Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

Заместителя начальника 3 управления – начальника 31 отдела военного института (научно-исследовательского) Военно-космической академии имени А.Ф.Можайского, доктора технических наук **Овчарова Владимира Александровича**

на диссертационную работу АБРАМОВА Максима Викторовича
«Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей»,

представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Динамичное развитие автоматизированных информационных систем, состоящих из большого числа компонентов различной степени автономности, в разноплановой программно-аппаратной конфигурации, связанных между собой различными по используемым технологиям и скорости передачи каналами связи и обменивающихся данными различных типов, определяет их влияние на организационные, экономические, политические и иные процессы. Информатизация общества существенно повышает актуальность вопросов информационной безопасности (ИБ). Несмотря на это, информационные системы стали более уязвимы к кибератакам, что связано с существенным ростом их частоты и сложности. Вместе с ростом количества киберпреступлений значительно увеличились и убытки от них, например, время, затрачиваемое на расследования подобных инцидентов, а также затраты на устранение последствий. При этом, вместе с ростом общего количества инцидентов ИБ, увеличивается доля социоинженерных атак. Актуальность исследований в области социоинженерных атак и разработки систем защиты от воздействий такого рода также подчёркивается крупными инцидентами, которые регулярно освещаются в бюллетенях по безопасности, в отчетах профильных изданий и средствах массовой информации.

В диссертационной работе М.В. Абрамова исследуется одна из **актуальных** проблем указанного направления – повышение 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. Иными словами, рассматриваются новые подходы к оценке параметров моделей за счёт автоматизации агрегации сведений из социальных сетей. Актуальность такой оценки подчёркивается широкой распространённостью социальных сетей, большим числом их пользователей в различных странах мира, доступностью информации для злоумышленника, приемлемой достоверностью такой информации, что особо отмечается в научных публикациях. Кроме того, актуальность диссертационного исследования подтверждается представлением его результатов на научных конференциях и получаемой грантовой поддержкой.

Таким образом, диссертационная работа Абрамова М.В., посвященная разработке методов и алгоритмов анализа защищённости пользователей информационных систем от социоинженерных атак на основе оценки параметров моделей выполнена на актуальную тему и представляет большой практический интерес.

Изложение результатов, полученных М.В. Абрамовым, предваряется анализом проблемы защиты пользователей информационных систем от социоинженерных атак. Обозначены важные роль и место проблемы защиты пользователей информационных систем от атак, проводимых с использованием методов социальной инженерии. Представлен подход к оценке информации в интересах рефлексивного управления, подход к анализу защищённости компьютерных сетей от программно-технических атак, основанный на анализе деревьев атак, а также его оптимизация в целях поддержки экспресс-диагностики. Основные теоретические результаты соискателя приводятся в третьей главе, где представлены измеряемые показатели, соотнесённые с регламентирующими документами. Сформулированы общие алгебраические модели, отмечается, что модели критичных документов и хостов информационной системы подробно рассматриваются в задачах защиты информации от программно-технических атак.

В ходе решения актуальной научной задачи автором получены следующие **новые научные результаты:**

1) усовершенствованные модели комплекса «критичные документы – информационная система – пользователь – злоумышленник», которые используются для оценки защищённости пользователей; следует отметить, что в более ранних подходах при оценке защищённости пользователей информационной системы не рассматривалась модель злоумышленника, при этом, разработанные автором методы и модели оценки защищённости опираются не только на профиль уязвимостей пользователей, но и на профиль компетенций злоумышленника;

2) модель оценки вероятности и опирающиеся на неё методы оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети, что отличает их от предложенных ранее, где эти оценки задавались экспертом вручную;

3) алгоритм идентификации аккаунтов сотрудников компании в социальной сети ВКонтакте, алгоритм автоматизированной оценки выраженности особенностей пользователей на основании данных, содержащихся в контенте, публикуемом в социальных сетях, алгоритм восстановления фрагмента мета-профиля пользователя информационной системы (а именно, родной город, город проживания, год рождения), построенные на основе агрегации доступных сведений.

Первый научный результат посвящен формализации и усовершенствованию моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» и построению на их основе вероятностных моделей оценки успеха социоинженерной атаки злоумышленника на пользователя, учитывающих различные конфигурации и ограничения. Предложена вероятностная модель оценки поражаемости критичных документов при социоинженерной атаке, метод оценки, учитывающий ограниченность ресурсов у злоумышленника.

Вторым научным результатом является вероятностная модель оценки и опирающиеся на неё методы оценки успеха многоходовой социоинженерной атаки, учитывающие результаты агрегации данных, извлекаемых из аккаунтов пользователей в социальной сети. Модель является адаптацией модели Белла–Тревино, где в качестве количества эпизодов используются факты интенсивности взаимодействия сотрудников компании в социальной сети.

В качестве третьего научного результата в диссертации представлены алгоритмы автоматизированного поиска и идентификации аккаунтов сотрудников компании в социальной сети ВКонтакте, автоматизированной оценки степени выраженности ряда особенностей пользователей на основании данных, содержащихся в контенте, публикуемом в социальных сетях, восстановления фрагмента мета-профиля пользователя информационной системы (а именно, родной город, город проживания, год рождения), построенные на основе агрегации доступных сведений. Следует отметить, что перечисленные выше алгоритмы и их реализация приведены впервые. На основании данных алгоритмов автором построена архитектура прототипа комплекса программ и их программная реализация.

Перечисленные научные результаты определяют вклад в теорию вероятностей и математическую статистику, теорию идентификации и системного анализа, тем самым, являются вкладом в науку. В совокупности новизна указанных результатов состоит в предложении методов анализа защищённости пользователей информационных систем от социоинженерных атак, основанных на агрегации сведений, извлекаемых из социальных сетей.

Достоверность и обоснованность полученных научных **результатов, положений, выводов** и предлагаемых **рекомендаций** обеспечивается корректностью и последовательностью использования апробированного математического аппарата, логической непротиворечивостью рассуждений, соответствием результатов теоретических исследований и данных, полученных в ходе экспериментальных исследований. Предложенные методы были реализованы в прототипе комплекса программ с последующим проведением экспериментов, результаты которых не противоречат закономерностям, известным специалистам в соответствующих областях знаний.

Теоретическая значимость диссертационной работы состоит в предложении вероятностных методов для анализа защищённости пользователей информационных систем от социоинженерных атак.

Практическая ценность выполненной диссертационной работы заключается в разработке моделей, алгоритмов и комплекса программ, которые позволяют автоматизировать оценку защищённости пользователей информационных систем от социоинженерных атак.

Предложенные в диссертации методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак в точности отвечают следующим составляющим **паспорту специальности** 05.13.19: «Методы и системы защиты информации, информационная безопасность»: «9. Модели и методы оценки защищенности информации и информационной безопасности объекта» (результаты 1 – 2), «13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (результаты 3 – 4), «14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» (результаты 3 – 4).

К несомненным **достоинствам** следует отнести широкое освещение результатов диссертационного исследования: соискатель опубликовал лично или в соавторстве 48 научных работ, из них – 2 монографии, 7 публикаций в изданиях, индексируемых Scopus/WoS, 6 статей в изданиях из «Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук», 40 докладов и тезисов на научных конференциях (из которых 9 единоличных), получены 7 свидетельств о регистрации программ для ЭВМ (РОСПАТЕНТ).

Работа хорошо оформлена, написана грамотно, на высоком научном уровне, а также обладает композиционным единством. Текст диссертационной работы изложен систематично и последовательно; в оглавлении отразилась логическая структура работы, обусловленная поставленной целью и задачами, сформулированными для ее достижения. Кроме того, работа содержит развитый ссылочный и библиографический аппарат; все прямые и косвенные цитаты, а также теоретические положения снабжены надлежащими ссылками на источники. **Автореферат** в полной мере отражает содержание диссертации. Все результаты, выносимые на защиту, **опубликованы**, в том числе основные результаты – в журналах 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», а также в изданиях, представленных на платформах цитирования WoS/SCOPUS.

Вместе с тем, при анализе работы были выявлены следующие недостатки.

1) В работе не уделено должного внимания обоснованию целесообразных мероприятий по защите пользователей информационных систем от социоинженерных атак.

2) В диссертационной работе важность документа автором предлагается оценивать через уровень его критичности, который, в конечном счёте, выражается в денежном эквиваленте. Однако, оценка такой степени может быть дана и с использованием градаций из Лайкерт-шкал, иначе говоря, для представления степени критичности можно использовать аппарат лингвистических переменных, свойственный для нечеткостного подхода. Следует отметить, что в диссертации не проводится компаративный анализ этих двух подходов, который мог бы, по крайней мере, обозначить еще одно направление дальнейших исследований.

3) Автором не разъясняется, чем обусловлен выбор метрики для степеней выраженности «некоторых особенностей пользователей информационных систем».

4) Методика оценки точности (разброса) вычисляемых величин вероятности защищённости (поражаемости) основывается на методе Монте-Карло, что, разумеется, корректно, однако, не упомянуты основания для выбора такого подхода.

Также имеют место недостатки методического характера.

5) На рисунках 17–24 нет пояснений, что откладывается на осях приведённого графика, представляющего результаты стохастического моделирования с помощью метода Монте-Карло при разных вероятностных распределениях значений параметров.

6) На рисунке 29 в системе компонент комплекса программ для оценки защищённости пользователя информационной системы не разъяснены подписи около связей между модулями.

7) На скриншотах программ не унифицированы наименования полей блоков: они выполнены где-то на русском, где-то на английском языке.

8) Блок-схемы алгоритмов выполнены в разных стилях, например, на рисунках 7, 10 и на рисунке 12.

9) В архитектуре прототипа комплекса программ не указано, как распределяются классы по модулям.

10) На страницах 9 и 13 имеют место следующие стилистические и грамматические ошибки: «опирающаеся» вместо «опирающиеся», страница 79 – «социинженерная» вместо «социоинженерная», страница 131 – «дальнейшего» вместо «дальнейшего», «социоионженерных» вместо «социоинженерных».

Однако, указанные выше недостатки носят частный характер, не оказывают существенного влияния на общую положительную оценку работы, и не снижают достоверности и значимости итогов диссертационного исследования.

На основе изложенного выше заключаю:

1) В целом диссертация Абрамова Максима Викторовича представляет собой законченную научно-квалификационную работу, в которой содержится **новое решение научной задачи** повышения оперативности обнаружения угроз социоинженерных атак за счёт автоматизации экспресс-оценки защищённости/поражаемости пользователей информационной системы от социоинженерных атак, обоснован путь ее разрешения, сформулированы частные задачи исследований, получены новые научные результаты и выработаны рекомендации по их применению.

2) Диссертационная работа является единолично написанной научно-квалификационной работой, содержит совокупность положений, выносимых на защиту, и свидетельствует о личном существенном вкладе автора в развитие области информационной безопасности, связанной с анализом защищённости пользователей от социоинженерных атак.

3) Содержание автореферата отражает содержание диссертации и позволяет составить целостное представление о проделанной работе и основных результатах, полученных в ходе исследований. Материалы диссертации изложены достаточно грамотно, логически последовательно и представлены в лаконичной форме.

4) Диссертационная работа «Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей» **отвечает всем критериям**, указанным в действующем «Положении о присуждении ученых степеней», утвержденным Постановлением Правительства РФ № 842 от 24.09.2013 (ред. от 28.08.2017), предъявляемым в отношении кандидатских диссертаций (в т.ч. указанным в п. 9, абз. 2), 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.

Заместитель начальника 3 управления – начальник 31 отдела
военного института (научно-исследовательского) Во
космической академии имени А.Ф.Можайского,
доктор технических наук

В.А. Овчаров

«14» мая 2018 г.

Личную подпись руки Владимира Александровича Овчарова, д.т.н., заместителя начальника 3 управления – начальника 31 отдела военного института (научно-исследовательского) Военно-космической академии имени А.Ф. Можайского, ФГБВОУ ВО «Военно-космическая академия имени А.Ф. Можайского» Министерства обороны Российской Федерации удостоверяю

Начальник отдела кадров
Военно-космической академии имени А.Ф.Можайс

ков

«16» мая 2018 г.