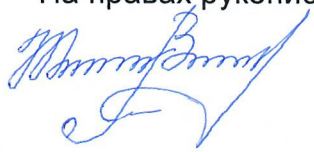
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт-Петербургский государственный университет»

Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук

На правах рукописи



АБРАМОВ Максим Викторович

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

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
д.физ.-мат.н. доцент Тулупьев А.Л.

Санкт-Петербург
2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы диссертации. Установившаяся в последнее время устойчивая тенденция роста количества атак на информационные системы, убытков от них, а также объёма ресурсов и времени, необходимых для нахождения виновных в подобных преступлениях, заставляет всё большее внимание уделять вопросам информационной безопасности [1–3, 28, 56, 105, 162, 213]. Эксперты сходятся во мнении об отсутствии перспектив к деградации или даже стабилизации данных показателей [213]. Актуальность проблем информационной безопасности постоянно подчёркивается на разных уровнях. В частности, Президентом РФ В.В. Путиным 15 января 2013 года был подписан указ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» [202]. 12 декабря 2014 года была представлена концепция этой системы [117]. 6 декабря 2016 года В.В. Путин утвердил новую доктрину ИБ [170], а 9 мая 2017 года подписал указ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [161].

Большая часть исследований в области информационной безопасности [9, 17, 23, 25, 37, 40, 51, 68, 115, 125, 127, 128, 136, 145, 153, 159, 160, 168, 189, 199] сегодня посвящена усовершенствованию её технической составляющей. В таком срезе вопросы информационной безопасности достаточно хорошо изучены, существуют разработки, позволяющие снизить вероятность успеха атаки злоумышленника. Среди них отметим [23, 140, 144, 145, 148–150, 152, 188, 214, 215]. В то же время пользователь информационной системы является одним из её самых уязвимых мест [45, 54, 178]. В отчётах крупных компаний и научной литературе [24, 30, 41, 112, 129, 130, 180, 190, 213] отмечается, что большая часть атак на информационную систему в настоящее время проводится с применением методов социальной инженерии. Актуальность проблем защищённости от социоинженерных атак и оценки степени этой защищённости (в частности

речь идёт о защищённости/поражаемости пользователей, персонала в целом, критичных документов) также подчёркивается инцидентами, которые становятся нам известны из сообщений СМИ. Одним из наиболее резонансных инцидентов стал взлом почты директора ЦРУ Джона Бреннана [167]. Американский подросток сначала выяснил некоторые детали аккаунта директора ЦРУ у сотового оператора Verizon, включая четыре последние цифры его банковской карты, номер почтового аккаунта AOL, 4-значный PIN-код и резервный номер мобильного телефона. А после завладел полным доступом к AOL-почте Бреннана, используя полученные от Verizon конфиденциальные данные для сброса старого пароля. Полученные данные были опубликованы на сайте WikiLeaks. Отметим, что всю потребовавшуюся для получения доступа к почте информацию злоумышленник получил не с помощью технического взлома базы данных сотового оператора, а в рамках телефонного разговора с сотрудниками компании.

Также резонансным стал инцидент, произошедший в 2013 году, когда Эдвард Сноуден похитил около 1.7 млн секретных файлов специальных служб США и часть из них передал газетам «Гардиан» (The Guardian) и «Вашингтон Пост» (The Washington Post) [166]. Скорее всего, Эдвард Сноуден не был инсайдером, но данный инцидент подчёркивает масштаб возможных эффектов от атак, произошедших не из-за программно-технических уязвимостей системы. Заметным стал случай с утечкой критичных документов об офшорах и сделках клиентов панамской юридической конторы Mossack Fonseca в 2016 году [110], после которого некоторые крупные политики были вынуждены подать в отставку.

Это не единичные случаи инцидентов ИБ, связанные с социоинженерными атаками. Не все материалы такого рода попадают в СМИ, часть из них описана в публикациях [57, 66, 96, 98, 123, 157, 174, 212].

Растущая сложность компьютерных сетей и механизмов их защиты [81, 141], увеличение числа уязвимостей пользователей, числа видов воз-

можных 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 разного масштаба, полноты, охвата и быстродействия автоматизированных средств (систем) анализа защищенности пользователей информационных систем. Эти системы призваны выполнять задачи по обнаружению уязвимостей пользователей информационной системы, информированию служб безопасности, выявлению возможных траекторий атакующих действий злоумышленников. В миссию таких систем должны войти идентификация отдельных пользователей или их групп, критичных с точки зрения защиты от социоинженерных атак, критичных сетевых ресурсов, поиск и анализ источников, содержащих критическую информацию о персонале, помощь в формировании политик безопасности соразмерных обнаруженным или ожидаемым угрозам, обеспечение лиц, принимающих решения, информацией, необходимой для выработки обоснованных решений по выбору защитных механизмов с учётом всего спектра известных условий [81]. Уязвимость пользователя определяется по аналогии с программно-технической уязвимостью и заключает в себе некоторую характеристику пользователя, которая делает возможным успех социоинженерного атакующего действия злоумышленника [109].

Подводя итог, отметим, 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 [97], в дальнейшем развитии, в частности, потребуется учитывать ограниченные ресурсы злоумышленников, подготовленность пользователей, возможности сотрудников, обеспечивающих безопасность информационной системы (в том числе в контексте социоинженерных атак), социальные сети и иные киберсоциальные системы, которые могут быть использованы злоумышленниками в качестве источников критичной информации о пользователях, особенности не только пользователей, но и злоумышленника (более точно, его компетенции, т.е. знания, умения, навыки по осуществлению социоинженерных атакующих воздействий разного рода).

Указанные противоречия и необходимость удовлетворить потребности, обозначенные тремя приведёнными выше аспектами, обеспечивает 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 автоматизированного построения профиля уязвимостей пользователя, что требует выявления и формализации связей между данными, содержащимися в контенте, публикуемом

пользователями, и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности. Кроме того, актуальны проблемы восстановления 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 информации, хранящейся в системе.

Степень разработанности темы. Т.В. Тулупьевой, А.Л. Тулупьевым был предложен подход к оценке защищённости пользователей информационной системы от социоинженерных атак [204, 205], на основе обобщения методологии анализа деревьев атак, выдвинутой И.В. Котенко и М.В. Степашкиным [142, 188]. В работе [97] 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 (результаты, достигнутые коллективом исследователей, в проблемно-постановочной и методологической части, отражены в монографии Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с. [96]).

Соискателем был разработан комплекс, «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 социоинженерного атакующих действий социоинженера-злоумышленника, 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 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, опирающаяся 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 пользователей (персонала) от таких атак.

Научная новизна исследования заключается в том, что предложены усовершенствованные модели комплекса «критичные документы — информационная система — пользователь — злоумышленник». Комплекс является развитием другого ранее разработанного комплекса [97], ключевой особенностью которого был учёт профиля уязвимостей пользователя. Основным элементом развития стало дополнение существующего комплекса «критичные документы – информационная система – пользователь» моделью злоумышленника. Впервые предложены основанные на указанном комплексе метод и 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.

Представлена новая вероятностная модель и опирающиеся на неё методы 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.

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.

Впервые разработана архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также 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» и основанные на нём метод и вероятностная модель оценки защищённости пользователя, опирающаяся на профиль компетенций злоумышленника и профиль уязвимостей пользователей;

2) вероятностная модель и опирающиеся на неё методы оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети;
3) 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) архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализация в указанном комплексе предложенных выше алгоритмов.

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).

Высокая **степень достоверности результатов** диссертации обеспечивается посредством глубокого анализа исследований по тематике ин-

формационной 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). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2013 г.
- XVII Международная конференция по мягким вычислениям и измерениям (SCM–2014), г. Санкт-Петербург, 2014 г.
- Шестая всероссийская научно-практическая конференция «Нечёткие системы и мягкие вычисления» (НСМВ–2014), г. Санкт-Петербург, 27–29 июня, 2014 г.
- Всероссийская научная конференция по проблемам информатики (СПИСОК–2014), г. Санкт-Петербург, 2014 г.
- Третья Международная научно-практическая конференция «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-14), г. Москва, 2014 г.
- XIV Санкт-Петербургская международная конференция «Региональная Информатика» (РИ-2014), г. Санкт-Петербург, 2014 г.
- Научная сессия НИЯУ МИФИ-2015, г. Москва, 2015 г.
- XVIII Международная конференция по мягким вычислениям и измерениям (SCM–2015), г. Санкт-Петербург, 2015 г.
- IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015), г. Санкт-Петербург, 28–30 октября 2015 г.

- Четвёртая Международная научно-практическая конференция «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-15), г. Москва, 2015 г.
- Всероссийская научная конференция по проблемам информатики (СПИСОК–2016), г. Санкт-Петербург, 2016 г.
- First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures, Moscow, 2016.
- First International Scientific Conference «Intelligent Information Technologies for Industry» (IITI’16), Sochi, 2016.
- XIX Международная конференция по мягким вычислениям и измерениям (SCM–2016), г. Санкт-Петербург, 2016 г.
- Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (г. Смоленск, 3-7 октября 2016 г.)
- Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». (Санкт-Петербург, 26-28 октября 2016 г.)
- XX Международная конференция по мягким вычислениям и измерениям (SCM–2017), г. Санкт-Петербург, 2017 г.
- 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 (Санкт-Петербург, 30 июня – 3 июля 2017 г.)
- VII всероссийская научно-практическая конференция «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ–2017 (г. Санкт-Петербург, 3–7 июля, 2017 г.)
- Second International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’17), Varna (Bulgaria), 2017.

- Первая Всероссийская научно-практическая конференция «Нечёткие системы и мягкие вычисления. Промышленные применения». Ульяновск, 2017.
- X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2017). Санкт-Петербург, 1–3 ноября 2017 г.
- 7-ая всероссийская научная конференция по проблемам информатики СПИСОК-2017. Санкт-Петербург, 25–25 апреля 2017 г.
- Школа-семинар по искусственному интеллекту. Тверь, 2018.
- Доклад на заседании учёного совета СПИИРАН 25.01.2018.

Результаты, полученные в диссертации, были использованы в научно-исследовательских проектах, поддержанных

1) грантами РФФИ:
   - «Гибридные методы, модели и алгоритмы анализа и синтеза оценок параметров латентных процессов в сложных социальных системах при информационном дефиците» (Грант РФФИ) № 14-01-00580-а, 2014–2016.
   - «Методология интеллектуального поиска маркеров в Интернет-контенте» (Грант РФФИ) № 14-07-00694-а, 2014–2016.
   - «Методы идентификации параметров социальных процессов по неполной информации на основе вероятностных графических моделей» (Грант РФФИ) № 16-31-00373, 2016–2018.
2) стипендиями Президента РФ:
   - Стипендия Президента Российской Федерации (пр. Министерства образования и науки РФ 418 от 22.04.2015)
   - Стипендия Президента Российской Федерации (пр. СПбГУ №4861/3 от 19.04.2017)

Публикации. По теме диссертации было сделано 48 публикаций и приравненных к ним научных работ. Из них — 2 монографии, 7 публика-

ций 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. Опубликованы статьи в следующих журналах из перечня рецензируемых научных изданий:

- Журнал «Информатизация и связь» [73];
- Журнал «Компьютерные инструменты в образовании» [90];
- Журнал «Нечеткие системы и мягкие вычисления» [95];
- Журнал «Информационно-управляющие системы» [81];
- Журнал «Автоматизация процессов управления» [72];
- Журнал «Научно-технический вестник информационных технологий, механики и оптики» [75].

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 [73] М.В. Абрамову принадлежит анализ алгоритмов обхода социального графа сотрудников компании, в [90] модель оценки защищённости пользователей информационной системы от социоинженерных атак злоумышленника, в [95] вероятностно-реляционные модели пользователя и злоумышленника, в [81] — модель профиля компетенций злоумышленника и оценки вероятности социоинженерной атаки злоумышленника, в [75] модель оценки вероятно-

сти успеха многоходовой социоинженерной атаки. Личный вклад соискателя в другие публикации, выполненные в соавторстве, представлен в диссертации.

Личный вклад М.В. Абрамова в другие публикации, сделанные с соавторами, характеризуется следующим образом: в [194] ему принадлежит модель информационной системы, отвечающей требованиям информационной безопасности; в [13, 14, 80, 93] формальное представление злоумышленника, включающее в себя его профиль компетенций; в [78, 91] — модель критичных документов и представление вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя; в [77, 79] — подход к моделированию распространения информации в социальных медиа на основании различных критериев; в [88, 94] — улучшенный алгоритм обхода графа межличностных связей пользователя; в [76] — представление некоторых элементов реализации алгоритмов для оценки защищённости/поражаемости пользователей и, опосредованно, критичных документов информационной системы от социоинженерных атак; в [65] — оценка статистических данных.

Структура и объем 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.

В первой главе диссертации приведён анализ проблемы защиты пользователей информационных систем от социоинженерных атак. Описываются 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.

Вторая глава посвящена результатам исследований, которые стали заделом для решения ряда задач, поставленных в настоящем диссертационном исследовании. В ней представлен подход к оценке информации в интересах рефлексивного управления, предложенные В.Ю. Осиповым [163]. 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. Представлены модели комплекса «информационная система — персонал — критичные документы» (по дис. А.А. Азарова [97]), на основании которых строились оценки поражаемости/защищённости пользователей и критичных документов информационной системы от социоинженерных атак.

В третьей главе представлены теоретические результаты, полученные соискателем. Рассмотрены модели комплекса «критичные документы – информационная система – пользователь – злоумышленник». Предложены модели для оценки вероятности успеха прямой социоинженерной атаки злоумышленника на пользователя, основанные на моделях профиля компетенций злоумышленника и профиля уязвимостей пользователя, оценки вероятности поражения критичных документов, для учёта

ограниченности ресурсов злоумышленника в оценках, оценки вероятности успеха многоходовой социоинженерной атаки. Представлены методы сбора и обработки сведений, извлекаемых из социальных сетей для оценки параметров модели пользователя и межпользовательских связях. Для этого представлено решение задачи автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, дальнейшая работа с найденными аккаунтами, которая заключается в восстановлении фрагментов мета-профилей пользователей на основании альтернативных источников информации; оценке степени выраженности некоторых особенностей пользователей, исходя из аудио- и текстового контента, публикуемого в их аккаунтах в социальной сети; оценке вероятности успеха прохождения социоинженерной атаки от пользователя к пользователю и модель оценки вероятности успеха многоходовой социоинженерной атаки.

В чётвёртой главе представлена архитектура прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем, а также реализация в указанном комплексе предложенных в диссертации алгоритмов. Реализация разработанных и предложенных в диссертации моделей, методов и алгоритмов в прототипе комплекса программ позволяет автоматизировать поиск сотрудников компании в социальной сети, оценку степени выраженности некоторых особенностей пользователей на основе данных, содержащихся в контенте, публикуемом пользователями социальных сетей. Также представлена автоматизация построения оценок защищённости пользователей информационных систем при многоходовых социоинженерных атаках, основанная на агрегации сведений из социальных сетей для анализа интенсивности взаимодействия сотрудников в компании.

Глава 1. ПРОБЛЕМА ОЦЕНКИ ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК: АНАЛИЗ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

Глава посвящена анализу проблемы защиты пользователей информационных систем от социоинженерных атак. Описываются место и роль проблемы защиты пользователей информационных систем от атак, проводимых с использованием методов социальной инженерии. 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.

1.1. МЕСТО И РОЛЬ ПРОБЛЕМЫ ЗАЩИЩИТЫ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК

Информационные технологии сегодня глубоко и повсеместно внедрены в нашу жизнь. Вместе с этим большую актуальность приобретают вопросы информационной безопасности. В последнее время киберпреступления стали происходить чаще, приносить большие убытки и требовать больше времени для установления виновных в подобных преступлениях и устранения последствий от них. Ежегодное исследование подразделения Hewlett Packard — Enterprise Security в сотрудничестве с Ponemon Institute показало, что среднегодовой убыток от киберпреступлений в 2016 году для компаний вырос на 12% в сравнении с 2015 годом и составил $17,36 млн [5, 105]. Наибольшие убытки терпят компании США, до $73 млн. Для полной ликвидации последствий инцидента сред-

нему американскому предприятию требуется 46 дней. Среди 237 компаний, принявших участие в опросе, размер убытков российских компаний — $2,4 млн. Этот показатель ниже прошлогоднего. Но такая динамика связана, прежде всего, с девальвацией российского рубля и ассоциированными с ней процессами [203].

Помимо прямого финансового ущерба, который терпят компании от киберпреступлений, также существенными являются и репутационные издержки, которые не всегда могут быть выражены в деньгах. Аналитики отмечают, что для финансовых организаций зачастую ущерб, нанесённый в следствие утраты репутации, превышает иные издержки [124, 183].

Общемировой тренд на рост убытков от киберпреступлений сохраняется уже на протяжении нескольких лет, что подтверждается ежегодными исследованиями Ponemon Institute при участии Hewlett Packard [1–5, 28, 56] (см. рисунок 1). Согласно исследованию компании Juniper Research, общемировой ущерб от кибератак вырос в 4 раза и при сохранении текущего уровня общие убытки мировой экономики от их осуществления составят $2,1 триллиона к 2019 году [162]. Первый заместитель председателя Сбербанка Лев Хасис считает, что оснований для снижения ущерба от киберпреступлений в будущем нет, он также отмечает, что проблема информационной безопасности становится для Сбербанка проблемой номер один [213]. Актуальность проблем информационной безопасности неоднократно подчёркивалась и Президентом РФ, Владимиром Путиным. Так 15 января 2013 году им был подписан указ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» [202]. 12 декабря 2014 года была представлена концепция этой системы [117].

Вообще говоря, проблема информационной безопасности имеет многовековую историю, но самостоятельную актуальность приобрела только во второй половине XX века в контексте начавшегося внедрения

автоматизированных систем в повседневную деятельность [156]. Информационная безопасность является одним из основных компонент национальной безопасности наряду с оборонной, экономической, социальной и другими [215]. Информационная безопасность включает в себя три раздела [215].

- Защита информации (программно-техническая защита и защита пользователей информационных систем от социоинженерных атак).
- Защита от информации.
- Добывание информации о потенциальных угрозах в информационной сфере.

Исследования в области защиты пользователей информационных систем от социоинженерных атак относятся к первому и третьему компонентам защиты информации. В настоящее время большая часть исследований посвящена усовершенствованию технической базы, осуществляющей контроль информационной безопасности. В таком срезе вопросы информационной безопасности хорошо изучены, разработано большое количество средств, позволяющих снизить вероятность успеха атаки злоумышленника [9, 17, 23, 25, 37, 40, 51, 68, 115, 125, 127, 128, 136, 153, 168, 189, 199]. Среди них отметим [23, 140, 144, 145, 148–150, 152, 188, 214, 215]. Однако пользователь информационной системы является одним из её самых уязвимых мест [45, 54, 178].

Согласно исследованиям Лаборатории Касперского наиболее распространённые инциденты информационной безопасности так или иначе связаны с действиями пользователей системы. Одним из наиболее эффективных видов атак на информационную безопасность является корпоративный шпионаж, которому подвергаются более четверти компаний и почти 80% из них успешно [129]. Понятие корпоративного шпионажа тесно связано с социальной инженерией [169]. В [213] отмечается, что бо-

лее 50% всех успешных атак осуществляется за счёт методов социальной инженерии. В [130] говорится о недооценке угроз информационной безопасности со стороны так называемых инсайдеров — людей, которые в силу своего служебного положения имеют доступ к конфиденциальной информации компании.

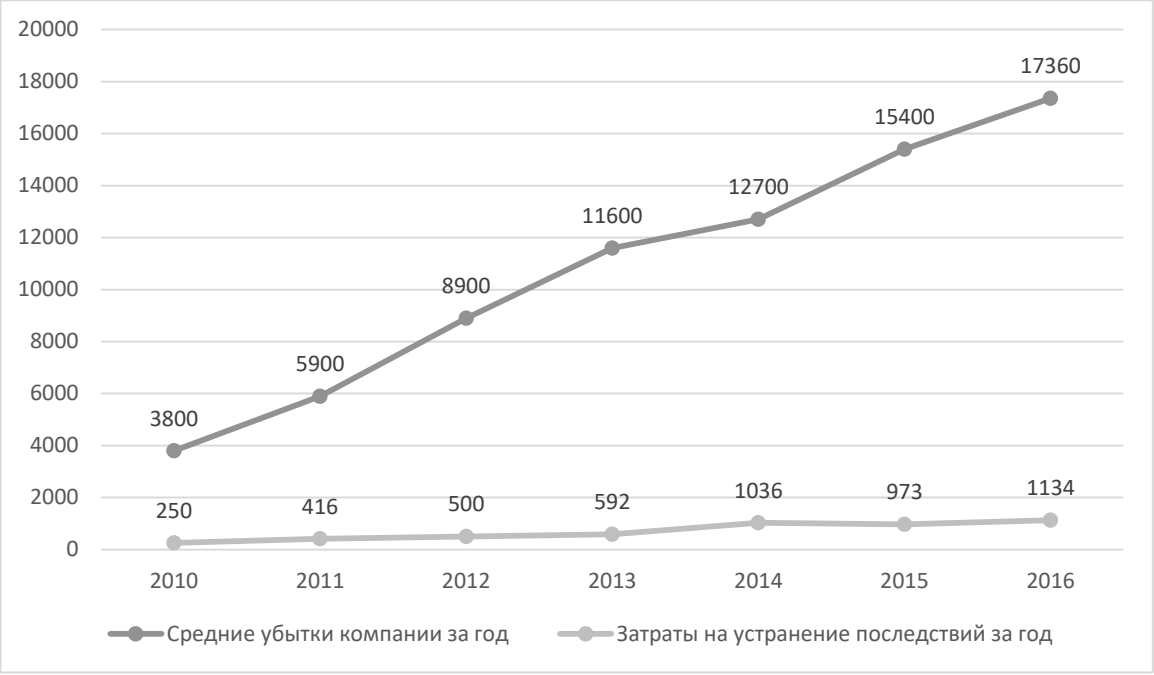


Рисунок 1 — График, отображающий средние убытки компании за год от киберпреступлений и затраты на устранение последствий кибератак в тысячах долларов США [1–5, 28, 56]

В целом, социоинженерные атаки сформировали заметную часть фронта угроз информационной безопасности информационных систем, что, в частности, актуализирует потребность в автоматизированном инструментарии анализа поражаемости/защищённости от социоинженерных атак, а в дальнейшей перспективе — в разработке организационных мер по уменьшению соответствующих рисков и приёмов и способов поиска наиболее вероятных путей реализации социоинженерных атак по наличию сведений об имевших место инцидентах. В настоящей диссертационной работе социоинженерная атака определяется как «набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной

или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности» [109].

Наиболее простым и часто упоминаемым в литературе примером социоинженерной атаки является ситуация, при которой новому сотруднику компании звонят по телефону и представляются начальником службы безопасности. Затем, ссылаясь на неполадки в системе информационной безопасности предприятия, выясняют у него логин и пароль для входа в систему [57].

Сотрудник компании, имеющий доступ к конфиденциальной информации, может преднамеренно или непреднамеренно нарушить её безопасность (конфиденциальность, целостность или доступность) [180, 190]. В исследовании В.С. Веденеева и И.В. Бычкова [112] отмечается, что 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. В частности, в России средний ущерб для компаний СМБ-сегмента (сегмент среднего и малого бизнеса) от серьёзного инцидента составляет 780 000 рублей, для крупных предприятий эта сумма может достигать 20 млн. рублей [129].

Актуальность исследований в области социоинженерных атак и разработки систем защиты от воздействий такого рода также подчёркивается крупными инцидентами, которые становятся известными. Так в 2013 году Эдвард Сноуден похитил около 1.7 млн секретных файлов специальных служб США и часть из них передал газетам «Гардиан» (The Guardian) и «Вашингтон Пост» (The Washington Post) [166]. Скорее всего, Эдвард Сноуден не был инсайдером, но данный инцидент подчёркивает масштаб

возможных эффектов от атак, произошедших не из-за программно-технических уязвимостей системы. В 2015 году произошёл другой крупный инцидент, который был связан с социоинженерными атаками. База данных известного сайта онлайн-бронирования Booking.com попала к злоумышленникам, которые разослали клиентам компании, забронировавшим апартаменты, письма с просьбой произвести стопроцентную предоплату [177]. Несмотря на возмущение многие из них произвели оплату.

Одним из наиболее резонансных инцидентов стал взлом почты директора ЦРУ Джона Бренана [167]. Американский подросток сначала выяснил некоторые детали аккаунта директора ЦРУ у сотового оператора Verizon, включая четыре последние цифры его банковской карты, номер почтового аккаунта AOL, 4-значный PIN-код и резервный номер мобильного телефона. Причем эта информация была получена не с помощью технического взлома базы данных сотового оператора, а в рамках телефонного разговора. А после завладел полным доступом к AOL-почте Бреннана, используя полученные от Verizon конфиденциальные данные для сброса старого пароля, а затем опубликовал данные на сайте WikiLeaks.

Это не единичные случаи инцидентов информационной безопасности, связанные с социоинженерными атаками. Не все материалы такого рода попадают в СМИ, часть из них описана в материалах [66, 110].

Таким образом, можно ожидать, что исследования в этой области помогут в создании многоуровневых систем безопасности, устойчивых к атакам злоумышленников, объединяющих программно-технические и социоинженерные её аспекты. При этом одной из важных задач в этой области является непрерывный мониторинг уровня защищённости информационной системы, сопряжённый со сбором и анализом различной информации. В последнее время постоянный интенсивный рост сложности информационных систем и механизмов их защиты [151], увеличение

числа уязвимостей пользователей, компетенций злоумышленников, использующих эти уязвимости, требует соответствующих научных исследований и разработок мощных автоматизированных средств (систем) анализа защищенности. Такие средства должны решать различные задачи, связанные с идентификацией и обнаружением уязвимостей пользователей, своевременному информированию служб безопасности и лиц, принимающих решения, выявлению возможных траекторий атак злоумышленников и ожидаемого уровня ущерба этих атак, поиска источников критичной информации о пользователях, наиболее уязвимых сетевых ресурсов, а также давать рекомендации для принятия мер, способствующих повышению уровня защищённости пользователей информационных систем и, как следствие, критичных документов.

Решение этих задач позволит существенно повысить защищенность пользователей информационных систем, то есть уменьшить вероятность успеха атаки злоумышленника на информационную систему. Для увеличения точности данной оценки предлагается расширение модели комплекса «информационная система — персонал — критичные документы» (ИСПКД) за счет включения профиля компетенций злоумышленника и перехода к более полной модели, а именно «критичные документы — информационная система — пользователь — злоумышленник» (КДИСПЗ).

1.2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОДХОДЫ К СИСТЕМАТИЗАЦИИ

Ряд источников [97, 106, 113, 133, 148, 175, 200, 201] посвящены поискам путей систематизации угроз информационной безопасности; результатами соответствующих исследовательских усилий являются классификации угроз по различному основанию. Основания таких классификаций опираются на один или несколько признаков [175, 200, 201]. Особо отметим источники [97, 114, 200], перечисление угроз информационной

безопасности и основания для их классификации в которых наиболее широки, в значительной степени покрывают иные, не столь богатые перечисления.

В работах [92, 97] приведена классификация, частично обобщающая указанные выше источники. Взяв за основу классификации из [92, 97, 200], представим их вариант, обновлённый за счёт внесения источников угроз, упоминаемых в [92, 97, 106, 113, 133, 148, 175, 200, 201]. Классификация представлена на рисунке 2.

Особое место в классификации угроз ИБ занимают web-атаки, которые могут быть классифицированы следующим образом [134].

- Аутентификация (выявление метода проверки идентификации пользователя)
  - Brute Force (Грубая сила — автоматизированный процесс подбора логинов, паролей, номеров кредитных карт или криптографических ключей)
  - Insufficient Authentication (неполное ограничение полномочий, происходит, когда web-сайт предоставляет злоумышленнику доступ к закрытым данным или функциональности без соответствующей авторизации)
  - Weak Password Recovery Validation (слабая процедура восстановления пароля)
- Авторизация (класс атак, целью которых является повышение уровня прав пользователя на сайте)
  - Credential/Session Prediction (прогнозирование сертификата/сессии, получение идентификатора сеанса из файлов cookie или URL-адреса)
  - Insufficient Session Expiration (незавершение сессии, возникает когда web -сайт разрешает использовать старые сертификаты или идентификаторы сессий для авторизации)

  - Session Fixation (фиксация сессии — принудительная установка идентификатора сессии в определённое значение)
- Атаки на стороне клиента
  - Content Spoofing (подмена содержания страницы)
  - Cross-site Scripting или XSS (межсайтовое выполнение сценариев — внедрение в web-страницу вредоносного кода и взаимодействие этого кода с сервером злоумышленника)
- Выполнение команд
- Информационное раскрытие
- Логические атаки

Выделяются следующие виды социоинженерных атак:

- фишинг [27]:
  - социальные сети: попытка манипулирования пользователем или получения информации через профиль пользователя в социальной сети;
  - электронная почта: фишинг-письма, которые используются для манипулирования пользователем с целью посещения им вредоносного веб-сайта или открытия вредоносного файла;
  - телефон: голосовой фишинг или «vishing», используемый для непосредственного извлечения информации или убеждения цели во взаимодействии со вредоносным веб-сайтом или ранее доставленным файлом;
  - физический: получение физического доступа к сайту или системам организации, использование обманного предлога или доставка физических носителей (например, USB-накопителя);
- телефонный фрикинг [157] — взлом телефонных систем с помощью подбора различных кодов. Техника появилась в конце 50-х в США. В корпорации Bell использовался тоновый набор с целью передачи служебных сигналов. Злоумышленники-социоинженеры пробовали по-

вторять эти сигналы, в случае успеха им удавалось совершать бесплатные телефонные звонки, а иногда и получать доступ к администрированию телефонной сети [157];

- претекстинг [157] — атака, при которой злоумышленник, представляясь другим человеком, по заранее подготовленному сценарию пытается получить конфиденциальную информацию;
    - квид про кво («услуга за услугу») — обращение злоумышленника в компанию по корпоративному телефону или электронной почте. Например, злоумышленник-социоинженер звонит в компанию по корпоративному телефону и сообщает, что занимается администрированием системы, но у него возникли некоторые технические проблемы, связанные с компьютером сотрудника. После чего предлагает свою помощь, и во время рекомендаций вынуждает пользователя выполнить действия, которые ему необходимы для компрометации системы. Согласно статистике, приведённой в [44], 90% офисных работников соглашаются сообщить свои конфиденциальные данные при личной заинтересованности;
- «дорожное яблоко» [44] — злоумышленник подбрасывает физические носители в места, где они могут быть легко найдены (обычно места общественного пользования: уборные, места для курения, переговорные, парковки т.п.), часто сотрудники компании проверяют эти носители на рабочих компьютерах;
- сбор информации из открытых источников (социальные сети, сайт компании);
- плечевой серфинг — наблюдение конфиденциальной информации через плечо;
- обратная атака [64], когда преступник побуждает жертву раскрывать личную информацию самостоятельно. Создаёт проблему, за решением которой пользователь вероятнее всего обратится именно к нему.

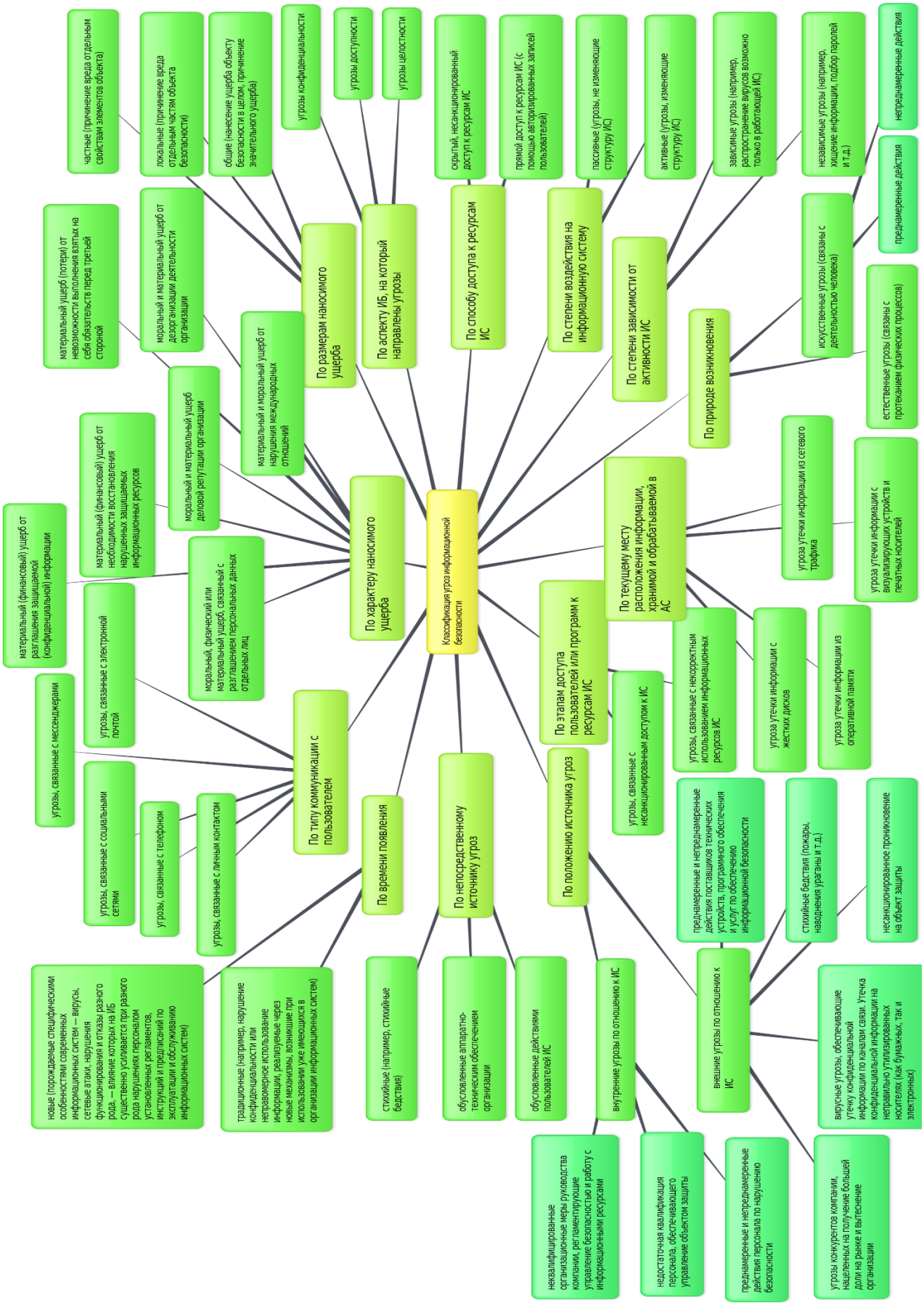


Рисунок 2 — Классификация угроз информационной безопасности основана на [92, 97, 106, 113, 133, 148, 175, 200, 201]

1.3. ПОДХОДЫ К ИССЛЕДОВАНИЯМ В ОБЛАСТИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Существуют несколько подходов к исследованиям в области социальной инженерии, которые связаны с решением задачи обеспечения защищённости пользователей информационных систем. Один из основных — это разработка стандартов и инструкций, регламентирующих работу сотрудников компании [36, 43, 59]. Но часто пользователи пренебрегают исполнением этих стандартов и компрометируют информационную систему.

Другой подход связан с защитой системы от социоинженерных атак на программно-техническом уровне. Среди таких исследований встречаются посвящённые правилам разграничения доступа, разработке DLP-систем, которые предназначены для мониторинга и блокирования подозрительных действий пользователя в системе (например, массового копирования документов, отправки критичных документов), но и они оказываются бессильны перед инсайдером, который может запомнить какую-то информацию, сфотографировать её на телефон и т.п.

При этом работы, связанные с анализом защищённости/поражаемости пользователей и критичных документов информационных систем от социоинженерных атак, а также разработкой систем упреждающей диагностики уязвимостей пользователей и бэктрекинга инцидентов, систематически не проводятся. Кроме того, хотя потребность в расследовании инцидентов упоминается как в научной литературе, так и в литературе управленческо-публицистического характера, до сих пор не предложены и не рассматриваются научные подходы к бэктрекингу инцидентов.

1.4. ОБОСНОВАНИЕ ЦЕЛИ И ЗАДАЧ ДИССЕРТАЦИИ

Изложенное выше является основанием актуальности общей цели исследования, которая 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. Вместе с тем необходимы инструменты для расследования подобных преступлений, поиска совокупностей обстоятельств, благодаря которым инцидент стал возможен. Важно также разработать систему профилактических мер, которые бы на основании результатов анализа защищённости пользователей информационной системы, позволяли уменьшить вероятность успеха социоинженерной атаки. Достижение этой цели видится результатом длительного междисциплинарного исследования, в рамках которого необходимо будет выяснить, как связаны уязвимости пользователя и степени выраженности некоторых особенностей его личности; разработать базы данных, содержащие перечни уязвимостей пользователя, атакующих действий злоумышленника, возможных ответных действиях пользователя и т.д.; агрегировать информацию из различных источников, на основании которой осуществлять построение профиля уязвимостей пользователя, оценивать возможные траектории распространения атаки.

Одна из частных целей, относящаяся к области технических наук, решается в данном диссертационном исследовании и заключается в формировании методики оценки поражения/защищённости пользователей и критичных документов информационных систем от социоинженерных атак, основанной на агрегации сведений из социальных сетей и других источников для автоматизации выявления связей между данными, содержащимися в контенте, публикуемом пользователями и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности, как основы для построения профиля уязвимостей, а также развитии существующего подхода, учиты-

вающего профиль уязвимостей пользователя, за счёт дополнения комплекса «критичные документы — информационная система — пользователь» моделью злоумышленника.

Достижение этой цели позволит автоматизированно строить оценки защищённости пользователей информационных систем от социоинженерных атак на основании агрегации информации из социальных сетей. Таким образом, необходимо будет затрачивать существенно меньшее время на ввод информации о системе для построения оценок защищённости пользователей. Для достижения этой цели необходимо решить ряд задач. В частности, для того чтобы агрегировать информацию из социальных сетей, необходимо автоматизированно осуществить там поиск аккаунтов сотрудников исследуемой компании. Для анализа извлекаемой информации требуется разработать методику автоматизированного выявления и формализации связей между данными, содержащимися в контенте, публикуемом пользователями, и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности. При этом важно агрегировать как можно более полные сведения о пользователях, что достигается за счёт применения методов восстановления мета-профиля пользователя информационной системы, где под мета-профилем пользователя понимаются его анкетные данные. Анализ собираемой информации позволяет строить оценки вероятностей успеха многоходовой социоинженерной атаки и прямой с использованием разработанных моделей и формализации моделей комплекса «критичные документы — информационная система — пользователь — злоумышленник».

1.5. ВЫВОДЫ ПО ГЛАВЕ 1

В главе произведён анализ предметной области подчёркнута актуальность исследований в области информационной безопасности и со-

циоинженерных атак. Отмечена тенденция к росту статистических показателей ущерба от киберпреступлений, времени, затрачиваемого на расследование таких преступлений, и иных ресурсов. Приведены примеры наиболее ярких инцидентов, произошедших с использованием методов социальной инженерии, которые стали известны из средств массовой информации. Представлена классификация угроз информационной безопасности, виды социоинженерных атак и web-атак. Обозначены важные место и роль проблемы анализа поражения/защищённости пользователей и, косвенно, критичных документов информационных систем от социоинженерных атак с выделением используемых подходов для повышения уровня защищённости пользователей информационной системы от социоинженерных атак.

На основании изложенного, сделаны выводы об актуальности исследований в области анализа защищённости пользователей информационных систем от социоинженерных атак, приведено обоснование постановки целей и задач диссертационного исследования, направленных на повышение опертивности 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.

Глава 2. ЭЛЕМЕНТЫ ПОДХОДОВ К АНАЛИЗУ ЗАЩИЩЁННОСТИ

Во второй главе рассмотрены результаты исследований, которые стали заделом для решения ряда задач, поставленных в настоящем диссертационном исследовании. Представлен подход к оценке информации в интересах рефлексивного управления, предложенные В.Ю. Осиповым [163]. 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. Представлены модели комплекса «информационная система — персонал — критичные документы» (по дис. А.А. Азарова [97]), на основании которых строились оценки поражаемости/защищённости пользователей и критичных документов информационной системы от социоинженерных атак.

2.1. ПОДХОД К ОЦЕНКЕ ИНФОРМАЦИИ В ИНТЕРЕСАХ РЕФЛЕКСИВНОГО УПРАВЛЕНИЯ КОНКУРЕНТАМИ

С понятием социальной инженерии тесно связаны понятия корпоративного (промышленного) шпионажа, конкурентной разведки и рефлексивного управления. В разных источниках предлагаются разные соотношения этих терминов [137, 163, 169]. Конкурентная разведка — сбор, обработка и анализ информации из различных источников, которая позволяет вырабатывать управленческие решения для повышения конкурентоспособности организации, проводимые без нарушения закона и с соблюдением этических норм [216]. Согласно [137], промышленный шпионаж — это форма недобросовестной конкурентной разведки. Иными словами, цели у конкурентной разведки и промышленного шпионажа совпадают и

заключаются в добывании и дальнейшем использовании коммерческой или служебной тайны, но различаются по форме. В основе конкурентной разведки лежит соблюдение этических и законодательных норм, тогда как при осуществлении промышленного шпионажа это не является обязательным [137].

Под рефлексивным управлением понимается процесс передачи оснований для принятия решений одним из противников другому [154, 163]. Таким образом, промышленный и корпоративный шпионаж нацелены на добывание информации, а рефлексивное управление сосредоточено на попытке заставить действовать определённым образом противника. В этом смысле понятие рефлексивного управления соприкасается с понятием социоинженерной атаки, но последнее шире и заключает в себе «совокупность прикладных психологических и аналитических приёмов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности» [109]. Для иллюстрации различий между этими терминами приведём простейшим пример социоинженерной атаки, который нельзя классифицировать как рефлексивное управление. Таким примером может быть такой вид атаки как плечевой серфинг, когда злоумышленник подглядывает через плечо жертвы конфиденциальную информацию.

Отметим модель ценности информации с точки зрения рефлексивного управления, предложенной в [163, 164], в соответствии с которой ценность информации S выражается как

$$S = \max_{j \in J} \min_{i \in I} \left\{ W_{2j} - W_{1i} - \sum_{r=1}^{N} a_r \left(C_{2.1rj} - C_{1ri} \right) - \sum_{r=1}^{N} a_r C_{2.2rj} \right\},$$

где W_{1i}, W_{2j} — конечные эффекты, получаемые конкурентом (далее потребителем), при отсутствии оцениваемой информации и при её наличии соответственно, I, J — совокупность способов достижения указанных эффектов соответственно при отсутствии оцениваемой информации и при

её наличии, C_{1ri}, C_{2rj} — затраты ресурса r конкурента для получения эффектов W_{1i}, W_{2j} соответственно, a_r — масштабирующий множитель для преобразования расхода ресурса r конкурента к системе измерений, допускающей сопоставление размеров расхода с размером конечных эффектов, N — число видов ресурсов, которыми располагает конкурент [163].

2.2. ПОДХОД К АНАЛИЗУ ЗАЩИЩЁННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ, ОСНОВАННЫЙ НА ОБРАБОТКЕ ДЕРЕВЬЕВ АТАК

В работах [142, 146] имитация и перебор возможных траекторий атак злоумышленника в форме деревьев атак стали основой подхода к анализу защищённости компьютерных сетей. Анализ защищённости опирается на модель анализируемой системы, которая основана на конфигурации и политике безопасности системы, внешних баз данных уязвимостей, данных о реальной системе, модели нарушителя и требованиях [141, 147]. При выполнении анализа, в первую очередь, генерируются графы допустимых траекторий атак. Исследования получившегося пространства траекторий позволяет идентифицировать «слабые места» распределённой киберфизической системы (компьютерной сети, компьютерной системы и т.п.), её уязвимости. На основе агрегации полученных сведений вычисляется оценка уровня защищённости киберфизической системы. Вычисления базируются на метриках безопасности [141, 147]. Помимо этого, система представляет рекомендации по усилению защищённости [141, 142, 146, 147]. В работе [208–210] предложено улучшение моделей и методик анализа защищённости компьютерных сетей на основании деревьев атак с учётом требования оперативности, которое позволяет сократить затраты времени на построение и анализ деревьев атак.

Исследования, описанные в работах [142, 146, 208–210], инспирировали научные изыскания в области автоматизации оценок защищённости

пользователей информационных систем от социоинженерных атак злоумышленника. По аналогии с предложенными в указанных работах подходами отправной точкой анализа является имитация социоинженерных атак, в результате которой получается совокупность допустимых графов атак злоумышленника на пользователя. Оценки степени защищённости пользователя вычисляются за счёт применения адаптированных метрик к полученной совокупности графов атак.

2.3. КОМПЛЕКС МОДЕЛЕЙ «КРИТИЧНЫЕ ДОКУМЕНТЫ – ИНФОРМАЦИОННАЯ СИСТЕМА – ПЕРСОНАЛ»

В работе [97] были рассмотрены некоторые модели, входящие в комплекс «критичные документы – информационная система – персонал». Часть этих моделей в совокупности с новыми используется для построения оценок защищённости пользователей информационных систем и поражаемости критичных документов в данном диссертационном исследовании. Информационная система в [97] представляет собой набор программно-технических устройств, таких как персональные компьютеры, периферийные устройства, сетевые кабели, адаптеры и иное оборудование. Каждое из этих устройств может быть ассоциировано с некоторыми информационными объектами разной степени критичности. В качестве информационных объектов в системе рассматриваются критичные документы. Модель критичных документов включает в себя компонент, связанный с хостами, с которых он доступен, и компонент, содержащий оценку его критичности, основанную оценке максимального уровня ущерба для компании при его компрометации. Формализация комплекса «критичные документы – информационная система – персонал» в [97] представляется в виде тройки (U,H,I), где U — пользователи информационной системы, H — хосты, а I — критичные документы, доступные с хостов информационной системы [97].

Автоматизированная информационная система включает в себя пользователей, которые обладают рядом характеристик, существенных для предпринимаемого исследования. В частности, среди этих характеристик можно выделить права доступа к критичным документам, некоторые индивидуальные особенности пользователя, влияющие на его действия в ответ на атакующие действия злоумышленника. В отличие от анализа защищённости программно-технической составляющей информационных систем, не учитывающего уязвимости пользователей, анализ защищённости пользователей от социоинженерных атак обладает рядом особенностей. Эти особенности связаны, с одной стороны, с недетерменированностью реакции на атакующие воздействия, с другой стороны с потенциальной неисчерпаемостью как особенностей и действий пользователей, так и перечнем компетенций злоумышленника. При программно-технической атаке, направленной на определённую уязвимость, существует узкий набор возможных ответных реакций системы, причём ответные реакции технической системы детерминированы: в одних и тех же условиях при одних и тех же объектах на одно и то же воздействие будет получен один и тот набор реакций. В случае с пользователем этот набор шире и многообразнее, а главное — реакции пользователя недетерминированы (но это не означает, что они абсолютно произвольны). Для оценки этих реакций и их возможных последствий был введен в рассмотрение профиль уязвимостей пользователей. В подходе, которого придерживаемся в диссертации, профиль уязвимостей пользователя представляется как набор пар уязвимость – выраженность уязвимости [195, 198].

Профиль уязвимостей пользователя не наблюдается непосредственно. Фрагменты профиля уязвимостей пользователя или сам профиль уязвимостей пользователя приходится строить по косвенной информации. Например [97], установлены связи между параметрами фрагмента профиля уязвимостей пользователя и степенью выраженность его

психологических особенностей (следует оговориться, что речь идёт о математической модели профиля уязвимостей пользователя, математической модели фрагмента профиля уязвимостей пользователя, математической модели психологических особенностей пользователя). Представляется правдоподобным, что, чем больше число (в определённых границах и с определёнными предположениями) источников косвенной информации удаётся использовать, тем лучше оказывается математическая модель профиля уязвимостей пользователя с точки зрения оценки вероятностей его реакций. Отметим, что в упомянутой модели [97] для оценки степени выраженности психологических особенностей пользователя с целью дальнейшего построения фрагмента профиля уязвимостей необходимо участие эксперта. Профиль уязвимостей пользователя представляет собой набор пар уязвимость — выраженность уязвимости и формализуется как $((R_1,D(R_1)),...,(R_k,D(R_k)))$, где $D(R_i)$ — степень выраженности уязвимости R_i пользователя [97].

На основе данной формализации в [97] предлагается модель оценки вероятности успеха социоинженерного атакующего воздействия злоумышленника на i-ую уязвимость пользователя j: $p_{ij} = 1 + \frac{1}{\ln\left(\frac{e^{D_j(R_i)}}{e^{M_i}}\right)}$, если $D_j < M_i$, где M_i — это максимальная степень выраженности i-ой уязвимости пользователя. По мнению автора, если $D_j = M_i$, то $p_{ij} = 1$. Отметим, что, весьма вероятно, формула содержит опечатку: это мнение обусловлено рассмотрением случая, когда $D_j(R_i) = 0$. В этом случае вероятность может получиться больше 1.

В [97] также представлена модель для расчёта оценки вероятности успеха социоинженерной атаки злоумышленника в социальном графе от пользователя m до пользователя j через пользователей i_k, которая выглядит следующим образом:

$$\tilde{P}_{m-\ldots-i_k-\ldots-j} = P_m \prod_{k=1}^{n-1} P_{i_k,i_{k+1}},$$

где $i_1 = m$, $i_n = j$, P_i — вероятность успеха атаки злоумышленника на пользователя i, $P_{i_k,i_{k+1}}$ — вероятность достижения i_{k+1}-ого пользователя злоумышленником через пользователя i_k. В модели используются экспертные оценки для вероятности успеха распространения социоинженерной атаки от пользователя к пользователю.

В работе [97] также представлена реализация моделей и алгоритмов в программных модулях системы автоматизированного анализа защищённости пользователей информационных систем от социоинженерных атак на языке C#.

В то же время в представленном подходе не учитывается специфика модели злоумышленника (ресурсы, которые ему доступны, степени владения определёнными атакующими действиями, начальные знания о системе). При этом «…важность изучения особенностей двух сторон взаимодействия – того, кто влияет, и того, на кого влияют, — подчеркивается в научной литературе. Известный специалист в области психологии влияния Роберт Чалдини в своей монографии [207] отмечал, что изучать психологию уступчивости он начал с серии экспериментов, позволяющих выяснить, какие принципы и особенности лежат в основе податливости в отношении просьб или требований, но вскоре понял, что нужно изучать и вторую сторону данного процесса» [81]. В своей работе он называет «профессионалами уступчивости» тех лиц, что способны склонить других к выполнению тех или иных просьб. По его мнению, такие люди знают, «как построить взаимодействие, чтобы собеседник уступил и выполнил просьбу или требование, понимают, как приёмы работают, а какие нет. Такие люди стараются, во что бы то ни стало, заставить окружающих пойти на уступки» [81]. При более глубоком рассмотрении вопроса в [207] были выделены существенные для дальнейшего изложения в диссертации аспекты: «люди, которые не знают, как вынудить других сказать “да”,

обычно терпят поражение; те же, кто знают, — процветают [207]. Р. Чалдини в результате своих наблюдений выводит шесть основных принципов влияния: принцип последовательности, принцип взаимного обмена, принцип социального доказательства, принцип авторитета, принцип благорасположения, принцип дефицита. Однако, в число главных принципов не было включено правило “личного материального интереса”, которое автор рассматривает как “некоторую аксиому, которая заслуживает признания, но не подробного описания”».

2.4. ВЫВОДЫ ПО ГЛАВЕ 2

В главе были рассмотрены результаты исследований, которые стали заделом для решения ряда задач, поставленных в настоящем диссертационном исследовании. Был представлен подход к оценке информации в интересах рефлексивного управления. Приведены термины, ассоциированные так или иначе с термином социальной инженерии, такие как корпоративный шпионаж, конкурентная разведка. Проведены границы между ними. Продемонстрировано, что промышленный и корпоративный шпионаж нацелены на добывание информации, а рефлексивное управление сосредоточено на попытке заставить действовать определённым образом противника. В этом смысле понятие рефлексивного управления соприкасается с понятием социоинженерной атаки, но последнее шире. Представлен подход к анализу защищённости компьютерных сетей от программно-технических атак, основанный на анализе деревьев атак, а также его оптимизация. Приведены компоненты комплекса «информационная система — персонал — критичные документы», которые использовались для моделирования и оценок защищённости пользователей информационной системы от социоинженерных атак. Отмечено, что в представленном подходе не учитывается ряд существенных факторов, влия-

ющих на оценку защищённости, например, специфика модели злоумышленника (ресурсы, которые ему доступны, степени владения определёнными атакующими действиями, начальные знания о системе).

Глава 3. РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ ОЦЕНКИ ПОРАЖАЕМОСТИ И ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК: ПАРАМЕТРЫ И УРАВНЕНИЯ

В третьей главе рассмотрены модели комплекса «критичные документы — информационная система — пользователь — злоумышленник». Предложены модели и методы для оценки вероятности успеха прямой социоинженерной атаки злоумышленника на пользователя, основанные на моделях профиля компетенций злоумышленника и профиля уязвимостей пользователя, оценки вероятности поражения критичных документов, для учёта ограниченности ресурсов злоумышленника в оценках, оценки вероятности успеха многоходовой социоинженерной атаки. Представлены методы и алгоритмы сбора и обработки сведений, извлекаемых из социальных сетей для оценки параметров модели пользователя и межпользовательских связях. Для этого представлено решение задачи автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, дальнейшая работа с найденными аккаунтами, которая заключается в восстановлении фрагментов мета-профилей пользователей на основании альтернативных источников информации; оценке степени выраженности некоторых особенностей пользователей, основанных на данных, извлекаемых из аудио- и текстового контента, публикуемого в их аккаунтах в социальной сети; оценке вероятности успеха прохождения социоинженерной атаки по одной связи от пользователя к пользователю и модель оценки вероятности успеха многоходовой социоинженерной атаки.

3.1. ИЗМЕРЯЕМЫЕ ПОКАЗАТЕЛИ

Общая цель исследования заключается в автоматизированном построении оценок защищённости пользователей информационных систем от социоинженерных атак и разработке систем упреждающей диагностики

уязвимостей пользователей. В диссертационной работе рассматриваются оценки защищённости (поражаемости) пользователей (опосредованно — критичных документов) информационных систем; причём вероятность поражения пользователя или вероятность поражения документа рассматривается как «вероятность сложного события», которую надо вычислить или оценить на основе сведений о вероятностях других событий, предполагающихся известными. При этом рассматриваются оценки вероятности успеха как прямых социоинженерных атак злоумышленника на пользователя, так и многоходовых, опосредованных, через цепочку пользователей. Также в работе предлагаются оценки вероятности поражения критичных документов, учитывающие агрегацию разных параметров, таких как ограниченность ресурсов злоумышленника, его профиль компетенций, профиль уязвимостей пользователя.

Данные показатели связаны с анализом защищённости информации, который регламентируется, в частности, следующими стандартами: ГОСТ Р 50922—2006 «Защита информации. Основные термины и определения» [122], ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» [119–121], ISO/IEC 17799 «Information technology – Security techniques – Code of practice for information security management» [35].

Регламентирующие документы [119–121] содержат требования и термины, относящиеся к объектам оценки, которые определяется как набор программных, программно-аппаратных и/или аппаратных средств, возможно сопровождаемых руководствами. Таким образом, ими затрагиваются программно-технические аспекты защиты информации.

Защита информации предполагает «деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию» [122]. При этом различаются правовая, техническая, криптографическая

и физическая защита информации по используемым методам. Защита пользователей информационных систем от социоинженерных атак связана с технической и физической защитой информации. При этом критичные документы и пользователи (сотрудники компании) как носители информации являются объектами защиты.

Злоумышленник в данном исследовании рассматривается как источник угрозы безопасности информации, а социоинженерная атака как угроза безопасности информации. Анализ защищённости пользователей информационной системы от социоинженерных атак представляет собой вид аудиторской проверки информационной безопасности в организации [122].

3.2. ПОДХОД, МЕТОДЫ И МОДЕЛИ ОЦЕНКИ ЗАЩИЩЁННОСТИ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК

Для оценки защищённости пользователей информационной системы необходимо учитывать ряд объектов и связей между ними, таких как критичные документы с уровнями их критичности для компании; хосты, с которых они доступны; связи между хостами, пользователи, имеющие доступ к определённым хостам и критичным документам, характеризующиеся профилями уязвимостей, доступами к хостам и документам, допусками в определённые контролируемые зоны, связями с другими пользователями; злоумышленники, характеризующиеся профилями компетенций, ресурсами, которые им доступны, начальными знаниями о системе, целями, точками входа в систему, связями с другими злоумышленниками. Перечисленные и иные сущности связаны с оценкой защищённости пользователей информационных систем от социоинженерных атак, рассмотрим их подробнее.

Сформулируем достаточно общие алгебраические модели для представления параметров, которые должны учитываться при построении

оценок защищённости пользователей информационных систем от социо-инженерных атак и оценок вероятности поражения критичных документов. Отметим, что модели критичных документов и хостов информационной системы подробно рассматривались в задачах защиты информации от программно-технических атак [152, 188, 208]. В рамках данного диссертационного исследования приведём адаптированные к тематике социо-инженерных атак модели указанных сущностей.

Модель критичных документов включает в себя ряд компонент, которые связаны с уровнем критичности для компании, расположением на хостах и доступом к документу с них, уровнем доступа пользователей к документу. Уровень критичности документа может выражаться в размере убытков для компании в случае его компрометации, выраженном финансово, репутационных издержках, иной шкале. В качестве одного из вариантов предлагается использовать систему уровней критичности документов, наиболее критичные документы будут относиться к первой группе, менее критичные ко второй и т.д. Документ может быть доступен с разных хостов, иметь разные уровни доступа с них (с одного хоста доступ только для чтения, с другого для чтения и редактирования). Разные пользователи могут также иметь разные уровни доступа к критичному документу. С учётом изложенного формальная модель критичного документа в комплексе 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 данный документ 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 включает в себя компоненты, связанные с приложениями, программным обеспечением, уста-

новленными на хосте, связями между хостами в информационной системе, пользователями, которые имеют доступ к хосту определённого уровня (доступ к инсталляции или удалению программного обеспечения, конфигурированию системы и т.п.), критичными документами, доступными с хоста. Хосты могут также иметь уровень критичности, связанный с критичностью доступных с него документов. Формализация модели хоста информационной системы, включающая описанные сущности, 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 $\left\{ \text{Soft}_j^i \right\}_{j=1}^{n}$ — программное обеспечение, установленное на хосте, $\left\{ \text{CD}_t^i \right\}_{t=1}^{r}$ — критичные документы, доступные с хоста, $\left\{ \text{Conn}_k^i \right\}_{k=1}^{m}$ — связи хоста с другими хостами информационной системы, $\left\{ \left(U_l^i; \text{LAH}_l^i \right) \right\}_{l=1}^{q}$ — пользователи с уровнями доступа к хосту, Lc^i — уровень критичности хоста, который может быть связан с критичностью доступных с него документов.

Модель пользователя информационной системы ассоциирована с профилем уязвимостей пользователя, представляющего собой набор пар уязвимость – выраженность уязвимости, уровнем доступа пользователя к хостам информационной системы, критичным документам, связями пользователей между собой, контролируемыми зонами, в которые пользователь имеет доступ, внутренним состоянием пользователя, которое может зависеть от ряда окружающих факторов (конфликт с начальством, ухудшение отношений в семье и прочее). Таким образом, она может быть формализована как $U_i = \left(\left\{ \left(V_j, D_i(V_j) \right) \right\}_{j=1}^{n}; \left\{ \left(\text{AH}_l^i; \text{LAH}_l^i \right) \right\}_{l=1}^{m}; \left\{ \left(\text{AD}_k^i; \text{LAD}_k^i \right) \right\}_{k=1}^{q}; \left\{ \text{Comm}_t^i \right\}_{t=1}^{r}; \left\{ \text{CA}_a^i \right\}_{a=1}^{b}; \text{State}^i \right)$, где $\left\{ \left(V_j, D_i(V_j) \right) \right\}_{j=1}^{m}$ — профиль уязвимостей пользователя, в котором V_j — уязвимость пользователя, а $D_i(V_j)$ — выраженность уязвимости V_j,

$\left\{\left(\mathrm{AH}_l^i;\mathrm{LAH}_l^i\right)\right\}_{l=1}^m$ — хосты с уровнем доступа к ним, $\left\{\left(\mathrm{AD}_k^i;\mathrm{LAD}_k^i\right)\right\}_{k=1}^q$ — документы с уровнем доступа к ним, $\left\{\mathrm{Comm}_t^i\right\}_{t=1}^r$ — тип взаимоотношений пользователя с другими пользователями информационной системы, $\left\{\mathrm{CA}_a^i\right\}_{a=1}^b$ — контролируемые зоны, в которые пользователь имеет доступ, State^i — внутреннее состояние пользователя, которое может влиять на его ответные действия при социоинженерном атакующем воздействии.

Модель злоумышленника включает в себя компоненты, связанные с профилем компетенций злоумышленника, который представляет собой набор пар вид атакующего действия и умение злоумышленника использовать этот вид атакующего действия, ресурсы доступные злоумышленнику, такие, например, как время или деньги, начальные знания злоумышленника о системе, цель, преследуемая злоумышленником, например, получение доступа к определённому критичному документу, некоторое действие пользователя, выход на определённого пользователя. Также злоумышленник может действовать не один, а в группе, соответственно в модель включены его связи с другими злоумышленниками. Формализация может быть представлена следующим образом

$$M_i = \left(\left\{\left(R_j, Q_i\left(R_j\right)\right)\right\}_{j=1}^n; \left\{\left(A_k, S_i\left(A_k\right)\right)\right\}_{k=1}^m; \left\{\mathrm{BK}_l^i\right\}_{l=1}^q; G^i; \left\{\mathrm{Comm}_t^i\right\}_{t=1}^r\right), \quad \text{где}$$

$\left\{\left(R_j, Q_i\left(R_j\right)\right)\right\}_{j=1}^n$ — 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) [81], $\left\{\mathrm{BK}_i\right\}_{i=1}^l$ — 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.

Вероятно, в контексте более широких исследований, связанных с анализом защищённости пользователей информационных систем от социоинженерных атак, модели будут дополнены новыми компонентами, оказывающими влияние на оценки защищённости пользователей информационной системы и оценки вероятностей поражения критичных документов. В диссертационной работе рассматриваются адаптированные к решаемым задачам модели описанных выше сущностей, чтобы избежать решения ряда вопросов, которые уже были исследованы в более ранних работах [97, 152, 188, 208].

Отметим также, что оценки защищённости/поражаемости пользователей могут меняться с течением времени. Например, если для сотрудников в компании был проведён тренинг по информационной безопасности, в рамках которого освещались вопросы потенциальных угроз, связанных с социоинженерными атаками, и методов противодействия им, то после него вероятность успеха атаки злоумышленника будет ниже. Пусть $p(0)$ — вероятность успеха социоинженерной атаки злоумышленника на пользователя сразу после проведения тренинга. Обозначим её $p_0 = p(0)$. Отметим, что $p_0 \in [0;1]$. Тогда можно ожидать, что с течением времени вероятность того, что пользователь окажется непораженным в результате атаки злоумышленника, будет меняться в силу постепенной утраты настороженности, забывания знаний, умений и навыков. Вопросы, связанные с убыванием эффекта обучения/прохождения повышения квалификации, рассмотрены в [155]. Если опереться на модель, что в течении заданного промежутка времени вероятность остаться защищенным убы-

вает с некоторой фиксированной долей α от текущего уровня такой вероятности, можно составить дифференциальное уравнение $\frac{dp}{dt} = -\alpha p$ при начальном условии $p(0) = p_0$. Вычислим p:

$$\frac{dp}{p} = -\alpha dt; \int \frac{dp}{p} = \int -\alpha dt; \ln p = -\alpha t + C; p = Ke^{-\alpha t}; p_0 = K; p = p_0 e^{-\alpha t}.$$

В диссертационной работе вопросы изменения вероятности успеха социоинженерной атаки злоумышленника на пользователя с течением времени не рассматриваются, поскольку сделан фокус на экспресс-оценке защищённости/поражаемости в некотором временном срезе — в некоторый заданный момент или в некоторый настолько короткий промежуток времени, что вероятности защищенности/поражаемости можно предположить постоянными.

3.2.1. Вероятностная модель оценки успеха социоинженерной атаки злоумышленника на пользователя, учитывающие профиль уязвимостей пользователя и профиль компетенций злоумышленника

Для построения оценок защищённости пользователей информационных систем от социоинженерных атак, оценок вероятности поражения критичных документов, вероятности успеха социоинженерной атаки необходимо разработать модель для оценки успеха прямой социоинженерной атаки злоумышленника на пользователя. При этом будем предполагать, что злоумышленник обладает бесконечным ресурсом (вопрос учёта ограниченности доступных злоумышленнику ресурсов будет рассмотрен ниже), не имеет начальных знаний о пользователях системы, его цель совпадает с атакуемым пользователем и он характеризуется некоторым профилем компетенций. Для оценки успеха прямой социоинженерной атаки злоумышленника на пользователя, которая будет учитывать модели профиля компетенций злоумышленника и профиля уязвимостей пользователя, введём соответствующие реляционные модели профиля

уязвимостей, профиля компетенций злоумышленника и их взаимосвязи (таблица 1).

Таблица 1 — Модели профиля уязвимостей пользователя и профиля компетенций злоумышленника

№	Название	Представление	Комментарии
1	Уязвимости пользователя	$\text{vulnerability}(\text{id},\text{name})$	Перечень уязвимостей пользователя с идентификационными номерами и наименованиями
2	Профиль уязвимостей пользователя	$\text{pv}(\text{user\_id},\text{v\_id},\text{dv})$	Связь пользователя с его профилем уязвимостей (с набором пар уязвимость – выраженность уязвимости).
3	Компетенции злоумышленника	$\text{attacks}(\text{id},\text{name})$	Перечень видов атакующих действий злоумышленника
4	Профиль компетенций злоумышленника	$\text{pc}(\text{attacker\_id},\text{a\_id},\text{sa})$	Сопоставленный злоумышленнику профиль компетенций злоумышленника.
5	Связь между видами атакующих действий и уязвимостями пользователя	$\text{pv\_pc}(\text{v\_id},\text{a\_id},\text{force})$	Уровень влияния с помощью определённого атакующего воздействия на определённую уязвимость пользователя.

Более подробно рассмотрим профиль компетенций злоумышленника. Он может быть охарактеризован степенью умения злоумышленника использовать определённые типы социоинженерных атакующих воздействий. Иначе говоря, профиль компетенций злоумышленника включает в себя виды социоинженерных атакующих воздействий и умение осуществлять эти воздействия [81].

Опираясь на опыт исследований аппаратных и программно-технических аспектов информационной безопасности и адаптируя его к области

социоинженерных атак, можно ожидать, что для построения и регулярного последующего пополнения списков атакующих воздействий, ресурсов и прочих параметров, входящих в модель злоумышленника, а также подходов к их оценке потребуется отдельное и непрерывно длящееся междисциплинарное исследование при участии специалистов по психологии, социологии, информатике и математике [197]. Чем полнее будут данные списки, тем более точные оценки можно получить. В предположении, что некая версия списков доступна, например, как в работе [197], продолжим дальнейшее развитие концепции.

Так, профиль компетенций злоумышленника может быть представлен в виде $((A_1,S(A_1)),...,(A_q,S(A_q)))$, где A_i — это вид социоинженерного атакующего воздействия, а $S(A_i)$ — степень владения злоумышленником данным атакующим воздействием [81]. Степень владения атакующим воздействием — это один из факторов, влияющих на оценку успешности атаки, выражающий некоторое умение злоумышленника [81].

При имитации социоинженерных атакующих воздействий, исходящих от злоумышленника, обладающего разными компетенциями, на пользователя, обладающего разными степенями выраженности уязвимостей, могут быть получены различные вероятностные оценки успеха социоинженерных атакующих воздействий. Успех социоинженерного атакующего воздействия злоумышленника будет определяться степенью владения им различными социоинженерными атакующими воздействиями и степенью выраженности уязвимостей атакуемого пользователя информационной системы. Отражающая указанное предположение модель оценки вероятности успеха социоинженерного атакующего воздействия с помощью определённого атакующего воздействия при заданном профиле компетенций злоумышленника и профиле уязвимостей пользователя может быть представлена в виде зависимости от ряда параметров

$p_{ij} = F\left(\left(A_i, S\left(A_i\right)\right), \left(V_j, D\left(V_j\right)\right), Q\right)$, где $S\left(A_i\right)$ — степень владения злоумышленником социоинженерным атакующим воздействием A_i, $D\left(V_j\right)$ — выраженность у пользователя уязвимости V_j, Q — матрица пороговых значений вероятностей (будет описана ниже), а p_{ij} — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя.

Очевидно, что $F\left(\left(A_i, S\left(A_i\right)\right), \left(V_j, D\left(V_j\right)\right), Q\right) = 0$, когда $S\left(A_i\right) = 0$ и $D\left(V_j\right) = 0$, или $S\left(A_i\right) = 0, \forall D\left(V_j\right)$, или $D\left(V_j\right) = 0, \forall S\left(A_i\right)$. При этом, если $D\left(V_j\right) \to \max$ и $S\left(A_i\right) \to \max$, то $F\left(\left(A_i, S\left(A_i\right)\right), \left(V_j, D\left(V_j\right)\right), Q\right) \to q_{ji}$. Примером такой функции может быть адаптированная триангулярная норма [104]. Отметим, однако, что не только триангулярная норма, т.к. не накладывается требования симметричности функции по аргументам. В этом отношении в дальнейших исследованиях для применения могут оказаться перспективными функции, которые используются в нечеткой логике для вычисления значений «некоммутативного» [10, 11, 99].

Ниже представлены некоторые примеры триангулярных норм, которые можно адаптировать для расчёта вероятности успеха социоинженерного атакующего воздействия злоумышленника [104].

Минимум T_M: $T_M\left(x, y\right) = \min\left(x, y\right)$;

Вероятностное произведение T_P: $T_P\left(x, y\right) = x \cdot y$;

t-норма Лукасевича T_L: $T_L\left(x, y\right) = \max\left(x + y - 1, 0\right)$;

t-норма Ягера:

$$T(x,y)=\begin{cases}\max\left(1-\left((1-x)^{\lambda}+(1-y)^{\lambda}\right)^{\frac{1}{\lambda}},0\right),\text{если } \lambda\in(0,\infty),\\ T_D(x,y),\text{если } \lambda=0,\\ T_M(x,y),\text{если } \lambda=1.\end{cases}.$$

В простейшем случае можно рассматривать задачу оценки вероятности успеха социоинженерного атакующего воздействия злоумышленника на определённую уязвимость пользователя при условии, что на одну уязвимость можно влиять с помощью одного типа воздействия. Т.е. вероятность успеха будет не нулевой только при одном варианте комбинации типа атакующего воздействия и уязвимости пользователя. Но в реальности одно и то же атакующее воздействие можно использовать для оказания влияния на разные уязвимости пользователя. Так, например, с помощью социоинженерного атакующего воздействия, заключающегося в предложении зарегистрироваться пользователю на каком-то привлекательном сайте, можно влиять на уязвимости пользователя, такие как техническая неосмотрительность, неопытность или халатность [96].

Отметим, что не на все уязвимости пользователей можно влиять с помощью всех атакующих действий злоумышленника. При этом необходимо ограничить максимально достигаемую вероятность, когда степени выраженности уязвимости пользователя и компетенций злоумышленника максимальны. Для формализации этого введём матрицу, которая будет содержать оценки вероятности успешности атаки при использовании злоумышленником определённого атакующего воздействия на определённую уязвимость пользователя. Элемент матрицы $q_{ji}=Q(j,i)$ характеризует максимальную достигаемую вероятность успеха атаки при максимальной i-ой компетенции злоумышленника и выраженности j-ой уязвимости пользователя. Рассмотрим таблицу 2, которая может служить примером задания значений матрицы Q.

В строках таблицы 2 представлены элементарные уязвимости пользователей информационных систем, в столбцах — атакующие действия злоумышленника, которые были выявлены в работе [195]. Всего было предложено пять уязвимостей: «техническая неосмотрительность», «слабый пароль», «техническая халатность и установка на получение личной выгоды», «техническая неопытность», «техническая безграмотность» [195]. Для краткости обозначим эти уязвимости V_1, V_2, V_3, V_4, V_5 соответственно. Кроме того, обозначим 7 простейших атакующих действий злоумышленника: «предложить зарегистрироваться на каком-то привлекательном сайте», «отправить письмо с “полезным” для пользователя приложением», «завязать виртуальное знакомство с пользователем в сети», «взломать», «подсмотреть», «подкупить», «предложить помощь в решении “компьютерных дел”» [195] как $A_1, A_2, A_3, A_4, A_5, A_6, A_7$.

Отметим, что атакующее воздействие, заключающееся, например, в отправке письма с «полезным» для пользователя содержанием, вероятнее всего будет иметь отклик у пользователей с сильно выраженными уязвимостями: техническая неосмотрительность, техническая неопытность и техническая безграмотность. В то же время, данное атакующее воздействие вряд ли приведёт к успеху с пользователем, у которого выше перечисленные уязвимости мало выражены, но имеет место использование слабого пароля. При этом, если у пользователя используется сильно выраженная уязвимость техническая неосмотрительность, а у злоумышленника высокая компетенция виртуального знакомства с пользователями в сети, то максимально возможная вероятность успеха социоинженерной атаки будет 0.8.

Таблица 2 — Атакующие воздействия злоумышленника и уязвимости пользователя [81]

$A_i, i =$ / $V_j, j =$	1	2	3	4	5	6	7

1	0.9	0.8	0.7	0	0	0	0
2	0	0	0	0.9	0.9	0	0
3	0.8	0	0	0	0	0.9	0
4	0.9	0.8	0.7	0	0	0	0
5	0.9	0.8	0	0	0	0	0.8

С учётом этого, приведённые примеры формул для оценки вероятности успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя примут следующий вид:

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

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

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

Также для формализации этой зависимости можно использовать параметризованную t-норму Ягера [104].

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

Отметим, что матрица Q в дальнейшем может быть заменена на более сложную функцию, которая будет учитывать расширенный круг параметров, связанных с профилем уязвимостей пользователя и профилем компетенций злоумышленника.

Таким образом, имеем оценку успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя. Но при атаке злоумышленник использует все имеющиеся у него компетенции, воздействуя на все уязвимости пользователя. Т.е. необходимо построить оценку успеха социоинженерной атаки злоумышленника на пользователя с использованием всех атакующих воздействий по отношению ко всем уязвимостям.

Если p_{ij} — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя, то $1-p_{ij}$ — 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 [18, 53]. Серия моделей, предложенных в [18, 53] позволяет увязать оценку риска с числом эпизодов рискованного поведения. 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.

3.2.2. Вероятностная модель оценки поражаемости критичных документов при социоинженерной атаке

При анализе защищённости информационных систем от социоинженерных атак важно учитывать не только оценки вероятности успеха атаки на пользователя, но и оценки вероятности доступа к критичным документам. При этом критичные документы могут иметь разные уровни критичности. В идеальном случае критичность документа лучше выразить финансово через ущерб компании при его компрометации и рассматривать поражаемость критичных документов подокументно, а на основе этих сведений рассчитать ожидаемый ущерб от социоинженерной атаки. Но этот подход не всегда представляется возможным и требует существенных ресурсов для реализации. Обычно критичные документы разделяют на группы по уровню критичности. К первой группе относятся наиболее критичные документы, к последней менее критичные. Рассмотрим три задачи, связанные с оценкой защищённости критичных документов, накладывающих определённые ограничения на модели. Отметим, что решение каждой задачи полезно, позволяет оценить поражаемость критичных документов, исходя из сложившихся требований. При решении задач будем считать, что если злоумышленник успешно атаковал пользователя, то он получил доступ к критичным документам, к которым пользователь имеет доступ.

Первая задача заключается в расчёте оценки вероятности поражаемости 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. В этом случае модели критичных документов и пользователя информационной системы с учётом ранее предложенных моделей в таблице 1 могут быть представлены следующим образом (таблица 3).

Таблица 3 — Модели пользователя и критичных документов

№	Название	Представление	Комментарий
1	Критичный документ	cd(id,lc)	Критичные документ характеризуется идентификационным номером и уровнем критичности.
2	Пользователь	users(id,lc)	Пользователь в системе имеет идентификационный номер, через который связан с другими атрибутами, и уровень доступа к критичным документам.

Для решения поставленной задачи предлагается использовать модель Белла–Тревино [18], описанную выше. 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.

Таким образом, имеем формулу для оценки вероятности того, что критичные документы уровня критичности r будут поражены, 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. При этом часто пользователи имеют доступ не только к документам какого-то одного уровня критичности, но и к документам уровня критичности ниже. Т.е. важно решить вторую задачу, связанную с оценкой поражаемости документов, которая заключается в расчёте оценки вероятности поражаемости 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.

Формула расчёта оценки вероятности поражаемости критичных документов первого (наивысшего) уровня критичности будет в этой задаче совпадать с формулой расчёта этой оценки в предыдущей задаче, поскольку к таким документам будут иметь доступ только пользователи этого уровня. Т.е.

$$H_1 = 1 - \prod_{k \in K_1} (1 - P_k),$$

где K_1 — множество пользователей, которые имеют доступ к документам первого уровня критичности, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, H_1 — оценка вероятности того, что критичные документы первого уровня критичности будут поражены. К критичным документам уровня ниже будут иметь доступ пользователи из первой группы, плюс пользователи, имеющие доступ непосредственно к этой группе и т.д. Таким образом, расчёт оценки вероятности поражаемости 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 уровня ниже, будет производиться следующим образом

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

где K_{r+1} — множество пользователей, которые имеют доступ к документам уровня критичности $r+1$, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, H_{r+1} — оценка вероятности того, что критичные документы уровня критичности $r+1$ будут поражены.

Моделирование распределения по уровням доступа может быть и иное. Например, когда пользователи имеют доступ не ко всем документам определённого уровня критичности, а только к части из них. Т.е. необходимо решить третью задачу, связанную с оценкой вероятности поражения критичных документов, которая 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. В этом случае можно рассчитывать оценки вероятности поражения каждого критичного документа, относящегося к определённому уровню критичности, а после агрегировать эти оценки. Но такой подход требует большого количества вычислительных и иных ресурсов. Предлагается разбить документы каждого уровня критичности на группы по количеству пользователей, имеющих к ним доступ. В результате на каждом уровне критичности будем иметь некоторое число документов n_m, к которым имеет доступ m пользователей. Вероятность поражения критичного документа через одного пользователя будем считать как среднее от вероятностей поражения всех пользователей информационной системы, имеющих доступ к критичным документам определённого уровня. Т.е. пусть $\overline{p} = \frac{\sum_{k=1}^{c} P_k}{c}$, где P_k — оценка вероятности того, что пользователь k будет успешно атакован злоумышленником, c — общее количество пользователей информационной системы, имеющих доступ к критичным документам определённого

уровня. Для оценки вероятности успеха поражения критичных документов определённого уровня критичности, к которым имеют доступ m пользователей, используем модель Белла–Тревино [18]. Таким образом, оценка вероятности поражения критичных документов, к которым имеют доступ m пользователей, будет выражаться как $n_m\left(1-\left(1-\bar{p}\right)^m\right)$, где $\bar{p}$ — вероятность поражения критичного документа через одного пользователя, n_m — количество документов, к которым имеют доступ m пользователей. На основании этого, расчёт оценки вероятности поражения критичного документа уровня r 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 — количество 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.

Предложены решения задачи оценки вероятности поражения критичных документов определённого уровня критичности с учётом разных принципов распределения доступа пользователей к ним. Решение задач предлагалось, исходя из предположения о том, что успех социоинженерного атакующего воздействия на пользователя означает компрометацию критичных документов, к которым он имеет доступ. Но вообще говоря, это не всегда так. Налаживание контакта с пользователем информационной системы не всегда гарантирует компрометацию критичных документов, доступных ему. Иными словами, получение доступа к критичному документу, к которому имеет доступ успешно атакованный пользователь информационной системы, носит вероятностный характер. Т.е. существует некоторая вероятность p получения доступа к критичному документу, к

которому имеет доступ успешно атакованный пользователь информационной системы. В этом случае оценка вероятности поражаемости 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 будет следующая

$$H_r = \left(1 - \prod_{k \in K_r} (1 - P_k)\right) p,$$

где K_r — множество пользователей, которые имеют доступ к документам уровня критичности r, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, 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.

Оценка вероятности поражаемости критичных 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 уровня ниже будет следующая

$$H_{r+1} = \left(1 - (1 - H_r) \prod_{k \in K_{r+1}} (1 - P_k)\right) p,$$

где K_{r+1} — множество пользователей, которые имеют доступ к документам уровня критичности $r + 1$, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, p — вероятность получения доступа к критичному документу, к которому имеет доступ успешно атакованный пользователь информационной системы, H_{r+1} — оценка вероятности того, что критичные документы уровня критичности $r + 1$ будут поражены.

Оценка вероятности поражения критичного документа определённого уровня критичности в случае, когда критичные документы разбиты

по уровням критичности, а пользователи имеют доступ к определённому количеству критичных документов каждого уровня критичности будет следующая

$$h_r = \frac{\sum_m n_m^r \left(1-\left(1-\overline{p}\right)^m\right)}{\sum_m n_m^r} p\,,$$

где n_m^r — количество критичных документов уровня критичности r, к которым имеют доступ m пользователей, $\overline{p}$ — вероятность поражения критичного документа через одного пользователя, p — вероятность получения доступа к критичному документу, к которому имеет доступ успешно атакованный пользователь информационной системы, h_r — оценка вероятности поражения критичного документа уровня критичности r.

Представляется правдоподобным предположение, что чем выше уровень критичности документа, тем меньше вероятность его компрометации при успешной социоинженерной атаке злоумышленника на пользователя, который имеет к нему доступ. Т.е. вероятность получения доступа к критичному документу, к которому имеет доступ успешно атакованный пользователь информационной системы, зависит от уровня критичности документа. Пусть p_r — вероятность получения доступа к критичному документу уровня r, к которому имеет доступ успешно атакованный пользователь информационной системы. Тогда формулы для задач расчёта оценки вероятности поражения критичных документов определённого уровня критичности будут следующими

$$H_r = \left(1-\prod\nolimits_{k\in K_r}\left(1-P_k\right)\right)p_r\,,$$

$$H_{r+1} = \left(1-\left(1-H_r\right)\prod\nolimits_{k\in K_{r+1}}\left(1-P_k\right)\right)p_r\,,$$

$$h_r = \frac{\sum_m n_m^r \left(1-\left(1-\overline{p}\right)^m\right)}{\sum_m n_m^r} p_r\,,$$

p_r — вероятность получения доступа к критичному документу уровня r. Например, для документов, относящихся к критичным документам высокого уровня критичности, p_r может равняться 0, наоборот для документов низкого уровня критичности — близко к 1 или 1.

Вообще говоря, еще одним правдоподобным предположением является то, что вероятность получения доступа к критичным документам зависит не только от их уровня критичности, но и степени выраженности уязвимостей пользователя, через которого осуществляется попытка получения доступа, а также соответствующих компетенций злоумышленника. Разные пользователи с разными степенями выраженности уязвимостей будут по-разному реагировать на социоинженерные атакующие воздействия злоумышленника в зависимости от его компетенций и степени критичности документа, к которому совершается попытка получения доступа. Т.е.

$$p_r^k = G\left(\left(A_i, S\left(A_i\right)\right), \left(V_j, D_k\left(V_j\right)\right), r\right),$$

где $S\left(A_i\right)$ — степень владения злоумышленником социоинженерным атакующим воздействием A_i, $D_k\left(V_j\right)$ — выраженность у пользователя k уязвимости V_j, причём $k \in K_r$, K_r — множество пользователей, имеющих доступ к документов уровня критичности r, а p_r^k — оценка вероятности поражения критичных документов уровня r через успешно атакованного k-ого пользователя, имеющего доступа к этим документам.

В этом случае оценка вероятности поражаемости 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 будет следующая

$$H_r = 1 - \prod_{k \in K_r}\left(1 - P_k p_r^k\right),$$

где K_r — множество пользователей, которые имеют доступ к документам уровня критичности r, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, p_r^k — оценка вероятности поражения критичных документов уровня r через успешно атакованного k-ого пользователя, имеющего доступа к этим документам, H_r — оценка вероятности того, что критичные документы уровня критичности r будут поражены.

Оценка вероятности поражаемости критичных 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 уровня ниже будет следующая

$$H_{r+1} = 1-(1-H_r)\prod_{k\in K_{r+1}}\left(1-P_k p_{r+1}^k\right),$$

где K_{r+1} — множество пользователей, которые имеют доступ к документам уровня критичности $r+1$, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, p_{r+1}^k — оценка вероятности поражения критичных документов уровня $r+1$ через успешно атакованного k-ого пользователя, имеющего доступа к этим документам, H_{r+1} — оценка вероятности того, что критичные документы уровня критичности $r+1$ будут поражены.

Оценка вероятности поражения критичного документа определённого уровня критичности в случае, когда критичные документы разбиты по уровням критичности, а пользователи имеют доступ к определённому количеству критичных документов каждого уровня критичности будет следующая

$$h_r = \frac{\sum_m n_m^r\left(1-\left(1-\bar{p}\right)^m\right)}{\sum_m n_m^r}\bar{p}_r,$$

где n_m^r — количество 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, а $\bar{p}_r$ — оценка вероятности поражения критичных документов уровня r, которая рассчитывается как среднее от оценок вероятностей получения доступа к документам уровня критичности r пользователей, имеющих к ним доступ. Т.е. $\bar{p}_r = \frac{\sum_{k \in K_r} p_r^k}{|K_r|}$, где p_r^k — оценка вероятности того, что злоумышленник получит доступ к критичному документу уровня r, к которому имеет доступ успешно атакованный пользователь k, K_r — множество пользователей, имеющих доступ к критичным документам уровня r.

Таким образом, имеем формулы для расчёта оценок вероятностей поражения критичных документов определённого уровня критичности в трёх случаях с разными способами построить модель распределения прав доступа к критичным документам в информационной системе.

3.2.3. Вероятностная модель и основанный на ней метод оценки успеха социоинженерной атаки, учитывающие ограниченность ресурсов злоумышленника

При построении оценок вероятности поражения критичных документов и оценок вероятности успеха социоинженерной атаки злоумышленника на пользователя не учитывалось то, что злоумышленник может быть ограничен не только своими компетенциями, но и доступными ему ресурсами (например, временем или деньгами). Т.е. помимо профиля компетенций при построении оценок необходимо принимать во внимание ресурсы, доступные злоумышленнику. Введём соответствующие модели (таблица 4)

Таблица 4 — Модели профиля уязвимостей пользователя и профиля компетенций злоумышленника

№	Название	Представление	Комментарии
1	Злоумышленник	$\text{attacker}(\text{id})$	Злоумышленник имеет идентификационный номер.
2	Виды ресурсов злоумышленника	$\text{resources}(\text{id},\text{name})$	Ресурсы, которые могут быть доступны злоумышленнику.
3	Ресурсы, доступные злоумышленнику	$\text{pr}(\text{att\_id},\text{r\_id},\text{count\_r\_id})$	Набор ресурсов, сопоставленный злоумышленнику.
4	Ресурсы, необходимые для совершения атаки на пользователя	$\text{ur}(\text{user\_id},\text{r\_id},\text{count\_r\_id})$	Количество каждого ресурсов, необходимых для совершения атаки на пользователя

Задача учёта ограниченности ресурсов злоумышленника при имитации социоинженерной атаки может ставиться в нескольких формулировках. В простейшем варианте необходимо определить оценку вероятности поражения критичного документа определённого уровня критичности, с учётом того, что для совершения атаки злоумышленнику требуется определённое фиксированное количество каждого ресурса. При этом атака не будет завершена успехом ни при каких обстоятельствах, если у злоумышленника нет этого количества каждого ресурса. Но можно предположить, что в действительности количество ресурса влияет на успех социоинженерной атаки иначе.

Усложняя задачу, можно рассмотреть её при условии, что не на всю атаку требуется определённое количество ресурса и атака не может состоятся, если пороговое значение не преодолено, а на совершение каждого атакующего воздействия злоумышленника. При этом ресурс затрачивается только на атакующие воздействия на пользователя и не используется для получения доступа к критичному документу.

В усложнённом варианте данная задача может формулироваться как расчёт оценки вероятности поражения критичного документа определённого уровня критичности, с учётом того, что при совершении каждого атакующего воздействия злоумышленник затрачивает определённое фиксированное количество каждого ресурса, а также для получения доступа к критичному документу злоумышленник затрачивает фиксированное количество ресурса.

Но вообще говоря, наиболее правдоподобным представляется то, что чем выше уровень критичности документа, тем больше ресурса необходимо злоумышленнику для получения доступа к нему. Количество затрачиваемого ресурса будет также отличаться для пользователей с разными степенями выраженности уязвимостей и злоумышленников, обладающих разными компетенциями. При этом необходимо учесть, что чем большее количество каждого ресурса злоумышленник использует для совершения атаки, темы выше будет вероятность её успеха. Также, для совершения каждого атакующего воздействия злоумышленник затрачивает определённое количество ресурса.

Рассмотрим задачу построения оценки успеха социоинженерной атаки злоумышленника на пользователя с учётом того, что злоумышленником используется определённое количество одного вида ресурса на каждое атакующее воздействие. Сначала для упрощения рассмотрим модель оценки, включающую два вида атакующих воздействий злоумышленника и один вид уязвимости пользователя, а затем дадим формулировку задачи в ее более общей постановке.

В случае двух рассматриваемых атакующих действий вероятности успеха атаки с использованием злоумышленника 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 злоумыш-

ленник 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 $v_{11} > 0, v_{21} > 0$. Предположим, что общее количество затрачиваемого злоумышленником на атаку ресурса $l = w_{11} + w_{21}$. При этом $0 \le l \le L$, где L — общее количество ресурса, имеющегося у злоумышленника. При таких предположениях, вероятность успеха атаки злоумышленника на пользователя будет выражаться следующим образом $P = 1 - (1 - p_{11})^{\frac{w_{11}}{v_{11}}} (1 - p_{21})^{\frac{w_{21}}{v_{21}}} = 1 - (1 - p_{11})^{\frac{w_{11}}{v_{11}}} (1 - p_{21})^{\frac{l - w_{11}}{v_{21}}}$. Её математическое ожидание в предположении, что w_{11} распределена равномерно, будет следующим

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

$$= 1 - \frac{v_{21}(1 - p_{21})^{\frac{l}{v_{11}}} e^{\frac{\ln(1-p_{11})l}{v_{21}} - \frac{\ln(1-p_{21})l}{v_{21}}}}{l(\ln(1 - p_{11}) - \ln(1 - p_{21}))} + \frac{v_{21}(1 - p_{21})^{\frac{l}{v_{11}}}}{l(\ln(1 - p_{11}) - \ln(1 - p_{21}))}$$

Если $p_{11} = p_{21}$, то математическое ожидание будет следующим

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

$$= 1 - \frac{v_{11}v_{21}(1 - p_{11})^{\frac{l}{v_{11}}} + v_{11}v_{21}(1 - p_{11})^{\frac{l}{v_{21}}}}{l(v_{21} - v_{11})\ln(1 - p_{11})}$$

Если $p_{11} = 1$ или $p_{21} = 1$, то вероятность успеха атаки $P = 1$, если $p_{11} = 0$ или $p_{21} = 0$, то вероятность успеха атаки $P = 0$.

Интересным также видится исследование максимального значения вероятности успеха социоинженерной атаки злоумышленника на пользователя при заданном объёме общего количества ресурса, затрачиваемого на атаку, I в зависимости от распределения количества используемого злоумышленником ресурса для каждого атакующего воздействия: $\max\limits_{0\le w_{11}\le I}\left(1-\left(1-p_{11}\right)^{\frac{w_{11}}{v_{11}}}\left(1-p_{21}\right)^{\frac{I-w_{11}}{v_{21}}}\right)$. Функция непрерывна; для поиска максимума ее следует исследовать на концах промежутка и в точках экстремума, где ее производная обращается в ноль.

В общем случае оценка вероятности успеха атаки злоумышленника с использованием всех доступных атакующих воздействий на k-ого пользователя при определённых предположениях может быть представлена следующим образом

$$P_k = 1-\prod_i\prod_j\left(1-p_{ij}^k\right)^{\frac{w_{ij}}{v_{ij}}},$$

где 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, 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. Её математическое ожидание будет рассчитываться следующим образом $\frac{1}{\int\limits_{\Omega_I}1d\Omega_I}\int\limits_{\Omega_I}\left(1-\prod_i\prod_j\left(1-p_{ij}^k\right)^{\frac{w_{ij}}{v_{ij}}}\right)d\Omega_I$, где

$$\Omega_l = \left\{ \begin{pmatrix} w_{11} \\ \vdots \\ w_{1n} \\ \vdots \\ w_{mn} \end{pmatrix}; w_{ij} \geq 0; \sum_{ij} w_{ij} = l \right\}.$$

Снова следует отметить, что не менее интересным является поиск максимума при заданном объёме общего количества ресурса, затрачиваемого на атаку, l в зависимости от распределения количества используемого злоумышленником ресурса для каждого атакующего воздействия: $\max_{\Omega_l} \left(1 - \prod_i \prod_j \left(1 - p_{ij}^k\right)^{\frac{w_{ij}}{v_{ij}}} \right)$.

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. Т.е. рассматривается 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 рассматриваются оценки при разных сочетаниях количества используемого ресурса для разных атакующих действий. 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

$$P_k = 1 - \prod_i \prod_l \left(1 - p_{ij}^k\right)^{\left\lfloor \frac{w_{ij}}{v_{ij}} \right\rfloor},$$

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. При этом атака считается возможной при условии $w_{ij} \geq v_{ij}$.

3.2.4. Вероятностная модель оценки успеха многоходовой социоинженерной атаки

Рассмотрены подходы к расчёту оценок вероятности поражения критичных документов, а также расчёту оценок успеха социоинженерной атаки злоумышленника на пользователя. Отметим, что социоинженерная атака может осуществляться как непосредственно на пользователя, так и опосредованно, через цепочку пользователей. Таким образом, необходимо поставить и решить три задачи оценки вероятности успеха (провала): 1) социоинженерной атаки злоумышленника на пользователя, 2) обеспечения (сохранения, удержания) состояния защищённости пользователей информационной системы, 3) поражения критичных документов. Многоходовой социоинженерной атакой будем называть атаку, при которой цель и точка входа не совпадают.

Многоходовая социоинженерная атака может осуществляться, например, через коллег пользователя и успех её развития, как правило, будет зависеть от интенсивности взаимодействия между сотрудниками в компании. Таким образом, для оценки вероятности успеха прохождения многоходовой социоинженерной атаки через сотрудников компании, необходимо определить интенсивность их взаимодействия между собой.

Предполагается, что чем многочисленнее связи между пользователями информационной системы, тем большее число способов потенциально доступно злоумышленнику для реализации атаки. Представляется весьма правдоподобным предположение, что чем больше количество и интенсивность связей между двумя сотрудниками, тем с большей вероятностью злоумышленник сможет развить социоинженерную атаку, переходя от одного из них к другому.

Рассчитывать оценки вероятности развития атаки от пользователя к пользователю предлагается на социальном графе взаимодействия, вершины которого сопоставляются пользователям, а дуги — связям между ними. Предлагается подход к расчёту этих оценок вероятностей, основанный в свою очередь на оценке вероятности перехода по дуге, причем эта оценка строится на основе сведений об интенсивности общения между соответствующей парой сотрудников. Подходы к сбору этих сведений будут представлены ниже.

Об интенсивности взаимодействия между сотрудниками можно судить на основании разных эпизодов этого взаимодействия. Пусть q_i — вероятность успеха социоинженерной атаки при одном эпизоде взаимодействия, тогда $1-q_i$ — вероятность того, что социоинженерная атака не завершится успехом при данном эпизоде.

Для расчёта оценки вероятности того, что социоинженерная атака не распространится между пользователями, предлагается адаптировать модель Белла–Тревино [18, 53]. Таким образом, оценка вероятности того, что социоинженерная атака не распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться по формуле

$$Q = \prod_i \left(1-q_i\right)^{n_t}$$

где q_i — вероятность успеха социоинженерной атаки при одном эпизоде взаимодействия, n_t — число эпизодов. Вероятность того, что социоинженерная атака распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться как вероятность дополнения указанного выше события «атака не распространится»:

$$P = 1 - Q.$$

Таким образом, алгоритм расчёта оценок вероятностей успеха социоинженерных атак сводится к сбору информации о связях пользователей [75], построению возможных, с точки зрения накопленной информации, деревьев атак [96] и агрегации полученной информации с помощью формул представленных выше для P и Q.

Описанным выше образом предлагается рассчитывать оценки вероятностей успеха прохождения атаки на сотрудника через другого сотрудника для всех пар сотрудников компании. Данные вероятности будут в свою очередь использоваться для расчёта оценок вероятности успеха многоходовой социоинженерной атаки на l-ого пользователя через m-ого по следующей формуле: $P_{ml} = P_m \prod_{i=m}^{l-1} P_{i,i+1}$, где P_m — вероятность успеха неопосредованной атаки злоумышленника на m-ого пользователя, а $P_{i,i+1}$ — соответствующая оценка вероятности распространения атаки на пользователя через другого пользователя. Вместе с тем оценка защищённости пользователей информационной системы от социоинженерной атаки следующая: $P = 1 - P_{ml}$.

Обобщая изложенное, 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.

Исходя из этого, оценка вероятности успеха атаки на пользователя информационной системы будет строиться на основании агрегации вероятностей успеха многоходовых атак на него и прямой атаки злоумышленника. Модель расчёта оценок защищённости пользователей информационных систем от многоходовых социоинженерных атак будет агрегировать оценки всех возможных траекторий реализации социоинженерной атаки на каждого пользователя. Пусть $\mathrm{Path}(m,f)$ — множество траекторий, по которым может развиваться социинженерная атака от пользователя m до пользователя f. Формализуя описанное, оценка вероятности того, что злоумышленник-социоинженер не сможет успешно атаковать пользователя f будет следующей:

$$\overline{Q}_f = \prod_{\mathrm{path}\in\mathrm{Path}(m,f)} \left(1-\tilde{P}_{\mathrm{path}}\right),$$

где $\tilde{P}_{\mathrm{path}}$ — оценка вероятности успеха социоинженерной атаки злоумышленника в социальном графе от пользователя m до пользователя f по траектории $\mathrm{path}\in\mathrm{Path}(m,f)$, а вероятность успеха социоинженерной атаки злоумышленника на пользователя по всем возможным траекториям будет выражаться следующим образом:

$$\overline{P}_f = 1-\overline{Q}_f.$$

Рассмотрим эту задачу с учётом ограничений ресурса, доступного злоумышленнику. Оценку успеха многоходовой социоинженерной атаки злоумышленника на пользователя будем рассчитывать с учётом того, что злоумышленником используется определённое количество одного вида ресурса на каждый переход от пользователя к пользователю. Для упрощения сначала рассмотрим модель оценки успеха атаки, включающую два перехода от пользователя к пользователю. В этом случае вероятности успеха перехода от первого пользователя ко второму и от второго к третьему будут следующими: $P_{12}\left(w_1\right)=1-\left(1-p_{12}\right)^{\frac{w_1}{v_1}}$, $P_{23}\left(w_2\right)=1-\left(1-p_{23}\right)^{\frac{w_2}{v_2}}$

, где w_1, w_2 — количество ресурса, которое злоумышленник готов использовать при первом и втором переходах. v_1, v_2 — количество ресурса, которое необходимо затратить при первом и втором переходах от первого пользователя ко второму и от второго к третьему соответственно, чтобы поразить их с вероятностями p_{12} и p_{23} соответственно, при этом $v_1 > 0, v_2 > 0$. Отметим, что общее количество затрачиваемого злоумышленником на атаку ресурса $l = w_1 + w_2$. При этом $0 \le l \le L$, где L — общее количество ресурса, имеющегося у злоумышленника. При таких предположениях, вероятность успеха многоходовой социоинженерной атаки злоумышленника на пользователя будет выражаться следующим образом

$$P_{13} = P_{12}(w_1)P_{23}(w_2) = \left(1-\left(1-p_{12}\right)^{\frac{w_1}{v_1}}\right)\left(1-\left(1-p_{23}\right)^{\frac{w_2}{v_2}}\right) = \left(1-\left(1-p_{12}\right)^{\frac{w_1}{v_1}}\right)\left(1-\left(1-p_{23}\right)^{\frac{l-w_1}{v_2}}\right).$$

Её математическое ожидание в предположении, что w_1 распределена равномерно, будет следующим

$$\frac{1}{l}\int_0^l \left(1-\left(1-p_{12}\right)^{\frac{w_1}{v_1}}\right)\left(1-\left(1-p_{23}\right)^{\frac{l-w_1}{v_2}}\right)dw_1 = \frac{1}{l}\left(w_1 + \frac{v_1 v_2 \left(1-p_{23}\right)^{\frac{l}{v_2}} e^{\frac{\ln(1-p_{12})w_1}{v_1} - \frac{\ln(1-p_{23})w_1}{v_2}}}{v_2\ln\left(1-p_{12}\right) - v_1\ln\left(1-p_{23}\right)} + \right.$$

$$\left. + \frac{v_2\left(1-p_{23}\right)^{\frac{l}{v_2}-\frac{w_1}{v_2}}}{\ln\left(1-p_{23}\right)} - \frac{v_1\left(1-p_{12}\right)^{\frac{w_1}{v_1}}}{\ln\left(1-p_{12}\right)} \right|_0^l = 1 + \frac{v_1 v_2 \left(1-p_{23}\right)^{\frac{l}{v_2}} e^{\frac{\ln(1-p_{12})l}{v_1} - \frac{\ln(1-p_{23})l}{v_2}} - v_1 v_2}{l v_2 \ln\left(1-p_{12}\right) - l v_1 \ln\left(1-p_{23}\right)} +$$

$$+ \frac{v_2 - v_2\left(1-p_{23}\right)^{\frac{l}{v_2}}}{l\ln\left(1-p_{23}\right)} - \frac{v_1 - v_1\left(1-p_{12}\right)^{\frac{l}{v_1}}}{l\ln\left(1-p_{12}\right)}$$

Если $p_{23} = 1$, то математическое ожидание будет следующим

$$\frac{1}{l}\int_0^l \left(1-\left(1-p_{12}\right)^{\frac{w_1}{v_1}}\right)dw_1 = \frac{1}{l}\left(w_1 - \frac{v_1\left(1-p_{12}\right)^{\frac{w_1}{v_1}}}{\ln\left(1-p_{12}\right)} \right|_0^l = 1 + \frac{v_1 - v_1\left(1-p_{12}\right)^{\frac{l}{v_1}}}{\ln\left(1-p_{12}\right)}.$$ Аналогично при $p_{12} = 1$. Если $p_{12} = 1$ и $p_{23} = 1$ одновременно, то $P_{13} = 1$. Если $p_{12} = 0$ или $p_{23} = 0$, то вероятность успеха атаки $P_{13} = 0$.

Интересным также видится исследование максимального значения вероятности успеха многоходовой социоинженерной атаки злоумышленника на пользователя при заданном объёме общего количества ресурса, затрачиваемого на атаку, l в зависимости от распределения количества используемого злоумышленником ресурса для каждого перехода от пользователя к пользователю: $\max\limits_{0\le w_1\le l}\left(\left(1-\left(1-p_{12}\right)^{\frac{w_1}{v_1}}\right)\left(1-\left(1-p_{23}\right)^{\frac{l-w_1}{v_2}}\right)\right)$. Функция непрерывна; для поиска максимума ее следует исследовать на концах промежутка и в точках экстремума, где ее производная обращается в ноль.

В общем случае оценка вероятности успеха многоходовой социоинженерной атаки злоумышленника на пользователя при определённых предположениях может быть представлена следующим образом

$$\overline{P}_{i_1-\ldots-i_k-\ldots-i_n}=1-\prod\nolimits_{1\le k\le n-1}\left(1-\tilde{P}_{i_k,i_{k+1}}\right)^{\frac{w_{i_k,i_{k+1}}}{v_{i_k,i_{k+1}}}},$$

где $w_{i,j}$ — количество ресурса, которое злоумышленник готов использовать при переходе от i-ого пользователя к j-ому. $v_{i,j}$ — минимальное количество ресурса, которое необходимо затратить при переходе от i-ого пользователя к j-ому, $\tilde{P}_{i,j}$ — вероятность успеха перехода от i-ого пользователя к j-ому, n — длина цепочки пользователей, через которых проходит атака, а $\overline{P_f}$ — оценка вероятности успеха многоходовой атаки злоумышленника. Её математическое ожидание будет рассчитываться следующим образом $\frac{1}{\int\limits_{\Omega_l}1d\Omega_l}\int\limits_{\Omega}\left(1-\prod\nolimits_n\left(1-\tilde{P}_{i,j}\right)^{\frac{w_{i,j}}{v_{i,j}}}\right)d\Omega_l$, где

$$\Omega_l=\left\{\begin{pmatrix}w_{i,i+1}\\ \vdots\\ w_{j-1,j}\end{pmatrix},w_{i,j}\ge 0;\sum\nolimits_{ij}w_{i,j}=l\right\}.$$

Также полезным видится исследование максимального значения вероятности успеха многоходовой социоинженерной атаки злоумышленника на пользователя при заданном объёме общего количества ресурса, затрачиваемого на атаку, l в зависимости от распределения количества используемого злоумышленником ресурса для каждого перехода от пользователя к пользователю: $\max\limits_{\Omega_l}\left(1-\prod_{1\le k\le n-1}\left(1-\tilde{P}_{i_k,i_{k+1}}\right)^{\frac{w_{i_k,i_{k+1}}}{v_{i_k,i_{k+1}}}}\right)$.

3.3. МЕТОД СБОРА И ОБРАБОТКИ СВЕДЕНИЙ ДЛЯ ОЦЕНКИ ПАРАМЕТРОВ МОДЕЛИ ПОЛЬЗОВАТЕЛЯ И МЕЖПОЛЬЗОВАТЕЛЬСКИХ СВЯЗЕЙ

Профиль уязвимостей пользователя представляет собой набор пар уязвимость — выраженность уязвимости. Для построения профиля уязвимостей могут учитываться различные особенности пользователя: социологические, культурантропологические, психологические и иные (рисунок 3). В рамках исследования не строится полный профиль пользователя со всеми возможными уязвимостями. Необходимо создание пополняемой базы данных, содержащий перечень уязвимостей пользователя, по аналогии с базами данных программно-технических уязвимостей. В исследовании предлагается математическая модель, которая покроет определенные классы уязвимостей, но поскольку в данном случае оцениваются уязвимости личности, то могут обнаружиться другие классы уязвимостей, для которых предложенная модель будет чрезмерным упрощением или не будет годиться вообще. Тогда могут появиться компоненты профиля уязвимостей пользователя новой структуры, может быть, более богатой, но сущность подхода не изменится, всё равно сведения об уязвимостях будут отражаться в профиле уязвимостей, который будет обрабатываться совместно с профилями компетенций злоумышленника для построения оценок вероятности успеха тех или иных атакующих действий злоумышленника. При этом сейчас даже простая модель будет полезна,

так как на ее основе строятся расчеты оценок вероятности успеха социо-инженерной атаки злоумышленника на пользователя и возникает возможность сопоставления результатов с наблюдавшейся ситуацией или с мнением экспертов. В зависимости от этого будет определена необходимость усложнения модели. Возможно, потребуется учитывать динамические изменения системы и состояний пользователя во время прохождения атаки; оценивать изменения компетенций и ресурсов злоумышленника.

Рисунок 3 — Источники информации для оценки параметров профиля уязвимостей пользователя

Рассмотрим процесс оценки некоторых параметров фрагмента профиля уязвимостей пользователя через оценку некоторых особенностей его личности. Оценить эти особенности пользователя можно на основании следующих источников: информации из отдела кадров, мнений экспертов, выбора пользователем стратегии в специальной компьютерной игре, контента, публикуемого в социальных сетях и иных источниках. В диссертационной работе особое внимание уделяется агрегации сведений

из социальных сетей, как источника информации для оценки степени выраженности некоторых особенностей личности пользователя, интенсивности взаимодействия между пользователями. Необходимость агрегации этих сведений ставит ряд задач, связанных с их сбором и обработкой, решение которых представлено в следующем разделе.

Отметим, что в качестве источника данных была выбрана социальная сети ВКонтакте (https://vk.com/). Согласно статистическим исследованиям, данная социальная сеть является одной из самых популярных на территории Российской Федерации [176, 184, 185].

3.3.1. Метод, модель и алгоритм автоматизированного поиска аккаунтов сотрудников компании в социальной сети

Для того, чтобы получить информацию о пользователе из социальной сети необходимо сначала осуществить там поиск его аккаунта. Находить аккаунты сотрудников компании можно вручную, используя фильтры, предоставляемые большинством социальных сетей. Но если в компании работает достаточно большое число сотрудников, то для осуществления поиска их аккаунтов вручную потребуется существенное время. Таким образом, актуальной видится задача разработки методов, моделей, алгоритмов и реализации автоматизации поиска аккаунтов сотрудников компании в социальных сетях. Некоторые подходы к решению данной задачи были представлены в [16, 58]. В данном разделе представлены методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте (https://vk.com).

На первом этапе необходимо построить классификатор, на основании которого аккаунт в социальной сети ВКонтакте будет относится к списку сотрудников или нет. Задача поиска и идентификации необходимых аккаунтов формально сводится к задаче бинарной классификации

при следующей формализации. Пусть X — множество страниц пользователей социальной сети ВКонтакте, а Y — множество наименований классов, в данном случае это множество состоит из двух классов: сотрудники и не сотрудники. Необходимо построить алгоритм

$$a : X \to Y,$$

который будет иметь возможность классифицировать любой $x \in X$ [193].

Для решения задачи классификации в рамках данной работы применяется структура дерева принятия решений. Данный метод обладает рядом преимуществ, среди которых корректность работы с необработанными данными, надёжность, удобство работы с большими объёмами данных [62].

Отметим, что данная структура использовалась в близких по тематике исследованиях [27], в которых анализировались цифровые следы сотрудников компании. Метод показал хорошие результаты, качество результирующего дерева было оценено на основе показателя f_1-score. Для дерева принятия решений рейтинг $f_1\text{-score} = 0.65$, альтернативная структура на основе «случайного леса» имела следующие показатели: $\text{precision} = 0.67$, $\text{recall} = 0.08$ и результирующее значение $f_1\text{-score} = 0.14$. Таким образом, в сравнении с методом «случайного леса» построение дерева решений показывает результаты лучше [27].

Для оценки качества классификатора используется ROC-кривая, которая при варьировании порога решающего правила показывает то, как зависит recall (доля найденных алгоритмом объектов – аккаунтов сотрудников компании, принадлежащих классу, из всех объектов класса) от FPR (False Positive Rate, количество объектов, которые были неправильно отнесены алгоритмом к классу сотрудников компании). Ниже на рисунке 4 представлена ROC-кривая, которая используется для анализа эффективности полученного классификатора, для примера IT-компании с заявленной численностью штата 1200 сотрудников:

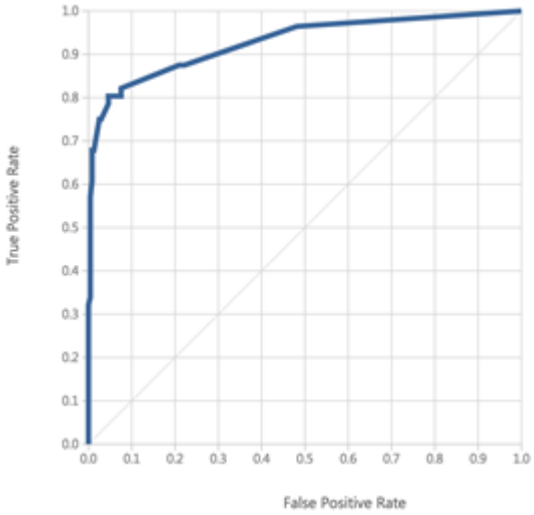


Рисунок 4 — ROC-кривая для классификатора, построенного на примере IT-компании

Для получения числовой характеристики ROC-кривой используется площадь под графиком AUC (Area Under Curve), чем ближе её значение к 1, тем лучше получился классификатор [69]. В примере на рисунке 4 получившийся показатель AUC = 0.928, что является хорошим результатом.

Построенное дерево принятия решений представлено на рисунке 5, оно 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.

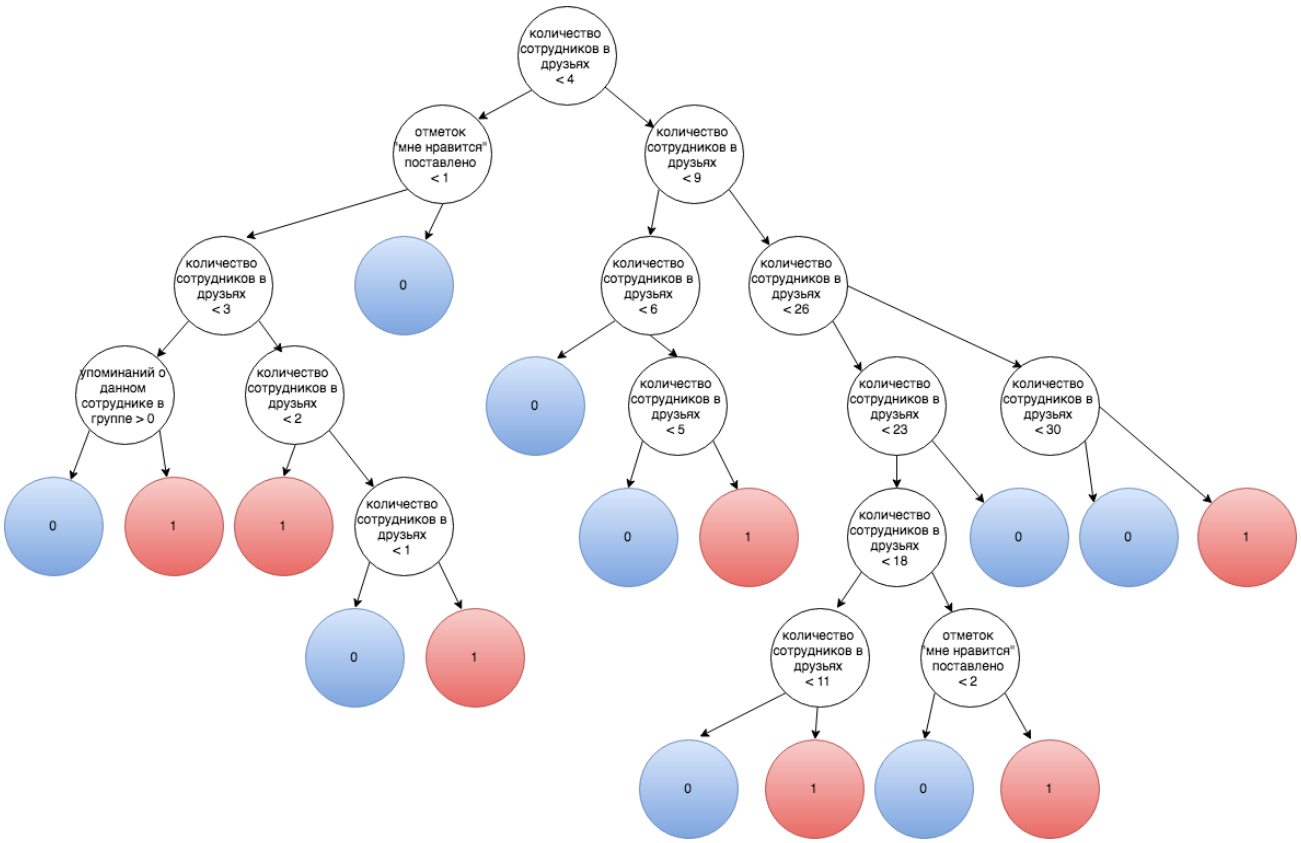


Рисунок 5 — Дерево принятия решений

Для повышения качества результирующего дерева необходимо строить собственный бинарный классификатор для каждой анализируемой компании. Это возможно только при полной автоматизации сбора и анализа целевой переменной для обучающей выборки. Для этого в обучающую выборку были добавлены страницы с указанным местом работы в анализируемой компании в качестве примеров со значением целевого параметра равного единице. На основе списка их друзей обучающая выборка дополнялась страницами пользователей, у которых указано текущее место работы в другой компании. На листинге 1 представлен фрагмент кода одного из классов, отвечающего за инициализацию поиска аккаунтов сотрудников компании, обучение классификатора, а также сбор аккаунтов.

Листинг 1 — Класс CreateSocialGraph, инициализирующий поиск аккаунтов сотрудников компании

```
public void createSocialGraph()
{
      CollectingTrainingDataset collector = new      CollectingTrainingDa-
taset("Кодельная", "116186911");
            collector.parseInformation();
            this.trainingDataset = collector.training_dataset;

      //обучение классификатора
      DecisionTreeBuilder dt = new  DecisionTreeBuilder(collector.training_da-
taset);
      dt.studyDT();

      //сбор оставшихся аккаунтов
      this.searcher = new EmployeesSearcher(dt, collector.companyName,
      collector.vkPageId);
      this.searcher.findAllEmployees();
      this.empSocialGraph = searcher.EmployeesSocialGraph;
}
```

В результате обучающая выборка была составлена из аккаунтов, в которых пользователи указали своё текущее место работы. Для обоснования того, что данное допущение не искажает результатов, необходимо оценить различия между выборками: обучающей и выборкой, составленной из аккаунтов, которые также принадлежат сотрудникам компании. В качестве признака для сравнения использовались количественные показатели, фиксируемые на странице компании в социальной сети, т.е. число отметок «Мне нравится» с аккаунтов под постами от имени сообщества компании в социальной сети ВКонтакте, число репостов, число комментариев. В условиях действующих ограничений, связанных с размером выборки и признаком, по которому будет производиться сравнение, был использован метод Манна–Уитни [138]. Тест показал, что эти выборки не отличаются. Таким образом, можно допустить, что обучающая выборка корректна.

После выполнения алгоритма имеем граф сотрудников компании, где каждой вершине сопоставлен идентификационный номер его аккаунта в социальной сети ВКонтакте, наличие ребра между двумя вершинами свидетельствует о том, что пользователи указали друг друга в качестве друзей. Для увеличения числа правильно идентифицированных аккаунтов сотрудников компании в социальной сети ВКонтакте, а также числа

найденный аккаунтов потенциальных сотрудников предлагается производить анализ вершин, длина пути от которых до вершин, включённых в обучающую и тестовую выборки, не превышала бы двух рёбер в графе. Особенность данного подхода заключается в его проактивности [135], т.е. наличии возможности предсказывать сложность алгоритма и объем вычислений, поскольку количество анализируемых страниц строго фиксировано. Основной недостаток подхода заключается в том, что перечень классифицируемых страниц сильно зависит от обучающей выборки. В исследовании не участвуют страницы пользователей, путь от которых в графе до попавших в обучающую выборку составлял больше 2 вершин, т.к. сложность проактивного алгоритма в этом случае будет сравнима с $O\left(n^m\right)$, где n — объем обучающей выборки, а m — максимальное расстояние от исследуемых вершин до вершин из обучающей выборки.

С одной стороны, собранная информация об аккаунтах сотрудников остаётся актуальной довольно продолжительное время и в программной реализации не требуется представление результатов в режиме реального времени, поэтому такая вычислительная сложность была бы допустима. Однако, присутствует другая проблема, связанная с ограничениями на взаимодействие с социальной сетью ВКонтакте для зарегистрированного приложения, от имени которого запускается парсер страниц. API ВКонтакте устанавливает ограничение в размере 5 запросов в секунду, которое снимается только при наборе приложением 10 000 клиентов. Разрабатываемое приложение на данный момент используется примерно 10 исследователями. Отметим также, что приложение не рассчитано на одновременное использование большим количеством пользователей с одного сервера. Для иллюстрации работы алгоритма на рисунке 6 представлено реальное множество сотрудников — множество «real employees», а область поиска ограничивается множеством «friends of 3».

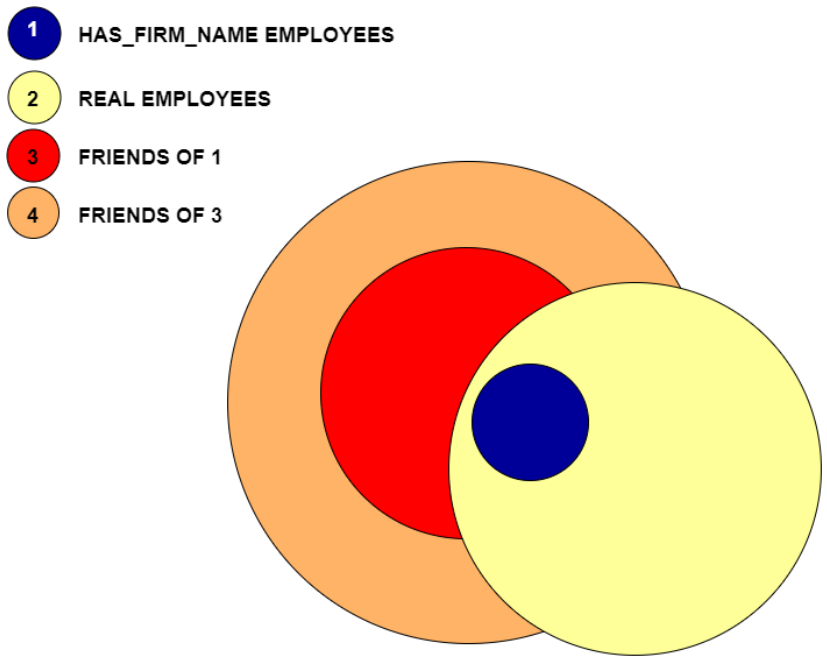


Рисунок 6 — Сфера поиска при начальной реализации алгоритма

При реализации особое внимание было уделено реактивности алгоритма, т.е. при каждой новой итерации будут выбираться найденные на последней итерации аккаунты сотрудников и анализироваться их списки друзей. Недостаток данного подхода заключается в его рекурсивности. Поскольку результаты работы программной реализации могут иметь погрешность, есть риск, что выполнение программы может потребовать существенного времени. Поэтому введена возможность ограничения числа аккаунтов для поиска, т.е. добавление условия выхода, например, когда программный модуль останавливает свою работу при отборе 1200 аккаунтов. Обычно число сотрудников компании известно, в связи с этим удобно указывать это число, как условие выхода. Пользователи, которые имеют больше одного аккаунта в социальной сети, будут скомпенсированы теми, кто не имеет ни одного аккаунта. В случае если выборка будет полностью релевантна, при этом сработает условие выхода, можно продолжить работу программного модуля. Проиллюстрируем некоторые шаги алгоритма автоматизированного поиска сотрудников компании в социальной сети ВКонтакте. Схема алгоритма представлена на рисунке 7.

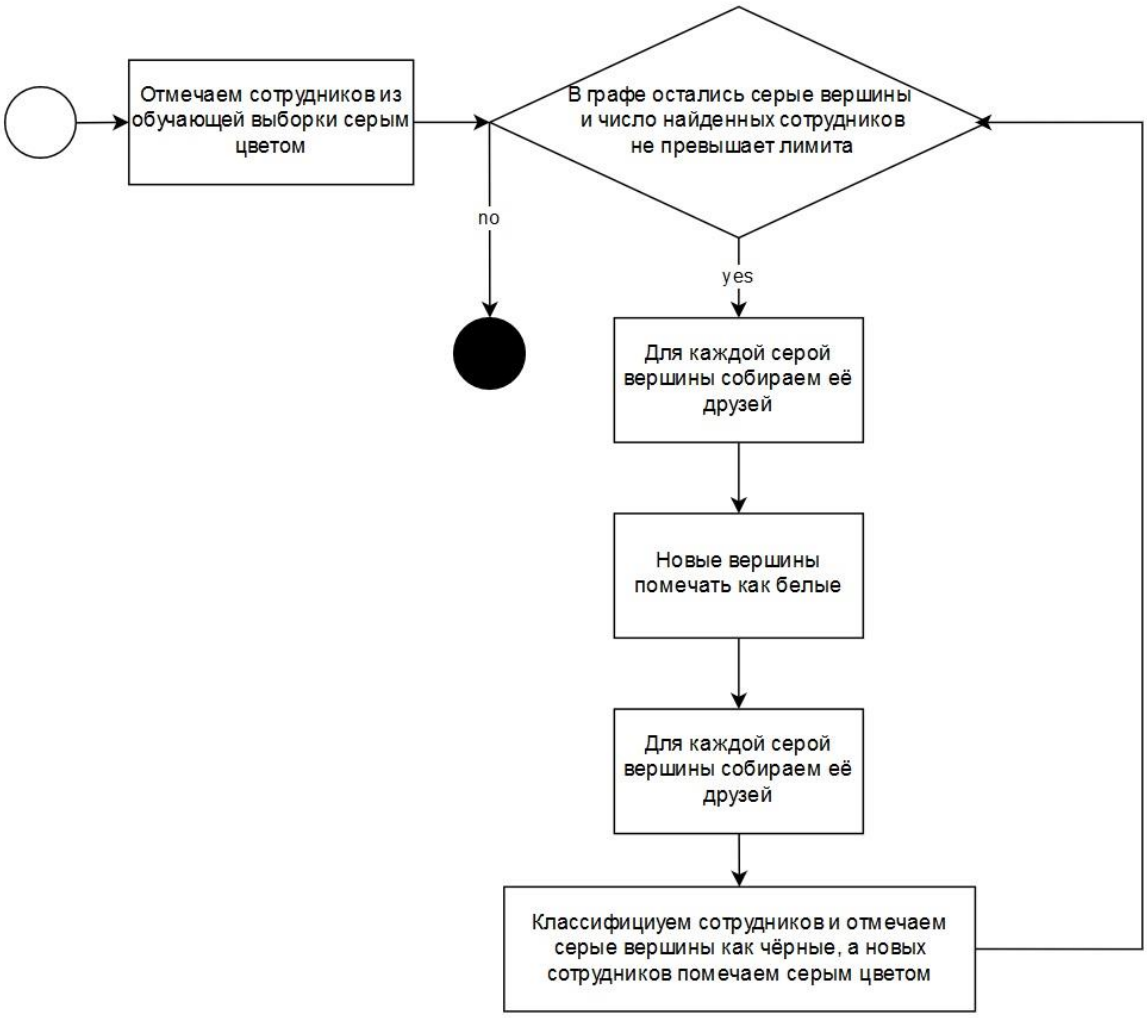


Рисунок 7 — Схема алгоритма

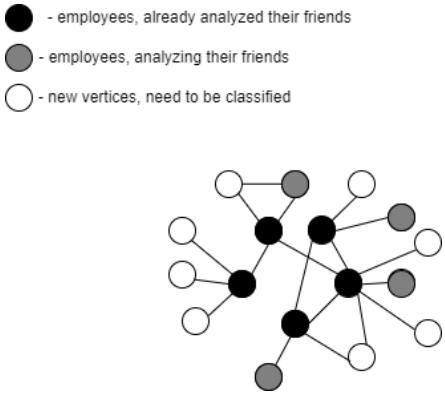
Вершины окрашиваются в черный, серый и белый цвета. Значения каждого цвета представлены ниже.

- White (белый) — означает, что вершину необходимо классифицировать, если это начало итерации, или же в вершине содержится ссылка на страницу non-employee (не сотрудника) в конце итерации. В последнем случае дальше поиск не пойдет;
- Grey (серый) — в вершине сотрудник, надо классифицировать его друзей;
- Black (чёрный) — в вершине сотрудник, список его друзей уже проанализирован и классифицирован.

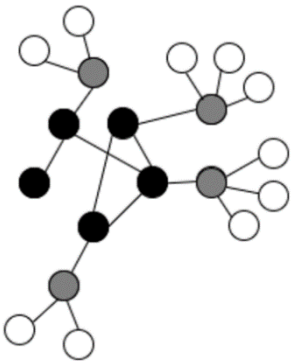
На рисунке 8 (а) представлен социальный граф связей сотрудников в момент первой итерации работы алгоритма. В чёрный цвет окрашены

вершины, сопоставленные сотрудникам из обучающей выборки, указавшим место работы в анализируемой компании. Остальные вершины были подвержены классификации. В результате вершины, классифицированные как аккаунты сотрудников компании из числа друзей идентифицированных ранее аккаунтов сотрудников, окрашиваются в серый цвет (рисунок 8 (б).

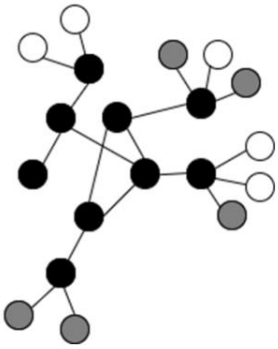
Далее осуществляется поиск среди вершин, связанных с серыми вершинами. Собирается коллекция из друзей серых вершин, а серые вершины перекрашиваются в чёрный цвет. Затем найденные вершины классифицируются и окрашиваются в зависимости от результирующего класса. Данные этапы алгоритма проиллюстрированы на рисунке 8 (в).



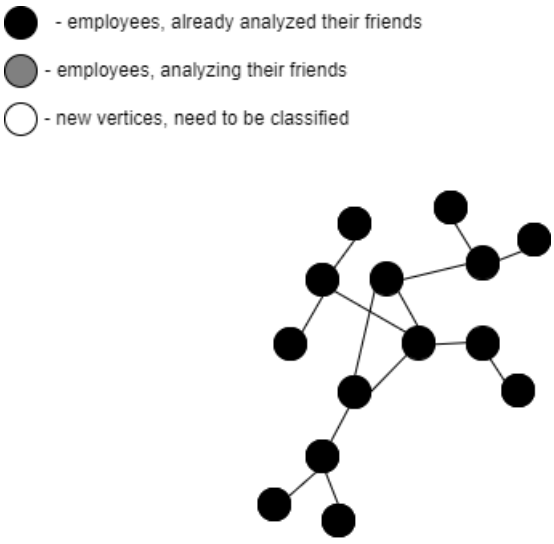
а) Первый шаг.



б) Второй шаг.



в) Третий шаг.



г) Результирующий граф.

Рисунок 8 — Шаги алгоритма

На финальной итерации не были выявили новые аккаунты сотрудников, поэтому белые вершины отсекаются. Результирующий граф представлен на рисунке 8 (г).

Данный реактивный подход позволяет осуществлять поиск, основываясь на более полном перечне выявленных сотрудников, а не только на тех, кто указал текущее место работы в графе «Карьера». Тем не менее, данный подход не гарантирует получение полного списка аккаунтов сотрудников компании. Это может быть связано с несколькими факторами, среди которых возможные ошибки классификатора, исключение из рассмотрения вершин, которые не попадают в одну компоненту связности графа социальных связей хотя бы с одной из вершин обучающей выборки. При увеличении глубины поиска сильно растёт вычислительная сложность алгоритма, опережая допустимые пороговые значения. Одно из возможных решений в данном случае — добавление интерфейса для ручного включения новых узлов в поиск (рисунок 9).

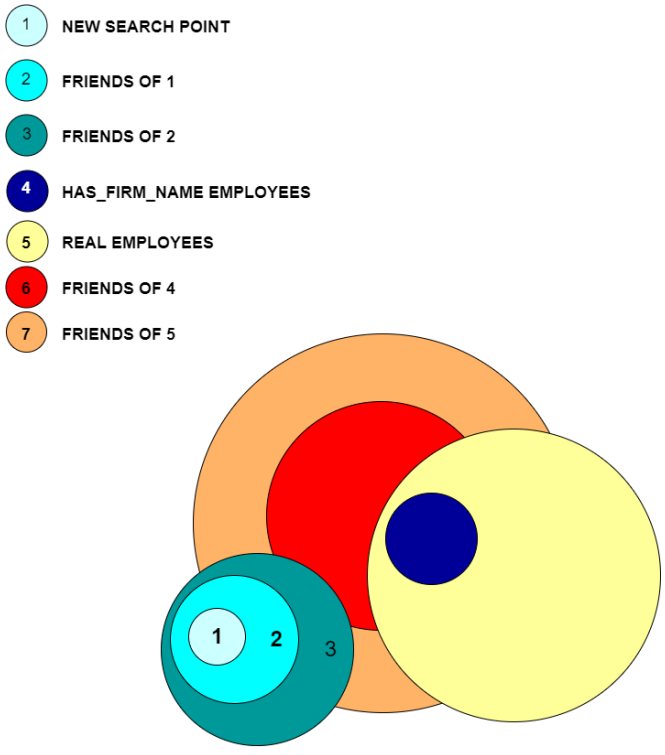


Рисунок 9 — Поиск после добавления нового узла

На основе представленного алгоритма автоматизированного поиска аккаунтов сотрудников строится граф социальных связей сотрудников. Алгоритм предусматривает возможность включения для анализа нового узла, в роли которого может выступать как аккаунт сотрудника компании, так и страница обычного пользователя социальной сети. Далее, на основе представленного выше подхода анализируются все друзья данного пользователя, а также друзья друзей пользователя. Таким образом, происходит проактивный просмотр двух поколений связей определенного узла, что позволяет расширить диапазон поиска и, соответственно, дополнить список уже найденных сотрудников. Иллюстрация изложенной концепции представлена на рисунке 9, её алгоритм приведён на рисунке 10.

На рисунке видно, что в случае ручного добавления нового узла (множество «1»), расширяется круг поиска на множество «3», что дополняет перечень страниц сотрудников компании. На рисунке 11 представлена иллюстрация возможных шагов алгоритма с учётом ручного добавления нового узла. Такой подход позволяет произвести более глубокий поиск аккаунтов сотрудников компании в социальной сети ВКонтакте, делает возможным контроль оператора за выполнением программного модуля.

Разработано программное обеспечение, которое позволяет автоматизированно осуществлять поиск аккаунтов сотрудников компании. Чтобы применить данный подход, необходимо задать ссылку на официальное сообщество компании в социальной сети и название анализируемой компании в том виде, в каком оно обычно указывается пользователями в графе «Карьера».

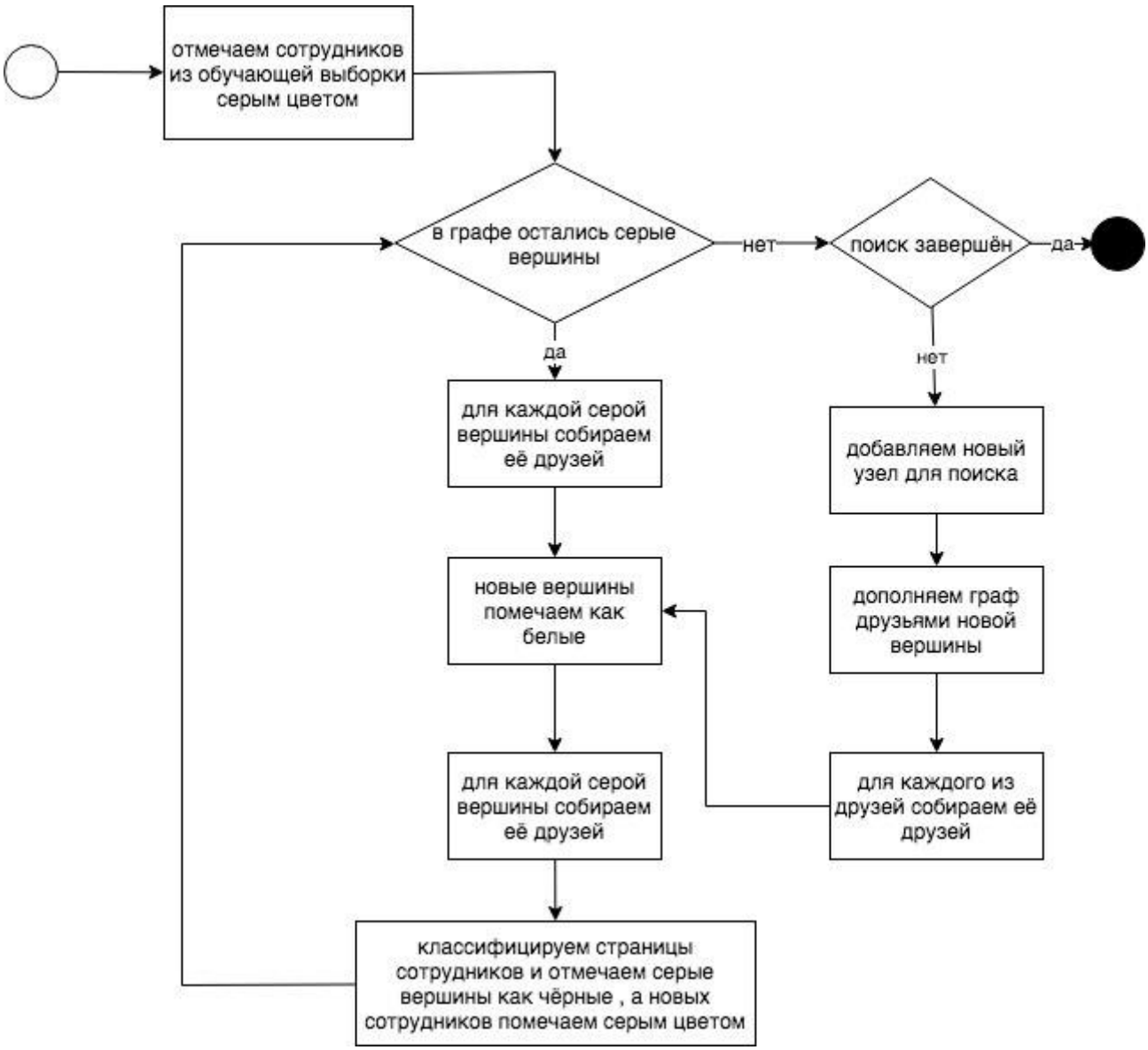
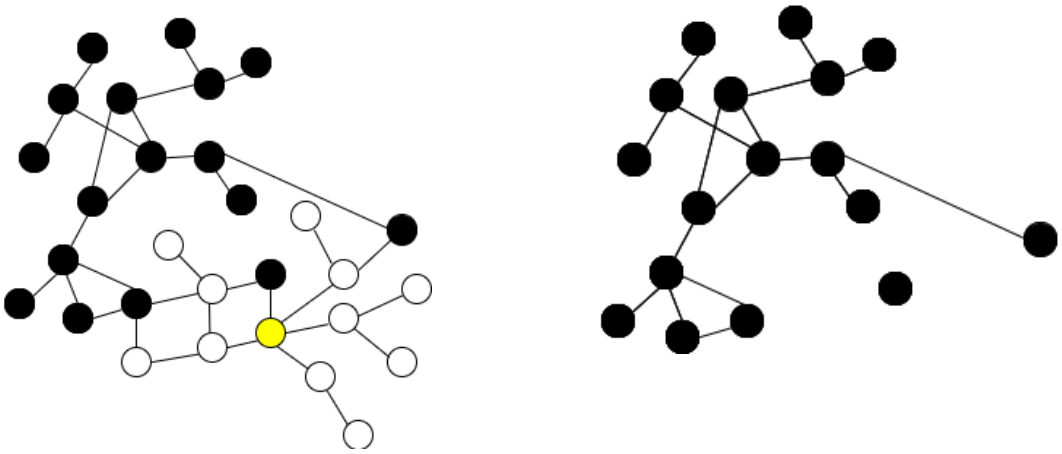


Рисунок 10 — Схема алгоритма, включающая дополнение поиска за счёт новых вершин

Разработанные методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте позволяют существенно сократить время, затрачиваемое на ввод параметров в комплексе программ для анализа защищённости пользователей информационной системы от социоинженерных атак. Перспективы дальнейшего направления исследований в этой области могут быть связаны с расширением числа анализируемых источников за счёт вклю-

чения других социальных сетей, визуализацией социального графа сотрудников компании на основании информации, извлекаемой из социальных сетей.



а) Добавление новой вершины.

б) Результирующий граф после дополнительного поиска

Рисунок 11 — Шаги алгоритма после добавления вручную нового узла

3.3.2. Метод и алгоритм оценки степени выраженности некоторых особенностей пользователей, основанный на автоматизации анализа данных, извлекаемых из социальных сетей

В более ранних работах [96] вероятности успеха социоинженерной атаки злоумышленника на пользователя задавались экспертно на основе анкетирования пользователей. Но если в анализируемой компании работает достаточно большое количество сотрудников, то занесение информации о них в программу становится трудоёмким процессом. В то же время данные, полученные из анкет, не всегда являются достоверными. При этом в настоящее время всё большее количество людей становятся пользователями социальных сетей [184, 185]. Большинство из них не задумывается о соблюдении мер информационной безопасности, добровольно публикуя данные о себе [63]. Между тем доступ к этим данным может также получить злоумышленник, следовательно — и учитывать их при планировании атаки. Такая информация имеет высокую ценность также потому, что выводы, основанные на публикуемом пользователем

контенте в социальной сети, как правило, больше соответствуют действительности, чем получаемые в рамках опросов или интервью [26,191].

Для построения модели, используемой при автоматизированной оценке степени выраженности некоторых особенностей пользователей использовались методы машинного обучения (см. ниже). Более подробно о том, как собирались данные для обучающей и тестовой выборок описано в приложении В. Объём собранной коллекции составил 600 единиц. Каждая единица представляет собой пост со страницы пользователя и набор значений степени выраженности его психологических характеристик [16, 101].

С помощью платформы Microsoft Azure Machine Learning были созданы, настроены и обучены две пробные модели. Первичное исследование решало задачу оценки степени выраженности психологической характеристики «Проекция». Модели для остальных характеристик строятся аналогично.

Первая модель основана на использовании метода опорных векторов (SVM), вторая — включает в себя нейронную сеть. В обеих моделях производится предварительная обработка текста, включающая:

- удаление пунктуации;
- удаление цифровых и специальных символов;
- приведение текста в нижний регистр;
- извлечение N-грамм и feature hashing;
- выбор признаков для обучения на основе фильтрации по степени влияния на обучение.

Кроме того, исходная выборка была поделена на обучающую и тестовую в соотношении 80% и 20% соответственно. Таким образом, модели работали с подготовленной обучающей выборкой, представленной в виде bag-of-words, а результат их обучения проверялся на тестовой выборке.

Метод опорных векторов использовался в качестве бинарного классификатора. Данные предварительно были разбиты на два класса: записи со степенью выраженности признака проекции выше 60 были классифицированы как 1; остальным был присвоен класс 0. Такая граница была выбрана на основании распределения значений используемой характеристики в исходной выборке.

На этапе извлечения N-грамм параметр N принимал значения 2 и 3. Кроме того, калибровке подвергались такие параметры модели, как количество итераций обучения i и коэффициент L_1-регуляризации λ, препятствующий переобучению. Эффективность модели оценивалась по параметру f-score.

Результаты оценки модели SVM с параметром $N = 2$ на тестовой выборке представлены в таблице 5. Результаты оценки модели SVM с параметром $N = 3$ на такой же тестовой выборке представлены в таблице 6.

Таблица 5 — Результаты оценки модели SVM с параметром $N = 2$ [16, 102]

i	λ			
	0.00001	0.0001	0.001	0.01
1	0.461538	0.462963	0.448598	0.480769
10	0.517857	0.513761	0.5	0.490909
50	0.564516	0.557377	0.548673	0.458716
100	0.598425	0.557377	0.556522	0.462963
200	0.573643	0.551181	0.54386	0.462963

Таблица 6 — Результаты оценки модели SVM с параметром $N = 3$ [16, 102]

i	λ			
	0.00001	0.0001	0.001	0.01

1	0.517241	0.526316	0.508876	0.47619
10	0.494253	0.502857	0.508671	0.549451
50	0.508475	0.502793	0.55914	0.533
100	0.530387	0.511111	0.541436	0.533
200	0.513966	0.532609	0.535519	0.485549

Как видно из таблиц 5 и 6, наилучший результат $\text{f-score} = 0.598$ показала модель с параметрами $N = 2$, $i = 100$, $\lambda = 0.00001$.

В качестве основы для второй модели был выбран аппарат нейронных сетей, который использовался для решения задачи регрессии, поскольку значения, описывающие психологические характеристики, изначально представляет собой числовые значения в определённом диапазоне.

Нейронная сеть, используемая при моделировании, имеет один скрытый слой с 1000 узлами. Начальные веса узлов равны $w = 0.1$. Используемая функция потерь – cross-entropy. Кроме того, значения выходного параметра «Проекция» были предварительно нормализованы. Во время предварительной обработки из текстовых записей были извлечены биграммы ($N = 2$).

В процессе обучения калибровке подвергались такие параметры нейронной сети, как скорость обучения l (learning rate) и количество итераций i. Для оценки эффективности модели использовался коэффициент определения (coefficient of determination, R_2). Результаты валидации нейронной сети с помощью тестовой выборки представлены в таблице 7.

Таблица 7 — Результаты валидации нейронной сети с помощью тестовой выборки [16, 102]

i	l			
	0.01	0.001	0.0001	0.00001
5	0.06055	0.06577	0.02447	-0.000061

10	0.12002	0.10141	0.05756	0.000913
20	0.14037	0.11045	0.04581	0.002787
40	0.227872	0.16591	0.09624	0.006283
80	0.16065	0.14376	0.05635	0.004521

Согласно таблице 7, наилучший результат $R_2 = 0.228$ показала модель с параметрами $l = 0.01,\ n = 40$.

На рисунке 12 представлена диаграмма алгоритма, реализующего методику выявления и формализации связей между данными, содержащимися в текстовом контенте, публикуемом пользователями в социальной сети ВКонтакте, и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности.

Таким образом, предложена методика автоматизированного выявления и формализации связей между данными, содержащимися в текстовом контенте, публикуемом пользователями в социальной сети ВКонтакте, и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности, которая в перспективе станет основой для построения фрагмента профиля уязвимостей пользователя. Были предложены две модели для анализа текстовой информации в социальных сетях. Дальнейшие исследования в этой области могут быть связаны с увеличением количества данных, используемых в процессе обучения. Кроме того, необходимо исследовать возможность сведения задачи регрессии к задаче классификации. Наиболее перспективным развитием построенной методики представляется применение методов так называемой ординальной классификации. Также одним из возможных вариантов может быть комбинация нескольких методов в одной модели (например, использование SVM для предварительного анализа текста, а затем применение полученных знаний в задаче более сложной классификации).

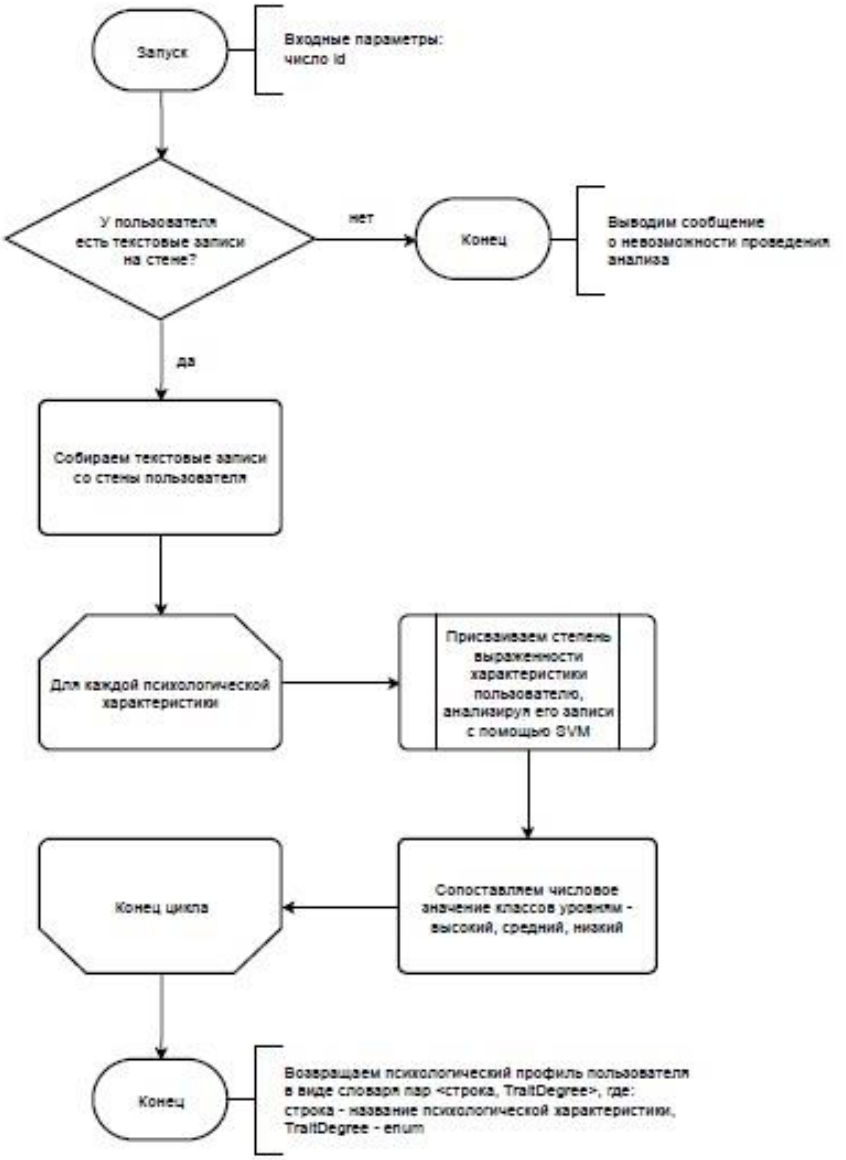


Рисунок 12 — Алгоритм автоматизации оценки степени выраженности ряда особенностей пользователей

3.3.3. Подход к автоматизации оценки некоторых особенностей пользователей на основании публикуемого ими аудиоконтента

Анализ аудиозаписей на странице пользователя позволяет сделать предположения о степени выраженности ряда особенностей его личности, таких как уровень самооценки, коммуникабельности, отношение к труду и иных характеристиках. Корреляция этих признаков отмечалась в научной литературе [20, 49, 50, 52]. Одним из первых о возможности оце-

нить степень выраженности некоторых особенностей личности, основываясь на его музыкальных предпочтениях, писал учёный-психолог из Университета Техаса в США Питер Джэйсон Рентфров. В своей статье [52] он отмечал важность музыки в повседневной жизни человека. Обращал внимание на то, что до недавнего времени музыку не рассматривали, как способ оценки степени выраженности психологических особенностей. Данная работа носит обзорный характер, в ней представлены возможные подходы к оценке степени выраженности некоторых особенностей личности, исходя из её музыкальных предпочтений, освящается ряд исследований, демонстрирующих, что музыка влияет на настроение, выбор музыки разнится от ситуации, индивидуальные предпочтения в музыке зависят от личностных особенностей.

Крупномасштабное исследование учёных из Эдинбурга [50], подкрепленное более ранней работой [49], выявило связь музыкальных предпочтений и уровня интеллектуального развития человека, который измеряли с помощью тестов на IQ. Также в ходе исследований была выявлена корреляция между предпочитаемыми музыкальными жанрами людей и рядом черт их характера. В рамках него было проведено анкетирование, в котором приняли участие более 36 000 человек разных национальностей из более чем 60 разных стран. Это исследование получило широкую огласку, было одним из самых обсуждаемых и распространяемых в сети Интернет [20, 131, 132, 158].

Описанные работы не имели программной реализации, которая бы позволила автоматизированно получать оценки степени выраженности некоторых особенностей личности с помощью устоявшегося инструментария, опираясь на их музыкальные предпочтения. Поэтому на основании результатов, описанных выше исследований, в частности [50], был разработан программный продукт, анализирующий списки аудиозаписей пользователей сети Вконтакте и оценивающий степень выраженности некоторых особенностей их личности. Программа принимает на

вход список числовых или строковых идентификаторов пользователей и производит анализ аудиозаписей для профиля каждого пользователя в этой социальной сети, выявляя его любимый музыкальный жанр. Далее предпочитаемые музыкальные жанры пользователей и наиболее выраженные их личностные качества выводятся в виде таблицы. В настоящий момент программа считает статистики, распределяя аудиозаписи по жанрам. В социальной сети ВКонтакте содержится информация о жанре композиций. Жанр, к которому отнесено большинство аудиозаписей пользователя считается предпочитаемым. На рисунке 13 представлен интерфейс описанного программного продукта.

Таким образом, используется следующая методика оценки некоторых особенностей пользователей на основании публикуемого ими аудиоконтента в социальной сети.

1. Поиск аккаунтов пользователей в социальной сети ВКонтакте, о которых заведомо известно, что они являются сотрудниками компании [58, 211].
2. Проверка настроек приватности в отношении списка их аудиозаписей. Продолжение работы, если плейлист открыт.
3. Сбор мета-информации об аудиозаписях, находящихся в списке пользователя, определение их жанра.
4. Построение распределения по музыкальным жанрам, представленным в плейлисте пользователя.
5. Оценка степени выраженности некоторых особенностей личности пользователя согласно распределению с использованием методики, описанной в [96].

Основной сложностью в ранжировании аудиозаписей пользователей является то, что не у всех аудиозаписей жанр определён корректно. Более того, в ряде случаев жанр произведения не указан. Этим обуславливается необходимость распознавания аудиозаписей плейлиста пользова-

теля и определения жанра. Для этих целей был проведён анализ известных систем, предоставляющих подобный функционал, таких как Shazam (https://www.shazam.com/ru), SoundHound (https://soundhound.com/), ACRCloud (https://www.acrcloud.com/ru/) и Gracenote (http://www.gracenote.com/). В ходе анализа были получены следующие результаты:

- системы Shazam и SoundHound показали хорошие результаты распознавания аудиозаписей, но, к сожалению, они не имеют публичного API, что не позволяет использовать их сейчас в программном модуле;
- система ACRCloud имеет приемлемое качество распознавания аудиозаписей, но представлена только платными версиями;
- система Gracenote бесплатна, но не распознала ни одной аудиозаписи из тестового набора, что не позволяет использовать её в разрабатываемом программном продукте.

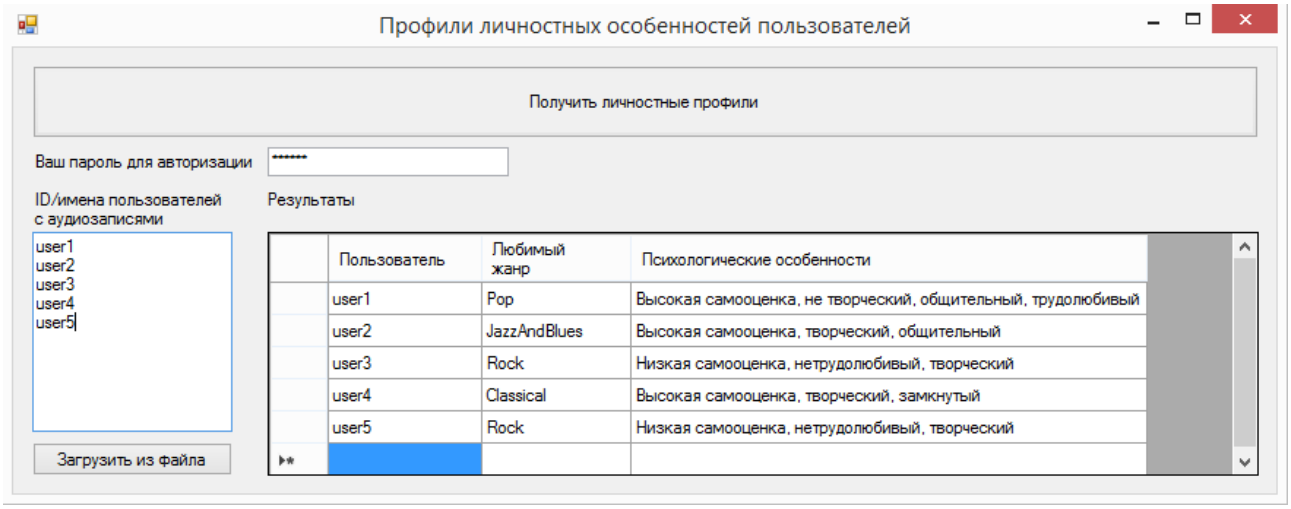


Рисунок 13 — Интерфейс программы для оценки степени выраженности некоторых особенностей пользователей на основании их музыкальных предпочтений

В [48, 61] приведены более подробные обзоры перечисленных инструментов для идентификации аудиозаписей. Таким образом, требуется либо разработка своего программного обеспечения для этих целей, либо реализация коллаборации с разработчиками текущих решений. Тем не менее при большом объёме аудиозаписей в аккаунте в социальной сети

ВКонтакте анализ на основе мета-информации показывает достаточно высокие результаты.

Таким образом, представленная методика позволяет производить автоматизированную оценку степени выраженности некоторых особенностей пользователей на основании публикуемого ими аудиоконтента. Полученные значения оценок степени выраженности некоторых особенных пользователей используются для оценки параметров профиля уязвимостей пользователя, формализованного выше, по методике, описанной в [96]. В итоге, учитываются альтернативные оценки степени выраженности некоторых особенностей пользователей, которые используются при построении фрагмента профиля уязвимостей пользователя.

3.3.4. Метод и алгоритмы восстановления фрагмента мета-профиля пользователя информационной системы

Для построения фрагмента профиля уязвимостей пользователя используются оценки степени выраженности некоторых особенностей его личности, которые могут рассчитываться на основании данных, извлекаемых из социальных сетей. Отметим, что для оценки степени выраженности некоторых особенностей пользователя, которые связаны с профилем его уязвимостей, важно анализировать наиболее подробную информацию о пользователе. При этом часто в аккаунте заполнены не все анкетные данные, которые способствовали бы построению оценок степени выраженности некоторых особенностей пользователя. Недостающие данные можно извлекать из аккаунтов пользователя в других социальных сетях, а также исходя из анализа аккаунтов пользователей, входящих в его социальное окружение (т.е. являющихся его друзьями). В разделе предложены методы восстановления мета-профиля пользователя информационной системы, где под мета-профилем пользователя понимаются его

анкетные данные. В диссертационном исследовании представлены подходы к восстановлению родного города пользователя, города проживания и даты рождения.

Как правило, сегодня пользователи имеют аккаунты в разных социальных сетях [186]. При этом нередко в каждом из аккаунтов какая-то часть информации не представлена, какая-то не является корректной. С учетом указанных обстоятельств одной из возможностей восстановления недостающих или недостоверных данных является использование в качестве источника контента из нескольких аккаунтов пользователя в разных социальных сетях. Вторая возможность связана с анализом аккаунтов пользователей, являющихся друзьями текущего. Подробнее рассмотрим каждый из подходов.

Первая задача, связанная с идентификацией аккаунтов пользователей социальных сетей не нова, но в текущей формулировке рассматривается впервые. Существующие подходы к её решению демонстрировали разные уровни эффективности [34, 46, 103, 126, 139]. Среди них особенно выделим методику, предложенную в работе [103]. В ней представлен подход к решению задачи поиска и сопоставления аккаунтов одного и того же человека в разных социальных сетях, приведена формализация, представлены методика и алгоритмы для сопоставления профилей одного и того же человека в Facebook и Twitter. Подход, представленный в настоящем диссертационном исследовании, является расширением данного на большее число социальных сетей с учётом большего количества параметров. При анализе аккаунтов учитываются не только анкетные данные пользователей (ФИО, место и год рождения, образование, работа, интересы, политические и религиозные взгляды и т.п.), характер (топологию) их связей, но и фотоматериалы с хештегами, геолокационная информация, отметки других пользователей, взаимная активность пользователей в виде лайков, репостов и прочих факторов.

Формальная постановка задачи может быть представлена следующим образом. Пусть есть n социальных графов с m вершинами. Необходимо найти такие $v_i^1..v_i^n : v_i^j \in V_j$, чтобы они принадлежали одному и тому же пользователю [72]. Иными словами, нужно построить проекции из одного социального графа в другой (рисунок 14). В данной иллюстративной задаче $n = 3$, рассматриваются три социальных графа.

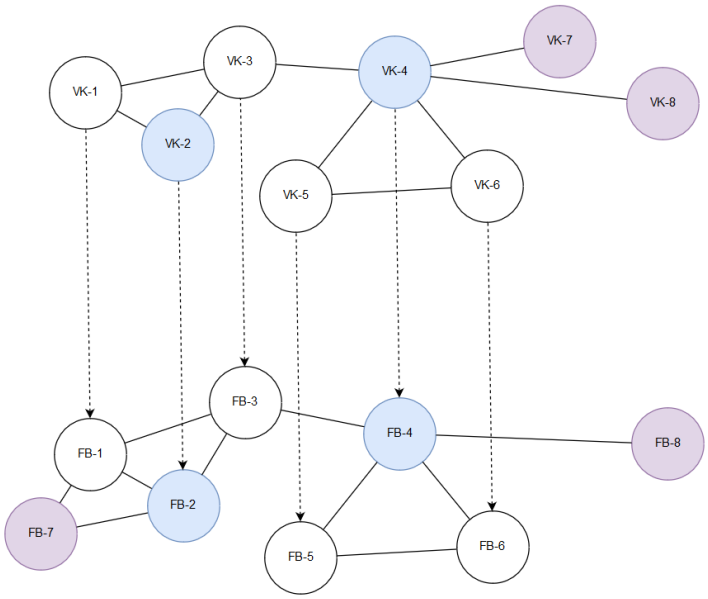


Рисунок 14 — Проекция из одного социального графа в другой

Для решения этой задачи предлагается методика идентификации аккаунтов одного пользователя в разных социальных сетях, состоящая из следующих шагов [58].

1. Поиск аккаунтов пользователей в социальной сети ВКонтакте, о которых заведомо известно, что они являются сотрудниками компании [58, 211]. 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 — ко-

торые 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 мета-профиль 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 подход 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.

Таким образом, мы будем иметь в лучшем случае три гипотезы по каждому пункту профиля (школа, ВУЗ и т.д.): первая — из информации, которую пользователь сам указал о себе; вторая — из анализа аккаунтов в других социальных сетях; третья — из анализа социальных связей. В случае совпадения двух или трёх гипотез будем считать, что информация соответствует истине. Если же гипотезы не совпадают или не все представлены, то верной будем считать третью. В приложении Г представлен листинг кода для идентификации города пользователя на основании информации, извлекаемой из его социального окружения в социальной сети ВКонтакте.

На данный момент реализованы методы и алгоритмы восстановления информации о городе проживания пользователя, родном городе и годе рождения. Для каждого из этих параметров, входящих в мета-профиль пользователя, разработаны свои алгоритмы, в силу отличающейся специфики анализа. На рисунке 15 представлена блок-схема алгоритма для восстановления информации о текущем городе проживания пользователя.

Тесты показывают, что при увеличении глубины анализа социального окружения, наблюдается рост точности идентификации недостающей информации, за счёт агрегации большего количества параметров. Т.е. для определения города проживания у пользователя используется не только информация его друзей, которые указали в анкете город проживания, но и оценки по такому же принципу нужного параметра у остальных друзей. Отметим, что при увеличении глубины анализа будет расти вычислительная сложность алгоритма. Для глубины 1 вычислительная сложность сравнима с $O\left(n^2\right)$, для глубины 2 — с $O\left(n^3\right)$, где n — это среднее количество друзей пользователя. Для определения недостающей информации предлагается использовать анализ глубиной 1.

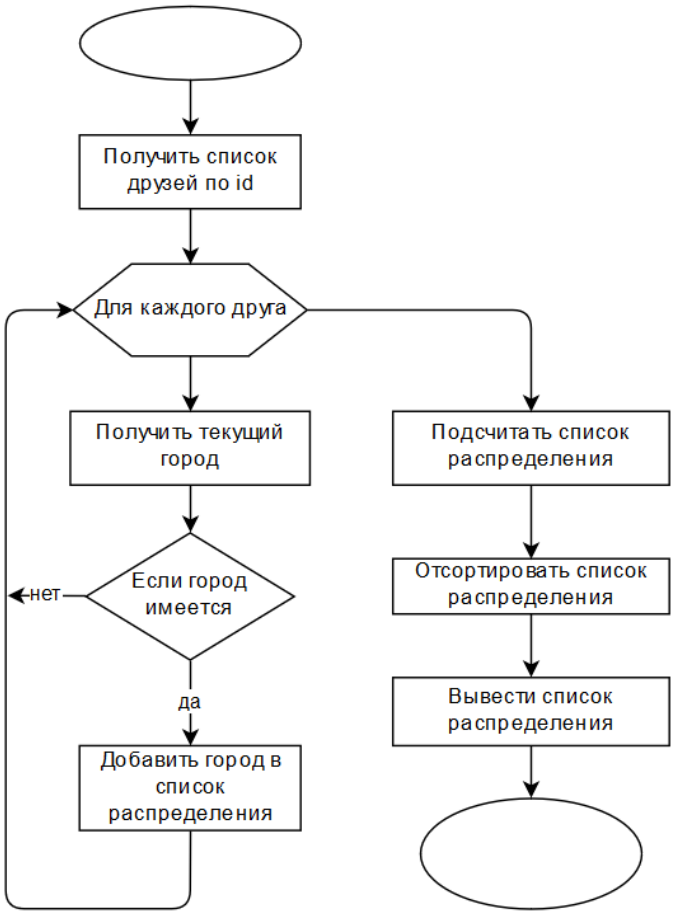


Рисунок 15 — Блок-схема алгоритма восстановления информации о городе проживания пользователя

Для определения возраста пользователя в случае, если он не указан в анкете, предлагается использовать другой алгоритм. К сожалению, опираться на методику, применяемую при определении города, в данном случае не удастся, поскольку значительно меньшее число пользователей социальных сетей не скрывают свой возраст, чем число пользователей, не скрывающих город [186]. Зачастую информацию о возрасте пользователя можно извлечь исходя из анализа данных его анкеты, таких как год обучения в школе, годы обучения в ВУЗе и т.п. Помимо этого, если указано место обучения, но не указан период, анализируются аккаунты пользователей — друзей текущего, у которых место обучения совпадает. Извлекается информация об их возрасте и делается предположение о том, что

возраст анализируемого пользователя совпадает с найденным значением. Программная реализация этого метода представлена в приложении Д. На рисунке 16 представлена блок-схема данного алгоритма.

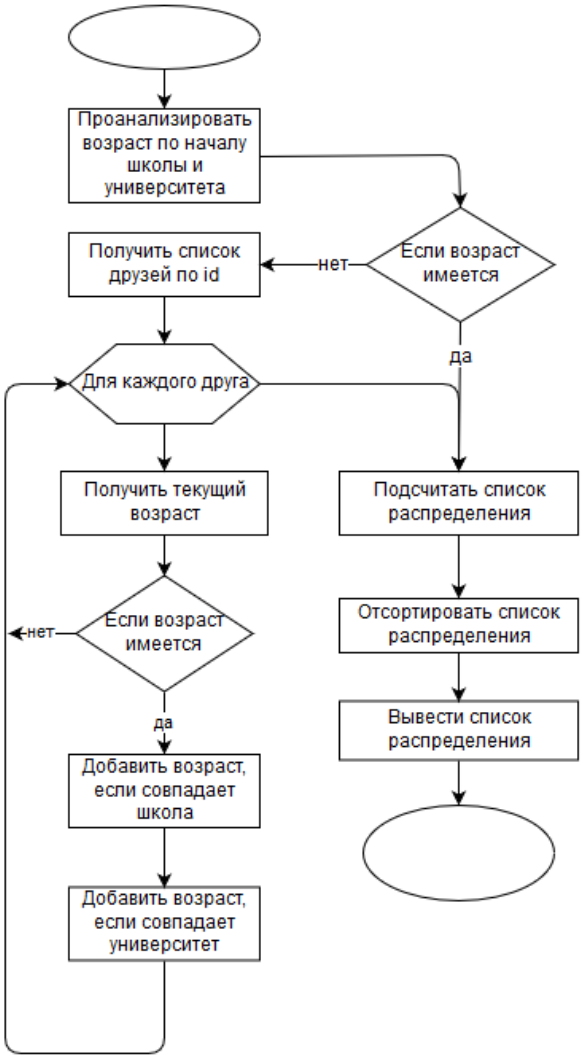


Рисунок 16 — Блок-схема алгоритма восстановления информации о возрасте пользователя

Таким образом, использование представленных методов восстановления фрагмента мета-профиля пользователя информационной системы даёт возможность оперировать расширенным объемом информации, что способствует построению оценки степени выраженности ряда особенностей его личности и последующего построения профиля уязвимостей пользователей информационной системы компании. При этом за счёт ав-

томатизация процесса сбора анкетных данных сокращается время, необходимое для ввода информации в систему оценки защищённости от социоинженерных атак.

3.3.5. Метод оценки вероятности успеха многоходовой социоинженерной атаки

В данном разделе представлено решение задачи разработки моделей и алгоритмов распространения социоинженерной атаки на прореженном социальном графе компании [22] и описанию методов расчёта оценок защищённости пользователей информационной системы от многоходовых социоинженерных атак, т.е. атак, где цель и точка входа не совпадают. Модели для оценки вероятности успеха многоходовой социоинженерной атаки на основании интенсивности взаимодействия между пользователями представлены в разделе 3.2.4. Ниже представлен подход к сбору и анализу сведений об интенсивности взаимодействия между пользователями. С точки зрения вычислений, цель состоит в разработке алгоритма расчёта вероятностей (оценок вероятностей) успеха социоинженерных атак. Данный алгоритм агрегирует информацию о следующих параметрах: наличие пользователей друг у друга в семейном положении, в публичных списках друзей (лучшие друзья, родственники, коллеги и т.д.), наличие общих фотографий (определяется по отметкам), интенсивность взаимной активности на страницах друг друга, выраженной в отметках «Мне нравится» (иными словами, в лайках) и репостах, пересечение в подписках и друзьях.

Исходя из подхода, представленного выше, для оценки вероятности успеха прохождения многоходовой социоинженерной атаки через сотрудников компании, необходимо определить интенсивность их взаимодействия между собой. Это можно сделать разными способами, например, прибегнув к экспертным оценкам. В диссертации предлагается подход к

оценке вероятности прохождения атаки между сотрудниками, основанный на интенсивности связей между ними, определяемом через анализ аккаунтов в социальных сетях.

Для оценки вероятностей успеха распространения многоходовой социоинженерной атаки строится социальный граф сотрудников компании. В социальном графе множество вершин сопоставлено множеству сотрудников компании, а множество рёбер — связями между ними. Отметим, что в общем случае в начале построения данный граф будет являться полным, поскольку каждая пара вершин будет смежной, и неориентированным. Ниже будут рассмотрены подходы к разрежению социального графа. Перейдём к расчёту оценок вероятностей успеха перехода от пользователя к пользователю при распространении социоинженерной атаки на рёбрах социального графа.

В подходе, предложенном ранее [96], вероятности успешности атаки на пользователя через другого пользователя задавались экспертно на основании характера их взаимоотношений. Такой подход является затруднительным для крупных компаний, где работает существенное количество сотрудников. Даже для относительно небольших компаний, например, состоящих из 20 человек, необходимо будет оценить вероятности перехода по 190 связям. При этом отметим, что отношения между сотрудниками в коллективе могут меняться с течением времени, что будет приводить к необходимости корректировки оценок вероятностей успеха распространения социоинженерной атаки. Таким образом, автоматизация процесса сопоставления дугам графа социальных связей оценок вероятностей успеха прохождения социоинженерной атаки через них позволит, в конце концов, сэкономить время на анализе степени защищенности. Предлагается подход к расчёту этих оценок вероятностей, основанный в свою очередь на оценке вероятности перехода по данной дуге, причем эта оценка строится на основе сведений об интенсивности общения

между соответствующей парой сотрудников. Оценки вероятности предполагается рассчитывать, исходя из общедоступных данных, публикуемых в социальных сетях.

Пусть p_{rel} — вероятность успеха распространения атаки от сотрудника к сотруднику, основанная на типе декларируемой в социальной сети связи. Тогда

$$p_{\text{rel}} = \begin{cases} p_0, \text{ (0) если пользователи отметили друг друга в графе семейное положение;} \\ p_1, \text{ (1) если пользователи находятся в публичных списках лучших друзей, но не (0);} \\ p_2, \text{ (2) если пользователи находятся в друзьях, но не (1);} \\ p_3, \text{ (3) если кто-то из пользователей подписан на другого, но не (2);} \\ p_4, \text{ (4) ничего из выше перечисленного.} \end{cases}$$

Также отметим, что $p_0 > \ldots > p_4$. Введём оценки вероятностей $p_{\text{likes}}, p_{\text{reposts}}, p_{\text{com\_photos}}, p_{\text{com\_groups}}$, характеризующие соответственно вклад отдельного эпизода каждого типа связи в оценку вероятности успеха распространения атаки от сотрудника к сотруднику. Кумулятивный вклад каждого типа связи тогда рассчитывается на основании числа лайков, репостов, общих фотографий и сообществ. При таких предположениях вероятности того, что социоинженерная атака не завершится успехом при одном эпизоде определенного типа связи, соответственно будут

$$1 - p_{\text{rel}}; 1 - p_{\text{likes}}; 1 - p_{\text{reposts}}; 1 - p_{\text{com\_photos}}; 1 - p_{\text{com\_groups}}.$$

Теперь требуется построить модель так, чтобы каждый эпизод в зависимости от типа связи вносил свой вклад в снижение оценки степени защищенности (если сформулировать строже — ожидаемого значения оценки степени защищенности).

Для этого используется модель Белла-Тревино, описанная выше. В рассматриваемом случае в качестве числа эпизодов (в данном контексте это число — характеристика интенсивности связи) будут выступать количественные показатели, извлекаемые из аккаунтов в социальных сетях

(число лайков, репостов, совместных фотографий, общих сообществ). Таким образом, оценка вероятности того, что социоинженерная атака не распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться по формуле

$$Q = (1-p_{\text{rel}})(1-p_{\text{likes}})^{\text{count\_likes}}(1-p_{\text{reposts}})^{\text{count\_reposts}}(1-p_{\text{com\_photos}})^{\text{count\_photos}}(1-p_{\text{com\_groups}})^{\text{count\_groups}},$$

где count_likes — сумма лайков пользователей друг другу, count_reposts — сумма репостов каждым записей другого, count_photos — число совместных фотографий, на которых отмечен другой пользователь, count_groups — число групп и публичных страниц, на которые подписаны оба пользователя. Вероятности того, что социоинженерная атака распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться как вероятность дополнения указанного выше события «атака не распространится»:

$$P = 1-Q.$$

Таким образом, алгоритм расчёта оценок вероятностей успеха социоинженерных атак сводится к сбору информации из социальных сетей о связях пользователей [58], построению возможных, с точки зрения накопленной информации, деревьев атак [96] и агрегации полученной информации с помощью формул представленных выше формул для P и Q.

Численный пример. Методика оценки такого рода параметров $p_0,...,p_4,p_{\text{likes}},p_{\text{reposts}},p_{\text{com\_photos}},p_{\text{com\_groups}}$ разрабатывается особо, более того, такие методики, неизбежно учитывающие широкий спектр сведений от экспертов, информационных источников, в т.ч. из систем, обрабатывающих большие данные, поддержанные или реализованные в интеллектуальных (когнитивных) системах, могут оказаться проприетарными, входящими в систему знаний организации, которые позволяют ей конкурировать на рынке [29]; но в иллюстративном вычислительном примере рассмотрим следующий набор значений:

$p_0 = 0.8,$ $p_3 = 0.4,$ $p_{\text{reposts}} = 0.5,$

$p_1 = 0.7,$ $p_4 = 0.2,$ $p_{\text{com\_photos}} = 0.6,$

$p_2 = 0.6,$ $p_{\text{likes}} = 0.3,$ $p_{\text{com\_groups}} = 0.2.$

Таким образом, в качестве примера, посчитаем значение оценки вероятности успеха прохождения атаки на одного пользователя через другого при следующих исходных данных. Пусть

- два пользователя состоят друг у друга в друзьях и не отмечены ни в семейном положении, ни в публичных списках лучших друзей;
- первый поставил второму один лайк, второй первому — ни одного лайка;
- не делали репостов друг друга;
- имеют одну совместную фотографию;
- имеют две общих подписки на сообщества.

В этом случае оценка вероятности успешного прохождения атаки на одного пользователя через другого, будет рассчитываться так:

$$P_{i,i+1} = 1-(1-p_{\text{rel}})(1-p_{\text{likes}})^{\text{count\_likes}}(1-p_{\text{reposts}})^{\text{count\_reposts}}(1-p_{\text{com\_photos}})^{\text{count\_photos}} \cdot$$

$$\cdot(1-p_{\text{com\_groups}})^{\text{count\_groups}} = 1-(1-0.6)(1-0.3)^1(1-0.5)^0(1-0.6)^1(1-0.2)^2 \approx 0.93.$$

Описанным выше образом предлагается рассчитывать оценки вероятностей успеха прохождения атаки на сотрудника через другого сотрудника для всех пар сотрудников компании. Данные вероятности будут в свою очередь использоваться для расчёта оценок вероятности успеха многоходовой социоинженерной атаки на основании моделей, представленных выше.

Таким образом, представленный подход позволяет сопоставлять рёбрам социального графа оценки вероятностей успеха распространения многоходовой социоинженерной атаки злоумышленника на пользователя на основании данных, получаемых из социальной сети. Отметим, что в иллюстративных целях были взяты определённые оценки вероятности

отдельного эпизода каждого типа связи в оценку вероятности успеха распространения атаки от сотрудника к сотруднику. В идеальном случае получить эти оценки можно исходя из опроса экспертов в анализируемой компании, но не всегда это возможно. Для оценки точности предлагается использовать метод Монте-Карло [31, 33, 67, 116]. Рассмотрим распределения вероятности $P_{i,i+1}$, полученные методом Монте-Карло для указанного выше примера для разных распределений вероятностей отдельных эпизодов каждого типа связи между сотрудниками в компании. При равномерно распределённых вероятностей отдельных эпизодов каждого типа связи между сотрудниками в компании на всём отрезке $[0,1]$ медиана и среднее будут иметь значения близкие к 0, а 90% доверительный интервал будет $(0.000048, 0.19)$ (рисунок 17).

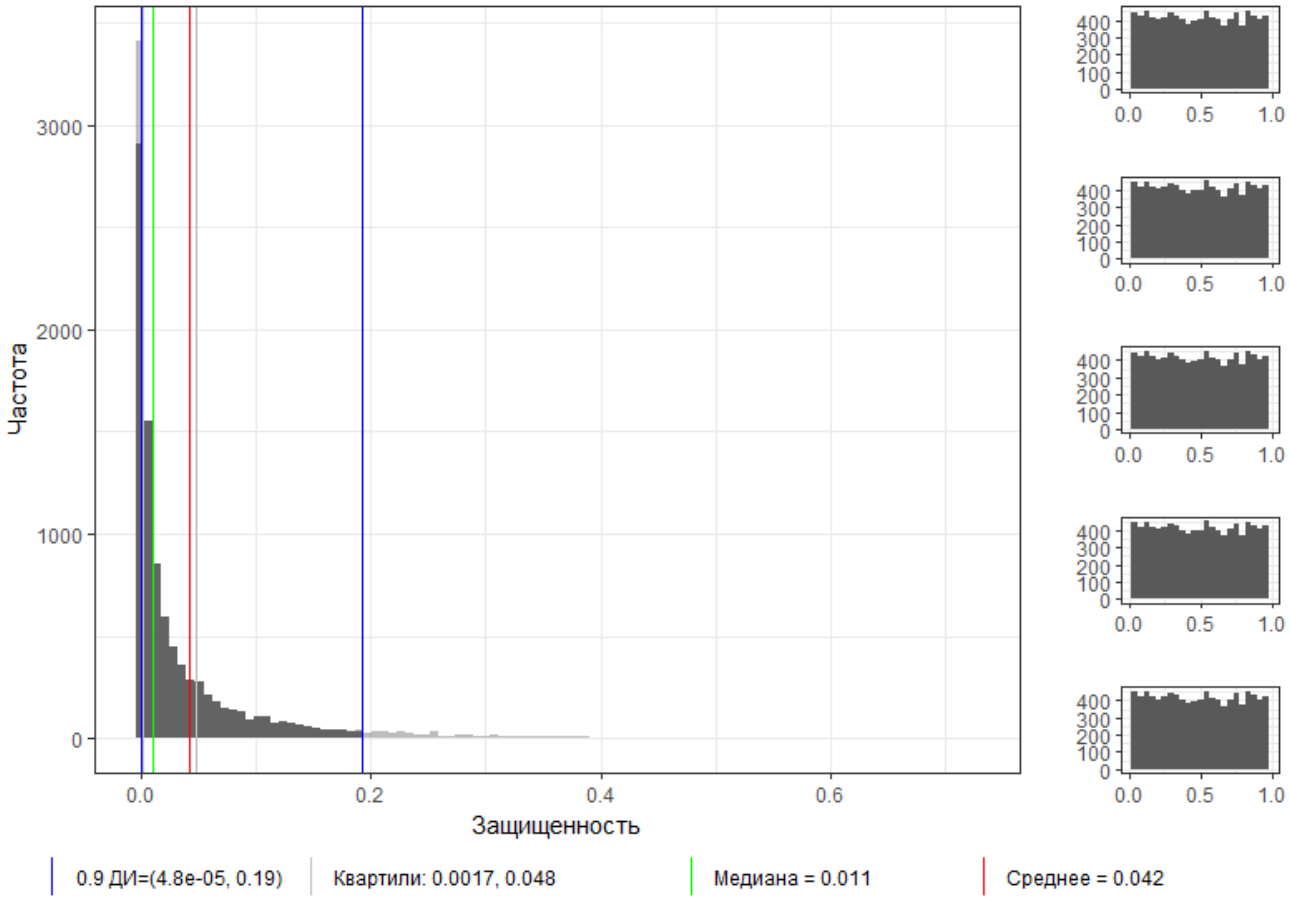


Рисунок 17 — Метод Монте-Карло для равномерно распределённых значений вероятностей $p_t^{i,i+1} \in [0,1]$

При этом ожидается, что вероятность успеха социоинженерной атаки злоумышленника на пользователя по одной связи будет невысокой. Рассмотрим случай при том же распределении вероятностей отдельных эпизодов каждого типа связи между сотрудниками в компании, с учётом того, что $p_t^{i,i+1} \in [0;0.5]$ (рисунок 18). В этом случае медиана и среднее совпадают и равняются 0.25, а 90% доверительный интервал — $(0.089,0.49)$ (рисунок 18).

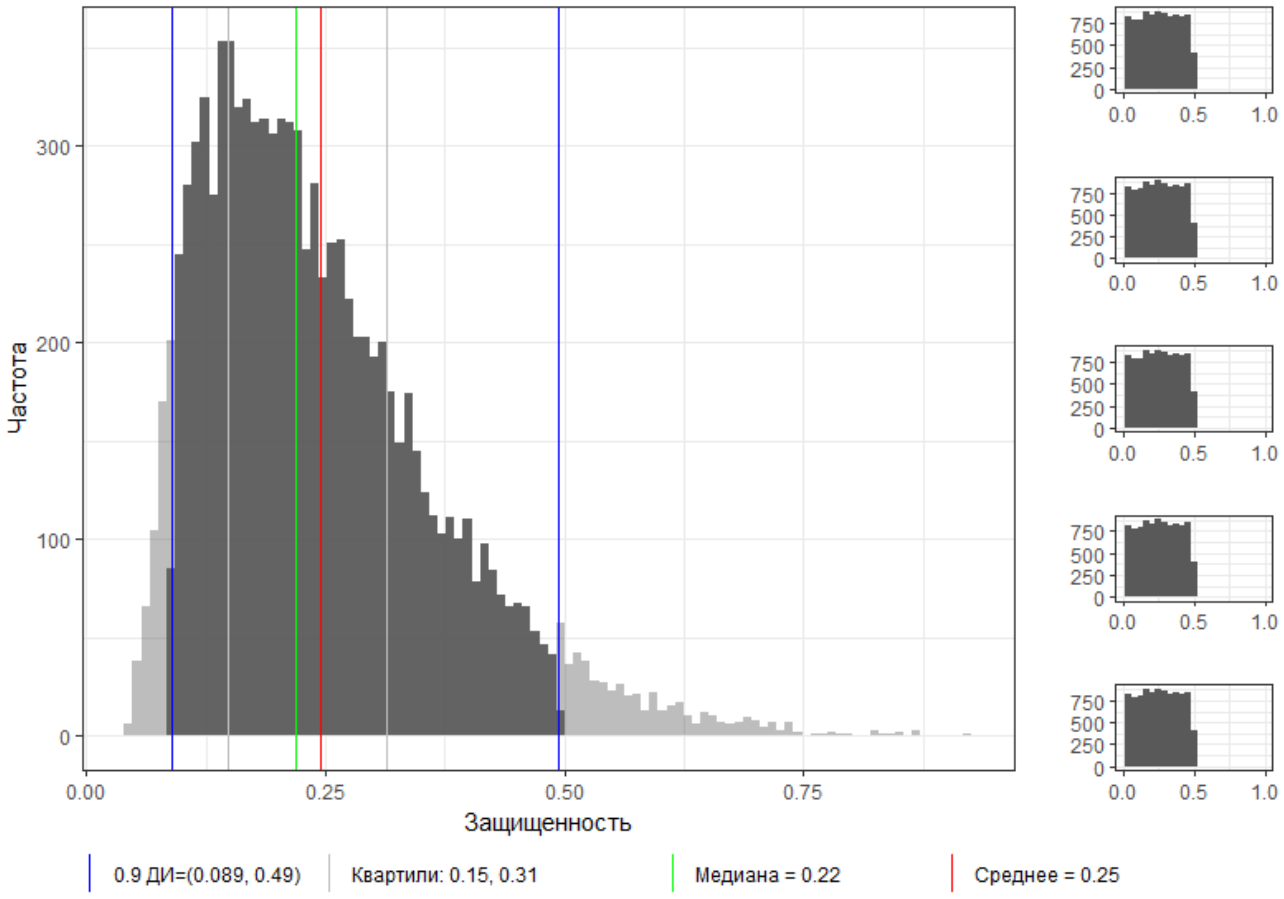


Рисунок 18 — Метод Монте-Карло для равномерно распределённых значений вероятностей $p_t^{i,i+1} \in [0,0.5]$

На рисунках 19–24 представлены распределения вероятности $P_{i,i+1}$, полученные методом Монте-Карло для бета-распределения $p_t^{i,i+1}$ с разными параметрами и ограничениями на $p_t^{i,i+1}$.

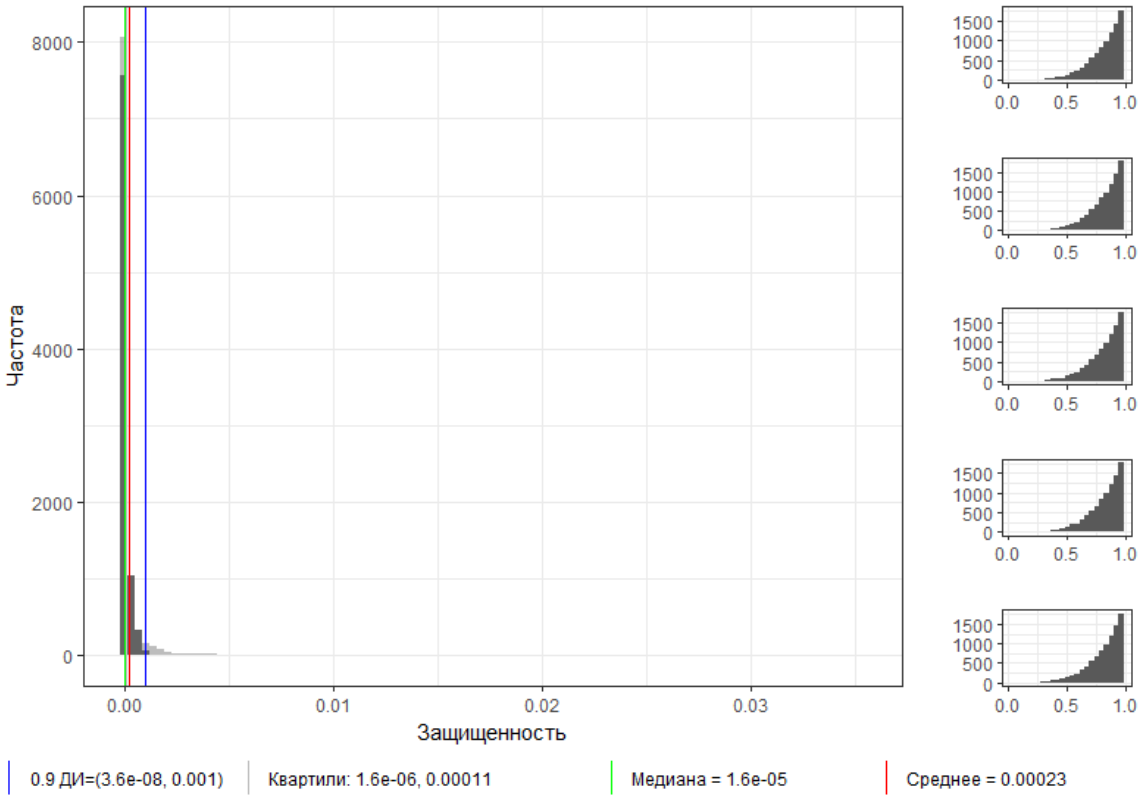


Рисунок 19 — Метод Монте-Карло для бета-распределённых значений вероятностей $p_t^{i,i+1} \in [0,1]$ с параметрами 5, 1

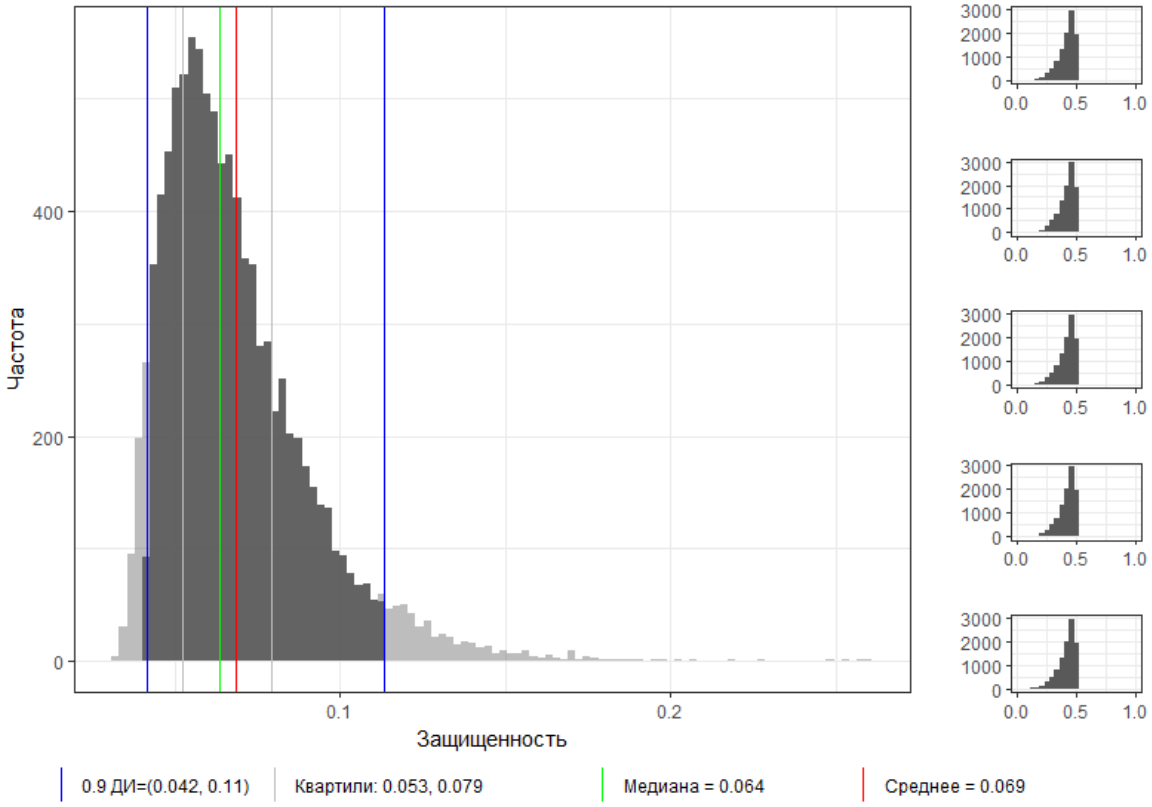


Рисунок 20 — Метод Монте-Карло для бета-распределённых значений вероятностей $p_t^{i,i+1} \in [0,0.05]$ с параметрами 5, 1

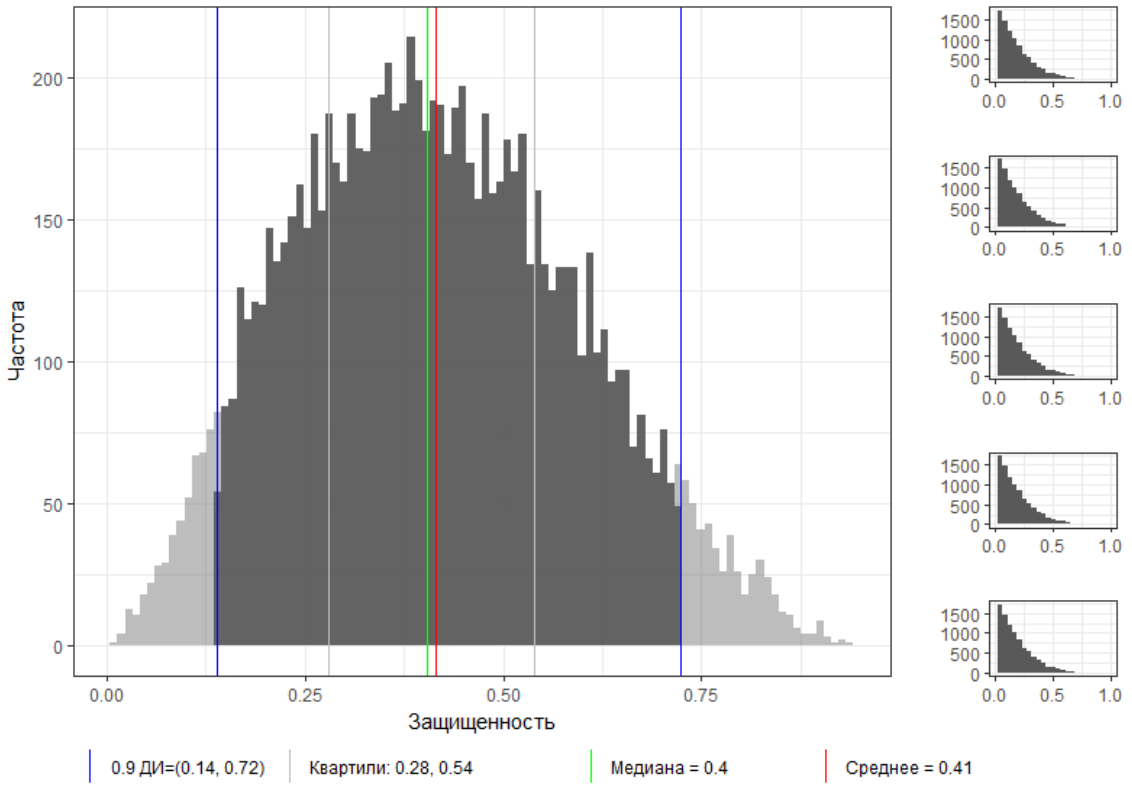


Рисунок 21 — Метод Монте-Карло для бета-распределённых значений вероятностей $p_t^{i,i+1} \in [0,1]$ с параметрами 1, 5

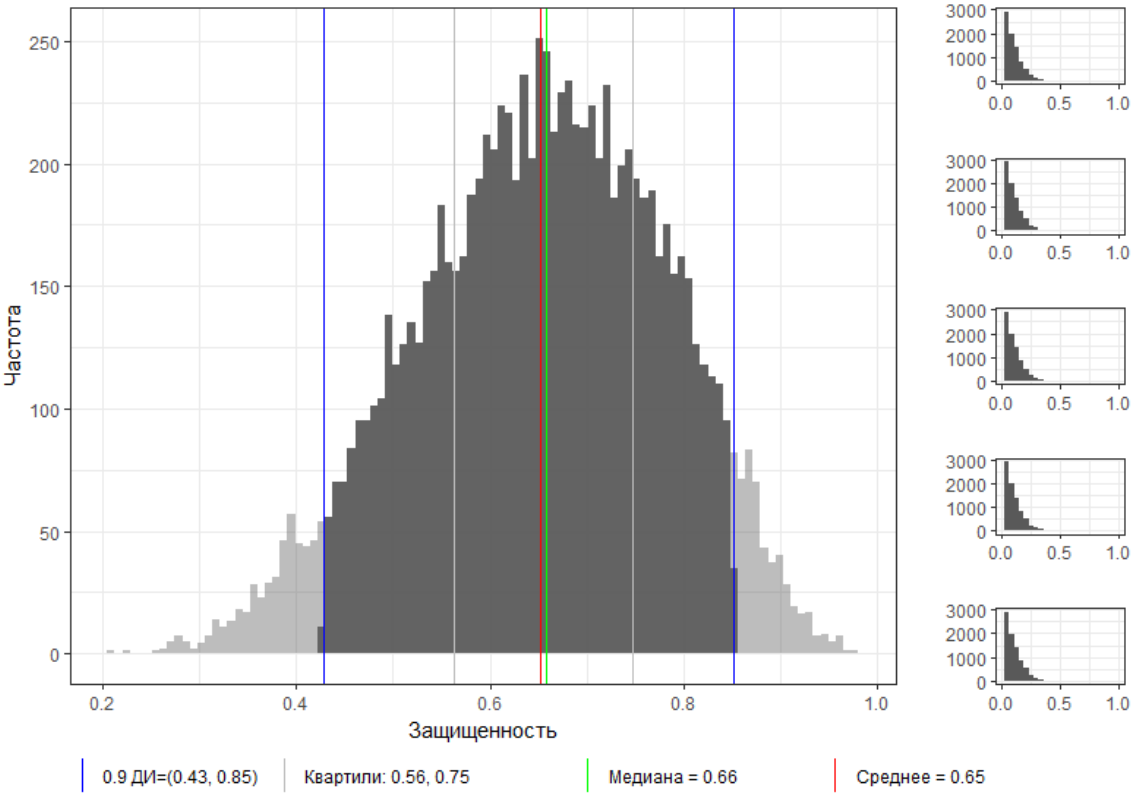


Рисунок 22 — Метод Монте-Карло для бета-распределённых значений вероятностей $p_t^{i,i+1} \in [0,0.05]$ с параметрами 1, 5

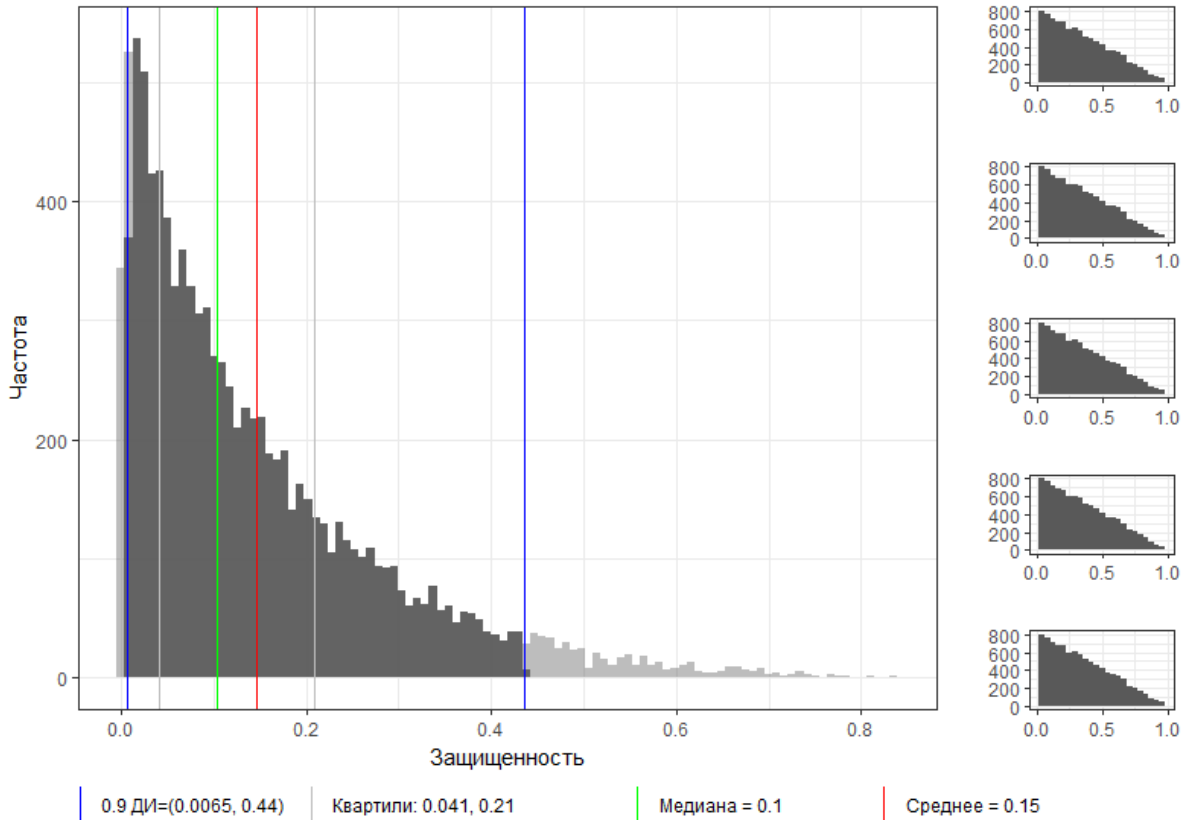


Рисунок 23 — Метод Монте-Карло для бета-распределённых значений вероятностей $p_t^{i,i+1} \in [0,1]$ с параметрами 1, 2

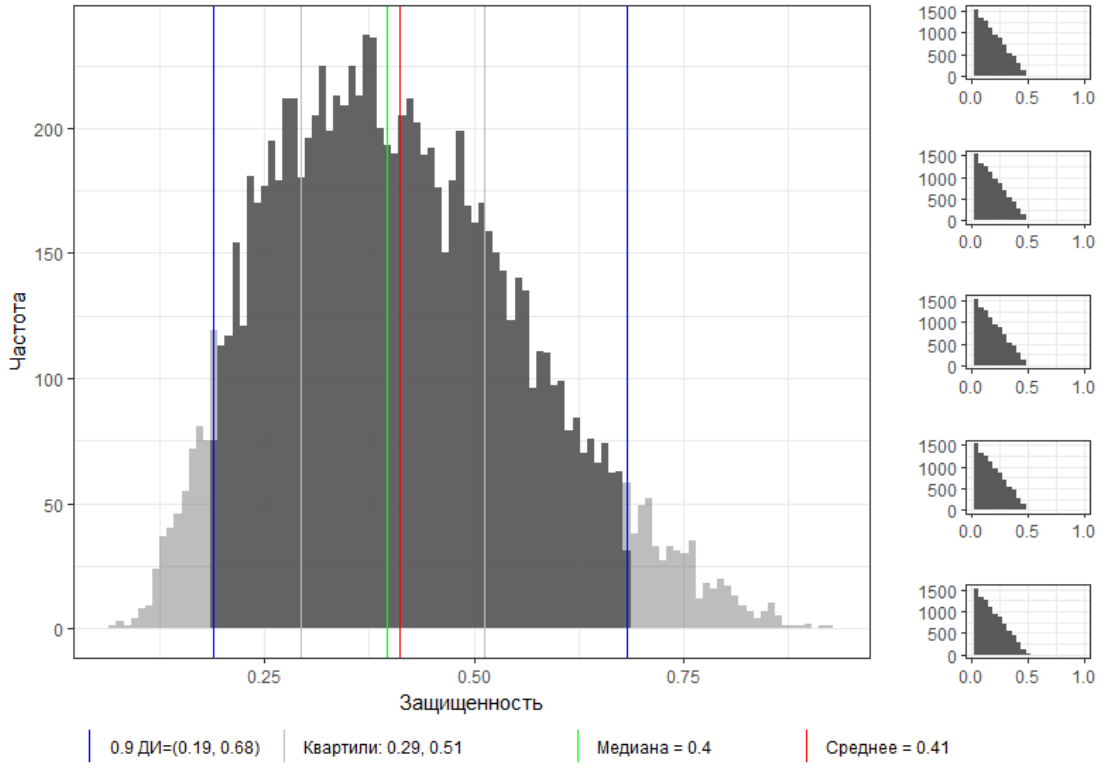


Рисунок 24 — Метод Монте-Карло для бета-распределённых значений вероятностей $p_t^{i,i+1} \in [0,0.05]$ с параметрами 1, 2

Отметим, что модель расчёта оценок защищённости пользователей информационных систем от многоходовых социоинженерных атак строится на основе агрегации оценок всех возможных траекторий реализации социоинженерной атаки на каждого пользователя. Разработанная программная реализация строит социальный граф компании и производит на нём расчёт оценок вероятности успеха перехода злоумышленника от пользователя к пользователю, на основании агрегации информации, извлекаемой из социальной сети ВКонтакте. Рёбрам социального графа сопоставлены оценки вероятностей, которые отражают характер интенсивности взаимодействия между сотрудниками (метод расчёта этих оценок описан выше). Изначально строится полный социальный граф (рисунок 25), обработка которого является довольно проблематичной в реализации задач аналитического моделирования даже для относительно небольшого числа сотрудников. Хранение и обработка такого графа требует больших затрат памяти и лишней работы процессора. Для иллюстрации этого факта возьмём среднюю компанию с численностью сотрудников 80 человек. Получим следующие показатели для числа рёбер и опосредованных атак, состоящих из цепочек, включающих трёх сотрудников.

$K_{80} = \frac{80(80-1)}{2} = 3160$; $A_{100}^{3} = 80 \cdot 79 \cdot 78 = 492960$, где K_{80} — число рёбер в социальном графе, состоящем из 80 сотрудников, а A_{80}^{3} — число цепочек, включающих трёх сотрудников. Таким образом, для достижения приемлемой сложности вычислений потребуется «проредить» полный граф.

Можно говорить о трех ключевых подходах к обработке и анализу получаемого социального графа:

1. Анализ полного графа — как контрольный образец (иными словами, «золотой стандарт» — теоретически идеальный, но дорогостоящий и в реальных задачах вычислительно недостижимый), используемый для сравнения с результатами анализа, полученными в соответствии с другими подходами;

2. Использование ограничений, связанных с устройством, организацией деятельности компании — как часто применяемый ограничитель, имеющий свои плюсы и минусы. В этом случае рёбра исключаются на основании экспертных оценок;
3. Использование пороговых значений — наиболее универсальный и допускающий автоматизацию способ, когда устанавливается минимальное значение для оценок вероятностей, а рёбра с оценками меньше этого значения исключаются из рассмотрения.

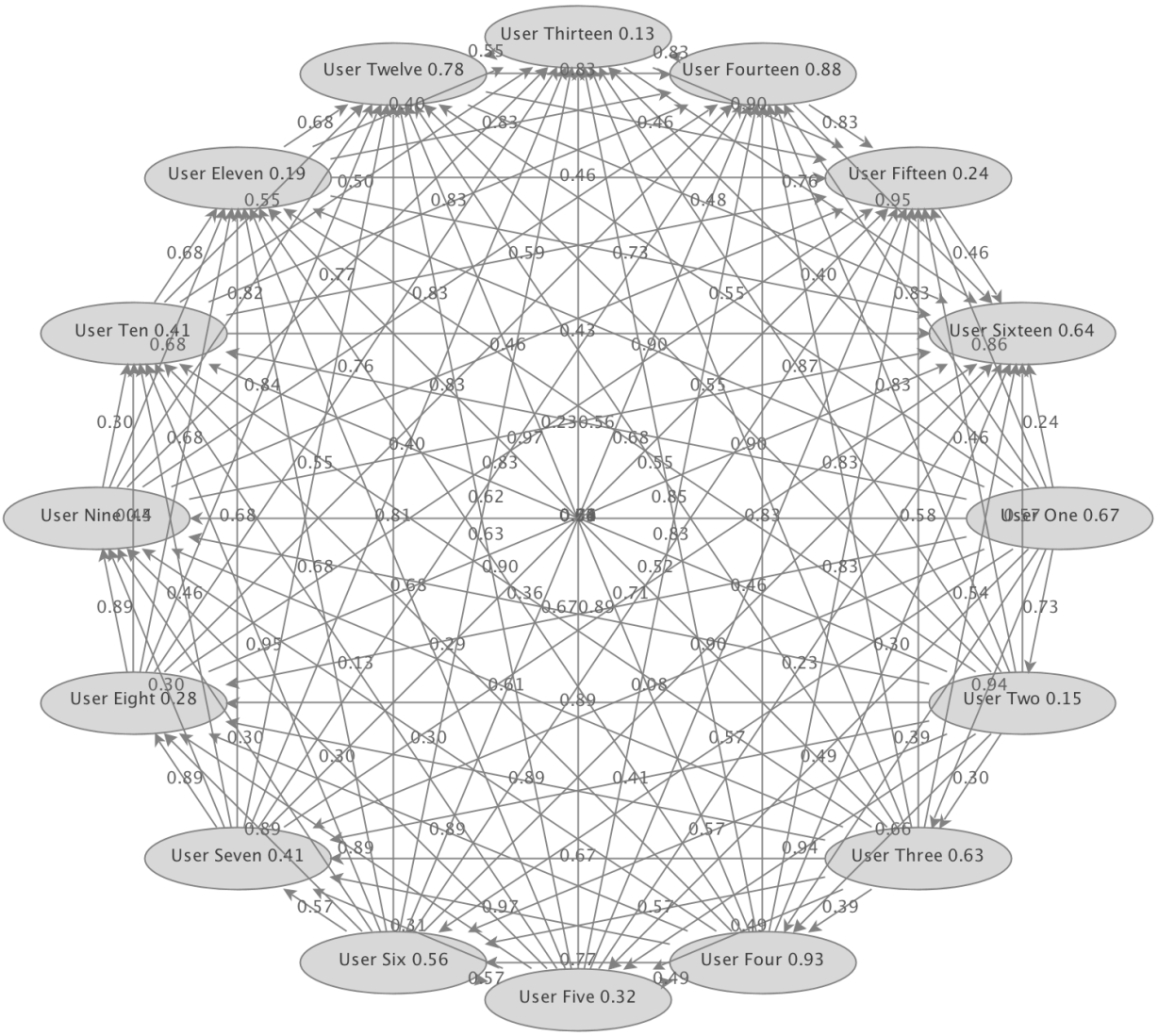


Рисунок 25 — Шаг первый — построение полного графа

Два последних подхода как раз позволяют вести вычисления на графе, более разреженном, чем полный социальный граф. В разрабаты-

ваемом алгоритме используется третий подход из приведенных выше, который позволяет при расчетах существенно сократить число рёбер, как предполагается, без существенной потери точности оценки вероятности успеха социоинженерной атаки, в силу того, что из рассмотрения исключаются малые вероятности, оказавшиеся ниже заданного порога. Компромиссы в отношении точности и скорости вычислений такого рода дискутировались в [15]. На рисунках 23–26 изображён граф для компании, состоящей из 16 человек, который был построен с помощью разработанного программного модуля, на дугах отмечены вероятности успеха распространения социоинженерной атаки, а в вершинах оценки вероятности успеха прямой социоинженерной атаки злоумышленника на пользователя, основанной на профиле уязвимостей пользователя. На рисунках 24–26 представлены примеры разрежения этого социального графа для разных пороговых значений оценок вероятности успеха распространения социоинженерной атаки по дуге.

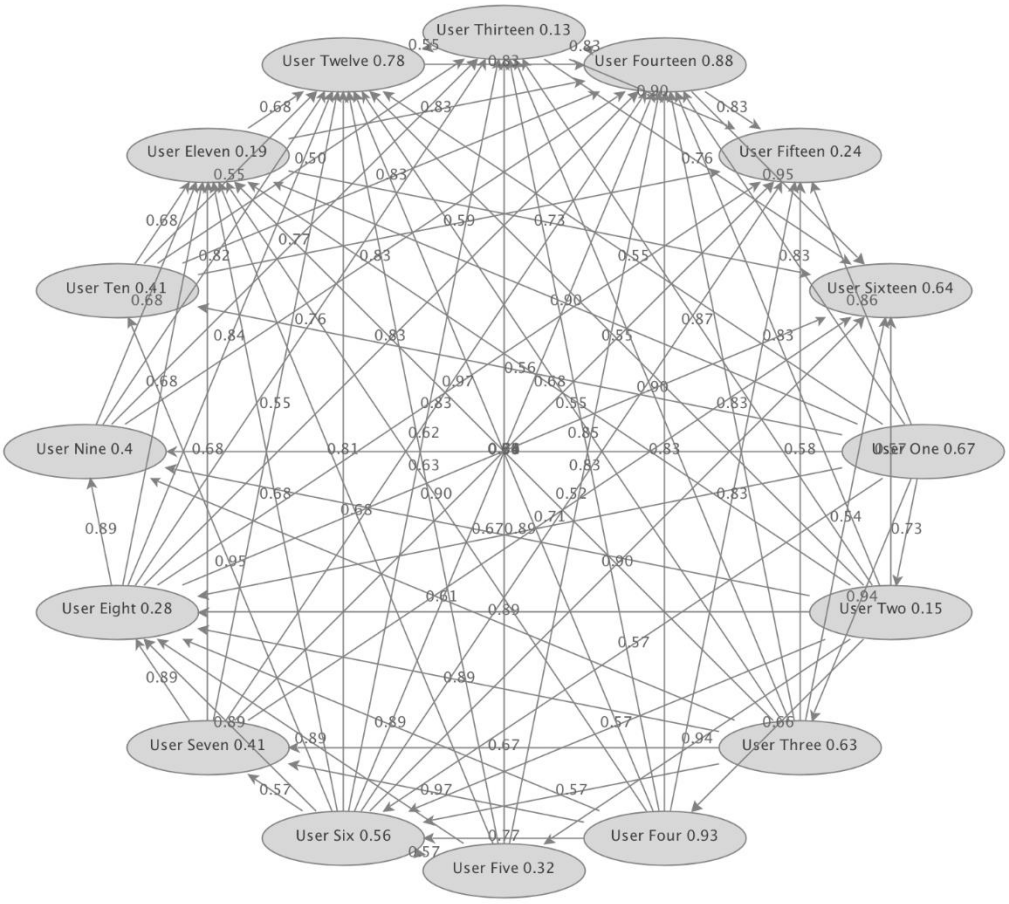


Рисунок 26 — Шаг второй — разрежение графа (50% дуг от полного графа)

Рисунок 27 — Шаг третий — разрежение графа (20% дуг от полного графа)

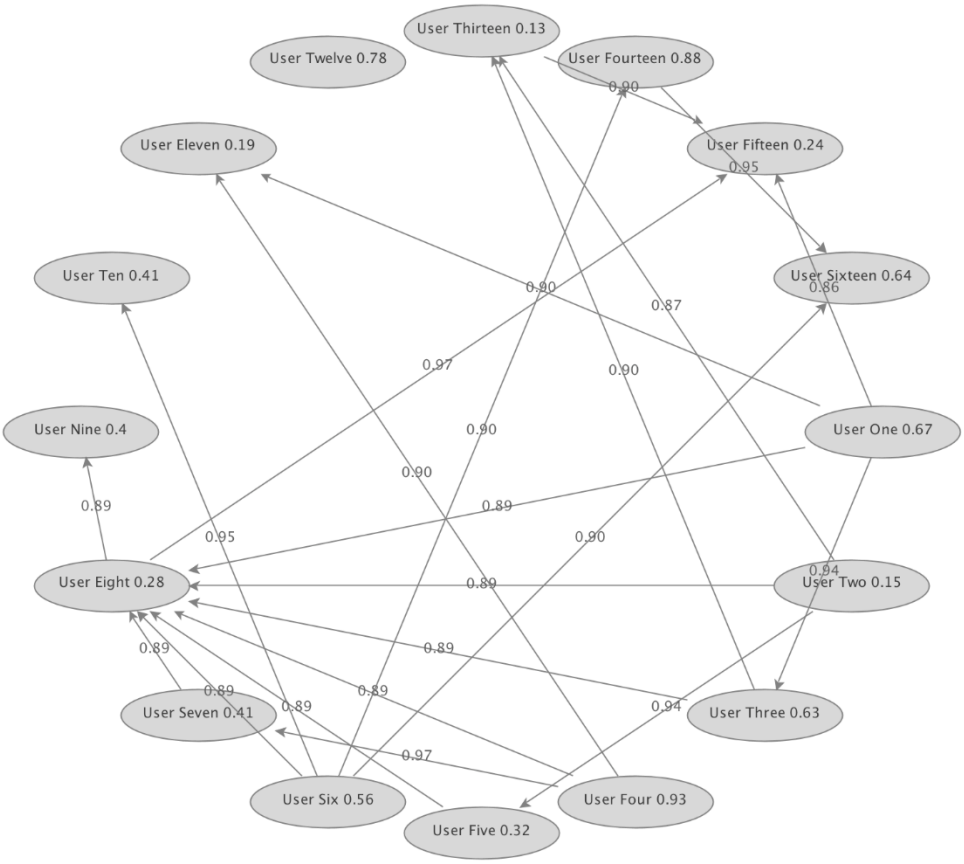


Рисунок 28 — Шаг четвёртый — разрежение графа (10% дуг от полного графа)

Для иллюстрации модели приведём расчёт оценки вероятности успеха атаки на пользователя Eleven. Так, например, оценка вероятности успеха атаки на пользователя Eleven через пользователей Eight, Seven, Four будет рассчитываться по формуле: $\tilde{P}_{8,7,4,11} = P_8\tilde{P}_{8,7}\tilde{P}_{7,4}\tilde{P}_{4,11} = 0.28 \cdot 0.89 \cdot 0.97 \cdot 0.9 \approx 0.22$. Также существуют другие траектории в социальном графе сотрудников компании, по которым может распространяться социоинженерная атака. Для иллюстративных целей допустим, что по результатам учёта ряда факторов оказались приняты к рассмотрению ещё четыре траектории, ведущие к пользователю Eleven: Eight, Seven, Four, Eleven; Six, Eight, Four, Eleven; Nine, Eight, Four, Eleven; Thirteen, Fifteen, One, Eleven; Eight, Three, One, Eleven (вопросы генерации деревьев атак рассмотрены в [97]). Оценка вероятности успеха распространения социоинженерной атаки по первой траектории рассчитана выше, оценим таким же образом оставшиеся траектории.

$$\tilde{P}_{6,8,4,11} = P_6\tilde{P}_{6,8}\tilde{P}_{8,4}\tilde{P}_{4,11} = 0.56 \cdot 0.89 \cdot 0.89 \cdot 0.9 \approx 0.4;$$

$$\tilde{P}_{9,8,4,11} = P_9\tilde{P}_{9,8}\tilde{P}_{8,4}\tilde{P}_{4,11} = 0.4 \cdot 0.89 \cdot 0.89 \cdot 0.9 \approx 0.28;$$

$$\tilde{P}_{13,15,1,11} = P_{13}\tilde{P}_{13,15}\tilde{P}_{15,1}\tilde{P}_{1,11} = 0.13 \cdot 0.9 \cdot 0.86 \cdot 0.9 \approx 0.09;$$

$$\tilde{P}_{8,3,1,11} = P_8\tilde{P}_{8,3}\tilde{P}_{3,1}\tilde{P}_{1,11} = 0.28 \cdot 0.89 \cdot 0.94 \cdot 0.9 \approx 0.21.$$

В таком случае оценка вероятности того, что злоумышленник-социоинженер не сможет успешно атаковать пользователя будет следующей:

$$Q_{11} = \prod_5 \left(1 - \tilde{P}_{m-\ldots-i_k-\ldots-11}\right) = (1-\tilde{P}_{8,7,4,11})(1-\tilde{P}_{6,8,4,11})(1-\tilde{P}_{9,8,4,11})(1-\tilde{P}_{13,15,1,11})(1-\tilde{P}_{8,3,1,11}) \approx$$
$$\approx 0.24,$$

а вероятность успеха атаки составит $P_f = 1 - Q_f \approx 0.76$.

Таким образом, представлен подход к агрегации сведений, извлекаемых из социальных сетей, для построения оценок вероятностей успешного распространения многоходовой социоинженерной атаки от пользователя к пользователю, обозначенные на дугах социального графа, а

также подход к оценке вероятности успеха социоинженерной атаки злоумышленника на пользователя с учётом возможных траекторий атаки. Полученные результаты создают перспективы для дальнейших исследований, связанных с последующим анализом возможных траекторий распространения многоходовых социоинженерных атак, что позволяет агрегировать расширенный набор параметров, влияющих на оценку защищённости пользователей информационных систем от социоинженерных атак.

3.4. ВЫВОДЫ ПО ГЛАВЕ 3

В главе представлены модели комплекса «критичные документы – информационная система – пользователь – злоумышленник», на их основе предложены вероятностные модели и метод для построения оценок защищённости пользователей информационных систем, оценок вероятности поражения критичных документов, оценок вероятности успеха социоинженерной атаки злоумышленника на пользователя. Разработаны метод, модель и алгоритмы автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, а также оценки степени выраженности некоторых особенностей пользователей на основании текстового и аудио контента. Приведены методы, позволяющие восстановить фрагмент мета-профиль пользователя социальной сети ВКонтакте на основании альтернативной информации, извлекаемой из других социальных сетей или исходя из социального окружения пользователя. Предложено автоматизированное решение задачи расчёта оценок вероятностей успеха прохождения социоинженерной атаки между пользователями на рёбрах социального графа компании, а также вывод оценок вероятности успеха многоходовой социоинженерной атаки злоумышленника на пользователя. Приведённый алгоритм создаёт основу для последующего анализа возможных траекторий распространения этих атак, что

способствует построению оценок защищённости пользователей информационной системы, агрегирующих расширенный набор параметров, влияющих на оценку. Полученные результаты обеспечивают агрегирование доступных из социальных сетей сведений о характере взаимоотношений между сотрудниками компании, интенсивности публикаций постов с текстовым или аудио контентом.

Одним из направлений дальнейших исследований является разработка методик оценки параметров, характеризующих влияние отдельных показателей на определение значения оценки вероятности. Предполагается, что методики могут опираться на экспертный подход, результаты полевых социально-психологических исследований или на комбинацию этих двух подходов. Также планируется обеспечить агрегирование информации не только из социальной сети ВКонтакте, но и других социальных сетей, а вместе с тем расширять число агрегируемых параметров для построения оценок.

Наконец, с точки зрения разработки программ превентивных вмешательств, нацеленных на предотвращение инцидентов в сфере информационной безопасности, связанных с социоинженерными атаками, учитывая то, что на тесноту/разреженность сложившихся в коллективе компании связей влиять затруднительно или бесполезно, можно пытаться уменьшить вероятность успешного использования злоумышленником той или иной связи между сотрудниками. Для этого необходимо разработать комплекс профилактических мер, среди которых могут быть такие как проведение соответствующих тренингов, ограничения (либо оптимизации распределения) прав доступа к критичным документам, перепланировки офисного пространства, а также изучить эффект от таких мер на изменение степени защищённости пользователей от социоинженерных атак.

Глава 4. ПРОТОТИП РАЗРАБОТАННОГО КОМПЛЕКСА ПРОГРАММ ДЛЯ ОЦЕНКИ ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЕЙ

В главе 4 представлены основные модули комплекса программ, предназначенного для автоматизированной оценки защищённости пользователей информационных систем от социоинженерных атак, который рассчитывает: оценки защищённости пользователей информационных систем с учётом многоходовых социоинженерных атак, оценки некоторых особенностей пользователей, служащих основой для построения профиля уязвимостей пользователя. Приведена реализация алгоритмов и методов, представленных в диссертации, использующихся для автоматизации идентификации аккаунтов сотрудников компании в социальной сети, модуля автоматизированного построения оценок степени выраженности некоторых особенностей пользователей на основании анализа данных, извлекаемых из контента, публикуемого ими в социальных сетях. Рассмотрена реализация автоматизации восстановления фрагмента мета-профиля пользователя на основании анализа данных, извлекаемых из социального окружения пользователя, а также из других социальных сетей, реализация автоматизации построения оценок вероятности успеха многоходовой социоинженерной атаки.

4.1. ОСНОВНЫЕ КОМПОНЕНТЫ КОМПЛЕКСА ПРОГРАММ

Основные компоненты разрабатываемого комплекса программ для анализа защищённости пользователей от социоинженерных атак и разработке систем упреждающей диагностики и бэктрекинга инцидентов представлена на рисунке 29.

Модуль «Поиск персонала» реализует методику идентификации аккаунтов сотрудников компании в социальной сети ВКонтакте на основании агрегации информации о различных параметрах, являющихся признаками этого.

Модуль «Психологические особенности» предназначен для автоматизированного построения профиля некоторых особенностей пользователя социальной сети ВКонтакте, как основы для последующего построения профиля уязвимостей пользователя. Данный модуль на входе получает список аккаунтов сотрудников компании в социальной сети, а на выходе выдаёт оценки некоторых особенностей личности, которые позволяют строить профили их уязвимостей.

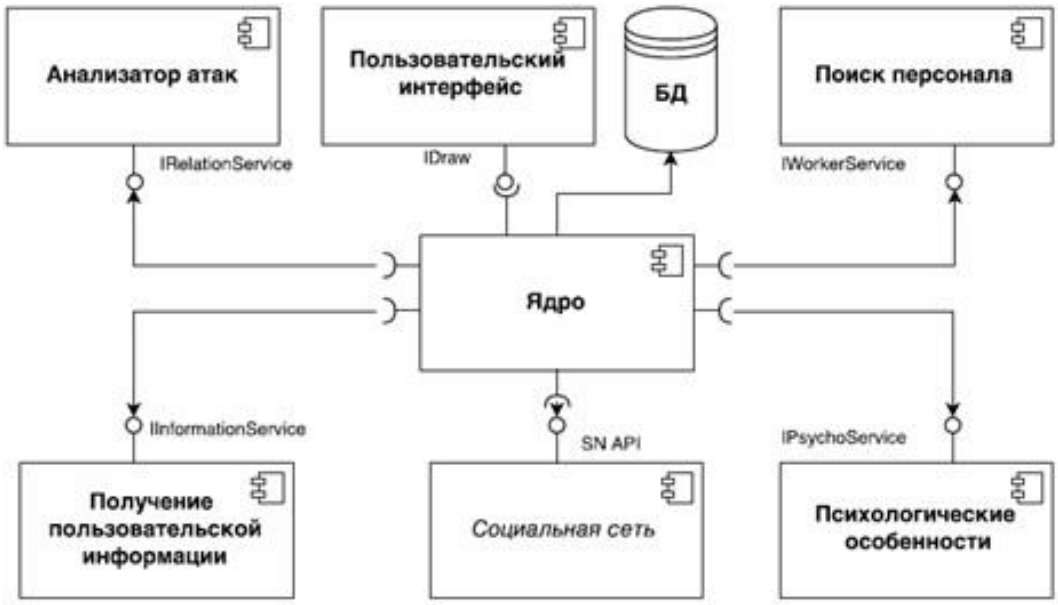


Рисунок 29 — Система компонент комплекса программ для оценки защищённости пользователя информационной системы

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 мета-профиля пользователя на основании контента, публикуемого в социальных сетях.

Архитектура протипа комплекса программ представлена на рисунке 30. На ней приведены классы, отвечающие за получение из графи-

ческого интерфейса обучающей выборки для дальнейешго поиска и идентификации аккаунтов сотрудников компании, структурировани, последующее обучение модели с помощью методов машинного обучения, построение дерева решений и классификатора аккаунтов на его основе. Также приведены классы для сбора необходимой при работе модулей информации из социальных сетей, её структурирования, расчёта оценок вероятности успеха социоионженерных атак, восстановления фрагментов мета-профиля родного города, города проживания и года рождения. Отмечены блоки, осуществляющие выгрузку, обработку и анализ постов из аккаунтов сотрудников компани, их классификацию и определение на её основе степени выраженности ряда особенностей пользователя.

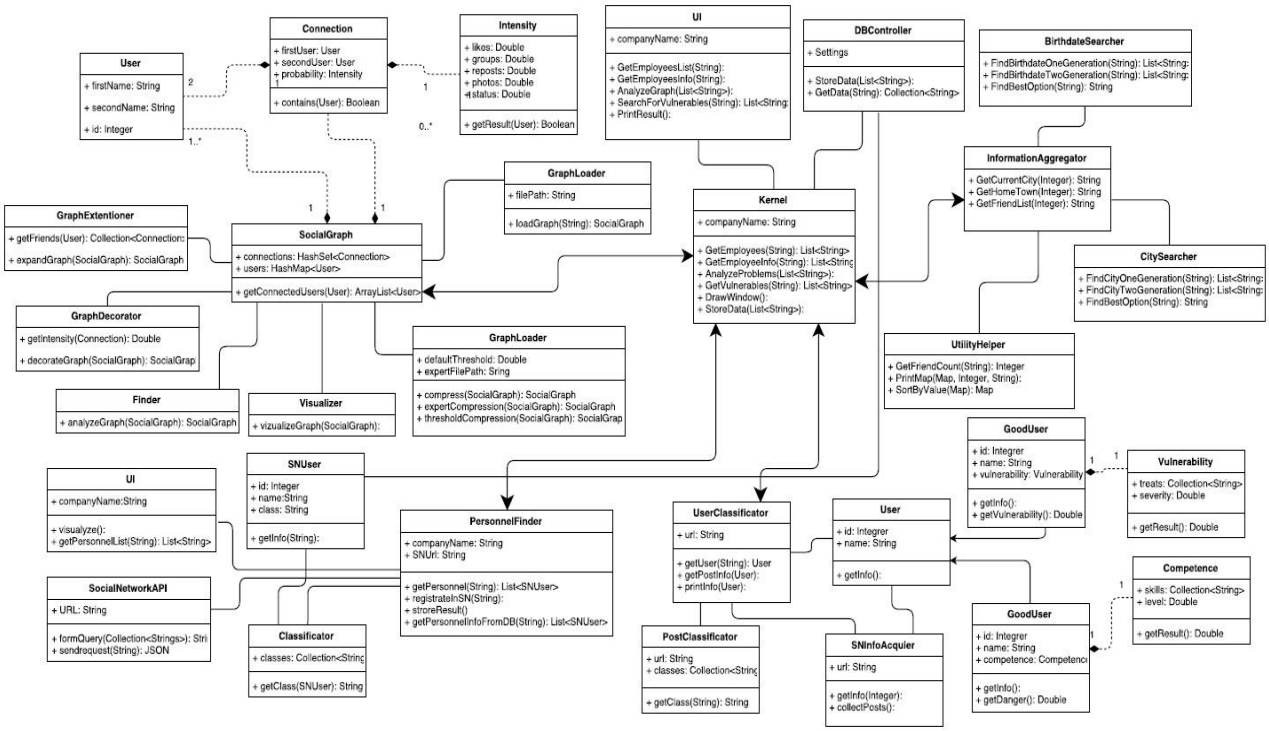


Рисунок 30 — Архитектура прототипа комплекса программ

4.2. АВТОМАТИЗАЦИЯ ИДЕНТИФИКАЦИИ СОТРУДНИКОВ КОМПАНИИ В СОЦИАЛЬНОЙ СЕТИ ВКОНТАКТЕ

Программный модуль, отвечающий за автоматизацию поиска сотрудников компании в социальной сети ВКонтакте, доступен для скачивания в

репозитории Github по ссылке https://github.com/nshindarev/vk-sea-lib (рисунок 31). Репозиторий содержит в себе три связанных проекта в одном решении:

- vk-sea-lib: библиотека, содержащая в себе основную бизнес-логику проекта;
- gui-platform-sim: исполняемый проект, позволяет использовать стандартный функционал библиотеки, реализован в виде Windows форм;
- connector-simulator: исполняемый проект, позволяет использовать функционал библиотеки. Все продукты исполнения программы логируются по уровням, логи выводятся в режиме реального времени на консоль, а также сохраняются в файле.

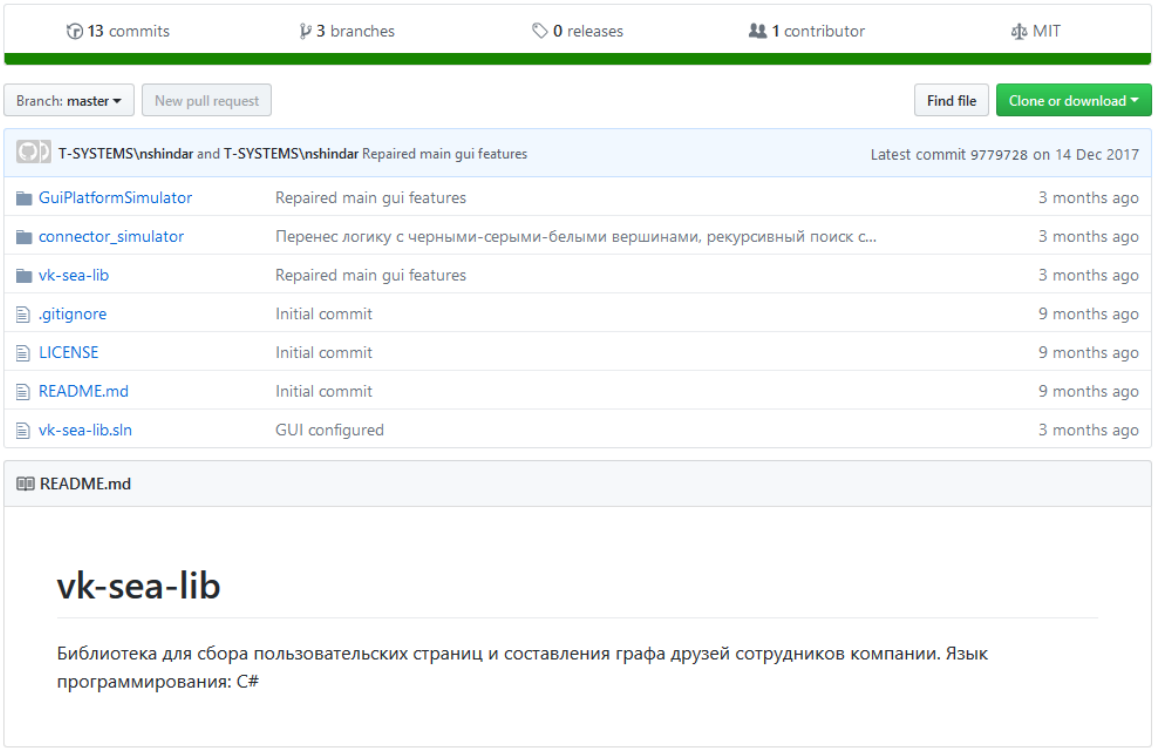


Рисунок 31 — Расположение проекта на сайте github.com

Проект реализован в среде Visual Studio Professional 2017. Для запуска необходимо воспользоваться файлом решения vk-sea-lib.sln. Для начала работы необходимо установить один из двух исполняемых проектов в качестве основного. При дальнейшем запуске проекта откроется

окно браузера, где для продолжения работы программы необходимо авторизоваться в социальной сети ВКонтакте. Модуль не может работать без авторизации в социальной сети. В случае успешного прохождения авторизации на консоли отображается Access token, который предоставляет VK API для текущей сессии. На рисунке 32 представлен консольный вывод при прохождении этапов авторизации и начала анализа пользовательских страниц.

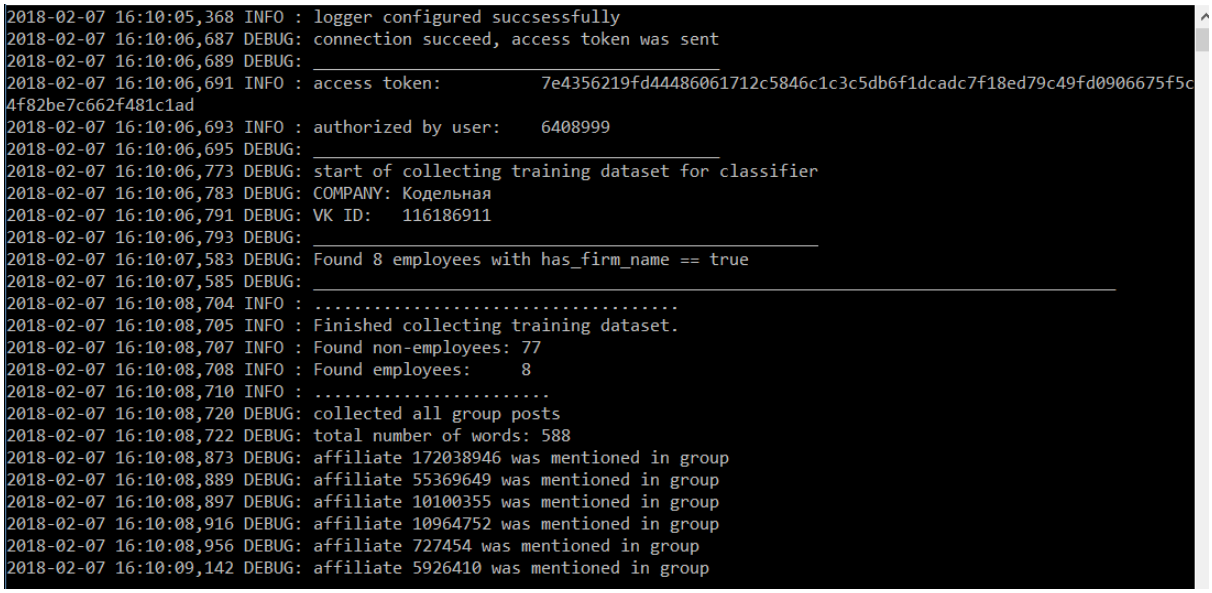


Рисунок 32 — Консольный вывод при прохождении этапов авторизации и начала анализа пользовательских страниц

После получения токена для данной сессии, взаимодействие с API осуществляется по протоколу HTTP с помощью POST и GET запросов. В ответ на запрос по умолчанию сервер возвращает ответ в формате JSON, фоормат может быть изменён на XML. Для упрощения взаимодействия с API в рамках данной работы было решено использовать общедоступную библиотеку VkNet, которая распространяется под лицензией MIT, что позволяет свободно использовать её в реализуемом программном модуле. С помощью зарегистрированного приложения можно осуществлять до пяти запросов к API в секунду. Это ограничение устанавливается для приложений, которыми пользуются менее 10 000 человек, оно приемлемо в рамках решения представленной задачи по поиску аккаунтов сотрудников

компании в социальной сети ВКонтакте. В результате подключения библиотеки VkNet всё взаимодействие с API сводится к обращениям к полям класса VkApiHolder, которые полученную JSON схему конвертируют в список объектов.

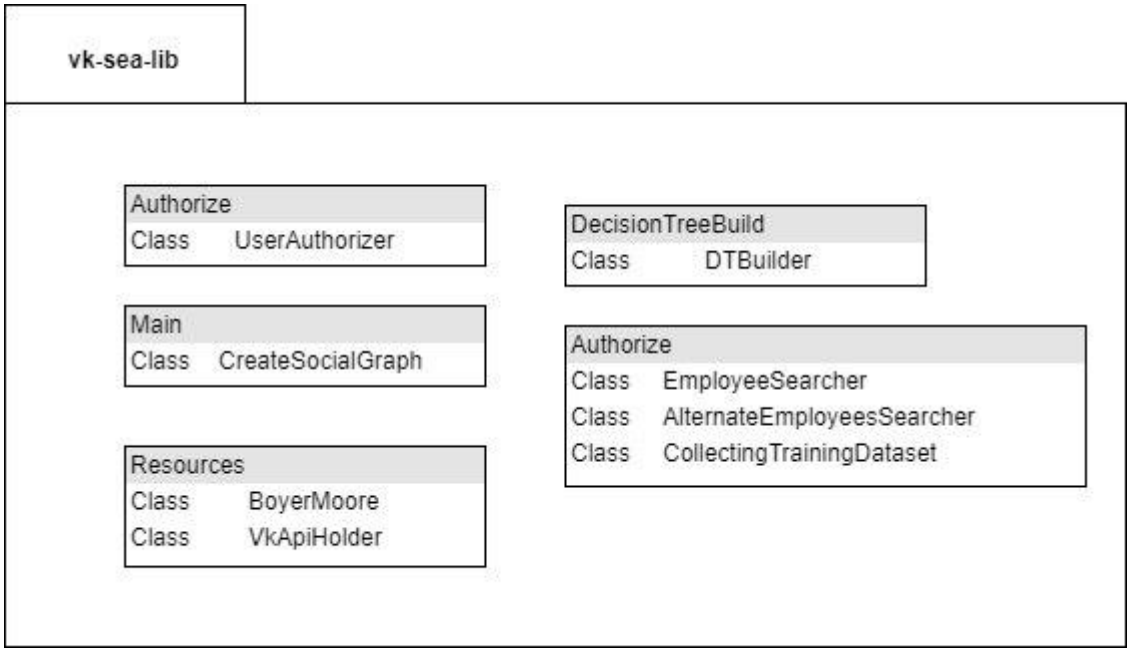


Рисунок 33 — Диаграмма классов модуля

На рисунке 33 представлена иерархия основных классов модуля, отвечающих за бизнес-логику приложения, реализованных на стороне backend. Предназначение каждого из класса представлено ниже.

- Authorize — классы, отвечающие за авторизацию приложения в социальной сети ВКонтакте.
- DecisionTreeBuild — отвечает за построение дерева принятия решений, на основе данных, собранных с помощью классов блока Parser.
- Parser — основная часть, предназначенная для сбора обучающей выборки классификатора, поиска аккаунтов сотрудников компании в социальной сети ВКонтакте. Сбор осуществляется на основе рекурсивного алгоритма.
- Resources — вспомогательные классы и алгоритмы.

Для изменения конфигурации запуска, а именно изменения анализируемой компании, или id её официальной группы в социальной сети ВКонтакте, необходимо изменить данные метода createSocialGraph() в классе CreateSocialGraph. Данный класс является центральным. При вызове метода createSocialGraph() выполняются все итерации по сбору пользовательских страниц. Класс представлен на листинге 2.

Листинг 2 — Класс CreateSocialGraph, инициализирующий поиск аккаунтов сотрудников компании

```
public void createSocialGraph()
{
      CollectingTrainingDataset collector = new      CollectingTrainingDa-
taset("Кодельная", "116186911");
            collector.parseInformation();
            this.trainingDataset = collector.training_dataset;

      //обучение классификатора
      DecisionTreeBuilder dt = new  DecisionTreeBuilder(collector.training_da-
taset);
      dt.studyDT();

      //сбор оставшихся аккаунтов
      this.searcher = new EmployeesSearcher(dt, collector.companyName,
      collector.vkPageId);
      this.searcher.findAllEmployees();
      this.empSocialGraph = searcher.EmployeesSocialGraph;
}
```

Проект vk-sea-lib данного модуля интегрируется в комплекс программ для оценки защищённости пользователей информационной системы от социоинженерных атак. Для интеграции был спроектирован внешний интерфейс таким образом, чтобы свести в одной компоненте последовательное выполнение всех основных автоматизированных программных элементов. Сам внешний программный интерфейс представлен на рисунке 34.

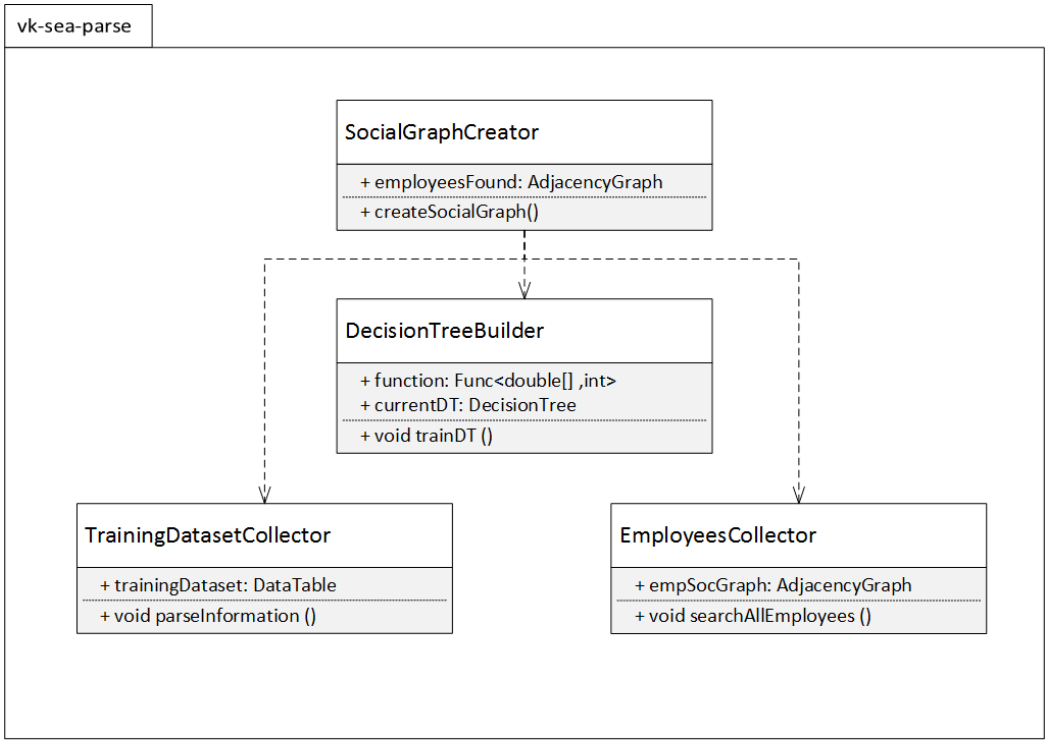


Рисунок 34 — Внешний программный интерфейс модуля

Также был разработан пользовательский графический интерфейс для ручной корректировки результатов работы программного модуля (рисунок 35). Интерфейс предоставляет возможность добавления id аккаунта сотрудника компании, если он не был найден с помощью программы. Также предусмотрена возможность удаления ошибочно идентифицированного аккаунта сотрудника компании из выборки. Помимо этого, при нажатии на кнопку «Search At Point» можно добавить идентификатор аккаунта в социальной сети, который предположительно связан с аккаунтами сотрудников компании. В этом случае программный модуль проанализирует друзей, содержащихся в этом аккаунте, и друзей друзей с целью поиска и идентификации новых аккаунтов сотрудников компании в социальной сети.

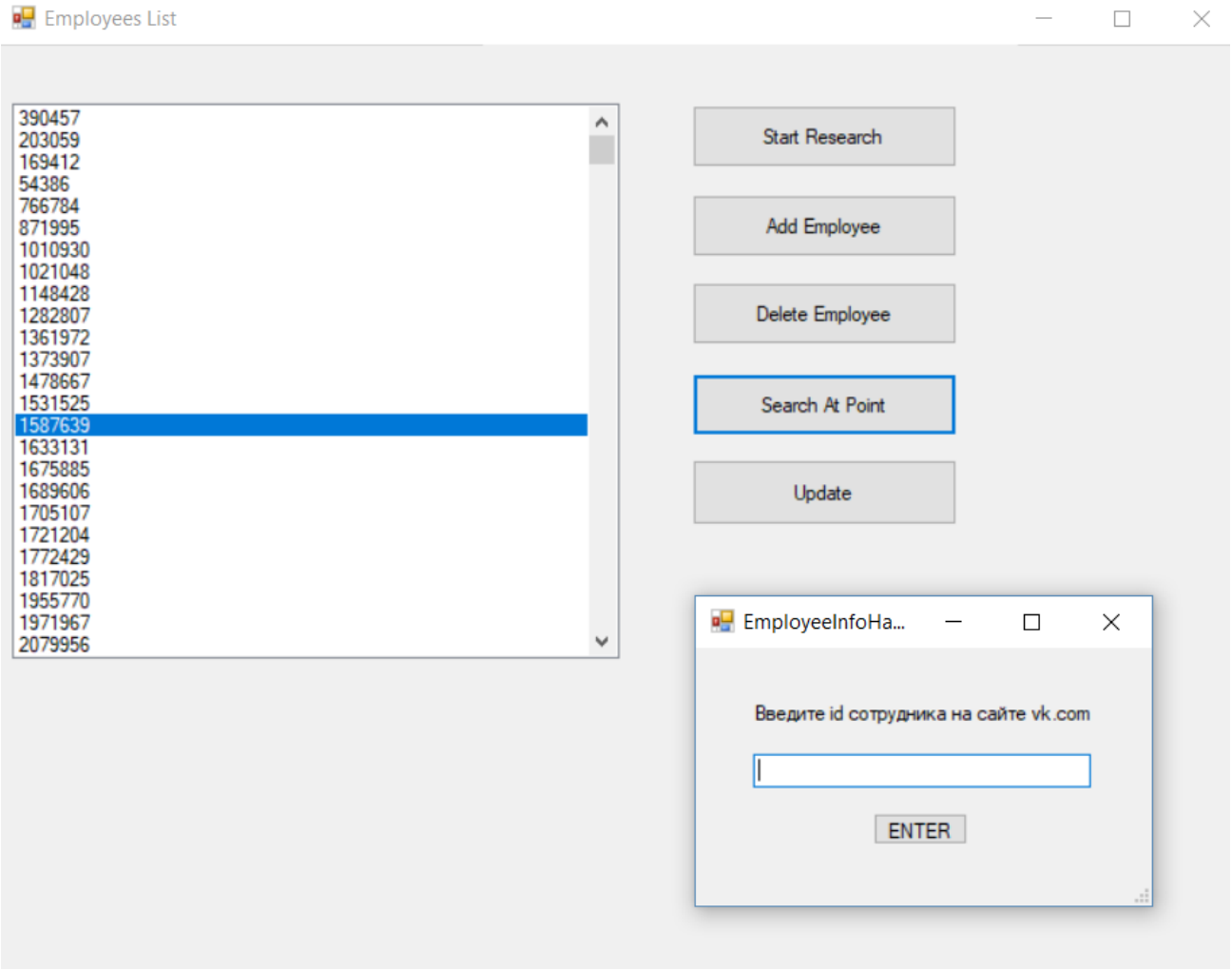


Рисунок 35 — Графический пользовательский интерфейс программного модуля

4.3. МОДУЛЬ АВТОМАТИЗИРОВАННОГО ПОСТРОЕНИЯ ОЦЕНОК НЕКОТОРЫХ ОСОБЕННОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ

Прототип модуля анализа текстовой информации в социальных сетях был разработан на языке C# с использованием фреймворка Accord.NET и библиотеки VkNet. Прототип модуля состоит из следующих компонент.

- Компонент для взаимодействия с API социальной сети ВКонтакте.
- Компонент, предназначенный для предварительной обработки текста.
- Компонент, производящий классификацию текстовых записей и построение психологического профиля.

Рассмотрим подробнее каждый из этих компонент. В компоненте для взаимодействия с API социальной сети ВКонтакте используется библиотека VkNet. Эта библиотека предоставляет класс VkApi. Для удобства создания экземпляра этого класса и вызова всех необходимых его методов был применён паттерн проектирования «Одиночка» (Singleton). Реализация данного подхода представлена в приложении Д. Кроме того, был создан класс VkApiWrapper, который используется, в частности, классами SocialNetwork и PsychProfile. Классы VkApiHolder и VkApiWrapper имеют уровень доступа internal, что запрещает обращения к ним извне пакета. Таким образом, сохраняется принцип инкапсуляции.

Компонент, предназначенный для предварительной обработки текста, состоит из классов TFIDF и StopWords. Класс TFIDF предназначен для приведения строковых документов к приемлемому для работы виду. Он содержит следующие методы.

- Transform – модернизирует список документов в список соответствующих значений TFIDF.
- TryLoadVocabulary – выполняет загрузку (десериализацию) предварительно созданного словаря N-грамм.
- GetVocabulary – в данном методе создаётся словарь по набору документов, указанных в методе Transform.

Фрагмент реализации класса TFIDF представлен в листинге 3.

Листинг 3 — Фрагмент реализации класса TFIDF

```
internal static class TFIDF {
      private static Dictionary<string, double> _vocabularyIDF = new   Dic-
tionary<string, double>();
      private static Dictionary<string, double> _filteredVocabularyIDF = new
      Dictionary<string, double>();

      public static double[][] Transform(string[] documents) {
            List<List<string>> stemmedDocs;
            List<string> vocabulary;

            int vocabularyThreshold = 2;
            int featuresAmount = 9000;

            vocabulary = GetVocabulary(documents, out stemmedDocs,
            vocabularyThreshold);
```

```
            TryLoadVocabulary();

            _filteredVocabularyIDF = _vocabularyIDF.OrderByDescending(t =>
            t.Value).Take(featuresAmount).ToDictionary(x => x.Key, x =>
            x.Value);

            return TransformToTFIDFVectors(stemmedDocs,
            _filteredVocabularyIDF);
      }

      internal static void TryLoadVocabulary(string filePath =   "vocabu-
lary.dat") {
            try {
                  using (FileStream fs = new FileStream(filePath,
                  FileMode.Open)) {
                  BinaryFormatter formatter = new BinaryFormatter();
                  _vocabularyIDF = (Dictionary<string,
                  double>)formatter.Deserialize(fs);
            }
      }
      catch (FileNotFoundException e) {
            throw (new FileNotFoundException("Словарь не найден", e.File-
Name));
      }
}

private static List<string> GetVocabulary(string[] docs, out
List<List<string>> stemmedDocs, int vocabularyThreshold) {
      List<string> vocabulary = new List<string>();
      Dictionary<string, int> wordCountList = new Dictionary<string, int>();
      stemmedDocs = new List<List<string>>();

      foreach (var doc in docs) {
            List<string> stemmedDoc = new List<string>();
            string[] parts2 = Tokenize(doc);

            List<string> words = new List<string>();
            foreach (string part in parts2) {
                  string stripped = Regex.Replace(part, "[^a-zA-Za-яA-Я0-9]",
                  "");

            if (!StopWords.stopWordsList.Contains(stripped.ToLower())) {
                  try {
                        string stem = stripped.ToLower();
                        words.Add(stem);

                        if (stem.Length > 0) {
                              if (wordCountList.ContainsKey(stem)) {
                                    wordCountList[stem]++;
                              }
                              Else {
                                    wordCountList.Add(stem, 0);
                              }

                              stemmedDoc.Add(stem);
                        }
                  }
                  Catch {}
            }
      }
      stemmedDocs.Add(stemmedDoc);
}

var vocabList = wordCountList.Where(w => w.Value >= vocabularyThreshold);
```

```
foreach (var item in vocabList) {
      vocabulary.Add(item.Key);
}

return vocabulary;
```

Класс StopWords содержит список стоп-слов (слов, которые не несут смысловой нагрузки и влияние которых на процесс обучения классификатора несущественно). Данный класс используется во время составления словаря по набору документов. Массив стоп-слов представлен в приложении Д.

Компонент, производящий классификацию текстовых записей и построение психологического профиля содержит восемь приватных полей класса MulticlassSupportVectorMachine<Linear>, который предоставляется фреймворком Accord.NET. Каждое из этих полей предназначено для хранения модели классификатора, предсказывающей значение степени выраженности определённой характеристики. При создании экземпляра класса SVM происходит загрузка файлов, описывающих модели, с внешнего носителя и создание экземпляров моделей на основе этих файлов. Другими словами, выполняется десериализация моделей классификаторов. Для выполнения предсказания уровня выраженности характеристики используется метод Decide() класса MulticlassSupportVectorMachine<Linear>, который возвращает номер предсказанного класса.

UML-диаграмма публичных классов, доступных для внешних вызовов, представлена на рисунке 36. Класс SocialNetwork содержит статический метод Authorize, который вызывает окно авторизации в социальную сеть «ВКонтакте». Класс PsychProfile представляет статический метод GetUserPsychProfile(), результатом которого является набор пар «характеристика» — «уровень выраженности характеристики». Возможные значения уровней выраженности содержатся в перечисляемом типе TraitDegree.

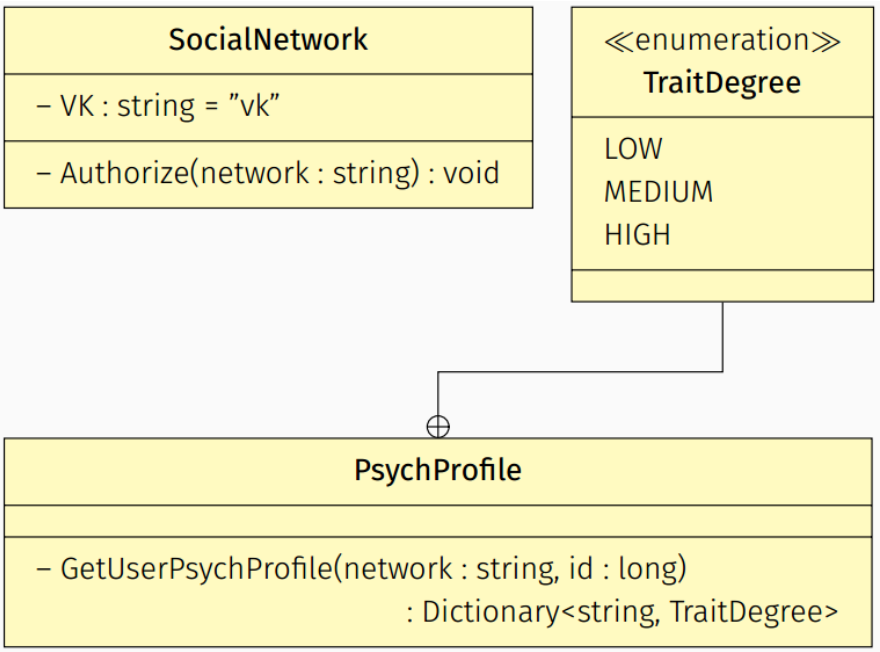


Рисунок 36 — Внешний программный интерфейс модуля

В листинге 4 представлен фрагмент класса PsychProfile, содержащий код метода построения профиля психологических особенностей пользователя, который принимает на вход строку с названием социальной сети и идентификатор пользователя в этой сети. На данный момент доступна только социальная сеть «ВКонтакте», в дальнейшем предполагается расширить список доступных социальных сетей.

Листинг 4 — Метод, реализующий построение профиля психологических особенностей пользователя.

```
public static class PsychProfile {
      public enum TraitDegree {
            LOW,
            MEDIUM,
            HIGH
      }

      public static Dictionary<string, TraitDegree> GetUserPsychProfile(string
      network, long id) {
            Dictionary <string, TraitDegree> result = new Dictionary<string,
            TraitDegree>();
            List<string> data = SocialNetwork.GetPosts(network, id);

            if (data.Count == 0)
            return null;

            var svmResult = new SVM().GetPsychProfile(data.ToArray());

            foreach (var item in svmResult) {
                  result.Add(item.Key, item.Value == 0 ? TraitDegree.LOW :
                  item.Value == 1 ? TraitDegree.MEDIUM :
```

```
                    TraitDegree.HIGH);
                }
        return result;
        }
}
```

Для интеграции функций модуля с комплексом программ было произведено подключение его в качестве внешней зависимости в конфигурационном файле комплекса. После этого на главном экране приложения были добавлены управляющие элементы (а именно, три кнопки и текстовое поле). Главный экран и описываемые элементы показаны на рисунке 37.

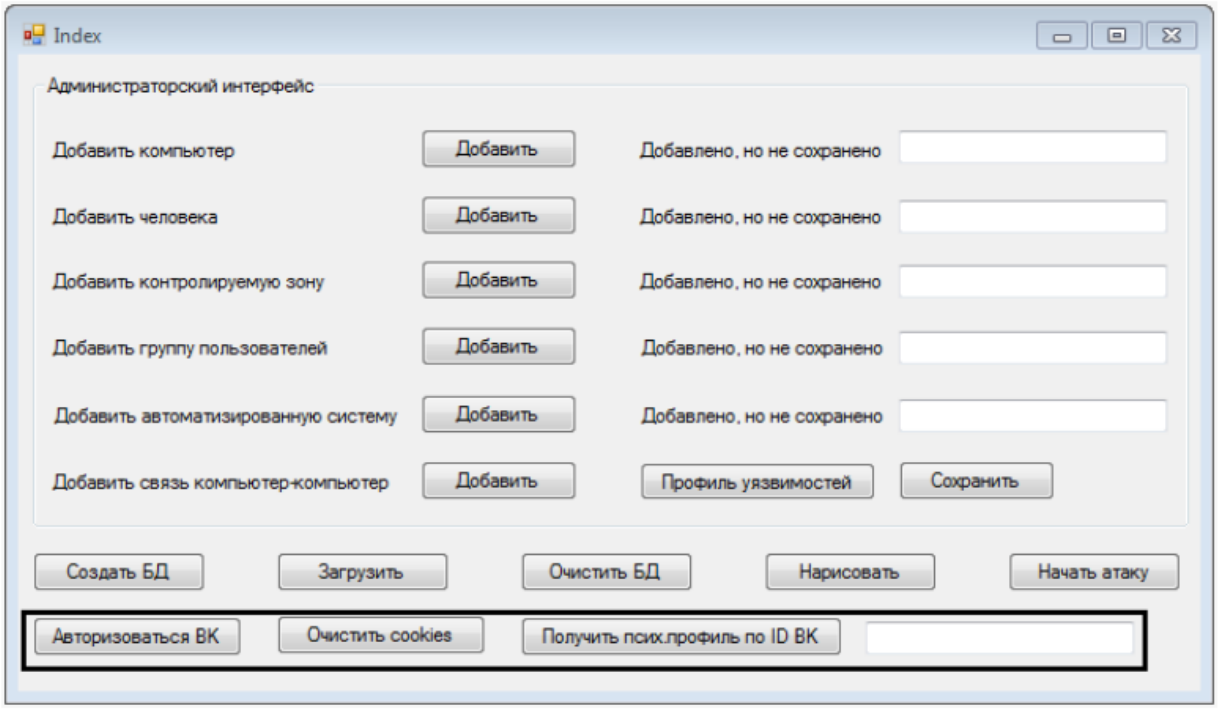


Рисунок 37 — Главное окно комплекса программ с добавленными элементами управления

По нажатию кнопки «Авторизоваться ВК» вызывается окно авторизации в социальной сети ВКонтакте. Элемент «Очистить cookies» запускает процесс очистки так называемых cookies, которые содержат информацию об авторизованном пользователе. Эта операция может потребоваться, если комплекс программ используется несколькими пользователями на одном компьютере.

При нажатии кнопки «Получить псих. профиль по ID ВК» происходит обращение ко внешнему интерфейсу разработанного модуля (для успешной работы предварительно необходимо ввести идентификатор интересующего пользователя социальной сети ВКонтакте в текстовое поле, расположенное справа от управляющего элемента). После выполнения внутренних операций модуля на экран выводится диалоговое окно с информацией о психологическом профиле пользователя. Пример диалогового окна представлен на рисунке 38 (идентификатор пользователя скрыт в целях защиты конфиденциальной информации).

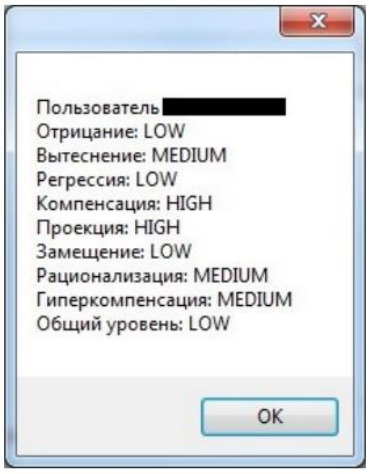


Рисунок 38 — Пример диалогового окна с информацией о психологическом профиле пользователя

Метод обработки события нажатия на управляющий элемент «Получить псих. профиль по ID ВК» с примером обращения к внешнему интерфейсу разработанного модуля показан в листинге 5.

Листинг 5 — Пример обращения ко внешнему интерфейсу прототипа модуля

```
using SocialNetworksAnalysis;
...
private void button10_Click(object sender, EventArgs e) {
      var psychProfile = PsychProfile.GetUserPsychProfile(SocialNetwork.VK,
      long.Parse(vkid.Text));

      if (psychProfile == null) {
            MessageBox.Show("Пользователь " + vkid.Text + ":\nНа стене нет
            текстовой информации, размещённой пользователем");
            return;
      }

      string s = "Пользователь " + vkid.Text + ":\n";
      foreach (string key in psychProfile.Keys)
```

```
        s += key + ": " + psychProfile[key] + "\n";
        MessageBox.Show(s);
}
```

4.4. АВТОМАТИЗАЦИЯ ВОССТАНОВЛЕНИЯ ФРАГМЕНТА МЕТА-ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯ

Данный программный модуль предназначен для восстановления фрагмента мета-профиля пользователя, основанного на агрегации информации из социальных сетей. Информация извлекается исходя из анализа социального окружения пользователя, а также на основании сведений, извлекаемых из других социальных сетей. На вход модуль получает набор идентификаторов пользователей, на выходе сопоставляет идентификаторам пользователей их мета-профили.

Для написания модуля использовался язык программирования Java вместе с реляционной системой управления базами данных MySQL. Также, для работы с социальными сетями были использованы различные средства API. Для работы с социальной сетью ВКонтакте использовалась технология VK API, которую предоставляет vk.com.

Структуру хранения информации о пользователе представляет собой класс Person. Устройство этого класса будет отличаться для разных социальных сетей. На данный момент этот класс выглядит следующим образом (листинг 6).

Листинг 6 — Структура хранения информации о пользователе

```
class PersonVK
{
        String nickname, name, surname;
        Integer id;
        String hometown, currcity, bdate;
        String[] school, university, work;
}
```

Поля никнейм, имя, фамилии и id — константные поля, которые заданы у всех пользователей социальной сети ВКонтакте. Далее на основании социального окружения пользователя делаются предположения о его родном городе, городе, в котором он проживает в данный момент, а также дате рождения. Для анализа социального окружения пользователя

необходимо получить идентификаторы друзей пользователя. На листинге 7 представлен пример реализации этого функционала.

Листинг 7 — Извлечение списков друзей пользователя

```
public static List<String> GetFriendsList(String id) {
	String request = "https://api.vk.com/method/friends.get?user_id=" + id +
	"&order=mobile&fields=onlain&namecase=nom&v=5.68";
	List<String> ans = new ArrayList<String>();
	String res, s;
	try {
		res = GetHtmlByURL(request);
		while(true) {
			Integer k = res.indexOf("id\":");
			if (k == -1)
				break;
			res = res.substring(k + 4);
			s = res.substring(0,res.indexOf(","));
			ans.add(s);
		}
	}
	catch (Exception ex) {
		System.out.println(ex.toString());
	}
	return ans;
}
```

На основании этой информации делаются предположения об остальных данных. Извлечение информации о родных городах друзей пользователя делается посредством методов, представленных в листинге 8.

Листинг 8 — Извлечение информации о родных городах друзей пользователя

```
public static String GetCurrentCity(String id) {
	String request = "https://api.vk.com/method/users.get?user_ids=" +
	id + "&fields=city&v=5.68";
	String ans = new String();
	try {
		ans = GetHtmlByURL(request);
		if (ans.indexOf("city") == -1)
			return "";
		ans = ans.substring(ans.indexOf("city"));
		ans = ans.substring(ans.indexOf("title"));
		ans = ans.substring(ans.indexOf(":") + 2);
		ans = ans.substring(0, ans.indexOf("\""));
	}
	catch (Exception ex) {
		System.out.println(ex.toString());
	}
	return ans;
}

public static String GetHomeTown(String id) {
	String request = "https://api.vk.com/method/users.get?user_ids=" + id +
	"&fields=home_town&v=5.68";
	String ans = new String();
	try {
		ans = GetHtmlByURL(request);
```

```
            if (ans.indexOf("home_town") == -1)
                  return "";
            ans = ans.substring(ans.indexOf("home_town"));
            ans = ans.substring(ans.indexOf(":") + 2);
            ans = ans.substring(0, ans.indexOf("\""));
      }
      catch (Exception ex){
            System.out.println(ex.toString());
      }
      return ans;
}
```

Обработка таких запросов строится следующим образом: создаётся срока реквеста, в который указывается тип запроса и id пользователя(-ей), на кого он будет распространяться. Далее, преобразовав результат запроса, который выдается в формате JSON с помощью метода GetHtmlByURL в строку, осуществляется парсинг нужной информации.

После извлечения всей необходимой информации необходимо построить распределение возможных вариантов данных для мета-профиля пользователя. Модуль получает список друзей пользователя, далее, для каждого пользователя определяет родной город (или же текущий город) и подсчитывает количество совпадений того или иного варианта. После этого города ранжируются по мере упоминаемости в анкетах друзей, статистика записывается в выходной файл. Город, упоминавшийся большее число раз считается городом пользователя.

Были проведены тесты работы программного модуля. На рисунке 39 представлены результаты восстановления информации о родном городе пользователя. Данные результаты были получены при глубине анализа 2. Т.е. проанализированы анкеты и друзей друзей пользователя. Исследуемый пользователь действительно живёт в данный момент в Красноярске и учился некоторое время в Санкт-Петербурге.

Было проведено тестирование работы программного модуля для определения значений трёх параметров: возраста, текущего города проживания и родного города. В качестве метода определения точности работы программы была выбрана кросс-валидация [42]. Кросс валидация –

это процедура эмпирического оценивания обобщающей способности алгоритмов, обучаемых по прецедентам [39]. Эта процедура особо подходит для расчёта точности подобных данных за счёт независимости выборок данных [39].

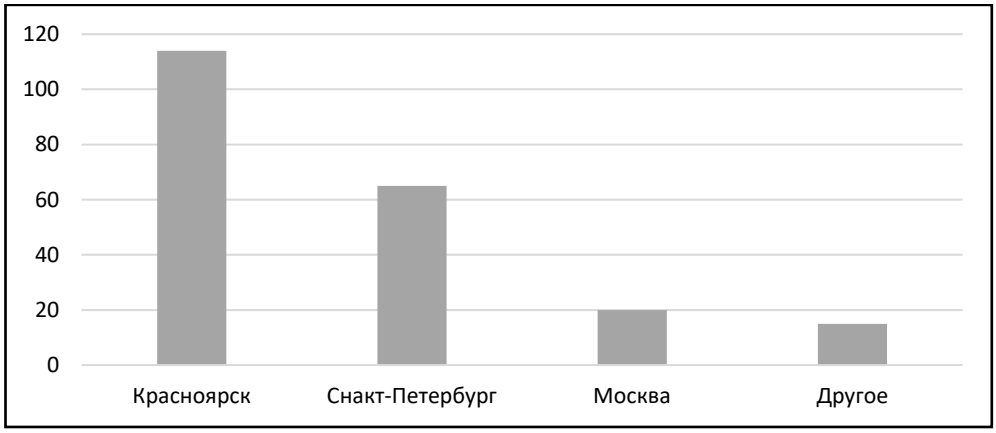


Рисунок 39 — Результаты работы по восстановлению города проживания программного модуля

Согласно данному методу, из выборки в n элементов случайно берутся около 80% данных и считается какая часть из них оказалось корректной. Для оценки точности работы представленного алгоритма с помощью программного модуля его реализующего было проанализировано 50 аккаунтов пользователей, про которых априорно была известна информация о родном городе, текущем городе проживания и возрасте. Среди них в отношении 46 аккаунтов был корректно определён родной город, 42 — корректно определён город проживания, 43 — корректно определён возраст.

Далее произвольным образом составлялись выборки по 40 аккаунтов из генеральной выборки, состоящей из 50 аккаунтов, и внутри каждой выборки определялась вероятность успешного распознавания данных фрагмента мета-профиля пользователя. Для каждой выборки из 40 элементов рассчитывались средние показатели корректности работы. Всего было произведено 30 таких выборок по 40 аккаунтов. Средний показатель точности по правильности определения родного города варьировался от 82% до 90%, города проживания — от 80% до 92%, возраста — от 90% до

97%. Результирующие показатели точности были рассчитаны как среднее от всех полученных значений и составили для родного города — 85,5% правильно идентифицированных аккаунтов, для текущего города проживания — 84,77% правильно идентифицированных аккаунтов, а для возраста — 91,75% правильно идентифицированных аккаунтов (рисунок 40).

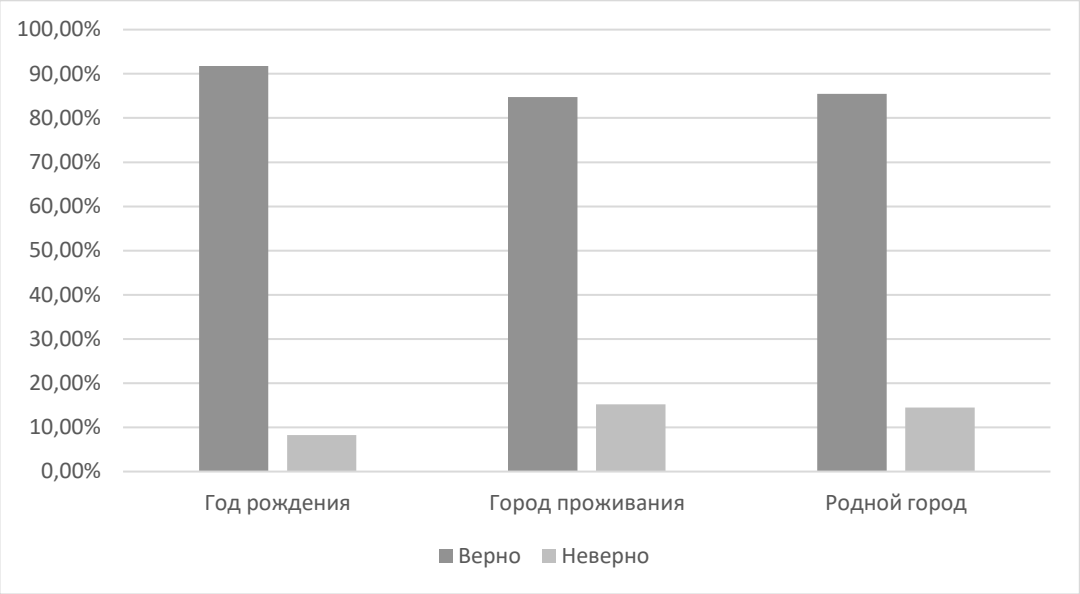


Рисунок 40 — Показатели оценки точности работы программного модуля

4.5. АВТОМАТИЗАЦИЯ ОЦЕНКИ ВЕРОЯТНОСТИ УСПЕХА МНОГОХОДОВОЙ СОЦИОИНЖНЕРНОЙ АТАКИ

Данный программный модуль предназначен для реализации модели оценки вероятности успеха многоходовой социоинженерной атаки на одного пользователя через другого. Он строит, обрабатывает и анализирует социальный граф взаимодействия сотрудников компании. В ходе работы данный комплекс осуществляет получение данных о сотрудниках из социальных сетей, путём отправки специализированных запросов API социальной сети (в данной работе рассматривается социальная сеть ВКонтакте).

Для разработки данного модуля использовался язык программирования Java в комплексе с реляционной системой управления базами данных MySQL. Для получения информации об интенсивности взаимодействия

сотрудников компании, выраженной в различных количественных показателях взаимной активности (лайки, репосты, совместные фотографии и др.) используется API социальной сети ВКонтакте VK API. Также в программном модуле используется библиотека для визуализации графов JGraphX, которая распространяется по открытой лицензии. Для сборки проекта использовалась технология Apache Maven, позволяющая «на лету» подключать необходимые библиотеки, API, и сервисы, используемые комплексом программ. Подробнее опишем структуру программного модуля.

Класс SocialGraph предназначен для построения социального графа взаимодействия сотрудников. Он агрегирует информацию об аккаунтах сотрудников компании, содержит набор рёбер социального графа в рамках поля SocialGraph.users. SocialGraph.users — структура типа HashMap (ассоциированный массив). Использование этой структуры упрощает определение того, содержится ли уже вершина данного пользователя в графе или нет. В качестве ключа выступает ID пользователя в социальной сети ВКонтакте. Поле SocialGraph.connections — объектного типа HashSet, предназначено для агрегации информации о связях в графе. Методы, реализуемые классом SocialGraph, включают в себя отображения списков SocialGraph.users и SocialGraph.connections. Метод SocialGraph.contains — производит проверку принадлежности связи (или ее аналога) социальному графу. Метод SocialGraph.getConnectedUsers возвращает список (ArrayList) всех пользователей, которые непосредственно связаны с данным.

Класс Connection представляет собой упорядоченную пару двух пользователей и характеристику интенсивности взаимодействия между двумя пользователями информационной системы компании. Класс содержит поля для хранения пользователей, участвующих во взаимодействии, а также поле Connection.possibility — оценка вероятности успеха

распространения социоинженерной атаки злоумышленника на пользователя через другого пользователя. Класс Connection включают в себя стандартный набор get/set методов, но также и метод Connection.contains, осуществляющий проверку участия в данном взаимодействии пользователя.

Класс User является наиболее низким в иерархии классом, отражающим присутствие конкретного пользователя в системе. Характеризует его с помощью полей firstName, secondName, id. User.id. Позволяет однозначно определить включение сотрудника в граф. Методы класса User включают себя стандартные set/get методы.

Вспомогательный класс Intensity предназначен для хранения информации о данных, извлекаемых из социальной сети ВКонтакте, характеризующих интенсивность взаимодействия сотрудников. На данный момент включает поля: Likes (отметки «Мне нравится», Groups (сообщества), Reposts (репосты), Photos (общие фотографии), Status (семейное положение).

Класс GraphLoader предназначен для построения социального графа взаимодействия сотрудников компании на базе CSV-файла, получаемого программным модулем от модуля «Поиск персонала», который содержит данные о списке сотрудников компании. Класс может обрабатывать файлы двух форматов, в первом случае — это список сотрудников, во втором — список рёбер графа (в данном случае граф не полный).

Вспомогательный класс GraphExtentioner специализируется на расширении графа сотрудников за счет включения дополнительных вершин в граф. В качестве новых вершин берутся наиболее близкие к рассматриваемому сотруднику пользователи социальной сети ВКонтакте. Метод GraphExtentioner.GetFriends отвечает за отправку запросов к API ВКонтакте, который возвращает коллекцию объектов типа «Connection», один из пользователей в которых – сотрудник, окружение которого мы включаем в анализ. Базовый метод GraphExtentioner.expandGraph предназначен для расширения социального графа.

Класс GraphDecorator отвечает за анализ данных, извлекаемых из социальной сети ВКонтакте. В его базовый функционал включёно вычисление интенсивности взаимодействия сотрудников компании и получение на этой основе оценок вероятности успеха распространения социоинженерной атаки злоумышленника на пользователя через другого пользователя.

Класс Visualizer предназначен для визуализации полученного социального графа. В нём используются соответствующие библиотеки JGraphX и JGraphT. Однако промежуточный слой, интерпретирующий структуру SocialGraph, а также отвечающий за настройку изображения, лежит в классе Visualizer.

Класс Compressor предназначен для выполнения разрежения графа в соответствии с заданным пороговым значением оценки вероятности успеха прохождения социоинженерной атаки на пользователя через другого пользователя. Разрежение графа может происходить разными способами, через задание пороговых значений для оценок вероятностей или через задание доли дуг от общего числа, которые нужно отобразить. Оператор, работающий с модулем может выбрать соответствующий вариант в зависимости от поставленных целей.

Метод Compressor.thresholdCompression реализует один из подходов к разрежению социального графа компании, основанного на исключении рёбер, оценки вероятности перехода по которым ниже заданного порогового значения.

На рисунке 41 представлена диаграмма описанных классов модуля со связями между ними.

Класс Finder реализует ключевую функциональность программного модуля. Данный класс отвечает за анализ социального графа взаимодействия сотрудников компании. Метод analyzeGraph отвечает за обход графа и выделение особенно критичных зон.

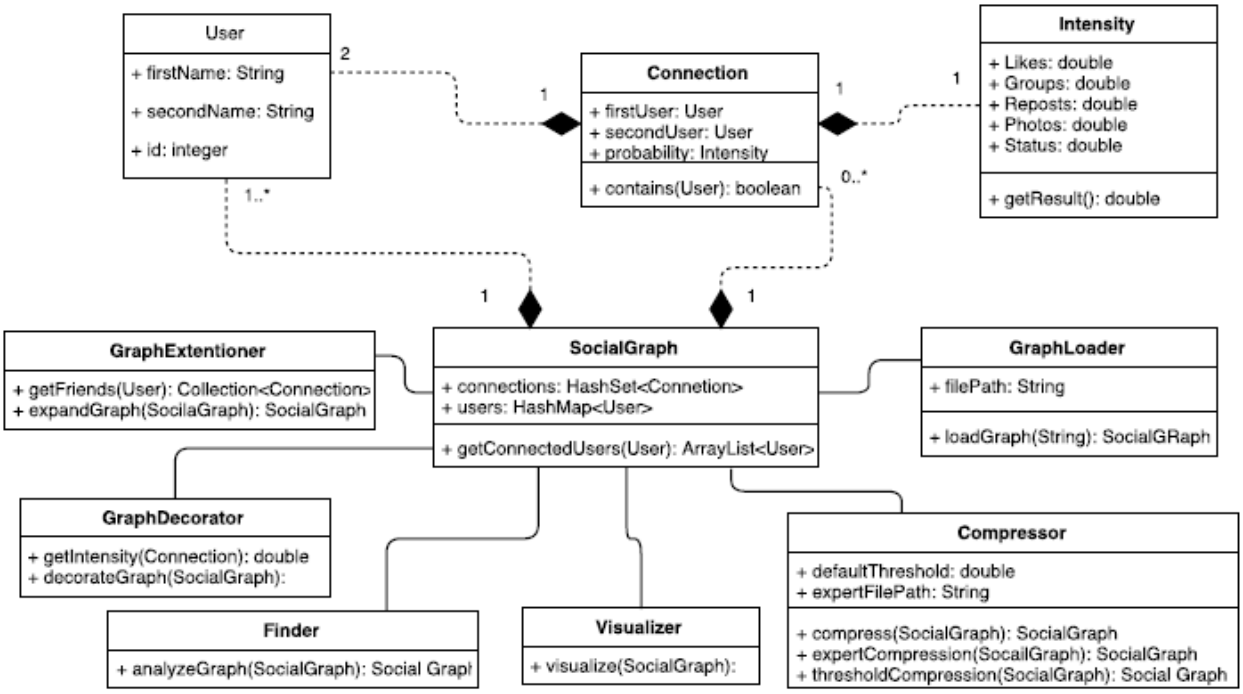


Рисунок 41 — Архитектура программного модуля

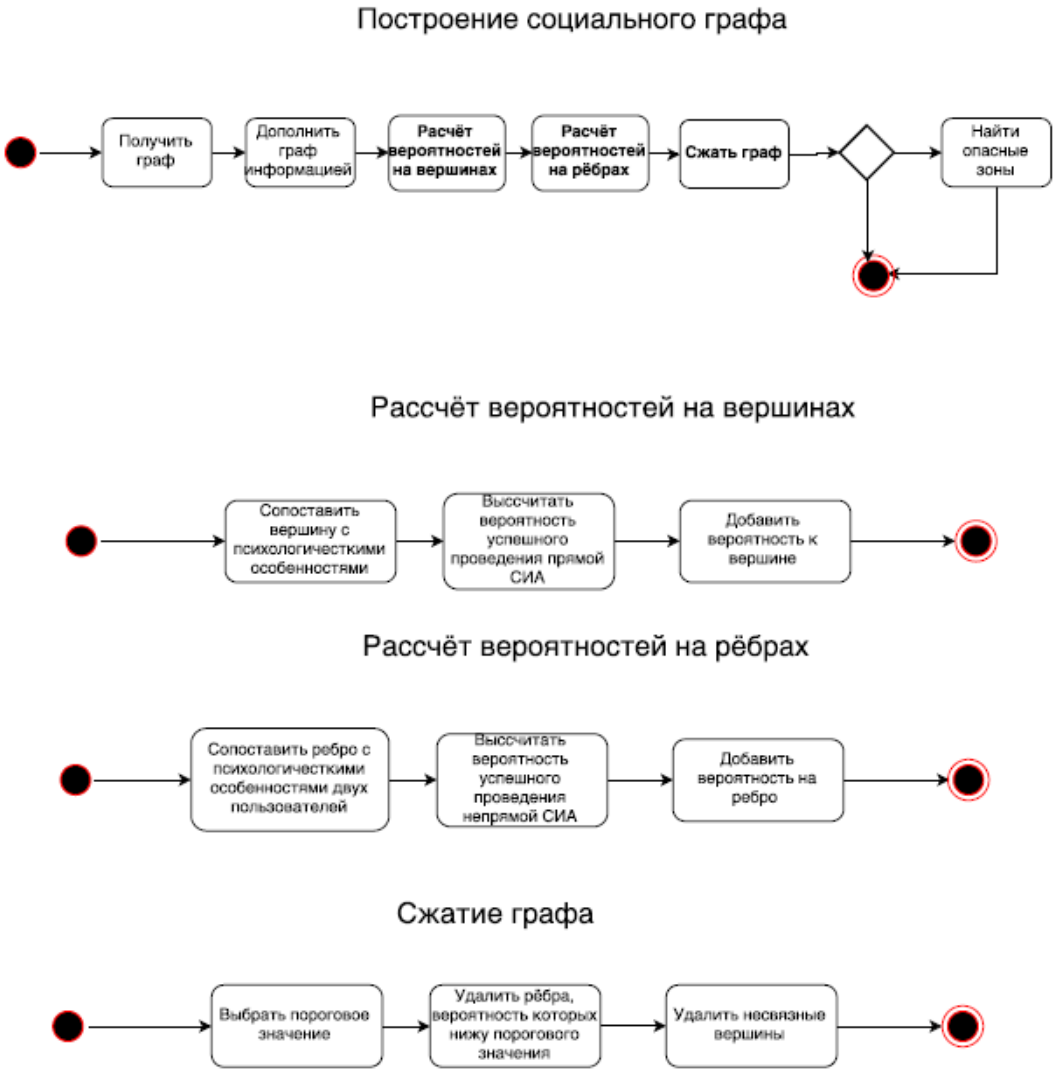


Рисунок 42 — Алгоритм обработки социального графа сотрудников компании

Для иллюстрации работы модуля Social Graph представлены диаграммы, демонстрирующие алгоритм построения социального графа и сопоставления рёбрам оценок вероятностей, на рисунке 42. Некоторые операции представлены отдельными развёртками, среди них вычисление значений вероятностей непосредственной атаки злоумышленника на пользователя, которая обозначается на вершинах графа и связана с профилем уязвимостей пользователей [97]; расчёт оценок вероятностей на рёбрах социального графа, а также обход социального графа. На рисунке 43 скриншот работы модуля прототипа комплекса программ.

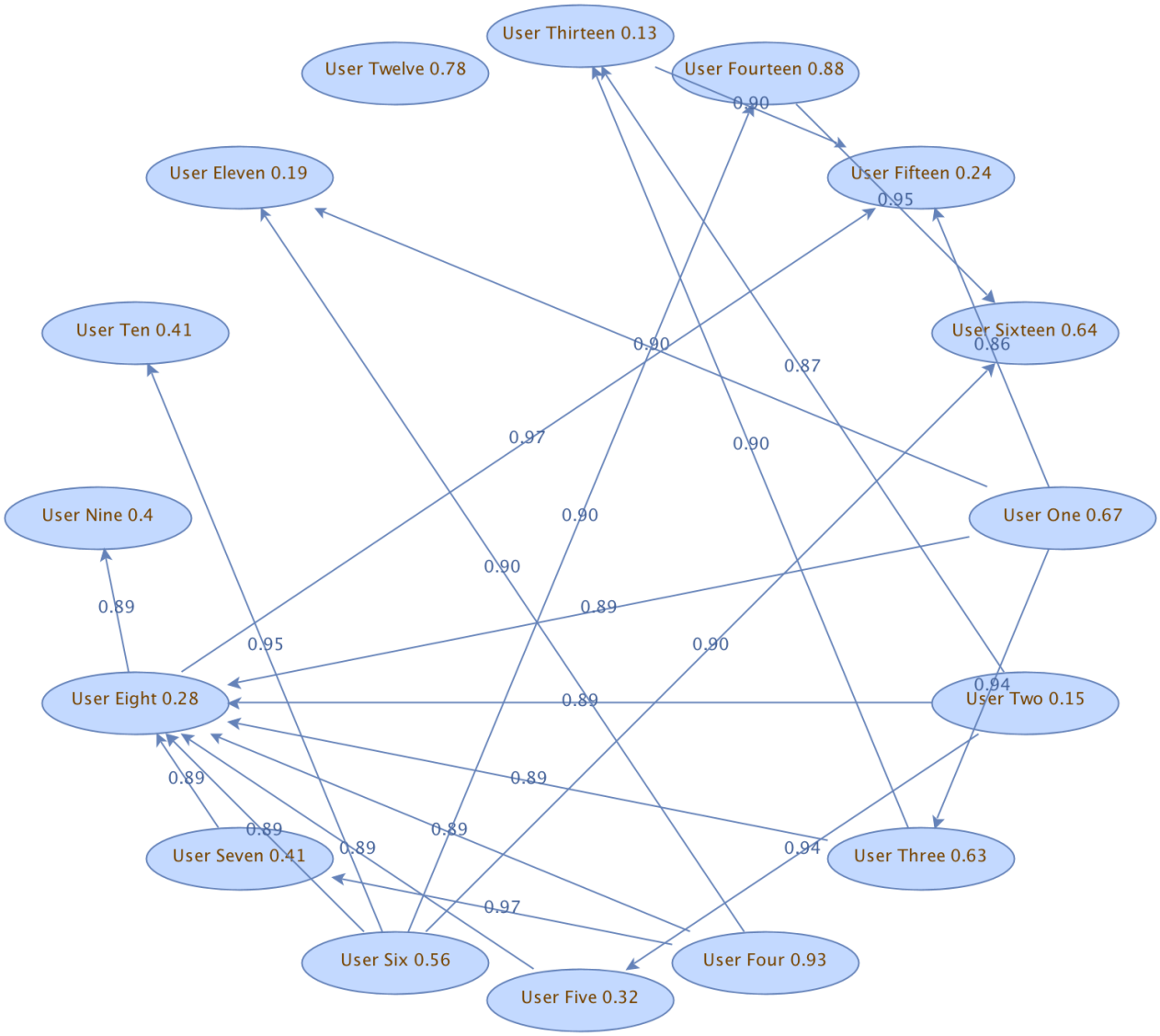


Рисунок 43 — Скриншот работы модуля комплекса программ, рассчитывающего вероятности успеха распространения социоинженерной атаки от пользователя к пользователю

На рисунке 43 в графе на рёбрах отмечены оценки вероятности распространения социоинженерной атаки от пользователя к пользователю. В вершинах отмечены вероятности успеха прямой социоинженерной атаки злоумышленника на пользователя.

4.6. ОЦЕНКА ОПЕРАТИВНОСТИ ЭКСПРЕСС-АНАЛИЗА

Чтобы продемонстрировать, что разработанные алгоритмы и реализация существенно сокращают время, необходимое для обнаружения угроз социоинженерных атак за счёт автоматизации ряда операций, которые ранее производились вручную, оценим скорость работы соотвествующих компонент комплекса программ в вычислительном эксперименте, а ручным трудозатратам дадим консервативную оценку, заведомо меньшую реальной за счет исключения из рассмотрения утомляемости эксперта, необходимости делать перерывы в работе, ограниченности трудового дня и пр. Результаты запусков программных модулей представлены в приложении И. Результаты вычислительных экспериментов были адаптированы для округлённых значений количества анализируемых объектов. Для упрощения будем также использовать округлённые в большую сторону значения времени работы разработанных программных модулей. Отметим, что в разное время суток модулям требуется разное время для работы. Это может быть связано с неравномерным суточных распределением нагрузки на сервера социальной сети.

Для идентификации аккаунтов сотрудников компании в социальной сети для организации в 100 человек программный модуль затрачивает около часа работы. Если предположить, что в среднем на идентификацию одного аккаунта эксперт затрачивает около 5 минут, то для идентификации 100 аккаунтов ему потребуется более 8 часов, т.е. полный рабочий день. Таким образом, разработанный программный модуль позволяет сократить время, необходимое для выполнения этой работы в 8 раз.

В задаче оценки выраженности некоторых особенностей личности пользователя производится анализ и классификация постов, опубликованных в его аккаунте. Пусть необходимо произвести эту оценку для 100 человек. Предположим, что среднее количество постов на странице каждого пользователя 100. В итоге получаем, что необходимо клиссифицировать 10 000 постов и по каждой сотне сделать вывод о степени выраженности некоторых особенностей пользователей, их опубликовавших. Предположим, что эксперту необходимо для классификации поста 3 секунды и ещё 10 секунд, чтобы сделать выводы по полученной классификации. В этом случае для решения задачи будет потрачено более 8.5 часов рабочего времени. Программный модуь при таком количестве пользователей и постов на их странице будет работать не более 30 минут. Получаем, что автоматизация решения данной задачи позволяет ускорить оценку в 17 раз.

Аналогично рассмотрим задачу восстановления фрагмента метапрофиля пользователей организации, состоящей из 100 сотрудников. Пусть у каждого из этих сотрудников порядка 100 друзей и у каждого из этих друзей ещё по 100 друзей. Если среди этих аккаунтов не будет пересечений, а эксперт решит действовать, опираясь на предложенный в работе метод, то ему предстоит проанализировать 1 000 000 аккаунтов. Даже если предположить, что всю необходимую информацию, содержащуюся в аккаунте, он сможет извлечь за 1 секунду, то ему потребуется более 7 недель рабочего времени, чтобы произвести такой анализ. Разработанному программному модулю на ту же работу в среднем требуется от 110 до 120 минут, в зависимости от количества друзей пользователей, чьи аккаунты анализруются.

При построении оценок успеха распространения социоинженерной атаки от пользователя к пользователю необходимо агрегировать информацию о разных событиях, свидетельствующих об интенсивности взаимо-

действия. Для каждой пары пользователей необходимо проанализировать, отмечены ли они в семейном положении друг у друга, посчитать лайки, репосты друга друга, совместные фотографии. Пусть для рассчёта оценки вероятности успеха распространения социоинженерной атаки между парой пользователей эксперту необходима 1 минута. Если в компании работает 100 сотрудников, то эксперту необходимо произвести анализ 4950 пар пользователей. На эту работу будет затрачено более 82 часов рабочего времни или около 10 рабочих дней. Разработанный программный модуль производит рассчёт оценок и строит визаулизацию социального графа для 100 пользователей в среднем за 250 минут. Время работы зависит от количества публикуемого пользователями контента и интенсивности их связей с другими пользователями. Таким образом, автоматизация выполнения этой задачи позволяет выполнить работу примерно в 20 раз быстрее.

Представленные оценки времни, необходимого эксперту на анализ разных аспектов, участвующих в анализе защищённости пользователей информационной системы, скорее всего, меньше, чем реальные значения, поскольку эксперт может уставать от монотонной работы, иметь необходимость периодического отдыха. Но даже если предположить, что ему не нужно отдыхать в течение рабочего дня, то вряд ли он будет успевать производить некоторые операции за секунду, как представлено в примерах. Таким образом, финальные оценки повышения оперативности в результате 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 могут быть ещё выше.

4.7. ВЫВОДЫ ПО ГЛАВЕ 4

В главе 4 представлена архитектура и реализация новых моделей и методов, предложенных в диссертационном исследовании, в основных модулях прототипа комплекса программ для автоматизированной оценки успеха социоинженерной атаки злоумышленника на пользователя. Представлена структура основных модулей прототипа комплекса программ, приведены листинги классов, использующихся для автоматизации идентификации аккаунтов сотрудников компании в социальной сети. Приведены интерфейсы и реализация модуля, автоматизирующего построение оценок степени выраженности некоторых особенностей пользователей на основании анализа данных, извлекаемых из контента, публикуемого ими в социальных сетях. Представлена автоматизация восстановления фрагмента мета-профиля пользователя на основании анализа данных, извлекаемых из социального окружения пользователя, а также из других социальных сетей. Приведена реализация автоматизации построения оценок вероятности успеха многоходовой социоинженерной атаки. Отмечены достигаемые результаты повышения оперативности экспресс-оценки защищённости пользователей информационных систем за счёт автоматизации агрегации результатов анализа данных, извлекаемых из социальных сетей.

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 основанная 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 опирающийся на неё 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, автоматизирован-

ной 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.

Все результаты, выносимые на защиту, являются новыми. Предложены новые 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 модель и основанный на ней метод оценки вероятности успеха социоинженерной атаки злоумышленника на пользователя, опирающаяся на профили уязвимостей пользователя и компетенций злоумышленника. На её основе предложена новая вероятностная модель и метод оценки успеха многоходовой социоинженерной атаки. 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. Разработан прототип комплекса программ, в который внедрена реализация новых моделей и алгоритмов, предложенных в диссертации.

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).

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).

СЛОВАРЬ ТЕРМИНОВ

Атака (атакующее действие) — несанкционированная попытка использования уязвимого места. Обычно атаки имеют определенную цель, например, нарушение бизнес-процессов или кражу информации [182].

Безопасность информации — состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами [187].

Граф социальных связей — граф, узлы которого представлены социальными объектами, такими как пользовательские профили с различными атрибутами (например: имя, день рождения, родной город и т.д.), сообщества, медиа-контент и т.д., а ребра — социальными связями между ними [47].

Документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования [171, 172].

Доступ к информации — 1. ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации [179];

2. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств [122].

Защита информации от непреднамеренного воздействия — деятельность по предотвращению воздействия на защищаемую информацию от ошибок пользователей информации, сбоев технических и программных

средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [122].

Защита информации от несанкционированного воздействия — деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных правил и правил на изменение информации, приводящего к искажению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [122].

Защита информации от несанкционированного доступа — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации [122].

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации (иностранными) разведками [122].

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации [122].

Защищённость пользователя (персонала) — степень его устойчивости к социоинженерным атакующим воздействиям злоумышленника [81].

Информационная безопасность — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [172]. В качестве стандартной модели безопасности часто приводят модель CIA (конфиденциальность— confidentiality, целостность— integrity, доступность—availability). Выделяют и другие категории: аутентичность (возможность установления автора информации) и аппелируемость (возможность доказать, что автором является именно заявленный человек и никто другой).

Информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы [171].

Конкурентная разведка — сбор, обработка и анализ информации из различных источников, которая позволяет вырабатывать управленческие решения для повышения конкурентоспособности организации, проводимые без нарушения закона и с соблюдением этических норм [216].

Критичный документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, имеющей ценность для компании [96].

Мета-профиль пользователя — набор анкетных данных пользователя, таких как ФИО, возраст, родной город, город проживания и др.

Многоходовая социоинженерная атака — социоинженерная атака, при которой целевой пользователь атакуется через цепочку пользователей с ним связанных.

Пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею [171].

Программно-техническая атака — программно-техническое воздействие, направленное на активизацию уязвимости [96].

Промышленный шпионаж — это форма недобросовестной конкурентной разведки [137].

Профиль уязвимостей пользователя — набор уязвимостей пользователя, характеризующих склонность пользователей к тем или иным действиям в ответ на социоинженерные атакующих воздействия злоумышленника [109]. В диссертации формализован как совокупность пар название уязвимости-степень выраженности уязвимости.

Рефлексивное управление — процесс передачи оснований для принятия решений одним из противников другому [154, 163].

Социоинженерная (социотехническая атака) — набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [109].

Уязвимость пользователя — некоторая характеристика пользователя, которая делает возможным успех социоинженерного атакующего действия злоумышленника [109].

СПИСОК ЛИТЕРАТУРЫ

1. 2012 Cost of Cyber Crime Study: United States [Электронный ресурс]. — Ponemon Institute. — 2012. — October — Режим доступа: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.
2. 2013 Cost of Cyber Crime Study: United States [Электронный ресурс]. — Ponemon Institute. — 2013. — October — Режим доступа: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.
3. 2014 Cost of Cyber Crime Study: United States [Электронный ресурс]. — Ponemon Institute. — 2014. — October — Режим доступа: http://resources.idgenterprise.com/original/AST-0130677_2014_US_Cost_of_Cyber_Crime_Study_FINAL_2.pdf.
4. 2015 Cost of Cyber Crime Study: United States [Электронный ресурс]. — Ponemon Institute. — 2015. — October — Режим доступа: https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf.
5. 2016 Cost of Cyber Crime Study & the Risk of Business Innovation: — Ponemon Institute. — 2016. — October — Режим доступа: http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf
6. Abramov, M.V. Identifying user's of social networks psychological features on the basis of their musical preferences / M.V. Abramov, A.A. Azarov //, 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM’2017). — St. Petersburg, 2017. — P. 90–92.
7. 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.
8. Abu-Musa, Ahmad A. Perceived security threats of computerized accounting information systems in the Egyptian banking industry / Ahmad

A. Abu-Musa // Journal of Information Systems. — 2006. — Vol. 20 — № 1. — P. 187– 203.

9. Aleshnikov, S. Problems of information security of the firm (manufacture) and a way of their decision / S. Aleshnikov, M. Aleshnikova // Vestnik IKBFU. — 2014. — № 10. — P. 155–161.
10. Aliev, R.A. Semantic analysis and experimental selection of appropriate fuzzy logics / R.A. Aliev // Proccedings of First Internat. Conf. on Soft Computing and Computing with Words in System Analysis, Decision and Control. — Antalya, Turkey. Verlag b- Quadrat Verlag, 2001. — P. 29–42.
11. Aliev, R.A. Soft computing and its applications in business and economics / R.A. Aliev, B. Fazlollahi, R.R. Fazlollahi — Springer, 2012. — 445 p.
12. Alshboul, A. Information systems security measures and countermeasures: protecting organizational assets from malicious attacks / A. Alshboul // Communications of the IBIMA. — 2010. — P. 1–9.
13. 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
14. 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.
15. Baccelli, F. Pairwise stochastic bounded confidence opinion dynamics: Heavy tails and stability / F. Baccelli, A. Chatterjee, S. Vishwanath //

IEEE Transactions on Automatic Control. — 2017. — Vol. 62. — Issue 11. — P. 5678– 5693.

16. 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.
17. Beckers, K.A pattern-based method for establishing a cloud-specific information security management system / K. Beckers, I. Côté, S. Faßbender, M. Heisel, S. Hofbauer // Requirements Engineering. — 2013. — Vol. 18 — Issue 4. — P. 343–395.
18. Bell, D.C. Modeling HIV Risk [Epidemiology] / D.C. Bell, R.A. Trevino // J. Acquir Immune Defic Syndr. — 1999. — Vol. 22. — Issue 3. — P. 280–287.
19. Cattell, H.E.P. The Sixteen Personality Factor Questionnaire (16PF) / Heather E.P. Cattell, A.D. Mead // The Sage Handbook of Personality Theory and Assessment: Personality Measurement and Testing. — Los Angeles, 2008. — P. 135–159.
20. Collingwood, J. Preferred Music Style Is Tied to Personality [Электронный ресурс]. / J. Collingwood // Psych Central. — Режим доступа: http://psychcentral.com/lib/preferred-music-style-is-tied-to-personality/.
21. Conte, H. R. The Life Style Index: A self report measure of ego defenses / H. R. Conte, A. Apter // Ego defenses: Theory and measurement. — Oxford, England 1995. — P. 179–201.
22. Corbellini, A. DPM: A novel distributed large-scale social graph processing framework for link prediction algorithms / A. Corbellini, D. Godoy, C. Mateos, S. Schiaffino, A. Zunino // Future Generation Computer Systems.—2018. — Vol. 78. — P. 474–480.

23. Desnitsky, V.A. Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network / V.A. Desnitsky, I.V. Kotenko // Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on. — 2017. — P. 500–502.
24. Ding, D. A survey on security control and attack detection for industrial cyber-physical systems / D. Ding, Q.L. Han, Y. Xiang, X. Ge, X.M. Zhang // Neurocomputing. — 2018. — Vol. 275. — P. 1674–1683.
25. Distefano, S. Information dependability in distributed systems: The dependable distributed storage system / S. Distefano, A. Puliafito // Integrated Computer-Aided Engineering. — 2014. — Vol. 21 — Issue 1. — P. 3–18.
26. Du, J. Community-Structured Evolutionary Game for Privacy Protection in Social Networks / J. Du, C. Jiang, K.C. Chen, Y. Ren, H.V. Poor // IEEE Transactions on Information Forensics and Security. — 2018. — Vol. 13. — Issue 3. — P. 574–589.
27. Edwards, M. Panning for gold: automatically analysing online social engineering attack surfaces / M. Edwards, R. Larson, B. Green, A. Rashid, A. Baron // Computers & Security. — 2017. — № 69. — Vol. 18–34.
28. First Annual Cost of Cyber Crime Study [Электронный ресурс]. — Ponemon Institute. — 2010 — July — Режим доступа: http://www.greycastlesecurity.com/resources/documents/Ponemon_Cost_of_CyberCrime_Study_07-10.pdf.
29. Ginni Rometty on the End of Programming [Электронный ресурс] — Bloomberg. — 2017. — Режим доступа: https://www.bloomberg.com/news/features/2017-09-20/ginni-rometty-on-artificial-intelligence.
30. Gupta, B.B. Fighting against phishing attacks: state of the art and future challenges / B.B. Gupta, A. Tewari, A.K. Jain, D. P. Agrawal // Neural Computing and Applications. — 2017. — Vol. 28. — № 12. — P. 3629– 3654.

31. Heydt, G.T. Distribution system reliability evaluation using enhanced samples in a Monte Carlo approach / G.T. Heydt, T.J. Graf // IEEE Transactions on Power Systems. — 2010. — T. 25. — Issue. 4. — P. 2006–2008.
32. Huber, M. Cheap and automated socio-technical attacks based on social networking sites / M. Huber, M. Mulazzani, S. Schrittwieser, E. Weippl // Artificial Intelligence and Security. — 2010. — P. 61–64.
33. Huda, A.S.N. Accelerated distribution systems reliability evaluation by multilevel Monte Carlo simulation: implementation of two discretisation schemes / A.S.N. Huda, R. Živanović // IET Generation, Transmission & Distribution. — 2017. — T. 11. — №. 13. — P. 3397–3405.
34. Irani, D. Large online social footprints–an emerging threat / D. Irani, S. Webb, L. Kang, P. Calton // International Conference on Computational Science and Engineering (CSE'09). — IEEE, 2009. — T. 3. — P. 271– 276.
35. ISO/IEC 17799 [Электронный ресурс]. — Электрон. текстовые дан. и граф. дан. — 2005. — Режим доступа: http://comsec.spb.ru/matherials/is/iso17799-2005.pdf.
36. ISO/IEC/IEEE 9945:2009 [Электронный ресурс]. — Информационные технологии. Интерфейс переносимой операционной системы (POSIX). Базовые технические требования — Вып. 7. — Режим доступа: http:// www.iso.org.
37. Itradat, A. Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study / A. Itradat, S. Sultan, M. Al-Junaidi, R. Qaffaf, F. Mashal, F. Daas // Jordan Journal of Mechanical & Industrial Engineering. — 2014. — Vol. 8 — Issue 2. — P. 102–118.
38. Jansson, K. Phishing for phishing awareness / K. Jansson, R. Solms // Behaviour & Information Technology. — 2013. — Vol. 32 — Issue 6. — P. 584– 593.

39. Kohavi, R. A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection. / R. Kohavi — 14th International Joint Conference on Artificial Intelligence, Palais de Congres Montreal, Quebec, Canada. — 1995. — С. 1137–1145.
40. Kondakci S. Epidemic state analysis of computers under malware attacks / S. Kondakci, Suleyman // Simulation Modelling Practice & Theory. — 2008. — Vol. 16 — Issue 5. — P. 571–584.
41. Kotenko, I. Generation of Source Data for Experiments with Network Attack Detection Software / I. Kotenko, A. Chechulin, A. Branitskiy // Journal of Physics: Conference Series. — IOP Publishing, 2017. — Vol. 820. — № 1. — P. 012033.
42. Langford, J. Quantitatively Tight Sample Complexity Bounds. / J. Langford — Carnegie Mellon Thesis. — 2002. — 124 с.
43. Leach, J. Improving user security behavior / J. Leach // Computers & Security. — 2003. — Т. 22. — №. 8. — P. 685–692.
44. Leyden, J. Office workers give away passwords for a cheap pen / J. Leyden // The Register. — 2003. — Т. 18.
45. Liu, J. A digital memories based user authentication scheme with privacy preservation / J. Liu, Q. Lyu, Q. Wang, X. Yu // PloS ONE. — 2017. — Vol. 12. — №. 11. — P. 0186925.
46. Malhotra, A. Studying user footprints in different online social networks / A. Malhotra, L. Totti, Jr W. Meira, P. Kumaraguru, V. Almeida // IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM’2012). — 2012. — P. 1065–1070.
47. Melville, P. Content-Boosted Collaborative Filtering for Improved Recommendations / P. Melville, R. Mooney, R. Nagarajan // University of Texas, USA: Материалы конф. / AAAI-02, Austin, TX, USA, 2002. — 2002. — С. 187–192.

48. Music Recognition: Gracenote vs ACRCloud [Электронный ресурс] — Режим доступа: http://music-recognition-and-discovery.tumblr.com/post/142618395465/music-recognition-gracenote-vs-acrcloud.
49. North, A.C. Musical preference, deviance, and attitudes towards celebrities / A.C. North, L. Desborough, L. Skarstein // Personality and Individual Differences. — 2005. — Vol. 38. — P. 1903–1914.
50. North, A.C. The social and applied psychology of music / A.C. North, D.J. Hargreaves // Oxford: Oxford University Press. — 2008.
51. Oliveira, A.R. A Layered Trust Information Security Architecture / A.R. Oliveira, L.J.G. Villalba, A.L.S. Orozco, F. Buiati, T.H. Kim // Sensors (14248220). — 2014. — Vol. 14 — Issue 12. — P. 22754–22772.
52. Rentfrow, P.J. The Role of Music in Everyday Life: Current Directions in the Social Psychology of Music / P.J. Rentfrow // Social and Personality Psychology Compass. — 2012. — Vol. 6 — № 5. — P. 402–416.
53. Samsonovich, A. V. On a roadmap for the BICA Challenge / A. V. Samsonovich // Biologically Inspired Cognitive Architectures. — 2012. — Т. 1. — P. 100–107.
54. Schaik, P. Risk perceptions of cyber-security and precautionary behavior / P. Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, P. Kusev // Computers in Human Behavior. — 2017. — Vol. 62. — Issue 11. — P. 5678–5693
55. Schwartz, S.H. An Overview of the Schwartz Theory of Basic Values / S.H. Schwartz // Online readings in Psychology and Culture. — 2012. — Vol. 2. — №. 1. — P. 11.
56. Second Annual Cost of Cyber Crime Study 2011 [Электронный ресурс]. — Ponemon Institute. — 2011. — August. — Режим доступа: http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf.

57. Shaw, E. The insider threat to information systems: The psychology of the dangerous insider / Shaw E., Ruby K.G., Post J.M. // Security Awareness Bulletin. — 1998. — T. 2. — №. 98. — P. 1–10.

58. 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.

59. Siadati, H. Mind your SMSes: Mitigating social engineering in second factor authentication / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon // Computers & Security. — 2017. — T. 65. — P. 14–28.

60. Social networks in Russia, winter 2015–2016. Numbers, trends, predictions [Электронный ресурс]. // Brand Analytics. — 2016. — Режим доступа: https://blog.br-analytics.ru/socialnye-seti-v-rossii-zima-2015-2016-cifry-trendy-prognozy/.

61. Stegner B. Which Music Identification App Is King? [Электронный ресурс] / B. Stegner // Режим доступа: http: //www.makeuseof.com/tag/music-identification-app-king/.

62. Struharik, R. A system for hardware aided decision tree ensemble evolution / R. Struharik, B. Vukobratović // Journal of Parallel and Distributed Computing. — 2018. — T. 112. — P. 67–83.

63. Su, S. Location-aware targeted influence maximization in social networks / S. Su, X. Li, X. Cheng, C. Sun // Journal of the Association for Information Science and Technology. — 2018. — Vol. 69. — № 2. — P. 229–241.

64. Terlizzi, M.A. Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance / M. A. Terlizzi, F. S. Meirelles, M. A. Viegas Cortez da Cunha // Journal of Applied Security Research. — 2017. — T. 12. — №. 2. — P. 224–252.

65. 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, Abramov M.V., Azarov A.A., Bordovskaya N.V. // Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. — 2016. — P. 31– 38.
66. Widman, J. 10 Massive Security Breaches [Электронный ресурс] / J. Widman // Information week Security — 2011. — Режим доступа: http://www.darkreading.com/attacks-and-breaches/10-massive-security-breaches/d/d-id/1096539.
67. Yang, J.L. Research on the reliability of distribution network and its influencing factors / J.L. Yang, C.G. Ma, Z.G. Lu, Y. Bai // Applied Mechanics and Materials. Trans Tech Publications. — 2014. — Vol. 490. — P. 1661–1665.
68. Zhang J. Information Security Risk Assessment of Smart Grid Based on Absorbing Markov Chain and SPA / J. Zhang, Q. Zeng, Y. Song, L. Cunbin // International Journal of Emerging Electric Power Systems. — 2014. — Vol. 15 — № 6. — P. 527–532.
69. Zweig, M.H. Receiver-operating characteristic (ROC) plots: a fundamental evaluation tool in clinical medicine / M.H. Zweig, G. Campbell // Clinical chemistry. — 1993. — Vol. 39. — №. 4. — P. 561–577.
70. Абдурахманова, К.Ф Программная реализация имитации социоинженерных атак с помощью марковских полей / К.Ф. Абдурахманова, М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев, Т.В. Тулупьева // Материалы 6-й всероссийской научной конференции по проблемам информатики «СПИСОК-2016». — СПб.: ВВМ. — Санкт-Петербург, 2016. — 26–29 апреля — С. 427–435.
71. Абрамов М.В. Комплекс программ для анализа достижимости критических документов и защищённости пользователей информационных систем / М.В. Абрамов // Материалы IX Санкт-Петербургская межрегиональной конференции «Информационная безопасность

регионов России» (ИБРР’2015). — СПб: СПОИСУ. — Санкт-Петербург, 2015. — 28–30 октября — С. 326.

72. Абрамов, М.В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак / М.В. Абрамов // Автоматизация процессов управления. — 2018. — №1.
73. 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.
74. Абрамов, М.В. Выявление психологических особенностей пользователей социальных сетей на основании музыкальных предпочтений / М.В. Абрамов, А.А. Азаров // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2017) в 2 т.— Санкт-Петербург, 2017. — 1 т. — С. 130–133.
75. Абрамов, М.В. Задачи анализа защищенности 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
76. Абрамов, М.В. Комплекс «критические документы — информационная система — персонал — злоумышленник» / М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева, А.Л. Тулупьев // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР’2015) — СПб.: СПОИСУ. — Санкт-Петербург, 2015. — 28–30 октября — С. 326–327
77. Абрамов, М.В. Концепция анализа распространения контента в социальных медиа на основании методов анализа защищенности пользователей информационных систем от социо-инженерных

атак / М.В. Абрамов, А.А. Азаров // Материалы XIV Санкт-Петербургской международной конференции Региональная Информатика (РИ’2014). — Санкт-Петербург, 2014. — С. 543.

78. Абрамов, М.В. Модели распространения информации в социальных медиа / М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев, А.А. Фильченков // Материалы Третьей Международной научно-практической конференции «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC’14). — Москва, 2014. — С. 112– 115.
79. Абрамов, М.В. Модели распространения информационных сообщений в социальных сетях / М.В. Абрамов, А.Л. Тулупьев, А.А. Азаров, А.А. Фильченков // Научная сессия НИЯУ МИФИ-2015 «Интеллектуальные системы и технологии» в 3 т. Аннотации докладов. — М.: НИЯУ МИФИ. — Москва, 2015. — 3 т. — С. 137.
80. Абрамов, М.В. Моделирование социоинженерных атак с использованием байесовских сетей доверия / М.В. Абрамов, А.А. Азаров // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2017) в 2 т. — Санкт-Петербург, 2016. — 1 т. — С. 71– 74.
81. 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.
82. Абрамов, М.В. Оценка вероятности успеха социоинженерного атакующего воздействия / М.В. Абрамов // Сборник научных трудов IV Международной летней школы-семинара по искусственному интеллекту для студентов, аспирантов, молодых ученых и специали-

стов «Интеллектуальные системы и технологии: современное состояние и перспективы» (ISYT'2017) — СПб.: Политехника-сервис. — Санкт-Петербург, 2017. — 30 июня – 3 июля — С. 9–14.

83. Абрамов, М.В. Подход к оценке вероятности успешности социоинженерной атаки / М.В. Абрамов // Материалы 6-й всероссийской научной конференции по проблемам информатики «СПИСОК-2016» — СПб.: ВВМ. — Санкт-Петербург, 2016. — 26–29 апреля — С. 436–442.
84. Абрамов, М.В. Подход к оценке защищённости пользователей информационных систем от социоинженерных атак / М.В. Абрамов // Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика» (РИ’2016). — СПб: СПОИСУ. — Санкт-Петербург, 2016. — 26–28 октября — С. 514.
85. Абрамов, М.В. Подход к построению системы упреждающей диагностики уязвимостей персонала к социоинженерным атакам / М.В. Абрамов // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР’2017). — СПб: СПОИСУ — Санкт-Петербург, 2017. — 1–3 ноября — С. 409–410.
86. Абрамов, М.В. Применение моделей распространения информации в социальных сетях к задачам анализа защищённости пользователей информационных систем от социо-инженерных атак / М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев, А.А. Фильченков // Нечёткие системы и мягкие вычисления (НСМВ’2014): труды Шестой всероссийской научно-практической конференции в 2 т. — СПб.: Политехника-сервис. — Санкт-Петербург, 2014. — 27-29 июня — 2 т. — С. 55–58.
87. Абрамов, М.В. Применение социальных сетей для анализа защищённости пользователей компании от социоинженерных атак / М.В.

Абрамов // Материалы Четвёртой Международной научно-практической конференции «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC’15) — Москва, 2015. — С. 294–297.

88. Абрамов, М.В. Распространение социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей / М.В. Абрамов, А.А. Азаров, А.А. Фильченков // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2015) в 2 т. — Санкт-Петербург, 2015. — 1т. — С. 329–331.
89. Абрамов, М.В. Реляционная модель расчёта вероятностной оценки уровня защищённости пользователя от социоинженерных атак / М.В. Абрамов // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием (КИИ’2016) — Смоленск: Универсум, 2016. — 3–7 октября — 1 т. — С. 203–211.
90. 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.
91. Азаров, А.А. Анализ распространения вредоносного контента среди пользователей социальных медиа / А.А. Азаров, А.А. Фильченков, М.В. Абрамов // Материалы всероссийской научной конференции по проблемам информатики «СПИСОК-2014» — СПб.: ВВМ — Санкт-Петербург, 2014. — С. 540–546.
92. Азаров, А.А. Основы мониторинга защищённости персонала информационных систем от социотехнических атак / А.А. Азаров // Труды СПИИРАН. — 2012. — Вып. 23. — С. 30–49.

93. Азаров, А.А. Представление комплекса «информационная система—критичные документы—персонал—злоумышленник» с помощью реляционно-алгебраического подхода / А.А. Азаров, А.А. Фильченков, М.В. Абрамов, А.Л. Тулупьев // Труды Международной конференции по мягким вычислениям и измерениям (SCM’2014) в 2 т. — Санкт-Петербург, 2014. — 1 т. — С. 66–69.

94. Азаров, А.А. Применение алгоритма обхода в ширину графа межличностных связей для анализа защищенности пользователей информационных систем / А.А. Азаров, М.В. Абрамов, Т.В Тулупьева // Интегрированные модели и мягкие вычисления в искусственном интеллекте. Сборник научных трудов VIII-ой Международной научно-технической конференции в 2 т. – М.: Физматлит. — Коломна, 2015. — 18–20 мая —2 т. — С. 774–779.

95. 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. —10 т. — № 2. — С. 209–221.

96. 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.

97. Азаров, А.А. Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищённости персонала информационных систем от социоинженерных атак: дис. канд.тех.нук: 05.13.19 / Азаров Артур Александрович. — СПб., 2013. — 232 с.

98. Алексеевских А. Мошенники изобрели способ звонить за счёт граждан [Электронный ресурс] / А. Алексеевских // Известия. — Режим

доступа: https://iz.ru/658024/anastasiia-alekseevskikh/v-rossii-poiavilas-novaia-moshennicheskaia-skhema.

99. Алиев, Р.А. Интеллектуальные роботы с нечёткими базами знаний / Р.А. Алиев — М.: Радио и связь, 1995. — 178 с.
100. Андрианов, В. В. Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В.В. Андрианов. — Режим доступа: http://bezopasnik.org/article/book/andrianov_infobez_biz_2011.pdf.
101. Багрецов, Г.И. Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети / Г.И. Багрецов, Н.А. Шиндарев, М.В. Абрамов, Т.В. Тулупьева // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВИТ–2017) в 2 т. — СПб.: Политехника-сервис. — Санкт-Петербург, 2017. — 3–7 июля — 1 т. — С. 9– 16.
102. Багрецов, Г.И. Подходы к разработке моделей для анализа текстовой информации в профилях социальной сети в целях построения профиля уязвимостей пользователя / Г.И. Багрецов, Н.А. Шиндарев, М.В. Абрамов, Т.В. Тулупьева // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2017) в 2 т. — Санкт-Петербург, 2017. — 1 т. — С. 134–137.
103. Бартунов, С. Идентификация пользователей социальных сетей в Интернет на основе социальных связей / С. Бартунов, А. Коршунов // Доклады Всероссийской научной конференции «Анализ изображений, сетей и текстов» (АИСТ–2012) — Екатеринбург, 2012. — 16– 18 марта.
104. Батыршин И.З., Недосекин А.О., Стецко А.А., Тарасов В.Б., Язенин А.В., Ярушкина, Н.Г. Нечёткие гибридные системы. Теория и практика / Н.Г. Ярушкина — М.: ФИЗМАЛИТ, 2007. — 208 с.

105. Блинкова, О. Среднегодовой убыток от киберпреступности составил для российских компаний $2,4 млн / О. Блинкова // IT News. — 2015. — № 10 (242). — С. 14.
106. Бондаренко, С.В. «Электронное государство» как социотехническая система / Бондаренко С.В. — Ростов-на-Дону: Центр прикладных исследований интеллектуальной собственности, 2005. — 6 с.
107. Бушмелёв Ф.В. Подход к построению профиля компетенций злоумышленника в задаче анализа защищённости информационной системы от социоинженерных атак / Ф.В. Бушмелёв, М.В. Абрамов // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР’2017) — СПб: СПОИСУ. — Санкт-Петербург, 2017. — 1–3 ноября — С. 413–414.
108. Бушмелёв, Ф.В. Обзор программного инструментария для визуализации сетей в микромире корпоративных офисов / Ф.В. Бушмелёв, М.В. Абрамов // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВИТ–2017) в 2 т. — СПб.: Политехника-сервис. — Санкт-Петербург, 2017. — 2 т. — С. 34–42.
109. Бычек В. Социальная инженерия в интеллектуальной битве «добра» и «зла» / В. Бычек, Е. Ершова // Защита информации. Инсайд. — 2006. —№ 6. — С. 20–27.
110. В Mossack Fonseca назвали "преступлением" утечку документов об офшорах [Электронный ресурс]. — Новости Mail.ru. — 2016. — Режим доступа: https://news.mail.ru/incident/25345775/?frommail=1.
111. Ванюшичева, О.Ю. Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками. / О.Ю. Ванюшичева, Т.В. Тулупьева, А.Е. Пащенко, А.Л. Тулупьев, А.А. Азаров // Труды СПИИРАН. — 2011. — Вып. 19. — С. 34– 47.

112. Веденеев, В.С. Средства поиска инсайдеров в корпоративных информационных системах / В.С. Веденеев, И.В. Бычков // Безопасность информационных технологий. — 2014. — № 1. — С. 9–13
113. Вихорев, С.В. Классификация угроз информационной безопасности [Электронный ресурс] / С.В. Вихорев // 2001. — Режим доступа: http://www.elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf.
114. Возможные угрозы информационной безопасности и их специфика [Электронный ресурс]. — Сайт E-NIGMA.RU. — Режим доступа: http://www.e-nigma.ru/stat/dip_2/.
115. Воробьев, В.И. Динамический метод обнаружения уязвимостей / В.И. Воробьев, Р.Р. Фаткиева //Информационно-измерительные и управляющие системы. — 2009. — Т. 7. — № 11. — С. 28–31.
116. Воробьев, В.И. Моделирование сетевого трафика методом Монте-Карло / В.И. Воробьев, Е.Л. Евневич, Р.Р. Фаткиева // Вестник Бурятского государственного университета. — 2010. — № 9. — С. 258–262.
117. Выписка из концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс]. — ФСБ РФ. — 2014. — Режим доступа: http://www.fsb.ru/files/PDF/Vipiska_iz _koncepcii.pdf.
118. Гатчин, Ю.А. Теория информационной безопасности и методология защиты информации. / Ю.А. Гатчин, В.В. Сухостат // СПб.: СПбГУ ИТМО. — 2010. — 98 с.
119. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. — М.: Стандартинформ, 2013. — 52 с.

120. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности. — М.: Стандартинформ, 2014. — 156 с.
121. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Компоненты доверия к безопасности. — М.: Стандартинформ, 2014. — 145 с.
122. ГОСТ Р. 50922-2006 Защита информации. Основные термины и определения. — М., 2008. — 12 с.
123. Демидова, Н. Два билета в мышеловке [Электронный ресурс] / Н. Демидова // Лаборатория Касперского. — Режим доступа: https://securelist.ru/two-tickets-trap/30831/.
124. Дорохов, В.Э. О рисках потери репутации организации вследствие инцидентов информационной безопасности / В.Э. Дорохов // Безопасность информационных технологий. — 2014. — №2. — С. 80– 82.
125. Дураковский, А.П. Целевые атаки с использованием уязвимости CVE-2013-3897 / А.П. Дураковский, Д.А. Мельников, В.Г. Сергеев // Безопасность информационных технологий. — 2014. — №3. — С. 60–65.
126. Зегжда, П.Д. Использование искусственной нейронной сети для определения автоматически управляемых аккаунтов в социальных сетях / П.Д. Зегжда, Е.В. Малышев, Е.Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы. — 2016. — № 4. — С. 9–15.
127. Зегжда, П.Д. Моделирование информационных систем для решения задачи управления безопасностью / П.Д. Зегжда, Д.П. Зегжда, А.И. Печенкин, М.А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы. — 2016. — № 3. — С. 7–16.

128. Зегжда, П.Д. Подход к построению обобщенной функционально-семантической модели кибербезопасности / П.Д. Зегжда, Д.П. Зегжда, Т.В. Степанова // Проблемы информационной безопасности. Компьютерные системы. — 2015. — № 3. — С. 17–25.
129. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса [Электронный ресурс]. — Лаборатория Касперского, 2014. — Режим доступа: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf.
130. Информационная безопасность предприятия. Информационная защита бизнеса [Электронный ресурс]. — SafenSoft. — Режим доступа: http://www.safensoft.ru/security.phtml?c=775.
131. Как определить характер по музыке [Электронный ресурс]. — Режим доступа: http://revisio.net/character/.
132. Как узнать характер человека по его любимой музыке? [Электронный ресурс]. — Режим доступа: http://www.gohappy.ru/article/689.
133. Касперский, Е. Современные угрозы информационной безопасности: классификация, причины и способы устранения [Электронный ресурс] / Е. Касперский // Бюллетень JetInfo. — 2004. — Режим доступа: http://www.nestor.minsk.by/sr/2004/04/40413.html.
134. Классификация web-атак [Электронный ресурс]. — Об Интернете, информационных технологиях и не только — Стайлер.рф, 2007. — Режим доступа: http://www.styler.ru/styler/classes-web-attack/.
135. Козлов, Д.Д. Использование интеллектуальных агентов для поиска информации в Интернет [Электронный ресурс] / Д.Д. Козлов, Р.Л. Смелянский // 2000. — Режим доступа: http://ea.dgtu.donetsk.ua:8080/bitstream/123456789/22964/1 использование интеллектуальных агентов для.pdf.

136. Колесов, Д.Н. Оценка вероятностей альтернатив по ординальной и интервальной экспертной информации / Д.Н. Колесов, Н.В. Хованов, М.С. Юдаева // Применение математики в экономике. — 2009. — С. 82–107.

137. Конкурентная разведка или промышленный шпионаж [Электронный ресурс]. — Корпоративный менеджмент. — Режим доступа: https://stakhanovets.ru/blog/promyshlennyj-shpionazh-socialnaya-inzheneriya/.

138. Корнеев, А.А. Условия применимости критериев Стъюдента и Манна-Уитни / А.А. Корнеев, А.Н. Кричевец // Психологический журнал. — 2011. — 32 т. — № 1. — С. 97–110.

139. Коршунов, А. Анализ социальных сетей: методы и приложения / А. Коршунов, И. Белобородов, Н. Бузун, В. Аванесов, Р. Пастухов, К. Чихрадзе, И. Козлов, А. Гомзин, И. Андрианов, А. Сысоев, С. Ипатов, И Филоненко., К. Чуприна, Д Турдаков., С. Кузнецов // Труды Института системного программирования РАН. – 2014. – Т. 26. – № 1. — С. 439–454.

140. Котенко, Д.И. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы / Д.И. Котенко, И.В. Котенко, И.Б. Саенко // Труды СПИИРАН. — 2012. — Вып. 22. — С. 5– 30.

141. Котенко, И.В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак / И.В. Котенко, М.В. Степашкин, Е.В. Дойникова // Проблемы информационной безопасности. Компьютерные системы. — 2011. — № 3. — С.40–57.

142. Котенко, И.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак / И.В. Котенко, М.В. Степашкин // Тр. ИСА РАН. — 2007. — Т. 31. — С. 126–207.

143. Котенко, И.В. Анализ защищенности компьютерных сетей на этапах проектирования и эксплуатации / И.В. Котенко, М.В. Степашкин, В.С. Богданов // Изв. вузов. Приборостроение. — 2006. — 49 т. — № 5. — С. 3–8.

144. Котенко, И.В. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников / И.В. Котенко, М.В. Степашкин, В.С. Богданов // Проблемы информационной безопасности. Компьютерные системы. — 2006. — № 2. — С. 7–24.

145. Котенко, И.В. Использование ложных информационных систем для защиты информационных ресурсов компьютерных сетей / И.В. Котенко, М.В. Степашкин // Проблемы информационной безопасности. Компьютерные системы. — 2005. — № 1. — С. 63–73.

146. Котенко, И.В. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности / И.В. Котенко, М.В. Степашкин, В.С. Богданов // Труды СПИИРАН. — 2006. — Т. 2. — № 3. — С. 30– 49.

147. Котенко, И.В. Оценка защищенности информационных систем на основе построения деревьев социо-инженерных атак / И.В. Котенко, М.В. Степашкин, Д.И. Котенко, Е.В. Дойникова // Изв. вузов. Приборостроение — 54 т. — № 12. — 2011. — С. 5–9.

148. Котенко, И.В. Перспективные направления исследований в области компьютерной безопасности. / И.В. Котенко, Р.М. Юсупов // Защита информации. Инсайд. — 2006. — № 2. — С. 46.

149. Котенко, И.В. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства / И.В. Котенко, И.Б. Саенко // Труды СПИИРАН. — 2012. — Вып. 22. — С. 84– 100.

150. Котенко, И.В. Применение технологии управления информацией и событиями безопасности для защиты информации в критически

важных инфраструктурах / И.В. Котенко, И.Б. Саенко, О.В. Полубелова, А.А. Чечулин // Труды СПИИРАН. — 2012. — Вып. 20. — С. 27–56.

151. Котенко, И.В. Системы-имитаторы: назначение, функции, архитектура и подход к реализации / И.В. Котенко, М.В. Степашкин // Изв. вузов. Приборостроение. — 2006. — 49 т. — № 3. — С. 3–8.
152. Котенко, И.В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода “нервная система сети” / И.В. Котенко, А.В. Шоров // Труды СПИИРАН. — 2012. — Вып. 22. — С. 45–70.
153. Крук, Е.А. Расчет вероятностных характеристик для дискретных каналов с памятью / Е.А. Крук, В.Б. Прохорова // Информационно-управляющие системы. — 2007. — № 5. — С. 56–58.
154. Лефевр, В.А. Алгебра конфликта / В.А. Лефевр, Г.Л. Смолян — М.: Знание, 1968. — 64 с.
155. Майер, Р.В. Компьютерная двухкомпонентная вероятностная модель изучения дисциплины / Р.В. Майер //Современное образование. — 2015. — №. 1. — С. 42–52.
156. Малюк, А.А. Теория защиты информации / А.А. Малюк — М.: Горячая линия — Телеком, 2012. — 184 с.
157. Митник, К. Д. Искусство обмана. / К. Д. Митник, В. Л. Саймон — М.: Компания АйТи, 2004. — 416 с.
158. Музыка и характер человека (Скажи мне, что ты слушаешь и я скажу кто ты) [Электронный ресурс]. — Режим доступа: http://mymusicmy.ru/music-help-life/muzyika-i-harakter
159. Нестерук Ф.Г., Молдовян А.А., Нестерук Г.Ф., Нестерук Л.Г. Квазилогические нейронечеткие сети для решения задачи классификации в системах защиты информации //Вопросы защиты информации. — 2007. — № 1. — С. 23–31.

160. Нестерук, Г.Ф. Организация иерархической защиты информации на основе интеллектуальных средств нейронечеткой классификации / Г.Ф. Нестерук, А.А. Молдовян, Ф.Г. Нестерук, А.А. Костин, С.И. Воскресенский // Вопросы защиты информации. — 2005. — №. 3. — С. 16–26.

161. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09.05.2017 No 203 [Электронный ресурс]. — Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201705100002

162. Общемировые убытки от киберпреступности составят $2.1 трлн до 2019 года [Электронный ресурс]. — Security Lab. — 2015. — Режим доступа: http://www.securitylab.ru/news/472924.php.

163. Осипов, В.Ю. Оценка информации в интересах рефлексивного управления конкурентами / В.Ю. Осипов, А.П. Кондратюк // Программные продукты и системы. — 2010. — № 2. — С. 64–68.

164. Осипов, В.Ю. Проблемы защиты от ложной информации в компьютерных сетях / В.Ю. Осипов, В.И. Воробьев, Д.К. Левоневский // Труды СПИИРАН. — 2017. — Т. 4. — № 53. — С. 97–117.

165. Осторожно: обнаружена новая схема обмана в Интернете [Электронный ресурс]. — Новости Mail.ru. — Режим доступа: https://hi-tech.mail.ru/news/internet-fraud-scheme/?frommail=1.

166. Пентагон подсчитал, что Э. Сноуден похитил 1,7 млн секретных файлов [Электронный ресурс]. — РБК. — 2014. — Режим доступа: http://top.rbc.ru/politics/10/01/2014/898589.shtml.

167. Подросток рассказал, как была взломана почта директора ЦРУ [Электронный ресурс]. — Hi-tech вести. — 2015. — Режим доступа: http://hitech.vesti.ru/news/view/id/7905.

168. Полубелова, О.В. Построение онтологий уязвимостей и применение логического вывода для управления информацией и событиями безопасности / О.В. Полубелова, И.В. Котенко // Безопасность информационных технологий. — 2013. — №1. — С. 21–24.
169. Промышленный шпионаж: социальная инженерия [Электронный ресурс]. — Стахановец: система контроля сотрудников. — Режим доступа: https://stakhanovets.ru/blog/promyshlennyj-shpionazh-socialnaya-inzheneriya/.
170. Путин утвердил новую доктрину информационной безопасности вселенной [Электронный ресурс]. — Новости Mail.ru. — 2016. — Режим доступа: https://news.mail.ru/politics/28029797/?frommail=1.
171. Российская Федерация. Законы. Закон Российской Федерации «Об информации, информатизации и защите информации» // Федер. закон : в ред. от 10.01.2003 №15-ФЗ.— М. : Ось-89, 2005. — 32 с.
172. Российская Федерация. Законы. Закон Российской Федерации «Об участии в международном информационном обмене» // Федер. закон: от 04.07.96 №85-ФЗ.
173. Рост объёма информации — реалии цифровой вселенной [Электронный ресурс]. — Технологии и средства связи. — 2013. — №1. — Режим доступа: http://www.tssonline.ru/articles2/fix-corp/rost-obema-informatsii--realii-tsifrovoy-vselennoy.
174. Рудченко, А.Д. Управление системами безопасности бизнеса [Электронный ресурс] / А.Д. Рудченко, А.В. Юрченко // Институт проблем безопасности. — Режим доступа: https://www.hse.ru/data/2015/02/19/1091002877/%D0%A2%D0%B5%D0%BC%D0%B0%20%E2%84%96%206.pptx.
175. С инсайдерской активностью можно успешно бороться. [Электронный ресурс]. — Компания Arinteg. — Режим доступа: http://www.arinteg.ru/ articles/s-insayderskoy-aktivnostyu-mozhno-uspeshno-borotsya-123099.html.

176. Самые популярные социальные сети в России 2016 [Электронный ресурс]. — Режим доступа: http://www.pro-smm.com/populyarnye-socialnye-seti-v-rossii-2016/.
177. Санжиев, А. Базы данных сайта Booking.com попали в руки мошенников [Электронный ресурс] / А. Санжиев // Вести. — 2015. — Режим доступа: http://www.vesti.ru/doc.html?id=2673139.
178. Сапронов, К. Человеческий фактор и его роль в обеспечении информационной безопасности [Электронный ресурс] / К. Сапронов // Режим доступа: http://www.interface.ru/home.asp?artId=17137.
179. Сборник руководящих документов по защите информации от несанкционированного доступа // М.: Гостехкомиссия России. — 1998.
180. Сергиевский, М. Сети – что это такое / М. Сергиевский // КомпьютерПресс. — 1999. — № 10. — С. 3–9.
181. Слёзкин, Н.Е. Подход к восстановлению мета-профиля пользователя информационной системы на основании данных из социальных сетей / Н.Е. Слёзкин, М.В. Абрамов, Т.В. Тулупьева // Сборник научных трудов Первой Всероссийской научно-практической конференции «Нечёткие системы и мягкие вычисления. Промышленные применения». — Ульяновск, УлГТУ, 2017. — 14–15 ноября — С. 394–399.
182. Словарь терминов. Современные подходы к обеспечению информационной безопасности [Электронный ресурс] // Режим доступа: http:// microsoft.com/Rus/Government/Newsletters/Issue22/07.mspx.
183. Смирнов, Е. Репутационный вред от киберпреступлений вдвое превышает финансовые потери банков [Электронный ресурс] / Е. Смирнов // Cnews, издание о высоких технологиях. — 2013. — Режим доступа: http://www.cnews.ru/news/top/reputatsionnyj_vred_ot_kiberprestuplenij.

184. Социальные сети в России [Электронный ресурс]. — Mail.Ru Group. — 2014. — Режим доступа: https://corp.imgsmail.ru/media/files/issledovanie-auditorij-sotcialnykh-setej.pdf.

185. Социальные сети в России, зима 2015–2016. Цифры, тренды, прогнозы. [Электронный ресурс]. — Brand Analytics. — 2016. — Режим доступа: https://blog.br-analytics.ru/socialnye-seti-v-rossii-zima-2015-2016-cifry-trendy-prognozy/.

186. Социальные сети в России, осень 2016. Цифры, тренды, прогнозы [Электронный ресурс]. — Digital. — 2016. — Режим доступа: https://adindex.ru/publication/analitics/100380/2016/12/8/156545.phtml

187. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Решение Коллегии Гостехкомиссии России №7/02.03.01 г. [Электронный ресурс] // Режим доступа: http: // www.confidentiality.strongdisk.ru.

188. Степашкин, М.В. Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак: дис. канд. техн. наук: 05.13.19 / Степашкин Михаил Викторович — СПб.:СПИИРАН, 2002. — 196 с.

189. Стюгин, М.А. Противодействие несанкционированному доступу путём модификации структур информированности субъектов / М.А. Стюгин // Безопасность информационных технологий. — 2014. — №3. — С. 105– 111.

190. Суворова, А.В. Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения / А.В. Суворова, А.Л. Тулупьев, А.Е. Пащенко, Т.В. Тулупьева, Т.В. Красносельских // Компьютерные инструменты в образовании. — 2010. — №4. — С. 30–38.

191. Суворова, А.В. Вероятностные графические модели социально-значимого поведения индивида, учитывающие неполноту инфор-

мации / А.В. Суворова, Т.В. Тулупьева, А.Л. Тулупьев, А.В. Сироткин, А.Е. Пащенко // Труды СПИИРАН. — 2012. — 3 т. — №. 22. — С. 101–112.

192. Сулейманов, А.А. Подход к построению и анализу социального графа сотрудников некоторой компании / А.А. Сулейманов, М.В. Абрамов // Сборник научных трудов Первой Всероссийской научно-практической конференции «Нечёткие системы и мягкие вычисления. Промышленные применения. — Ульяновск, УлГТУ, 2017. — 14–15 ноября — С. 389– 393.
193. Толмачев, И.Л. Бинарная классификация на основе варьирования размерности пространства признаков и выбора эффективной метрики / И.Л. Толмачев, М.В. Хачумов // Искусственный интеллект и принятие решений. — 2010. — №. 2. — С. 3–10.
194. Тулупьев, А.Л. Защита конфиденциальных данных на интернет-портале редакции электронного научного журнала / А.Л. Тулупьев, М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева // VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР’2013). — СПб.: СПОИСУ — Санкт-Петербург, 2013. — 23–25 октября — С. 228–229.
195. Тулупьев, А.Л. Информационная модель пользователя, находящегося под угрозой социоинженерной атаки / А.Л. Тулупьев, А.А. Азаров, А.Е. Пащенко // Труды СПИИРАН. — 2010. —Вып. 2 (13). — С. 143–155.
196. 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, А.В. Торопова, Д.Г. 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. — 4 т. — 300 с.

197. Тулупьев, А.Л. Психологические особенности персонала, предрасполагающие к успешной реализации социо-инженерных атак / А. Л. Тулупьев, Т. В. Тулупьева, А. А. Азаров, О. Ю. Григорьева // Научные труды Северо-Западного института управления РАНХиГС. — 2012. — 3 т. — Вып. 3(7). — С. 256–266.

198. Тулупьева, Т.В. Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак / Т.В. Тулупьева, А.Л. Тулупьев, А. А. Азаров, А. Е. Пащенко // Труды СПИИРАН. — 2011. — Вып. 18. — С. 74–92.

199. Тумоян, Е.П. Метод оптимизации автоматической проверки уязвимостей удалённых информационных систем / Е.П. Тумоян, Д.А. Кавчук // Безопасность информационных технологий. — 2013. — №1. — С. 25– 30.

200. Угрозы информационной безопасности предприятия. [Электронный ресурс]. — Компания Arinteg. — Режим доступа: http://www.arinteg.ru/ articles/ugrozy-informatsionnoy-bezopasnosti-25800.html.

201. Угрозы информационной безопасности. [Электронный ресурс]. — Безопасность жизнедеятельности. — Режим доступа: http://www.bezzhd.ru/ 91_ugrozy_informacionnoj_bezopasnosti.

202. Указ Президента РФ от 15.01.2013 N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс]. — Российская Газета. — 2013. — Режим доступа: http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html.

203. Ущерб от киберпреступлений в банковской сфере РФ снизился в три раза [Электронный ресурс]. — Интерфакс. — 2015. — Режим доступа: http://www.interfax.ru/russia/473574.

204. Фролова, А.Н. Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы/ А.Е. Пащенко, Т.В. Тулупьева, А.Л. Тулупьев // Труды СПИИРАН. — 2008. — № 7. — С. 170–176.

205. Фролова, А.Н. Возможный подход к анализу защищенности информационных систем от социоинженерных атак / Т.В. Тулупьева, А.Е. Пащенко, А.Л. Тулупьев // Труды V Санкт-Петербургская региональная конференции «Информационная безопасность регионов России» (ИБРР-2007) (Санкт-Петербург, 23–25 октября 2007 г.) — СПб.: СПОИСУ, 2007. — С. 195–199.

206. Фролова, Е. Самые популярные социальные сети в России [Электронный ресурс] / Е. Фролова // Про СММ. Просто о фейсбук и инстаграм. — 2016. — Режим доступа: http://www.pro-smm.com/populyarnye-socialnye-seti-v-rossii/.

207. Чалдини, Р. Психология влияния. Убеждай, воздействуй, защищайся / Р. Чалдини — СПб.: Питер. — 2010. — 336 с.

208. Чечулин, А.А. Методика оперативного построения, модификации и анализа деревьев атак / А.А. Чечулин // Труды СПИИРАН. — 2013. — Т. 26. — С. 40–53.

209. Чечулин, А.А. Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак / А.А. Чечулин, И.В. Котенко // Проблемы информационной безопасности. Компьютерные системы. — 2014. — № 3. — С. 56–59.

210. Чечулин, А.А. Построение графов атак для анализа событий безопасности / А.А. Чечулин, И.В. Котенко // Безопасность информационных технологий. — 2014. — № 3. — С.135–141.

211. Шиндарев, Н.А. Построение вероятностной графической модели для оценки успешности социоинженерной атаки / Н.А. Шиндарев,

М.В. Абрамов // Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика» (РИ’2016). — СПб: СПОИСУ. — Санкт-Петербург, 2016. — 26–28 октября — С. 522– 523.

212. Щербаков, А. Осторожно мошенники рассылают опасные SMS [Электронный ресурс] / А. Щербаков // Новости Mail.ru. — Режим доступа: https://hi-tech.mail.ru/news/sms-virus/?frommail=1.
213. Юзбекова, И. Сбербанк оценил годовой ущерб России от киберпреступлений в $1 млрд [Электронный ресурс] / И. Юзбекова // РБК. — 2015. — Режим доступа: http://www.rbc.ru/technology_and_media/09/12/2015/566837819a7947e4cbc991b6.
214. Юсупов, Р.М. Концептуальный и научно-методологические основы информатизации / Р.М. Юсупов, В.П. Заболотский. — СПб: Наука, 2009. — 544 с.
215. Юсупов, Р.М. Наука и национальная безопасность. / Р.М Юсупов. — СПб: Наука, 2011. — 376 с.
216. Ющук, Е.Л. Конкурентная разведка / Е.Л. Ющук — М.: Вершина, 2006. — 238 с.

СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

Список рисунков

Список таблиц

ПРИЛОЖЕНИЕ А. СВИДЕТЕЛЬСТВА О РЕГИСТРАЦИИ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2014618173

Браузерный классификатор на основе вхождения ключевых слов для базы данных документов, выгруженных посредством сервиса IQBuzz в формате .xls

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный гуманитарный университет имени М.А. Шолохова» (RU)***

Авторы: ***см. на обороте***

Заявка № **2014615962**
Дата поступления **20 июня 2014 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***12 августа 2014 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов

Авторы: ***Абрамов Максим Викторович (RU), Азаров Артур Александрович (RU), Бродовская Елена Викторовна (RU), Фильченков Андрей Александрович (RU)***

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2017610561

«Программа оценки силы социальных связей на основе данных социальной сети «ВКонтакте»»

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования «Московский педагогический государственный университет» (ФГБОУ ВО «МПГУ») (RU)***

Авторы: ***Абрамов Максим Викторович (RU), Азаров Артур Александрович (RU), Фильченков Андрей Александрович (RU)***

Заявка № **2016660930**
Дата поступления **18 октября 2016 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***12 января 2017 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2017616876

VK Data Parser for Social Engineering Attacks Modeling Version 01 (VK Data Parser for SEA Modeling v.01)

Правообладатели: ***Багрецов Георгий Игоревич (RU), Абрамов Максим Викторович (RU), Азаров Артур Александрович (RU), Тулупьев Александр Львович (RU)***

Авторы: ***Багрецов Георгий Игоревич (RU), Абрамов Максим Викторович (RU), Азаров Артур Александрович (RU), Тулупьев Александр Львович (RU)***

Заявка № **2017614091**
Дата поступления **26 апреля 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***19 июня 2017 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2017618730

Training Affiliate Data Parser for Social Engineering Attacks Modeling Version 01 (TADP For SEA Modeling v.01)

Правообладатели: ***Шиндарев Никита Андреевич (RU), Тулупьев Александр Львович (RU), Абрамов Максим Викторович (RU), Азаров Артур Александрович (RU)***

Авторы: ***Шиндарев Никита Андреевич (RU), Тулупьев Александр Львович (RU), Абрамов Максим Викторович (RU), Азаров Артур Александрович (RU)***

Заявка № **2017615693**
Дата поступления **13 июня 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***08 августа 2017 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018612139

Parsing Employees Pages in Websites of Social Network for Social Engineering Attacks Modeling Version 01 (PEP in WSSN v.01)

Правообладатели: ***Шиндарев Никита Андреевич (RU), Абрамов Максим Викторович (RU), Тулупьев Александр Львович (RU)***

Авторы: ***Шиндарев Никита Андреевич (RU), Абрамов Максим Викторович (RU), Тулупьев Александр Львович (RU)***

Заявка № **2017663765**
Дата поступления **25 декабря 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 февраля 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018612149

Employees Social Interactions Graph Analyzer for Social Engineering Attacks Modeling Version 01 (ESIGA For SEA Modeling v.01)

Правообладатели: ***Сулейманов Алексей Александрович (RU), Абрамов Максим Викторович (RU), Тулупьев Александр Львович (RU)***

Авторы: ***Сулейманов Алексей Александрович (RU), Абрамов Максим Викторович (RU), Тулупьев Александр Львович (RU)***

Заявка № **2017663718**
Дата поступления **25 декабря 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 февраля 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018612147

User Data Aggregator for Social Engineering Attacks Modeling Version 01 (SocND Aggregator v.01)

Правообладатели: ***Слезкин Никита Евгеньевич (RU), Абрамов Максим Викторович (RU), Тулупьев Александр Львович (RU)***

Авторы: ***Слезкин Никита Евгеньевич (RU), Абрамов Максим Викторович (RU), Тулупьев Александр Львович (RU)***

Заявка № **2017663715**
Дата поступления **25 декабря 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 февраля 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

ПРИЛОЖЕНИЕ Б. СБОР ДАННЫХ ДЛЯ ОЦЕНКИ ПСИХОЛГИЧЕСКИХ ОСОБЕННОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ С ПОМОЩЬЮ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Для оценки степени выраженности психологических особенностей пользователей на основании текстового контента, публикуемого в социальной сети ВКонтакте, использовались методы машинного обучения. Были опрошено 60 человек от 19 до 21 года разного пола на предмет оценки степени выраженности их психологических особенностей. В исследовании использовались следующие методики.

1. Методика Ш. Шварца для изучения ценностей личности [55].
2. Методика LSI (Life Style Index) [21].
3. 16-факторный личностный опросник Р. Кеттелла [19].

Для каждого респондента был сохранён адрес его персональной страницы в сети «ВКонтакте». Таким образом, в исходных данных каждому адресу (т.е. каждому участнику опроса) соответствовал набор из числовых значений, означающих степень выраженности той или иной психологической характеристики.

С каждой из страниц, указанных в результатах опроса, были собраны текстовые записи (посты) владельца аккаунта, находившиеся в открытом доступе. После собранные данные были сохранены в файл для дальнейшего использования на платформе Microsoft Azure Machine Learning. Каждая строка данного файла — это пост со страницы пользователя и набор значений его психологических характеристик. Объём собранной коллекции составил 600 единиц.

С помощью платформы Microsoft Azure Machine Learning были созданы, настроены и обучены две пробные модели. Первичное исследование решало задачу оценки степени выраженности психологической характеристики «Проекция». Проекция — один из видов психологической защиты, неосознаваемое отвержение собственных эмоционально неприемлемых установок или желаний и приписывание их другим объектам

(людям или животным) [4]. Модели для остальных характеристик строились аналогично.

ПРИЛОЖЕНИЕ В. ФУНКЦИЯ ДЛЯ ВОССТАНОВЛЕНИЯ ГОРОДА ПОЛЬЗОВАТЕЛЯ НА ОСНОВАНИИ ДАННЫХ СОЦИАЛЬНОГО КРУГА ПОЛЬЗОВАТЕЛЯ

```
City[] getCurrentCity(String id)
{
      // текущий город анализируемого пользователя
      City mycity = getMyCity(id);

      // текущие города друзей пользователя
      City[] cities = getFriendsCities(id);

      // распределение городов
      map<String, int> distr = getDistributionByList(cities);

      // если текущий город анализируемого пользователя присутствует, то
добавляем этот город в результирующее распределение с некоторым коэффици-
ентом
      if (myCity != null)
            distr = distr.UpgradeDistribution(myCity);
//возвращаем результат и распределение, либо его часть
}
```

ПРИЛОЖЕНИЕ Г. ФУНКЦИЯ ДЛЯ ВОССТАНОВЛЕНИЯ ВОЗРАСТА ПОЛЬЗОВАТЕЛЯ НА ОСНОВАНИИ ДАННЫХ СОЦИАЛЬНОГО КРУГА ПОЛЬЗОВАТЕЛЯ

```
BDate[] getBDate(String id)
{
      // извлекаем год рождения анализируемого пользователя
      BDate myBDate = getMyBDate(id);

      // года рождения друзей пользователя
      BDate[] bDates = getFriendsBDates(id);
      map<String, int> distr = getDistributionByList(bDates);

      // возраст друзей пользователя у которых совпадают школы
      BDate[] simSchool = getSimilarFriendsSchool(id);
      map<String, int> distr2 = getDistributionByList(simSchool);

      // возраст друзей пользователя у которых совпадают ВУЗы
      BDate[] simUniversity = getSimilarFriendsUniversity(id);
      map<String, int> distr3 = getDistributionByList(simUniversity);

      //возраст из анкеты пользователя с коэффициентом
      distr = distr.UpgradeDistribution(myBDate);
      distr1 = distr1.UpgradeDistribution(myBDate);
      distr2 = distr2.UpgradeDistribution(myBDate);

      //объединяем полученные распределения
      distr = distr.combine(distr1.combine(distr2));
      return distr;
}
```

ПРИЛОЖЕНИЕ Д. НЕКОТОРЫЕ ЭЛЕМЕНТЫ РЕАЛИЗАЦИИ МОДЕЛЕЙ И АЛГОРИТМОВ ДЛЯ АВТОМАТИЗИРОВАННОГО РАСЧЁТА ОЦЕНОК НЕКОТОРЫХ ОСОБЕННОСТЕЙ ЛИЧНОСТИ

Применение паттерна «Одиночка» (Singleton)

```
internal class VkApiHolder {
      private static readonly Lazy<VkApi> vkApiHolder = new Lazy<VkApi>(() =>
      new VkApi());

      private VkApiHolder() { }
      internal static VkApi Api {
            get { return vkApiHolder.Value; }
      }
}
```

VkApiHolder, реализация паттерна «Одиночка»

```
internal class VkApiWrapper
{
      internal static void VkAutorize() {
            new VKAuthorize().ShowDialog();
      }

      internal static List<string> GetPostsFromVk(long id) {
            List<string> data = new List<string>();

            List<Post> posts = new List<Post>();

            try {
                  posts = VkApiHolder.Api.Wall.Get(new WallGetParams() {
                        OwnerId = id,
                        Filter = WallFilter.Owner,
                        Count = 100
                  }).WallPosts.ToList();
            }
            catch (InvalidParameterException) {
                  // Пропускаем неопознаваемые записи
                  for (uint i = 0; i < 100; i++) {
                        Thread.Sleep(400);
                        try {
                              var curPost = VkApiHolder.Api.Wall.Get(new
                              WallGetParams() {
                              OwnerId = id,
                              Filter = WallFilter.Owner,
                              Count = 1,
                              Offset = i
                        }).WallPosts.ToList();
                        if (curPost.Count == 1) {
                              posts.Add(curPost[0]);
                        }
                  }
            catch (InvalidParameterException) { }
      }
}

foreach (Post post in posts) {
      string s = post.Text + " ";
```

```
      if (post.CopyHistory.Count != 0) {
            s += post.CopyHistory.First().Text;
      }
      s = s.Replace(Environment.NewLine, " ")
      .Replace("\n", " ")
      .Replace("\r", " ")
      .Replace("\"", "")
      .Replace(";", " ")
      .Replace(",", " ")
      .Replace("'", "")
      .Trim();
      if (s == string.Empty) continue;
            data.Add(s);
      }
      return data;
      }
}
```

Массив стоп-слов

```
internal static class StopWords {
      internal static string[] stopWordsList = new string[] { "а", "без", "бу-
дет", "бы", "был", "была", "были", "было", "быть", "в", "вам", "вас", "вдруг",
"ведь", "во", "вот", "все", "всех", "всю", "вы", "г", "где", "да", "даже",
"для", "до", "его", "ее", "её", "ей", "ему", "если", "есть", "еще", "ещё",
"ж", "же", "за", "зачем", "и", "из", "или", "им", "их", "к", "как", "какая",
"какой", "которого", "которые", "кто", "куда", "ли", "между", "меня", "мне",
"мой", "моя", "мы", "на", "над", "надо", "нас", "не", "него", "нее", "неё",
"ней", "нет", "ни", "нибудь", "ним", "них", "ничего", "но", "ну", "о", "об",
"он", "она", "они", "от", "перед", "по", "под", "после", "потом", "при",
"про", "раз", "с", "сам", "свое", "своё", "свою", "себе", "себя", "со", "так",
"такой", "там", "тебя", "тем", "то", "того", "том", "тот", "три", "тут", "ты",
"у", "уж", "уже", "хоть", "чего", "чем", "через", "что", "чтоб", "чтобы",
"чуть", "эти", "этого", "этой", "этом", "этот", "эту", "я"};
}
```

ПРИЛОЖЕНИЕ Е. АКТЫ О ВНЕДРЕНИИ

АКТ О ВНЕДРЕНИИ

результатов диссертационного исследования

1. Наименование научного исследования: «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей»

2. Ф.И.О. автора: Абрамов Максим Викторович, аспирант кафедры информатики Санкт-Петербургского государственного университета, младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации РАН.

3. Краткая аннотация: исследование посвящено формированию методики оценки защищённости пользователей информационных систем от социоинженерных атак. Данное исследование является развитием существующего подхода, разработанного Тулупьевым А.Л., Азаровым А.А. и Тулупьевой Т.В. Существенный прогресс достигнут в оценке параметров модели профиля уязвимостей пользователя, за счёт агрегации сведений из социальных сетей и иных источников для автоматизации выявления связей между данными, содержащимися в контенте, публикуемом пользователями и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности, как основы для построения профиля уязвимостей, а также дополнения комплекса «критичные документы — информационная система — пользователь» моделью злоумышленника.

4. Результаты исследования используются в оценке рисков утечки конфиденциальной информации, проводимой отделом информатизации и связи администрации Центрального района Санкт-Петербурга.

5. Форма внедрения: проверка сведений, подаваемых персоналом, о представленности в социальных сетях, автоматизированный поиск аккаунтов в других социальных сетях, оценка психологических характеристик пользователей информационной системы администрации, поиск вероятных траекторий утечки информации для внедрения дополнительных параметров в политику разграничения доступа.

6. Эффект внедрения: автоматизированное выявление и формализация связей между данными, содержащимися в контенте, публикуемом пользователями, и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности.

Первый заместитель главы
администрации Центрального района
города Санкт-Петербурга, к.э.н. П.М. Спивачевский

«05» 03 2018 г.

LLC Meteor
199178, Saint-Petersburg
Line 18 V.O, d.31,
office 4-N
Tel./Fax. +7 (812) 633-34-46
E-mail: meteor.ltd.co@gmail.com

ООО «Метеор»
199178, Санкт-Петербург
Линия 18-ая В.О., дом 31,
пом. 4-Н
Tel./Fax. +7 (812) 633-34-46
E-mail: meteor.ltd.co@gmail.com

Исх.17/03 от 02.03.2018

Акт

внедрения результатов диссертационной работы Абрамова М.В. на соискание учёной степени кандидата технических наук

Я, Генеральный директор ООО «Метеор», настоящим подтверждаю, что результаты диссертационного исследования «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» на соискание учёной степени кандидата технических наук Абрамова М.В., а именно: методика автоматизированного выявления и формализации связей между данными, содержащимися в контенте, публикуемом пользователями в социальных сетях, и результатами, получаемыми с помощью устоявшегося инструментария оценки степени выраженности ряда особенностей его личности, а также комплекс программ, реализующий модели «критичные документы – информационная система – пользователь – злоумышленник» и связи между ними для оценки защищённости пользователей от социоинженерных атак использовались в работе hr-отдела для модернизации кадровой политики и принятия решений о приёме на работу.

Генеральный директор ООО «Метеор» Задесенец Н.С.

Общество с ограниченной ответственностью «Метеор»
199178, г. Санкт-Петербург, Линия 18-ая В.О., дом 31, помещение 4-Н
ИНН 7801605018/ КПП 780101001

Тел/Факс: +7 (812) 633-34-4
E-mail: meteor.ltd.co@gmail.com

ПРОМЫШЛЕННО – КОММЕРЧЕСКАЯ ГРУППА РАДУГА

ЗАВОД им. КОЗИЦКОГО

ЗАО «Завод им. Козицкого»
Россия, 199178, Санкт-Петербург, В.О., 5-линия, 70
Тел.: (812) 323 1818, тел./факс: (812) 323 5650
www.raduga.spb.ru E-mail:zavod@raduga.spb.ru
ОКПО 46956258 ОГРН 1027800507932
ИНН 7801098875 КПП 780101001

Акт
об использовании результатов диссертационного исследования
Абрамова Максима Викторовича
«Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей»

Настоящий Акт составлен в том, что результаты диссертационной работы, а именно:

- модель оценки вероятности успеха многоходовой социоинженерной атаки и подход к оценке защищённости пользователя информационной системы от социоинженерных атак;
- методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте;
- методы восстановления мета-профиля пользователя информационной системы, построенные на основе агрегации доступных сведений;

используются в работе отдела кадров ЗАО «Завод им. Козицкого», а также службой безопасности для анализа защищённости пользователей информационной системы предприятия. Использование результатов диссертационного исследования способствует своевременному принятию кадровых решений, организации профессиональных тренингов персонала, направленных на повышение уровня знаний и навыков в области обеспечения информационной безопасности, а также оценке степени выраженности уязвимостей пользователей через их аккаунты в социальной сети ВКонтакте.

С уважением,

Генеральный директор
ЗАО «Завод им. Козицкого» Л.В. Меличев

ПРИЛОЖЕНИЕ Ж. ПУБЛИКАЦИИ СОИСКАТЕЛЯ 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 – пользо-

ватель – 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. —10 т. — № 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.
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, Abramov M.V., Azarov A.A., Bordovskaya N.V. // 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., Azarov A.A. Identifying user's of social networks psychological features on the basis of their musical preferences //Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on. – IEEE, 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.

Научные тезисы и доклады, опубликованные в других изданиях

16. Тулупьев, А.Л. Защита конфиденциальных данных на интернет-портале редакции электронного научного журнала / А.Л. Тулупьев, М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева // VIII Санкт-Петербургская

межрегиональная конференция «Информационная безопасность регионов России» (ИБРР’2013). — СПб.: СПОИСУ — Санкт-Петербург, 2013. — 23–25 октября — С. 228–229.

17. Азаров, А.А. Представление комплекса «информационная система—критичные документы—персонал—злоумышленник» с помощью реляционно-алгебраического подхода / А.А. Азаров, А.А. Фильченков, М.В. Абрамов, А.Л. Тулупьев // Труды Международной конференции по мягким вычислениям и измерениям (SCM’2014) в 2 т. — Санкт-Петербург, 2014. — 1 т. — С. 66–69.
18. Абрамов, М.В. Применение моделей распространения информации в социальных сетях к задачам анализа защищённости пользователей информационных систем от социо-инженерных атак / М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев, А.А. Фильченков // Нечёткие системы и мягкие вычисления (НСМВ’2014): труды Шестой всероссийской научно-практической конференции в 2 т. — СПб.: Политехника-сервис. — Санкт-Петербург, 2014. — 27-29 июня — 2 т. — С. 55–58.
19. Азаров, А.А. Анализ распространения вредоносного контента среди пользователей социальных медиа / А.А. Азаров, А.А. Фильченков, М.В. Абрамов // Материалы всероссийской научной конференции по проблемам информатики «СПИСОК-2014» — СПб.: ВВМ — Санкт-Петербург, 2014. — С. 540–546.
20. Абрамов, М.В. Модели распространения информации в социальных медиа / М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев, А.А. Фильченков // Материалы Третьей Международной научно-практической конференции «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC’14). — Москва, 2014. — С. 112–115.
21. Абрамов, М.В. Концепция анализа распространения контента в социальных медиа на основании методов анализа защищенности пользователей информационных систем от социо-инженерных атак / М.В.

Абрамов, А.А. Азаров // Материалы XIV Санкт-Петербургской международной конференции Региональная Информатика (РИ’2014). — Санкт-Петербург, 2014. — С. 543.

22. Абрамов, М.В. Модели распространения информационных сообщений в социальных сетях / М.В. Абрамов, А.Л. Тулупьев, А.А. Азаров, А.А. Фильченков // Научная сессия НИЯУ МИФИ-2015 «Интеллектуальные системы и технологии» в 3 т. Аннотации докладов. — М.: НИЯУ МИФИ. — Москва, 2015. — 3 т. — С. 137.
23. Азаров, А.А. Применение алгоритма обхода в ширину графа межличностных связей для анализа защищенности пользователей информационных систем / А.А. Азаров, М.В. Абрамов, Т.В Тулупьева // Интегрированные модели и мягкие вычисления в искусственном интеллекте. Сборник научных трудов VIII-ой Международной научно-технической конференции в 2 т. – М.: Физматлит. — Коломна, 2015. — 18–20 мая — 2 т. — С. 774–779.
24. Абрамов, М.В. Распространение социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей / М.В. Абрамов, А.А. Азаров, А.А. Фильченков // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2015) в 2 т. — Санкт-Петербург, 2015. — 1т. — С. 329–331.
25. Абрамов, М.В. Комплекс «критические документы — информационная система — персонал — злоумышленник» / М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева, А.Л. Тулупьев // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР’2015) — СПб.: СПОИСУ. — Санкт-Петербург, 2015. — 28–30 октября — С. 326–327.
26. Абрамов, М.В. Комплекс программ для анализа достижимости критических документов и защищённости пользователей информационных

систем / М.В. Абрамов // Материалы IX Санкт-Петербургская межрегиональной конференции «Информационная безопасность регионов России» (ИБРР’2015). — СПб: СПОИСУ. — Санкт-Петербург, 2015. — 28–30 октября — С. 326.

27. Азаров, А.А. Прототип комплекса программ для анализа защищённости пользователей информационных систем, построенный на основе алгоритмов обхода графов социальных связей пользователей / А.А. Азаров, М.В. Абрамов, А.Л. Тулупьев, Т.В. Тулупьева // Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. — 2015. — С. 554–557.
28. Абрамов, М.В. Применение социальных сетей для анализа защищённости пользователей компании от социоинженерных атак / М.В. Абрамов // Материалы Четвёртой Международной научно-практической конференции «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC’15) — Москва, 2015. — С. 294–297.
29. Абрамов, М.В. Моделирование социоинженерных атак с использованием байесовских сетей доверия / М.В. Абрамов, А.А. Азаров // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2017) в 2 т. — Санкт-Петербург, 2016. — 1 т. — С. 71– 74.
30. Абрамов, М.В. Реляционная модель расчёта вероятностной оценки уровня защищённости пользователя от социоинженерных атак / М.В. Абрамов // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием (КИИ’2016) — Смоленск: Универсум, 2016. — 3–7 октября — 1 т. — С. 203–211.
31. Абрамов, М.В. Подход к оценке защищённости пользователей информационных систем от социоинженерных атак / М.В. Абрамов // Юбилейная XV Санкт-Петербургская международная конференция

«Региональная информатика» (РИ’2016). — СПб: СПОИСУ. — Санкт-Петербург, 2016. — 26-28 октября. — С. 514.

32. Шиндарев, Н.А. Построение вероятностной графической модели для оценки успешности социоинженерной атаки / Н.А. Шиндарев, М.В. Абрамов // Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика» (РИ’2016). — СПб: СПОИСУ. — Санкт-Петербург, 2016. — 26-28 октября — С. 522–523.
33. Абдурахманова, К.Ф Программная реализация имитации социоинженерных атак с помощью марковских полей / К.Ф. Абдурахманова, М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев, Т.В. Тулупьева // Материалы 6-й всероссийской научной конференции по проблемам информатики «СПИСОК-2016». — СПб.: ВВМ. — Санкт-Петербург, 2016. — 26–29 апреля — С. 427– 435.
34. Абрамов, М.В. Подход к оценке вероятности успешности социоинженерной атаки / М.В. Абрамов // Материалы 6-й всероссийской научной конференции по проблемам информатики «СПИСОК-2016» — СПб.: ВВМ. — Санкт-Петербург, 2016. — 26–29 апреля — С. 436–442.
35. Абрамов, М.В. Выявление психологических особенностей пользователей социальных сетей на основании музыкальных предпочтений / М.В. Абрамов, А.А. Азаров // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2017) в 2 т. — Санкт-Петербург, 2017. — 1 т. — С. 130–133.
36. Багрецов, Г.И. Подходы к разработке моделей для анализа текстовой информации в профилях социальной сети в целях построения профиля уязвимостей пользователя / Г.И. Багрецов, Н.А. Шиндарев, М.В. Абрамов, Т.В. Тулупьева // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM’2017) в 2 т. — Санкт-Петербург, 2017. — 1 т. — С. 134–137.

37. Абрамов, М.В. Оценка вероятности успеха социоинженерного атакующего воздействия / М.В. Абрамов // Сборник научных трудов IV Международной летней школы-семинара по искусственному интеллекту для студентов, аспирантов, молодых ученых и специалистов «Интеллектуальные системы и технологии: современное состояние и перспективы» (ISYT'2017) — СПб.: Политехника-сервис. — Санкт-Петербург, 2017. — 30.06–3.07 — С. 9–14.
38. Багрецов, Г.И. Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети / Г.И. Багрецов, Н.А. Шиндарев, М.В. Абрамов, Т.В. Тулупьева // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВИТ–2017) в 2 т. — СПб.: Политехника-сервис. — Санкт-Петербург, 2017. — 3–7 июля — 1 т. — С. 9–16.
39. Бушмелёв, Ф.В. Обзор программного инструментария для визуализации сетей в микромире корпоративных офисов / Ф.В. Бушмелёв, М.В. Абрамов // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» (НСМВИТ–2017) в 2 т. — СПб.: Политехника-сервис. — Санкт-Петербург, 2017. — 2 т. — С. 34–42.
40. Сулейманов, А.А. Подход к построению и анализу социального графа сотрудников некоторой компании / А.А. Сулейманов, М.В. Абрамов // Сборник научных трудов Первой Всероссийской научно-практической конференции «Нечёткие системы и мягкие вычисления. Промышленные применения. — Ульяновск, УлГТУ, 2017. — 14–15 ноября — С. 389–393.
41. Слёзкин, Н.Е. Подход к восстановлению мета-профиля пользователя информационной системы на основании данных из социальных сетей / Н.Е. Слёзкин, М.В. Абрамов, Т.В. Тулупьева // Сборник научных тру-

дов Первой Всероссийской научно-практической конференции «Нечёткие системы и мягкие вычисления. Промышленные применения». — Ульяновск, УлГТУ, 2017. — 14–15 ноября — С. 394–399.

42. Абрамов, М.В. Подход к построению системы упреждающей диагностики уязвимостей персонала к социоинженерным атакам / М.В. Абрамов // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР'2017). — СПб: СПОИСУ — Санкт-Петербург, 2017. — 1–3 ноября — С. 409–410.
43. Бушмелёв Ф.В. Подход к построению профиля компетенций злоумышленника в задаче анализа защищённости информационной системы от социоинженерных атак / Ф.В. Бушмелёв, М.В. Абрамов // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР'2017) — СПб: СПОИСУ. — Санкт-Петербург, 2017. — 1–3 ноября — С. 413–414.
44. Шиндарев, Н.А. Анализ страниц пользователей социальной сети «ВКонтакте» с целью выявления сотрудников заданной компании / Н.А. Шиндарев, М.В. Абрамов, А.Л. Тулупьев // Материалы 7-й всероссийской научной конференции по проблемам информатики «СПИСОК-2017». — СПб.: ВВМ — Санкт-Петербург, 2017. — 25–25 апреля. — С. 420–425.
45. Абрамов, М.В. Оценка защищённости пользователя информационной системы от социоинженерных атак на основе комплекса «критичные документы – информационная система – персонал – злоумышленник» / М.В. Абрамов // Материалы 7-й всероссийской научной конференции по проблемам информатики «СПИСОК-2017». — СПб.: ВВМ — Санкт-Петербург, 2017. — 25–25 апреля. — С. 388–394.
46. Сулейманов, А.А. Автоматизация построения социального графа сотрудников компании на основе публикуемого ими контента в социаль-

ных сетях / А.А. Сулейманов, М.В. Абрамов // Школа-семинар по искусственному интеллекту: сборник научных трудов. — Тверь: ТвГТУ, 2018. — С. 32–40.

47. Шиндарев, Н.А. Рекурсивный алгоритм выявления пользовательских страниц сотрудников на основе анализа социальных сетей / Н.А. Шиндарев, М.В. Абрамов // Школа-семинар по искусственному интеллекту: сборник научных трудов. — Тверь: ТвГТУ, 2018. — С. 23–31.
48. Абрамов, М.В. Защита пользователей информационных систем от социоинженерных атак. / М.В. Абрамов, Т.В. Тулупьева, А.Л. Тулупьев // Всероссийский форум «Система распределенных ситуационных центров как основа цифровой трансформации государственного управления. — 2017.

Зарегистрированные программы для ЭВМ

49. Абрамов, М.В. Браузерный классификатор на основе вхождения ключевых слов для базы данных документов, выгруженных посредством сервиса IQBuzz в формате .xls / М.В. Абрамов, А.А. Азаров, Е.В. Бродовская, А.А. Фильченков — Свидетельство о государственной регистрации программы для ЭВМ №2014618173 от 12.08.2014. Роспатент. — 2014.
50. Абрамов, М.В. Программа оценки силы социальных связей на основе данных социальной сети «ВКонтакте» xls / М.В. Абрамов, А.А. Азаров, А.А. Фильченков — Свидетельство о государственной регистрации программы для ЭВМ №2017610561 от 12.01.2017. Роспатент. — 2017.
51. Багрецов, Г.И. VK Data Parser for Social Engineering Attacks Modeling Version 01 (VK Data Parser for SEA Modeling v.01) / Г.И. Багрецов, М.В. Абрамов, А.А. Азаров, А.Л. Тулупьев — Свидетельство о государственной регистрации программы для ЭВМ №2017616876 от 19.06.2017. Роспатент. — 2017.

52. Шиндарев, Н.А. Training Affiliate Data Parser for Social Engineering Attacks Modeling Version 01 (TADP For SEA Modeling v.01) / Н.А. Шиндарев, А.Л. Тулупьев, М.В. Абрамов, А.А. Азаров // Свидетельство о государственной регистрации программы для ЭВМ №2017618730 от 08.08.2017. Роспатент. — 2017.
53. Слезкин, Н.Е. User Data Aggregator for Social Engineering Attacks Modeling Version 01 (SocND Aggregator v.01). / Н.Е. Слезкин, М.В. Абрамов, А.Л. Тулупьев // Свидетельство о государственной регистрации программы для ЭВМ №2018612147 от 25.12.2017. Роспатент. — 2017.
54. Сулейманов, А.А. Employees Social Interactions Graph Analyzer for Social Engineering Attacks Modeling Version 01 (ESIGA For SEA Modeling v.01) / А.А. Сулейманов, М.В. Абрамов, А.Л. Тулупьев // Свидетельство о государственной регистрации программы для ЭВМ №2018612149 от 25.12.2017. Роспатент. — 2017.
55. Шиндарев, Н.А. Parsing Employees Pages in Websites of Social Network for Social Engineering Attacks Modeling Version 01 (PEP in WSSN v.01) / Н.А. Шиндарев, М.В. Абрамов, А.Л. Тулупьев // Свидетельство о государственной регистрации программы для ЭВМ №2018612139 от 25.12.2017. Роспатент. — 2017.

ПРИЛОЖЕНИЕ И. ВРЕМЯ РАБОТЫ ПРОГРАММНЫХ МОДУЛЕЙ

На листинге представлены фрагменты одного из логов работы модуля для автоматизированной идентификации аккаунтов сотрудников компании в социальной сети ВКонтакте. Полный лог занимает более 4 тысяч строк, поэтому его части пропущены, на их месте строки с многоточием. Данный лог был составлен в ходе обработки 89 аккаунтов. Программному модулю потребовалось для этого около 40 минут. Ещё 9 пусков для тех же данных показали похожие результаты, время работы менялось от 36 минут 25 секунд до 43 минут 18 секунд, стандартное отклонение составило 2 минуты 21 секунду, среднее время работы программы — 39 минут 35 секунды, а медиана — 39 минут 46 секунд.

```
2018-02-16 19:57:02,325  INFO  logger configured successfully
2018-02-16 19:57:04,473  DEBUG connection succeed, access token was sent
.....................................
2018-02-16 19:57:15,973  INFO  .....................................
2018-02-16 19:57:15,976  INFO  Finished collecting training dataset.
2018-02-16 19:57:15,979  INFO  Found non-employees: 81
2018-02-16 19:57:15,981  INFO  Found employees:     8
2018-02-16 19:57:15,984  INFO  ......................
.....................................
2018-02-16 20:37:55,471  DEBUG status grey for id 23992
2018-02-16 20:37:55,473  DEBUG status grey for id 24612
```

В следующем листинге приведён фрагмент кода, в котором реализован вывод времени после анализа каждого аккаунта на предмет степени выраженности некоторых особенностей личности его владельца. Время работы разработанного программного модуля зависит от количества постов на странице пользователя. Для 12 разных пользователей с разным числом постов на странице время работы программы варьировалось от 0.3 секунд до 61.67 секунд, стандартное отклонение составило 27.02 секунд. а среднее и медиана составили 0.61 и 0.68 секунды соответственно. При 10 разных запусках программы для 12 аккаунтов время выполнения показало меньший разброс от 175.32 секунд до 198.57, стандартное отклонение — 8.51 секунды, среднее — 189.45 секунд, а медиана — 192.29 секунды.

```
private void button10_Click(object sender, EventArgs e)
{
    long[] ids = new long[] {
        90342575,
        2724404,
        6408999,
        6649825,
        930855,
        7560093,
        34838386,
        145586920,
        35665250,
        203437876,
        57276942,
        93530797,
    };

    textBox6.Clear();

    foreach (long id in ids)
    {
        double time = 0;
        for (int i = 0; i < 5; i++)
        {
            var start = DateTime.Now;
            var psychProfile = PsychProfile.GetUserPsychProfile(SocialNetwork.VK, id);
            var currentTime = DateTime.Now - start;
            time += currentTime.TotalSeconds;
        }
        time = time / 5;
        textBox6.Text += id + "\t\t" + time + Environment.NewLine;
    }
}
```

На данном листинге представлена часть кода, которая включает операторы вывода времени начала и окончания работы программного модуля для восстановления фрагмента мета-профиля пользователя. Было сделано 10 запусков программы для 62 аккаунтов. Для каждого аккаунта определялись родной город, город проживания и год рождения. В разное время суток разработанному программному модулю потребовалось разное время для анализа. В вечернее время потребовалось наибольшее количество времени — 75 минут и 3 секунд, наименьшее время было затрачено в 4 часа ночи — 57 минут и 30 секунд, стандартное отклонение составило 6 минут и 31 секунда. Среднее время работы программного модуля составило 65 минут и 35 секунд, медиана — 66 минут и 1 секунда.

```
if (command.equals("all"))
        {
            long startTime = System.currentTimeMillis();
            for (int i = 0; i < ids.length; i++) {
                vkapicity.FindCityDeep2(ids[i], "city");
                vkapicity.FindCityDeep2(ids[i], "home_town");
                vkapibdate.FindBDateDeep2(ids[i]);
            }
            long finishTime = System.currentTimeMillis();
            long timeSpent  = finishTime - startTime;
```

```
            System.out.println("start: " + startTime + ", finish: " + finishTime + ".
Delta = " + timeSpent + "ms = " + (double)timeSpent/1000 + "sec = " + (dou-
ble)timeSpent/60000 + "min");
            return;
        }
```

На заключительном листинге приложения приведён фрагмент кода разработанного программного модуля для построения оценок вероятности успеха многоходовых социоинженерных атак, в котором содержится вывод времени начала, завершения и длительность работы программы. Для 10 запусков при построении оценок для 100 пользователей были получены следующие результаты. Минимальное время работы — 226 минут 11 секунд, максимальное время работы — 284 минуты 29 секунд, стандартное отклонение — 20 минут 46 секунд, среднее — 249 минут 17 секунд, медиана — 248 минут 34 секунд.

```
      if (command.equals("analyze")) {
       long startTime = System.currentTimeMillis();

                  SocialGraph graph = GraphLoader.getGraph(csvFile);

                  Visualizer.visualize(graph);
                  System.out.println("Please, type to proceed");
                  next = in.next();

                  graph = GraphExtension.expandGraph(graph, "vk.com");

                  Visualizer.visualize(graph);
                  System.out.println("Please, type to proceed");
                  next = in.next();

                  graph = GraphDecorator.decorateGraph(graph, "vk.com");

                  Visualizer.visualize(graph);
                  System.out.println("Please, type to proceed");
                  next = in.next();

                  graph = Compressor.compress(graph, "threshold");

                  Visualizer.visualize(graph);
                  System.out.println("Please, type to proceed");
                  next = in.next();

                  graph = Finder.findDangerousZones(graph);

                  Visualizer.visualize(graph);

       long finishTime = System.currentTimeMillis();
       long timeSpent = finishTime - startTime;
       System.out.println("start: " + startTime + ", finish: " + finishTime + ". Delta =
" + timeSpent + "ms = " + (double)timeSpent/1000 + "sec = " + (double)timeSpent/60000 +
"min");
       return;
}
```

ПРИЛОЖЕНИЕ К. РАСШИРЕННОЕ ОГЛАВЛЕНИЕ