УНИВЕРСИТЕТ ИТМО

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный
исследовательский университет
информационных технологий,
механики и оптики» (Университет ИТМО)

Кронверкский проспект, д. 49, г. Санкт-Петербург,
Российская Федерация, 197101
тел.: (812) 232-97-04 | факс: (812) 232-23-07
od@mail.ifmo.ru | www.ifmo.ru

11.05.2018 № 4-25/866

"УТВЕРЖДАЮ"

Проректор по научной работе

Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургского национального исследовательского университета

сите

На № 073-10-01/200.1 от 05.04.2018 СПИИРАН

ОТЗЫВ

ведущей организации — федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» на диссертацию Максима Викторовича Абрамова «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертационной работы

Диссертационная работа **Абрамова Максима Викторовича** посвящена решению актуальной научной проблемы — повышению оперативности обнаружения угроз социоинженерных атак за счёт 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.

Компьютерные системы, хранящие и обрабатывающие информацию, активно используются во многих отраслях производства и сфере услуг. Столь широкое распространение информационных технологий заставляет уделять всё более заметное внимание вопросам информационной безопасности. В последнее время атаки на информационные системы стали происходить чаще, приносить большие убытки и требовать больше ресурсов и времени для уста-

новления виновных в подобных преступлениях. Одним из наиболее эффективных видов атак на информационную безопасность является корпоративный шпионаж, которому подвергаются более четверти компаний и почти 80% из них успешно.

Сотрудник компании, имеющий доступ к конфиденциальной информации, может преднамеренно или непреднамеренно нарушить её безопасность (конфиденциальность, целостность или доступность). Санкционированный пользователь информационной системы, вероятно, знаком с рядом сотрудников, обслуживающих и администрирующих информационную систему; имеет ряд разрешений на доступ к документам, хранящимся в информационной системе; может знать аутентификационные данные коллег; обладает физическим доступом к некоторым компьютерам. В связи с этим, взаимодействие пользователей информационной системы со злоумышленниками может нанести серьёзный ущерб компании.

Все сказанное определяет ***актуальность темы*** диссертационной работы **Абрамова Максима Викторовича**, проблематика которой соответствует научной специальности «Методы и системы защиты информации, информационная безопасность».

Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации

1. Предложены усовершенствованные модели комплекса «критичные документы — информационная система — пользователь — злоумышленник». Комплекс является развитием другого ранее разработанного комплекса, ключевой особенностью которого был учёт профиля уязвимостей пользователя. Основным элементом развития стало дополнение существующего комплекса «критичные документы – информационная система – пользователь» моделью злоумышленника. Впервые предложена основанная на указанном комплексе вероятностная модель оценки успеха социоинженерной атаки злоумышленника на пользователя, опирающаяся на профиль уязвимостей пользователя и профиль компетенций злоумышленника. Модели, разработанные ранее, использовали только профиль уязвимостей пользователя.
2. Представлена новая вероятностная модель оценки успеха многоходовой социоинженерной атаки. Ранее эти оценки задавались экспертно, в диссертационном исследовании предложены модель оценки и автоматизация расчёта оценок вероятности успеха социоинженерной атаки на пользователя через другого пользователя. В модели используется метод оценки вероятности сложного события. Оценка строится на основании интенсивности связей сотрудников в компании, предположение о которых делается исходя из сведений, извлекаемых из социальной сети ВКонтакте.

3. Впервые предложены алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, основанные на методах машинного обучения. Обучающая выборка составлялась из аккаунтов пользователей, которые указали в графе карьера место работы. Впервые предложена модель, которая позволяет автоматизированно на основании данных, содержащихся в контенте, публикуемом пользователями в социальных сетях, давать оценки степени выраженности ряда особенностей их личности. Предложены новые методы, позволяющие дополнить фрагмент мета-профиля пользователя информационной системы, которые построены на основе агрегации доступных сведений из альтернативных источников. Задача в такой формулировке ранее не ставилась. Включает в себя в качестве подзадачи идентификацию аккаунтов пользователей в разных социальных сетях, подходы к решению которой предлагались. В диссертационном исследовании предложено расширение подхода для решения этой подзадачи на увеличенном списке социальных сетей.
4. Разработана программная реализация предложенных в диссертационном исследовании новых алгоритмов в прототипе комплекса программ для оценки защищённости/поражаемости пользователей информационных систем.

Обоснованность и достоверность научных положений и выводов

Высокая степень достоверности результатов диссертации обеспечивается посредством глубокого анализа исследований по тематике информационной безопасности и социоинженерных атак, корректного применения математических методов, подтверждается согласованностью полученных результатов, их успешной апробацией на международных и российских научных конференциях, внедрениями, а также публикацией итогов исследований в ведущих рецензируемых изданиях.

Значимость для науки и практики результатов, полученных автором диссертации.

Основными научными достижениями автора является разработка новых моделей и алгоритмов, позволяющих производить анализ защищённости пользователей информационных систем от социоинженерных атак. Полученные научные результаты вносят существенный вклад в развитие современных методов защиты пользователей информационных/киберфизических/киберсоциальных систем от социоинженерных атак.

Разработанные методы, модели, алгоритмы и реализация создают основу для получения оценок защищённости/поражаемости пользователей информационной системы на основании информации, извлекаемой из их аккаунтов в социальных сетях. Предложенные подходы позволяют производить анализ возможных траекторий распространения многоходовых социо-

что в свою очередь способствует расширению числа учитываемых факторов, влияющих на оценку защищённости пользователей информационной системы, и позволяет искать постановки задач бэктрекинга атак в одной из удачных для такого поиска решений форм.

Результаты, представленные в диссертации, дают инструмент для автоматизированной оценки степени выраженности ряда особенностей их личности на основании анализа данных, содержащихся в контенте, публикуемом пользователями в социальных сетях. Эти результаты используются впоследствии для построения профилей уязвимостей пользователей, лежащих в основе оценок вероятности успеха социоинженерной атаки злоумышленника. Включение модели злоумышленника позволяет агрегировать большее число параметров, влияющих на успех социоинженерной атаки. Также, полученные в диссертации результаты, создают предпосылки для построения постоянно пополняемых баз данных, содержащих перечни уязвимостей пользователей, типов атакующих действий злоумышленника, типов ответных действий пользователя, компетенций злоумышленника по аналогии с базами данных программно-технических уязвимостей.

Все сказанное свидетельствует о важности расширения сферы проводимых исследований и их практических приложений, что позволяет рекомендовать их продолжение и применение результатов в организациях — СПИИРАН, заводе им. Козицкого, СПбГУ, Университете ИТМО, НЯУ МИФИ, УлГТУ, Банке Санкт-Петербург.

Общая оценка диссертационной работы

Диссертационная работа выполнена на актуальную тему на хорошем научном уровне, ее отличает полнота и логичность изложения материала, хорошая структурированность и завершенность. Полученные результаты имеют высокую значимость для решения как теоретических задач оценки защищённости/поражения пользователей и, опосредованно, критичных документов, так и практических задач анализа защищённости от социоинженерных атак, выработка рекомендаций для лиц, принимающих решения.

Содержание диссертационной работы в полной мере отражено в автореферате. Основные результаты работы опубликованы в 48 печатных работах. Кроме того, следует отметить активность в участии в конференциях различного уровня, о чем свидетельствуют полнотекстовые доклады, опубликованные в трудах научных конференций, а также тезисы докладов.

В то же время следует указать ряд замечаний к тексту диссертационной работы.

1. На странице 65 диссертации автор приводит формулу для вычисления оценки вероятности поражения критичных документов, к которым имеют доступ m пользователей. Данная формула некорректна, поскольку значения оценок могут

быть больше 1, вероятно допущена ошибка и множитель n_m лишний. Следующая формула, которая опирается на указанную, верная.

2. При расчёте оценки вероятности успеха многоходовой социоинженерной атаки используется произведение вероятностей распространения атаки от пользователя к пользователю, при этом не оговаривается, сделано ли предположение о том, что данные события являются независимыми.
3. Формула для расчёта оценки вероятности распространения атаки от пользователя к пользователю представляет собой разность 1 и произведения большого числа множителей $1-p$, возведённых в некоторую степень; не окажется ли так, что это произведение будет иметь достаточно низкое значение, а это, в свою очередь, приведёт к высоким значениям вероятности успеха распространения атаки? Т.е. в ряде случаев вероятность распространения атаки будет близка к 1. Действительно ли риски распространения атаки настолько высоки?
4. Для оценки вероятности распространения социоинженерной атаки от пользователя к пользователю используются сведения, извлекаемые из социальных сетей, такие как взаимные лайки, репосты и т.п. Недостаточно ясно соотношение того, что можно обработать или учесть указанным методом, и того, что в целом сказывается на распространении «влияния»/атаки социоинженера. В частности, метод ориентирован на работу с данными социальных сетей, но нельзя исключить, что общение между сотрудниками в коллективе никак не отражено в социальной сети.
5. На рисунке 9 («Поиск после добавления нового узла») и рядом подписи сделаны на английском языке, не очень понятно, чем это обусловлено.
6. В автореферате не вполне чётко отражен личный вклад автора в полученный результат, связанный с модулем прототипа комплекса программ для поиска аккаунтов сотрудников компании в социальной сети.
7. В диссертационной работе рассмотрена оценка вероятности успеха социоинженерной атаки злоумышленника на пользователя с учётом ограниченности ресурса, но рассмотрен только один вид ресурса. Для того, чтобы рассмотреть эту задачу с нескольких точек зрения, имело бы смысл выполнить выкладки для нескольких видов ресурсов.
8. В работе также встречаются пунктуационные ошибки, опечатки; в частности, на с. 76 пропущена запятая в первом сложносочинённом предложении последнего абзаца, на с. 130 в последнем абзаце используется слово «протип» вместо «прототип», на с. 131 пропущена буква во второй строке: написано

«структурировани» вместо «структурировании», и буква в десятой строке — «компани» вместе «компании», и др.

В целом отмеченные недостатки не влияют на корректность выводов диссертации, представляющую собой законченную научно-квалификационную работу, в которой решена задача повышения оперативности обнаружения угроз социоинженерных атак за счёт 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, имеющая существенное значение для развития 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.

Полученные результаты имеют высокую научную ценность и практическую значимость. Результаты апробированы на ряде международных конференций и в рамках нескольких научно-исследовательских работ, получивших поддержку в форме грантов или стипендий. Имеются шесть публикаций в изданиях, содержащихся в «Перечне рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук».

Диссертация «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» соответствует всем критериям, предъявляемым в отношении кандидатских диссертаций, которые установлены «Положением о присуждении ученых степеней», утвержденным Постановлением Правительства РФ № 842 от 24 сентября 2013 (редакция от 28 августа 2017), а ее автор Максим Викторович Абрамов заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Доклад Абрамова Максима Викторовича заслушан на расширенном семинаре кафедры безопасности киберфизических систем ФГАОУ В ертационная работа и отзыв обсуждены и одобрены, протокол се 018 года.

Декан факультета безопасности информац технологий, кандидат технических наук, доцент А. Заколдаев

Заведующий кафедрой безопасности киберфизи систем, доктор технических наук, доцент .В. Беззатеев