ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01,
СОЗДАННОГО НА БАЗЕ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА
ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК, ФЕДЕРАЛЬНОЕ АГЕНТСТВО НАУЧНЫХ
ОРГАНИЗАЦИЙ, ПО ДИССЕРТАЦИИ
НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета 07.06.2018 г. № 2

О присуждении Абрамову Максиму Викторовичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 05 апреля 2018 г. (протокол заседания № 1) диссертационным советом Д 002.199.01, созданным на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Федеральное агентство научных организаций, 199178, Россия, Санкт-Петербург, 14я линия В.О., дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Абрамов Максим Викторович, 1990 года рождения, в 2013 г. окончил Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет» по специальности «Прикладная информатика (в сфере международных отношений)» (диплом № СА 10623), в 2016 г. окончил очную аспирантуру в Федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет» (СПбГУ). Справка о сдаче кандидатских экзаменов № 19/209 от 26 декабря 2017 года, выдана Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук

(СПИИРАН). В настоящее время Максим Викторович Абрамов работает младшим научным сотрудником лаборатории теоретических и междисциплинарных проблем информатики в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН), Федеральное агентство научных организаций.

Диссертация выполнена на кафедре информатики Федерального государственного бюджетного учреждения высшего образования «Санкт-Петербургский государственный университет» (СПбГУ), Правительство Российской Федерации, и в лаборатории теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), Федеральное агентство научных организаций.

Научный руководитель — доктор физико-математических наук, доцент ТУЛУПЬЕВ Александр Львович, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), заведующий лабораторией теоретических и междисциплинарных проблем информатики.

Официальные оппоненты:

ОВЧАРОВ Владимир Александрович, доктор технических наук, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Военно-космическая академия имени А.Ф. Можайского» Министерства обороны Российской Федерации, заместитель начальника 3 управления — начальник 31 отдела военного института (научно-исследовательского);

КРАСОВ Андрей Владимирович, кандидат технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», кафедра защищённых систем связи, заведующий кафедрой,

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский

национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО), г. Санкт-Петербург, в своем положительном отзыве, подписанном Сергеем Валентиновичем Беззатеевым, доктором технических наук, доцентом, заведующим кафедрой безопасности киберфизических систем Университета ИТМО, Даниилом Анатольевичем Заколдаевым, кандидатом технических наук, доцентом, деканом факультета безопасности информационных технологий Университета ИТМО и утвержденном Владимиром Олеговичем Никифоровым, доктором технических наук, профессором, проректором по научной работе, председателем Научно-технического совета Университета ИТМО, указала, что диссертационная работа М.В. Абрамова представляет собой законченную научно-квалификационную работу, в которой решена задача повышения оперативности обнаружения угроз социоинженерных атак за счёт автоматизации экспресс-оценки защищённости/поражаемости пользователей информационной системы от социоинженерных атак, учитывающей результаты агрегации сведений из социальных сетей и других источников, для оценки параметров моделей указанных пользователей и связей между ними, имеющая существенное значение для развития подходов к обеспечению внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и к оценке защищенности информации и информационной безопасности объекта.

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

Диссертация «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» соответствует всем критериям, предъявляемым в отношении кандидатских диссертаций, которые установлены «Положением о присуждении ученых степеней», утвержденным Постановлением Правительства РФ № 842 от 24 сентября 2013

(редакция от 28 августа 2017), а ее автор Максим Викторович Абрамов заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 72 опубликованные работы, в том числе по теме диссертации опубликовано 55 работ, из них в рецензируемых научных изданиях опубликовано 6 работ (из которых одна единоличная), в изданиях, индексируемых Scopus/WoS — 7, докладов и тезисов на научных конференциях — 40 (из которых 9 единоличных), монографий — 2 (в соавторстве), соискатель также является соавтором 7 программ для ЭВМ, на которые получены свидетельства о государственной регистрации (РОСПАТЕНТ).

Научные результаты опубликованы в 55 научных трудах общим объемом 56,375 п.л., причём основные научные результаты опубликованы в 20 научных трудах объёмом 5,123 п.л., из которых 5 статей в рецензируемых научных изданиях объемом 2,31 п.л., выполнены в соавторстве, 1 статья объемом 0,625 п.л. — единолично, 7 работ объёмом 2,188 п.л. в соавторстве опубликовано в изданиях, индексируемых на платформах Scopus/WoS, а также получено 7 свидетельств о государственной регистрации программ для ЭВМ (РОСПАТЕНТ). Наиболее значимые работы по теме диссертации:

1. **Абрамов, М.В.** Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак / **М.В. Абрамов** // Автоматизация процессов управления. 2018. №1(51). С. 34–40.
2. **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. *Личный вклад соискателя – 65%.*
3. 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. *Личный вклад соискателя – 35%.*
4. Азаров, А.А. Применение вероятностно-реляционных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» для анализа защищенности пользователей информационных систем от социо-инженерных атак / А.А. Азаров, **М.В. Абрамов**, Т.В. Тулупьева, А.А. Фильченков // Нечеткие системы и мягкие вычисления. 2015. №2. С.209–221. *Личный вклад соискателя – 45%.*

5. **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. *Личный вклад соискателя – 55%.*
6. **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. *Личный вклад соискателя – 60%.*

Оригинальность содержания диссертации составляет не менее 90% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве, без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 18 отзывов, все отзывы положительны:

1) Федеральное государственное бюджетное образовательное учреждение высшего образования «Тверской государственный университет». Отзыв составил декан факультета прикладной математики и кибернетики, доктор физико-математических наук, профессор А.В. Язенин. Замечания: Соискатель резонно предлагает использовать t-норму как основу для совместного учета степени выраженности уязвимости пользователя и уровня владения атакующим воздействием при формировании оценки успеха социоинженерного атакующего воздействия, не указав, однако, на основе каких ожидаемых свойств оценки такой выбор сделан и не обсудив более широкий класс вариантов, где перестановка аргументов может привести к несовпадающим результатам. Кроме того, t-нормы активно используются в нечеткой логике и в теории копул, рассмотрение связи с которыми могло бы привести к содержательным для рассматриваемой в диссертации предметной области ассоциациям;

2) Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ». Отзыв составила профессор кафедры кибернетики, доктор технических наук, профессор, академик РАЕН Г.В. Рыбина. Замечания: Судя по тексту

автореферата, предложенные вероятностные модели оценки защищённости/поражаемости документов разного уровня критичности от социоинженерных атак не учитывают оценку злоумышленника вероятности того, что пользователь, успешно им атакованный, имеет доступ к подобным документам. Данный аспект открыл бы, на мой взгляд, возможность моделировать атаки злоумышленника с учётом его начальных знаний о соответствующей киберсоциальной системе;

3) Федеральное государственное бюджетное учреждение науки Институт программных систем имени А.К. Айламазяна Российской академии наук. Отзыв составил заведующий лабораторией интеллектуального управления, главный научный сотрудник исследовательского центра мультипроцессорных систем, доктор технических наук, профессор В.М. Хачумов. Замечания: 1. В пункте 1 Заключения предложение «Предложены усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник» фактически повторяет смысл первого предложения этого пункта; 2. Имеет место перегруженность некоторых предложений сложными оборотами с многочисленными запятыми; 3. На рисунке 3 записи на скриншотах интерфейсов оказались практически нечитаемыми;

4) Федеральное государственное бюджетное образовательное учреждение высшего образования «Национальный исследовательский университет «МЭИ». Отзыв составил профессор кафедры прикладной математики Института информатики и вычислительной техники, д.т.н., профессор И.Б. Фоминых. Замечания: на 12 странице автореферата соискатель упоминает проактивные методы, которые используются для расширения пространства поиска за счёт ручного включения новых вершин, однако не поясняется, что понимается под проактивностью в данном случае;

5) Северо-Западный институт управления – филиал РАНХиГС. Отзыв составил заведующий кафедрой бизнес-информатики, математических и статистических методов, доктор военных наук, кандидат технических наук, профессор В.Н. Наумов. Замечания: соискатель не затрагивает гранулярность — существенную особенность данных и знаний, доступных для формирования искомых оценок, от которых, в свою очередь, тоже можно ожидать наличия подобной особенности;

6) Федеральное государственное бюджетное образовательное учреждение высшего образования «Ульяновский государственный технический университет». Отзыв составила первый проректор — проректор по научной работе, заведующая кафедрой «Информационные системы», Н.Г. Ярушкина. Замечания: соискатель в качестве компонент модели злоумышленника вводит модель профиля компетенций злоумышленника и ресурсов. Далее на их основе вполне правильно предлагаются вероятностные модели для оценки степени защищённости пользователей информационных систем и критичных документов. Вместе с тем ресурс, доступный злоумышленнику, можно рассматривать неразрывно с его применением и включить в качестве компетенции в профиль компетенций злоумышленника. Вероятно, такой подход позволит рассмотреть новые вероятностные модели оценки защищённости пользователей от социоинженерных атак;

7) Федеральное государственное бюджетное учреждение науки Институт проблем транспорта им. Н.С. Соломенко РАН. Отзыв составил заместитель директора по научной работе д.т.н., доцент В.И. Комашинский. Замечания: стоит отметить, что некоторые виды атакующих воздействий могут быть взаимосвязаны, что даёт возможность рассматривать классы атакующих воздействий и строить профиль на их основании, этот вопрос не рассматривается в автореферате;

8) Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации». Отзыв составил сотрудник Академии ФСО России, доктор технических наук, профессор И.А. Саитов. Замечания: не обоснован выбор математического аппарата при формировании оценок защищённости/поражаемости пользователей. Вызывает сомнение возможность получения конструктивных оценок предложенными гибридными (нечеткостно-вероятностными) моделями, при этом к настоящему времени в предметной области информационной безопасности имеется развитой и хорошо апробированный математический аппарат исследования переменных, заданных в нечётком базисе. Из автореферата не ясно, учитывались ли погрешности оценки эксперта (при оценке степени компетентности злоумышленника) из-за субъективности, ошибок, некомпетентности или злонамеренности собственно

эксперта. Это не позволяет оценить качество итогового решения задачи анализа защищённости данных групп пользователей;

9) Государственная корпорация «РОСТЕХ» Акционерное общество «Российская электроника» Акционерное общество «Научно-исследовательский институт программных средств». Отзыв составил начальник научно-исследовательского отдела, кандидат технических наук С.В. Максимов. Замечания: в названии темы исследования в качестве одной из задач сформулирована оценка параметров разработанных моделей, однако способ решения этой задачи в автореферате описан слишком абстрактно; в качестве цели исследования выступает повышение оперативности обнаружения угроз за счёт автоматизации оценки защищённости пользователей, представляется, что в данном случае причина и следствие поменялись местами, угрозы являются совокупностью условий и факторов, создающих опасность нарушения защищённости пользователей (ГОСТ Р 50922-2006), т.е. логичнее было бы повышать оперативность оценки защищённости пользователей за счёт автоматизации обнаружения угроз; неясно, каким образом и откуда будут получаться исходные данные (ресурсы доступные злоумышленника, степень владения им атакующими воздействиями, выраженность у пользователя уязвимости и т.п.) для разработанных моделей и методов;

10) Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича». Отзыв составил заведующий базовой кафедрой специальных средств связи, доктор технических наук, доцент В.В. Котов. Замечания: на рисунке 1 по оси ординат отложена частота, но нет пояснения что имеется в виду; на рисунке 2 подписи компонент выполнены на русском языке, а дуги, их соединяющие подписаны на английском, существовала ли необходимость делать рисунок билингвальным;

11) Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I». Отзыв составил заведующий кафедрой «Информационные и вычислительные системы», доктор технических наук, профессор А.Д. Хомоненко. Замечания: в третьей главе для проведения экспресс-оценки с целью ускорения

расчёта оценки защищённости/поражаемости количество ресурса рассматривается как величина, которая допускает «квантование», но не указано с какой частотой ресурс будет «квантоваться» и от чего это значение будет зависеть. При меньшей частоте «квантования» будет получен меньший объём данных для обработки и меньшая точность при определении достижения пороговой величины, тогда как при большей частоте точность определения достижения пороговой величины увеличивается, но и увеличивается объём данных для обработки. В автореферате отсутствуют оценки затрат вычислительных ресурсов на реализацию разработанной архитектуры прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем;

12) Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управление и радиоэлектроники». Отзыв составил проректор по научной работе и инновациям, заведующий кафедрой безопасности информационных систем, доктор технических наук, профессор Р.В. Мещеряков и старший научный сотрудник кафедры безопасности информационных систем, кандидат технических наук О.О. Евсютин. Замечания: неясно, каким образом в предлагаемых моделях (модель критичных документов, модель хостов информационной системы и т.д.) учитывается временная динамика информационной системы. В частности, множество пользователей, имеющих доступ к i-му документу определённого уровня, может быть различным в разные моменты времени. Автор указывает, что количество ресурса, которым обладает злоумышленник, рассматривается не как непрерывная величина, а как величина, которая допускает «квантование». Однако непонятно, каким образом следует квантовать такой ресурс злоумышленника, как его личностные особенности (стр. 8 автореферата). В автореферате не определено неоднократно упоминаемое понятие многоходовой социоинженерной атаки;

13) Федеральное государственное бюджетное учреждение «Научно-исследовательский испытательный центр подготовки космонавтов имени Ю.А. Гагарина». Отзыв составили главный научный сотрудник, доктор технических наук Б.И. Крючков и начальник отдела, кандидат технических наук С.Н. Ковригин. Замечания: при прочтении работы серьёзные недостатки не были выявлены, однако

стоит отметить, что в модели вероятности успеха социоинженерного атакующего воздействия злоумышленника с использованием i-ого атакующего воздействия на j-ую уязвимость пользователя используется матрица пороговых значений. Интересно было бы рассмотреть использование в модели пороговой функции;

14) Федеральный научно-производственный центр акционерное общество «Научно-производственное объединение «Марс». Отзыв составил главный научный сотрудник, доктор технических наук, доцент Г.П. Токмарёв. Замечания: в диссертационной работе в качестве компонент модели злоумышленника соискателем закономерно рассматриваются доступные ему ресурсы, профиль компетенций, начальные знания о системе, цели и связи. Тем не менее, в качестве ещё одного компонента по аналогии с профилем пользователя можно рассматривать личностные особенности злоумышленника, которые способствуют проведению социоинженерной атаки;

15) Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Отзыв составил заведующий кафедрой технологий интроскопии, доктор технических наук А.В. Фёдоров. Замечания: соискатель употребляет термин «многоходовая социоинженерная атака», но не поясняет в тексте автореферата его значение; список публикаций можно было бы сократить до основных работ, где изложены научные результаты, выносимые на защиту, а полный список указать в диссертации, так как на некоторые из них соискатель в автореферате не ссылается;

16) Федеральное государственное бюджетное учреждение «Национальный исследовательский центр «Курчатовский институт» (НИЦ «Курчатовский институт»). Отзыв составил руководитель Отделения нейрокогнитивных наук и интеллектуальных систем, кандидат технических наук, доцент В.Э. Карпов. Замечания: неясно, как связаны между собой задачи поиска сотрудников компании в соцсети ВКонтакте с решением задач выявления уязвимостей. Для чего и, главное, каким образом определяются политические и религиозные взгляды, каким образом последние влияют на безопасность. Неясна степень практической проработанности результатов исследования. Неясно, существует ли экспериментальное подтверждение

предлагаемым в работе теоретическим моделям. Судя по тексту автореферата, исследования завершены лишь созданием прототипа программного комплекса (хотя в тексте упоминаются акты о внедрении результатов диссертационной работы);

17) Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский университет Государственной противопожарной службы МЧС России». Отзыв составил профессор кафедры прикладной математики и информационных технологий, доктор технических наук, профессор М.В. Буйневич. Замечания: содержание глав даётся крайне неравномерно: на первую и вторую главы отводится по одному абзацу, тогда как на третью — 6 страниц, а на четвёртую — 1 страница. Формулировка третьего основного научного результата содержит в основном практическую значимость, а не его определение или суть. Не раскрыто понятие «выраженности ряда особенностей пользователей», что не позволяет напрямую соотнести алгоритмы автоматизированного поиска аккаунтов сотрудников с областью информационной безопасности и защиты информации. В списке работ, опубликованных автором по теме диссертации, не приведены свидетельства о государственной регистрации программ для ЭВМ, которые служат доказательствами достоверности и авторства основных научных результатов, и которые в соответствии с п.13 «Положения о порядке присуждения учёных степеней» относятся к публикациям в рецензируемых изданиях;

18) Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения». Отзыв составили профессор кафедры № 14, кандидат технических наук Н.А. Шехунова, заведующий кафедрой №14, доктор технических наук, профессор Ю.Е. Шейнин, учёный секретарь кафедры №14, кандидат технических наук Н.А. Громова; утвержден ректором ГУАП, доктором экономических наук Ю.А. Антохиной. Замечания: судя по автореферату, автор предлагает подход к автоматизированному анализу защищённости пользователей. Очевидно, что за счёт автоматизации предполагается достигнуть существенного повышения оперативности обнаружения угроз от возможных социоинженерных атак, однако, из автореферата не ясно построены ли в диссертации метрики оценки повышения оперативности.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н. В.А. Овчаров является известным ученым в области информационной безопасности, технологии мониторинга сетей, анализа трафика, кластерного анализа, теории вычислительной сложности; к.т.н., доцент, А.В. Красов — известный специалист в области программно-технических методов защиты информации; ведущая организация, Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», является известной как в России, так и за рубежом организацией в области разработки моделей и методов для анализа защищённости и обеспечения защиты информации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны методы, модели, алгоритмы и их реализация, которые создают основу для получения оценок защищённости/поражаемости пользователей информационной системы на основании информации, извлекаемой из их аккаунтов в социальных сетях;

предложены:

усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник», который является развитием другого ранее разработанного комплекса, имевшего ключевой особенностью учёт профиля уязвимостей пользователя, основным отличающим элементом развития стало дополнение существующего комплекса «критичные документы — информационная система — пользователь» моделью злоумышленника, впервые предложена модель и основанный на ней метод оценки вероятности успеха социоинженерной атаки злоумышленника на пользователя, опирающиеся на профили уязвимостей пользователя и компетенций злоумышленника;

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

методы, модели, алгоритмы и их реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте, основанные на

методах машинного обучения, в целях оценки параметров моделей используются данные, извлекаемые из социальных сетей, модель, которая позволяет автоматизированно на основании данных, содержащихся в контенте, публикуемом пользователями в социальных сетях, давать оценки степени выраженности ряда особенностей их личности, а также новые методы, позволяющие дополнить фрагмент мета-профиля пользователя информационной системы, которые построены на основе агрегации доступных сведений из альтернативных источников;

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

доказана перспективность использования предложенных моделей, методов и алгоритмов анализа защищённости пользователей информационных систем от социоинженерных атак злоумышленников;

введены:

- новые методы и алгоритмы для оценки параметров модели пользователя, входящей в комплекс «критичные документы – информационная система – пользователь – злоумышленник»;
- параметры, оценка которых позволяет строить профиль уязвимостей пользователей, используемой при расчёте вероятности успеха социоинженерной атаки злоумышленника на пользователя;

Теоретическая значимость исследования обоснована тем, что:

Доказаны корректность работы построенных методов и алгоритмов для оценки параметров моделей пользователя и профиля уязвимостей пользователя, и выполнимость теоретических утверждений, составляющих основу процесса разработки программной архитектуры;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использованы 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;

изложены методологические и методические основы исследования в области автоматизированного анализа защищённости пользователей информационных систем от социоинженерных атак;

раскрыты

проблемные аспекты в области информационной безопасности, связанные с защитой пользователей от социоинженерных атак;

основные подходы к защите и анализу защищённости пользователей киберсоциальных систем от социоинженерных атак;

основания классификаций угроз информационной безопасности и подходы к их систематизации;

изучены существующие подходы к исследованиям в информационной безопасности и социальной инженерии, подходы к оценке информации в интересах рефлексивного управления, анализу защищённости компьютерных сетей, основанных на обработке деревьев атак;

проведена модернизация существующих методов и моделей оценки защищённости пользователей информационных систем от социоинженерных атак злоумышленника.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

- 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
- 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;
- комплекс программ, реализующий модели «критичные документы – информационная система – пользователь – злоумышленник» и связи между ними для оценки защищённости пользователей от социоинженерных атак;

применяются при оценке рисков утечки конфиденциальной информации, проводимой отделом информатизации и связи администрации Центрального района Санкт-Петербурга; успешно используются в кадровой работе отдела кадров ЗАО «Завод им. Козицкого», а также в работу службы безопасности для анализа защищённости пользователей информационной системы предприятия; с позитивными результатами были применены в работе HR-отдела для модернизации кадровой политики и принятия решений о приёме на работу ООО «Метеор», а также использованы при выполнении работ по проектам:

«Социоинженерные атаки в корпоративных информационных системах: подходы, методы и алгоритмы выявления наиболее вероятных траекторий», грант РФФИ № 18-37-00323 мол_а (соискатель — руководитель проекта);

«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;

«Методология интеллектуального поиска маркеров в Интернет-контенте», грант РФФИ № 14-07-00694-а;

«Методы идентификации параметров социальных процессов по неполной информации на основе вероятностных графических моделей», грант РФФИ № 16-31-00373;

определены возможности и перспективы практического использования полученных результатов диссертации в оценке рисков утечки конфиденциальной

информации, в кадровой работе отдела кадров, в работе HR-отдела для модернизации кадровой политики и принятия решений о приёме на работу;

созданы методы и алгоритмы для 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;

представлены итоги диссертационного исследования, заключающиеся в решении научной задачи повышения оперативности обнаружения угроз социоинженерных атак за счёт автоматизации экспресс-оценки защищённости/поражаемости пользователей информационной системы от социоинженерных атак, учитывающей результаты агрегации сведений из социальных сетей и других источников, для оценки параметров моделей указанных пользователей и связей между ними, имеющая существенное значение для развития подходов к обеспечению внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и к оценке защищенности информации и информационной безопасности объекта, рекомендации по применению результатов работы в индустрии и в научных исследованиях и перспективы дальнейшей разработки тематики, связанные с построением оценок защищённости пользователей информационных систем на основании информации, извлекаемой из их аккаунтов в социальных сетях.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ

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

теория построена на известных методах и принципах, проверенных данных с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области информационной безопасности и защиты пользователей от социоинженерных атак;

использованы полученные характеристики времени работы для сравнения с результатами, достижимыми при выполнении анализа операторов вручную;

установлено качественное и количественное соответствие результатов решения задачи повышения оперативности обнаружения угроз социоинженерных атак за счёт автоматизации экспресс-оценки защищённости/поражаемости пользователей информационной системы от социоинженерных атак, учитывающей результаты агрегации сведений из социальных сетей и других источников, для оценки параметров моделей указанных пользователей и связей между ними.

использованы современные методики сбора и обработки исходной информации из социальных сетей, представительные выборочные совокупности с обоснованием подбора объектов (единиц) наблюдения и измерения и т.п.)

Личный вклад соискателя состоит в:

- изучении современного состояния науки в области анализа защищённости информационных систем, в частности от социоинженерных атак;
- исследовании существующих подходов и методов защиты пользователей информационных систем от социоинженерных задач, а также классифицировании угроз информационной безопасности;
- постановке задачи разработки и учёта в оценках защищённости модели злоумышленника и профиля компетенций злоумышленника;
- разработке подхода к оценке защищённости пользователя с использованием усовершенствованных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник»;

- построении метода и вероятностной модели оценки защищённости пользователя, опирающиеся на профиль компетенций злоумышленника и профиль уязвимостей пользователей;
- разработке вероятностной модели и опирающихся на неё методов оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети;
- построении алгоритмов автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте;
- автоматизации оценки выраженности ряда особенностей пользователей на основании данных, содержащихся в контенте, публикуемом пользователями социальных сетей;
- восстановлении фрагмента мета-профиля пользователя информационной системы (а именно, родного города, города проживания, года рождения), построенных на основе агрегации доступных сведений;
- разработке архитектуры прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем;
- реализации прототипа комплекса программ для оценки защищённости/поражаемости пользователей информационных систем;
- подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что Абрамов М.В. в своей диссертационной работе решил научную задачу оперативного 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, имеющую важное социально-экономическое и хозяйственное значение. Диссертационная работа соответствует требованиям (в том числе п. 9, абз. 2) действующей редакции Положения о присуждения учёных степеней, утверждённого постановлением Правительства РФ № 842 от 24.09.2013.

На заседании 07.06.2018 г. диссертационный совет принял решение присудить М.В. Абрамову ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 23 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 22, против нет, недействительных бюллетеней 1.

Председатель ди
доктор техничес
член-корреспонд Юсупов Рафаэль Мидхатович

Ученый секрета
кандидат технич Зайцева Александра Алексеевна
07.06.2018 г.