ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
САНКТ-ПЕТЕРБУРГСКИЙ ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(СПИИРАН)

УДК 004.8
ГРНТИ 81.96.00, 81.93.29, 28.23.35
№ госрегистрации АААА-А18-118101590069-7
Инв. № _____

УТВЕРЖДАЮ
Директор СПИИРАН
д.т.н., профессор РАН

_____ А.Л. Ронжин

___.03.2020

ОТЧЕТ

О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

СОЦИОИНЖЕНЕРНЫЕ АТАКИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ: ПОДХОДЫ, МЕТОДЫ И АЛГОРИТМЫ ВЫЯВЛЕНИЯ НАИБОЛЕЕ ВЕРОЯТНЫХ ТРАЕКТОРИЙ

Грант РФФИ № 18-37-00323 мол_а

(заключительный)

Руководитель темы,
ст. науч. сотр., к.т.н. _____ М.В. Абрамов
___.03.2020

Ответственный исполнитель,
мл. науч. сотр. _____ А.О. Хлобыстова
___.03.2020

Санкт-Петербург 2020 г.

СПИСОК ИСПОЛНИТЕЛЕЙ

Ст. науч. сотр., к.т.н. _____ ___.03.2020 Абрамов Максим Викторович (отчет)

Мл. науч. сотр. _____ ___.03.2020 Хлобыстова Анастасия Олеговна (отчет)

Мл. науч. сотр. _____ ___.03.2020 Корепанова Анастасия Андреевна (отчет)

Мл. науч. сотр. _____ ___.03.2020 Максимов Анатолий Григорьевич (отчет)

Мл. науч. сотр. _____ ___.03.2020 Харитонов Никита Алексеевич (отчет)

Мл. науч. сотр. _____ ___.03.2020 Завалишин Арсений Дмитриевич (отчет)

Мл. науч. сотр. _____ ___.03.2020 Олисеенко Валерий Дмитриевич (отчет)

Стажер-исследователь_____ ___.03.2020 Багрецов Георгий Игоревич (отчет)

Стажер-исследователь_____ ___.03.2020 Бушмелёв Фёдор Витальевич (отчет)

Стажер-исследователь_____ ___.03.2020 Слезкин Никита Евгеньевич (отчет)

Стажер-исследователь_____ ___.03.2020 Сулейманов Алексей Александрович (отчет)

РЕФЕРАТ

Отчет 122 с., 19 рис., 8 табл., 156 источников, 13 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ЗАЩИТА ИНФОРМАЦИИ, СОЦИОИНЖЕНЕРНЫЕ АТАКИ, ЗАЩИТА ПОЛЬЗОВАТЕЛЯ, ПРОФИЛЬ КОМПЕТЕНЦИЙ ЗЛОУМЫШЛЕННИКА, ПРОФИЛЬ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ, ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ, СОЦИОТЕХНИЧЕСКИЕ СИСТЕМЫ

Объектом исследования являются социальные сети и извлекаемые из них данные, а также данные, получаемые в результате прохождения пользователями психологических тестов.

Проект поддержан грантом РФФИ № 18-37-00323, отчет представлен за весь период реализации.

Основной **целью** проекта является разработка моделей, методов и алгоритмов выявления траекторий наиболее вероятного распространения социоинженерной атаки.

Методология проекта основывается на агрегировании информации из различных социальных сетей, построении социального графа сотрудников компании, его визуализации и дальнейшем использовании при нахождении вероятностных оценок распространения социоинженерного атакующего воздействия, выявления наиболее критичных траекторий распространения социоинженерных атак.

В ходе работы была предложена концепция программного комплекса для оценки защищённости пользователей информационных систем от социоинженерных атак, приведена его архитектура. Предложены подходы для агрегации данных о пользователе из социальных сетей и восстановления фрагмента метапрофиля. Разработан метод квантификации типов взаимоотношений пользователей. Представлен подход к построению, анализу и визуализации социального графа сотрудников. Представлен алгоритм для вывода коэффициентов дуг социального графа, используемых при расчёте вероятности успеха опосредованной социоинженерной атаки. Предложены алгоритмы вычисления вероятности поражения критичных документов информационной системы путем анализа социального графа сотрудников компании. Предложен подход к увеличению оперативности оценки защищённости критичных документов при многоходовых социоинженерных атаках. Предложен подход к идентификации траекторий, оценка вероятности успеха прохождения атаки по которым будет наиболее высокой. Предложен подход к решению задачи выявления наиболее критичной траектории реализации многоходовой социоинженерной атаки с точки зрения наибольшего ущерба для организации. Представлена гибридная модель нахождения наиболее критичных траекторий распространения многоходовых социоинженерных атак, прохождение злоумышленника по которым имеет в совокупности наивысшую степень вероятности и принесёт наибольший убыток компании. Разработан подход к бэктрекингу по инцидентам, основывающийся на оценках вероятности успеха одноходовых и многоходовых социоинженерных атак, позволяющий осуществлять первичное расследование инцидентов, связанных с реализацией социоинженерных атак. Разработаны программные модули, реализующие предложенные алгоритмы. Опубликовано 37 работ (из них 1 монография, 9 SCOPUS, 7 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», 12 РИНЦ). Получено 11 свидетельств о регистрации ПрЭВМ (Роспатент).

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящий отчет о НИР (итоговый) содержит сведения о результатах работы над проектом № 18-37-00323, поддержанным грантом РФФИ. Результаты первого года выполнения проекта отражены в отчете, зарегистрированном в ЦИТИС №АААА-Б19-219031590043-5 от 15.03.2019.

Актуальность. В наши дни прослеживается тенденция роста числа и повышения качества киберпреступлений, совершаемых с применением методов социальной инженерии [1]. Данный факт находит своё подтверждение, как в сообщениях о крупных инцидентах, связанных с нарушением безопасности, компрометацией личных данных и применением мошеннических схем [2, 3], так и в отчётах крупных мировых компаний об актуальных угрозах [1, 4]. К примеру, по данным федеральной торговой комиссии США [5] одним из популярных видов атак являются романтические аферы, только в США в 2018 году общий ущерб от них составил порядка 143, 2 600. Всё вышеперечисленное определяет актуальность и необходимость проблемы повышения уровня защищённости пользователей информационных систем от социоинженерных атак. Важной составляющей этой проблемы является задача автоматизации анализа защищённости пользователей. Для решения этой задачи необходимо разработать концепцию программного коплекса для оценки защищённости пользователей информационных систем от социоинженерных атак, сконструировать архитектуру этого программного комплекса, разработать алгоритмы для модулей, отвечающих за моделирование распространения социоинженерной атаки на социальном графе сотрудников, агрегации и анализа данных о пользователей информационной системы из социальных сетей.

Коллективом исследователей был разработан комплекс «критичные документы — информационная система — пользователь — злоумышленник» [6], который является дополнением существовавшего до этого комплекса «критичные документы — информационная система – пользователь». За счёт агрегирования сведений о более широком

круге факторов, влияющих на оценку вероятности успеха социоинженерного атакующего воздействия злоумышленника, и развития моделей комплекса «информационная система — персонал — критичные документы», удалось получить более точные оценки уязвимости системы.

Коллективом исследователей была предложена формальная модель злоумышленника и входящая в неё модель профиля компетенций злоумышленника, на основании которых построена многофакторная оценка вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя. Были разработаны и представлены модель пользователя информационной системы, включающая в себя модель профиля уязвимостей пользователя и модель злоумышленника, включающая в себя модель профиля компетенций злоумышленника. Предложен подход к формализации профиля компетенций злоумышленника и расчёту вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя с использованием определённого типа атаки и уязвимости.

Подход к оценке защищённости пользователей при многоходовых атаках, а также к расчёту оценок вероятности распространения атаки от пользователя к пользователю был представлен в [7]. Отметим, что в [7] оценка вероятности успеха многоходовой социоинженерной атаки рассчитывается в предположении, что оценки вероятности распространения атаки от одного пользователя к другому и обратно равны. Однако оценка вероятности распространения атаки от пользователя к пользователю в прямом и обратном направлении может быть разной, соответственно необходимо рассматривать ориентированный социальный граф. Также в [7] не рассматриваются вопросы поиска наиболее критичных траекторий распространения атаки.

Основной целью проекта является разработка моделей, методов и алгоритмов выявления траекторий наиболее вероятного распространения социоинженерной атаки. Цель достигается за счёт формализации моделей комплекса «критичные документы — информационная система — персонал — злоумышленник» и последующем построении модели траектории распространения социоинженерной атаки злоумышленника на пользователя информационной системы. Успех распространения социоинженерной атаки через пользователей информационной системы зависит от характера взаимоотношений между

сотрудниками. Вероятность прохождения атаки между разными сотрудниками разная. Необходимо разработать подход к оценке вероятности распространения социоинженерной атаки между сотрудниками компании в зависимости от характера их взаимоотношений. Также необходимо разработать методику выявления наиболее вероятных траекторий распространения социоинженерных атак.

Для достижения поставленной цели в рамках настоящего проекта были поставлены следующие задачи.

- Разработка реляционной модели взаимосвязей между аккаунтами одного сотрудника в разных социальных сетях.
- Разработка методики восстановления данных мета-профиля, на основании контента из аккаунтов разных социальных сетей.
- Разработка классификации характеров взаимоотношений между сотрудниками компании, основанная на оценке вероятности успеха прохождения социоинженерного атакующего воздействия между ними.
- Построение и визуализация социального графа пользователей информационной системы.
- Разработка методики выявления наиболее вероятных траекторий распространения социоинженерной атаки злоумышленника на пользователя.
- Алгоритмизация и визуализация разработанной методики.
- Разработка архитектуры и подходов к синтезу вероятностных графических моделей, на основе которых можно реализовать бэктрекинг по инцидентам.
- Разработка лабораторного прототипа программного комплекса, который на основании агрегации данных из различных социальных сетей строит социальный граф сотрудников компании и визуализацию наиболее вероятных траекторий распространения социоинженерной атаки злоумышленника, а также поддерживает элементы бэктрекинга по инцидентам.

В ходе исследования было опубликовано 37 работ (из них 9 SCOPUS, 7 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», 12 РИНЦ). Получено 11 свидетельств о регистрации ПрЭВМ (Роспатент).

Отчет составлен по результатам выполнения НИР, поддержанной грантом РФФИ № 18-37-00323 (Приложение А).

1 Психологические особенности, психические состояния пользователя и профиль его уязвимостей

В данном исследовании рассматриваются основы социальной манипуляции, как способа воздействия на пользователей информационной системы, к которой злоумышленник пытается получить доступ для нарушения информационной безопасности компании. Приведены примеры уязвимостей пользователя к социоинженерным атакам. Обозначена взаимосвязь между психологическими особенностями пользователя и его уязвимостями, а также неоходимость учета психического состояния при оценке последствий атакующего действия злоумышленника (Приложение Г). Полученные результаты составляют основу для математического моделирования профиля уязвимостей пользователя, построения иерархии моделей данного профиля. На их основе можно оценить вероятность успешной реализации атакующего воздействия злоумышленника на пользователя.

2 Автоматизация анализа социальных сетей

Представлена концепция программного комплекса автоматизированной системы анализа защищённости пользователей компьютерных сетей от социоинженерных атак. Приведена архитектура прототипа программного комплекса, изложены подходы к построению алгоритмов для модулей, отвечающих за моделирование распространения социоинженерной атаки на социальном графе сотрудников и восстановление метапрофиля пользователя на основании контента, публикуемого в социальных сетях. Представлен подход к построению и анализу социального графа сотрудников, дана критическая оценка разработанных ранее методов. Представлен алгоритм для вывода коэффициентов дуг социального графа, используемых при расчёте вероятности успеха опосредованной социоинженерной атаки (Приложение Д). Описанная концепция программного комплекса даёт основу для автоматизированного сбора и анализа данных из социальных сетей, влияющих на успех социоинженерной атаки, и позволяет производить более точные оценки защищённости пользователей информационной системы.

3 Агрегирование данных из социальных сетей для восстановления фрагмента мета-профиля пользователя

Исследование посвящено разработке подхода к агрегированию данных из социальных сетей для восстановления фрагмента мета-профиля пользователя. Приводится формализация задачи сопоставления аккаунтов пользователя в разных социальных сетях. Представлены алгоритмы для восстановления фрагмента мета-профиля пользователя, формализована задача сопоставления аккаунтов пользователя в разных социальных сетях. Приведённые алгоритмы были реализованы в программном модуле (Приложение Е). Данные алгоритмы и реализация делают существенный вклад в построение профиля уязвимостей пользователя, который служит основой для анализа оценки защищённости пользователей информационных систем от социоинженерных атак.

4 Идентификация аккаунтов пользователя в двух социальных сетях

Предлагается подход к решению задачи сопоставления профилей пользователей разных социальных сетей и идентифицикации тех из них, которые принадлежат одному человеку. Предложен соответствующий метод, основанный на сопоставлении социального окружения и значений атрибутов профиля аккаунтов в двух разных социальных сетях (Приложение Ж). Проведено сравнение результатов применения различных моделей машинного обучения к решению данной задачи. Новизна подхода заключается в предложенном новом комбинировании различных методов и приложении к новым социальным сетям. Практическая значимость исследования заключается в автоматизации процесса определения принадлежности профилей в различных социальных сетях одному пользователю. Данные результаты могут быть применены в задаче построения мета-профиля пользователя информационной системы для последующего построения профиля его уязвимостей.

5 Квантификация типов отношений пользователей

Предлагается подход к квантификации лингвистических значений переменной и рассмотрение его применения на примере типов взаимоотношений пользователей, пред-

ставленных в популярной в России социальной сети «ВКонтакте» (Приложение З). Используются результаты социологического опроса, по которым находятся порядковые частотности, а затем применяется аппарат теории вероятностей. Настоящее исследование полезно при изучении влияния типов взаимоотношений пользователей на выполнение какой-либо просьбы, а также находит своё применение при построении социального графа сотрудников организации и опосредовано при получении оценок успеха распространения многоходовых социоинженерных атак.

6 Построение вероятностных оценок поражения критичного документа

Освещается подход к анализу защищенности критичных документов в информационной системе компании при многоходовых социоинженерных атаках. Задача решается с использованием моделей комплекса «критичные документы — информационная система — пользователи — злоумышленник». Рассматриваются подходы к вычислению вероятности поражения критичных документов информационной системы. Предложены алгоритмы вычисления данных вероятностей путем анализа социального графа сотрудников компании (Приложение И). Предложенный в исследовании подход оптимизирует время анализа защищённости информационной системы при многоходовых социоинженерных атаках. Что в свою очередь даёт возможность своевременно производить диагностику системы на предмет выявления наиболее уязвимых мест при социоинженерном атакующем воздействии злоумышленника.

7 Выявление наиболее вероятной траектории распространения многоходовой социоинженерной атаки

Рассматриваются вопросы выявления наиболее критичных траекторий распространения многоходовых социоинженерных атак в социальном графе сотрудников компании. Предложен подход к идентификации наиболее критичных траекторий, оценка вероятности успеха прохождения атаки по которым будет наиболее высокой. В простейшем случае задача сводится к нахождению в графе пути, в котором произведение весов всех рёбер, входящих в данный путь, максимально. Представлен подход к решению задачи сокращения ресурсозатратности алгоритма при поиске наиболее критичной траектории

на полном графе с большим количеством вершин. Произведена адаптация выбранного алгоритма для указанного контекста, предложен подход к разрежению графа при поиске наиболее критичной траектории. Представленные методы и алгоритмы реализованы в программном коде, для верификации результатов расчетов выполнены численные эксперименты (Приложение К). Разработанное программное обеспечение, основанное на предложенных методе и алгоритме, дополняет функционал предшествующих версий прототипов программ для анализа защищенности пользователей информационных систем от социоинженерных атак. Позволяет учитывать более широкий круг факторов, влияющих на оценку.

8 Выявление наиболее критичной траектории распространения многоходовой социоинженерной атаки с точки зрения ожидаемого ущерба

В данном исследовании впервые предлагается рассматривать траектории социоинженерных атак, наиболее критичные с точки зрения ожидаемого ущерба для организации, а не с точки зрения вероятности успеха поражения пользователя и, опосредованно, критичных документов, к которым он имеет доступ. В исследовании предлагается подход к решению задачи выявления наиболее критичной траектории реализации многоходовой социоинженерной атаки. Под наиболее критичной траекторией понимается наиболее вероятная траектория реализации атаки, которая принесёт наибольший ущерб организации. (Приложение Л) В качестве дальнейшего развития направления исследований можно рассмотреть модели, более детально описывающие контекст и учитывающие распределение вероятностей поражения доли документов, доступных пользователю, предлагающие модели для построение интегральных оценок ущерба, ассоциированных с пораженным пользователем, различные политики доступа и учет иерархии документов с точки зрения их критичности или ценности.

9 Гибридная модель выявления наиболее критичной траектории распространения многоходовой социоинженерной атаки

В данном исследовании предлагается гибридная модель нахождения наиболее критичных траекторий распространения многоходовых социоинженерных атак, прохожде-

ние злоумышленника по которым имеет в совокупности наивысшую степень вероятности и принесёт наибольший убыток компании. Решение задачи поиска наиболее критичных траекторий опирается на предположение о том, что уже рассчитаны оценки вероятности успеха прямой социоинженерной атаки на пользователя, оценки степени критичности документов, оценки вероятности распространения социоинженерной атаки от пользователя к пользователю, строящиеся на основе лингвистических нечётких переменных.(Приложение М) Описанная модель находит своё применение при построении оценок защищённости пользователей информационных систем от многоходовых социоинженерных атак и способствует своевременному информированию лиц, принимающих решения, об имеющихся в системе уязвимостях.

10 Подход наибольшего правдоподобия к задаче выявления траекторий социоинженерных атак

Целью исследования является усовершенствование инструментария расследования инцидентов информационной безопасности за счет разработки подходов наибольшего правдоподобия, направленных на выявление сценариев (траекторий) развития социоинженерных атак и скомпрометированных пользователей информационных систем. В качестве используемых методов выступают вероятностный подход к оценке степени уязвимости пользователей к социоинженерным атакам, графовая модель представления информационной системы организации, в которой отражены профили пользователей и взаимосвязи между ними, а также доступные им критические документы. Новизна работы заключается в том, что ранее расследование инцидентов информационной безопасности основывалось только на технических характеристиках и не учитывало подверженность персонала социоинженерному воздействию. Предлагается подход, основывающийся на оценках вероятности успеха одноходовых и многоходовых социоинженерных атак, опирающихся в том числе на профиль уязвимостей пользователя (Приложение Н). Результатом работы является подход, позволяющий осуществлять первичное расследование инцидентов информационной безопасности, связанных с реализацией социоинженерных атак, за счет разработки метода наибольшего правдоподобия, направленного на выявление траекторий социоинженерных атак и скомпрометированных пользователей ин-

формационных систем. Практическая значимость полученных результатов заключается в формировании инструмента для лиц, принимающих решения, дающем возможность сократить пространство поиска при расследовании инцидентов, связанных с успешной реализацией социоинженерной атаки; минимизировать время, необходимое для расследования преступления; определить основу для последующей разработки рекомендательных систем, способствующих понижению рисков реализации социоинженерных атак.

ЗАКЛЮЧЕНИЕ

Результаты работы, представленные в данном отчёте, закладывают основу для разработки систем упреждающей диагностики и проведения первичного расследования инцидентов информационной безопасности, связанных с реализацией социоинженерных атак, позволяют учесть более широкий круг факторов при анализе защищённости информационной системы от кибератак, предоставляют возможность быстро и эффективно находить наиболее уязвимые места информационной системы. Предложенная система комплексного анализа защищённости пользователей информационных систем позволят лицам, принимающим решения, производить своевременные меры по повышению уровня защищённости организации.

Была предложена концепция программного комплекса для оценки защищённости пользователей информационных систем от социоинженерных атак. Приведена архитектура прототипа программного комплекса, изложены подходы к построению алгоритмов для модулей, отвечающих за моделирование социоинженерной атаки на социальном графе сотрудников и восстановление мета-профиля пользователя на основании контента, публикуемого в социальных сетях.

Разработан алгоритм сопоставления аккаунтов пользователей в социальных сетях «ВКонтакте» и «Одноклассники» для определения аккаунтов, принадлежащих одному пользователю, предложены подходы для восстановления фрагмента мета-профиля. Разработан метод квантификации типов взаимоотношений пользователей, основанный на оценке вероятности успеха прохождения социоинженерного атакующего воздействия между ними.

Представлен подход к построению, анализу и визуализации социального графа сотрудников, дана критическая оценка разработанных ранее методов. Представлен алгоритм для вывода коэффициентов дуг социального графа, используемых при расчёте вероятности успеха опосредованной социоинженерной атаки. Предложены алгоритмы

вычисления вероятности поражения критичных документов информационной системы путем анализа социального графа сотрудников компании. Также был предложен подход к увеличению оперативности оценки защищённости критичных документов при многоходовых социоинженерных атаках.

Предложен подход к идентификации наиболее критичных траекторий, оценка вероятности успеха прохождения атаки по которым будет наиболее высокой. Произведён обзор алгоритмов, применение которых возможно при решении данной задачи, осуществлена адаптация выбранных алгоритмов к решению задачи поиска наиболее критичной траектории распространения социоинженерной атаки. Разработан алгоритм выявления наиболее критичной траектории и выполнена его реализация. Был предложен подход к решению задачи выявления наиболее критичной траектории реализации многоходовой социоинженерной атаки с другой точки зрения — с точки зрения наибольшего ущерба для организации. В результате была представлена учитывающая обе точки зрения гибридная модель нахождения наиболее критичных траекторий распространения многоходовых социоинженерных атак, прохождение злоумышленника по которым имеет в совокупности наивысшую степень вероятности и принесёт наибольший убыток компании.

Разработан подход к бэктрекингу по инцидентам, основывающийся на оценках вероятности успеха одноходовых и многоходовых социоинженерных атак, позволяющий осуществлять первичное расследование инцидентов информационной безопасности, связанных с реализацией социоинженерных атак, за счет разработки метода наибольшего правдоподобия, направленного на выявление траекторий социоинженерных атак и скомпрометированных пользователей информационных систем.

Разработаны программные модули, реализующие предложенные алгоритмы.

Практическая значимость полученных результатов заключается в расширении возможностей существующего программного комплекса для анализа защищенности пользователей информационных систем от социоинженерных атак. Разработанные методы и алгоритмы лягут в основу решения задачи поиска наиболее критичных траекторий реализаций атак в информационной системе с учетом уровней доступа пользователей и критичности документов. Перспективы дальнейшего исследования также заключаются

в разработке систем упреждающей диагностики и бэктрекинга инцидентов успешных социоинженерных атак. Также перспективы дальнейших исследований могут быть связаны с разработкой подходов к моделированию и оценке вероятностей успеха распространения многоходовых социоинженерных атак, в частности, может быть использован аппарат байесовских сетей [8].

Отраженные в отчете теоретические результаты были опубликованы в российских рецензируемых журналах (7 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» и одна из них с индексацией в SCOPUS), а также представлены на российских и международных конференциях разного уровня (9 публикаций с индексацией в SCOPUS и 12 публикации с индексацией РИНЦ) (Приложение Б). Результаты исследования были также отражены в монографии. Кроме того, теоретические и алгоритмические разработки были частично реализованы в ряде программ — компонент комплекса программ; часть указанных компонент прошла регистрацию в качестве программ для ЭВМ в Роспатенте (11 регистраций) (Приложение В). Математические формулировки определений и обоснование результатов приведены в Приложениях Г—Н.

По тематике гранта защищена диссертация «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» Абрамовым Максимом Викторовичем, приказ Минобрнауки № 331/нк от 12 декабря 2018 г. (приложение № 27), стр. 51, позиция 2, получен диплом кандидата наук серия КНД №082790.

Таким образом, все задачи исследования выполнены, а цель — достигнута.

ПРИЛОЖЕНИЕ А
Перечень грантов, заказанных НИР, контрактов, хоздоговоров, которыми поддерживались исследования по данной НИР

1. Грант РФФИ, проект № 18-37-00323 — «Социоинженерные атаки в корпоративных информационных системах: подходы, методы и алгоритмы выявления наиболее вероятных траекторий», руководитель М.В. Абрамов.

ПРИЛОЖЕНИЕ Б
Список публикаций в рамках проекта

1. *Абрамов М.В., Тулупьев А.Л.,Тулупьева Т.В.* Социоинженерные атаки: социальные сети и оценки защищенности пользователей // СПб.: ГУАП, 2018. — 266 с.
2. *Хлобыстова А.О., Абрамов М.В., Тулупьев А.Л., Золотин А.А.* Поиск кратчайшей траектории социоинженерной атаки между парой пользователей в графе с вероятностями переходов // Информационно-управляющие системы. — 2018. — С. 74—81. doi:10.31799/1684-8853-2018-6-74-81 (SCOPUS, Список ВАК, РИНЦ).
3. *Khlobystova A.O., Abramov M.V., Tulupyev A.L.* An approach to estimating of criticality of social engineering attacks traces // Studies in Systems, Decision and Control. — 2019. — P. 446–456. doi: 10.1007/978-3-030-12072-6_36 (SCOPUS).
4. *Malchevskaya E., Kharitonov N., Zolotin A., Abramov M.* External Consistency Maintenance Algorithm for Chain and Stellate Structures of Algebraic Bayesian Networks: Statistical Experiments for Running Time Analysis // Advances in Intelligent Systems and Computing. Proceedings of the Third International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'18). — Springer, 2018. — P. 23–30. DOI: 10.1007/978-3-030-01821-4_3. (SCOPUS)
5. *Khlobystova A.O., Abramov M.V., Tulupyev A.L.* Identifying the most critical trajectory of the spread of a social engineering attack between two users // The Second International Scientific and Practical Conference "Fuzzy Technologies in the Industry – FTI 2018". CEUR Workshop Proceedings. — P. 38–43. (SCOPUS).
6. *Suleimanov A., Abramov M., Tulupyev A.* Modelling of the social engineering attacks based on social graph of employees communications analysis // Proceedings of 2018 IEEE Industrial Cyber-Physical Systems (ICPS). St.-Petersburg. 2018. — P. 801–805. (SCOPUS).

7. *Khlobystova A.O., Abramov M.V., Tulupyev A.L.* Soft Estimates for Social Engineering Attack Propagation Probabilities Depending on Interaction Rates Among Instagram Users // International Symposium on Intelligent and Distributed Computing. — Springer, Cham, 2019. — P. 272–277. doi: 10.1007/978-3-030-32258-8_32 (SCOPUS)
8. *Khlobystova A.O., Abramov M.V., Tulupyev A.L.* Employees' social graph analysis: a model of detection the most criticality trajectories of the social engineering attack's spread // Advances in Intelligent Systems and Computing. Proceedings of the 4th International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'19). — Springer, 2019. (SCOPUS) (ожидает индексации)
9. *Khlobystova A.O., Tulupyeva T.V., Maksimov A.G., Korepanova A.A.* An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations // Advances in Intelligent Systems and Computing. Proceedings of the 4th International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'19). — Springer, 2019. (SCOPUS) (ожидает индексации)
10. *Abramov M. V., Tulupyev A. L.* Soft Estimates of User Protection from Social Engineering Attacks // Conference on Artificial Intelligence and Natural Language. — Springer, Cham, 2019. — P. 47–58. (SCOPUS)
11. *Абрамов М.В.* Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак // Автоматизация процессов управления. 2018. №1(51). — С. 34–40. (Список ВАК, РИНЦ)
12. *Суворова А.В., Смирнова К.Р., Будин Е.А., Тулупьева Т.В., Тулупьев А.Л., Абрамов М.В.* Исследовательский проект как инструмент обучения методам анализа текста: предсказание класса поста в социальной сети // Компьютерные инструменты в образовании. — 2018. — N 3. — С. 49–64. (Список ВАК, РИНЦ).
13. *Хлобыстова А.О., Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л.* Социальное влияние на пользователя в социальной сети: типы связей в оценке поведенческих рисков, связанных с социоинженерными атаками // Управленческое консультирование. — 2019. — N 3. — С. 104–117. doi: 10.22394/1726-1139-2019-3-104-117 (Список ВАК, РИНЦ)

14. *Хлобыстова А. О., Абрамов М. В., Тулупьев А. Л.* Подходы наибольшего правдоподобия к задаче выявления траекторий социоинженерных атак и скомпрометированных пользователей информационных систем // Системы управления, связи и безопасности. — 2019. — N 3. — С. 202–219. doi: 10.24411/2410-9916-2019-10310 (Список ВАК, РИНЦ)
15. *Максимов А.Г., Завалишин А.Д., Абрамов М.В., Тулупьев А.Л.* Молекулярная дескрипция сульфида кадмия // Компьютерные инструменты в образовании. — 2019. — N 3. (Список ВАК, РИНЦ)
16. *Корепанова А.А., Олисиенко В.Д., Абрамов М.В., Тулупьев А.Л.* Применение методов машинного обучения в задаче идентификации аккаунтов пользователя в двух социальных сетях // Компьютерные инструменты в образовании. — 2019. — N 3. (Список ВАК, РИНЦ)
17. *Сулейманов А.А., Абрамов М.В., Тулупьев А.Л.* Оценка вероятности поражения критичного документа при многоходовых социоинженерных атаках // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2018). Санкт-Петербург. Том 1–2. — 2018. — Т. 1. — С. 130–133. (РИНЦ).
18. *Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В.* Агрегирование данных из социальных сетей для восстановления фрагмента мета-профиля пользователя // Шестнадцатая Национальная конференция по искусственному интеллекту с международным участием КИИ-2018 (24–27 сентября 2018 г., г. Москва, Россия). Труды конференции. В 2-х томах. — 2018. — Т 1. — С. 189–197. (РИНЦ).
19. *Абрамов М.В., Тулупьев А.Л., Сулейманов А.А.* Задача анализа защищённости пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей // Научно-технический вестник информационных технологий, механики и оптики. — 2018. — N 2. — С. 313–321. doi: 10.17586/2226-1494-2018-18-2-313-321. (РИНЦ).
20. *Абрамов М.В., Слезкин Н.Е., Тулупьева Т.В.* Агрегация данных из социальных сетей для определения наиболее вероятной конфигурации пропущенных значений параметров мета-профиля пользователя // Сборник докладов Международной кон-

ференции по мягким вычислениям и измерениям (SCM-2018). Санкт-Петербург. Том 1–2. — 2018. — Т. 1. — С. 118–121. (РИНЦ).

21. *Корепанова А.А., Абрамов М.В., Тулупьева Т.В.* Идентификация аккаунтов пользователей в социальных сетях «Вконтакте» и «Одноклассники» // Семнадцатая Национальная конференция по искусственному интеллекту с международным участием. КИИ–2019 (21–25 октября 2019 г., г. Ульяновск, Россия). Сборник научных трудов. В 2 т. — Ульяновск: УлГТУ, 2019. — Т.2. — С. 153–163. (РИНЦ)
22. *Абрамов М.В.* Модель оценки защищенности пользователей информационных систем от социоинженерных атак, опирающаяся на профиль компетенций злоумышленника и профиль уязвимостей пользователя // Региональная информатика (РИ–2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ–2018)». (Санкт–Петербург, 24–26 октября 2018 г.): Материалы конференции. — СПб: СПОИСУ, 2018. — С. 539–540.
23. *Азаров А.А., Абрамов М.В., Шиндарев Н.А.* Идентификация аккаунтов сотрудников компании в социальной сети с целью построения фрагмента профиля уязвимостей пользователя // Региональная информатика (РИ–2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ–2018)». (Санкт–Петербург, 24–26 октября 2018 г.): Материалы конференции. — СПб: СПОИСУ, 2018. — С. 540–543.
24. *Багрецов Г.И.* Построение профиля уязвимостей пользователя социальной сети в условиях неполной информации // Региональная информатика (РИ–2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ–2018)». (Санкт–Петербург, 24–26 октября 2018 г.): Материалы конференции. — СПб: СПОИСУ, 2018. — С. 543–544.
25. *Бушмелев Ф.В., Харитонов Н.А.* Использование байесовских сетей при анализе защищенности пользователей информационных систем от социоинженерных атак // Региональная информатика (РИ–2018). XVI Санкт–Петербургская международная конференция «Региональная информатика (РИ–2018)». (Санкт-Петербург, 24–26 октября 2018 г.): Материалы конференции. — СПб: СПОИСУ, 2018. — С. 544–545.

26. *Хлобыстова А. О., Абрамов М.В.* Выявление наиболее критичных траекторий распространения многоходовых социоинженерных атак // Региональная информатика (РИ–2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ–2018)». (Санкт-Петербург, 24–26 октября 2018 г.): Материалы конференции. — СПб: СПОИСУ, 2018. — С. 560–561.
27. *Шаламов Р. А., Абрамов М.В., Тулупьева Т. В., Азаров А. А.* Автоматизация оценки степени выраженности психологических особенностей пользователей для принятия кадровых решений: тестирование в социальной сети // Материалы конференции «Информационные технологии в управлении» (ИТУ–2018). — СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. — С. 497–500.
28. *Хлобыстова А. О., Абрамов М. В., Тулупьев А. Л.* Идентификация наиболее вероятных траекторий социоинженерных атак в управлении рисками, ассоциированными с пользователями/персоналом // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). — СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. — С. 493–496.
29. *Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В.* Психологические особенности, психические состояния пользователя и профиль его уязвимостей в контексте социоинженерных атак // Психология психических состояний: сб. статей студентов, магистрантов, аспирантов и молодых ученых. — Казань, 2019. — С. 312–317.
30. *Хлобыстова А.О., Абрамов М.В.* Распределение прав доступа в системе как мера понижения вероятности успеха социоинженерной атаки // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г.: Материалы конференции — СПб.: СПОИСУ. — С. 454–455.
31. *Хлобыстова А.О.* «SHARENTING» — как угрозообразующее поведение к социоинженерным атакам // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г.: Материалы конференции — СПб.: СПОИСУ. — С. 452–454.
32. *Корепанова А.А., Тулупьева Т.В.* Идентификация аккаунтов пользователя в различных социальных сетях по социальному окружению // Информационная безопас-

ность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г.: Материалы конференции — СПб.: СПОИСУ. — С. 442–443.

33. *Корепанова А.А.* Сопоставление пользовательских аккаунтов на основе поведенческих паттернов // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г.: Материалы конференции — СПб.: СПОИСУ. — С. 441–442.
34. *Хлобыстова А.О., Абрамов М.В.* Подход к анализу социального графа сотрудников компании с целью повышения уровня защищённости информационной системы от СИА // Материалы 8-й всероссийской научной конференции по проблемам информатики СПИСОК-2019. (23–26 апреля 2019 г. Санкт-Петербург). — СПб.: ВВМ, 2019.
35. *Хлобыстова А.О., Корепанова А.А.* Ранжирование траекторий распространения СИА в зависимости от ожидаемого ущерба // Материалы 8-й всероссийской научной конференции по проблемам информатики СПИСОК-2019. (23–26 апреля 2019 г. Санкт-Петербург). — СПб.: ВВМ, 2019.
36. *Корепанова А.А., Абрамов М.В., Олисеенко В.Д*. Сопоставление публичных анкет аккаунтов пользователей в различных социальных сетях // Материалы 8-й всероссийской научной конференции по проблемам информатики СПИСОК-2019. (23–26 апреля 2019 г. Санкт-Петербург). — СПб.: ВВМ, 2019.
37. *Корепанова А.А.* Сопоставление алгоритмов восстановления пропущенных данных профиля // Материалы 8-й всероссийской научной конференции по проблемам информатики СПИСОК-2019. (23-–26 апреля 2019 г. Санкт-Петербург). — СПб.: ВВМ, 2019.

ПРИЛОЖЕНИЕ В
Список программ для ЭВМ, алгоритмов и баз данных, разработанных на основе результатов, полученных в НИР

1. *Слезкин Н.Е., Сулейманов А.А., Абрамов М.В., Тулупъев А.Л., Тулупъева Т.В.* User Data Aggregation for Social Engineering Attacks Modeling Version 02 (SocND Aggregator v.02) (Свидетельство). Свид. о госуд. регистрации No 2018615900(17.05.2018). Роспатент.
2. *Сулейманов А.А., Слезкин Н.Е., Абрамов М.В., Тулупъев А.Л. Тулупъева Т.В.* Employees Social Graph Analyzer for Social Engineering Attacks Modeling Java Version 01 (ESGA for SEA Modeling j.v.01). Свид. о госуд. регистрации No 2018615561(10.05.2018). Роспатент.
3. *Сулейманов А.А., Абрамов М.В., Тулупъев А.Л.* Employees Social Interactions Graph Analyzer for Social Engineering Attacks Modeling Version 01 (ESIGA For SEA Modeling, v.01). Свид. о госуд. регистрации No 2018612149 (13.02.2018). Роспатент.
4. *Слезкин Н.Е., Абрамов М.В., Тулупъев А.Л.* User Data Aggregation for Social Engineering Attacks Modeling Version 01 (SocND Aggregator v.01) Свид. о госуд. регистрации No 2018612147 (13.02.2018). Роспатент.
5. *Шиндарёв Н.А., Абрамов М.В., Тулупъев А.Л.* Parsing Employees Pages in Websites of Social Network for Social Engineering Attacks Modeling Version 01 (PEP in WSSN, v.01). Свид. о госуд. регистрации No 2018612139 (13.02.2018). Роспатент.
6. *Бушмелев Ф.В., Абрамов М.В., Тулупъев А.Л.* Social Engineering Attacks Security Assessment of Critical Documents, Version 01 for Java (SEA S Assessment CD jav.v.01) (Свидетельство). Свид. о гос. рег. прогр. для ЭВМ. Рег. № 2019610853 (11.02.2019)

7. *Хлобыстова А.О., Абрамов М.В., Тулупьев А.Л.* Identifying critical trajectory of the spread of a social engineering attack, Version 01 for Java (ICTS SEA jav.v.01) (Свидетельство). Свид. о гос. рег. прогр. для ЭВМ. Рег. № 2019610872 (12.02.2019)
8. *Хлобыстова А.О., Абрамов М.В., Тулупьев А.Л, Тулупьева Т.В.* Quantification of relationship represented in the social network, Version 01 for CSharp (QR SN cs.v.01) (Свидетельство). Свид. о гос. рег. прогр. для ЭВМ. Рег. № 2019610870 (12.02.2019)
9. *Корепанова А.А., Абрамов М.В., Тулупьев А.Л* Social Network Data Aggregator for "VK" and "OK.ru", Version 01 for CSharp (SNDA cs.v.01) (Свидетельство). Свид. о гос. рег. прогр. для ЭВМ. Рег. № 2019612298 (14.02.2019)
10. *Максимов А.Г., Завалишин А.Д., Абрамов М.В., Тулупьев А.Л.* Not/and/or Expression Simplifier Version 01 (n/a/o ExpSimp v.01) (Свидетельство). Свид. о гос. рег. прогр. для ЭВМ. Рег. № 2019666364 (09.12.2019)
11. *Завалишин А.Д., Максимов А.Г., Абрамов М.В., Тулупьев А.Л.* Realization b-tree with compression Version 01 for CPlusPlus (RoBtreeCom v.01) (Свидетельство). Свид. о гос. рег. прогр. для ЭВМ. Рег. № 2019666627 (12.12.2019)