УТВЕРЖДАЮ
ВрИО директора СПИИРАН

ОНЖИН

УТВЕРЖДАЮ
ГУ
В

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного образовательного учреждения высшего образования
«Санкт-Петербургский государственный университет»

Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН)

Диссертация «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» выполнена на кафедре информатики Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет» и в лаборатории теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН).

В период подготовки диссертации соискатель Максим Викторович Абрамов проходил обучение в аспирантуре Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет».

В 2013 году М.В. Абрамов закончил Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет», математико-механический факультет по специальности «Прикладная информатика в сфере международных отношений».

Удостоверение о сдаче кандидатских экзаменов №19/209 выдано 26 декабря 2018 года Федеральным государственным бюджетным

учреждением науки «Санкт-Петербургский институт информатики и автоматизации российской академии наук».

Научный руководитель – Тулупьев Александр Львович, доктор физико-математических наук, доцент, профессор кафедры информатики Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет», заведующий лабораторией теоретических и междисциплинарных проблем информатики Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

По итогам обсуждения принято следующее заключение

Актуальность работы

Возросшая сложность компьютерных сетей и механизмов защиты, увеличение числа уязвимостей пользователей, а также возможностей по реализации социоинженерных атак обуславливает необходимость разработки 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, определению критичных сетевых ресурсов и выбору адекватной угрозам политики безопасности, которая задействует наиболее подходящие в заданных условиях защитные механизмы.

Таким образом, актуальной является проблема формирования моделей, методов и алгоритмов автоматизированного анализа защищенности критичной информации и пользователей информационных систем от социоинженерных атак. Развитие указанных моделей, методов и алгоритмов будет способствовать построению оценки уровня защищённости системы от социоинженерных атак, а также созданию комплекса программ, который будут агрегировать широкий круг факторов в мониторинге уровня защищенности информационных систем. Вместе с тем 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. Также 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, которые будут способствовать повышению степени защищённости системы.

Цель диссертационной работы

Цель диссертационной работы заключается в формировании методики оценки защищённости пользователей информационной системы от социоинженерных атак, основанной на развитии существующего подхода, учитывающего профиль уязвимостей пользователя, за счёт 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 дополнения комплекса «критичные документы — информационная система — пользователь» моделью злоумышленника.

Теоретическая и практическая значимость результатов

Разработанные модели, методы, алгоритмы и реализация создают основу для оценок защищённости 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 ставить задачу бэктрекинга атак в одной из удачных для поиска решений форм.

Результаты, представленные в диссертации, дают инструмент для 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. 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 программно-технических уязвимостей.

Научная новизна работы

1. Представлена модель оценки вероятности успеха многоходовой социоинженерной атаки на одного пользователя через другого. 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.
2. Предложены модели комплекса «критичные документы — информационная система — пользователь — злоумышленник». Комплекс является развитием существующего подхода к анализу защищенности пользователей информационных систем от социоинженерных атак злоумышленника, основанном на учёте профиля уязвимостей пользователя, за счёт дополнения существующего комплекса «критичные документы — информационная система — пользователь» моделью злоумышленника.
3. Разработана модель оценки вероятности успеха социоинженерной атаки злоумышленника на пользователя, объединяющая профиль уязвимостей пользователя, а также профиль компетенций злоумышленника. Модели, разработанные ранее, использовали только профиль уязвимостей пользователя. Разработанная модель выражена в построении зависимости от соответствующих параметров киберсоциальной системы.
4. Впервые разработаны методы, модели, алгоритмы и реализация автоматизированного поиска аккаунтов сотрудников компании в социальной сети ВКонтакте. Алгоритм основан на методах машинного обучения. Обучающая выборка составлялась из пользователей, которые указали в графе карьера место работы.
5. Разработана методика 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. Впервые представлена автоматизация решения этой задачи, которая основана на методах машинного обучения.
6. Разработаны методы, позволяющие дополнить мета-профиль 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.

7. Разработан прототип комплекса программ, реализующий заявленные модели и алгоритмы.

Степень достоверности и новизна результатов проведенных исследований

Обоснованность и достоверность представленных в диссертационной работе научных положений обеспечивается за счет глубокого анализа исследований по тематике информационной безопасности и социоинженерных атак, согласованности полученных результатов, успешной апробацией основных результатов на международных и российских научных конференциях, внедрениями этих результатов, а также публикацией основных положений, раскрывающих данные результаты, в ведущих научных изданиях.

Результаты работы докладывались на 29 научных мероприятиях как в России, так и за рубежом:

1. International Conference of Young Scientists Automation & Control, St.-Petersburg, 2013.
2. Научная сессия НИЯУ МИФИ-2014, г. Москва, 2014 г.
3. Всероссийская научная конференция по проблемам информатики (СПИСОК–2014), г. Санкт-Петербург, 2014 г.
4. XVII Международная конференция по мягким вычислениям и измерениям (SCM–2014), г. Санкт-Петербург, 2014 г.
5. IV международная социологическая конференция «Продолжая Грушина», г. Москва, 27–28 февраля 2014 г.
6. Шестая всероссийская научно-практическая конференция «Нечёткие системы и мягкие вычисления» (НСМВ–2014), г. Санкт-Петербург, 27–29 июня, 2014 г.
7. XXIII Всероссийские чтения студентов, аспирантов и молодых учёных с международным участием, г. Тула, 2014 г.
8. Третья Международная научно-практическая конференция «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-14), г. Москва, 2014 г.
9. XIV Санкт-Петербургская международная конференция «Региональная Информатика» (РИ-2014), г. Санкт-Петербург, 2014 г.
10. XVII Всероссийской объединенной конференции «Интернет и современное общество», г. Санкт-Петербург, 2014 г.
11. Conference on Electronic Governance and Open Society: Challenges in Eurasia (EGOSE–2014), St.-Petersburg, 2014.
12. Научная сессия НИЯУ МИФИ-2015, г. Москва, 2015 г.
13. V социологическая Грушинская конференция «Большая социология: расширение пространства данных», г. Москва, 12–13 марта 2015.

14. XVIII Международная конференция по мягким вычислениям и измерениям (SCM–2015), г. Санкт-Петербург, 2015 г.
15. IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015), г. Санкт-Петербург, 28–30 октября 2015 г.
16. Четвёртая Международная научно-практическая конференция «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-15), г. Москва, 2015 г.
17. Конференция Российской академии образования и МГУ им. М.В. Ломоносова «Цифровое детство», г. Москва, 2015 г.
18. Всероссийская научная конференция по проблемам информатики (СПИСОК–2016), г. Санкт-Петербург, 2016 г.
19. First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures, Moscow, 2016.
20. First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16), Sochi, 2016.
21. XIX Международная конференция по мягким вычислениям и измерениям (SCM–2016), г. Санкт-Петербург, 2016 г.
22. Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (г. Смоленск, 3-7 октября 2016 г.)
23. Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». (Санкт-Петербург, 26-28 октября 2016 г.)
24. XX Международная конференция по мягким вычислениям и измерениям (SCM–2017), г. Санкт-Петербург, 2017 г.
25. 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.)
26. VII всероссийская научно-практическая конференция «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ–2017 (г. Санкт-Петербург, 3–7 июля, 2017 г.)
27. Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17), Varna (Bulgaria), 2017.
28. Первая Всероссийская научно-практическая конференция «Нечёткие системы и мягкие вычисления. Промышленные применения». Ульяновск, 2017.
29. X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2017). Санкт-Петербург, 1–3 ноября 2017 г.

Личное участие соискателя в получении результатов, изложенных в диссертации

Все представленные в диссертации результаты получены автором лично. В программах для ЭВМ реализация алгоритмов, воплощающая результаты диссертации, выполнена соискателем.

Полнота изложения материалов диссертации в работах, опубликованных соискателем

В опубликованных соискателем работах полно и ясно изложены все результаты диссертационного исследования; выполнены требования к публикациям основных научных результатов диссертации, предусмотренные пунктами 11 и 13; соблюдены требования, установленные пунктом 14 «Положения о присуждении ученых степеней».

Публикации автора по теме диссертации

В монографиях

1. 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.

2. Тулупьев А.Л., Тулупьева Т.В., Суворова А.В., Абрамов М.В., Золотин А.А., Зотов М.А., Азаров А.А., Мальчевская Е.А., Левенец Д.Г., Торопова А.В., Харитонов Н.А., Бирилло А.И., Сольницев Р.И., Микони С.В., Орлов С.П., Толстов А.В. Мягкие вычисления и измерения. Модели и методы: монография. Том III / под ред. д.т.н., проф. С.В. Прокопчиной. – М.: ИД «Научная библиотека», 2017. – 300 с.

Статьи 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

3. Абрамов М.В., Азаров А.А. Анализ распространения имитированной социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей // Информатизация и связь. 2015. Вып. 2. С. 69–76.

4. Азаров А.А., Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Анализ защищенности групп пользователей информационной системы от социоинженерных атак: принципы и программная реализация // Компьютерные инструменты в образовании. 2015. № 4. С. 52–60.

5. Азаров А.А., Абрамов М.В., Тулупьева Т.В., Фильченков А.А. Применение вероятностно-реляционных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» для анализа защищенности пользователей информационных систем от социо-инженерных атак // Нечеткие системы и мягкие вычисления. 2015. Т. 10, № 2. С. 209–221.

6. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа

защищённости персонала информационных систем от социоинженерных атак //Информационно-управляющие системы. 2016. №4. С. 77–84.

7. Абрамов М.В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак // Автоматизация процессов управления. – 2018. – №1. С. .

В изданиях, индексируемых в реферативных базах Scopus и Web Of Science

8. Filchenkov A., Azarov A., Abramov M. What is more predictable in social media: Election outcome or protest action? // Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia. 2014. P. 157-161.

9. Azarov A.A., Abramov M.V., Tulupyeva T.V., Tulupyev A.L. Users' of Information System Protection Analysis from Malefactor's Social Engeneering Attacks Taking into Account Malefactor's Competence Profile // Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. 2016. P. 25–30.

10. Tulupyeva T.V., Tulupyev A.L., Abramov M.V., Azarov A.A., Bordovskaya N.V. Character Reasoning of the Social Network Users on the Basis of the Content Contained on Their Personal Pages // Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. 2016. P. 31–38.

11. Azarov A.A., Abramov M.V., Tulupyev A.L., Tulupyeva T.V. Models and algorithms for the information system's users' protection level probabilistic estimation //Advances in Intelligent Systems and Computing. Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16). Vol. 2. 2016. P.39–46.

12. Abramov M. V., Azarov A. A. Social engineering attack modeling with the use of Bayesian networks //Soft Computing and Measurements (SCM), 2016 XIX IEEE International Conference on. – IEEE, 2016. – С. 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., Shindarev N.A., Abramov M.V., Tulupyeva T.V. Approaches to development of models for text analysis of information in social network profiles in order to evaluate user's vulnerabilities profile //Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on. – IEEE, 2017. – P. 93–95.

15. Shindarev N., Bagretsov G., Abramov M., Tulupyeva T., Suvorova A. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities //Advances in Intelligent Systems and Computing. Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17). Vol. 1. 2017. P.441–447

В сборниках трудов конференций

16. Тулупьев А.Л., Абрамов М.В., Азаров А.А., Тулупьева Т.В. Защита конфиденциальных данных на интернет-портале редакции электронного научного журнала // Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 23–25 октября 2013 г.): Материалы конференции. СПб.: СПОИСУ, 2013. С. 228–229.

17. Абрамов М.В. Защита конфиденциальной информации на интернет-портале редакции электронного научного журнала // Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 23–25 октября 2013 г.): Материалы конференции. СПб.: СПОИСУ, 2013. С. 76.

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

19. Абрамов М.В., Азаров А.А., Тулупьев А.Л., Фильченков А.А. Применение моделей распространения информации в социальных сетях к задачам анализа защищённости пользователей информационных систем от социо-инженерных атак // Нечёткие системы и мягкие вычисления (НСМВ-2014): труды Шестой всероссийской научно-практической конференции. (г. Санкт-Петербург, 27-29 июня, 2014 г.). — в 2 т. Том 2. — СПб.: Политехника-сервис, 2014. 55-58 с.

20. Азаров А.А., Фильченков А.А., Абрамов М.В. Анализ распространения вредоносного контента среди пользователей социальных медиа. // СПИСОК-2014: Материалы всероссийской научной конференции по проблемам информатики (23–25 апреля 2014 Санкт-Петербург). СПб: ВВМ, 2014. С. 540–546.

21. Абрамов М.В., Азаров А.А., Тулупьев А.Л., Фильченков А.А. Модели распространения информации в социальных медиа // Материалы Третьей Международной научно-практической конференции «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-14). Москва. 2014. с. 112-115.

22. Абрамов М.В., Азаров А.А. Концепция анализа распространения контента в социальных медиа на основании методов анализа защищенности пользователей информационных систем от социо-инженерных атак // Материалы XIV Санкт-Петербургской международной конференции Региональная Информатика «РИ-2014». Санкт-Петербург. 2014 с. 543.

23. Абрамов М.В., Тулупьев А.Л., Азаров А.А., Фильченков А.А. Модели распространения информационных сообщений в социальных сетях // Научная сессия НИЯУ МИФИ-2015. Аннотации докладов. В 3 т. Т. 3. Интеллектуальные системы и технологии. М.: НИЯУ МИФИ. Москва. 2015. С. 137.

24. Азаров А.А., Абрамов М.В., Тулупьева Т.В. Применение алгоритма обхода в ширину графа межличностных связей для анализа защищенности пользователей информационных систем // Интегрированные модели и мягкие вычисления в искусственном интеллекте. Сборник научных трудов VIII-ой Международной научно-технической конференции (Коломна, 18-20 мая 2015 г.). в 2-х томах. Т2. –М.: Физматлит. 2015. С 774-779

25. Абрамов М.В., Азаров А.А., Фильченков А.А. Распространение социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2015). Санкт-Петербург. Том 1-2. 2015. 329-332 с.

26. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Комплекс «критические документы — информационная система — персонал — злоумышленник» // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 28–30 октября 2015 г.): Материалы конференции. СПб: СПОИСУ, 2015. С. 326–327

27. Абрамов М.В. Комплекс программ для анализа достижимости критических документов и защищённости пользователей информационных систем // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 28–30 октября 2015 г.): Материалы конференции. СПб: СПОИСУ, 2015. С. 326

28. Азаров А.А., Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В. Прототип комплекса программ для анализа защищённости пользователей информационных систем, построенный на основе алгоритмов обхода графов социальных связей пользователей // Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2015. С. 554–557.

29. Абрамов М.В. Применение социальных сетей для анализа защищённости пользователей компании от социоинженерных атак // Материалы Четвёртой Международной научно-практической конференции «Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты» (ISC-15). Москва. 2015. с. 294-297.

30. Абрамов М.В., Азаров А.А. Моделирование социоинженерных атак с использованием байесовских сетей доверия // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2016). Санкт-Петербург. Том 1-2. Т. 1. 2016. С. 71–74.

31. Абрамов М.В. Реляционная модель расчёта вероятностной оценки уровня защищённости пользователя от социоинженерных атак. // Пятнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (г. Смоленск, 3-7 октября 2016 г.): Труды конференции. Т. 1. Смоленск: Универсум, 2016. С. 203–211.

32. Абрамов М.В. Подход к оценке защищённости пользователей информационных систем от социоинженерных атак // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». (Санкт-Петербург, 26-28 октября 2016 г.): Материалы конференции. СПб: СПОИСУ, 2016. С. 514.

33. Шиндарев Н.А., Абрамов М.В. Построение вероятностной графической модели для оценки успешности социоинженерной атаки // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». (Санкт-Петербург, 26-28 октября 2016 г.): Материалы конференции. СПб: СПОИСУ, 2016. С. 522-523.

34. Абдурахманова К.Ф., Абрамов М.В., Азаров А.А., Тулупьев А.Л., Тулупьева Т.В. Программная реализация имитации социоинженерных атак с помощью марковских полей // Материалы 6-й всероссийской научной конференции по проблемам информатики СПИСОК-2016. (26–29 апреля 2016 г. Санкт-Петербург). СПб.: ВВМ, 2016. С. 427–435.

35. Абрамов М.В. Подход к оценке вероятности успешности социоинженерной атаки // Материалы 6-й всероссийской научной конференции по проблемам информатики СПИСОК-2016. (26–29 апреля 2016 г. Санкт-Петербург). СПб.: ВВМ, 2016. С. 436–442.

36. Абрамов М.В., Азаров А.А. Выявление психологических особенностей пользователей социальных сетей на основании музыкальных предпочтений. // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2017). Санкт-Петербург. Том 1-2. Т. 1. 2017. С. 130–133.

37. Багрецов Г.И., Шиндарев Н.А., Абрамов М.В., Тулупьева Т.В. Подходы к разработке моделей для анализа текстовой информации в профилях социальной сети в целях построения профиля уязвимостей пользователя. // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2017). Санкт-Петербург. Том 1-2. Т. 1. 2017. С. 134–137.

38. Абрамов М.В. Оценка вероятности успеха социоинженерного атакующего воздействия // 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 (Санкт-Петербург, 30 июня – 3 июля 2017 г.). — СПб.: Политехника-сервис, 2017. С. 9–14

39. Багрецов Г.И., Шиндарев Н.А., Абрамов М.В., Тулупьева Т.В. Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети. // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ–2017 (г.

Санкт-Петербург, 3–7 июля, 2017 г.). — в 2 т. Т. 1. — СПб.: Политехника-сервис, 2017. С. 9–16

40. Бушмелёв Ф.В., Абрамов М.В. Обзор программного инструментария для визуализации сетей в микромире корпоративных офисов // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ–2017 (г. Санкт-Петербург, 3–7 июля, 2017 г.). — в 2 т. Т. 2. — СПб.: Политехника-сервис, 2017. С. 34–42

41. Сулейманов А.А., Абрамов М.В. Подход к построению и анализу социального графа сотрудников некоторой компании. // Сборник научных трудов Первой Всероссийской научно-практической конференции «Нечёткие системы и мягкие вычисления. Промышленные применения». (г. Ульяновск, 14-15 ноября, 2017 г.). – Ульяновск, УлГТУ, 2017. С. 389-393

42. Слёзкин Н.Е., Абрамов М.В., Тулупьева Т.В. Подход к восстановлению мета-профиля пользователя информационной системы на основании данных из социальных сетей. // // Сборник научных трудов Первой Всероссийской научно-практической конференции «Нечёткие системы и мягкие вычисления. Промышленные применения». (г. Ульяновск, 14-15 ноября, 2017 г.). – Ульяновск, УлГТУ, 2017. С. 394-399.

43. Абрамов М.В. Подход к построению системы упреждающей диагностики уязвимостей персонала к социоинженерным атакам. // Информационная безопасность регионов России (ИБРР-2017). X Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 1–3 ноября 2017 г.): Материалы конференции. СПб: СПОИСУ, 2017. С. 409–410.

44. Бушмелёв Ф.В., Абрамов М.В. Подход к построению профиля компетенций злоумышленника в задаче анализа защищённости информационной системы от социоинженерных атак. // Информационная безопасность регионов России (ИБРР-2017). X Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 1–3 ноября 2017 г.): Материалы конференции. СПб: СПОИСУ, 2017. С. 413–414.

Свидетельства о регистрации программ для ЭВМ

45. Абрамов М.В., Азаров А.А., Бродовская Е.В., Фильченков А.А. Браузерный классификатор на основе вхождения ключевых слов для базы данных документов, выгруженных посредством сервиса IQBuzz в формате .xls // Свидетельство о государственной регистрации программы для ЭВМ №2014618173 от 12.08.2014. Роспатент.

46. Абрамов М.В., Азаров А.А., Фильченков А.А. Программа оценки силы социальных связей на основе данных социальной сети «ВКонтакте» // Свидетельство о государственной регистрации программы для ЭВМ №2017610561 от 12.01.2017. Роспатент.

47. Багрецов Г.И., Абрамов М.В., Азаров А.А., Тулупьев А.Л. VK Data Parser for Social Engineering Attacks Modeling Version 01 (VK Data Parser for SEA Modeling v.01) // Свидетельство о государственной регистрации программы для ЭВМ №2017616876 от 19.06.2017. Роспатент.

48. Шиндарев Н.А., Тулупьев А.Л., Абрамов М.В., Азаров А.А.Training Affiliate Data Parser for Social Engineering Attacks Modeling Version 01 (TADP For SEA Modeling v.01) // Свидетельство о государственной регистрации программы для ЭВМ №2017618730 от 08.08.2017. Роспатент.

В монографии [1] М.В. Абрамову принадлежат результаты, связанные с моделью злоумышленника, формализацией его профиля компетенций, модель оценки вероятности социоинженерной атаки злоумышленника на пользователя с учётом профиля уязвимостей пользователя и профиля компетенций злоумышленника, а также обзор предметной области, в котором обозначены место и роль исследований в области социальной инженерии.

В монографии [2] М.В. Абрамову принадлежат результаты, связанные с анализом защищённости пользователей информационных систем от социоинженерных атак.

Личный вклад Абрамова М.В. в ключевые публикации с соавторами характеризуется следующим образом. В статьях, опубликованных в журналах из перечня российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук, результаты распределяются следующим образом. В [3] М.В. Абрамову принадлежит анализ алгоритмов обхода социального графа сотрудников компании, в [4] модель оценки защищённости пользователей информационной системы от социоинженерных атак злоумышленника, в [5] вероятностно-реляционные модели пользователя и злоумышленника, в [6] — модель профиля компетенций злоумышленника и оценки вероятности социоинженерной атаки злоумышленника.

В других публикация М.В. Абрамову принадлежат следующие результаты: в [9] ему принадлежит модель информационной системы, отвечающей требованиям информационной безопасности; в [10] — подходы к обработке информации, извлекаемой из социальных сетей; в [11], [12] — модели оценки защищённости пользователей информационных систем от социоинженерных атак, а также модели злоумышленника и пользователя информационной системы; в [13], [14] — подход к автоматизированной оценке некоторых особенностей личности на основании их музыкальных предпочтений, информация о которых извлекается из социальной сети; в [15] — подходы к автоматизированному поиску аккаунтов сотрудников компании в социальной сети ВКонтакте. формальное представление злоумышленника, включающее в себя его профиль компетенций; в [18], [19] — модель критичных документов и представление вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя; в [20], [21], [22], [23], [26] — подход к моделированию распространения информации в социальных медиа на основании различных критериев; в [24], [25] — улучшенный

алгоритм обхода графа межличностных связей пользователя; в [27], [28] — представление программного продукта, предназначенного для анализа защищённости пользователей информационных систем и критичных документов от социоинженерных атак; в [30] — вероятностно-реляционная модель комплекса «критичные документы – информационная система – пользователь – злоумышленник».

Ценность научных работ соискателя, с точки зрения методов и систем защиты информации, состоит в завершении построения модели оценки вероятности успеха многоходовой социоинженерной атаки и оценки успеха социоинженерной атаки злоумышленника на пользователя с учётом профилей уязвимостей пользователя и компетенций злоумышленника. Также были предложены модели комплекса «критичные документы – информационная система – пользователь – злоумышленник». С прикладной точки зрения, ценность научных работ состоит в формировании комплекса программ, реализующих разработанные методы, модели и алгоритмы автоматизированного поиска сотрудников компании в социальных сетях, подходы к оценке некоторых особенностей личности на основании контента (текстового и аудио), публикуемого ими в социальных сетях, а также методов восстановления мета-профиля пользователя информационных систем.

Соответствие специальности

Содержание диссертационного исследования М.В. Абрамов отвечает формуле научной специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность». Кроме того, полученные результаты соответствуют следующим пунктам: «9. Модели и методы оценки защищенности информации и информационной безопасности объекта», «13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности», «14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» паспорта специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность».

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

Проект заключения принят на заседании экспертной группы, сформированной решением декана математико-механического факультета СПбГУ от 09.02.2018 № 79-22-18 в составе 5 человек, протокол №1 от «15» февраля 2018 года.

Присутствовало на заседании экспертной группы 5 чел. Результаты голосования: «за» — 5 чел., «против» — 0 чел., «воздержалось» — 0 чел.

Проект заключения принят на заседании расширенного семинара лаборатории информационно-вычислительных систем и технологий программирования и лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН.

Присутствовало на заседании расширенного семинара 22 чел. Результаты голосования: «за» — 22 чел., «против» — 0 чел., «воздержалось» — 0 чел., протокол № 1 от «09» февраля 2018 г.

(подпись председателя расширенного семинара, СПИИРАН)

(Василий Юрьевич Осипов, доктор технических наук, профессор, заведующий лабораторией информационно-вычислительных систем и технологий программирования СПИИРАН)

«12» февраля 2018 г.

(подпись председателя экспертной группы, СПбГУ)

(Андрей Николаевич Терехов, доктор физико-математических наук, профессор, заведующий кафедрой системного программирования СПбГУ)

«15» февраля 2018 г.