ОТЗЫВ

на автореферат диссертации Максима Викторовича Абрамова *«Методы и алгоритмы анализа защищенности 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»

Диссертационная работа посвящена проблеме оценки параметров комплекса моделей «критичные документы – информационная система – пользователь – злоумышленник» с целью построения автоматизированной системы анализа защищенности пользователей от социоинженерных атак. Суть подобных атак – использование таких особенностей личностей как доверчивость, лень, желание прийти на помощь и других для получения доступа к ресурсам и политикам безопасности корпоративных систем и сетей. Актуальность проблемы определяются ростом числа и разнообразием угроз, учет которых важен для лиц, обеспечивающих информационную безопасность.

Представленный в настоящем диссертационном исследовании подход к агрегации сведений из социальных сетей, служащих для оценки параметров моделей, позволяет решить проблему за счет выявления уязвимостей пользователя, угрожающих наиболее масштабными последствиями. Это, в свою очередь, позволяет проводить превентивные меры по нивелированию обнаруженных слабых мест и существенно повышает уровень защищенности пользователей от социоинженерных атакующих воздействий злоумышленника.

В работе предложены усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник», формализованные с помощью алгебраических и реляционных моделей, а также методы и алгоритмы агрегации сведений из социальных сетей. Все представленные в диссертационном исследовании алгоритмы реализованы в прототипе комплекса программ, что позволяет проводить вычислительные эксперименты.

Полученные соискателем результаты могут быть применены на практике. В частности, разработанные модели позволяют оценивать защищенность пользователей информационных систем и, опосредованно, критичных документов, что создает основу для формализации задачи поиска возможных инцидентов. Вместе с тем прослеживается необходимость создания баз данных, содержащих перечни уязвимостей пользователей, возможных ответных действий при атакующих воздействиях злоумышленника.

В качестве незначительных редакторских замечаний к автореферату, не влияющих на его качество, можно отметить:

1. В пункте 1 Заключения предложение «Предложены усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник» фактически повторяет смысл первого предложения этого пункта;

2. Имеет место перегруженность некоторых предложений сложными оборотами с многочисленными запятыми.

3. На рисунке 3 записи на скриншотах интерфейсов оказались практически нечитаемыми.

Диссертация Абрамова М.В. является законченным самостоятельным исследованием, обладает актуальностью и новизной, ее результаты прошли апробацию и опубликованы в изданиях, рекомендованных ВАК РФ. Диссертация отвечает требованиям, предъявляемым к кандидатским диссертациям, содержащимся в действующем «Положении о порядке присуждения ученых степеней», а Абрамов М.В. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Заведующий лабораторией
интеллектуального управления, г.н.с. ИЦМС
ИПС им. А.К.Айламазяна РАН, д.т.н., проф. _

В.М. Хачумов
13.04.2018

Контактная информация:
Адрес: 152021 Ярославская область, Переславский район, с.Веськово, ул. Петра Первого, д.4 «а»
Телефон: 8 (910)976-5814
email: vmh48@mail.ru
Веб-сайт: https://sites.google.com/site/iamforintelligent/