СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный цифровой мир характеризуется большой информационной конфронтацией. Не исключением стали и социальные сети, которые с каждым днем все больше охватывают сферы нашего существования. Множество разнонаправленных социальных сетей предоставляют возможность своим пользователям следить за мировыми новостями, обмениваться фотографиями, видео и музыкой и общаться.

Но иногда возникает потребность не только находить нужную информацию на просторах интернета, но и хранить ее, чтобы в будущем можно было быстро найти ту или иную новость, статью или же нужный для работы или учебы сайт. Можно сказать, что для этого подходит и обычный Интернет-браузер на персональном компьютере, но он имеет сильное ограничение. Ограничение заключается в том, что больше ни с какого другого устройства или персонального компьютера мы не можем получить доступ к ранее сохраненной информации и поделиться ей с другими пользователями не сможем. А, к примеру, если что-либо произойдет с нашим компьютером, заражение вредоносным программным обеспечением (ПО) или же выход из строя жесткого диска, то все сохраненные данные из нашего Интернет-браузера будут потеряны. Это может стать большой проблемой тем пользователями, которые пользуется функцией сохранения в закладки нужной им информацией [1].

В связи с этим, наряду с вышесказанными социальными сетями, существуют специальные веб-сервисы, имеющие название «социальные закладки» (англ., socialbookmarking). У данных веб-сервисов отсутствует вышеописанное ограничение, присущее Интернет-браузерам. Они работают круглосуточно и доступ к сохраненным закладкам можно получить из любой точки мира с любого устройства имеющего доступ в интернет.

Такие сайты позволяют искать нужную информацию в интернете, согласно предпочтениям пользователя. Такой механизм поиска обусловлен выбранными

настройками данного веб-сервиса, к примеру, поиск по категориям и ключевым словам. Также на подобных сайтах присутствует возможность создавать закладки с найденной информацией, чтобы в дальнейшем еѐ можно было легко найти, а также имеется возможность поделиться ей с другими пользователями, чтобы они смогли с помощью выбранного ранее набора закладок найти для себя что-то новое, интересное и полезное [1].

На сегодняшний день существует большое количество сетей социальных закладок, которые находят применение по всему миру.

Однако,довольно часто, из-за своей простоты использования и огромному количеству пользователей, такие веб-сервисы становятся инструментом для продвижения других сайтов или рекламы [2].

С использованием сетей социальных закладок появляется возможность осуществлять большое многообразие действий [2]:

1) создавать и делиться информацией с другими пользователями с минимальными временными задержками, без ограничений (Twitter);

2) принимать участие в обсуждениях новых технологий, политики, науки и многих других тематик (Digg, Slashdot);

3) обмениваться разнообразной литературой (BibSonomy);

4) создавать коллекции изображений и фотографий по интересам или каким-либо событиям (Pinterest);

5) размещать, комментировать и оценивать различные новости (Reddit, Fark);

6) написание собственных новостных статей и получение оценок по выдвинутой на обсуждение проблеме или интересному факту, от других пользователей (NewsVine);

7) обмениваться информацией о популярных трендах в культуре, дизайне, маркетинге и бизнесе (Akonter.com);

8) легко и без временных задержек делиться информацией с друзьями (FriendFeed, Bitly);

9) создание, размещение и пользование ценным контентом и информацией предназначенной для большой аудитории разработчиков специализированного программного обеспечения (DZone).

Это небольшая основная часть возможностей предоставленным пользователям в социальных сетях закладок.

Но, как уже упоминалось ранее, из-за простоты и дешевизны пользования такими сервисами, в сетях социальных закладок может распространяться контент, который имеет возможность тем или иным образом навредить пользователю, который был ознакомлен с ним. Это действие может навредить пользователю данной социальной сети с технической стороны, к примеру, отказ работы Интернет-браузера или его персонального компьютера в результате заражения вредоносным программным обеспечением, или нести психологическое воздействие на пользователя в виде пропаганды террора, наркотиков и т.п. Все вышесказанное зависит он вида распространяемого в социальной сети закладок вредоносного контента.

Таким образом, из вышеприведенной информации можно сделать выводы о возможных рисках при использовании данных веб-сервисов [3]:

1) проявляется вероятность при просмотре закладок других пользователей перейти на сайт с вредоносным контентом, закладка на который была добавлена умышленно;

2) при взломе аккаунта пользователя, который использует данный веб-сервис, злоумышленник может добавить в закладки пользователя сайт с вредоносным контентом или выложить в открытый доступ конфиденциальную информацию о пользователе и его финансовые данные, которые будут видны всем пользователям данной социальной сети;

3) так как данный тип социальных сетей популярен среди друзей, которые часто делятся интересной информацией друг с другом, то появляется вероятность того, что взломают вашего друга и злоумышленник, может отправить вам сообщение, к примеру, ссылку на сайт с вредоносным контентом, и вы ничего не

подозревая, получив эту ссылку от доверенного лица подвергнитесь вредоносному воздействию;

4) в сетях социальных закладок, достаточно много контента представленного программным обеспечением, предназначенного для самых разных нужд. При этом данное программное обеспечение находится в открытом доступе и бесплатно. В связи с этим появляется вероятность скачать с сайта не то ПО, которое вы хотели, а то ПО которое может навредить вашему ПК;

5) пользуясь данными веб-сервисами, можно по неосторожности, добавить в закладки сайты, которые должны были остаться в секрете от других пользователей.

Выше представленные риски при использовании сетей социальных закладок являются основными и наиболее распространенными на сегодняшний день.

В случае если количество данный веб-сервисов будет продолжать расти, то и количество пользователей вследствиеэтого также будет увеличиваться. В связи с этим, количество реализуемых угроз, которые возможны в данном типе социальных сетей, такие как спам, информационно-психологическое воздействие, фишинг, фарминг и другие, с целью получения информации, представляющей интерес злоумышленнику, постоянно растет. Это говорит о широких возможностях для злоумышленников по осуществлению различных деструктивных воздействий [1, 2, 3].

В связи с вышесказанным появляется вероятность того, что вредоносный контент начнет распространяться в самой социальной сети, циркулируя между еѐ узлами (пользователями) тем самым порождая диффузию контента (эпидемический процесс) [4].

На основе приведенными выше высказываниями, можно сказать, что**актуальность темы исследования** обусловлена следующими проблемами:

- активным пользованием людьми социальными сетями;
- вероятным преобладанием вредоносно контента;
- необходимостью всестороннего анализа диффузию контента возникающей в социальных сетях;

– необходимостью обеспечения безопасности пользователям социальных сетей;

– созданием рекомендаций, по противодействию возникающимдиффузии контента.

Таким образом, в данной области исследования необходимо создание научно-методического обеспечения, которое позволит дать рекомендации по управлению и регулированиюдиффузией контента, которая возникают в данном типе социальных сетей.

Степень разработанности темы исследования. Исследование вышеуказанных угроз на данный момент является одним из актуальных направлений как отечественных, так и зарубежный ученых [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16], которые имеют отношение к сетям социальных закладок, распространения вредоносного контента, а также возникновению диффузии контента в социальных сетях. К таким исследованиям относится:

1) общая информация о сетях социальных закладок (ССЗ) (их понятие, разновидности, количество пользователей, приобщенных к ним) [1, 2, 4, 6, 8, 9, 12, 14, 15, 16, 17, 18];

2) наиболее популярные сервисы ССЗ, существующие по всему миру, в том числе и в России [2, 5, 7, 8];

3) история возникновения непосредственно самих ССЗ и в общем контексте социальных сетей[9, 11, 14, 16, 19];

4) статистические данные, отражающие динамику использования нынешних ССЗ среди подписчиков [20, 21, 22, 23, 24, 25];

5) аналитические исследования и опросы на просторах Интернета по данной проблематике [24, 25, 26, 27, 28, 29, 30];

6) преимущества и недостатки ССЗ [7, 9, 23, 27, 31];

7) информация для определения взвешенности графа и ценности его информации [32, 33, 34, 35, 36];

8) сведения, включающие различные модели и метрики [35, 36, 37, 38, 40, 41, 49, 43, 44, 45, 46, 47];

9) сведения о вредоносном контенте, распространяемом в ССЗ, возможные угрозы и риски [31, 41, 43, 48, 49, 50, 51];

10) различные меры и средства противодействия вредоносному контенту [51, 52, 53, 54, 55, 56, 57];

Тем не менее, несмотря на большое количество исследований и работ посвященных социальным сетям, оказалось, что достаточно слабо проработаны вопросы диффузионных процессов протекающих в них, а также вопросы регулирования данных процессов.

Таким образом, необходимость развития и усовершенствования научно-методического обеспечения, основываясь на подробном анализе диффузионных процессов контента и регулирования ими, для обеспечения безопасности пользователей сети социальных закладок остается актуальной.

Объектом исследования является новостная социальная сеть закладокSlashdot, оказывающаяся под воздействием вредоносного контента.

Предметом исследования является микромодель процесса распространения вредоносного контента для социальной сети Slashdot.

Цель исследования состоит в определении того, каким образом социальная сеть Slashdotможет является опасной в случае распространения в ней деструктивного контента.

Для достижения цели необходимо решить следующие задачи:

1) анализ социальной сети Slashdot, выявление всех сетевых ресурсов для размещения контента и их классификация. Классификация разновидности циркулирующего в сети контента, выделение субъектов, функционирующих в сети и установление между этими субъектами функциональных связей;

2) получение различных метрик и матриц (смежности, инцидентности, взвешенной центральности и т.д.);

3) создание вероятностных моделей информационной диффузии;

4) построение модели диффузии контента через вторичные источники его популяризации на основе полученных микромоделей;

5) выделение системы регулирования диффузионными процессами и составление рекомендаций по уменьшению деструктивного воздействия в социальной сети Slashdot.

Результаты, выносимые на защиту. После выполнения данной работы на защиту будут вынесены следующие пункты:

1) звездная матрица социальной сети Slashdot, полученная на основе собранной статистики в виде трехместного предиката и отражающая взаимосвязи между узлами сети;

2) матрицы взвешенной центральности и удельного баланса трафика в вершинах социальной сети Slashdot, полученные с использованием предложенного алгоритма преобразования исходных данных;

3) проранжированная усеченная матрица социальной сети Slashdot, полученная в результате алгоритма осуществления репрезентативной выборки;

4) усеченный граф социальной сети Slashdot;

5) графики трафиковциркулирующих в социальной сети контентовпри моделировании эпидемического процесса;

6) графики противоборства двух типов контентов при моделировании процесса диффузии;

7) рекомендации по регулированию диффузионных процессов для различных типов субъектов.

Новизна результатов:

1) в отличие от аналогов, опираясь на полученные результаты, была представлена выборка социальной сети (усеченный граф), удобная для дальнейшего анализа социальной сети Slashdot;

2) с использованием специально разработанного программного обеспечения, были получены графики циркулирующих трафиков в социальной сети при диффузии одного и двух контентов;

3) были выработаны рекомендации для различных типов субъектов в данной социальной сети, на основе проведенного анализа.

Теоретическая значимость работы. Теоретическая значимость данной работы заключается в:

1) нахождении и доказательстве репрезентативной выборки генеральной совокупности социальной сети Slashdot;

2) построении наглядных графиков циркулирующего в социальной сети трафика различных типов контентов;

3) анализ поведенного моделирования и выработка рекомендаций на основе полученных результатов моделирования.

Практическая ценность результатов. Результаты, выносимые на защиту, обладают следующей практической ценностью:

1) на основе структурно-функциональных особенностей сетей социальных закладок и распространяемого в них вредоносного контента можно выявить характерные признаки деструктивного воздействия вредоносного программного обеспечения, а всесторонний анализ сети в качестве взвешенного графа позволяет определить ущерб вследствие реализации угрозы;

2) анализ звездной матрицы, матриц взвешенной центральности и удельного баланса позволяет определить, как связаны узлы между собой, а также какие из них являются наиболее уязвимыми;

3) моделирование процесса распространения вредоносного контента позволяет определить пути и методы осуществления негативного воздействия, оценить возможный риск реализации угрозы и его параметры.

Методы исследования. В исследовании применяются методы системного анализа, теории вероятностей и математической статистики, теории графов.

ЗАКЛЮЧЕНИЕ

Таким образом, в результате выполнения выпускной квалификационной работы были получены следующие итоги.

В первой части данной работы был дан понятийный аппарат для социальной сети.

Также представлена подробная и всесторонняя классификация контента, циркулирующего в социальной сети Slashdot. В первую очередь его можно рассмотреть, как положительный и негативный (нежелательный).

Также контент может быть представлен в виде текста, изображения, видеофайла или совмещенной форме – гибридной.

Были рассмотрены и подробно описаны сетевые ресурсы данной социальной сети. Они разделяются на ресурсы коллективного пользования (новостная лента, магазин) и на ресурсы персонального пользования (профиль пользователя).

Проклассифицированы объекты данной социальной сети и субъекты, которые с ними взаимодействуют. Было выяснено, что все субъекты с учетом проявления их активности в данной социальной сети можно разделить на активных и пассивных пользователей.

Также было установлено, что субъекты данной социальной сети способны обмениваться контентом между собой посредством определенного набора действий (функций). Набор действий в социальной сети зависит от того авторизован ли пользователь или нет.

С учетом полученных классификаций контента, субъектов и их действий, а также сетевых ресурсов данной социальной сети построена структурно-функциональная модель социальной сети Digg с учетом всех ее особенностей.

В данной модели функциональные связи представляют собой сложную структуру взаимодействия контента, сетевых ресурсов и субъектов, функционирующих в заданном сетевом пространстве.

Во второй части 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 в 5% от генеральной совокупности и графическим методом показано подобие выборки.

В третьей части были получены результаты моделирования диффузионного процесса для сети социальных закладок Digg 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 (восприимчивого, инфицированного, защищенного, умершего, латентного), графики риска и шанса для разных тематик. Исходя из них, было установлено, что данные несильно изменяются при попытке атаки в один из слоев.

Далее была рассмотрена модель противоборства двух различных контентов в трех наиболее опасных с точки зрения тематиках: «Политика», «Социум», «Статьи».

Для них были представлены соответствующие графики трафика, риска и шанса, позволяющие оценить, на сколько эффективно проходит эпидемия благодаря заражению двумя различными видами контента.

В четвертой части были даны рекомендации по регулированию диффузионным процессом и составление рекомендаций по уменьшению деструктивного воздействия социальной сети Digg.

Помимо всего, были получены:

– зведная матрица для сети социальных закладок Digg, полученные на основе собранной статистики в виде трехместного предиката и отражающие взаимосвязи между узлами сети;

– матрицы взвешенной центральности и удельного баланса для сети социальных закладок, 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 социальных закладок, полученная на основе микрофракталов для одного и/или нескольких типов контента.

Эти результаты являются ценной частью для создания научно-методического обеспечения в целях предотвращения распространения вредоносного контента как в сетях социальных закладок, так и во всемирной паутине вообще.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

СПИСОК ЛИТЕРАТУРЫ

1 Назарчук А.В., О сетевых исследованиях в социальных науках / МГУ им. М. В. Ломоносова – М:. Типография МГУ, 2008. – 73 с.

2 Anthonisse J. M., The rush in a directed graph / J.M. Anthonisse // Technical Report BN 9/71. – 1971 p.Ahn Y. Analysis of topological characteristics of huge onlane social networking services / Y. Ahn, S. Han, H. Knak, S. Moon, H. Jeong // 16th International Conference on the World Wide Web. – 2007. – P. 835–844.

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

4 Alba R.A., graph-theoretic definition of a sociometric clique / Richard D. Alba / Journal of Mathematical Sociology. – 1973. – P. 113–126.

5 Borodin A., Finding authorities and hubs from link structures on the World Wide Web / A. Borodin, Roberts, P. Tsaparas / Proceedillgs of the 10th International World Wide Web Conference. – 2001. – P. 415–429.

6 Jennifer Golbeck. Introduction to Social Media Investigation: A Hands-on Approach. Waltham: Elsevier Inc., 2015.– P. 323–326.

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

8 Valerio Arnaboldi, Andrea Passarella, Marco Conti, Robin I.M. Dunbar. Online Social Networks: Human Cognitive Constraints in Slashdot Personal Graphs. Waltham: Elsevier Inc., 2015. – P. 21–36.

9 Barbara Carminati, Elena Ferrari, Marco Viviani. Security and Trust in Online Social Networks. Morgan&Claypool, 2014.– P. 61–82.

10 Бреер В.В., Стохастические модели социальных сетей / В.В. Бреер; Управление большими системами, № 27. – 2009. – С. 169–204.

11 CaldarelliG., Structure of cycles and local ordering in complex networks / G. Caldarelli, R. Pastor-Satorras, A. Vespignani / Eur, Phys. – 2004. – P. 183–186.

12 Додонов А.Г., Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. – Киев: Наукова думка, 2011. – 256 с.

13 Ермолова Н.С., Продвижение бизнеса в социальных сетях Facebook, Twitter, Google+. / М.:АльпинаПаблишер, 2013. – 357 с.

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

15 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.

16 Barabasi R. Albert Emergence of scaling in random networks / Albert R. Barabasi; Science. – 2012. – P. 509–512.

17 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.

18 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.

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

20 F. Fouss, and A. Pirotte, and J.M. Renders, and M. Saerens, Random-walk computation of similarities between nodes of a graph, with application to collaborative recommendation, IEEE Transactions on Knowledge and Data Engineering (TKDE), Vol.19, 2006. – 2007 p. – P. 98–103.

21 L. Gou and X. L. Zhang and H. H Chen and J. H. Kim and C.L. Giles, Social Network Document Ranking, JCDL ’10 Proceedings of the 10th annual joint conference on Digital libraries, New York, NY, USA, 2010, – P. 313–322.

22 P. De Meo And E. Ferrara And G. Fiumara, Finding Similar Users In Facebook, Social Networking And Community Behavior Modeling: Qualitative And Quantitative Measurement, IGI Global, 2011. – P. 304–323.

23 E. Navarro and Y. Chudy and B. Gaume, Community detection in a bipartite graph and its application to the automatic classification of web search results (Kodex System), First day for models and network analysis: Mathematics and Computer Science Approaches: MARAMI, Toulouse, France, 2010. – P. 337–343.

24 T.Y. Ouyang, Leveraging Temporal Features for Link Prediction in Communication Networks, Massachusetts Institute of Technology, DHS Summer Internship Report, 2007. – P. 600–612.

25 PanagiotisKarampelas. Techniques and Tools for Designing an Online Social Network Platform. NewHampshire: Hellenic American University, 2013.– P. 36–38.

26 Brin S. N., The anatomy of a large-scale hypertextual Web search engine / S. Brin, L. Page / Compllt. Netw. – 1998. – P. 107–117.

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

28 Neuman M.E.J. The Physics of Networks / Physical Today (2008), November. – 2008. – P. 23–37.

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

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

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

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

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

34 GuenterB. SpamArchive, 2010. – Электрон.дан. – Режим доступа: http://untroubled.org/spam/.

35 Sullivan T. The myth of spam volatility / T.Sullivan // 2004. – Электрон. дан. – Режимдоступа: http://www.qaqd.com/research/mit04sum.html.

36 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.

37 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.

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

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

40 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.

41 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.

42 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.

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

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

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

46 Fronczak A. Higher order clustering coefficients in Barabasi-Albert networks / A. Fronczak, J.A. Holyst, M. Jedynak, J. Sienkiewicz / PhysicaA316. – 2002. – P. 688–694.

47 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. – 280 p.

48 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.

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

50 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. 141–154.

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

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

53 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.

54 Johnson S. Entropic origin of disassortativity in complex networks / S. Johnson, J.J. Torres, J. Marro, M.A. Muñoz / Physical Review Letters. – 2010. – 4 p.

55 Kauai HI: IEEE. Freeman, L. C. (1979). Centrality in social networks conceptual clarification. Social Networks, 1(3), 2014, – P. 215–239.

56 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. – 160 p.

57 Grinyaev, S. Russia in global information society: threats, risks and possible ways of their neutralization / S. Grinyaev, – Electron. it is given. – Access mode: http://www.noravank.am/upload/pdf/419_ru.pdf.

58 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.

59 Ковалев С. С., Шишаев М. Г. Современные методы защиты от нежелательных почтовых рассылок // Труды Кольского научного центра РАН, 2011 – № 7. – Р. 4–6.

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

61 Социальная сеть Slashdot. – Электрон. Дан. – Режим доступа: http://slashdot.org.

62 Социальная сеть Slashdot – Вопросы и ответы. – Электрон. Дан. – Режим доступа: https://slashdot.org/faq.

63 Статистические данные посещения социальной сети. – Электрон. Дан. – Режим доступа: http://www.alexa.com/.

64 Тищенко В. И. Социальные сети и виртуальные сетевые сообщества / Верченов Л. Н., Ефременко Д. В., Тищенко В. И. / М: ИНИОН РАН, 2013. – 360 с.

65 Абрамов К. Г., Распространение нежелательной информации в социальных сетях Интернета / К.Г. Абрамов, Ю.М. –2014. – С.45–48.

66 Техническая реализация Фишинг атаки.– Электрон. Дан. – Режим доступа: http://www.technicalinfo.net/papers/Phishing.html.

67 Ущерб от фишинга. – Электрон. Дан. – Режим доступа: http://www.itsec.ru/newstext.php?news_id=24180

68 Статистика социальной сети Slashdot. – Электрон. Дан. – Режим доступа: http://konect.uni-koblenz.de/networks/slashdot-zoo.

69 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.

70 Губанов Д.А., Социальные сети: модели информационного влияния, управления и противоборства / Губанов Д.А., Новиков Д.А., Чхаратишвили А.Г. // Проблемы управления в социальных медиа. – 2009. – С. 203–205.

71 Большая Стенфордская Коллекция Сетевых Данных.– Электрон. Дан. – Режим доступа: https://snap.stanford.edu/data/.

72 Средство визуализации данных. – Электрон. Дан. – Режим доступа: https://gephi.org/.

73 Гмурман В.Е., Теория вероятностей и математическая статистика. Учебное пособие. Высшее образование. – Москва, 2006 – С. 243.

74 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.

75 George Casella, Roger L. Berger. Hypothesis Testing // Statistical Inference. – Second Edition. – Pacific Grove, CA: Duxbury, 2002. – 660 p.

76 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.

77 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.

78 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.

79 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.

80 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. 173–176.

81 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.

82 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. – P. 296–313.

83 L. Ben Jabeur and L. Tamine and M. Boughanem, A social model for Literature Access: Towards a weighted social network of authors, CORIA, University Publication Center, 2010. – P. 403–404.

84 C. Bothorel, Social network analysis and unpopular content recommendation, Review of New Information Technologies (RNIT), Vol. A.5, 2011. – P. 41–49.

85 M. R. Bouadjenek and H. Hacid, LAICOS: A social web search engine, WW Panel CNRS, 2012. – P. 24–53.

86 Z. Zhang and H. Wang and C. Wang and H. Fang, Modeling Epidemics Spreading on Social Contact Networks, IEEE Transactions on Emerging Topics in Computing, USA, 2014. – P. 410–419.

87 M. E. J. Newman, The spread of epidemic disease on networks, The center of Study of Complex Systems, University of Michigan, 2002. – P. 201–204.

88 C. Bauckhage and K. Kersting and F.Hadiji, Maximum Entropy Models of Shortest Path and Outbreak Distributions in Networks, TU Dortmund University, Dortmund, Germany, 2015. – P. 213–234.

89 Y. Moreno and L. F. Costa, The role of centrality for the identification of influential spreaders in complex networks, New York, USA, 2014. – P. 48–52.

90 J. Cannarella and J. A. Spechler, Epidemical modeling of online social network dynamics, Department of Machanical and Aerospace Engineering, Princeton University, Princeton, NJ, USA, 2014. – P. 63–66.

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

92 B. A. Prakash and D. Chakrabarti and N. Valler and M. Faloutsos and C. Faloutsos, Threshold Conditions for Arbirtary Cascade Models on Arbitrary Networks, Knowladge and Infarmation Systems manuscript No. KAIS-12-3483R1, 2012. – 30 p.

93 M. R. Bouadjenek and H. Hacid and M. Bouzeghoub and J. Daigremont, New Social approach for expansion query in web 2.0, CORIA, 2011. – P. 41–48.

94 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.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

8 (952) 106-88-60 vk.com/a.projectit a.projectit