

## **ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА**

доктора технических наук, профессора Липатникова Валерия Алексеевича на диссертацию Витковой Лидии Андреевны, выполненную на тему «Модели, алгоритмы и методика противодействия вредоносной информации в социальных сетях» и представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

### **1. Актуальность темы диссертационного исследования**

Сегодня, большие вызовы создают существенные риски для государства, общества и личности, но одновременно с этим представляют собой важный фактор для появления новых возможностей и перспектив научно-технологического развития в области информационной безопасности. Одними из наиболее значимых вызовов с точки зрения научно-технического развития Российской Федерации являются новые внешние угрозы национальной безопасности, обусловленные ростом международной конкуренции и конфликтности, глобальной и региональной нестабильностью, и усиление их взаимосвязи с внутренними угрозами национальной безопасности. Необходимо повышение эффективности противодействия информационных угрозам в социальных сетях, в пространстве которых сегодня отражаются внутренние и внешние государственные и общественные конфликты, где противник активно использует любые доступные ему способы манипулирования общественным сознанием и душевным спокойствием личности для достижения своих целей. При этом, глубина проникновения социальных сетей в повседневную жизнь человека возрастает с каждым днем. Преимущество социальных сетей состоит в возможности участников коммуникации оперативно транслировать информацию на большую аудиторию, публиковать медиа информацию, вовлекать новых участников в различные мероприятия или сообщества. Только за последние пять лет частью повседневной жизни современного общества стали более десяти различных платформ социальных сетей и уже очевидной проблемой информационной безопасности современного общества стала вредоносная информация. Кроме того, отдельные функции



социальных сетей, такие как добавление в друзья, возможность комментирования и т.д., массового внедряются в различные сервисы: новостные сайты, банки, онлайн магазины и прочее.

Период пандемии показал то, насколько эта проблема вредоносной информации в социальных сетях критична. Волны паники и страхов, порождаемые информационными атаками, недостоверная информация о распространении вируса, компании антивакцинации, теории заговора. Все это может приводить не только к ухудшению психического состояния общества, но и агрессивным действиям, связанным с порчей имущества, а также действиям влияющих на физическую безопасность и состояние здоровья граждан.

В связи с этим, можно утверждать, что диссертационное исследование, выполненное соискателем, по разработке моделей, алгоритмов и методик для повышения эффективности противодействия вредоносной информации в социальных сетях, является актуальным, имеющим существенное значение для государства, общества и личности.

## **2. Структура диссертационной работы**

Структура диссертационной работы выглядит логичной и цельной, название глав и разделов соответствует выбранной теме и направлению исследований. В первой главе достаточно полно раскрыт обзор релевантных моделей, алгоритмов и систем, описаны требования к методике. Во второй главе содержится описание комплексов моделей и алгоритмов. В третьей главе диссертации описывается методика противодействия, архитектура системы и программные прототипы компонентов, а также теоретическая и экспериментальная оценка положений, выносимых на защиту.

## **3. Новизна исследования и полученных научных результатов**

Автор на защиту выносит следующие основные научные результаты:

1. Комплекс моделей социальной сети, источника и вредоносной информации.

В комплекс объединены множество параметров, характеризующих источник информации, социальную сеть как среду распространения, вредоносную информацию и информационно-признаковая модель. При этом в комплекс входят новые классы и атрибуты, новые связи между ними.

2. Комплекс алгоритмов анализа источников вредоносной информации и ранжирования контрмер.



Комплекс обеспечивает анализ и сортировку объектов воздействия для противодействия вредоносной информации. Кроме того, входящие в комплекс алгоритмы ранжирования источников по потенциалу и сортировки объектов воздействия учитывают такие характеристики как количество сообщений источника, уровень обратной связи от аудитории социальных сетей на сообщения с вредоносной информацией. Предложенный алгоритм вредоносной информации и ранжирования контрмер разделен на ряд независимых алгоритмов, после каждого из которых может быть рассчитана отдельная оценка объекта воздействия и/или ранг контрмеры. Подобный подход обеспечивает формирование пар цель-контрмера без значительного увеличения требуемых ресурсов и времени. Для алгоритма ранжирования контрмер была разработана классификация возможных мер противодействия и предложены отдельные метрики.

3. Методика противодействия вредоносной информации в социальной сети.

Методика противодействия вредоносной информации в социальных сетях отличается своей ориентированностью на автоматизированный и автоматический выбор объектов воздействия и мер противодействия вредоносной информации из списка ранжированных контрмер. Помимо этого, разработанная методика отличается от существующих использованием авторских алгоритмов анализа и оценки источников и ранжирования контрмер, благодаря чему повышается обоснованность принятия решения о противодействии цели и выбора контрмеры и сокращается время работы оператора в процессе противодействия вредоносной информации в социальных сетях.

4. Архитектура и программные компоненты системы противодействия вредоносной информации.

Архитектура и программные прототипы компонентов ориентированы на ранжирование и выбор доступных контрмер в системе. В архитектуру входят оригинальные компоненты анализа и оценки источника вредоносной информации, база данных с информацией о мерах противодействия вредоносной информации, информация об агентах реализации. Таким образом, архитектура обеспечивает формирование наборов исходных данных для исследований и разработок в области противодействия вредоносной



информации, а также для исследований и разработок решений для систем поддержки принятия решения.

При этом при решении поставленной научной задачи Виткова Л.А. использовала в работе в качестве методов и методологии системный и сравнительный анализ, объектно-ориентированный подход и структурный синтез, методы ранжирования, экспертной оценки, проектирования архитектур и программных систем.

#### **4. Степень обоснованности и достоверность полученных научных результатов**

Достоверность основных выводов и результатов диссертации подтверждается:

- сравнительным анализом существующих научных и практических разработок в области противодействия вредоносной информации;

- корректностью предложенных концептуальных и математических моделей, алгоритмов и методики, апробацией основных теоретических положений диссертации в печатных трудах, докладах на российских и международных научно-технических конференциях, и семинарах;

- результатами проведенных экспериментов на основе разработанных программных прототипов, теоретической оценкой методики и алгоритмов и анализом результатов опроса экспертов по оценке разработанной методики;

- положительными результатами внедрения основных научных положений диссертации в отечественных проектах, на предприятии и в учебном процессе ВУЗов.

#### **5. Значимость полученных результатов для науки и для практики**

Теоретическая значимость полученных результатов заключается в совершенствовании науки информационной безопасности за счет введения новых классов, объектов, атрибутов и связей между ними для анализа и оценки информационных объектов и информационного обмена в информационном пространстве. Разработан новый подход к сортировке и ранжированию информационных объектов, а также за счет определения набора новых классов и метрик для мер противодействия.

Представленные результаты диссертационного исследования могут представлять интерес как для разработчиков перспективных систем противодействия вредоносной информации в социальных сетях, так и для



существующих вендоров в качестве расширения функционала систем мониторинга.

## **6. Недостатки и рекомендации**

Давая общую положительную оценку выполненного автором исследования, следует отметить ряд недостатков, выявленных при оппонировании работы:

1. Комплекс моделей социальных сетей учитывает не все объекты и их атрибуты в мессенджерах, видеохостингах.

2. При моделировании противодействия не учитывается время, необходимое для сбора данных из социальных сетей и их предобработку.

3. Не обоснован выбор технологий, используемых в архитектуре прототипа, реализующего предложенную методику.

4. Оформление отдельных элементов диссертационной работы не соответствует ГОСТ Р 7.0.11—2011.

5. В диссертации схема методики оформлена (рис. 3.2) не по ГОСТ 19.701-90 (ИСО 5807-85).

Отмеченные недостатки не носят принципиального характера, не влияют на общую положительную оценку работы, не влияют на новизну, теоретическую и практическую значимость, обоснованность и достоверность полученных в диссертации результатов.

## **7. Заключение**

Автореферат отражает основное содержание диссертационной работы.

Диссертация является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований, содержится решение важной научной задачи разработки новых и совершенствовании имеющихся методов и средств защиты информации.

Диссертация обладает внутренним единством, имеет четкую структуру, написана понятным языком. Результаты диссертационного исследования опубликованы автором с необходимой полнотой и свидетельствуют о личном вкладе автора диссертации в науку. Основные положения диссертации изложены в 20 публикациях, в том числе, в 8 статьях, индексируемых в базе данных Web of Science и/или Scopus, и в 6 статьях в рецензируемых изданиях из перечня ВАК России, получено 3 свидетельства о государственной регистрации программ для ЭВМ и баз данных.

Все это характеризует соискателя как вполне сложившегося исследователя, умеющего самостоятельно ставить и решать сложные научно-технические задачи.

Актуальность и важность поставленных и решенных в диссертации задач, современный технический и методический уровень их решения позволяют сделать заключение, что данная работа отвечает пп. 9-14 «Положения о присуждении ученых степеней», предъявляемых к кандидатским диссертациям

По своей теме, содержанию и полученным результатам диссертация соответствует п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса», п. 5 «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет» паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», а ее автор ВИТКОВА Лидия Андреевна заслуживает присуждения ученой степени кандидата технических наук по данной специальности.

Официальный оппонент:

Доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи имени Маршала Советского Союза С.М. Буденного Министерства обороны РФ

Липатников Валерий Алексеевич

«25» 05 2021 г.

Подпись Липатникова В.А. ЗАВЕРЯЮ

Помощник начальника академии по службе войск и безопасности  
военной службы начальник строевого отдела  
полковник

А.Головин



ФИО:	Липатников Валерий Алексеевич
Ученая степень:	доктор технических наук
Ученое звание:	профессор
Место работы:	научно-исследовательский центр Военной академии связи имени Маршала Советского Союза С.М. Буденного Министерства обороны РФ
Должность:	Старший научный сотрудник
Рабочий почтовый адрес:	194064, г. Санкт-Петербург, К-64, Тихорецкий проспект, д. 3
Телефон (рабочий):	+7 (812) 247-98-35
Адрес электронной почты:	vas@mil.ru