МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»
(ГУАП)

ул. Большая Морская, д. 67, лит. А, Санкт-Петербург, 190000, Тел. (812) 710-6510, факс (812) 494-7057,
E-mail: common@aanet.ru ОГРН 1027810232680, ИНН/КПП 7812003110/783801001

06.06.2018 № 74-10-26/18 На № _____ от _____

УТВЕРЖДАЮ

Ректор ГУАП, д-р эк. наук

Ю.А. Антохина

«06» 06 2018 г.

ОТЗЫВ

кафедры аэрокосмических и программных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения 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».

Актуальность работы. В настоящее время проблема анализа защищенности информационных систем, пользователей таких систем и критичных документов, которые хранятся в них, является одной из значимых проблем в области обеспечения информационной безопасности в я.

Диссертационное исследование, выполненное Абрамовым М.В., посвящено автоматизации процесса оценивания защищённости/поражаемости пользователей информационной системы от социоинженерных атак, которое учитывает результаты агрегации сведений из социальных сетей и других источников, для экспресс-оценки параметров моделей указанных пользователей и связей между ними. Под социоинженерными атаками злоумышленника автор имеет ввиду методы социотехники, направленные на получение той или иной информации от пользователей информационных систем. Автор отмечает синонимичность понятий «социоинженерная атака» и «социотехническая атака».

Основные задачи социотехники пересекаются с задачами взлома защиты информационной системы: цель - получение неавторизованного доступа к системе или информации для совершения мошенничества, сетевого вторжения, промышленного шпионажа, или просто для разрушения системы или сети. В качестве основных целей часто выступают телефонные компании, крупные корпорации и финансовые институты, военные и правительственные агентства, и больницы. Организации подвергаются этим атакам зачастую потому, что они являются наиболее простым путём получения незаконного доступа, чем многие виды технических атак. Даже для людей-техников зачастую существенно проще совершить телефонный звонок и создать контекст, при котором необходимые данные будут переданы устно. Именно так злоумышленники зачастую и поступают.

Диссертация М.В. Абрамова направлена на анализ защищенности пользователей именно от такого рода воздействий, это позволяет считать тему диссертационной работы *актуальной*

Новизна, теоретическая и практическая значимость полученных в диссертации результатов не вызывают сомнений. Основными на наш взгляд являются следующие результаты:

- вероятностная модель и предложенный на ее основе метод оценки успеха многоходовой социоинженерной атаки;
- алгоритм автоматизированной оценки выраженности ряда особенностей пользователей на основании данных, содержащихся в контексте пользовательских сообщений;
- алгоритм восстановления фрагмента мета-профиля пользователя(родной город, место проживание, год рождения и пр.), построенные на основе агрегации доступных сведений, полученных из сети.

В качестве замечания по работе можно отметить следующее. Судя по автореферату, автор предлагает подход к автоматизированному анализу защищенности пользователей. Очевидно, что за счёт автоматизации предполагается достигнуть существенного повышения оперативности обнаружения угроз от возможных социоинженерных атак, однако, из автореферата не ясно построены ли в диссертации метрики оценки повышения оперативности.

Приведенное замечание не оказывают существенного влияния на положительную оценку работы в целом.

М.В. Абрамов имеет внушительный список публикаций в научных изданиях из Перечня рецензируемых научных изданий, в которых опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук. Диссертация работа М.В. Абрамова представляется законченным самостоятельным исследованием, выполненным на высоком математическом уровне, обладает актуальностью, новизной и отвечает требованиям, предъявляемым к кандидатским диссертациям, содержащимся в действующем Положении о порядке присуждения ученых степеней. Это позволяет утверждать, что М.В. Абрамов заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Отзыв подготовил,
профессор кафедры № 14,
канд.техн. наук Н. А. Шехунова

Отзыв рассмотрен и утвержден на заседании кафедры аэрокосмических компьютерных и программных систем 15 мая 2018 года, протокол № 10

Зав. кафедрой№ 14
д-р техн. наук, профессор йнин

Ученый секретарь кафедры, канд. техн. наук Н.А. Громова

Наименование организации: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»
Адрес: Россия, 190000, г. Санкт-Петербург, ул. Б. Морская, 67, лит. А
Телефон: +7 (812) 710-65-10
Факс: +7 (812) 494-7057
Email: common@aanet.ru