Если хочешь в бизнесе мира - готовься к информационной войне, или по-современному - к информационной операции

Динамика информационных потоков и информационные операции

В отслеживании динамики веб-публикаций, анализе информационной обстановки, отражении сетевых информационных атак помогут системы контент-мониторинга

Школа ИТМ «Интернет-разведка для руководителя»

Ранее считалось, что информация всего лишь обеспечивает осведомленность людей о событиях и фактах в окружающем их мире. Информация воспринималась как полезный ресурс, предназначенный для расширения человеческих возможностей. В современных условиях информацию все чаще рассматривают как средство противоборства, оружие, которое не наносит физического вреда, но подрывает основы действия механизмов организации и управления. Термин «информационные операции» (ИО), получивший широкое распространение в начале нового тысячелетия, более точно, чем устоявшийся термин «информационные войны», отражает место и роль информационного противоборства. Информационные операции – это понятие, которое охватывает информационное воздействие на массовое сознание, воздействие на информацию, необходимую ему для принятия решений, а также на информационно-аналитические системы.

Что такое информационная операция

Основная задача информационных операций состоит в манипулировании массовым сознанием с такими целями, как, например, внесение в общественное сознание и сознание отдельных людей определенных идей и взглядов, дезориентация людей и их дезинформация, ослабление определенных убеждений людей, устоев общества и т. д. Уровень готовности к проведению информационных операций сегодня считается ключевым фактором успеха проведения любой социальной процедуры, кампании.

Хотя понятие «информационных операций» явно не определяется в нормативных документах многих государств, включая Украину и Россию, они повсеместно осуществляются для обеспечения политических, экономических интересов политических партий, правительств, политических движений, для реализации власти и обеспечения национальных интересов как на территории своих, так и чужих государств. В Законе Украины «Об основах национальной безопасности Украины» (статья 7) среди потенциальных угроз в информационной сфере отдельно отмечаются угрозы информационных воздействий: «…стремление манипулировать общественным сознанием, в частности, путем распространения недостоверной, неполной или предубежденной информации».

ИО – на службе государства

Для нашей страны можно привести поучительный опыт Республики Израиль. На протяжении многих лет это государство борется за свое существование во враждебном окружении. Именно для проведения информационных операций израильское правительство в 2009 году объявило о наборе добровольцев в «армии» блоггеров, которые помимо иврита владеют иностранными языками, для участия в блогах и форумах в интересах этой страны.

В США при Министерстве обороны успешно действует государственная структура – «подразделение стратегических коммуникаций», цель которого «завоевывать ум и сердце» своих граждан и людей, проживающих за пределами этой страны. Под такие коммуникации подпадает все – от связей с общественностью до народной дипломатии и информационных операций. Лишь в 2009 году из федерального бюджета США на содержание этого подразделения было выделено 4,7 миллиарда долларов, из них 547 млн. – на связи с общественностью.

Фундамент технологии ИО

Фундаментом технологии современных информационных операций являются принципы синергетики, концепции эмерджентности, учет «системных эффектов». Предполагается, что запущенные в результате специальных кампаний информационные воздействия должны саморазвиваться, лавинообразно расширяться, приводя их инициаторов к желаемым результатам. Синергетические подходы базируются на рассмотрении общества как чрезвычайно сложной системы, каждый элемент которой имеет множество степеней свободы, и поэтому гарантируют корректность результатов моделирования лишь на качественном уровне.

Есть ли стандартный план?

Очевидно, не существует единственного, «стандартного» плана проведения информационных операций. Можно лишь рассмотреть примерную, полученную путем обобщения некоторых реализованных информационных операций, последовательность действий при их осуществлении.

На практике информационная операция, как правило, реализуется следующим образом: в результате предварительной разведки вырабатывается план оперативного управления и намечаются соответствующие мероприятия оперативной разведки, которые являются приближенной моделью решения, после чего реализуется оперативное управление противником. На этапе оперативной разведки определяется уровень отклонения первоначальной модели от реальности, и если оно незначительно, то реализуется первоначальный план. В противном случае строится новый план оперативного управления и управления противником. Далее цикл повторяется до тех пор, пока оперативная разведка не подтвердит модель.

Типы информационных операций

Различают два основных **типа информационных операций** – наступательные и оборонительные. Однако на практике, большинство из них являются смешанными.

План типовой информационной операции включает совпадающие на верхнем уровне для информационных операций всех типов такие этапы, как оценка, планирование, исполнение и завершающая фаза.

Безусловно, исследования такого многоаспектного явления, как информационные операции составляют не только (а может, и не столько) теоретический, но и сугубо практический интерес. Составляющие информационных операций как явлений, отдельные тематические сюжеты, в частности

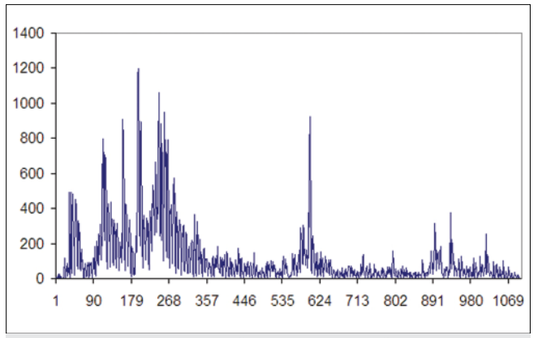


Рис. 1. Динамика веб-публикаций по запросу «птичий грипп» (здесь и далее по горизонтальной оси - дни (с момента начала анализа), а по вертикальной оси - количество публикаций)

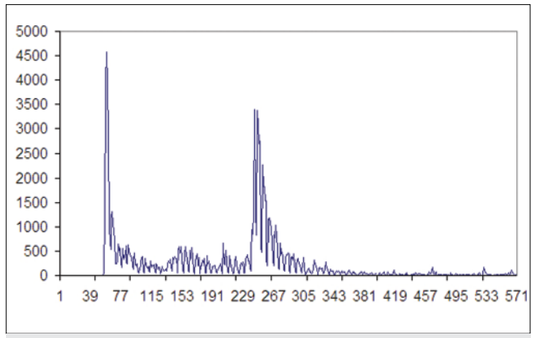


Рис. 2. Динамика веб-публикаций по запросу «свиной грипп»

отдельные их проявления, а тем более их совокупность, могут трактоваться как реальные или потенциальные события, реальные или потенциальные угрозы.

При ретроспективном анализе любого явления интерес представляют определенные характеристики его развития, а именно:

- количественная динамика, присущая явлению, например, количество событий в единицу времени или количество сообщений относительно явления;
- определение критических, пороговых точек, которые отвечают количественной динамике явления;
- определение проявлений явления в критических точках, например, выявления основных сюжетов публикаций в СМИ (в том числе и веб-публикаций) относительно выбранного явления;
- ранжирование проявлений в критических точках, исследование динамики развития отдельных определенных проявлений до и после определения критических точек;
- статистический анализ общей динамики и динамики отдельных проявлений, на основе которых осуществляются попытки прогнозирования развития явления и отдельных его проявлений.

Сетевая информационная атака

Обычная сетевая информационная атака в веб-среде сегодня производится следующим образом: как правило, создается и некоторое время функционирует веб-сайт (назовем его «первоисточником»), при этом он публикует вполне корректную информацию. В час X на его странице появляется документ, обычно компромат на объект атаки, достоверный либо сфальсифицированный. Затем происходит так называемая «отмывка информации». Документ перепечатывают интернет-издания двух типов – заинтересованные в атаке и те, кому попросту не хватает информации для заполнения своего информационного поля. В случае претензий все перепечатывающие издания ссылаются на «первоисточник», и в крайнем случае по просьбе/требованию объекта атаки удаляют со своих веб-сайтов информацию. Первоисточник при необходимости также снимает информацию либо вовсе ликвидируется (после чего оказывается, что он зарегистрирован в Интернете на несуществующее лицо). Вместе с тем информация уже разошлась, задача первоисточника выполнена, атака стартовала.

Взаимосвязь событий и системы контент-мониторинга

Современное информационное пространство представляет собой уникальную возможность получения информации по любому вопросу, но при наличии соответствующего инструментария, применение которого позволяет анализировать взаимосвязь возможных событий или событий, которые уже происходят, с информационной активностью определенного круга источников информации.

Эту взаимоувязанность можно проиллюстрировать на конкретных примерах. Исследования проводились на наборе документальных массивов, которые содержат сообщение онлайновых СМИ разных объемов, собранных из сети Интернет системой InfoStream, которая обеспечивает интеграцию и мониторинг сетевых информационных ресурсов.

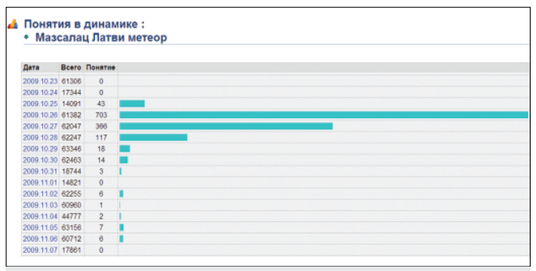


Рис. 3. Динамика веб-публикаций по тематике появления метеорита в Мазсалаце

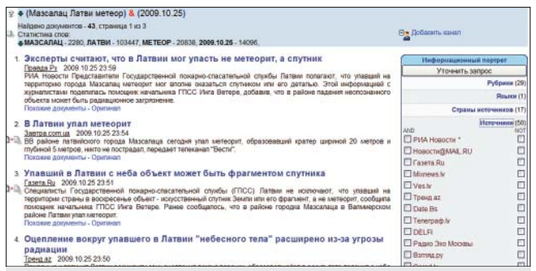


Рис. 4. Публикации в начале изучаемого информационного сюжета (темы)

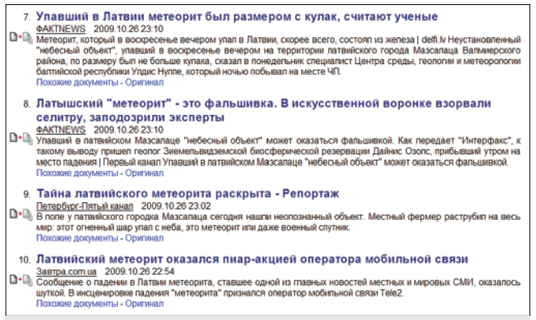


Рис. 5. Публикации в «пиковый» период жизни информационного сюжета

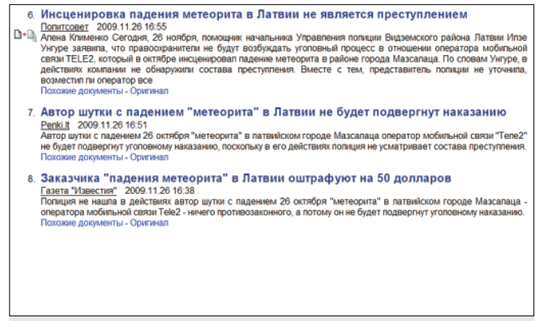


Рис. 6. Завершение жизненного цикла информационного сюжета

С помощью этой системы выполняется автоматизированный сбор информации из веб-сайтов в режиме реального времени, ее структуризация, группирование за семантическими признаками и предоставление доступа к информации в поисковых режимах. Системой InfoStream охватываются новости из 4000 источников – отечественных и зарубежных веб-сайтов, осуществляются их обработка и обобщение. Система обеспечивает доступ к уникальному ретроспективному фонду, объем которого превышает 80 млн. записей за 15 лет.

Количество веб-публикаций в день по какой-либо теме, а особенно изменения (динамика) этой величины порой позволяют даже небольшим специалистам в предметной области делать более-менее точные выводы.

Динамика веб-публикаций

Получить данные динамики веб-публикаций возможно, например, ежедневно заходя на сайты интеграторов новостей (news.yandex.ru, webground.su, uaport.net). Конечно, в лучшем положении находятся пользователи платных систем мониторинга типа Интегрум или InfoStream. Именно на основе последней системы получена удивительная статистика по количеству веб-публикаций на тему эпидемий гриппа в разные периоды.

К примеру, на рис. 1. показана динамика публикаций в RUNet по запросу «птичий грипп» за период с середины 2005 года до конца первого полугодия 2008 года, полученная с помощью системы InfoStream.

Безусловно, мелкие колебания количества веб-публикаций, связанные с недельной цикличностью можно сглаживать, но все равно на рис. 1 видны три большие пиковые области, с максимумами, приходящимися на декабрь-январь в течение трех лет. Видно, как из года в год тема (даже в критические сезоны) теряла свою актуальность. Итак, наблюдается периодичность, снижение актуальности, колоколообразная форма динамики в критические сезоны.

Совсем иначе выглядит динамика веб-публикаций по запросу «свиной грипп» (рис. 2). Данные получены с момента появления в RUNet первых сообщений по этой теме (второй квартал 2009 года) до октября 2010 года.

Можно видеть два внезапно возникающих пика в апреле 2008 года и конец октября 2009 года. Затем количество веб-публикаций резко уменьшается – практически по гиперболической зависимости. Первый пик связан с первыми проявлениями в мире вируса A/H1N1 и выделениями во всем мире (прежде всего в США) огромных средств на борьбу с ним, другой – с осенними проявлениями во всех странах мира, но прежде всего, в России и Украине. Абсолютные пиковые значения более чем в 3 раза превысили пиковые значения птичьего гриппа.

Официальная статистика нам уже рассказала, что с последней эпидемией удалось успешно справиться, смертность от A/H1N1 оказалась более низкой, чем от обычного сезонного. Налицо вспышки активности веб-публикаций, очень быстро рассасывающиеся. Очевидно, сообщения о свином гриппе вначале носили сенсационный характер, но затем не было естественной информационной подпитки. Если бы в средние века был Интернет, то информация о волнах чумы, наверное, имела бы такой же характер… Но последствия тогда были иными. Действительно, очень удобная платформа для сторонников идеи конспирологии и всемирных заговоров.

Как видим, отсутствие естественной информационной подпитки выражается в резком всплеске количества публикаций, а затем также в достаточно резком (гиперболическом или даже экспоненциальном) спаде. Зачастую информационные операции сопровождаются именно таким поведением динамики веб-публикаций.

Пример информационной операции

Приведем пример одной такой информационной операции, проводимой в конце октября 2009 года оператором мобильной связи Tele[2] из Латвии. Речь шла о мистификации по поводу падения метеорита в городе Мазсалац. График динамики публикаций по этой теме, полученный с помощью системы InfoStream, приведен на рис. 3.

Первые публикации 25 октября были посвящены самому факту появления «метеорита» и попыткам объяснить его космическое происхождение (Рис. 4).

По-видимому, вопреки ожиданиям мистификаторов, наибольший отклик в веб-пространстве получило их разоблачение – информационная операция вышла из под контроля своих авторов (рис. 5).

И, наконец, хвост информационного сюжета полностью посвящен мерам наказания мистификаторов (рис. 6).

Анализ информационной атаки

Перейдем к анализу более серьезного инцидента. В декабре 2008 года в Украине произошла публичная знаковая

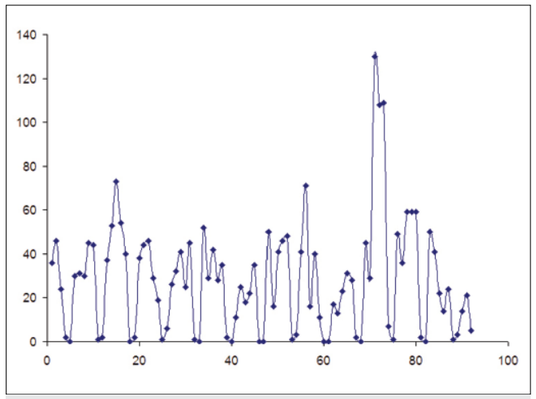


Рис. 7. Интенсивность публикаций в Интернете по теме «Оранта»

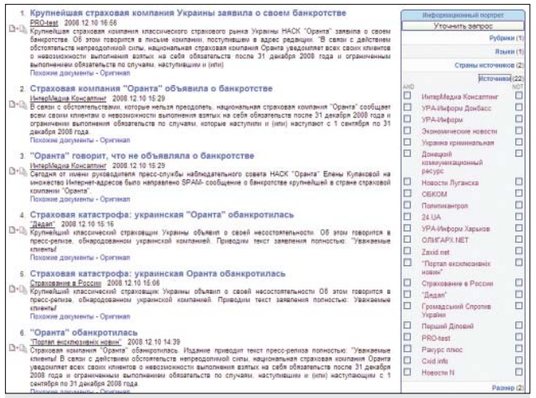


Рис. 8. Первые часы атаки. Самые «оперативные» источники

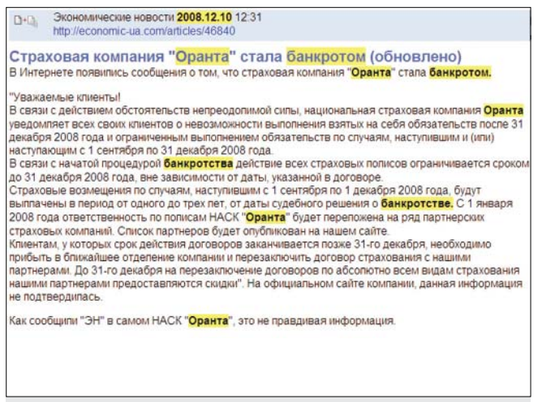
информационная атака на рынке страхования. Это была настоящая информационная операция против НАСК «Оранта». В этом случае первоисточником компромата оказался не веб-сайт, а информационное сообщение, разосланное электронной почтой тысячам пользователей Интернета. В результате применения специальных технических приемов, оно разошлось с обозначением адреса пресс-службы объекта атаки. Итак, 10 декабря 2008 года в районе 11:30 в виде спама было разослано информационное сообщение, в котором говорилось о том, что страховая компания «Оранта» заявляет о банкротстве. По предварительным данным, информация разлетелась по 1000 адресам, естественно, данные попали к конкурентам и в СМИ. В сообщении говорилось, что компания с 31 декабря 2008 года прекращает выполнять взятые перед клиентами обязательства.

В связи со случившимся НАСК «Оранта» обратилась в правоохранительные органы с просьбой расследовать данный инцидент и наказать виновных. Произошедшее с «Орантой» очень напоминало ситуацию с «Проминвестбанком», с этим согласились многочисленные эксперты. Ведь как банковский бизнес, так и страховой основываются на доверии клиентов, которое легче всего подрывается именно информационными атаками. Олег Спилка, председатель наблюдательного совета НАСК «Оранта», сообщил: «Это мероприятие готовилось целенаправленно для того, чтобы дискредитировать страховую компанию и подорвать ее репутацию». Не вдаваясь в детали возможных целей атаки (смена владельцев, борьба за блокирующий пакет акций, уничтожение компании и т. п.), с помощью ретроспективного анализа проследим за динамикой публикаций в сети Интернет, в которых упоминалась НАСК «Оранта». На рис. 7. приведена посуточная динамика количества соответствующих публикаций. На этой диаграмме, кроме всего прочего, отчетливо виден спад интенсивности публикаций по данной теме в начале декабря 2008 г., что вполне можно воспринимать как некоторое «затишье перед бурей».

Несмотря на отдельные пики в 16-й и 55-й день квартала, все же наибольший интерес представляет экстремум, приходящийся именно на 10-12 декабря.

Проследим за ходом информационной операции, рассматривая сообщения, публикуемые в разные промежутки времени.

На рис. 8 приведен список публикаций по теме «Оранта» в течение первых часов атаки. По словам Олега Спилки, в течение двух часов с начала атаки все почтовые серверы НАСК «Оранта» были выведены из строя, поэтому опровержение в сети задержалось.


Экономические новости **2008.12.10** 12:31
http://economic-ua.com/articles/46840

Страховая компания "Оранта" стала банкротом (обновлено)

В Интернете появились сообщения о том, что страховая компания "**Оранта**" стала **банкротом.**

"Уважаемые клиенты!
В связи с действием обстоятельств непреодолимой силы, национальная страховая компания **Оранта** уведомляет всех своих клиентов о невозможности выполнения взятых на себя обязательств после 31 декабря 2008 года и ограниченным выполнением обязательств по случаям, наступившим и (или) наступающим с 1 сентября по 31 декабря 2008 года.
В связи с начатой процедурой **банкротства** действие всех страховых полисов ограничивается сроком до 31 декабря 2008 года, вне зависимости от даты, указанной в договоре.
Страховые возмещения по случаям, наступившим с 1 сентября по 1 декабря 2008 года, будут выплачены в период от одного до трех лет, от даты судебного решения о **банкротстве.** С 1 января 2008 года ответственность по полисам НАСК "**Оранта**" будет перепожена на ряд партнерских страховых компаний. Список партнеров будет опубликован на нашем сайте.
Клиентам, у которых срок действия договоров заканчивается позже 31-го декабря, необходимо прибыть в ближайшее отделение компании и перезаключить договор страхования с нашими партнерами. До 31-го декабря на перезаключение договоров по абсолютно всем видам страхования нашими партнерами предоставляются скидки". На официальном сайте компании, данная информация не подтвердилась.

Как сообщили "ЭН" в самом НАСК "**Оранта**", это не правдивая информация.

Рис. 9. Опровержение?

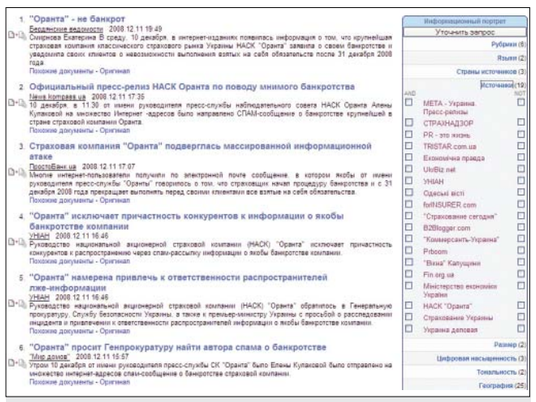


Рис. 10. Сообщения с опровержением

Школа ИТМ «Интернет-разведка для руководителя»

В 12:31 на сайте «Экономические новости» появляется странное «обновленное» сообщение с парадоксальным последним предложением (рис. 9).

После этого руководство НАСК «Оранта» опубликовало в Интернете первые опровержения, не спеша обвинять конкурентов в происшедшем, а затем все же признав атаку целенаправленной и выгодной третьим лицам.

На рис. 10 приведен список публикаций, посвященных опровержению сообщения о банкротстве за следующий день (11 декабря), а также наиболее активных источников, опубликовавших эти сообщения. Безусловный интерес аналитиков вызывает сравнение источников, приведенных на рис. 8 и 10.

Дальнейший спад публикаций по теме НАСК «Оранта» и возвращение его на нормальный «средний» уровень свидетельствует о том, что компания своими осторожными и точными действиями смогла с успехом противостоять информационной операции.

Многочисленные практические примеры позволяют выработать некоторую общую методику проведения оборонительной информационной операции с использованием системы контент-мониторинга веб-ресурсов, включающую сбор информации с публикациями в веб-пространстве о компании, определение динамики появления сообщений, анализ этой динамики, определение источников, публикующих наибольшее количество негатива, и «первоисточников» – тех источников, которые первыми опубликовали негативную информацию. Затем выявляются вероятные «заказчики», влияющие на издательскую политику отдельных онлайновых СМИ. Затем прогнозируются дальнейшие шаги воздействия, вероятные последствия и организуется информационное противодействие.

Системы контент-мониторинга и анализ информационной обстановки

Именно системы контент-мониторинга лучше всего подходят для оперативного анализа информационной обстановки. Причины для этого три: во-первых, они обеспечивают оперативность, которую не могут обеспечить поисковые системы (время индексации сетевого контента даже лучшими из них составляет от нескольких суток до нескольких недель), во-вторых, всегда обеспечивают необходимую полноту как в плане источников, так и представления материалов источников, в отличие от обычных агрегаторов новостей, и в-третьих, содержат необходимые аналитические средства, которые могут предоставить пользователю информацию об интенсивности публикаций по заданной тематике в необходимый период времени.

Дмитрий Ландэ,
заместитель директора Информационного центра «ЭЛВИСТИ»