ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Сентябрь 2018 Том 6 № 3 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
September 2018 Vol. 6 Iss. 3 ISSN 2307-1303 http://www.itt.sut.ru

ОБЗОР СТЕПЕНИ РАЗРАБОТАННОСТИ ТЕМЫ МОНИТОРИНГА И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Л. А. Виткова[1, 2*]

[1] СПИИРАН, Санкт-Петербург, 199178, Российская Федерация
[2] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
* Адрес для переписки: iskinlidia@gmail.com

Аннотация
В своей работе автор представляет обзор работ и исследований в области мониторинга социальных сетей, информационных конфликтов, противодействия угрозам информационно-психологической безопасности государства. Круг работ, посвященных анализу, обобщению и поиску решения в области информационно-психологической безопасности в социальных сетях весьма ограничен. Хотя, при этом аспекты обеспечения технической информационной безопасности проработаны достаточно полно. **Предмет исследования.** Предметом исследования выступают существующие научные школы, алгоритмы и методики мониторинга и противодействия информационным операциям в сети Интернет. **Метод.** Проведён обзор фундаментальных исследований. **Основные результаты.** Проведено исследование степени разработанности темы, которое показало, что сегодня возникло противоречие между научным обеспечением технических и информационно-психологических аспектов информационной безопасности. **Практическая значимость.** Практическая значимость научных результатов исследования заключается в выборе направления выхода из сложившейся проблемной ситуации. Необходима разработка и практическая реализация современной методологии противодействия информационно-психологическим операциям в сложных социальных медиа и организационно-технических системах, в частности в социальных сетях.

Ключевые слова
информационно-психологическая безопасность, мониторинг социальных сетей, социальные сети, противодействие, контрмеры.

Информация о статье
УДК 316.776.2
Язык статьи – русский.
Поступила в редакцию 21.08.18, принята к печати 03.09.18.

Ссылка для цитирования: Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Том 6. № 3. С. 1–9.

OVERVIEW OF THE INVESTIGATIONS IN THE AREA OF MONITORING AND COUNTERACTION TO THREATS TO INFORMATION-PSYCHOLOGICAL SECURITY IN SOCIAL NETWORKS

L. Vitkova[1, 2*]

[1] SPIIRAS, St. Petersburg, 199178, Russian Federation
[2] SPbSUT, St. Petersburg, 193232, Russian Federation
* Corresponding author: iskinlidia@gmail.com

Abstract—The paper presents an overview of investigations in the field of social networks analysis, information conflicts, countering threats to information and psychological security of the state.
The range of investigations devoted to the analysis, generalization and search for solutions in the field of information and psychological security in social networks is very limited. Although, at the same time aspects of technical information security have been worked out in deep details. **Research subject.** The subject of the investigation is the scientific schools, algorithms and methods of monitoring and counteraction to information operations in the Internet. **Method**. Fundamental investigations are reviewed. **Core results.** The investigation of the developments in the analyzed area showed that today there is a contradiction between the scientific provision of technical, informational and psychological aspects of information security. **Practical relevance.** The practical significance of the investigation results lie in the proposed solutions for the current challenges of the analyzed area. It is necessary to develop and implement a modern methodology for counteraction to information and psychological operations in complex social media and technical systems, in particular in social networks.

Keywords—information and psychological security, monitoring of social networks, social networks, counteraction, countermeasures.

Article info
Article in Russian.
Received 21.08.18, accepted 03.09.18.

For citation: Vitkova L.: Overview of the Investigations in the Area of Monitoring and Counteraction to Threats to Information-Psychological Security in Social Networks // Telecom IT. 2018. Vol. 6. Iss. 3. pp. 1–9 (in Russian).

Введение

Актуальность темы обусловлена тем, что при высоком уровне распространения социальных сетей и отсутствия четких правовых механизмов контроля за ними, политические оппоненты, международные террористические и экстремистские организации, криминальные структуры осознают возможности, которые они могут использовать в рамках информационного противоборства. В информационном пространстве социальных сетей происходит явное и скрытое манипулирование сознанием со стороны различных организаций, групп и стран. Соответ-

ственно, представляется обоснованным говорить об информационно-психологической безопасности государства, как о процессе баланса между возникающими и воздействующими угрозами в информационном пространстве, эффективностью их выявления и нейтрализации.

В своем докладе на форуме «Инфофорум-2017» референт аппарата Совета Безопасности РФ Дмитрий Грибков озвучил основные аспекты информационной безопасности государства, которыми руководствовались члены Совета Безопасности во время подготовки обновленной Доктрины информационной безопасности Российской Федерации [1]. Аспекты были разделены на информационно-технические и информационно-психологические. В настоящее время информационно-технические аспекты информационной безопасности достаточно хорошо проработаны, в то время как, информационно-психологические аспекты нуждаются в дополнительных исследованиях, проектах и работах со стороны специалистов и ученых.

Одновременно с этим одной из фундаментальных научных проблем, решаемых в настоящее время, является разработка методологических основ интеллектуального анализа информационных объектов в информационном пространстве социальных сетей. Современные средства массовых коммуникаций являются информационными системами. При этом в каждой информационной системе есть свои типы объектов, все системы подстраиваются под пользователя, отслеживают активность и вовлеченность, обмениваются данными через единые аналитические площадки. Общество и личность погружены в информационное пространство, в социальные сети, где непрерывно разворачиваются информационно-психологические операции. Целью таких операций в информационном пространстве социальных сетей является усиление влияния и установления контроля за аудиторией. В результате информационных операций одни участники соперничества утрачивают преимущества, другие получают и используют их в дальнейшем развитии.

Процессы и конфликты, протекающие в информационно-психологическом поле государства, являются отражением на эту сферу политической активности различных государств, отдельных групп, объединений или иных субъектов деятельности современного информационного общества. При этом обратные процессы также имеют силу. То есть конфликты и процессы в информационно-психологическом поле государства могут порождать события и конфликты групп, меняющие общество в целом. Важно то, что информационно-психологические процессы, порождающие изменения состояния безопасности государства и общества в интересах противника, протекают, как правило, в скрытой (латентной) форме и мы обнаруживаем результат воздействия на информационно-психологическое поле со стороны противника, только в момент его кульминации, когда противник достиг цели. Поэтому создание новых элементов систем мониторинга, обнаружения и противодействия информационно-психологическим операциям в пространстве социальных сетей представляется актуальным.

Степень разработанности темы

В основу процесса формирования методологии теории информационного противоборства в информационной сфере государства легли теории радиоэлектронной борьбы и информационной безопасности. Но, одновременно с этим,

создание и развитие научно-методического аппарата информационного противоборства тесно связано с такими науками, как политология, социология, психология, в частности с методологией исследований информационного конфликта.

Сегодня ведутся исследования по развитию методологии информационного конфликта в психологической и социально-политических сферах. В монографии А. Г. Чхартишвили и Д. А. Новикова «Модели влияния в социальных сетях» дается обзор моделей влияния в социальных сетях, авторы рассматривают воздействие на целевую аудиторию «лидеров мнений», блогеров, журналистов [2]. В работах Д. А. Губанова, В. В. Цыганова, С. Н. Бухарина, М. В. Литвиненко, С. П. Расторгуева и других подробно рассматривались модели информационного конфликта [3, 4, 5, 6]. В трудах и монографиях И. М. Левкина тщательно проработаны информационно-признаковое моделирование угроз национальной безопасности [7, 8, 9]. Генерал-полковник милиции Б. Н. Мирошников в своих работах, например, в монографии «Сетевой фактор. Интернет и общество», рассуждает об отсутствии авторства, морали и правовых законодательных основ в информационной сфере и пишет о том, что информационная война не имеет ни границ, ни адресов. А временная «нулевая» отметка известна лишь тому, кто ее начал [10].

Процесс конвергенции естественно-научного и социально-гуманитарного знания необходим для дальнейшего научно-технологического развития информационной безопасности государства и общества в целом. Поэтому в анализе современного состояния исследований в данной работе мы отталкиваемся от того, что для успешного достижения цели необходимо опираться как на технические достижения, так и на социо-гуманитарные.

Научные исследования, направленные на обнаружение и противодействие информационно-психологическим воздействиям, могут быть разделены на несколько областей.

К технической области относятся:

1. Методы сбора и хранения данных.
2. Методы интеллектуального анализа данных.
3. Методы визуализации данных и поддержки принятия решений.
4. Системы мониторинга информационного пространства сети Интернет.

К социо-гуманитарной области относятся:

1. Правовые аспекты информационной безопасности в сети Интернет.
2. Методы анализа влияния массовых коммуникаций.
3. Методы анализа информационно-психологических операций.
4. Методы противодействия информационно-психологическим операциям.

Анализ современных исследований в области мониторинга информационного пространства, методов сбора и хранения данных показывает, что прежде всего ученые решают технические вопросы оптимизации систем хранения, повышения производительности и разработки алгоритмов работы с большими данными, активно рассматриваются подходы к анализу социальных сетей.

Общий подход к мониторингу и классификации веб-страниц был представлен И. В. Котенко, А. А. Чечулиным и др. в [11]. Данный подход был основан на анализе различных аспектов веб-страниц для определения тематической направленности. Основным аспектом, который использовался для определения категории, был текст веб-страницы. Однако, в результате экспериментов, авторы

пришли к выводу, что использование текста не подходит для анализа таких категорий веб-сайтов как «новости», «блоги», «социальные сети» и др. Это обусловлено тем, что веб-страницы данных категорий могут содержать одновременно тексты, посвященные различной тематике. Для выявления таких категорий было предложено использовать структурные особенности веб-страниц. Общий подход, объединяющий анализ текстового содержимого, структурных особенностей и URL адреса представлен в [12, 13]. Данный подход, позволяет с достаточно высокой точностью определять категорию веб-страницы, что было доказано результатами экспериментов. Однако, при работе с категорией «социальные сети» было обнаружено, что важной информацией является не только категория конкретного информационного объекта (сообщения, группы и т. д.), но и пути распространения данной информации. Выявление источников и ретрансляторов информации позволяет значительно повысить эффективность методов противодействия.

Социальные сети сегодня в сети Интернет являются не только средством общения, но и инструментом маркетинга, рекламы и социальных исследований. Takeshi Sakaki, Makoto Okazaki, Yutaka Matsuo в своих работах в 2013 году описывали системы быстрого обнаружения и оповещения о землетрясениях, основанные на анализе сообщений из микроблогов «Твиттера» [14]. Adam Sadilek, Henry A. Kautz, Vincent Silenzio еще в 2012 году показали возможность использования социальных сетей для обнаружения эпидемий гриппа и прогнозировании его распространения [15].

L. Zaden и др. [16] говорят о том, что анализ недостающих узлов в связях, которые возникают или только могут возникнуть в социальных сетях, может повысить эффективность прогнозов и моделирования развития событий. В [17] авторы опираются на анализ нечетко структурированных динамических систем, для визуализации при анализе используют граф, но цель проанализировать потоки или повысить качество представления информации на графе перед собой не ставят.

A. Barabasi et al. [18] нашли связь между объектами социальной сети и проанализировали закон распределения связей между узлами. Показали, что узлы в сетях связаны асимметрично, для социальной сети справедливо распределение узлов по числу связей в виде степенного закона (безмасштабное распределение узлов по числу связей), т. е., в такой сети отсутствуют узлы с типичным числом связей (*Scale-free networks*).

Также значимые научные работы – это исследования взаимовлияния объектов социальной сети (в том числе подходы, основанные на использовании понятий «структурные пустоты», «информационный купол») [19] и информационных каскадов [20] и др.

Активно развивается такое направление, как социально-сетевой анализ (SNA). Социально-сетевой анализ – это способ изучения социальных сетей, как набора сущностей, между которыми есть определенные отношения. В SNA величина позитивной корреляции узла социальной сети характеризуется такими индикаторами, как степень (*degree*), собственный вектор (*eigenvector*), мера близости (*closeness*) и центральность к посредничеству (*betweenness-centrality*). Таким образом, в процессе анализа выделяют наиболее популярные (влиятельные) узлы и их связи с другими объектами. T. Opsahl и др. [19] описывают социальную

связанность с использованием трех различных индексов: центральная степень (*Degree centrality*), как показатель распределения уровня власти и влияния в сети, близость узла к центру сети, его взаимосвязь с центром других узлов.

Методы, опирающиеся на анализ контента, довольно широко используют методы машинного обучения, среди подходов основанных на анализе социальных графов машинное обучение также набирает популярность.

На базе ИСП РАН в рамках проекта под руководством Д. Ю. Турдакова и С. Д. Кузнецова разработаны аналитические системы «Текстера» и «Талисман». Были разработаны модель и оригинальный метод для генерации случайных графов, обладающих основными свойствами социальных сетей (распределение степеней, диаметр, коэффициент кластеризации и т. д.) и заданной структурой сообществ пользователей. Для реализации использовались существующие технологии и алгоритмы Больших данных. Система «Талисман» может вычислять и прогнозировать эпидемии гриппа, анализировать демографические параметры социальных сетей. Но система не разрабатывалась для мониторинга информационной безопасности государства, поиска источников атаки, ретрансляторов, анализа нарушений и не была адаптирована [21].

G. Attardi и A. Gulli предложили использовать метод анализа URL для управления информационной сферой. Авторы исходят из предположения, что страницу в Интернете будут редко посещать, если ее адрес не отражает каким-то образом его тематику [22].

Среди исследований, выделяются методы анализа эмоциональной окраски текстовых сообщений. В последние годы были предложены не привязанные к конкретным веб-сайтам или системам комментирования методы для решения задачи автоматического извлечения комментариев. В данном направлении следует выделить работы H. A. Kao, H. H. Chen [23], J. Barua, D. Patel, V. Goyal [24].

Отдельно стоит сказать о том, что анализ состояния исследований в области информационной безопасности показывает: современные работы в основном направлены на обеспечение нормативно-правовых или информационно-технических аспектов информационной безопасности в сети Интернет. Например, на мониторинг информационных систем, анализ качественных или количественных характеристик связей узлов в социальных сетях, кластеризацию полученных данных, систематизацию, хранение и прочее.

В то же время модели, методы, методики и алгоритмы в области обеспечения информационно-психологических аспектов информационной безопасности разработаны недостаточно. В частности, задача разработать информационно-признаковые модели воздействия нарушителя в сети интернет, проанализировать каналы распространения информации, разработать методики противодействия информационно-психологическим операциям в современных работах не ставилась.

Заключение

Возникло **противоречие** между научным обеспечением технических и информационно-психологических аспектов информационной безопасности. Направлением выхода из сложившейся проблемной ситуации является разра-

ботка и практическая реализация современной методологии противодействия информационно-психологическим операциям в сложных социальных медиа и организационно-технических системах, в частности в социальных сетях.

Работа проводилась при поддержке гранта РНФ 18-11-00302.

Литература

1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

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

3. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Модели репутации и информационного управления в социальных сетях // Управление большими системами. 2009. № 26.1. С. 209–234.

4. Цыганов В. В., Бухарин С. Н. Информационные войны в бизнесе и политике: Теория и методология. М.: Академический Проект, 2007. 336 с.

5. Расторгуев С. П., Литвиненко М. В. Информационные операции в сети Интернет. М.: АНО ЦСОиП, 2014. 128 с.

6. Расторгуев С. П. Математические модели в информационном противоборстве. Экзистенциальная математика. М.: АНО ЦСОиП, 2014. 260 с.

7. Левкин И. М., Борщенко В. В. Информационные свойства геополитического пространства // Геополитика и безопасность. 2017. № 4 (40). С. 39–45.

8. Левкин И. М., Науменко К. А., Виткова Л. А. Особенности информационно-психологического воздействия в интернете // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР). 2017. С. 365–367.

9. Левкин И. М., Микадзе С. Ю. Добывание и обработка информации в деловой разведке. СПб.: ИТМО, 2015. 460 с.

10. Мирошников Б. Н. Сетевой фактор. Интернет и общество. Взгляд. М.: Инфорос, 2012. 208 с.

11. Kotenko, I., Chechulin, A., Shorov, A., Komashinsky, D. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking // Lecture Notes in Computer Science. 2014. Vol. 8557. pp. 39–54.

12. Novozhilov, D, Kotenko, I., Chechulin, A. Improving the Categorization of Web Sites by Analysis of HTML-Tags Statistics to Block Inappropriate Content // 9th International Symposium on Intelligent Distributed Computing. 2016. pp. 257–263.

13. Kotenko, I., Chechulin, A., Komashinsky, D. Categorization of Web Pages for Protection against Inappropriate Content in the Internet // International Journal of Internet Protocol Technology. 2017. Vol. 10. Iss. 1. pp. 61–71.

14. Sakaki, T., Okazaki, M., Matsuo, Y. Tweet Analysis for Real-Time Event Detection and Earthquake Reporting System Development // IEEE Transactions on Knowledge & Data Engineering. 2013. Vol. 25. pp. 919–931.

15. Sadilek, A., Kautz, H. A., Silenzio, V. Modeling Spread of Disease from Social Interactions // Sixth International Conference on Weblogs and Social Media (ICWSM). 2012.

16. Zadeh, L., Abbasov, A., Shahbazova, S. Fuzzy based Techniques in Human like Processing of Social Network Data // International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2015. Vol. 23. No. Suppl. 1. pp. 1–14.

17. Zhang, E., Wang, G., Gao, K., Zhao, X., Zhang, Y. Generalized Structural Holes Finding Algorithm by Bisection in Social Communities // 6th International Conference on Genetic and Evolutionary Computing. 2013. pp. 276–279.

18. Barabasi, A., Bonabeau, E. Scale-Free Networks // Scientific American Journal. 2003. Vol. 288. Iss. 5. pp. 50–59.

19. Opsahl, T., Agneessens, F., Skvoretz, J. Node centrality in weighted networks: Generalizing degree and shortest paths // Social Networks Journal. 2010. Vol. 32. Iss. 3. pp. 245–251.

20. Liu, Q., Zhang, L. Information Cascades in Online Reading: An Empirical Investigation of Panel Data // Library Hi Tech Journal. 2016. Vol. 32. Iss. 4. pp. 687–705.

21. Трофимович Ю. С., Козлов И. С., Турдаков Д. Ю. Подходы к определению основного места проживания пользователей социальных сетей на основе социального графа // Труды Института системного программирования РАН. 2016. Т. 28. Вып. 6. С. 185–196.

22. Attardi, G., Gulli, A., Sebastiani, F. Automatic Web Page Categorization by Link and Context Analysis // 1st European Symposium on Telematics, Hypermedia and Artificial Intelligence (THAI). 1999. pp. 105–119.

23. Kao, H. A., Chen, H. H. Comment Extraction from Blog Posts and its Applications to Opinion Mining // Seventh international conference on Language Resources and Evaluation (LREC). 2010.

24. Barua, J., Patel, D., Goyal, V. TiDE: Template Independent Discourse Data Extraction // Lecture Notes in Computer Science. 2015. Vol. 9263. pp. 149–162.

References

1. Presidential Decree of 05.12.2016 No. 646 "On approval of the Information Security Doctrine of the Russian Federation" // SZ RF. 2016. № 50. Art. 7074.

2. Gubanov, D., Novikov, D., Chkhartishvili, A. Social Networks: Models of Information Influence, Control and Confrontation. M.: Fizmatlit, 2010. 228 p.

3. Gubanov, D., Novikov, D., Chkhartishvili, A. Models of Reputation and Information Control in Social Networks // Large-Scale Systems Control. 2009. No. 26.1. pp. 209–234.

4. Tsyganov, V., Bukharin, S. Information Wars in Business and Politics: Theory and Methodology. M.: Akademicheskiy Proekt, 2007. 336 p.

5. Rastorguev, S., Litvinenko, M. Information Operations on the Internet. M.: ANO TsSOiP, 2014. 128 p.

6. Rastorguev, S. Mathematical Models in Information Confrontation. Existential Mathematics. M.: ANO TsSOiP, 2014. 260 p.

7. Levkin, I., Borshchenko, V. Information Properties Geopolitical Space // Geopolitika i bezopasnost'. 2017. No. 4 (40). pp. 39–45.

8. Levkin, I., Naumenko, K., Vitkova, L. The Features of Information-Psychological Influence on the Internet // X St. Petersburg Interregional Conference "Information Security of Russian Regions" (ISRR). 2017. pp. 365–367.

9. Levkin, I., Mikadze, S. Mining and Processing of information in BI Service. SPb.: ITMO, 2015. 460 p.

10. Miroshnikov, B. Network Factor. Internet and Society. View. M.: Inforos, 2012. 208 p.

11. Kotenko, I., Chechulin, A., Shorov, A., Komashinsky, D. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking // Lecture Notes in Computer Science. 2014. Vol. 8557. pp. 39–54.

12. Novozhilov, D, Kotenko, I., Chechulin, A. Improving the Categorization of Web Sites by Analysis of HTML-Tags Statistics to Block Inappropriate Content // 9th International Symposium on Intelligent Distributed Computing. 2016. pp. 257–263.

13. Kotenko, I., Chechulin, A., Komashinsky, D. Categorization of Web Pages for Protection against Inappropriate Content in the Internet // International Journal of Internet Protocol Technology. 2017. Vol. 10. Iss. 1. pp. 61–71.

14. Sakaki, T., Okazaki, M., Matsuo, Y. Tweet Analysis for Real-Time Event Detection and Earthquake Reporting System Development // IEEE Transactions on Knowledge & Data Engineering. 2013. Vol. 25. pp. 919–931.

15. Sadilek, A., Kautz, H. A., Silenzio, V. Modeling Spread of Disease from Social Interactions // Sixth International Conference on Weblogs and Social Media (ICWSM). 2012.

16. Zadeh, L., Abbasov, A., Shahbazova, S. Fuzzy based Techniques in Human like Processing of Social Network Data // International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2015. Vol. 23. No. Suppl. 1. pp. 1–14.

17. Zhang, E., Wang, G., Gao, K., Zhao, X., Zhang, Y. Generalized Structural Holes Finding Algorithm by Bisection in Social Communities // 6th International Conference on Genetic and Evolutionary Computing. 2013. pp. 276–279.

18. Barabasi, A., Bonabeau, E. Scale-Free Networks // Scientific American Journal. 2003. Vol. 288. Iss. 5. pp. 50–59.

19. Opsahl, T., Agneessens, F., Skvoretz, J. Node centrality in weighted networks: Generalizing degree and shortest paths // Social Networks Journal. 2010. Vol. 32. Iss. 3. pp. 245–251.

20. Liu, Q., Zhang, L. Information Cascades in Online Reading: An Empirical Investigation of Panel Data // Library Hi Tech Journal. 2016. Vol. 32. Iss. 4. pp. 687–705.

21. Trofimovich, Yu., Kozlov, I., Turdakov, D. Approaches to Estimate Location of Social Network Users based on Social Graph // Trudy ISP RAN. 2016. Vol. 28. Iss. 6. pp. 185–196.

22. Attardi, G., Gulli, A., Sebastiani, F. Automatic Web Page Categorization by Link and Context Analysis // 1st European Symposium on Telematics, Hypermedia and Artificial Intelligence (THAI). 1999. pp. 105–119.

23. Kao, H. A., Chen, H. H. Comment Extraction from Blog Posts and its Applications to Opinion Mining // Seventh international conference on Language Resources and Evaluation (LREC). 2010.

24. Barua, J., Patel, D., Goyal, V. TiDE: Template Independent Discourse Data Extraction // Lecture Notes in Computer Science. 2015. Vol. 9263. pp. 149–162.

Виткова Лидия Андреевна – младший научный сотрудник,
СПИИРАН, Санкт-Петербург, 199178;
старший преподаватель, СПбГУТ,
Санкт-Петербург, 193232
Российская Федерация, iskinlidia@gmail.com

Vitkova Lidiya – Research Assistant, SPIRAS, St. Petersburg, 199178;
Senior Lecturer, SPbSUT, St. Petersburg, 193232,
Russian Federation, iskinlidia@gmail.com