СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования.

В настоящее время сеть Интернет является основным источником получения информации для большинства людей. Подробный анализ большого количества социальных исследований показывает существенный прирост числа пользователей с каждым годом [1-3]. Согласно последним исследованиям, изложенных в докладе ООН «The State of Broadband 2017: Broadband catalyzing sustainable development», количество пользователей Интернета достигло отметки в 3,58 млрд человек, что составляет практически половину населения земного шара [1]. Что касается нашей страны, то доля интернет-пользователей в России составляет около 80% [2]. Примечательно, что среди молодых людей в возрасте от 16 до 29 лет этот показатель достиг 97% [3].

В связи с высокой популярностью социальных сетей они помимо выполнения функций поддержки общения, обмена мнениями и получения информации всё чаще становятся объектами и средствами информационного управления, а также ареной информационного противоборства. Они являются существенным инструментом информационного влияния, в том числе – в целях манипулирования личностью, социальными группами и обществом в целом, а также полем информационной войны [4-7].

Термин «социальная сеть» был введен задолго до появления Интернета и традиционных интернет-сетей. В 1954 году американский социолог Джеймс Барнс так обозначил социальную структуру, состоящую из группы узлов, которыми являются социальные объекты (общность, социальная группа, человек, личность, индивид) [8]. С развитием Интернета этот термин стал широко применяться для обозначения ресурсов, функционал которых позволяет представлять себя в Интернете, создавать собственную страничку и общаться с другими пользователями. Сегодня в общепринятом понятии под социальной сетью понимают интернет-площадку, сайт, который позволяет зарегистрированным на нем

пользователям размещать информацию о себе и коммуницировать между собой, устанавливая социальные связи.

Социальная сеть (от англ. social networks) – это социальная структура, состоящая из группы узлов, которыми являются социальные объекты (люди, группы людей, сообщества, организации) и связей между ними (социальных взаимоотношений) [9].

Для России самой популярной социальной сетью является ВКонтакте. Число активных пользователей на 2017 год составляет около 100 млн [10]. В социальной сети ВКонтакте в сутки пользователи отправляют 5 млрд. сообщений и 1 млрд. раз ставят отметку «Мне нравится». Все эти данные говорят о высокой популярности социальной сети.

Все социальные сети для общения имеют структуру автоматизированной социальной среды, которая обеспечивает коммуникации не только отдельных пользователей, но и групп, которые образовались при объединении общих интересов пользователей.

Но вместе со всеми преимуществами социальные сети представляют собой серьезную угрозу информационной безопасности. Любая социальная сеть определяется контентом, который она содержит. В информационных сетях может распространяться контент практически любого характера, в том числе и деструктивного. Значительная часть информационного потока содержит недостоверное или вводящее в заблуждение содержание. Данный феномен получил название фальшивых или фейковых новостей.

В связи с высокой популяризацией термин «фейк» стали использовать очень расширительно, называя фейком и фотографии, обработанные в Photoshop, иногда и видеоролики, смонтированные в видеоредакторе, страницы в социальных сетях, созданные от имени других (как правило, известных) людей, анекдотические истории, которые распространяют так называемые шоу-площадки и развлекательные ресурсы. В общем случае, фейк – это целенаправленное использование выдуманных и специально сфабрикованных новостей, главной целью которых является подрыв репутации какого-либо института, организации или

персоны. Наиболее точными синонимами фейковой новости является дезинформация или вброс фальшивки. Как правило, создатель новостного фейка имеет цель что-то дискредитировать или кого-то опорочить. Даже если вскоре информационные агентства разоблачат фейковую новость, фейк сработает на психологию восприятия как манипуляция. Фейковые новости оставляют в сознании аудитории неприятный осадок даже после того, как проверка фактов проведена и подделка разоблачена [11].

Фейк (от англ. fake) – это информационная мистификация или намеренное распространение дезинформации в социальных сетях и традиционных СМИ [12]. Фейк по-английски означает «подделка».

Термин «фейковые новости» в последние годы становится все более распространенным. Успех фальшивых новостей связан с рядом причин социального и психологического характера. Даже в идеальных условиях, когда пользователи нацелены на выявление и отказ от распространения низкокачественной информации, поток информации настолько велик, что в результате информационной перегрузки и потери бдительности всё равно становится возможным попадание в него значительной доли дезинформации. В реальном же мире, особенно в условиях социальных сетей, пользователи которых разделены на сообщества с тенденцией к поляризации политических и иных взглядов, на доверие к информации нередко влияют предубеждения участников и механизмы группового подкрепления. Кроме того, сами по себе алгоритмы социальных сетей построены таким образом, что приоритет получают не материалы, заслуживающие доверия, а те, которые привлекают больше внимания пользователей.

Хотя дезинформация в новостных сообщениях — это не новое явление, онлайновые системы распространения информации, особенно построенные по модели социальных сетей, являются для неё особенно подходящей средой. Связано это с тем, что механизмы, которые определяют популярность определённого сообщения, легко подвержены манипуляции с использованием специальных программ (так называемых «ботов»), имитирующих активность реальных пользователей, либо «бригад» — специально организованных дезинформационных

групп, действующих аналогичным образом. Такие боты или бригады становятся центрами сети социальных контактов, втираясь в доверие к пользователям, которые также начинают участвовать в распространении фейкового контента.

Как показывают исследования, относительно небольшое количество используемых ботами или бригадами учётных записей позволяет создать существенный по объёму поток дезинформации[13-16]. Для этого используется несколько стратегий. Во-первых, изначально информация организованно тиражируется ботами, чтобы она была замечена алгоритмами социальных сетей, неспособными отличить реальный «вирусный» интерес пользователей от накручиваемого искусственно. Во-вторых, боты используют механизмы социальных сетей, такие как хеш-теги и комментарии, чтобы привлечь внимание пользователей, выступающих центрами влияния. Наконец, используются технические средства, такие как TOR-сеть и прокси-серверы, для того, чтобы скрыть реальное местонахождение пользователей и создать видимость географического разнообразия их местонахождения.

Таким образом, социальные сети все чаще используются в качестве эффективной среды распространения ложной информации, недобросовестной конкурентной борьбы и политической пропаганды.

Согласно исследованиям около 78% людей доверяют информации, которая публикуется в социальных сетях. [17]. Пользователи не читают материалы, на которые ссылается социальная сеть, и не проверяют достоверность фактов, представленных в заголовке, текстовом анонсе, на иллюстрации и в самом материале. Это дает потенциальную возможность воздействовать на ожидания пользователей, которые зачастую не соответствуют действительности, и формировать выгодную для какой-либо стороны общественную точку зрения.

Например, размещение поддельных репостов на материалы ведущих экономических СМИ, чьи бренды имеют репутацию доверенных, относительно состояния национальной экономики и курсов валют может спровоцировать панику у населения того или иного региона.

Как показали события вокруг выборов президента в США и экономической ситуации в России, которые сопровождались массовыми вбросами ложной информации в социальные сети, внесением правок в «Википедию», ростом активности фейковых аккаунтов и другими подобными действиями, технология может быть весьма востребована и в Facebook, и в ВКонтакте, и в Twitter, и в других социальных сетях.

Таким образом, актуальность исследования обусловлена следующим.

1. Отсутствием на настоящее время исследований в сфере управления информационными рисками в социальных сетях, учитывающих особенности конкретных социальных сетей, их контента, в частности социальной сети для общения ВКонтакте, при распространении фейковой информации, оказывающей деструктивно-управляющее воздействие на пользователей сетей.

2. Наличием в информационных сетях огромного количества фейковой информации, которая носит деструктивный характер.

3. Ограниченной осведомленностью людей, особенно молодежи, об определении ложной и истинной информации, которая распространяется в социальных сетях.

Таким образом, в данной области необходимо создание комплексного научно-методического обеспечения, которое позволит подробно исследовать процессы распространения фейков в социальных сетях для общения.

Исследования предшествующих моделей распространения фейков в социальных сетях указывают на неполноту и несовершенство этих моделей, в связи с этим возникают следующие **противоречия.**

1. Существующие модели [40-44] распространения фейков не учитывают особенности распространения фейкового контента в некоторых социальных сетях. В связи с этим является логичным изучение основных способов распространения фейков в социальной сети для общения ВКонтакте.

2. Упомянутые выше модели распространения фейков не учитывают потенциальную возможность пользователей подвергнуть сомнению полученную информацию и проверить ее на достоверность, что не соответствует

действительности, так как у пользователя есть большое количество альтернативных источников информации, по которым он может установить ложность фейка.

3. В предыдущих работах не проводилось автоматизированное моделирование процессов распространения фейков в социальных сетях, что не позволяет в достаточной мере сделать выводы об успешности распространения фейков при различных параметрах.

Степень проработанности темы исследования. Касательно вопросов исследования информационных рисков [18, 19] в социальных сетях опубликовано достаточно много работ, в которых проанализированы и структурированы как сами способы распространения вредоносного контента, так и были предложены меры и средства для противодействия [30, 35, 40-44]. Однако данные работы не рассматривали распространение фейкового контента в социальных сетях, что не позволяет в достаточной мере исследовать процесс распространения фейков в социальной сети для общения ВКонтакте.

Работа выполнена в соответствии с одним из основных направлений ФГБОУ ВПО «Воронежский государственный технический университет» «Управление информационными рисками и обеспечение безопасности инфокоммуникационных технологий» на базе Воронежского научно-образовательного центра управления информационными рисками.

Объектом исследования является социальная сеть для общения ВКонтакте, в которой происходит распространение фейковой информации.

Предметом исследования являются модели распространения фейков в социальных сетях для общения.

Цель исследования состоит в разработке дискретной вероятностной модели распространения фейков, учитывающей особенности конкретных социальных сетей, в частности социальной сети для общения ВКонтакте.

Для достижения поставленной цели представляется необходимым решить следующие **задачи**.

1. Произвести формализацию описания социальной сети для общения ВКонтакте с учетом особенностей распространения фейкового контента, а также определить основные способы распространения фейков в социальных сетях.

2. Разработать дискретную вероятностную модель распространения фейков, учитывающую особенности конкретных социальных сетей, в частности социальной сети для общения ВКонтакте.

3. В программном комплексе «NetEpidemic» реализовать возможность моделирования процесса распространения фейков на основе разработанной модели.

Новизна результатов.

1. Систематизированы общие подходы к описанию и формализации фейков, определены основные способы распространения фейкового контента в социальной сети ВКонтакте. Впервые предложено выражение для нахождения эффективности фейкового контента, учитывающее особенности контента социальной сети ВКонтакте.

2. Впервые предложена дискретная вероятностная модель распространения фейков SEIHRZ, отличающаяся от аналогов тем, что учитывает потенциальную возможность пользователей подвергнуть сомнению полученную информацию и проверить ее на достоверность, таким образом позволяя пользователям приобрести иммунитет к фейку.

3. Впервые смоделирован процесс распространения фейков по модели SEIHRZ в специализированном программном обеспечении «NetEpidemic».

Практическая ценность работы заключается в том, что:

- исследование способов распространения фейков в социальной сети ВКонтакте позволяют расширить и дополнить моделирование эпидемий и соответственно представить более цельную картину функционирования социальных сетей при распространении фейкового контента;

- предложенная модель распространения фейков в социальных сетях раскрывает новые возможности для распространения деструктивного контента, в связи с этим совершенствуются методы управления рисками;

- моделирование процессов распространения фейков в социальных сетях позволяет разработать эффективные способы противодействия процессам распространения фейков.

Методы исследования. В исследовании предполагается использовать методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы аналитического моделирования.

ЗАКЛЮЧЕНИЕ

Данная дипломная работа посвящена исследованию процессов распространения фейков в социальной сети для общения ВКонтакте. В результате выполнения работы были получены следующие основные результаты.

1. Произведена формализация описания социальной сети для общения ВКонтакте, представлены классификация и характеристики фейков. Также была описана специфика фейковой информации, были выделены основные особенности ее распространения в социальных сетях. Приведенная классификация фейков может служить основой для формализации представления фейков и их учета при построении моделей распространения фейкового контента в социальных сетях. Была предложена формула нахождения эффективности контента.

2. Была предложена дискретная вероятностная модель SEIHRZ распространения фейкового контента, учитывающая особенности социальной сети ВКонтакте. Вероятности переходов для предложенной модели были собраны методом опроса пользователей социальной сети.

3. Произведено автоматизированное моделирование процессов распространения фейков на основе разработанной модели SEIHRZ, проведено сравнение с существующими моделями распространения фейков. Также было произведено наглядное сравнение способов распространения между обычными пользователями и при помощи социальных ботов.

В ходе проделанной работы была достигнута поставленная цель: разработана и дискретная вероятностная модель распространения фейков, учитывающая особенности социальной сети ВКонтакте, получившая название SEIHRZ. Продемонстрирована работа данной модели в специализированном программном обеспечении «NetEpidemic».

Перспективные направления развития. В проделанном исследовании стояла цель рассмотреть и разработать вероятностную модель распространения фейковой информации. Следовательно, будущие разработки могут состоять в

формировании модели ограничения и предотвращения распространения фейкового контента в социальных сетях на основе предложенных систем.

Указанные перспективные направления развития показывают высокую актуальность и необходимое изучение тематики распространения фейкового контента не только в социальных сетях, но и в других сферах.

СПИСОК ЛИТЕРАТУРЫ

1 THE STATE OF BROADBAND 2017: BROADBAND CATALYZING SUSTAINABLE DEVELOPMENT - Электрон. дан. - Режим доступа: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf.

2 TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS - Электрон. дан. - Режим доступа: http://www.internetworldstats.com/top20.htm.

3 Количество пользователей интернета в России - Электрон. дан. - Режим доступа: http://www.bizhit.ru/index/users_count/0-151.

4 Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А Новиков, А. Г. Чхартишвили. – М.: Физматлит, 2010. - 228с.

5 Губанов Д. А. Модели влияния в социальных сетях (обзор) / Д. А. Губанов, Д. А Новиков, А. Г. Чхартишвили // Управление большими системами. – 2009. — 70 с.

6 Губанов Д. А. Модели распределенного контроля в социальных сетях / Д. А. Губанов, Д. А Новиков // Системы управления и информационные технологии. – 2009. – №37 – С. 124–129.

7 Губанов Д. А. Модели репутации и информационного управления в социальных сетях / Д. А. Губанов, Д. А Новиков, А. Г. Чхартишвили // Математическая теория игр и ее приложения. – 2009. – С.14–37.

8 Дужникова А.С. Социальные сети: современные тенденции и типы пользования / А.С. Дужникова // Мониторинг общественного мнения: экономические и социальные перемены – 2010. - №5(99). – 289 с.

9 Воронкин А.С. Социальные сети: эволюция, структура, анализ. - Электрон. дан. - Режим доступа: https://cyberleninka.ru/article/v/sotsialnye-seti-evolyutsiya-struktura-analiz.

10 ВКонтакте - Электрон. дан. – Режим доступа: https://vk.com/page-47200925_44240810.

11 Фейковые новости как паразит социальных сетей – Электрон. дан. – Режим доступа: http://elar.urfu.ru/bitstream/10995/47847/1/journ_staff_2017_010.pdf.

12 Википедия. Фейк. – Электрон. дан. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B9%D0%BA_(%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%B8%D1%8F).

13 Alymov A.S. Detection of bot programs that mimic the behavior of people in the social network "Vkontakte" / A.S. Alymov, V.V. Baranjuk, O.S. Smirnova // International Journal of Open Information Technologies vol. 4, №. 8, 2016.

14 Евсеева А.О. Идентификация ботов в социальных сетях на базе технологий интеллектуального анализа данных / А. О. Евсеева, Р. И. Гумерова, А. С. Катасёв, А. П. Кирпичников // Вестник технологического университета. 2017. Т.20, №5 С.87-90.

15 Катасёв А.С. Нейросетевая модель идентификации ботов в социальных сетях / А. С. Катасёв, Д. В. Катасёва, А. П. Кирпичников, А. О. Евсеева // Вестник технологического университета. 2015. Т.18, №16 С.253-256.

16 Chesnokov V.O. APPLICATION OF THE COMMUNITY ALLOCATION ALGORITHM IN THE INFORMATION CONFRONTATION IN THE SOCIAL NETWORKS / Вопросы кибербезопасности №1(19) – 2017 С.37-44.

17 Morozova A.A. VALIDITY OF INFORMATION IN SOCIAL NETS AND CRITERIA OF ITS VERIFICATION (BY THE EXAMPLE OF VKONTAKTE) / Bulletin of Chelyabinsk State University. 2017. No. 6 (402). Philology Sciences. Iss. 106. Pp. 75-83.

18 Остапенко Г.А. Информационные риски в социальных сетях / Г.А. Остапенко, Л.В. Паринова, В.И. Белоножкин, И.Л. Батаронов, К.В. Симонов./ Под ред. член-корр. РАН Д.А. Новикова, 2013. - 161с.

19 Паринов А.В. Социальные сети как среда распространения деструктивного контента / А.В. Паринов, Д.В. Гусев, Е.А. Автонова, Е.В. Гусев, В.А. Кургузкин, С.С. Тихонова / Информация и безопасность. – 2017. – Т. 20. – Вып.1. – С. 5-38.

20 Number of social media users worldwide from 2010 to 2021 (in billions) – Электрон. дан. – Режим доступа: https://www.statista.com/statistics/ 278414/number-of-worldwide-social-network-users.

21 Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions) - Электрон. дан. - Режим доступа: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users.

22 Захарова: отношение к инициативам РФ на Генассамблее ООН заметно улучшилось – Электрон. дан. – Режим доступа: http://tass.ru/politika/4583209.

23 Lewandowsky S. Misinformation and Its Correction: Continued Influence and Successful Debiasing / S. Lewandowsky, U. Ecker, C. Seifert // Psychological Science in the Public Interest . – 2014. – Vol. 13. №3. – P. 106 – 131.

24 ВКонтакте – Электрон. дан. – Режим доступа: https://vk.com/.

25 Описание методов API – Электрон. дан. – Режим доступа: https://vk.com/dev/methods.

26 Google & Facebook to target fake news sites by harshening ads policies – Электрон. дан. – Режим доступа: https://www.rt.com/usa/367063-google-facebook-fake-news/.

27 Алымов А.С. Детектирование бот-программ, имитирующих поведение людей в социальной сети «ВКонтакте» / А.С. Алымов, В.В. Баранюк, О.С. Смирнова // International Journal of Open Information Technologies. – 2016. – Vol. 4. № 4. – С. 55 – 59.

28 Kind S. Social Bots / S. Kind, M. Bovenschulte, S. Ehrenberg-Siles, T. Jetzke, S. Weide. – 2017. – 16 с.

29 Ferrara E. The Rise of Social Bots / E. Ferrara, O. Varol, C. Davis, F. Menczer. – 2017. – 11 с.

30 Reuter C. Rumors, Fake News and Social Bots in Conflicts and Emergencies: Towards a Model for Believability in Social Media / C. Reuter, M. Kaufhold, R. Steinfort. – 2017. – 9 с.

31 Grimme C. Social Bots: Human-Like by Means of Human Control? / C. Grimme, M. Preus, L. Adam // University of Muster, Germany. – 2017. – С. 1 – 36.

32 Статистика по профилям пользователей ВКонтакте – Электрон. дан. – Режим доступа: https://habrahabr.ru/post/123856/.

33 Stochastic rumours. / Daley, D. J., and Kendal, D. G., J. Inst. Maths Applics 1965 – P. 42-55.

34 Karelin V.V. Generalized model of information spreading in continuous time / V.V. Karelin, V.M. Bure, M.V. Svirkin // Vestnik of Saint Peterburg University. – 2017. – Vol. 13. №1. – P. 74 – 80.

35 Wang Ya. A Rumor Spreading Model with Control Mechanism on Social Networks / Ya. Wang, X. Yang, J. Wang // Chinese journal of physics. – 2015. – Vol. 52. №2. – P. 816 – 829.

36 Фальконе Я.И. Анализ методов моделирования распространения информационных угроз в социальных сетях / Я.И. Фальконе, Г.П. Жигулькин / Научно-технический вестник Поволжья. – 2017. – Вып. №2. – С. 125-127.

37 Захарченко А. Черводинамика: причины и следствия // Защита информации. Конфидент. – 2004. - №2. - С. 50-55.

38 Анзина Т.И. К вопросу о медиаконтенте и развитии критического мышления / Т.И. Анзина, Е.Ю. Рожина, И.В. Селиванова / Новое в лингвистике и методике преподавания иностранных и русского языков: сборник научных трудов по материалам I Международной научно-практической конференции 28 февраля 2017. – г. Оренбург: Научно-издательский центр «Открытое знание», 2017. – С. 4 – 12.

39 R. Isea Mathematical analysis of the spreading of a rumor among different subgroups of spreaders / R. Isea, R. Mayo-Garcia / Fundación Instituto de Estudios Avanzados, IDEA. – 2015.

40 Zhao L. SIR rumor spreading model in the new media age / L. Zhao, H. Cui, X. Qui // Physica A: Statistical Mechanics and its Applications. – 2013. – Vol. 392. №4. – P. 995-1003.

41 Wang J. SIR Rumor Spreading Model with Network Medium in Complex Social Networks // J. Wang, Y. Wang // Chinese journal of physics. – 2015. – Vol. 53. №1. – P. 1 – 16.

42 Stanoev A. Modeling the Spread of Multiple Concurrent Contagions on Networks // A. Stanoev, D. Trpevski, L. Kocarev // Macedonian Academy of Sciences and Arts, Skopje, Macedonia. – 2014. – Vol. 9. №6. – P. 1 – 16.

43 Dong S. SEIR Model of Rumor Spreading in Online Social Network with Varying Total Population Size / S. Dong, Y. Deng, Y. Huang // Chinese Physical Society and IOP Publishing Ltd. – 2017. – Vol. 68. №4.

44 Chengcheng Shao The spread of fake news by social bots / Chengcheng Shao, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, and Filippo Menczer // Indiana University, Bloomington, 2017.

45 Filippo Menczer Misinformation on social media: Can technology save us? - Электрон. дан. – Режим доступа: https://theconversation.com/misinformation-on-social-media-can-technology-save-us-69264.

46 Hunt Allcott Social Media and Fake News in the 2016 Election / Hunt Allcott, Matthew Gentzkow // Journal of Economic Perspectives, Vol. 31, 2017.

47 Charlotte Henry Social Networks Can Learn from Apple to Solve ‘Fake News’ – Электрон. дан. – Режим доступа: https://www.macobserver.com/columns-opinions/editorial/social-networks-can-learn-apple-solve-fake-news.

48 How can social networks cope with the spread of fake news? – Электрон. дан. – Режим доступа: https://thequestion.com/questions/188986/how-can-social-networks-cope-with-the-spread-of-fake-news.

49 Claire Wardle Fake news. It’s complicated – Электрон. дан. – Режим доступа: https://firstdraftnews.com/fake-news-complicated.

50 Alan E. Mislove. Online Social Networks: Measurement, Analysis, and Applications to Distributed Information Systems. Houston, Texas: RICE University, 2009.

51 Valerio Arnaboldi, Andrea Passarella, Marco Conti, Robin I.M. Dunbar. Online Social Networks: Human Cognitive Constraints in Facebook and Twitter Personal Graphs. Waltham: Elsevier Inc., 2015.

52 Barbara Carminati, Elena Ferrari, Marco Viviani. Security and Trust in Online Social Networks. Morgan&Claypool, 2014.

53 Panagiotis Karampelas. Techniques and Tools for Designing an Online Social Network Platform. New Hampshire: Hellenic American University, 2013.

54 Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.

55 Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 410-415.

56 Optimization of expert methods used to analyze information security risk in modern wireless networks / S.A. Ermakov, A.S. Zavorykin, N.S. Kolenbet, A.G. Ostapenko, A.O Kalashnikov // Life Science Journal. – 2014. – № 11(10s). – P. 511-514.

57 Assessment of the system's EPI-resistance under conditions of information epidemic expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, D.V. Gusev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (3). – P. 1781-1784.

58 Peak risk assessing the process of information epidemics expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251-255.

59 Discreet risk-models of the process of the development of virus epidemics in non-uniform networks / V.V. Islamgulova, A.G. Ostapenko,,N.M. Radko, R.K. Babadzhanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – P. 306-315.

60 Albert R., Barabasi A.-L. Statisticalmechanics of complex networks / Rev. Mod. Phys. 2002. – P. 47-54.

61 Eckmann J.-P. Curvature of colinks uncovers hidden thematic layers in the world wide web / J.-P. Eckmann, E. Moses / Proc. Noll. Acad. Sci. – 2002. –P. 5825-5829.

62 Flake, G. w. Self-organization and identification of Web communities / G. w. Flake, S. R. Lawrence, C.L. Giles, F.M. Coetzee / IEEE Computer. – 2002. – № 35. – P. 66-71.

63 Lauritzen S.L. Local computations with probabilities on graphical structures and their application in expert systems / S. L. Lauritzen and D. J. Spiegelhalter. - Journal Royal Stati1tical Society B, 50, 1988.– P. 28-35.

64 Haythornthwaite C. 2005. Social networks and internet connectivity effects. Information, Communication & Society, 8(2), – P. 125–147.

65 Alan Mislove Measurement and Analysis of Online Social Networks – P.4-5.

76 Freeman L. C. The Development of Social Network Analysis / L.C. Freeman//Empirical Press. – 2004. – P. 30.

77 Fronczak A. Higher order clustering coefficients in Barabasi-Albert networks / A. Fronczak, J.A. Holyst, M. Jedynak, J. Sienkiewicz / Physica A 316. – 2002. –P. 688-694.

78 Dorogovtsev S.N., Evolution of Networks: From Biological Networks to the Internet and WWW / S.N. Dorogovtsev, J.F.F. Mendes; - Oxford, USA: Oxford University Press, 2003. – P. 280.

79 Abassi A. Betweenness centrality as a driver of preferential attachment in the evolution of research collaboration networks / A. Abassi, L. Hossain, L. Leydesdorff // Journal of Informetrics. – 2012. – № 6. – P. 403–412.

80 Tsvetovat M., Social Network Analysis for Startups: Finding Connections on the Social Web. — O'Reilly, 2011. — P. 45. — 192 c.

81 Freeman L. C. Centrality in valued graphs: A measure of betweenness based on network flow / L. C. Freeman, S. P. Borgatti, D.R. White// Soc. Networks. –1991. – № 13. – P. 141-154.

82 lbert R., A.-L.Error and attack tolerance of complex networks // Nature. Vol. 406, (2000). – P. 378–382.

83 Newman, M. E. Finding and evaluating community structure in networks / M. E. J. Newman, M. Girvan // Phys. Rev. E 69. –2004.– P. 53-58.

84 Ren W. Consensus seeking in multiagent systems under dynamically changing interaction topologies / W. Ren, R.W. Beard // IEEE Trans. on Automatic Control. – 2005. – Vol. 50, N 5. – P. 655–661.

85 Barabasi A. L., Network medicine: a network-basedapproach to human disease. Nat. Rev. Genet. 12, 2011. – P. 56–68.

86 Barabasi R. Albert Emergence of scaling in random networks / Albert R. Barabasi; Science. - 1999. – P. 509-512.

87 Абрамов К. Г., Моделирование распространения нежелательной информации в социальных медиа / К.Г. Абрамов, Ю.М. Монахов; Труды XXX Всероссийской научно-технической конференции. Проблемы эффективности и безопасности функционирования сложных технических и информационных систем / Серпуховский ВИ РВ. - 2011. – ч. IV. - С. 178-182.

88 Монахов Ю.М., Моделирование распространения нежелательной информации в социальных медиа / Ю.М. Монахов, К.Г. Абрамов; Вестник КГУ им. Н.А. Некрасова. - 2011. – Т.17, №3. - С. 15-18.

89 Монахов Ю.М., Аналитическая модель дезинформированной узла социальной сети / Ю.М. Монахов, М.А. Медведникова; ИММОД-2011. - Санкт-Петербург, 2011. – Т. II. – 400 с., - С. 178- 180.

90 Ball F. Epidemics with two levels of mixing / F. Ball, D. Mollison, G. Scalia-Tomba, / Annals of Applied Probability. – 1997. – № 7. – P. 46–89.

91 Поляков И. В. Хранение и обработка графа социальных сетей / И. В. Поляков, А. А. Чеповский, А. М. Чеповский / Вестн. НГУ. Сер. Информ. технологии. – 2013. – Т. 11, вып. 4. – С. 77–83.

92 Ball, F. Epidemics with two levels of mixing / F. Ball, D. Mollison, G. Scalia-Tomba, // Annals of Applied Probability. – 1997. – № 7. – P. 46–89.

93 Networks: Structure and Dynamics / Physics Reports, 424 (2006).–P. 175 – 308.

94 Berberich K. Time-aware authority ranking / K. Berberich, M. Vazirgiannis, G. Weikum. - Int. Math., 2(3), - 2005. - P. 301–332.

95 Neuman M.E.J. The Physics of Networks / Physical Today (2008), November.– P. 33 – 38.

96 Абрамов К. Г., Распространение нежелательной информации в социальных сетях Интернета / К.Г. Абрамов, Ю.М. – С.45-48.

97 Волобуев С.В. Философия безопасности социотехнических систем / С.В. Волобуев. – М.: Вузовская книга, 2002. – 360 с.

98 Bar-Yossef, Z. Local approximation of PageRank and Reverse PageRank / Z. Bar-Yossef, L.-T. Mashiach / Proceedings CKIM'08. – 2008. – 36 p.

99 Benzi M. Ranking Hubs and Authorities Using Matrix Functions / M. Benzi, E. Estrada, C. Klymko //CS Technical Report TR. – 2012. – 30 p.

100 Черняк, Л. Сервисы и теории социальных сетей Текст. / Л. Черняк / Открытые системы. СУБД. 2008. - № 8. - С. 25-31.

101 Громов Ю.Ю., Анализ живучести информационных сетей / Информационные процессы и управление. – 2006. – №1. – С. 138–155.

102 Губанов Д.А. Модели информационного влияния и информационного управления в социальных сетях / Д. А. Губанов, Д. А. Новиков А. Г. Чхартишвили / Проблемы управления. 2009. – №5, – С. 28-35.

103 Абрамов К.Г., Модели распространения вредоносных программ в топологически гетерогенных социальных сетях - Электрон. Дан. - К.Г. Абрамов, Ю.М. Монахов; Труды НТС. Комитет по информатизации, связи и телекоммуникациям Администрации Владимирской области. – 2010. – С.156-161.

104 Duchi J. "Efficient Online and Batch Learning Using Forward Backward Splitting /J. Duchi,Y. Singer // Journal of Machine Learning Research, vol. 10, 2009.–pp. 2899– 2934.

105 Goodman J. Spam and the ongoing battle for the inbox / J. Goodman, G. V. Cormack, D. Heckerman// Commun. ACM 50. vol. 2. –2007. – pp. 24–33.

106 Biggio B. Evade Hard Multiple Classifier Systems, vol. 245. Springer Berlin / B. Biggio, G. Fumera, F. Roli. // Heidelberg. – 2008. – pp. 15–38.

107 Опросы ВКонтакте - Электрон. дан. - Режим доступа: https://vk.com/polls4you.

108 Daley D. J. Epidemic Modelling. / D. J. Daley, J. Gani // Cambridge University Press Cambridge UK. – 2000. – P. 1-16.

109 Information spreading on dynamic social networks./ Chuang Liu, Zi-Ke Zhang, Commun Nonlinear Sci Numer Simulat 19, 2014 – P. 896–904.

110 Agent-Based Modelling of Epidemic Spreading using Social Networks and Human Mobility Patterns - Электрон. дан. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.409.662&rep=rep1&type=pdf.

111 Fake Profiles in Online Social Networks / Mudasir Ahmad Wani, Suraiya Jabin, 30 May 2017 – P. 31.

112 Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model. / Krombholz, K., Merkl, D., &Weippl, E. Journal of Service Science Research, 4(2), 2012 – P. 175-212.

113 Modeling and Analyzing the Interaction between Network Rumors and Authoritative Information. / L.Xia, G.Jiang, Y.Song, B.Song, Entropy 17, 2015 – P.471-482.

114 Epidemic outbreaks in complex heterogeneous networks. / Yamir Moreno, Romualdo Pastor-Satorras, Alessandro Vespignani, The European Physical Journal B, Volume 26, Issue 4, February 1, 2008 – P. 521–529.

115 Golbeck J. Introduction to Social Media Investigation: A Hands-on Approach / J. Golbeck // Waltham: Elsevier Inc. – 2015. – P. 323–326.

116 Abassi A. Betweenness centrality as a driver of preferential attachment in the evolution of research collaboration networks / A. Abassi, L. Hossain, L. Leydesdorff // Journal of Informetrics. – 2012. – № 6. – P. 412.

117 Alba R.A. graph-theoretic definition of a sociometric clique / R.D. Alba // Journal of Mathematical Sociology. – 1973. – P. 126.

118 NetEpidemic - Электрон. дан. – Режим доступа: http://localhost:63522/Home/EpidemiModeler.

119 Vozhzhova A.V. Leaders of opinions on social networks / A.V. Vozhzhova, Yu.V. Pupkova // Научные труды КубГТУ. – 2017. – № 6. – С.86 – 93.

120 vk.com – Электрон. дан. – Режим доступа: https://vk.com/teamnavalny

121 vk.com – Электрон. дан. – Режим доступа: https://vk.com/page-59800369_50382925.

122 The Koblenz Network Collection – Электрон. дан. – Режим доступа: http://konect.uni-koblenz.de/networks/.

123 Agarwal A. Sentiment analysis of Twitter data / A. Agarwal, B. Xie, I. Vovsha, O. Rambow, R. Passonneau // LSM ’11 Proceedings of the Workshop on Languages in Social Media, Association for Computational Linguistics. – 2011. – P. 623.

123 Guilherme F. Role of centrality for the identification of influential spreaders in complex networks / F. Guilherme, L. Andre, M. Pablo, A. Francisco // Universidade de São Paulo, Biblioteca Digital da ProduçãoIntelectual – BDPI. – 2014. – P. 2–8.

124 Skaza J. Mathematical Modeling of Trending Topics on Twitter / J. Skaza // Senior Capstone Project for Jonathan S. Skaza. – 2014. – P. 3–5.

125 Tixier A. J. A Graph Degeneracy-based Approach to Keyword Extraction / A. J. Tixier, F. D. Malliaros, M. Vazirgiannis //Conference on Empirical Methods in Natural Language Processing (EMNLP). – 2016. – Vol. 22.

126 vk.com – Электрон. дан. – Режим доступа: https://vk.com/page-2158488_53417896.