученой степени кандидата технических наук.

Доктор технических наук, профессор,
проректор по научной работе и инновациям,
заведующий кафедрой безопасности информационных систем
ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Адрес: 634050, г. Томск, пр. Ленина, 40
Тел.: +7 (382-2) 51-43-02
E-mail: mrv@keva.tusur.ru

Р. В. Мещеряков

Кандидат технических наук,
старший научный сотрудник кафедры
безопасности информационных систем
ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Адрес: 634050, г. Томск, пр. Ленина, 40
Тел.: +7 (382-2) 51-43-02

О. О. Евсютин