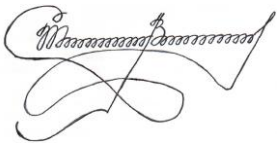
На правах рукописи



АБРАМОВ Максим Викторович

МЕТОДЫ И АЛГОРИТМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК: ОЦЕНКА ПАРАМЕТРОВ МОДЕЛЕЙ

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург — 2018

Работа выполнена в лаборатории теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук и на кафедре информатики Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет».

Научный руководитель — **ТУЛУПЬЕВ Александр Львович,**
доктор физико-математических наук, доцент, заведующий лабораторией теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

Официальные оппоненты — **ОВЧАРОВ Владимир Александрович**,
доктор технических наук, заместитель начальника 3 управления военного института Федерального государственного бюджетного военного образовательного учреждения высшего образования «Военно-космической академии имени А.Ф. Можайского» Министерства обороны Российской Федерации;

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

Ведущая организация — Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Защита диссертации состоится **«07» июня 2018 г. в 16 часов 00 минут** на заседании диссертационного совета Д.002.199.01, созданного на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук по адресу: 199178, Санкт-Петербург, 14 линия В.О., д. 39.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, http://www.spiiras.nw.ru.

Автореферат разослан **«___» апреля 2018 года.**

Ученый секретарь
диссертационного совета Д.002.199.01,
кандидат технических наук — А.А. Зайцева

Общая характеристика работы

Актуальность темы диссертации. Растущая сложность компьютерных сетей и механизмов их защиты, увеличение числа уязвимостей пользователей и видов возможных социоинженерных атак, вовлечение всё большего числа критичных документов в электронный документооборот форсируют рост потребности в проведении соответствующих поисковых исследований, а также в проектировании и разработке автоматизированных средств анализа защищенности пользователей информационных систем. Эти средства призваны выполнять задачи по обнаружению уязвимостей пользователей, информированию служб безопасности, выявлению возможных траекторий атакующих действий злоумышленников, идентификации отдельных пользователей или их групп, критичных с точки зрения защиты от социоинженерных атак, критичных сетевых ресурсов, поиска и анализа источников, содержащих критическую информацию о персонале, обеспечению лиц, принимающих решения, информацией, необходимой для выработки обоснованных решений по выбору защитных механизмов.

Анализ публикаций показал, что с одной стороны, ощущается острая потребность в обеспечении процесса принятия решений по поддержанию и повышению степени защищённости от социоинженерных атак персонала информационных систем и, опосредованно, критичных документов, содержащихся в этих информационных системах, оценками и инструментами, автоматизирующими получение этих оценок в отношении степени защищённости указанных персонала и критичных документов. С другой стороны, в зависимости от потребности оперативности оценок, учёта в них различных факторов, доступной информации, которая может агрегироваться для получения указанных оценок, методы, модели и алгоритмы автоматизации их формирования, а также вовлечённые информационные источники могут быть достаточно разнообразны и давать основу для постоянно развивающихся исследований. С третьей стороны, хотя уже существуют определённые наработки, в дальнейшем развитии, в частности, потребуется учитывать ограниченные ресурсы злоумышленников, подготовленность пользователей, возможности сотрудников, обеспечивающих безопасность информационной системы, социальные сети и иные киберсоциальные системы, которые могут быть использованы злоумышленниками в качестве источников критичной информации о пользователях, особенности злоумышленника (более точно, его компетенции).

Необходимость удовлетворить потребности, обозначенные тремя приведёнными выше аспектами, обосновывает актуальность избранной темы диссертационного исследования, которая нацелена на учёт при анализе и построении оценок степени поражаемости/защищённости пользователей информационной системы и, в конечном итоге, критичных документов информационной системы сведений, извлекаемых из социальных сетей, и вносит свой вклад в развитие системы соответствующих моделей, методов и алгоритмов оценки защищенности информации, нацеленных на автоматизацию оценки уровня защищённости системы от социоинженерных атак — на создание элементов комплекса программ, который будет агрегировать широкий круг факторов в мониторинге уровня защищенности информационных систем. В частности, актуальна проблема автоматизированной экспресс оценки степени выраженности ряда особенностей личности пользователей на основании анализа данных, содержащихся в контенте, публикуемом ими в социальных сетях. Кроме того, актуальны проблемы восстановления фрагмента мета-профиля пользователя, под которым понимаются его анкетные данные, для агрегации большего количества сведений при формализации указанных связей. Эти сведения позволят строить оценки вероятностей успеха социоинженерной атаки злоумышленника на пользователя и оценки защищённости пользователей, что будет способствовать более глубокому анализу защищённости персонала информационных систем от социоинженерных атак и, в указанном срезе, повышению степени защищённости собственно критичных документов, хранящихся в системе.

Степень разработанности темы. Т.В. Тулупьевой, А.Л. Тулупьевым был предложен подход к оценке защищённости пользователей информационной системы от социоинженерных атак на основе обобщения методологии анализа деревьев атак, выдвинутой И.В. Котенко и М.В. Степашкиным. А.А. Азаровым были предложены реляционно-вероятностные методы и модели оценки степени защищённости пользователей, причём развитие социоинженерной атаки имитировалось с помощью комплекса моделей, в который входили модель пользователя с фрагментом профиля его уязвимостей, модель критичных документов, модель компьютерной сети, включая хосты. Коллектив учёных на базе лаборатории ТиМПИ СПИИРАН провел ряд исследований по тематике социоинженерных атак (достигнутые результаты в проблемно-постановочной и методологической части, отражены в монографии [1]).

Также заделом для диссертационного исследования послужили работы Десницкого В.А., Дойниковой Е.В., Зегжды П.Д., Кий А.В., Козленко А.В., Копчак Я.М., Кондратюк А.П. Котенко И.В., Крук Е.А., Молдовяна Н.А., Молдовяна А.А., Осипова В.Ю., Разумова Л., Саенко И.Б., Собецкого И., Степашкина М.В., Харечкина П.В., Чечулина А.А., Шорова А.В., Юсупова Р.М., Beckers K., Buiati F., Côté I., Cunbin L., Faßbender S., Heisel M., Hofbauer S., Kondakci S., Kim T.H., Oliveira A.R., Orozco A.L.S., Song Y., Villalba L.J.G., Zhang J., Zeng Q.

Соискателем был разработан комплекс моделей «критичные документы – информационная система – пользователь – злоумышленник», который является расширением существовавшего до этого комплекса «критичные документы – информационная система – пользователь». За счёт агрегирования сведений о более широком круге факторов, влияющих на оценку вероятности успеха или провала социоинженерных атакующих действий злоумышленника-социоинженера, удалось построить многоаспектные оценки защищённости/поражаемости пользователей и критичных документов информационной системы.

Цель исследования заключается в повышении 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. (В автореферате и диссертации для краткости вместо термина экспресс-оценка используется термин оценка).

Цель диссертационной работы достигается решением совокупности следующих **задач**:

- разработать подход к оценке защищённости пользователя с использованием усовершенствованных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» и основанные на нём метод и вероятностную модель оценки защищённости пользователя, опирающиеся на профиль компетенций злоумышленника и профиль уязвимостей пользователей;
- разработать вероятностную модель и опирающиеся на неё методы оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети;
- построить алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, автоматизированной оценки выраженности ряда особенностей пользователей на основании данных, содержащихся в контенте, публикуемом пользователями социальных сетей, восстановления фрагмента мета-профиля пользователя информационной системы (а именно, родной город, город проживания, год рождения), построенные на основе агрегации доступных сведений;
- разработать архитектуру прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализовать в указанном комплексе предложенные выше алгоритмы.

Объектом исследования являются модели киберсоциальной системы «критичные документы – информационная система – пользователь – злоумышленник».

Предметом исследования являются взаимосвязи между элементами указанной киберсоциальной системы и параметры этих элементов, определяющие в сочетании контекст возможной реализации социоинженерных атак, а также способы оценки этих параметров на основе информации из аккаунтов в социальных сетях, которые, в свою очередь, существенны для формирования оценки степени защищённости/поражаемости пользователей (персонала) от таких атак.

Научная новизна. Все результаты, выносимые на защиту, являются новыми.

- 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 отличающим элементом развития стало дополнение существующего комплекса «критичные документы — информационная система — пользователь» моделью злоумышленника. Впервые предложена модель и основанный на ней метод оценки вероятности успеха социоинженерной атаки злоумышленника на пользователя, опирающиеся на профили уязвимостей пользователя и компетенций злоумышленника.
- Предложены новые вероятностная модель и метод оценки успеха многоходовой социоинженерной атаки, отличающиеся тем, что позволяют учесть результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети.

- В целях оценки параметров моделей используются данные, извлекаемые из социальных сетей, для чего впервые разработаны методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, основанные на методах машинного обучения. 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. Также предложены новые методы, позволяющие дополнить фрагмент мета-профиля пользователя информационной системы, которые построены на основе агрегации доступных сведений из альтернативных источников.
- Впервые разработана архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также осуществлена реализация в указанном комплексе предложенных в диссертации новых алгоритмов.

Теоретическая и практическая значимость работы. 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 социоинженерных атак, а также рассчитывать вероятности реализации каждой такой траектории, 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.

Методология диссертационного исследования заключается в постановке и формализации задач, связанных с оценками защищённости/поражаемости пользователей и критичных документов, описании моделей сущностей, используемых для построения оценок, разработке моделей, методов и алгоритмов для оценки некоторых параметров моделей, апробации полученных теоретических результатов посредством их реализации в модулях комплекса программ и его тестировании. Методология основана на моделях комплекса «критичные документы – информационная система – пользователь – злоумышленник», формализация которых делает возможным исследование изучаемых систем методами теории вероятностей, поиска и сопоставления информации, информатики.

Методы, используемые в диссертации, включают методы поиска, сопоставления и анализа сведений, извлекаемых из социальных сетей, характеризующих интенсивность общения между сотрудниками в компании, дающих возможность оценить степени выраженности некоторых особенностей их личности, как основы для дальнейшего построения профиля уязвимостей пользователя и оценок их защищённости, методы теории вероятностей для построения оценок вероятности успеха социоинженерной атаки злоумышленника на пользователя, а также оценок защищённости пользователей.

Положениями, выносимыми на защиту, являются

1) подход к оценке защищённости пользователя с использованием усовершенствованных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» составляет основу метода и вероятностной модели оценки защищённости пользователя, опирающихся на профиль компетенций злоумышленника и профиль уязвимостей пользователей;

2) разработанные вероятностная модель и опирающиеся на неё методы оценки успеха многоходовой социоинженерной атаки учитывают результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети;

3) предложенные алгоритмы позволяют производить автоматизированный поиск аккаунтов сотрудников компании в социальной сети ВКонтакте, автоматизированную оценку выраженности ряда особенностей пользователей на основании данных, содержащихся в контенте, публикуемом пользователями социальных сетей, восстановление фрагмента мета-профиля пользователя информационной системы (а именно, родной город, город проживания, год рождения), построенного на основе агрегации доступных сведений;

4) архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем является основой для реализации в указанном комплексе предложенных выше алгоритмов.

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.

Апробация результатов. Итоги исследования были представлены на ряде научных мероприятий: Информационная безопасность регионов России (ИБРР–2013, ИБРР–2015, ИБРР–2017); Международная конференция по мягким вычислениям и измерениям (SCM–2014, SCM–2015, SCM–2016, SCM–2017); VI всероссийская научно-практическая конференция «Нечёткие системы и мягкие вычисления» (НСМВ–2014); Всероссийская научная конференция по проблемам информатики (СПИСОК–2014, СПИСОК–2016, СПИСОК–2017); Международная научно-практическая конференция «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-14, ISC-15); XIV Санкт-Петербургская международная конференция «Региональная Информатика» (РИ-2014, РИ-2016); Научная сессия НИЯУ МИФИ-2015; First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures, (BICA–2016); International Scientific Conference «Intelligent Information Technologies for Industry» (IITI'16, IITI'17); 15-ая национальная конференция по искусственному интеллекту с международным участием КИИ-2016; IV Международная летняя школа-семинар по искусственному интеллекту для студентов, аспирантов, молодых ученых и специалистов «Интеллектуальные системы и технологии: современное состояние и перспективы» ISYT–2017; VII всероссийская научно-практическая конференция «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ–2017; 1-ая Всероссийская научно-практическая конференция «Нечёткие системы и мягкие вычисления. Промышленные применения» (Ульяновск, 2017); Школа-семинар по искусственному интеллекту (Тверь, 2018); доклад на заседании учёного совета СПИИРАН 25.01.2018.

Результаты, полученные в диссертации, были использованы в НИР, поддержанных 1) грантами РФФИ: «Социоинженерные атаки в корпоративных информационных системах: подходы, методы и алгоритмы выявления наиболее вероятных траекторий» № **18-37-00323-мол_а**, 2018–2019, соискатель — руководитель проекта; «Гибридные методы, модели и алгоритмы анализа и синтеза оценок параметров латентных процессов в сложных социальных системах при информационном дефиците» № **14-01-00580-а**, 2014–2016; «Методология интеллектуального поиска маркеров в Интернет-контенте» № **14-07-00694-а**, 2014–2016; «Методы идентификации параметров социальных процессов по неполной информации на основе вероятностных графических моделей» № **16-31-00373**, 2016–2018; 2) стипендиями Президента РФ: пр. Минобрнауки РФ **418 от 22.04.2015**, пр. СПбГУ № **4861/3 от 19.04.2017**.

Публикации по теме диссертации. Было сделано 48 публикаций и приравненных к ним научных работ по теме диссертации, из них — 2 монографии, 7 публикаций в изданиях, индексируемых Scopus/WoS, 6 статей в изданиях из «Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук», 40 докладов и тезисов на научных конференциях (из которых 9 единоличных), получены 7 свидетельств о регистрации программ для ЭВМ (РОСПАТЕНТ). Полный перечень публикаций соискателя по теме диссертации представлен в приложении Ж диссертационной работы.

Личный вклад Абрамова М.В. в ключевые публикации с соавторами характеризуется следующим образом. В статьях, опубликованных в журналах из перечня российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук, результаты распределяются следующим образом. В [3] М.В. Абрамову принадлежит анализ алгоритмов обхода

социального графа сотрудников компании, в [4] модель оценки защищённости пользователей информационной системы от социоинженерных атак злоумышленника, в [5] вероятностно-реляционные модели пользователя и злоумышленника, в [6] — модель профиля компетенций злоумышленника и оценки вероятности социоинженерной атаки злоумышленника, в [8] модель оценки вероятности успеха многоходовой социоинженерной атаки. Личный вклад соискателя в другие публикации, выполненные в соавторстве, описан в диссертации.

Структура и объём диссертации. Текст работы включает в себя введение, четыре главы, заключение, словарь терминов, список литературы (более 200 позиций), список иллюстративного материала (рисунки и таблицы) и приложения, содержащие свидетельства о регистрации программ для ЭВМ, некоторые элементы реализации заявленных в работе моделей, методов и алгоритмов, акты о внедрении результатов диссертационной работы. Общий объём диссертации — 232 страницы.

Основное содержание работы

Во введении диссертационной работы обоснована актуальность исследования, приведены цель и задачи работы, описана научная новизна, теоретическая и практическая значимость исследования, представлены методология и методика. Также во введении обозначена обоснованность и достоверность представленных в работе научных положений, приведены информация об апробации результатов исследования, сведения о публикациях автора и вкладе в основные из них, сделанные в соавторстве.

В первой главе диссертации приведён анализ проблемы защиты пользователей информационных систем от социоинженерных атак. Обозначены важные место и роль проблемы защиты пользователей информационных систем от атак, проводимых с использованием методов социальной инженерии. В главе представлены основные подходы к разрешению этой проблемы, среди которых выделяются два основных класса. Первый связан с подходами к формированию различных стандартов, регламентирующих работу сотрудников компании, соблюдение которых позволит минимизировать риски утечки критичной информации. Второй связан с разработкой программного обеспечения для оперативного принятия мер по обеспечению безопасности критичных документов, в случае сомнительных действий пользователя.

Во второй главе диссертации представлены результаты исследований, которые стали заделом для решения ряда задач, поставленных в настоящей диссертационной работе. В ней представлен подход к оценке информации в интересах рефлексивного управления, предложенный В.Ю. Осиповым. Также в главе приведены термины, ассоциированные так или иначе с термином социальной инженерии, такие как корпоративный шпионаж, конкурентная разведка, рефлексивное управление. Представлен подход И.В. Котенко и М.В. Степашкина к анализу защищённости компьютерных сетей от программно-технических атак, основанный на анализе деревьев атак, а также его оптимизация, предложенная А.А. Чечулиным, в целях поддержки экспресс-диагностики. Рассмотрены модели комплекса «информационная система — персонал — критичные документы» (по дис. А.А. Азарова), на основании которых строились оценки поражаемости/защищённости пользователей и критичных документов информационной системы от социоинженерных атак.

В третьей главе представлены теоретические результаты, полученные соискателем. Приведены показатели, которые будут измеряться, и соотнесены с регламентирующими документами. Сформулированы общие алгебраические модели для представления параметров, которые должны учитываться при построении оценок защищённости пользователей информационных систем от социоинженерных атак и оценок вероятности поражения критичных документов. Отмечается, что модели критичных документов и хостов информационной системы подробно рассматриваются в задачах защиты информации от программно-технических атак.

Модель критичных документов содержит компоненты, которые связаны с уровнем критичности для компании, расположением на хостах и доступом к документу с них, уровнем доступа пользователей к документу и иные. Формальная модель критичного документа может выглядеть следующим образом $\mathrm{CD}_i = \left(\mathrm{Lc}^i; \left\{ H_j^i \right\}_{j=1}^{n}; \left\{ \left(U_k^i; \mathrm{LAD}_k^i \right) \right\}_{k=1}^{m} \right)$, где Lc^i — уровень критичности документа, $\left\{ H_j^i \right\}_{j=1}^{k}$ — хосты, с которых он доступен, $\left\{ \left(U_k^i; \mathrm{LAD}_k^i \right) \right\}_{k=1}^{m}$ — пользователи, имеющие доступ к i-ому документу определённого уровня, LAD_k^i — уровень доступа.

Модель хостов информационной системы представима в виде $H_i = \left(\left\{ \text{Soft}_j^i \right\}_{j=1}^n ; \left\{ \text{CD}_t^i \right\}_{t=1}^r ; \left\{ \text{Conn}_k^i \right\}_{k=1}^m ; \left\{ \left(U_l^i ; \text{LAH}_l^i \right) \right\}_{l=1}^q ; \text{Lc}^i \right)$, где $\left\{ \text{Soft}_j^i \right\}_{j=1}^n$ — установленное на нём программное обеспечение, $\left\{ \text{CD}_t^i \right\}_{t=1}^r$ — критичные документы, доступные с него, $\left\{ \text{Conn}_k^i \right\}_{k=1}^m$ — его связи с другими хостами, $\left\{ \left(U_l^i ; \text{LAH}_l^i \right) \right\}_{l=1}^q$ — пользователи с уровнями доступа к хосту, Lc^i — уровень критичности хоста, который связан с критичностью доступных с него документов.

Модель пользователя информационной системы может быть формализована как $U_i = \left(\left\{ \left(V_j, D_i(V_j) \right) \right\}_{j=1}^n ; \left\{ \left(\text{AH}_l^i ; \text{LAH}_l^i \right) \right\}_{l=1}^m ; \left\{ \left(\text{AD}_k^i ; \text{LAD}_k^i \right) \right\}_{k=1}^q ; \left\{ \text{Comm}_t^i \right\}_{t=1}^r ; \left\{ \text{CA}_a^i \right\}_{a=1}^b ; \text{State}_g^i \right)$, где $\left\{ \left(V_j, D_i(V_j) \right) \right\}_{j=1}^m$ — профиль уязвимостей пользователя, в котором V_j — уязвимость, а $D_i(V_j)$ — выраженность V_j, $\left\{ \left(\text{AH}_l^i ; \text{LAH}_l^i \right) \right\}_{l=1}^m$ — хосты с уровнем доступа к ним, $\left\{ \left(\text{AD}_k^i ; \text{LAD}_k^i \right) \right\}_{k=1}^q$ — документы с уровнем доступа к ним, $\left\{ \text{Comm}_t^i \right\}_{t=1}^r$ — тип взаимоотношений пользователя с другими пользователями информационной системы, $\left\{ \text{CA}_a^i \right\}_{a=1}^b$ — контролируемые зоны, доступные ему, State_g^i — внутреннее состояние, которое может влиять на его ответные действия при атаке.

Формализация модели злоумышленника может быть представлена следующим образом $M_i = \left(\left\{ \left(R_j, Q_i\left(R_j\right) \right) \right\}_{j=1}^n ; \left\{ \left(A_k, S_i\left(A_k\right) \right) \right\}_{k=1}^m ; \left\{ \text{BK}_t^i \right\}_{t=1}^q ; G^i ; \left\{ \text{Comm}_t^i \right\}_{t=1}^r \right)$, где $\left\{ \left(R_j, Q_i\left(R_j\right) \right) \right\}_{j=1}^n$ — ресурсы, доступные злоумышленнику (например, время, деньги или личностные особенности злоумышленника), $\left\{ \left(A_k, S_i\left(A_k\right) \right) \right\}_{k=1}^m$ — профиль компетенций злоумышленника (компетенция злоумышленника и степень умения использовать им определённое атакующее действие рассматриваются как синонимы), $\left\{ \text{BK}_i \right\}_{i=1}^l$ — начальные знания злоумышленника об архитектуре системы (её сотрудниках, их уязвимостях, доступных им критичных документах, взаимоотношениях персонала и контролируемых зонах), G^i — цель злоумышленника, $\left\{ \text{Comm}_t^i \right\}_{t=1}^r$ — связи злоумышленника с другими злоумышленниками.

Далее в работе вводятся адаптированные реляционные модели профиля уязвимостей пользователя, профиля компетенций злоумышленника, связей между ними, пользователя, критичных документов и злоумышленника, которые используются при построении оценок защищённости/поражаемости пользователей и критичных документов. Для построения оценок защищённости пользователей информационных систем от социоинженерных атак, оценок вероятности поражения критичных документов, вероятности успеха социоинженерной атаки необходимо построить модель для оценки успеха прямой социоинженерной атаки злоумышленника на пользователя. Для этой оценки, которая будет учитывать модели профиля компетенций злоумышленника и профиля уязвимостей пользователя, вводятся соответствующие реляционные модели профиля уязвимостей, профиля компетенций злоумышленника и их взаимосвязи.

Профиль компетенций злоумышленника может быть охарактеризован степенью умения злоумышленника использовать определённые типы социоинженерных атакующих воздействий. Формализация профиля компетенций злоумышленника может быть представлена в виде $((A_1, S(A_1)), \ldots, (A_q, S(A_q)))$, где A_i — это вид социоинженерного атакующего воздействия, а $S(A_i)$ — степень владения злоумышленником данным атакующим воздействием. Степень владения атакующим воздействием — это один из факторов, влияющих на оценку успешности атаки, выражающий некоторое умение злоумышленника.

При имитации социоинженерных атакующих воздействий успех такого воздействия злоумышленника будет определяться степенью владения им различными социоинженерными атакующими воздействиями и степенью выраженности уязвимостей атакуемого пользователя ин-

формационной системы: $p_{ij} = F\left(\left(A_i, S(A_i)\right), \left(V_j, D\left(V_j\right)\right), Q\right)$, где $S(A_i)$ — степень владения злоумышленником социоинженерным атакующим воздействием A_i, $D\left(V_j\right)$ — выраженность у пользователя уязвимости V_j, Q — матрица пороговых значений вероятностей, а p_{ij} — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя. Отмечается, что примером такой функции может служить треугольная норма, но не только она. Примеры адаптированных треугольных норм для оценки вероятности успеха:

$$p_{ij} = F\left(\left(A_i, S(A_i)\right), \left(V_j, D\left(V_j\right)\right), Q\right) = \min\left(S(A_i), D\left(V_j\right)\right) q_{ji};$$

$$p_{ij} = F\left(\left(A_i, S(A_i)\right), \left(V_j, D\left(V_j\right)\right), Q\right) = S(A_i) D\left(V_j\right) q_{ji};$$

$$p_{ij} = F\left(\left(A_i, S(A_i)\right), \left(V_j, D\left(V_j\right)\right), Q\right) = \max\left(S(A_i) + D\left(V_j\right) - 1, 0\right) q_{ji}.$$

Также для формализации этой зависимости можно использовать параметризованную t-норму Ягера.

$$p_{ij} = F\left(\left(A_i, S(A_i)\right), \left(V_j, D\left(V_j\right)\right), Q\right) = \begin{cases} \max\left(1 - \left(\left(1 - S(A_i)^{q_{ji}}\right) + \left(1 - D\left(V_j\right)^{q_{ji}}\right)\right)^{\frac{1}{q_{ji}}}, 0\right), \text{если } q_{ji} \in (0,1], \\ 0, \text{если } q_{ji} = 0. \end{cases}$$

Пусть p_{ij} — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя, тогда $1 - p_{ij}$ — оценка вероятности того, что социоинженерное атакующее воздействие не завершится успехом при одном эпизоде определенного типа атакующего воздействия на определённую уязвимость. Теперь требуется построить модель так, чтобы каждый эпизод в зависимости от типа атакующего воздействия и уязвимости вносил свой вклад в снижение оценки степени защищенности (если сформулировать строже — ожидаемого значения оценки степени защищенности).

Для расчёта оценки вероятности того, что социоинженерная атака злоумышленника с использованием всех имеющихся у него компетенций на все уязвимости пользователя не завершится успехом, предлагается адаптировать модель Белла–Тревино. В данном случае в качестве числа эпизодов будут выступать количества компетенций злоумышленника и уязвимостей пользователя, которые могут быть задействованы при атаке. Таким образом, оценка успеха социоинженерной атаки злоумышленника на пользователя с использованием всех атакующих воздействий по отношению ко всем уязвимостям будем выражаться следующим образом $P_k = 1 - \prod_i \prod_l \left(1 - p_{ij}^k\right)$, где p_{ij}^k — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость k-ого пользователя, а P_k — оценка вероятности успеха атаки злоумышленника с использованием всех доступных атакующих воздействий на k-ого пользователя.

Также предлагаются оценки вероятности поражения критичных документов при социоинженерной атаке. Для этого вводятся соответствующие реляционные модели. Данная задача может быть сформулирована по-разному в зависимости от исходных условий. Например, задача может заключаться в расчёте оценки вероятности поражения критичных документов определённого уровня критичности с учётом того, что критичные документы разбиты по группам, исходя из их уровня критичности, и каждый пользователь информационной системы имеет доступ к документам какого-то одного уровня критичности.

Пусть P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником (формула представлена выше). Тогда вероятность того, что критичные документы определённого уровня критичности не будут поражены через k-ого пользователя, имеющего к нему доступ, выражается как $1 - P_k$. Отметим, что к критичным документам определённого уровня критичности имеет доступ не один, а некоторое множество пользователей. С

учётом этого оценка вероятности того, что критичные документы определённого уровня критичности будут поражены выражается как $H_r = 1 - \prod_{k \in K_r} (1 - P_k)$, где K_r — множество пользователей, которые имеют доступ к документам уровня критичности r, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, H_r — оценка вероятности того, что критичные документы уровня критичности r будут поражены.

Вторая задача заключается в расчёте оценки вероятности поражения документов определённого уровня критичности в случае, когда критичные документы разбиты по группам по уровню критичности, и пользователи имеют доступ к критичным документам своего уровня критичности и документам всех уровней ниже.

Формулы расчёта оценки вероятности поражения критичных документов первого (наивысшего) уровня критичности и последующих:

$$H_1 = 1 - \prod_{k \in K_1} (1 - P_k), \; H_{r+1} = 1 - (1 - H_r) \prod_{k \in K_{r+1}} (1 - P_k),$$

где K_1, K_{r+1} — множества пользователей, которые имеют доступ к документам первого и $r+1$ уровня критичности соответственно, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, H_1, H_{r+1} — оценки вероятностей того, что критичные документы первого и $r+1$ уровня критичности будут поражены.

Третья задача заключается в построении оценки вероятности поражения критичного документа определённого уровня критичности, исходя из того, что критичные документы разбиты по уровням критичности, а пользователи имеют доступ к определённому количеству критичных документов каждого уровня критичности. Расчёт оценки вероятности поражения критичного документа уровня r в этом случае выражается следующим образом $h_r = \frac{\sum_m n_m^r \left(1 - \left(1 - \bar{p}\right)^m\right)}{\sum_m n_m^r}$, где n_m^r — число критичных документов уровня критичности r, к которым имеют доступ m пользователей, $\bar{p}$ — вероятность поражения критичного документа через одного пользователя, h_r — оценка вероятности поражения критичного документа уровня критичности r. $\bar{p}$ может быть рассчитана следующим образом $\bar{p} = \frac{\sum_{k=1}^{c} P_k}{c}$, где P_k — оценка вероятности того, что пользователь k будет успешно атакован злоумышленником, c — общее число пользователей информационной системы, имеющих доступ к критичным документам определённого уровня.

Также представлены оценки поражения критичных документов разного уровня критичности, с учётом того, что налаживание контакта с пользователем информационной системы не всегда гарантирует компрометацию критичных документов, доступных ему. Формулы для приведённых выше задач расчёта оценки вероятности поражения критичных документов определённого уровня критичности в этом случае будут соответствующие

$$H_r = \left(1 - \prod_{k \in K_r} (1 - P_k)\right) \mathring{p}_r, \; H_{r+1} = \left(1 - (1 - H_r) \prod_{k \in K_{r+1}} (1 - P_k)\right) \mathring{p}_r, \; h_r = \frac{\sum_m n_m^r \left(1 - \left(1 - \bar{p}\right)^m\right)}{\sum_m n_m^r} \mathring{p}_r,$$

где K_r — множество пользователей, которые имеют доступ к документам уровня критичности r, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, $\mathring{p}$ — вероятность получения доступа к критичному документу, к которому имеет доступ успешно атакованный пользователь информационной системы, H_r — оценка вероятности того, что критичные документы уровня критичности r будут поражены, n_m^r — количество критичных документов уровня критичности r, к которым имеют доступ m пользователей, $\bar{p}$ — вероят-

ность поражения критичного документа через одного пользователя, h_r — оценка вероятности поражения критичного документа уровня критичности r.

Рассмотрена задача построения оценки успеха социоинженерной атаки злоумышленника на пользователя с учётом того, что злоумышленником используется определённое количество одного вида ресурса на каждое атакующее воздействие, при этом общее количество ресурса ограничено. В примере для двух атакующих действий вероятности успеха атаки с использованием злоумышленником первого и второго вида воздействия соответственно будут следующими: $P_1 = 1-(1-p_{11})^{\frac{w_{11}}{v_{11}}}$, $P_2 = 1-(1-p_{21})^{\frac{w_{21}}{v_{21}}}$, где w_{11}, w_{21} — количество ресурса, которое злоумышленник готов использовать при первом и втором социоинженерном атакующем воздействии на первую уязвимость пользователя. v_{11}, v_{21} — количество ресурса, которое необходимо затратить при первом и втором социоинженерном атакующем воздействии на первую уязвимость пользователя, чтобы поразить его с вероятностями p_{11} и p_{21} соответственно, при этом $v_{11} > 0, v_{21} > 0$. Предполагается, что общее количество затрачиваемого злоумышленником на атаку ресурса $I = w_{11} + w_{21}$. При этом $0 \le I \le L$, где L — общее количество ресурса, имеющегося у злоумышленника. При таких предположениях, вероятность успеха атаки злоумышленника на пользователя будет выражаться следующим образом $P = 1-(1-p_{11})^{\frac{w_{11}}{v_{11}}}(1-p_{21})^{\frac{w_{21}}{v_{21}}} = 1-(1-p_{11})^{\frac{w_{11}}{v_{11}}}(1-p_{21})^{\frac{I-w_{11}}{v_{21}}}$. Её математическое ожидание в предположении, что w_{11} распределена равномерно, следующее

$$\frac{1}{I}\int_0^I \left(1-(1-p_{11})^{\frac{w_{11}}{v_{11}}}(1-p_{21})^{\frac{I-w_{11}}{v_{21}}}\right) dw_{11} = \frac{1}{I}\left(w_{11} - \frac{v_{21}(1-p_{21})^{\frac{I}{v_{11}}} e^{\frac{\ln(1-p_{11})w_{11}}{v_{21}} - \frac{\ln(1-p_{21})w_{11}}{v_{21}}}}{\ln(1-p_{11}) - \ln(1-p_{21})} \right)\Bigg|_0^I =$$

$$= 1 - \frac{v_{21}(1-p_{21})^{\frac{I}{v_{11}}} e^{\frac{\ln(1-p_{11})I}{v_{21}} - \frac{\ln(1-p_{21})I}{v_{21}}}}{I\left(\ln(1-p_{11}) - \ln(1-p_{21})\right)} + \frac{v_{21}(1-p_{21})^{\frac{I}{v_{11}}}}{I\left(\ln(1-p_{11}) - \ln(1-p_{21})\right)}.$$

В некоторых случаях при $p_{11} = p_{21}$, $p_{11} = 1$, $p_{21} = 1$, $p_{11} = 0$ или $p_{21} = 0$, вероятность успеха атаки и математическое ожидание считаются иначе.

Хотя известны приведенные выше модели, явно или неявно опирающиеся на свертки распределений вероятности, для проведения экспресс-оценки с целью ускорения расчёта оценки защищённости/поражаемости количество ресурса рассматривается не как непрерывная величина, а как величина, которая допускает «квантование», т.е. будем считать, что эффект от атакующего действия проявится только если злоумышленник затратил объем ресурса выше некоторой заданной пороговой величины. Пусть w_{ij} — количество ресурса, которое злоумышленник готов использовать при i-ом социоинженерном атакующем воздействии на j-ую уязвимость пользователя. v_{ij} — минимальное количество ресурса, которое необходимо затратить при i-ом социоинженерном атакующем воздействии на j-ую уязвимость пользователя. Тогда оценка вероятности успеха атаки злоумышленника с использованием всех доступных атакующих воздействий на k-ого пользователя при определённых предположениях может быть представлена следующим образом $P_k = 1 - \prod_i \prod_I \left(1-p_{ij}^k\right)^{\left\lfloor \frac{w_{ij}}{v_{ij}} \right\rfloor}$, где p_{ij}^k — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость k-ого пользователя, а P_k — оценка вероятности успеха атаки злоумышленника с использованием всех доступных атакующих воздействий на k-ого пользователя.

Подход к оценке вероятности успеха многоходовой социоинженерной атаки основан на оценке вероятности перехода по дуге, причем эта оценка строится на базе сведений об интенсивности взаимодействия между соответствующей парой сотрудников. Формула для расчёта оценок вероятностей распространения социоинженерной атаки между двумя пользователями

будет иметь следующий вид: $P_{i,i+1} = 1 - \prod_t \left(1 - p_t^{i,i+1}\right)^{n_t}$, где $p_t^{i,i+1}$ — вероятность успеха социоинженерной атаки злоумышленника на пользователя по t-ой связи, n_t — число эпизодов, $P_{i,i+1}$ — оценка вероятности успеха распространения атаки на пользователя $i+1$ через пользователя i. Возникающие вопросы оценки разброса (иными словами, точности) вычисляемых оценок вероятности успеха атаки решаются с помощью применения рандомизации значений параметров и исследования получающегося распределения значений искомой величины; в частности, такое эмпирическое распределение можно получить с помощью метода Монте-Карло (рисунок 1).

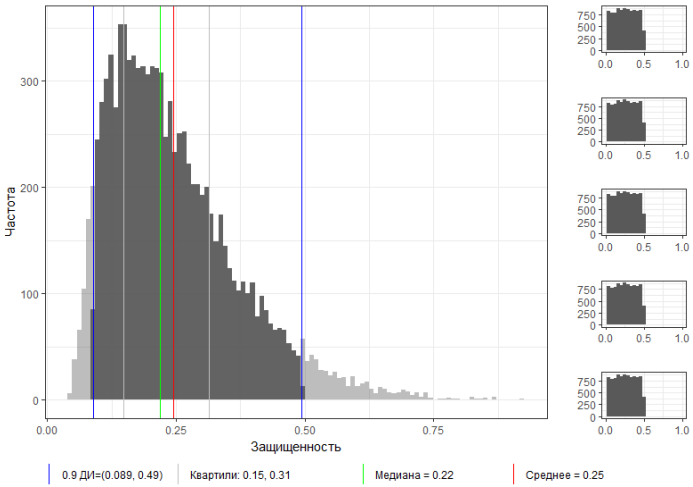


Рисунок 1 — Распределение значений оценки защищённости при равномерном распределении параметров $p_t^{i,i+1} \in [0,0.5]$

Предлагается подход к сбору и обработке сведений для оценки параметров моделей пользователя и межпользовательских связей. Данные сведения извлекаются из социальных сетей. Для автоматизированного поиска аккаунтов сотрудников компании в социальной сети используются методы машинного обучения. Строится дерево принятия решений, которое содержит в узлах следующие критерии для принятия решения:

1) наличие названия компании в графе «Карьера»;
2) упоминание имени сотрудника на стене официальной группы компании;
3) результат анализа топологии сети для данной страницы;
4) проверка наличия данной страницы в списке подписок компании;
5) счётчик отметок «Мне нравится», оставленных данным пользователем на стене группы компании.

Используются проактивные методы для расширения пространства поиска за счёт ручного включения новых вершин (аккаунтов пользователей).

Для автоматизированного построения оценок степени выраженности некоторых особенностей пользователей агрегируются данные, содержащиеся в контенте, публикуемом пользователями социальных сетей. На основе этих данных и результатов более ранних исследований строится обучающая выборка, которая используется для разработки модели классификатора методами машинного обучения. Выделяется методика и её реализация в алгоритме, включающем шаги проверки наличия у пользователя контента на странице, сбора текстовых записей на странице, анализа записей с помощью SVM и присвоением степени выраженности каждой характеристике.

Предложены методы восстановления фрагмента мета-профиля пользователя информационной системы, построенные на основе агрегации доступных сведений. В частности, предложены методы для восстановления информации о родном городе пользователя, городе проживания и годе рождения. В качестве источников информации могут выступать сведения, извлекаемые из аккаунтов пользователя в других социальных сетях, а также сведения, получаемые за счёт анализа его социального окружения. Методика идентификации аккаунтов одного пользователя в разных социальных сетях, состоит из следующих шагов:

1. Поиск аккаунтов пользователей в социальной сети ВКонтакте, о которых заведомо известно, что они являются сотрудниками компании. Иными словами, поиск v_i, где $i \in [1...m]$, m — количество сотрудников компании;

2. Поиск аккаунтов в социальных сетях Facebook и Instagram, потенциально ассоциированных с найденными аккаунтами пользователей в социальной сети ВКонтакте. Т.е. поиск v_i^1, v_i^2, v_i^3 — которые принадлежат одному сотруднику. В простейшем случае аккаунты будут привязаны друг к другу. В противном случае поиск осуществляется исходя из параметров, перечисленных ниже;

3. В каждой тройке аккаунтов будут анализироваться анкетные данные (ФИО, место и год рождения, образование, работа, интересы, политические и религиозные взгляды и т.п.), характер их социальных связей, фотоматериалы с хештегами, геолокационной информацией, отметками других пользователей, взаимная активность пользователей в виде лайков, репостов и прочих факторов;

4. На основе проведённого анализа будут отсеяны тройки или элементы троек, которые были выбраны ошибочно, остальные будут включены в базу данных;

5. На основе информации из аккаунтов каждой тройки будет построен фрагмент мета-профиля пользователя, содержащий более полную информацию о сотруднике компании, которая послужит базой для построения психологического профиля пользователя. Мета-профиль пользователя включает в себя анкетные данные (ФИО, место и год рождения, образование, работа, интересы, политические и религиозные взгляды и т.п.).

Второй метод связан с анализом социального окружения пользователя. Наряду с поиском недостающей информации в аккаунтах других социальных сетей анализируется социальное окружение пользователя в социальной сети ВКонтакте (т.е. друзья пользователя). Для этого предлагается группировать списки его друзей по различным параметрам: возрасту, школе, ВУЗу и т.д. Предположительно, к наибольшей по численности группе в каждой категории будет относиться анализируемый пользователь. Т.е., например, пользователь не указал на своей странице школу, которую заканчивал. Производится анализ списка его друзей, определяются пользователи, указавшие в своём аккаунте оканчиваемую школу, максимальная по количеству упоминаний школа считается школой, в которой учился данный пользователь. Данный метод реализуется в модуле прототипа комплекса программ.

В четвёртой главе представлена архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализация в указанном комплексе предложенных в диссертации алгоритмов. На рисунке 2 приведена система основных модулей прототипа комплекса программ и их описание. Модуль «Поиск персонала» реализует методику идентификации аккаунтов сотрудников компании в социальной сети на основе агрегации свидетельств, указывающих на это. Модуль «Психологические особенности» автоматизированно строит профиль ряда особенностей пользователя социальной сети, как основы для профиля уязвимостей пользователя. На входе он получает список аккаунтов сотрудников компании в социальной сети, а на выходе выдаёт оценки некоторых особенностей личности, которые позволяют строить профили их уязвимостей.

Рисунок 2 — Система компонент комплекса программ

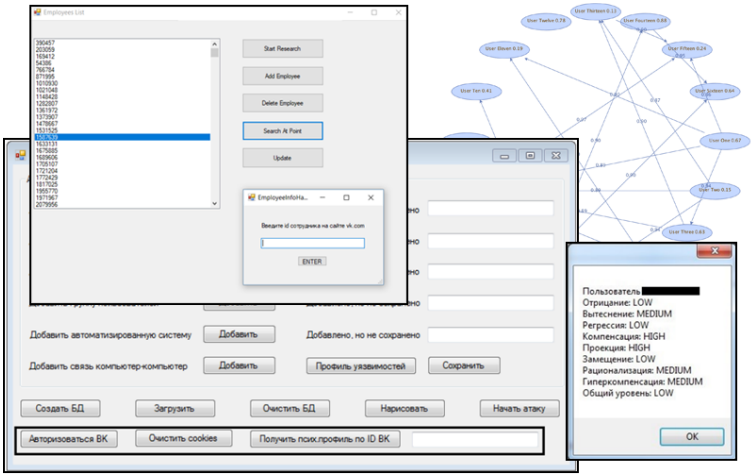


Рисунок 3 — Интерфейсы комплекса программ

Модуль «Анализатор атак» в качестве входных данных посредством API получает json-файл, содержащий аккаунты сотрудников компании в социальной сети ВКонтакте, а на выходе передаёт json-файл с размеченными рёбрами. На рёбрах отмечены оценки вероятностей распространения социоинженерной атаки на пользователя через другого пользователя. Модуль «Получение пользовательской информации» предназначен для автоматизации восстановления фрагмента мета-профиля пользователя на основании контента, публикуемого в социальных сетях. Также в главе представляются скриншоты работы, пользовательских и программных интерфейсов некоторых модулей прототипа комплекса программ.

Заключение

В диссертационной работе решена научная 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; в том числе получены следующие научные результаты, составляющие **итоги** исследования:

1. Разработаны подход к оценке защищённости пользователя с использованием усовершенствованных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» и основанные на нём вероятностная модель и метод оценки защищённости пользователя, опирающиеся на профиль компетенций злоумышленника и профиль уязвимостей пользователей. Предложены усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник»;
2. Представлены вероятностная модель и основанный на ней метод оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети. В модели используется метод оценки вероятности сложного события. Оценка строится на основании интенсивности наблюдаемого в социальной сети взаимодействия сотрудников в компании;
3. Разработаны алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, автоматизированной оценки выраженности ряда особенностей пользователей на основании данных, содержащихся в контенте, публикуемом пользователями социальных сетей, восстановления фрагмента мета-профиля пользователя информационной системы (а именно, родной город, город проживания, год рождения), построенные на основе агрегации доступных сведений;
4. Разработаны архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализация в указанном комплексе предложенных выше алгоритмов.

Сформулированы **рекомендации** по применению результатов работы в индустрии и в научных исследованиях. Результаты, представленные в диссертации, дают инструмент для автоматизации построения оценки некоторых особенностей пользователей на основе данных, извлекаемых из контента, публикуемого ими в социальных сетях. Эти оценки используются при построении их профилей уязвимостей, лежащих в основе оценок вероятности успеха социоинженерной атаки злоумышленника. Включение модели злоумышленника позволяет агрегировать большее количество параметров, влияющих на успех социоинженерной атаки. Также, полученные в диссертации результаты создают перспективы 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. Эти инструменты могут использоваться в работе HR-департаментов, службах информационной безопасности для предоставления информации лицам, принимающим решения.

В качестве **перспектив дальнейшей разработки тематики** можно выделить исследования, связанных с построением оценок защищённости пользователей информационных систем на основании информации, извлекаемой из их аккаунтов в социальных сетях. Предложенные подходы позволяют производить анализ возможных траекторий распространения многоходовых социоинженерных атак, а также рассчитывать вероятности реализации каждой такой траектории, 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 поиска решений форм. Кроме того, необходимо разрабатывать методики для оценки компетенций соответствующего профиля злоумышленника. Ограничения на компетенции и ресурсы злоумышленника могут оцениваться путём обратного моделирования от критичного документа к злоумышленнику. Видится обоснованным развитие модели ресурсов злоумышленника и её учёта в имитации социоинженерных атак. Кроме того, представляется интересным развитие моделей для представления и анализа динамики защищённости пользователей, а также эффектов превентивных воздействий (превентивных программ).

Соответствие паспорту специальности. Положения, выносимые на защиту, соотнесены с пунктами паспорта специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность»: «9. Модели и методы оценки защищенности информации и информационной безопасности объекта» (результаты 1–2), «13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (результаты 3–4), «14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» (результаты 3–4).

Список работ, опубликованных автором по теме диссертации

Монографии

1. Азаров, А.А. Социоинженерные атаки. Проблемы анализа / А.А. Азаров, Т.В. Тулупьева, А.В. Суворова, А.Л. Тулупьев, М.В. Абрамов, Р.М. Юсупов. СПб.: Наука, 2016. 352 с.
2. Тулупьев, А.Л. Мягкие вычисления и измерения. Модели и методы: монография / А.Л. Тулупьев, Т.В. Тулупьева, А.В. Суворова, М.В. Абрамов, А.А. Золотин, М.А. Зотов, А.А. Азаров, Е.А. Мальчевская, Д.Г., Торопова А.В. Левенец, Н.А. Харитонов, А.И. Бирилло, Р.И. Сольницев, С.В. Микони, С.П. Орлов, А.В. Толстов; под ред. д.т.н., проф. С.В. Прокопчиной. М.: ИД «Научная библиотека», 2017. 3 т. 300 с.

Статьи, опубликованные в журналах из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук

3. Абрамов, М.В. Анализ распространения имитированной социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей / М.В. Абрамов, А.А. Азаров // Информатизация и связь. 2015. Вып. 2. С. 69–76.
4. Азаров, А.А. Анализ защищенности групп пользователей информационной системы от социоинженерных атак: принципы и программная реализация / А.А. Азаров, М.В. Абрамов, А.Л. Тулупьев, Т.В. Тулупьева // Компьютерные инструменты в образовании. 2015. № 4. С. 52–60.

5. Азаров, А.А. Применение вероятностно-реляционных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» для анализа защищенности пользователей информационных систем от социо-инженерных атак / А.А. Азаров, М.В. Абрамов, Т.В. Тулупьева, А.А. Фильченков // Нечеткие системы и мягкие вычисления. 2015. №2. С.209–221.
6. Абрамов, М.В. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак / М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева, А.Л. Тулупьев // Информационно-управляющие системы. 2016. № 4. С. 77–84.
7. Абрамов, М.В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак / М.В. Абрамов // Автоматизация процессов управления. 2018. №1(51). С. 34–40.
8. Абрамов М.В. Задача анализа защищённости пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей / М.В. Абрамов, А.Л. Тулупьев, А.А. Сулейманов // Научно-технический вестник информационных технологий, механики и оптики. 2018. № 2. С. 313–321.

Статьи, опубликованные в изданиях WoS/Scopus

9. Azarov, A.A. Users' of Information System Protection Analysis from Malefactor's Social Engeneering Attacks Taking into Account Malefactor's Competence Profile / A.A. Azarov, M.V. Abramov, A.L. Tulupyev, T.V. Tulupyeva // Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. 2016. P. 25–30.
10. Tulupyeva, T.V. Character Reasoning of the Social Network Users on the Basis of the Content Contained on Their Personal Pages / T.V. Tulupyeva, A.L. Tulupyev, M.V. Abramov, A.A. Azarov, N.V. Bordovskaya // Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. 2016. P. 31–38.
11. Azarov, A.A. Models and algorithms for the information system's user's protection level probabilistic estimation / A.A. Azarov, M.V. Abramov, A.L. Tulupyev, T.V. Tulupyeva // Advances in Intelligent Systems and Computing. Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16). 2016. Vol. 2. P. 39–46.
12. Abramov, M.V. Social engineering attack modeling with the use of Bayesian networks / M.V. Abramov, A.A. Azarov // XIX IEEE International Conference on Soft Computing and Measurements (SCM'2016). St. Petersburg, 2016. P. 58–60.
13. Abramov M.V. Identifying user's of social networks psychological features on the basis of their musical preferences / M.V. Abramov, A.A. Azarov // XX IEEE International Conference on Soft Computing and Measurements (SCM'2017). St. Petersburg, 2017. P. 90–92.
14. Bagretsov, G.I. Approaches to development of models for text analysis of information in social network profiles in order to evaluate user's vulnerabilities profile / G.I. Bagretsov, N.A. Shindarev, M.V. Abramov, T.V. Tulupyeva // XX IEEE International Conference on Soft Computing and Measurements (SCM'2017). St. Petersburg, 2017. P. 93–95.
15. Shindarev, N. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities / N. Shindarev, G. Bagretsov, M. Abramov, T. Tulupyeva, A. Suvorova // Advances in Intelligent Systems and Computing. Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17). 2017. Vol.1. P.441–447.

Кроме того, были опубликованы 40 докладов и тезисов на научных мероприятиях (из которых 9 единоличных), получены 7 свидетельств о регистрации программ для ЭВМ (РОСПАТЕНТ). Полный перечень публикаций соискателя по теме исследования представлен в приложении Ж диссертационной работы.