Акционерное общество
«Лаборатория противодействия промышленному шпионажу»
(АО «Лаборатория ППШ»)

199178, Россия, Санкт-Петербург, наб.реки Смоленки, д.25, лит.Е, пом.31 т. (812) 702-7383; ф.: (812)309-4509
e-mail: lab@pps.ru http://www.pps.ru

«01» июня 2021 года № 164/21

Экз. 2

УТВЕРЖДАЮ
Генеральный директор

В.И. Ненашев

«1» 06 2021 г.

ОТЗЫВ

ведущей организации на диссертационную работу Витковой Лидии Андреевны на тему: «Модели, алгоритмы и методика противодействия вредоносной информации в социальных сетях», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

Среди проблем, которые находятся в центре современных исследований, отдельное внимание уделяется противодействию вредоносной информации в пространстве социальных сетей: специалисты характеризуют информационные сети, описывают их особенности, разрабатывают системы анализа и мониторинга данных, занимаются выделением из общей массы именно вредоносной информации, рассматривают каналы распространения и источники вредоносной информации. При этом практически все методы предусматривают блокирование конкретных постов с информацией нежелательного содержания без оценки их популярности у аудитории. Большинство современных исследователей и специалистов в области информационной безопасности сходятся в общем мнении, что выявление и блокировка наиболее активных источников вредоносной информации, видится более перспективным решением, значительно экономящим время и технические ресурсы. И в настоящее время по-прежнему существует необходимость в создании рабочей методики противодействия вредоносной информации, а также выработке рекомендаций, в том числе практического характера.

По этой причине актуальность темы диссертационных исследований не вызывает сомнений.

НОВИЗНА И ДОСТОВЕРНОСТЬ НАУЧНЫХ РЕЗУЛЬТАТОВ

Научные результаты, полученные в диссертационной работе:

1) комплекс моделей социальной сети, источника и вредоносной информации;

2) комплекс алгоритмов анализа источников вредоносной информации и ранжирования контрмер;

3) методика противодействия вредоносной информации в социальной сети;

4) архитектура и программные компоненты системы противодействия вредоносной информации.

Модели и алгоритмы анализа источников вредоносной информации в социальных сетях отличаются применением комплексного подхода к решению задачи противодействия вредоносной информацией с учетом признаков и свойств активности источника, страницы на которой опубликовано сообщение, аудитории сообщений.

Методика противодействия вредоносной информации в социальных сетях отличается использованием предложенного комплекса моделей социальной сети, источника, вредоносной информации и информационно-признаковой модели, а также предложенного комплекса алгоритмов анализа источников и ранжирования контрмер.

Архитектура и программная реализация системы противодействия вредоносной информации в социальных сетях отличаются использованием предложенной методики противодействия, введением оригинальных компонентов анализа и оценки источника, авторской базы данных контрмер и агентов реализации, обеспечивающей ранжирование и выбор доступных контрмер в системе для заданных типов вредоносной информации.

Отличительной особенностью разработанных автором предложений является строго аргументированное обоснование системотехнических решений, направленных на повышение информационной безопасности в социальных сетях. Достоверность полученных научных результатов подтверждается наличием двух свидетельств о регистрации программ для ЭВМ и одного свидетельства о регистрации базы данных.

ЗНАЧИМОСТЬ ВЫВОДОВ И РЕКОМЕНДАЦИЙ СОИСКАТЕЛЯ ДЛЯ НАУКИ И ПРАКТИКИ И ВОЗМОЖНЫЕ ПУТИ ИХ ИСПОЛЬЗОВАНИЯ

Практическая значимость результатов исследования состоит в том, что разработанные методика, модели и алгоритмы могут быть использованы при создании эффективной системы противодействия вредоносной информации, в которой используются алгоритмы ранжирования и сортировки объектов воздействия, что в конечном счете повышает обоснованность выбора целей для противодействия, тем самым оказывая положительное влияние на эффективность.

Теоретическая значимость диссертационной работы определяется ее вкладом в развитие теории и методов информационной безопасности, что проявляется в следующих аспектах: введены новые классы, объекты, их атрибуты и связи для анализа и оценки информационных объектов и информационного обмена в социальных сетях, расширены классы алгоритмов сортировки и ранжирования для анализа объектов в социальных сетях, введены классы контрмер, разработан набор критериев мер противодействия и предложены новые компоненты архитектуры системы противодействия и описаны функциональные связи между ними.

Личный вклад определяется в осуществлении самостоятельного научно-теоретического анализа исследуемой области знаний о информационной безопасности; в разработке и обосновании основных положений, которые вынесены соискателем на защиту.

Отраженные в диссертационной работе исследования проведены в рамках следующих НИР: грант российского научного фонда РНФ № 18-71-10094 «Мониторинг и противодействие вредоносному влиянию в информационном пространстве социальных сетей»; грант РНФ № 18-11-00302 «Интеллектуальная обработка цифрового сетевого контента для эффективного обнаружения и противодействия нежелательной, сомнительной и вредоносной информации». Полученные результаты внедрены в учебный процесс СПбГУТ им. проф. М.А. Бонч-Бруевича (учебный курс «Технологии обеспечения информационной безопасности больших данных») и СПбГУПТД (учебные курсы «Комплексная защита на предприятии», «Технологии и методы программирования»), применяются в рабочем процессе репутационного агентства «Glorystory» (компания ООО «Жасмин»). Результаты исследования представлены в заявках, победивших на следующих конкурсах: 1) Конкурс инноваций и инновационных проектов в номинации «А» «Конкурс концептуальных идей, методик, рекомендаций» 2016/2017 г. от Международной академии связи; 2) Конкурс субсидий

молодым ученым, молодым кандидатам наук вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, в 2018 г.

Полученные соискателем результаты целесообразно использовать в специальных службах органов внутренних дел, осуществляющих специальные технические мероприятия по противодействию вредоносной информации в социальных сетях, в том числе в УФСБ по Санкт-Петербургу и Ленинградской области, в Федеральной службе охраны Российской Федерации (ФСО России), в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Разработанные модели, алгоритмы, методики и архитектура системы противодействия могут быть использованы для повышения информационной безопасности в социальных сетях за счет обоснованного выбора объектов воздействия для мер противодействия. Потенциально перспективным направлением использования результатов исследования, полученных соискателем, может быть анализ источников вредоносных сообщений в социальных сетях, содержащих призывы к суициду детей и подростков. Эти же результаты возможно использовать на уровне администрации города и районов для поиска самых активных источников и каналов распространения информации о наркотиках через социальные сети.

СОДЕРЖАНИЕ И ОФОРМЛЕНИЕ ДИССЕРТАЦИИ

Диссертационная работа представлена в виде завершенной научно-квалификационной работы, которая включает в себя введение, три раздела, заключение, список источников литературы (162 наименования) и 6 приложений. Объем работы 173 станицы машинописного текста, в том числе 35 рисунков и 15 таблиц. Распределение материала по разделам последовательное и логичное, а стиль его изложения достаточно ясный и технически грамотный.

Автореферат в целом правильно отражает основные результаты диссертационной работы, которые опубликованы в 20 научных трудах, в том числе – 6 в рецензируемых изданиях из перечня ВАК, 8 – в изданиях, индексируемых в международных базах данных Scopus и Web of Science, также получено 2 свидетельства о государственной регистрации программ для ЭВМ и 1 свидетельство о государственной регистрации базы данных. Содержание публикаций соответствует научным положениям, выносимым автором на защиту.

Вместе с тем в диссертационной работе необходимо отметить наличие недостатков.

Во-первых, имеют место недостатки формального характера: отдельные рисунки (например, рисунок 2.12) плохо напечатаны или представлены в сжатой форме (их можно было бы вынести в приложение), присутствуют грамматические ошибки, опечатки.

Во-вторых, ключевое понятие «вредоносной информации» определено не достаточно нейтрально, смешано, а при попытке понять заложенный автором в это понятие смысл из текста возникает следующая ситуация: термин «вредоносная информации» используется и для рекламы, спама, и для обозначения призывов к террористической, экстремистской активности, а также для обозначения утечек конфиденциальной информации. Это обстоятельство существенно усложняет процесс оценки размера области исследования и сферы применения полученных результатов.

В-третьих, из текста третьего раздела вытекает, что автор использовал комплект программного обеспечения, разработанный им при экспериментальной оценке положений, выносимых на защиту. Приведенные в приложениях к работе свидетельства о регистрации программ для ЭВМ подтверждают, что архитектура разработана автором лично и совместно с разработанными алгоритмами обладает общностью. Однако в работе новизна самой программной реализации доказана неубедительно и нет сравнения программных прототипов с существующими аналогами, нет обоснования выбора языка Python для программной реализации и библиотеки Pandas.

В-четвертых, одной из самых важных проблем противодействия вредоносной информации является ее обнаружение в социальных сетях, в том числе семантический анализ текстов и сообщений, однако этот аспект в диссертации не раскрыт.

В-пятых, в диссертации диаграмма комплекса алгоритмов (рис 2.15) оформлена в соответствии со стандартом UML, а в автореферате схема комплекса алгоритмов (рис. 1) оформлена в соответствии с ГОСТ 19.701-90, в диссертации блок-схемы отдельных алгоритмов (рис. 2.10, рис. 2.11, рис. 2.12) и схема методики (3.2) выполнены с отклонением от ГОСТ 19.701-90.

Однако отмеченные недостатки имеют частный характер, принципиально не влияя на полученные в диссертационной работе научные результаты.

ВЫВОДЫ ПО РАБОТЕ

Диссертационная работа Витковой Л.А. является законченной научно-квалификационной работой, в которой решена актуальная задача исследования, заключающаяся в разработке модельно-методического аппарата для противодействия вредоносной информации в социальных сетях, и имеющая существенное значение для повышения информационной безопасности в информационной сфере государства. Диссертация характеризует автора как сформированного специалиста, способного самостоятельно исследовать широкий круг теоретических и практических вопросов, получать обоснованные выводы и рекомендации. Содержание диссертации соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность». В целом диссертационная работа Витковой Л.А. соответствует требованиям п.п. 9–14 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации №842 от 24 сентября 2013 года, предъявляемым к кандидатским диссертациям.

Диссертация и отзыв на неё обсуждены и одобрены на заседании комиссии подразделения аттестации объектов информатизации, протокол № 1 от 01 июня 2021 года.

Отзыв составили:

Кандидат технических наук, доцент,
заместитель генерального
директора по научной работе — Андрей Владимирович Лысов

Кандидат технических наук, доцент,
Начальник отдела аттестации
объектов информатизации — Андрей Петрович Кондратюк

Технический специалист,
кандидат технических наук — Новаковский Сергей Николаевич