

## СОДЕРЖАНИЕ

Введение	7
1 Социальные сети для авторских записей и социальная сеть LiveJournal	14
1.1 Понятийный аппарат	14
1.2 Социальные сети для авторских записей и их модели	17
1.3 Структурно функциональные особенности сети	19
2 Топологические и вероятностные параметры сети LiveJournal	27
2.1 Исходные данные для моделирования сети	27
2.2 Репрезентативная выборка из сети LiveJournal	29
3 Моделирование процесса диффузии контента в репрезентативной выборке из социальной сети LiveJournal	42
3.1 Моделирование процесса диффузии контента для единственной разновидности контента	42
3.2 Моделирование процесса диффузии контента для двух конкурирующих контентов	58
4 Рекомендации по управлению диффузией процессом для рассматриваемых контентов в сети LiveJournal	62
4.1 Расчет риска и шанса на основе результатов моделирования диффузионных процессов	62
4.2 Выработка рекомендаций по регулированию процесса информационной диффузии	72
Заключение	87
Список литературы	90

## ВВЕДЕНИЕ

В настоящее время люди не представляют себя без электронных девайсов, которые позволяют пользоваться всевозможными услугами сети интернет, находясь в любой точке города, области [1], страны. Конечно, есть отдаленные уголки планеты, где нет мобильной связи, нет сети интернет, нет и людей в том количестве, что обитают в городах. Сейчас все чаще на улице можно встретить подростков, которые вместо игр со сверстниками предпочитают игры в телефоне или планшете. Вместо реального общения люди выбирают виртуальное общение, синоним которому - одиночество.

Люди находят в сети терабайты «полезной» для себя информации и одновременно предоставляют ее еще кому-то, становясь одним звеном в общей цепочке «новостей», «блогов», «чатов». В интернете нет преград, нет норм морали, нет совести. Есть только оплаченный раз в месяц доступ к сети, где циркулирует информация. Есть в этом огромный плюс: не надо ходить в библиотеки, искать где-то пропавшую старую энциклопедию. В один клик можно получить все ответы на интересующие вопросы [2]. Но помимо и полезной информации можно получить грамотно подобранную и ложную информацию, поданную как подлинную. Порой не надо искажать факты целиком, а только грамотно направить, немного изменить один фрагмент, чтобы исказить смысл всего запроса целиком. Пользователь видит лишь текст, а верить ему или нет, решает он сам. Очень сложно распознать где правда, а где ложь, тем более, что интернет [2] — это огромная свалка информации.

В 21 веке людей из разных районов, городов, областей и стран стали объединять социальные сети, сети, которые позволяли общаться, не обращая внимание на расстояние, делиться мнениями, не боясь показаться глупым. В социальных сетях создается иллюзия огромного мира вокруг каждого пользователя, все так близко, но и одновременно далеки друг от друга. Пользователи социальных сетей делятся друг с другом волнующей их информацией, аргументируют, высказываются за и против. Социальные сети позволяют пользователям

объединяться в группы по интересам, организовывать встречи и собрания, вести дискуссии по разным интересующим тематикам.

В социальных сетях присутствует разнородная информация [1,3], касающаяся досуга людей их вкусов, интересов. Открытые фотографии с отпуска говорят о том, что человек либо в отпуске, либо только приехал. Хотя порой такие дилеммы не возникают потому, что люди сами делятся информацией о том, когда и куда они поедут. Социальные сети [4], как глобальные анкеты для людей, желающих сделать свою жизнь публичной, а настройки приватности, которые также присутствуют в социальных сетях никогда не будут ограничениями для администраторов сети и для людей, желающих их обойти - злоумышленников.

На данную тематику было проведено уже достаточно исследований [5] и с данная работа проводится для обобщения ранее полученных результатов, и выведения новых знаний и результатов, путем алгоритмизации и глубокого анализа распространения сетевого контента внутри социальной сети LiveJournal.

В настоящее время известно множество социальных сетей, таких как: LinkedIn, Vk, Facebook, Turnout, Langled, Drive2, Goodreads, Ok, LiveJournal [2,4]. Социальные сети можно разделить на сети обмена мультимедиа контентом, сети для общения [11-15], сети по интересам, сети для знакомств, справочные сети, сети для бизнеса и многие другие:

1. Социальные сети для общения: Facebook, VK, Loveplanet.
2. Социальные сети для обмена фото-видео информацией: Youtube, Instagram.
3. Социальные сети по интересам: Last.fm, Tagged
4. Сервисы социальных закладок: Diigo, Flipboard, Scoop.it.
5. Социальные сети для авторских записей (еще эти сети иногда называют блоговыми сетями): Livejournal, Twitter, Blogger.
6. Социальные сети для коллективных обсуждений: 4PDA, ответы Mail.ru.
7. Социальные сети для отзывов и обзоров: TripAdvisor, Яндексмаркет [14].

Данная классификация имеет условный характер. Также все социальные сети можно разделить на три большие категории:

- Социальные сети по интересам.
- Социальные сети для общения.
- Гибридные сети.

Социальные сети по интересам основываются на графе интересов, где связи между узлами социальной сети строятся на основе интересов этих узлов [5]. Каждый пользователь сети имеет некоторый круг интересующих его вопросов и соответственно коммуницирует он с теми пользователями, у которых схожие с ним интересы. Если взять набор интересов одного пользователя и соответственно набор интересов другого пользователя, то пересечение двух множеств интересов будет означать связь между двумя пользователями-узлами сети [6]. Все коммуникации пользователей будут так или иначе инициированы общими интересами [7].

Социальные сети для общения созданы для построения социальных связей между людьми с целью дальнейшего общения или просто знакомства [8-11]. Данные социальные сети имеют большую популярность среди пользователей и имеют гораздо большее число зарегистрированных пользователей. Граф социальных связей имеет большее количество вершин и большую связность.

Но стоит отметить и те, и другие в чистом виде выделить проблематично. Поэтому все чаще встречаются сети гибридные в основе, которых, либо граф социальный, либо граф интересов [12, 13]. В социальных сетях много различных групп по интересам - сообществ, что подразумевает образование в социальной сети для общения подграфа по интересам. И наоборот социальные сети по интересам включают пользователей, которые общаются друг с другом порой, отходя от темы, что приводит к образованию так называемого социального подграфа внутри графа по интересам.

Помимо рядовых пользователей, ничем не отличающихся друг от друга есть и реальные злоумышленники, которые рассылают с помощью ботов спами ссылки на фишинговые сайты, или призывают к поддержке экстремистских группировок.

Такая информация передается от пользователя к пользователю. Кто-то поверил предоставленной злоумышленником информации и сам стал распространять аналогичную информацию со своими друзьями, коллегами, знакомыми. Пользователи, распространяющие информацию, искренне верят в нее, потому готовы спорить, убеждать в своей правоте, всячески доказывать подлинность предоставленной информации. Таким образом, опасен становится не столько первоисточник информации, сколько последствия - люди которые последуют за этим мнением, как новые очаги передачи деструктивной информации, спама или экстремистского содержания. Распространение такого рода информации (спам, экстремистские ролики) сопровождается движением всех известных «окон Овертона» [12, 13], когда идея из полностью отрицаемого постепенно полностью входит в жизнь как одного человека, так и общества в целом.

Распространение нежелательного контента происходит несколько стихийно, аналогично эпидемиям вирусных инфекций, возникающих среди людей или животных. Исследование данного вопроса строится на моделировании процесса заражения единичного элемента - источника и затем уже необходимо разбить процесс на временные промежутки - фазы и изучать распространение эпидемии внутри каждой фазы [7]. Процесс распространения эпидемии будет очень интересен тем что, у каждого пользователя условно есть некая характеристика, обуславливающая его подверженность к заражению. Некоторые пользователи будут быстро подвергаться заражению, некоторые наоборот будут обладать иммунитетом [6].

**Степень проработанности темы исследования** довольно таки разбросана и не обобщена. Существует множество различных данных о статистике посещений, количестве пользователей, обсуждаемых тематиках, различная аналитика дальнейшего роста сети. Существует некоторая информация и метриках, и моделях графа, о вредоносном трафике, возможных рисках и угрозах.

Статистика говорит о стремительном росте социальной сети, и как следствие оказывается влияние на жизнь пользователей, их мнение уже в реальной жизни.

Получается некий перенос виртуальной жизни на реальную. Данная проблематика весьма актуальна.

**Актуальность работы** также будет заключаться в том, что открытость социальных сетей позволяет осуществить распространение вредоносного сетевого контента внутри социальной сети LiveJournal и его блокировка не может быть осуществлена оперативно. Глобальные фильтры и хранилища информации собственные дата центры по борьбе с такого рода эпидемиями помогают, но оперативно это сделать не всегда представляется возможным ввиду того, что социальные сети для авторских записей постоянно растут, пользователей становится все больше и блогов соответственно тоже.

**Объектом** исследования будет считаться социальная сеть LiveJournal в условиях моделирования распространения сетевого контента.

**Предметом** данного исследования будет считаться модель анализа распространения сетевого контента и оценки рисков в социальной сети LiveJournal.

**Цель** исследования: выработка обобщенного способа снижения и управления рисками в блогговой социальной сети LiveJournal в результате распространения сетевого контента.

**Задачи** исследования:

1. Анализ структурно-функциональных особенностей сети в ходе распространения сетевого контента.
2. Анализ статистических данных.
3. Создание необходимого информационного обеспечения для моделирования эпидемических процессов, включая получение репрезентативной выборки, сокращающей размерность модели.
4. Многовариантное моделирование распространения контента, включая различные тематики, начальные условия по внедрению деструктивного контента, моделирование противоборства для различных тематик.
5. Анализ результатов моделирования.
6. Выработка рекомендаций по регулированию рисков и шансов.

### **На защиту выносятся:**

- схемы, определяющие особенности архитектуры сети и протекающих в ней процессов в том числе: структурная схемы ресурсов сети, классификация объектов и субъектов сети, схемы действий и возможностей;
- метрики по исходные статистики сети для авторских записей LiveJournal;
- графики распространения эпидемии при различных условиях, для различных тематик, а также графики, описывающие информационную диффузию в сети для двух конкурирующих контентов, полученные при помощи специально разработанного программного обеспечения и отражающие результаты моделирования;
- методология управления информационной диффузией в сети для авторских записей LiveJournal в контексте её структурно-функциональных особенностей, основанная на результатах моделирования распространения эпидемии.

**Практическая значимость** данной работы заключается в нахождении способа достижения минимального значения риска в результате возникновения эпидемии в блогговой социальной сети LiveJournal.

**Новизна** данной в данной дипломной работе будет заключаться в специфическом подходе в осуществлении репрезентативной выборки из имеющейся статистики и созданию эквивалентной сети. Репрезентативность выборки достигается путем сравнения отклонений параметров распределения выборки и статистики. В результате чего совпадение с исходной выборкой доходит до 95%. Размер сети существенно снижается за счет отбора вершин по критерию удельного трафика. В работе используется дискретное вероятностное моделирование, дискретно, по шагам рассматриваются этапы моделирования. Источников заражения бывает несколько, атаки на социальную сеть распределены во времени и пространстве. С помощью реализованного программного продукта получается рассмотреть пошагово распространение эпидемии и детально рассмотреть в отличие

от аналогового моделирования распространение вредоносного трафика и зараженных вершин.

Результаты данной работы могут быть полезны для анализа распространения сетевого трафика в социальных сетях, анализируя сам граф социальных связей, а не его эквивалент и возможности применения методов оценки рисков для данных сетей.

## ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен всесторонний анализ социальной сети для авторских записей LiveJournal в целях исследования методов и моделей для предотвращения распространения вредоносного контента. В ходе выполнения работы были получены следующие результаты:

1. В первой главе дипломной работы был описан понятийный аппарат для социальной сети. Кроме того, представлены классификации:

- контента, циркулирующего в социальной сети для авторских записей LiveJournal;

- сетевых ресурсов данной сети, которые разделяются на ресурсы коллективного пользования и на ресурсы персонального пользования, также было дано их подробное описание;

- объектов и субъектов социальной сети. Все субъекты можно разделить на активных и пассивных пользователей, были установлены действия и функции, посредством которых, субъекты обмениваются контентом в социальной сети LiveJournal;

С учетом всех полученных классификаций в первой главе была построена структурно-функциональная модель социальной сети для авторских записей LiveJournal с учетом всех ее особенностей. В построенной модели функциональные связи представляют сложную структуру взаимодействия контента, сетевых ресурсов и субъектов, функционирующих в заданном сетевом пространстве.

2. Во второй главе работы были выполнены алгоритмы преобразования исходных данных сети и нахождения репрезентативной выборки, получена визуальная модель исследуемой сети, а также вычислены соответствующие матрицы, позволяющие провести анализ распространения контента в социальной сети. Доказана репрезентативность выборки генеральной совокупности с помощью критерия согласия Пирсона, найдено среднеквадратичное отклонение выборки, показано подобие выборки математическим и графическим методом.

Кроме этого были получены:

- звездная матрица для сети LiveJournal, полученная на основе собранной статистики в виде трехместного предиката и отражающие взаимосвязи между узлами сети;

- матрицы взвешенной центральности и удельного баланса для исследуемой сети, полученные с помощью специально разработанного математического алгоритма и позволяющие определить не только наиболее центральные вершины в анализируемой сети, но и те вершины, которые являются генераторами или потребителями контента;

- микромодель распространения вредоносного контента, циркулирующего в сетях авторских записей, полученная на основе микрофракталов для одного или нескольких типов контента.

3. В третьей главе выпускной квалификационной работы были получены результаты моделирования диффузионного процесса в сети для авторских записей LiveJournal. Узлы заражали в трех различных слоях на основе представленного в разделе микрофрактала. Для сети были получены усредненные графики диффузионного процесса для различных тематик, графики трафика в узлах различного состояния.

Была представлена модель противоборства двух различных контентов, для которых были построены соответствующие графики трафика, риска и шанса, позволяющие оценить, на сколько успешно проходит эпидемия.

4. В четвертой главе были даны рекомендации по регулированию диффузионным процессом и рекомендации по уменьшению деструктивного воздействия в социальной сети для авторских записей LiveJournal. Рекомендации были написаны как для рядовых пользователей, так и для модераторов сайта. А также описаны общие методы регулирования такие как:

- фильтрация трафика;
- фильтрация содержания;
- установление правил;
- гибкие настройки конфиденциальности;

- профилактика в сфере ИБ;
- блокирование информации по тематике;
- временное блокирование узла распространителя;
- временное ограничение функционала сети.

Результаты, представленные в данной выпускной квалификационной работе, являются значимыми для создания научно-методического обеспечения в целях предотвращения распространения вредоносного контента в сети для авторских записей LiveJournal.

## СПИСОК ЛИТЕРАТУРЫ

- 1 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.
- 2 Ahn Y. Analysis of topological characteristics of huge online social networking services / Y. Ahn, S. Han, H. Knak, S. Moon, H. Jeong // 16th International Conference on the World Wide Web. – 2007. – P. 844.
- 3 Alba R.A. graph-theoretic definition of a sociometric clique / R.D. Alba // *Journal of Mathematical Sociology*. – 1973. – P. 126.
- 4 Официальный сайт социальной сети LiveJournal–Электрон. Дан. – Режим доступа: <http://www.livejournal.com>
- 5 Anthonisse J.M. The rush in a directed graph / J.M. Anthonisse // *Technical Report BN*. – Vol. 9. №71. – 1971 – P.194.
- 6 Arnaboldi V. Online Social Networks: Human Cognitive Constraints in Slashdot Personal Graphs / V. Arnaboldi, A. Passarella, M. Conti, R. Dunbar // Waltham: Elsevier Inc. – 2015.– P. 36.
- 7 Ball F. Epidemics with two levels of mixing / F. Ball, D. Mollison, G. Scalia-Tomba // *Annals of Applied Probability*. – 1997. – № 7. – P. 89.
- 8 Karampelas P. Techniques and Tools for Designing an Online Social Network Platform / P. Karampelas // NewHampshire: Hellenic American University.– 2013.– P.38.
- 9 Bar-Yossef Z. Local approximation of PageRank and Reverse PageRank / Z. Bar-Yossef, L.T. Mashiach // *Proceedings CKIM*. – 2008. – P. 38.
- 10 Bauckhage C. Maximum Entropy Models of Shortest Path and Outbreak Distributions in Networks / C. Bauckhage, K. Kersting, F.Hadiji// TU Dortmund University, Dortmund, Germany. – 2015. – P. 234.
- 11 Ben Jabeur L. A social model for Literature Access: Towards a weighted social network of authors / L. Ben Jabeur, L. Tamine, M. Boughanem // CORIA, University Publication Center. – 2010. – P. 451.

- 12 Barabasi A.L. Network medicine: a network-based approach to human disease / A.L. Barabasi // Nat. Rev. Genet. – 2011. – P. 68.
- 13 Barabasi R.A. Emergence of scaling in random networks / R.A. Barabasi // Science. – 2012. – P. 512.
- 14 Carminati B. Security and Trust in Online Social Networks / B. Carminati E. Ferrari, M. Viviani // Morgan&Claypool, 2014. -P. 341.
- 15 Golbeck J. Introduction to Social Media Investigation: A Hands-on Approach / J. Golbeck // Waltham: Elsevier Inc., 2015. -P. 236.
- 16 V. Arnaboldi. Online Social Networks: Human Cognitive Constraints in Facebook and Twitter Personal Graphs / V. Arnaboldi, A. Passarella, M. Conti, R. I.M. Dunbar // Waltham: Elsevier Inc., 2015. -P. 227.
- 17 Carminati B. Security and Trust in Online Social Networks / B. Carminati, E. Ferrari, M. Viviani // Morgan&Claypool. – 2014.– P. 120.[4]
- 18 Benzi M. Ranking Hubs and Authorities Using Matrix Functions / M. Benzi, E. Estrada, C. Klymko // CS Technical Report TR. – 2012. – P. 30.
- 19 Bothorel C. Social network analysis and unpopular content recommendation / C. Bothorel // Review of New Information Technologies (RNIT). – Vol. 5. № 11. – 2011. – P. 49.
- 20 Flake G. Self-organization and identification of Web communities / G. Flake, S.R. Lawrence, C.L. Giles, F.M. Coetzee / IEEE Computer. – 2002. – № 35. – P. 471.
- 21 Golbeck J. Introduction to Social Media Investigation: A Hands-on Approach / J. Golbeck // Waltham: Elsevier Inc. – 2015. – P. 323–326.
- 22 Borodin A. Finding authorities and hubs from link structures on the World Wide Web / A. Borodin, M. Roberts, P. Tsaparas / Proceedings of the 10th International World Wide Web Conference. – 2001. – P. 429.
- 23 Dorogovtsev S.N. Evolution of Networks: From Biological Networks to the Internet and WWW / S.N. Dorogovtsev, J.F.F. Mendes // Oxford University Press. – 2003. – P. 280.

- 24 Duchi J. Efficient Online and Batch Learning Using Forward Backward Splitting / J. Duchi, Y. Singer // Journal of Machine Learning Research. – Vol. 10. № 5. – 2009. – P. 2934.
- 25 Ermakov S.A. 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. – Vol. 10. № 11. – P. 511–514.
- 26 Fouss F. Random-walk computation of similarities between nodes of a graph, with application to collaborative recommendation / F. Fouss, A. Pirotte, J.M. Renders, M. Saerens // IEEE Transactions on Knowledge and Data Engineering (TKDE). – Vol.19.№2. – 2006. – P. 103
- 27 Freeman L.C. Centrality in social networks conceptual clarification / L.C. Freeman // Social Networks. Kauai HI: IEEE. – Vol.1. №3. – 2014. – P. 239.
- 28 Berberich K. Time-aware authority ranking / K. Berberich, M. Vazirgiannis, G. Weikum. - Int. Math. –Vol. 2. №3.– 2005. – P. 332.
- 29 Haythornthwaite C. 2005. Social networks and internet connectivity effects / C. Haythornthwaite // Information, Communication & Society. –Vol. 8.№2. – P. 147.
- 30 Biggio B. Evade Hard Multiple Classifier Systems / B. Biggio, G. Fumera, F. Roli. // Heidelberg. – 2008. – P. 38.
- 31 Bouadjenek M.R. A social web search engine / M.R. Bouadjenek, H. Hacid // WW Panel CNRS.– 2012. – P. 153.
- 32 Bouadjenek M.R. New Social approach for expansion query in web 2.0 / M.R. Bouadjenek, H. Hacid, M. Bouzeghoub // CORIA. – 2011. – P. 148.
- 33 Brin S. N. The anatomy of a large-scale hypertextual Web search engine / S. Brin, L. Page / Complt. Netw. –1998. – P. 117.
- 34 Caldarelli G. Structure of cycles and local ordering in complex networks / G. Caldarelli, R. Pastor-Satorras, A. Vespignani // Eur, Phys. – 2004. – P. 286.
- 35 Cannarella J. Epidemical modeling of online social network dynamics / J. Cannarella, J.A. Spechler // Department of Mechanical and Aerospace Engineering, Princeton University, Princeton, NJ, USA. – 2014. – P.66.

- 36 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. 5829.
- 37 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. – 2010. – № 13. – P. 154.
- 38 База данных статистики по социальным сетям [Электронный ресурс] / <https://drive.google.com/open?id=0BxTtsLdUO4tbUkQwUXpLU1liMG8>, свободный. Загл. с экрана
- 39 Средство визуализации данных. – Электрон. Дан. – Режим доступа: <https://gephi.org/>.
- 40 База данных статистики по социальным сетям [Электронный ресурс]. / <http://konect.uni-koblenz.de/networks/soc-LiveJournal1>, свободный. Загл. с экрана
- 41 Лемешко Б.Ю. Статистический анализ данных, моделирование и исследование вероятностных закономерностей. Компьютерный подход: Монография / Б.Ю. Лемешко, С.Б. Лемешко, С.Н. Постовалов, Е.В. Чимитова. // Новосибирск: Изд-во НГТУ, 2011. – 888 с.
- 42 Casella G. Hypothesis Testing / G. Casella, Roger L. Berger // Statistical Inference, Pacific Grove, CA: Duxbury. – 2002. – P. 660.
- 43 Guenter B. Spam / Archive. // – 2010. – Electron. It is given. – Access mode: <http://untroubled.org/spam/>.
- 44 Freeman L.C. The Development of Social Network Analysis / L.C. Freeman // Empirical Press. – 2004. – P. 30.
- 45 Fronczak A. Higher order clustering coefficients in Barabasi-Albert networks / A. Fronczak, J.A. Holyst, M. Jedynek, J. Sienkiewicz // Physica. – 2002. – P. 694.
- 46 Goodman J. Spam and the ongoing battle for the inbox / J. Goodman, G. V. Cormack, D. Heckerman // ACM Transactions on Internet Technology (TOIT). – Vol. 2. № 5. – 2007. – P. 33.
- 47 Gou L. Social Network Document Ranking / L. Gou, X. L. Zhang, H. H Chen // Proceedings of the 10th annual joint conference on Digital libraries, New York, NY, USA, 2010. – P. 322.

48 Grinyaev S. Russia in global information society: threats, risks and possible ways of their neutralization – Electron. It is given. – Access mode: [http://www.noravank.am/upload/pdf/419\\_ru.pdf](http://www.noravank.am/upload/pdf/419_ru.pdf).

49 Islamgulova V.V. 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. Babadzhyanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – P. 305 –315.

50 Johnson S. Entropic origin of disassortativity in complex networks / S. Johnson, J.J. Torres, J. Marro, M.A. Muñoz // Physical Review Letters. – 2010. – P. 424.

51 Kalashnikov A.O. Attacks to information and technological infrastructure of crucial objects: assessment and regulation of risks: Monograph / A.O. Kalashnikov, E.V. Yermilov, O.N. Choporov, K.A. Razinkin, N.I. Barannikov; under the editorship of the Member correspondent of RAS D.A. Novikov. – Voronezh: Scientific Book publishing house. – 2013. – P. 150 – 160.

52 Lauritzen S.L. Local computations with probabilities on graphical structures and their application in expert systems / S.L. Lauritzen, D.J. Spiegelhalter. // Journal Royal Statiltical Society B. – Vol. 50. – 1988. – P. 135.

53 Albert R. Error and attack tolerance of complex networks / R. Albert, H. Jeong, A.L. Barabási // Nature. – Vol. 406. № 2000. – P. 382.

54 Meo P. De. Finding Similar Users in Facebook, Social Networking and Community Behavior Modeling: Qualitative and Quantitative Measurement / P. De. Meo, E.Ferrara, G.Fiumara // IGI Global. – 2011. – P. 304.

55 Mislove A.E. Measurement and Analysis of Online Social Networks/ A.E. Mislove // Houston, Texas: RICE University. – 2008. – P. 140.

56 Mislove A.E. Online Social Networks: Measurement, Analysis, and Applications to Distributed Information Systems / A.E. Mislove // Houston, Texas: RICE University. – 2009. – P. 340.

57 Moreno Y., CostaL.F. The role of centrality for the identification of influential spreaders in complex networks / Y.Moreno, L.F. Costa // New York, USA. – 2014. – P.130.

- 58 Navarro E. Community detection in a bipartite graph and its application to the automatic classification of web search results (Kodex System) / E. Navarro, Y. Chudy, B. Gaume // Mathematics and Computer Science Approaches, Toulouse, France. – 2010. – P. 343.
- 59 Newman M. E. Finding and evaluating community structure in networks / M.E. Newman, M.J. Girvan // Phys. Rev. E 69. – 2004. – P. 58.
- 60 Newman M.E. The Physics of Networks / Physical Today. – 2008. – P. 23–37.
- 61 Newman M.E. The spread of epidemic disease on networks / M.E. Newman // The center of Study of Complex Systems, University of Michigan. – 2002. – P. 214.
- 62 Ostapenko A.G. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 154–176.
- 63 Ostapenko G.A. 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. – Vol. 3. №25. – P. 405–420.
- 64 Ostapenko G.A. 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. – Vol. 3. №25. – P. 410–415.
- 65 Ouyang T.Y., Leveraging Temporal Features for Link Prediction in Communication Networks / T.Y. Ouyang // Massachusetts Institute of Technology, DHS Summer Internship Report. – 2007. – P. 612.
- 66 Prakash B.A. Threshold Conditions for Arbitrary Cascade Models on Arbitrary Networks, Knowledge and Information Systems manuscript // B.A. Prakash, D. Chakrabarti, N. Valler, M. Faloutsos, C. Faloutsos // Review of New Information Technologies (RNIT). – 2012. – P. 30.

67 Radko N.M. 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. 1784 – 1784.

68 Radko N.M. 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. 3. №5. – P. 296–313.

69 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. № 5. – P. 655–661.

70 Sullivan T. The myth of spam volatility – Electron. It is given. – Access mode: <http://www.qaqd.com/research/mit04sum.html>.

71 Tsvetovat M. Social Network Analysis for Startups: Finding Connections on the Social Web / M. Tsvetovat // O'Reilly.– 2011. – P. 192.

72 Woo J. Epidemic model for information diffusion in web forums: experiments in marketing exchange and political dialog / J. Woo, H. Chen // Graduate School of Information Security, Korea University, Anam-ro, Seoul, Korea. – 2016. – P. 19.

73 Zhang Z. Modeling Epidemics Spreading on Social Contact Networks / Z. Zhang, H. Wang, C. Wang, H. Fang // IEEE Transactions on Emerging Topics in Computing, USA.– 2014. – P. 419.

74 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, 2011. – ч. IV. – С. 178–182.

75 Абрамов К. Г. Распространение нежелательной информации в социальных сетях Интернета / К.Г. Абрамов, Ю.М. Монахов // Труды НТС. Комитет по информатизации, связи и телекоммуникациям, 2014. – 128 с.

76 Бондаренко С.В. Социальная система киберпространства / С.В. Бондаренко // Информационное общество, 2002. – Вып.1. – С.61–64.

- 77 Бреер В.В. Стохастические модели социальных сетей / В.В. Бреер // Управление большими системами, 2009. – 204 с.
- 78 Абрамов К.Г. Модели распространения вредоносных программ в топологических гетерогенных социальных сетях / К.Г. Абрамов, Ю.М. Монахов // Труды НТС. Комитет по информатизации, связи и телекоммуникациям Администрации Владимирской области, 2010. – 382 с.
- 79 Громов Ю.Ю. Анализ живучести информационных сетей / Ю.Ю. Громов // Информационные процессы и управление, 2006. – С. 138–155.
- 80 Додонов А.Г. Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. // Тюмень: Научный дом, 2011. – 256 с.
- 81 Черняк Л.М. Сервисы и теории социальных сетей / Л. М. Черняк // Открытые системы. СУБД, 2008.– № 8. – 78 с
- 82 Губанов Д.А. Модели информационного влияния и информационного управления в социальных сетях / Д. А. Губанов, Д. А. Новиков А. Г. Чхартишвили // Проблемы управления в социальных медиа, 2009. – 120 с.
- 83 Губанов Д.А. Социальные сети: модели информационного влияния, управления и противоборства /Д.А.Губанов, Д.А.Новиков, А.Г. Чхаратишвили; под ред. чл.-корр. РАН Д.А. Новикова. – М.: Издательство физико-математической литературы, 2010. – 288с.
- 84 Гузев Ю.Н. Применение метрик сети для обоснования критерия оценки сетевого конфликта / Ю.Н. Гузев, А.Л. Линец, Е.Ю. Чапурин // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем: Сб. науч. тр.; под ред. чл.-корр. РАН В.И. Борисова, 2015. – Вып. 2 – С. 10–20.
- 85 Ермолова Н.С. Продвижение бизнеса в социальных сетях Facebook, Twitter, Google+. /Н.С. Ермолова. – М.: Альпина Паблишер, 2013. –357 с.
- 86 Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман // Учебное пособие. Высшее образование, 2006. – 243 с.
- 87 Техническая реализация фишинг атаки.–Электрон. Дан. – Режим доступа:<http://www.technicalinfo.net/papers/Phishing.html>.

88 Ковалев С.С. Современные методы защиты от нежелательных почтовых рассылок /С.С.Ковалев, М.Г.Шишаев. – Труды Кольского научного центра РАН,2011.– 20 с.

89 Монахов Ю.М. Аналитическая модель дезинформированной узла социальной сети / Ю.М. Монахов, М.А. Медведникова. – Санкт-Петербург, 2011. – 400 с.

90 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.

91 Тищенко В.И. Социальные сети и виртуальные сетевые сообщества / Л.Н. Верченков, Д.В. Ефременко, В.И. Тищенко // ИНИОН РАН, 2013. – 360 с.

92 Ущерб от фишинга. – Электрон. Дан. – Режим доступа: <http://www.itsec.ru/newstext.php>.