ОТЗЫВ

официального оппонента
на диссертацию Абрамова Максима Викторовича
«Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей», представленную к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 — Методы и системы защиты информации, информационная безопасность

Актуальность работы

Актуальность вопросов информационной безопасности сегодня регулярно подчёркивается в различных научных публикациях, распоряжениях крупных государственных деятелей, средствах массовой информации и иных источниках. В последнее время атаки на информационные системы стали происходить чаще, приносить большие убытки и требовать больше времени для расследования таких преступлений. При этом по статистике наиболее эффективными являются внутренние (инсайдерские) атаки, которые в той или иной степени используют психологические уязвимости пользователей системы, а не программно-технические уязвимости системы. Такие атаки называется социоинженерными.

При этом в последнее время постоянно усложняется структура компьютерных сетей и механизмов их защиты, но в то же время не остаются неизменными и другие аспекты информационной безопасности, связанные с пользователями. Увеличивается количество используемых злоумышленниками уязвимостей пользователей и, как следствие, растёт количество возможностей по реализации атак. Описанное выше обусловливает необходимость разработки мощных автоматизированных средств (систем) анализа защищенности пользователей информационных/киберфизических/киберсоциальных систем.

В диссертационной работе Абрамова Максима Викторовича рассматриваются вопросы, связанные с анализом защищённости пользователей информационных систем от социоинженерных атак, экспресс-оценкой защищённости с учётом данных, извлекаемых из аккаунтов пользователей в социальных сетях. В соответствии с вышеперечисленным, работа является актуальной.

Основные научные результаты и их новизна

Следующие результаты, представленные в диссертационной работе, являются наиболее значимыми:

1) модели комплекса «критичные документы – информационная система – пользователь – злоумышленник». Модель и основанный на ней метод оценки вероятности успеха социоинженерной атаки злоумышленника на пользователя, опирающиеся на профили уязвимостей пользователя и компетенций злоумышленника.

2) вероятностная модель и метод оценки успеха многоходовой социоинженерной атаки, отличающиеся тем, что позволяют учесть результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети.

3) методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, основанные на методах машинного обучения. Модель, которая позволяет автоматизированно на основании данных, содержащихся в контенте, публикуемом пользователями в социальных сетях, давать оценки степени выраженности ряда особенностей их личности. Новые методы, позволяющие дополнить фрагмент мета-профиля пользователя информационной системы, которые построены на основе агрегации доступных сведений из альтернативных источников.

4) архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализация в указанном комплексе предложенных в диссертации новых алгоритмов.

Новизна первых трех (теоретических) результатов состоит в предложении новых моделей, методов и алгоритмов, использующихся при оценке защищённости/поражаемости пользователей информационных систем от социоинженерных атак. Новизна последнего результата заключается в практической реализации новых методов анализа защищённости/поражаемости пользователей.

Обоснованность и достоверность результатов

Достоверность и обоснованность результатов работы обеспечены строгими математическими выкладками и корректным использованием методов соответствующих математических дисциплин. Предложенные методы были реализованы в прототипе комплекса программ с последующим проведением многочисленных экспериментов, результаты которых показывает их хорошую согласованность с теоретическими выводами, а также соответствуют представлениям специалистов в предметной области.

Результаты диссертации апробированы на ряде ведущих российских и зарубежных конференций. Автором опубликовано 40 научных работ в трудах конференций и 6 статей в научных изданиях из перечня российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук («Информационно-управляющие системы», «Информатизация и связь», «Нечёткие системы и мягкие вычисления», «Компьютерные инструменты в образовании», «Научно-технический вестник информационных технологий механики и оптики», «Автоматизация процессов управления»).

Значимость результатов, полученных в диссертации, для науки и практики

В диссертационной работе разработаны новые метод, модели и алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, основанные на методах машинного обучения. Модель, которая позволяет автоматизированно на основании данных, содержащихся в контенте, публикуемом пользователями в социальных сетях, давать оценки степени выраженности ряда особенностей их личности. Новые методы, позволяющие дополнить фрагмент мета-профиля пользователя информационной системы, которые построены на основе агрегации доступных сведений из альтернативных источников.

Разработанные модели, методы и алгоритмы позволяют автоматизированно строить оценки защищённости/поражаемости пользователей и, опосредованно, критичных документов. За счёт увеличения оперативности получения данной информации лица, принимающие решения, смогут предпринимать меры, позволяющие повысить степень защищённости киберсоциальной системы.

Полученные результаты представляют собой основу для решения смежных задач, возникающих при анализе защищённости пользователей. Одним из возможных направлений развития является разработка системы упреждающей диагностики и бэктрекинга инцидентов.

Перспективным представляется практическое использование разработанных методов при обеспечении поддержки принятия решений в области обеспечения информационной безопасности, кадровой политике, что подтверждается использованием результатов диссертационной работы в государственной организации и на коммерческих предприятиях, а также при выполнении ряда проектов РФФИ, направленных на изучение подходов к анализу защищённости пользователей информационных систем от социоинженерных атак.

Недостатки и замечания по диссертационной работе

1) на рисунках встречаются интерфейсы различных модулей прототипа комплекса программ, на которых английский и русский языки используются без очевидного принципа выбора: где-то только русский, где-то только английский, где-то оба вместе (рис. 35), — непонятно, чем это обусловлено;

2) на рис. 35 представлен графический пользовательский интерфейс программного модуля, на котором в левой части приведен список чисел. Вероятно, числа соответствуют идентификационным номерам пользователей в социальной сети, но представляется не очень удобным работать с таким интерфейсом, поскольку каждый раз, когда оператор захочет узнать, кто скрывается под идентификационным номером, ему

придётся открыть страницу социальной сети и набрать номер в адресной строке браузера;

3) в разных местах диссертации используются разные обозначения для пользователей в комплексе моделей «критичный документы – информационная система – пользователь – злоумышленник», где-то пользователь, где-то персонал;

4) на рис. 3 (стр. 83) не расшифровывается аббревиатура ПУ;

5) при описании более широкого контекста исследований соискатель справедливо затрагивает вопросы, связанные с динамикой параметров моделей, хотя это и не входит непосредственно в цель, задачи, объект и предмет исследований; вместе с тем, при рассмотрении указанной категории вопросов соискатель ограничивается моделью забывания/постепенной утраты компетенций, которая не учитывает эффекты от возможных мероприятий (тренинги, повышение квалификации, другие способы поддержки настороженности в отношении тех или иных категорий социоинженерных атак);

6) особенности работы модулей прототипа комплекса программ описаны весьма сжато. В частности, в тексте диссертации не указано, используются ли при агрегации сведений из социальных сетей параллельные запросы с нескольких IP-адресов или последовательные;

7) при чтении диссертации было выявлено небольшое число неточностей в употреблении знаков, например: с. 33 — тире с переносом на следующую строку; с. 62 — пропущена запятая в последнем сложноподчинённом предложении первого абзаца после таблицы, с. 73, с. 77, с. 80 — пропущены знаки препинания после формул.

Следует отметить, что указанные замечания не влияют на корректность итогов выполненной диссертационной работы.

Заключение

Автореферат отражает содержание диссертации, в нем представлены все основные результаты и положения, выносимые на защиту. Все полученные в диссертационном исследовании результаты опубликованы в изданиях из Перечня российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук, а также в приравненных к ним изданиях. Кроме того, соискатель имеет 7 зарегистрированных программ для ЭВМ, разработанных (в соавторстве) в процессе диссертационного исследования.

Диссертация Абрамова Максима Викторовича представляет собой законченную научно-квалификационную работу и содержит решение задачи 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.

Диссертационная работа Абрамова Максима Викторовича «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» удовлетворяет требованиям, установленным в текущей редакции «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 (с последующими изменениями), а ее автор, Абрамов Максим Викторович, достоин присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент,
Заведующий кафедрой защищённых систем связи Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», кандидат технических наук, доцент

А.В. Красов

15 апреля 2018 г.

Контактная информация:
Адрес: РФ, набережная реки Мойки, д.61, Санкт-Петербург, 191186
Телефон: +7 (812) 326-31-50
Факс: +7 (812) 326-31-59
email: rector@sut.ru
Веб-сайт: https://www.sut.ru/