

Д. В. Ландэ, д-р техн. наук,

В. А. Додонов,

Т.В. Коваленко

Ин-т проблем регистрации информации НАН Украины

(Украина, 03113, Киев, ул. Шпака, 2,

тел. (044) 456 83 89, e-mail: dwlande@gmail.com)

Информационные операции в компьютерных сетях: моделирование, выявление, анализ

The models of information dissemination allowing to recognition of information operations are considered. The architecture of system of identification of information operations in network media, methodology of analytical research which is based on the use of tools of the analysis and visualization of information streams and network structures is presented.

Ключевые слова: информационные операции, поддержка принятия решений, информационное пространство, контент-мониторинг.

Введение. Информационная операция является компонентой информационной войны, содержание которой направлено на реализацию предварительно спланированных психологических воздействий на враждебную, дружескую или нейтральную аудиторию путем информационного влияния на установки и поведение с целью достижения заранее определенных преимуществ [1]. Поле боя современных информационных операций распространяется на глобальные компьютерные сети, где формируются многочисленные информационные потоки. В результате анализа поведения тематических информационных потоков, были выявлены типичные, базовые профили их поведения [2], например, когда после быстрого информационного всплеска подготовки следует плавный спад (публикации о стихийных бедствиях), или, напротив, предполагается длительная информационная подготовка, после чего идет резкий спад (публикации об планируемых заранее мероприятиях). Существуют тематические потоки, характеризующиеся симметричной кривой динамики, как узкие, кратковременные, так и растянутые во времени.

Модель распространения информации. Для создания мультиагентной модели распространения информации, прежде всего, необходимо сформировать близкое к реальности виртуальное информационное пространство, населенное виртуальными агентами, с которыми ассоциируются отдельные документы. Предполагается, что отдельные агенты могут:

- 1) самозарождаться;
- 2) порождать новых агентов;
- 3) «умирать» – исчезать из пространства агентов;
- 4) получать ссылки от других агентов.

Агент обладает «потенциалом», зависящим от его возраста, авторитетности (ссылок на него) и плодовитости (количества порожденных им агентов).

Варьирование четырьмя параметрами управления позволили смоделировать профили поведения информационных сюжетов. В результате проведенных исследований была реализована программа эволюции пространства агентов, исследована эволюция мультиагентной системы, найдены аналогии с реальными тематическими информационными потоками. Были выявлены статистические закономерности, относящиеся к жизненному циклу отдельных сообщений,

распределение которых, соответствует распределению Вейбулла. Данные моделирования были проверены путем исследования реальной сети микроблогов Twitter [3]. Совпадение результатов моделирования и параметров распределения реальной сети позволяют говорить о закономерности, присущей реальным сетям, а также об адекватности модели.

Фазы информационной операции. Предполагается, что системное нарушение типовой динамики некоторых информационных сюжетов в открытом информационном пространстве может свидетельствовать об информационных операциях [4]. При этом следует ориентироваться на этапы информационных атак (рис. 1), и при этом уже по первым трем можно с большой вероятностью предсказать будущие события [5].

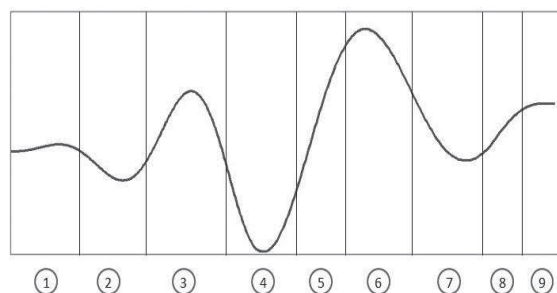


Рис. 1 – Обобщенная диаграмма, соответствующая всем этапам жизненного цикла информационных операций: 1 – фон; 2 – затишье; 3 – «артподготовка»; 4 – затишье; 5 – атака/триггер роста; 6 – пик завышенных ожиданий; 7 – утрата иллюзий; 8 – общественное осознание; 9 – продуктивность/фон

Приведенные зависимости могут быть использованы в качестве шаблонов для выявления информационных операций. Достоинством этого метода, является простота его реализации, а главный недостаток заключается в том, что с их помощью информационную операцию можно надежно распознать лишь на ее финальной стадии. Как расширение данной мультиагентной модели распространения информации можно рассматривать модель, в которой учитывается структура формируемой сети [6]. В рамках этой модели каждый агент – источник информации, а связи в сети агентов – факты перепечатки или «пересказа». В основе модели лежит предположение, что при проведении информационных операций наиболее рейтинговые источники перепечатывают информацию у наименее рейтинговых, или образуются кластеры низкорейтинговых источников, перепечатывающих одну и ту же новость. В рамках формализации этой модели выбирается несколько десятков параметров топологии сетей распространения информации, которые сравниваются с некоторыми эталонными значениями. К достоинствам модели следует отнести ее формальную строгость и соответствие активно развивающемуся направлению Complex Networks, а к недостаткам – малую корреляцию с содержательной стороной информационных операций, а также вычислительную сложность.

Система выявления информационных операций. В качестве основных задач такого класса систем рассмотрим:

- построение сценариев противодействия деструктивным информационным воздействиям на основе онтологии понятий предметной области объекта атаки;

- контент-мониторинг информационного пространства на основе знаний экспертов, заложенных в такую онтологию;
- выявление трендов и аномалий в тематических информационных потоках;
- выявление внешних информационных воздействий;
- прогнозирование развития ситуаций;
- выработка сценариев возможных информационных противодействий.

Для решения приведенных выше задач, предполагается, что система информационной поддержки должна состоять из трех основных подсистем, а именно: подсистемы создания онтологии понятий предметной области, подсистемы мониторинга информационного пространства, подсистемы аналитической обработки.

Пример. Ниже приведены результаты экспресс-анализа тематического информационного потока, соответствующего объекту – Национальной академии наук Украины, с учетом рисков, которым она подвергалась во второй половине 2015 года. В результате анализа средствами системы контент-мониторинга InfoStream был сформулирован запрос за период с 01.07.2015 по 31.12.2015, в результате отработки которого был получен тематический информационный поток объемом 1932 документа из украинского сегмента веб-пространства. Для выявления информационных операций доступными аналитическими средствами анализировалась динамика публикаций по целевой тематике (рис. 2).

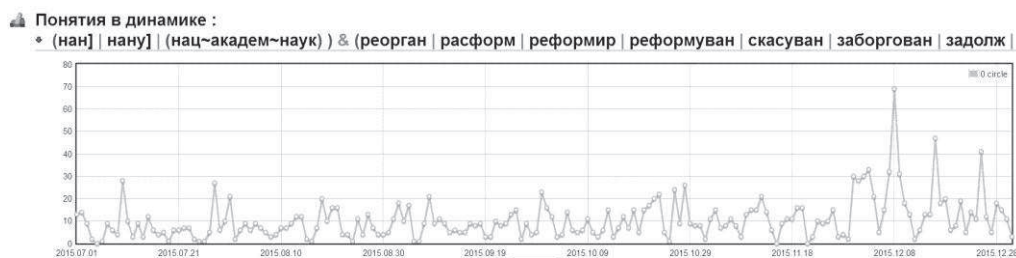


Рис. 2. Динамика тематического информационного потока

Для выявления степени «близости» фрагментов исследуемого временного ряда диаграмме информационной операции в различных масштабах предлагается использовать «вейвлет-анализ», который в настоящее время нашел применение как в естественных науках, так и в социологии [8]. Вейвлет-коэффициенты показывают, насколько поведение процесса в данной точке аналогично вейвлету в данном масштабе. На вейвлет-скейлограмме (рис. 3) видны все характерные особенности исходного ряда: масштаб и интенсивность периодических изменений, направление и значение трендов, наличие, расположение и продолжительность локальных особенностей. В работе [9] показано, что вейвлеты «мексиканская шляпа» и Морле наиболее точно отражает динамику информационных операций. После определения критических точек с помощью системы контент-мониторинга выполняется построение основных сюжетных цепочек из сообщений, соответствующих запросу за выбранные даты. Таким образом определяются основные события за указанные даты:

- *Национальную академию наук хотят пустить по ветру... (Vector News) 2015.12.03*
- *Під Радою мітингують молоді вчені (Левый берег) 2015.12.08*
- *Український уряд руйнує українську науку (2000.ua) 2015.12.08*

- **"У науки - связаны руки": возле АП митингуют сотрудники НАН Украины (УНИАН) 2015.12.16**

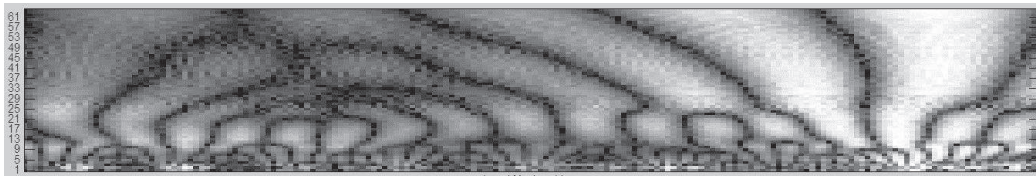


Рис.3. Вейвлет спектрограмма (вейвлет Морле) рассматриваемого информационного потока

Проведенный анализ, в частности, показывает, что в отношении НАН Украины ведется целенаправленная информационная операция, противодействие которой широко отражается в информационном пространстве страны.

Заключение. В работе в качестве методологической основы детектирования информационных операций предложено исследование динамики информационных потоков.

Предложена архитектура системы выявления и анализа информационных операций, базирующаяся на онтолого-управляемом подходе.

Предложенная методика позволяет решить сформулированную задачу, ее можно использовать в качестве основы для проведения аналитической и прогнозной деятельности на основе исследования контента современных компьютерных сетей. В дальнейшем на основе полученных результатов планируется разработка моделирующего комплекса.

1. *Information operations roadmap.* – DoD US. – Washington, D.C.: GPO, 2003.
2. *Додонов А.Г., Ландэ Д.В.* Методика аналитического исследования динамики событий на основе мониторинга веб-ресурсов сети Интернет // Информационные технологии и безопасность: основы обеспечения информационной безопасности: Материалы международной научной конференции ИТБ-2014. – К.: ИПРИ НАН Украины, 2014. – С. 3-17.
3. *Ландэ Д.В., Грайворонская А.Н., Березин Б.А.* Мультиагентная модель распространения информации в социальной сети // Реєстрація, зберігання і обробка даних, 2016. - Т. 18. - N 1. - С. 23-30.
4. *Горбулін В.П., Додонов О.Г., Ландэ Д.В.* Інформаційні операції та безпека суспільства: Загрози, протидія, моделювання: монографія. – К.: Інтертехнологія, 2009. – 164 с.
5. *Додонов А.Г., Ландэ Д.В.* Мультиагентная модель поведения тематических информационных потоков // Материалы VI Всероссийской мультиконференции по проблемам управления (30 сентября – 5 октября 2013 г.) – Т. 4. – Ростов-на-Дону: Издательство Южного федерального университета, 2013. – С. 102-107.
6. *Потемкин А.В.* Выявление информационных операций в средствах массовой информации сети Интернет: диссертация ... кандидата технических наук: 05.13.10 / Потемкин Алексей Владимирович; [Место защиты: Брянский государственный технический университет]. – Брянск, 2015. – 144 с.
7. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Сценарный анализ эффективности управления информационной поддержкой государственной политики России в Арктике. // Национальная безопасность / nota bene. – 2011. – № 6. – С. 104-137.
8. *Давыдов А.А.* Системная социология. – М.: Издательство ЛКИ, 2008. – 192 с.
9. *Додонов А.Г., Ландэ Д.В., Бойченко А.В.* Сценарный подход при исследовании динамики информационных потоков в сети Интернет // Открытые семантические технологии проектирования интеллектуальных систем (OSTIS-2015): материалы V междунар. науч.-техн. конф. (Минск 19-21 февраля 2015 года) / - Минск: БГУИР, 2015. - С. 225-230.

Национальная академия наук Украины

Институт проблем моделирования в энергетике им. Г.Е. Пухова



МОДЕЛИРОВАНИЕ-2016

SIMULATION-2016

25-27 мая 2016, Киев

Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины
НИИ многопроцессорных вычислительных систем им А.В. Каляева
Южного Федерального Университета, Россия
Национальный технический университет «Львовская политехника»
Институт кибернетики им.В.М. Глушкова НАН Украины
Национальный авиационный университет Украины
Донецкий национальный технический университет
Институт электродинамики НАН Украины
Институт проблем регистрации информации НАН Украины
Щецинский технический университет, Польша
Институт специальной связи и защиты информации НТУУ «КПИ»
Ташкентский государственный технический университет, Узбекистан
Компания «Юстар», Украина
Энергосервисная компания «ПАТРИОТ-НРГ»

Сборник трудов конференции

МОДЕЛИРОВАНИЕ-2016

SIMULATION-2016

25-27 мая 2016, Киев

УДК 004.94

М74

Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, НИИ многопроцессорных вычислительных систем им А.В. Каляева Южного Федерального Университета (Россия), Национальный технический университет «Львовская политехника», Институт кибернетики им.В.М. Глушкова НАН Украины, Национальный авиационный университет Украины, Донецкий национальный технический университет, Институт электродинамики НАН Украины, Институт проблем регистрации информации НАН Украины, Щецинский технический университет (Польша), Институт специальной связи и защиты информации НТУУ «КПИ», Ташкентский государственный технический университет (Узбекистан), Компания «Юстар» (Украина), Энергосервисная компания «ПАТРИОТ-НРГ» проводят Пятую международную конференцию МОДЕЛИРОВАНИЕ-2016.

Конференция проходит в Институте проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, г. Киев, 25-27 мая 2016 г.

ISBN 978-966-02-7928-5

Все материалы поданы в авторской редакции. Прошли рецензирование.

40. *А.А. Кузнецов, И.Н. Белозерцев, А.В. Андрушкевич* Нелинейные узлы замен блочных симметричных шифров 183
41. *О. Г. Додонов, А. И. Кузьмичов* Моделювання ризиків у проектно-орієнтованому організаційному управлінні засобами стохастичної оптимізації середовища ASP 187
42. *Н. А. Куликовская, Р. К. Кудерметов* Модель распределенной компьютерной системы с семантическими веб-сервисами 191
43. *В. В. Кучанський* Імітаційна модель електропередачі надвисокої напруги для дослідження резонансних перенапруг 194
44. *Д. В. Ландэ, В. А. Додонов, Т.В. Коваленко* Информационные операции в компьютерных сетях: моделирование, выявление, анализ 197
45. *А.В.Латышев* О моделировании механизмов сознания 201
46. *Н. А. Литвинов* Компонент генерации шаблонов и библиотек JNI 205
47. *В.В.Максимова, С.И.Мазухина, Т.А.Черепанова, Т.Т.Горбачева* Применение физико-химического моделирования в экологических исследованиях 209
48. *Т.Т.Горбачева, С.И.Мазухина, Т.А.Черепанова, В.В.Максимова* Физико-химическое моделирование состава вод наземных экосистем Мурманской области РФ 213
49. *Ю. Л. Меньшиков* Лучшее для прогноза адекватное математическое описание динамических систем 217
50. *В. І. Ночвай, В. В. Циганок* Модель прийняття рішень з розподілу ресурсів між проектами в соціоекологічній системі 221
51. *А. Г. Додонов, В. Г. Пуятин, С. А. Куценко, А.А. Юрасов* Управление процессом моделирования при решении функциональных задач на АРМ компьютерной модели СОУ АК 225
52. *Д. В. Самсоненко* Моделювання варки утфелю у вакуум-апаратах 229
53. *В. М. Седенков* Домен-независимое проектирование: теория, технология, система 233
54. *А. С. Соколенко* Проблемы реализации системы персонального GPS мониторинга 237