

## ОТЗЫВ

на автореферат диссертации Максима Викторовича Абрамова «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».

Вопросы обеспечения информационной безопасности, в период информационной эпохи, становятся все более и более актуальными. В настоящее время, одним из ключевых направления развития мировой и национальной транспортных систем является их цифровизация и интеллектуализация, в этих условиях проблема обеспечения защиты информационных систем транспорта различной модальности (автомобильного, авиационного, железнодорожного и водного) становится одной из самых актуальных. Нарушения информационной безопасности на транспорте могут приводить, к самым разным негативным и трагическим последствиям.

Обычно инциденты нарушения информационной безопасности представляются связанными с программно-техническим взломом, однако способов получения доступа к конфиденциальной информации больше. В частности, для этих целей могут быть использованы некоторые методы социальной инженерии, которые в последнее время становятся всё более эффективными в сравнении с программно-техническими атаками, что отмечается статистикой крупных компаний в индустрии. Таким образом, актуальна проблема защиты пользователей информационных систем от социоинженерных атак и связанная с ней задача анализа защищённости сотрудников организаций от такого рода воздействий. Диссертационная работа М.В. Абрамова посвящена решению актуальной проблемы 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.

Автором разработаны вероятностные модели оценки защищённости/поражаемости пользователей/критичных документов, основанные на формализации комплекса «критичные документы – информационная система – пользователь – злоумышленник». Предложены новые методы и алгоритмы оценки параметров указанных моделей посредством агрегации сведений, получаемых из анализа контента, публикуемого пользователями социальных сетей.

Соискатель уместно использует в формализации модели злоумышленника профиль его компетенций в качестве одного из компонент, представляя его как набор пар: вид атакующего действия – умение злоумышленника использовать этот вид атакующего действия.

Вместе с тем, стоит отметить, что некоторые виды атакующих воздействий могут быть взаимосвязаны, что даёт возможность рассматривать классы атакующих воздействий и строить профиль на их основании, этот случай не рассматривается в автореферате. Отмеченное замечание не снижает ценности полученных соискателем результатов.

В целом диссертация соискателя М.В. Абрамова является законченной самостоятельной научно-квалификационной работой, обладает актуальностью и новизной, отвечает требованиям, предъявляемым к кандидатским диссертациям, содержащимся в действующем Положении о порядке присуждения ученых степеней. Соискатель имеет достаточное количество публикаций в научных изданиях из Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата технических наук

Таким образом, соискатель заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Заместитель директора по на  
Института проблем тран  
Н.С. Соломенко Российской ак  
доктор технических наук, доцент



В.И. Комашинский  
25.04.2018

Контактная информация:  
Адрес: 12-я линия В.О., д.13, Сант  
Телефон/Факс: +7(812) 323-29-54  
email: kama54@rambler.ru  
Веб-сайт: <http://www.iptran.ru/>