# Технологии информационных войн в интернете

Автор: Нежданов Игорь Юрьевич

# Оглавление

## Вместо предисловия

Информационные войны это давняя технология достижения своих целей. Они в том или ином виде присутствуют в человеческом обществе очень давно, возможно, с того момента, как человек научился говорить. В разное время в рамках информационных войн использовались слухи, газеты, листовки, книги, кино, радио, телевидение… Практически все средства распространения информации (искусство, кстати, тоже). Но на рубеже XX и XXI веков появился интернет – среда, предназначенная для манипулирования информацией (ее создания, модификации, распространения и потребления). В основе интернета лежит информация, и он лучше всего подходит для манипулирования ею. Именно по этой причине с появлением интернета информационные войны перешли на новый качественный уровень. Именно интернет сделал информационные войны легко реализуемыми (быстрыми, дешевыми, не знающими границ).
Вот об этом симбиозе и пойдет речь – о том, как осуществляются информационные войны в интернете. Но не с точки зрения общих рассуждений о добре и зле, и не с точки зрения стратегий (как в анекдоте про сову и мышей), а о технологической составляющей. Помните, как мыши пришли к сове за советом «нас все обижают – как нам эту проблему решить?». На что сова рекомендовала им стать ежами. А на вопрос «как это реализовать?» ответила: «Я не знаю – я стратег». О том, что и как делается в интернете для осуществления информационного воздействия на людей (манипулирования ими). О том, какие существуют сервисы и технические решения, которые можно использовать в ходе противодействия информационным войнам. Но в начале нужно разобраться – что такое информационная война.

## Что это такое – «информационная война»

Сейчас наиболее распространены два варианта определения информационной войны:
1) Воздействие на гражданское население и/или военнослужащих другого государства путём распространения определённой информации. Термин «информационно-психологическая война» был заимствован из словаря военных кругов США. Перевод этого термина («information and psychological warfare») с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война» в зависимости от контекста конкретного официального документа или научной публикации. В этом смысле также используется термин психологическая война — психологическое воздействие на гражданское население и (или) военнослужащих другого государства с целью достижения политических или чисто военных целей.
2) Целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.
Понятно, что это воздействие на людей, причем воздействие на их мнение о чем-то. Например, на мнение о существующем устройстве их государства, на мнение об эффективности правительства их государств, на их отношение к собственной Родине (если говорить об информационных войнах планетарного масштаба). Или на мнение людей по поводу коррумпированности членов той или иной партии, их связи с криминалом (если говорить об информационных войнах между разными политическими силами внутри страны). Или на мнение клиентов компании о качестве продукции этой компании (если речь идет об информационных войнах в бизнесе). В этом смысле понятия «информационная война» и «управление репутацией» очень близки. А если сказать иначе, то информационная война – это формирование мнения людей о чем-то или о ком-то и через такое формирование – управление действиями этих людей – манипулирование ими. Собственно, это и есть конечная цель информационной войны – управление действиями людей.
Если говорить в понятиях именно войны, то информационная война (Information war) – это воздействие на противника посредством информации с деструктивными целями. Понятие это очень широкое и в наш век информатизации включает в себя очень многое. Но все эти методы, технологии и техники объединяет цель (деструктивное воздействие на противника) и то,

посредством чего это воздействие осуществляется (информация). На западе информационные войны принято называть кибервойнами (Cyber-warfare).
Деструктивное воздействие на противника – это всё что угодно, но главное, чтобы во вред противнику. Максимум это полное уничтожение, а минимум – нанесение вреда инфраструктуре, ущерба экономике, создание проблем в госуправлении и т.п. Хотя бы минимальная проблема – например, задержка в передаче команды. Вроде ничего, но только не в случае с критическими системами. Например, в атомной электростанции, коих много, или в системе боевого управления военным кораблем, или в системе предупреждения о ракетном нападении… В критичных системах такой мизер может оказаться фатальным. И задержку в передаче команды можно организовать по-разному: увеличить время реакции или перевести таймер чуть назад, или зародить немного сомнения в голове у курьера или секретаря, а еще лучше у клерка, который транслирует такую команду… Он ее еще и модифицировать может. Очень по-разному можно осуществить деструктивное воздействие на противника.
Но есть некоторое двоякое толкование понятий «информационная» и «кибер». Дело в том, что для обывателя более понятно понятие «вирус», «троян» и т.п. Видимо, в силу их более частого и давнего употребления. Все знают, что это плохо, что это противозаконно, что это наносит вред. А потому об этом можно порассуждать, даже не особо понимая предмет. Совсем другое дело психологическое воздействие на человека посредством информации, да еще с использованием интернета в качестве средства доставки. Это тоже информационная война. Можно говорить о расширении понятия «информационная война» – трояны, вирусы и прочие зловреды, ведь это тоже информационная война. Фактически это воздействие на инфраструктуру принятия решений (трактовка, предложенная Александром Токаренко) с целью ее уничтожения или нарушения ее работы. В эту структуру принятия решений входит и человек как источник информации, элемент ее обработки, передачи, использования (в т.ч. и для принятия решений).
Исходя из этого, можно более четко очертить ту сферу, о которой пойдет речь далее. Это воздействие на человека с помощью информации, используя интернет-технологии, с целью манипулирования им.

## Мировые тенденции

В интернете вообще и в соцсетях в частности присутствует все больше народа, причем активного народа – тех, кто жаждет действия, а не довольствуется созерцанием. Или тех, кто в жизни ничего из себя не представляет, а в интернете, надеясь на анонимность, начинает вести себя как колхозный гопник. Кроме того, в интернете есть возможность любому стать распространителем информации («типа» журналистом), а информация распространяется крайне быстро, и границы государств этому не помеха. Мало того, в интернете можно с минимальными затратами создать иллюзию любого масштаба и ориентированную на любые социальные группы (страны, регионы, организации…). В том числе и иллюзию как негативную по отношению кому бы то ни было, так и позитивную. А это уже манипулирование пользователями на уровне их фундаментальных понятий о «добре и зле», о том, «что такое хорошо и что такое плохо». С другой стороны, извечная борьба за ресурсы и рынки сбыта (в политике за электорат) только ужесточается. Что заставляет искать новые инструменты влияния. Вот и обратили многие сильные мира сего свое внимание на этот эффективный, дешёвый и доступный инструмент.

### *Активность спецслужб в области информационных войн.*

Государства не могут не замечать наличие такого инструмента. Причем как с точки зрения его использования, так и с точки зрения защиты от него. В ряде стран на государственном уровне приняты решения об использовании интернета (соцсетей) в интересах этих стран (США, Великобритания, Китай, Индия, Франция, Германия). В рамках этих решений соцсети активно вовлекают как в сбор информации (пассивный и активный), так и для организации активных мероприятий (манипулирование общественным мнением). Параллельно ведутся разработки систем, позволяющих максимально автоматизировать процесс сбора и процесс анализа информации, и процесс ее распространения, а значит, и ведения информационных войн. А технологии влияния через интернет уже не тестируются, а активно используются.

### *США*

США как страна-создатель интернета является на данный момент лидером в гонке кибервооружений. Госструктуры US давно активно «осваивают» в том числе и соцсети. Для этих исследований и для разработки решений в США используются возможности нескольких организаций – DARPA, IARPA и ARL. Причем в последние годы в их работе наблюдается выраженный крен на исследование и разработку новых технологий социальных взаимодействий в сетях, узлами которых являются люди, тексты, образы и компьютерные устройства. Иными словами, эти три уважаемые организации тратят максимум усилий на развитие технологий для исследования активности людей во взаимодействии друг с другом посредством обмена данными в интернете. В рамках этого тренда разрабатываются решения, касающиеся:

-Когнитивно- и социально-сетевой психологии;

-Нейро-сетевого взаимодействия;

-Функционирования сетей и интеллектуальных агентов.

Работы идут сразу по нескольким направлениям. Точнее сказать, по ряду направлений они уже практически закончены и результаты используются. **На правовом уровне** силовики, опираясь на принятые поправки к законам, имеют практически «прямой» вход на серверы соцсетей. Только в 2012 году Палата представителей Конгресса США приняла сразу несколько законов и поправок, связанных с кибернетической безопасностью: The Cybersecurity Enhancement Act of 2011 (Закон об усилении кибернетической безопасности), H.R. 2096, Advancing America's Networking and Information Technology Research and Development Act of 2012 (Совершенствование НИОКР в области сетевых и информационных технологий), H.R. 3834, Cyber Intelligence Sharing and Protection Act H. R. 3523 (Закон об обмене и защите разведывательной информации в области кибернетической безопасности), Federal Information Security Amendments Act H. R. 4257 (Дополнения в федеральный закон об информационной безопасности).

**На техническом уровне** создана инфраструктура – центры накопления и обработки информации, где архивируются данные с глубиной не менее трех лет и установлены суперкомпьютеры со значительными скоростями работы. Причем центры обработки есть как на федеральном уровне (межведомственные), так и локальном уровне (ведомственные). Разрабатываются новые технологии обработки больших массивов данных и извлечения знаний.

**На технологическом уровне** ведутся разработки решений для автоматизации уже не только мониторинга, но и подготовки и реализации активных мероприятий в интернете. В 2012 году DARPA (координатор разработок в данном направлении) планирует потратить на кибертехнологии в общей сложности 208 млн долларов по сравнению с 120 млн в прошлом, 2011-м, году. В целом на стратегию по созданию средств для информвойны, кибератак и защиты от них на 2013-2017 годы DARPA выделено 1,54 млрд долларов. Подробности ниже.
**На организационном уровне** в 2006 году создано IARPA (Intelligence Advanced Research Projects Activity) – Агентство передовых разведовательных исследовательских проектов в структуре директората национальной разведки США Director of National Intelligence (DNI) – еще более закрытая организация, ведущая разработки в интересах разведки. Ее цель стать авангардом авангарда перспективных и прорывных IT-разработок. Ее основной принцип – разрабатывать то, без чего можно прекрасно обойтись сегодня, но зато в будущем это станет сильно критичным. Основные направления работы:
-радикальное повышение отдачи от собираемой информации (анализ, использование информации);
-поиск методов искусственных озарений и интуитивных проникновений в суть того, что содержится в собранной информации (опять технологии анализа);
-разработка технологий противодействия новым возможностям противников в интернете.

## DARPA

DARPA (англ. Defense Advanced Research Projects Agency – агентство передовых оборонных исследовательских проектов) – агентство Министерства обороны США, отвечающее за разработку новых технологий для использования в вооружённых силах. Миссией DARPA является сохранение технологического превосходства вооруженных сил США, предотвращение внезапного для США появления новых технических средств вооруженной борьбы, поддержка прорывных исследований, преодоление разрыва между фундаментальными исследованиями и их применением в военной сфере. (Wikipedia)

DARPA разрабатывала и развивает целое «семейство» проектов, прямо или косвенно связанных с ведением информационно-психологических войн.

**Terrorism Information Awareness – TIA**
В 2001 году DARPA запустила проект «Знания информации о терроризме» (Terrorism Information Awareness – TIA), который заключается в создании и испытании опытного образца системы, позволяющей на основе больших объемов не связанной информации в различных базах данных (в т.ч. и в соцсетях) выявить группу лиц, готовящихся совершить террористический акт на территории США. Проект успешно реализован и развивается. А в настоящее время стал фундаментом для последующих разработок в области анализа данных из открытых источников (в т.ч. и из интернета). Созданная система включает в себя несколько подсистем: перевод с иностранных языков на английский и обратно, выявление скрытых данных, определение не явных связей, распознавание образов, корпоративный анализ информации для принятия решений. На основе статистического анализа информации из баз данных и интернета система определяет корреляции (взаимосвязь) таких, на первый взгляд, случайных и не связанных между собой событий как: заказ билетов, заявки на визы, получение водительских прав, бронирование номеров в отелях, покупка химикатов и взрывчатых веществ, приобретение огнестрельного

оружия и другие подозрительные действия, включая уже известные террористические акты. По заранее определенным разведпризнакам определяются потенциально опасные события и/или последовательности событий, которые отдаются в углубленное исследование.

**Machine Reading Program**

В 2009 году DARPA запустила проект «Машинное чтение» (Machine Reading Program). Целью программы является создание автоматизированной системы чтения и понимания текстов на естественном языке, способной извлекать востребованную информацию из текста без участия человека. Проект был инициирован с целью развития «Знания информации о терроризме» (Terrorism Information Awareness — TIA). Руководит проектом Дэвид Феруччи (David Ferrucci), заведующий департаментом семантического анализа и синтеза Исследовательского центра IBM им. Уотсона.

**Integrated Crisis Warning System**

В 2010 году запущена программа Integrated Crisis Warning System (ICEWS ) — информационная интегрированная система раннего предупреждения о возникновении кризисных ситуаций. Система ICEWS предназначена для мониторинга, оценки и выделения основных индикаторов, указывающих на нарастание социальной напряженности в обществе. Основным источником информации для системы являются соцсети. На реализацию программы в 2010-2011 гг. израсходовано 19 млн дол. В 2012 г. на эти цели планировалось затратить около 5,3 млн дол.

**Anomaly Detection at Multiple Scales**

С 2010 года разрабатывается программа Anomaly Detection at Multiple Scales, которая предназначена для выявления аномальных процессов, происходящих в обществе, наблюдения за неадекватным поведением отдельных индивидуумов и групп людей. И вновь основным объектом наблюдения являются соцсети. На реализацию программы в 2011-2012 гг. выделено 22,5 млн $.

**Math for Social Networks**

В 2011 году DARPA запустила новую программу Math for Social Networks, целью которой является разработка новых математических методов анализа социальных сетей с построением в реальном времени связей, указывающих на происходящие изменения в реальном мире. В рамках программы было создание расширенной теории моделирования сети, которая включает в себя выполнение пространственно-временного анализа; изучение влияния изменения в сетях на объекты, поведение которых может быть смоделировано.

Эти механизмы мониторинга социальных сетей с применением инструментов анализа пространственно-временных взаимосвязей и контента позволяют решить две основные задачи: прогнозировать назревание нежелательных событий и выявлять отдельных лиц и враждебно настроенных группировок, подозреваемых в подготовке терактов.

**Plan X**

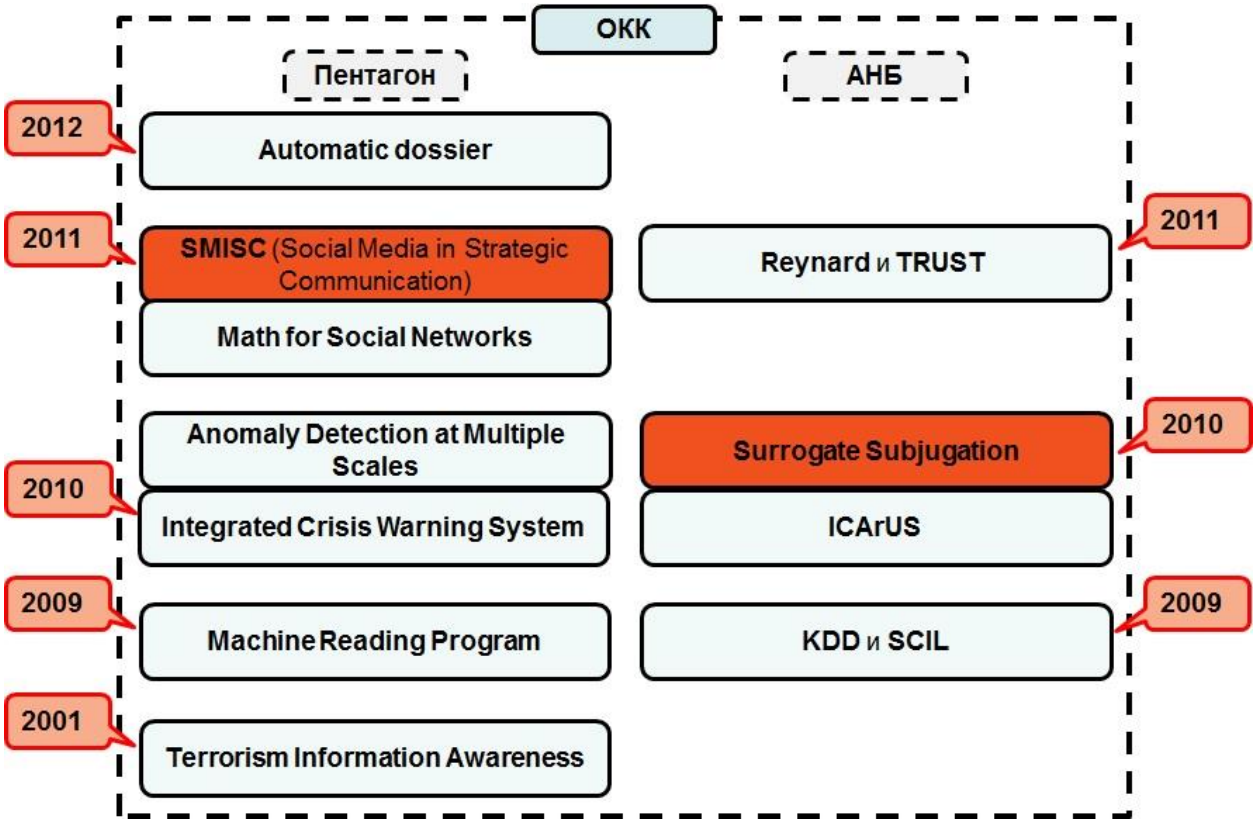
В 2012 году DARPA запустило программу под кодовым названием «Plan X». Согласно официальному документу, целью проекта «Plan X» является «создание революционных технологий, которые позволят понимать, планировать и управлять информвойной в режиме реального времени, в крупных масштабах, в динамичных сетевых инфраструктурах». Здесь имеются ввиду и кибервойны (нанесение ущерба программам и технике) и инфовойны (манипулирование людьми). Проект рассчитан на 5 лет. Бюджет проекта 110 млн $. Именно этот проект планируется сделать основным (обобщающим) среди «родственных» проектов, связанных с пассивным и активным использованием кибернетического пространства.

**Automatic dossier**

В июне 2012 года по заказу DARPA военный подрядчик Raytheon BBN Technologies создал компьютерную систему, которая автоматически составляет досье на граждан и организации, собирая информацию из открытых источников (социальных сетей, форумов, чатов, блогов).

Помимо работы по прямому упоминанию объекта система идентифицирует изучаемого по косвенным признакам, по связям, по образам (фото и видео материалы), по голосу (радио). Система может работать на трех уровнях эвристичности. Запуск системы в «боевом» режиме был запланирован на февраль 2013 года. У нас была не одна возможность убедиться, что система работает. И работает вполне эффективно. Опытные образцы подобной системы также были созданы компаниями SRI International и IBM.

**«Родственные проекты»**
Проекты, связанные с исследованиями социальных сетей или задействованные в них полностью либо частично.
ICArUS — Интегрированная нейро-когнитивная архитектура для понимания смысла текстов. «Вычерпывание» смыла из текстов.
KDD — Обнаружение и распространение знаний. Тоже «вычерпывание» смысла, но смысла, применимого для решения конкретных задач.
SCIL — Социо-культурный контент языка. Выявление из текстов национальных, социальных, культурных особенностей носителя языка.
TRUST — Средства проверки надежности сообщений. Фактически это технология сопоставления и стыковки данных, но автоматизированная и не нуждающаяся в участии человека.
Reynard — Извлечение ценной информации из социальных сетей и виртуальных миров. Тоже «вычерпывание» смыслов, но в данном случае смыслов вполне конкретных, обозначенных оператором.




## IARPA

**IARPA** (англ. Intelligence Advanced Research Projects Activity — Агентство по перспективным исследованиям разведывательного сообщества) — исследовательское агентство в США, находящееся в подчинении у Директора национальной разведки США. IARPA было создано в 2006 году как аналог DARPA для выполнения научных исследований для разведывательного сообщества США (по крайней мере, 16 правительственных агентств, занимающихся разведкой) путем объединения Disruptive Technology Office АНБ (ранее известного как Advanced Research and

Development Activity), National Technology Alliance из NGIA и Intelligence Technology Innovation Center из ЦРУ. (Wikipedia)


**«Intelligence Advanced Research Projects Activity»**
В IARPA создан центр по исследованию социально-когнитивных сетей Social Cognitive Network Academic Research Center (SCNARC). Перед этим центром поставлена задача практической проверки разработанных теоретических моделей безмасштабных сетей на больших объемах реальных данных.

Создан исследовательский центр Composite Networks: Understand, Predict, and Influence изучения человеко-машинных сетей.

В рамках этого мегапроекта создан «Альянс коллаборативных сетевых технологий» The Network Science Collaborative Technology Alliance (NS CTA), учредителями которого являются ARL, ряд других госагентств и консорциум четырех исследовательских центров: SCNARC, центр по исследованию информационных сетей INARC, центр по исследованию коммуникационных сетей CNARC и центр трансдисциплинарных сетевых исследований IRC. Задача каждого из этих центров и всего альянса – прорывное повышение возможностей людей и компьютеров, работающих в единой сети.

Кроме того, IARPA ведет менее крупные, но важные связанные с использованием социальных сетей исследования:

**Aggregative Contingent Estimation (ACE)**
Агрегатная оценка работы коллективного разума – технология исследования социальных групп с целью понять, как происходит формирование идей, их развитие, распространение, как можно оказывать влияние на коллективный разум.

Дополнительной целью программы является поиск возможности значительно улучшить точность и своевременность прогнозов для широкого спектра типов событий за счет агрегирования суждений многих аналитиков разведки.

Программа рассчитана на работу в следующих областях:
- эффективное выявление суждений по самым разным проблемам.
- учет суждений, основанных на фактах, и необоснованных суждений.
- статистический анализ совокупности суждений по проблеме.
- удобное представление агрегированных прогнозов.

**Metaphor**
Обнаружение и структурирование культурных традиции через изучение смысла метафор, через особенности языка, через особенности общения. Выявление на основе этого основных убеждений и мировоззрений представителей исследуемой культуры.

В первом этапе двухфазной программы исполнители будут развивать автоматизированные инструменты и методы распознавания, определения и классификации языковых метафор.

На втором этапе программа должна будет характеризовать различные культурные перспективы, представляющие интерес для разведывательного сообщества, и предложить варианты их использования.

**FUSE**
Обнаружение грядущих научных прорывных открытий через выявление повышения интереса к теме, исчезновение темы, нестандартных решений, необычных исследований и т.п..

**Sirius**
Использование игровых практик для выявления и управления когнитивными предубеждениями, для выработки навыков, для формирования устойчивых психотипов.

## Пентагон

Пентагон (от греч. πεντάγωνον — «пятиугольник») — штаб-квартира Министерства обороны США, имеющего форму правильного пятиугольника. Находится в штате Виргиния недалеко от Вашингтона (почтовый адрес: Арлингтон, Виргиния 22202, США). Как символ американских военных часто «Пентагон» метонимически обозначает Министерство обороны США. (Wikipedia)

В 2010 было создано в нынешнем виде Объединенное киберкомандование (Unified U.S. Cyber Command). В состав ОКК были отданы и две уже существовавшие на тот момент структуры Пентагона – Объединенная группа по операциям в глобальной сети (Joint Task Force-Global Network Operations, JTF-GNO) и Объединенное командование структурных компонентов сетевых боевых действий (Joint Functional Component Command – Network Warfare, JFCC-NW). Штаб-квартира ОКК находится в Форт-Миде, штат Мэриленд, а организационно входит в структуру Стратегического командования США. Объединенный оперативный центр ОКК (US Cyber Command Joint Operations Center — USCYBERCOM JOC), размещенный на новой территории в районе Форт-Мид, получил кодовое название «Объект-М» (Site-M). Площадь 19000 кв.м. стоимость объекта 119 млн долл.

В своей деятельности ОКК руководствуется документом Комитета начальников штабов ВС США под названием «Доктрина проведения информационных операций» (Joint doctrin of infomation operations), и руководством JP 3-13 «Информационные операции», в котором все положения доктрины приведены в соответствие с требованиями современных условий. Именно в компетенцию ОКК входят и информационные войны.

В 2010 г. Пентагон проводил оценку проекта Surrogate Subjugation (разработка компании Visual Purple), предусматривающего создание системы автоматизированного мониторинга социальных сетей, чатов и тематических форумов и активной работы на них с целью оказания необходимого влияния на аудиторию. Система создает виртуальную копию человека (так называемый «суррогат»), участвующего в онлайн-обсуждениях определенной темы. В каждом конкретном

случае при регистрации «суррогата» на форумах в его профиле указывается специально подобранная биографическая легенда, политико-экономические взгляды, а также круг интересов и увлечений. Все эти сведения призваны оказывать определенное воздействие на отношение участников интернет-общения к «суррогату» и его высказываниям, а также влиять на смысловой характер и политическую окраску генерируемых ответов и комментариев.

С начала 2011 года Пентагон развивает систему SMISC (Social Media in Strategic Communication – в переводе «социальные медиа в стратегической коммуникации»), которая отслеживает все политические дискуссии и устанавливает, является ли это случайным продуктом коллективного разума или пропагандистской операцией со стороны враждебной нации или группы. Проект уникальный тем, что в нем поставлена задача революционного прорыва в использовании сетевых технологий для контроля и управления обществом. В объявлении о приеме заявок на участие в проекте прямо так и сказано – никакие эволюционные методики, алгоритмы и модели не предъявлять. Только революционные.

Проект рассчитан приблизительно на три года. Подрядчики получат в общей сложности около $42 млн. В директивах Пентагона указывается, что «алгоритмы подобных программ направлены на выявление и отслеживание формирования, развития и распространения идей и понятий (мемов) в социальных сетях, что позволит в дальнейшем самостоятельно и умышленно инициировать пропагандистские кампании в зависимости от цели, региона и интересов США»

Заявленные цели проекта, согласно оригинальному описанию, таковы:
-обнаружение, классификация, измерение и отслеживание: а) образования идей и концепций (мемов); б) целенаправленного распространения сообщений и дезинформации;
-распознавание структур пропагандистских кампаний и операций влияния на сайтах и сообществах социальных медиа;
-идентификация участников и их намерений, измерение эффекта кампаний влияния;
-противодействие враждебным кампаниям влияния с помощью контрсообщений.

Фактически SMISC может быстро отмечать слухи и появляющиеся темы в соцмедиа, вычислять, кто и что за этим стоит, и выстраивать противодействие. SMISC способна понять, случайный ли это продукт коллективного разума или пропагандистская операция со стороны враждебной нации или группы. Как только SMISC улавливает, что была запущена операция влияния, она помогает бороться с ней, отправляя контрсообщения. Или самостоятельно запускать манипулятивные процессы.

Обозначен перечень технологий, которые присутствуют в системе: лингвистический анализ, распознавание информационных паттернов, анализ трендов, настроений, общественного мнения и «культурных нарративов», теория графов, автоматическое создание контента, боты, краудсорсинг.

Система ограниченно уже применялась на арабских форумах и социальных сетях для организации «арабской весны» и для дальнейшей координации действий оппозиции.

В интересах Пентагона используются разработанные специалистами BBN Technologies (BBN) системы мониторинга телерадиовещания (Broadcast Monitoring System — BMS) и сети Интернет (Web Monitoring System -WMS). Система BMS реализует возможности автоматической обработки информации на английском, арабском, фарси, мандаринском диалекте китайского и испанском языках. При этом поисковые запросы могут формироваться на английском или языке оригинала. Система WMS обеспечивает возможность мониторинга веб-ресурсов на 75 языках мира и используется в том числе Командованием специальных операций США (SOCOM), Центральным командованием США (CENTCOM) и Командованием спецопераций в зоне Тихого океана (SOCPAC). Единый центр контроля информационного пространства сети Интернет на основе WMS в

интересах указанных трех командований расположен в штаб-квартире SOCOM на авиабазе Макдилл (Macdill AFB) в Тампе, шт. Флорида. Наряду с обработкой информационного контента также производится анализ популярности, структуры и программной части интернет-ресурса. В результате создаются в электронном виде рефераты содержательной части веб-сайтов, а также еженедельные обзоры блогов, форумов и интернет-чатов. Данные материалы размещаются на закрытом портале SOCOM, посвященном проблематике ведения информационных войн (SOCOM IW Portal), и закрытом ресурсе разведсообщества США (Intellipedia). Доступ к ним возможен из защищенных сетей Пентагона и разведывательного сообщества.

Перспективным направлением взаимодействия с BBN Technologies в Пентагоне считают наращивание функциональных возможностей единого комплекса мониторинга и анализа зарубежных СМИ FMMS (Foreign Media Monitoring System), который обеспечивает обработку данных, получаемых в ходе одновременного контроля телерадиовещательных каналов и веб-ресурсов.

ВВС США приступило к подготовке комплексной программы под названием CWOC (Cyberspace Warfare Operations Capabilities) – «Возможности ведения военных операций в киберпространстве». В тендерной документации проекта сказано, что американские ВВС хотят быть в состоянии «уничтожать, ослаблять, нарушать, вводить в заблуждение, искажать и захватывать» компьютерные сети и центры управления противника. В документе, в частности, говорится о «выводе из строя, в том числе при помощи DDoS-атак, заражении и взломе операционных систем, серверов и иных сетевых устройств противника», а также об «установлении временного контроля над киберпространством». Сумма, выделенная на проект, – 10 млн $.

## АНБ

Агентство национальной безопасности Соединённых Штатов (англ. National Security Agency, NSA) — подразделение радиотехнической и электронной разведки Министерства обороны США, входящее в состав Разведывательного сообщества на правах независимого разведывательного органа. Сформировано в составе МО США 4 ноября 1952 года. По числу военнослужащих и вольнонаемных сотрудников и по размеру бюджета является крупнейшим в США разведывательным ведомством. (Wikipedia)

Американское Агентство национальной безопасности (NSA) строит в пустыне в штате Юта самое большое на сегодняшний день хранилище данных. Так называемый «Центр данных Юты» будет последним недостающим элементом в колоссальном комплексе распределенного хранения и обработки информации (помимо уже эксплуатируемых суперкомпьютерных кластеров штаб-квартиры АНБ Форт Мид (шт.Мерилэнд), исследовательского криптоаналитического центра Оук Ридж (шт. Теннеси), дата-центра Лекленд в Сан-Антонио (шт. Техас)). Там же (в Юте) установлен один из самых мощных в мире суперкомпьютеров. Пиковая производительность этой суперкомпьютерной сети пока держится в тайне, но, по оценкам экспертов, она будет составлять не менее 50 петафлоп (10**15 операций с плавающей точкой в сек) – оценки построены на основе энергомощностей комплекса, мощностей охладительных системы и количестве обслуживающего персонала. Площадь объекта 2,3 гектара. Проект First Intelligence Community Comprehensive National Cyber-security Initiative Data Center стоимостью два миллиарда долларов создаётся для

хранения и обработки цифровых данных, собранных в результате слежки: интернет-трафик, видео с камер наблюдения, записи телефонных разговоров и т.д. По оценкам экспертов, дата-центр АНБ сможет хранить и обрабатывать йоттабайты информации.

В США уже несколько лет действуют технологии сквозного мониторинга трафика электронной почты и телефонных звонков. Работы идут в рамках проекта АНБ под названием Stellar Wind, а также силами контртеррористического подразделения ФБР и других правоохранительных органов в рамках системы Threat and Local Observation Database (TALON).

## ЦРУ

Центральное разведывательное управление США, ЦРУ (англ. Central Intelligence Agency, CIA) — агентство Федерального правительства США, основной функцией которого является сбор и анализ информации о деятельности иностранных организаций и граждан. Основной орган внешней разведки и контрразведки США. Деятельность ЦРУ бывает сопряжена с возможностью её официального непризнания. (Wikipedia)

«Центр открытых источников» ЦРУ, который неофициально называют «Vengeful librarians», ведет постоянный мониторинг зарубежных соцсетей, порталов и СМИ, по результатам которого создается ежедневный отчет для Белого Дома. Центр создан в 2001 году.

В настоящее время инвестиционное подразделение ЦРУ «In-Q-Tel» финансирует стартап «Visible Technologies», который занимается разработкой системы мониторинга блогов и социальных сайтов в Сети. Разработка «Visible Technologies» позволяет ежедневно подвергать мониторингу более полумиллиона различных сайтов, проверяя посты в блогах, а также комментарии на форумах и сервисах Flickr, YouTube, Twitter и Amazon. Правда, на сегодняшний день технология Visible Technologies не приспособлена для мониторинга популярных «закрытых» социальных сетей, таких как Facebook.

## МВБ

Министерство Внутренней Безопасности (Department of Homeland Security DHS) «в целях содействия в противостоянии будущим террористическим атакам на Соединенные Штаты и по всему миру» инициировало создание на основе лаборатории Pacific Northwest National Laboratory (PNNL) Национального центра по визуализации и аналитике (National Visualization and Analytics

Center (NVAC)). Позже работы по поиску новых подходов в сфере «визуальной аналитики» в США стали координироваться организацией Visual Analytics Community (VAC), которая стала «площадкой» для создания систем анализа больших данных (в т.ч. и данных социальных сетей).

В 2009 г. сотрудники регионального центра South-East Regional Visualization and Analytics Center (SRVAC) заявили о разработке программного пакета, специально предназначенного для осуществления мультимедийного анализа вещательных каналов на разных языках.

В 2010 г. лаборатория PNLL объявила о создании «набора инструментов визуальной аналитики, который объединяет современные технологии определения характеристик мультимедийных данных, осуществления поиска, фильтрации и классификации и предоставляет конечным пользователям целостный подход для выявления и обнаружения взаимосвязей в мультимедийном пространстве».

В 2011 г. сотрудниками лаборатории PNLL были отмечены две разработки: программный комплекс IN-SPIRE и визуальная аналитическая среда Starlight. IN-SPIRE предназначен для анализа больших коллекций неструктурированных текстовых документов и визуализации его результатов. Визуальная аналитическая среда Starlight представляет собой платформу для визуального анализа, позволяющую пользователям в интерактивном режиме переключаться между различными представлениями информации, например, одновременно работать с временными, геопространственными, сетевыми и другими формами отображения.

### VACCINE

Visual Analytics for Command, Control, and Interoperability Environments Center (VACCINE) – «Центр визуальной аналитики для сред управления, контроля и взаимодействия». Основной задачей центра является «создание методов и инструментов для анализа и управления большими объемами информации во всех сферах деятельности в области обеспечения внутренней безопасности». В том числе и для анализа данный соцсетей.

Проект «Визуальная аналитика для следственного анализа текстовых документов» (Visual Analytics for Investigative Analysis on Text Documents). Разработанная визуальная аналитическая система способна находить и обрабатывать текстовые документы с географической привязкой, идентифицировать интересующую информацию, отображать информацию с помощью интерактивного интерфейса, вводить в интерактивном режиме информацию, выработанную аналитиком, и сразу приводить информацию в соответствие со вновь введенными данными.

Проект «Мультимедийная визуальная аналитика для следственного анализа» (Multimedia Visual Analytics for Investigative Analysis). В рамках этого проекта разрабатывается комплексная система всестороннего визуального анализа мультимедийных данных, которая формирует «потоки событий» либо «кластеры событий». Каждый поток или кластер «начинается» от какого-нибудь значимого события (например, появление в определенное время в заданном месте), которое затем сопровождается потоком связанных текстовых блоков и последующих событий.

### ФБР

Федеральное бюро рассле́дований (англ. Federal Bureau of Investigation, FBI, ФБР) — американское ведомство при министерстве юстиции США, подчиняется Генеральному прокурору. Основано в 1908 году. Входит в состав Разведывательного сообщества США. Имеет полномочия расследовать нарушения федерального законодательства страны и обеспечивать безопасность государства, страны, нации и президента. Гражданам США известна как структура, проводящая общую проверку тех, кто подал заявление на приём на государственную службу. Под общую юрисдикцию ФБР попадают не менее 200 категорий федеральных преступлений. (Wikipedia)


Федеральное бюро расследований США (ФБР) давно следит за общением пользователей социальных сетей Facebook, Twitter и др. и сервиса Skype с целью обнаружения лиц, замешанных в обмене инсайдерской информацией.

В январе 2012 ФБР сообщило, что ищет подрядчиков на создание программы, которая будет предоставлять информацию о возможных внутренних и глобальных угрозах в тех или иных регионах мира на основе данных из соцсетей.

Согласно тендерному объявлению, программа должна собирать информацию из «открытых источников» и иметь возможность:

– Обеспечить автоматизированный поиск и фильтрацию информации из социальных сетей, включая Facebook и Twitter.

– Позволять поиск по новым ключевым словам.

– Отображать различные уровни угроз на географических картах, возможно, с использованием цветового кодирования для обозначения приоритетности угроз. Предпочтительно использование карт Google 3D и Yahoo Maps.

– Предусматривать широкий спектр данных о терроризме — как в США, так и во всем мире.

– Переводить твиты с иностранных языков на английский.

## Google

Инвестиционные подразделения интернет-гиганта Google и ЦРУ вложили деньги в компанию-разработчика программы для мониторинга содержимого Сети в реальном времени. Эта компания называется Recorded Future — ее ПО ежедневно анализирует тысячи веб-сайтов, блогов и аккаунтов на сервисе Twitter, обнаруживая связи между различными людьми, организациями, событиями и происшествиями — как прошедшими, так и возможными в будущем. «Движок временной аналитики» программы умеет «выходить за рамки поиска», обнаруживая невидимые связи между документами, в которых идет речь об одних и тех же или схожих организациях и событиях. Ключевой функцией этой программы является анализ собранной информации на предмет определения лиц, причастных к тому или иному событию, и мест происшествия.

Технология Recorded Future умеет выделять из информации на сайтах отдельных людей, места и мероприятия, упоминаемые ими. После этого программа изучает, где и когда эти мероприятия или события происходят («пространственный и временной анализ»), а также определяет тон этого документа. Далее специальные алгоритмы искусственного интеллекта применяются для того, чтобы установить интересующие связи между различными игроками. На сегодняшний день у Recorded Future есть индекс из более чем 100 млн событий, который хранится на серверах компании Amazon.

Эксперты отмечают, что Recorded Future без сомнений сможет использовать свое ПО для раннего обнаружения различных возможных событий и трендов и для прогнозирования событий.

Кроме того, в лаборатории «Google X» идут работы по созданию искусственного интеллекта для автоматизации общения в соцсетях (читай: для автоматизации активных мероприятий в интернете).

### *Великобритания*

Британская разведслужба **GCHQ** с 2008 года использует программу слежения **Optic Nerve**. Помимо уже ставшего привычным контроля общения в социальных сетях или почтовых сообщений, Optic Nerve позволяет осуществлять перехват видео и текста из чатов пользователей Yahoo, видеочаты Xbox 360 и трафик с веб-камер. Также действует программа Tempora, которая делает возможным подключение к оптоволоконным кабелям, отвечающим за передачу интернет-трафика в Великобританию и из страны.
Но после скандалов 2013 года, связанных с раскрытием информации о программе слежения, правительство туманного Альбиона стало активно легализовывать возможность слежки за гражданами. Так, правительство Королевства закрепило за собой право перехватывать коммуникации в социальных сетях, чьи серверы находятся в Соединенном королевстве или США.

### *В других странах*

В других странах также прекрасно понимают и угрозы в данной области, и получаемые возможности, а по тому также работают над проблемой информационно-психологических войн в интернете.

#### Китай

На слуху у всех Китай. Особенно в разрезе киберпротивостояния с США. Стоит обратить внимание на структуру киберподразделений КНР. «На вершине иерархии» киберподразделений Китая стоит Третье управление Генерального штаба НОАК (управление технической разведки), которое отвечает за организацию и проведение радиотехнической разведки и РЭБ — радиоэлектронной борьбы, а также операций в киберпространстве, в том числе и операций психологического влияния. Кроме того, структура несет ответственность за обеспечение кибербезопасности НОАК. В интересах управления функционирует не менее трех научно-исследовательских институтов и двенадцати оперативных бюро. Управление состоит из множества подразделений, одно из которых (известное как войсковая часть 61398), отвечающее за англоязычные объекты, расположено в Шанхае. Штаб-квартира самого 3-го Управления находится в Пекине, но в Шанхае, Циндао, Чжухае, Харбине, Чэнду и других городах имеются ее подразделения, отвечающие в том числе за радиоэлектронную разведку, перехват электронных сообщений, анализ информации разведывательных спутников, дешифровку сообщений, выявление пропагандистских операций противника и организацию операций влияния.

По данным агентства Mandiant, опубликовавшим 60 страничный доклад о кибервойсках КНР, наиболее активным из китайских участников этой деятельности является отдел «APT1», который, по мнению экспертов американской компании, является организацией операторов, проводящих с 2006 года кампанию кибервоздействия против широкого круга целей. Имеются ввиду как сбор информации (кибер-шпионаж) и противодействие ему, так и мероприятия влияния на граждан противника и противодействия такому влиянию. Авторам доклада удалось установить, что этот отдел размещается в 12-этажном здании в районе Пудонг в Шанхае. В этом же здании располагается и ряд подразделений войсковой части №61398 Народно-освободительной армии Китая (НОАК) и управление информационно-психологических операций в интернете.

Помимо министерства обороны КНР, вопросами обеспечения кибербезопасности также занимается министерство общественной безопасности (МОБ). Основные функции МОБ в сфере

охраны киберпространства осуществляет Департамент безопасности средств связи и коммуникаций, который выполняет следующие меры:

— проведение исследований в области информационной безопасности;

— финансирование академических грантов для проведения исследований по вопросам безопасности в киберпространстве (в том числе среди учебных заведений министерства образования);

— сертификация продукции коммерческого сектора для использования в государственных электронных системах;

— управление компаниями, обеспечивающими безопасность коммерческой информации, и др.

Но ключевую роль в обеспечении информационной и кибербезопасности играет 11-е бюро Министерства государственной безопасности (МГБ) КНР — Радиоэлектронная разведка и компьютерная безопасность (аналог АНБ США). Именно в его ведении выработка стратегии Китая в области кибербезопасности, в том числе и в области информационно-психологических операций в интернете, и координация усилий других ведомств в данной области.

### В других странах

В **Израильской армии** существует так называемое «Подразделение 8200», которое занимается кибервойнами в широком смысле этого слова, от оборонительных и наступательных кибероперациий до операций психологического влияния. Этому подразделению дано право подбирать из числа призывников самых подготовленных молодых людей и стимулировать их к тому, чтобы использовать свой интеллект для борьбы с электронными системами стран-противников или создавать вирусы, применяемые в кибервойне.

Во **Франции** активно работают над данной тематикой. А само направление передано в Управление внешней безопасности Франции (Direction générale de la Sécurité extérieure, DGSE), которое занимается всеми видами операций в киберпространстве, в том числе и психологическими.

В **Германии** направление кибербезопасности передано в Федеральную разведывательную службу (Bundesnachrichtendienst, BND). BND уже израсходовала €6,22 на запуск системы мониторинга сетевого трафика, испытания проводились летом 2014 года. Программа отслеживает данные, находящихся в открытом доступе в соцсетях и блогах, выявляя и блокируя нежелательную информацию на немецком языке, определяя попытки влияния на граждан и подбирая сценарии противодействия таким попыткам. В планах BND также финансирование в размере €4,5 миллионов на проект «Nitidezza» по перехвату и взлому зашифрованного HTTPS-трафика. Не исключено, что к 2020 году часть этих средств будет потрачена на приобретение на черном рынке эксплоитов «нулевого дня» и неопубликованных уязвимостей. На программу будет возложена задача повысить надежность защиты правительственных компьютерных систем, сообщает издание Der Speigel. Помимо перечисленных программ, в разработке находится план мониторинга интернет-трафика за пределами Германии. Например, €4,5 миллиона было в своё время выделено на проект "Swop", который значительно расширил доступ спецслужбы к международному интернет-трафику.

Также известно, что подобные работы ведутся в Индии, в Турции, в Иране, а не так давно очередной раз всплыли данные о Северокорейском подразделение «Bureau 121», которое отвечает за активность в киберпространстве.

## Цели информационной войны

### *Основное*

Основная цель любой информационной войны – деструктивное воздействие на противника. Такое воздействие возможно по нескольким направлениям. Можно оказывать воздействие на саму информацию (уничтожать, модифицировать, украсть). Делать это можно по-разному. Например,

при помощи зловредов – специально созданных программ (они же вирусы, трояны, черви и прочие гадости). Можно воздействовать на элементы инфраструктуры, использующие эту информацию (перехватывать управление, выводить из строя, менять технические характеристики). Опять же можно это осуществить по-разному, в том числе и с помощью зловредов, эксплуатирующих всевозможные уязвимости. А еще можно воздействовать на людей с помощью информации (обманывать, формировать общественное мнение). Такое воздействие нужно для возможности управлять людьми – манипулировать ими – сделать так, чтобы выбранные манипулятором люди совершили нужный ему поступок. Этот поступок может быть действием или бездействием.
Желание действовать или бездействовать достигается через такое воздействие на целевую группу, которое сподвигнет этих людей разделить продвигаемую манипулятором точку зрения (идею, мысль). Другими словами, обрабатываемая группа людей должна в конечном счете иметь вполне конкретное мнение по целевой проблеме. Например, негативное мнение о политике правительства своей страны, а заодно и позитивное мнение о политике правительства манипулятора…

### *Как это решается*

Просто так никто не разделит вашу точку зрения. Если отбросить вариант «за деньги», то для достижения поставленной цели необходимо использовать всё те же «старые, добрые» технологии пропаганды, но с «поправкой» на интернет. Если совсем упростить, то нужно, чтобы продвигаемую идею увидело как можно больше представителей целевой аудитории, увидело как можно чаще, увидело на тех ресурсах, которым больше доверяет, увидело в том контексте (медиа-окружении), который сделает информацию менее отторгаемой… В общем, ничего нового. А кто не знаком с принципами пропаганды – можно и современную рекламу в пример привести. Эксплуатируются те еже механизмы.
Теперь, что нужно сделать, чтобы этот механизм заработал? Тоже ничего нового, но с поправкой на интернет как средство доставки контента до конечного потребителя – в нашем случае, до мишени.

#### Максимально распространить идею

Максимально распространить продвигаемый контент – это значит сделать так, чтобы как можно больше человек увидели его. В определенных кругах эта методика называется «посев» – одна и та же информация многократно дублируется в разных источниках. Как минимум в блогах (созданных специально для этого) и на форумах от лица ников, опять же созданных для распространения. Понятно, что это самая примитивная модель, но даже она работает весьма эффективно, при условии, что распространитель не поленился и сделал достаточно блогов, записей в них, перепостов, зафрендил сторонних пользователей и т.п... «Ложь, повторённая тысячу раз, становится правдой» – этот принцип давно известен и используется. В рекламе он также используется, правда преподносится как средство повышения узнаваемости бренда или что-то в этом роде.

#### Создать видимость массовости

Создать видимость, что продвигаемую вами мысль разделяет большое число людей в интернете, можно с помощью создания видимости активного обсуждения. Это не что иное, как комментирование продвигаемого контента – создание большого числа комментов к материалу за короткий период времени. При этом поначалу в комментариях могут «участвовать» всё те же искусственно созданные аккаунты. И если сами комментарии достаточно интересны или провокационны, то постепенно в процесс втянутся и реальные персонажи. В этом случае материал начнет продвигать себя сам.

#### Создать видимость значимости

В этом случае цель – придать «вес» материалу. Это достигается за счет помещения материал в ТОП обсуждений, в ТОП выдачи поисковиков и т.п. То есть необходимо сделать ваш материал

наиболее комментируемым – содержащим максимальное число комментов. Это непросто. К некоторым публикациям число комментариев доходит до десятков тысяч. Но если в процессе создания «видимости массовости» работа была проделана хорошо, то материал и так уже попадет в ТОП обсуждений за счет числа комментов.
Для попадания же в ТОП выдачи поисковиков на материал нужно сделать достаточное число релевантных ссылок. Но об этом ниже.

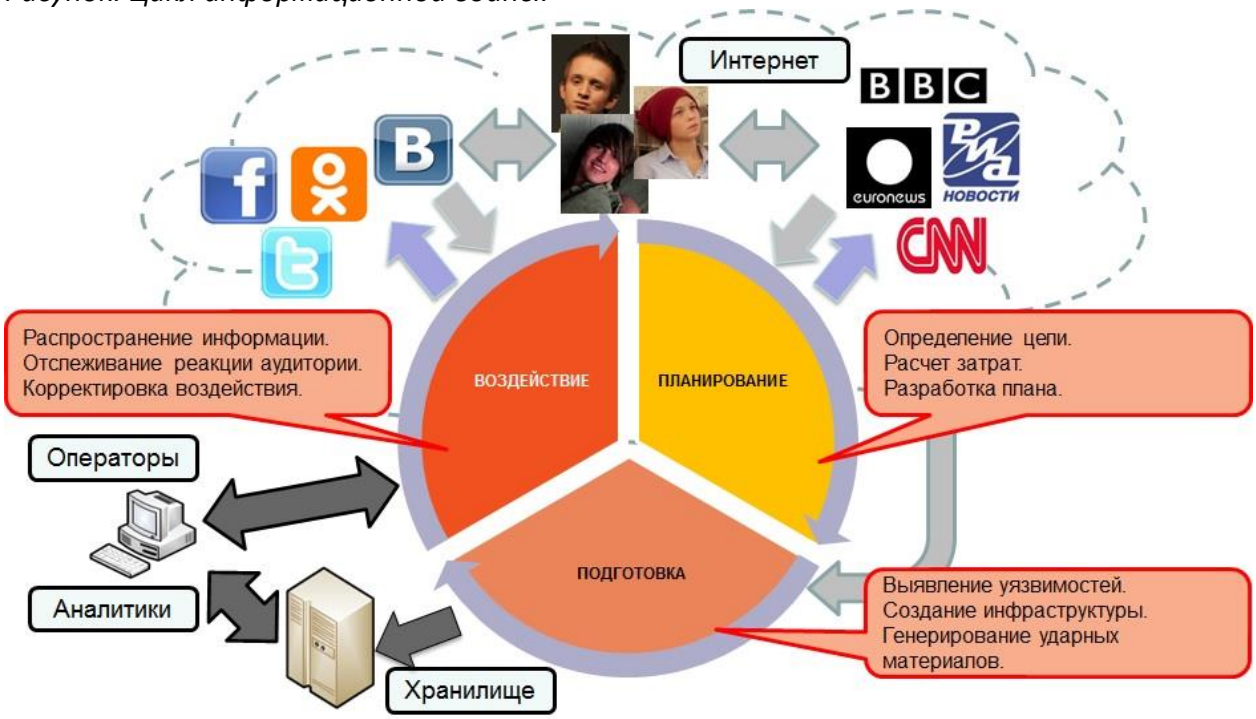
## Основы информационной войны

### *Последовательность шагов агрессора*

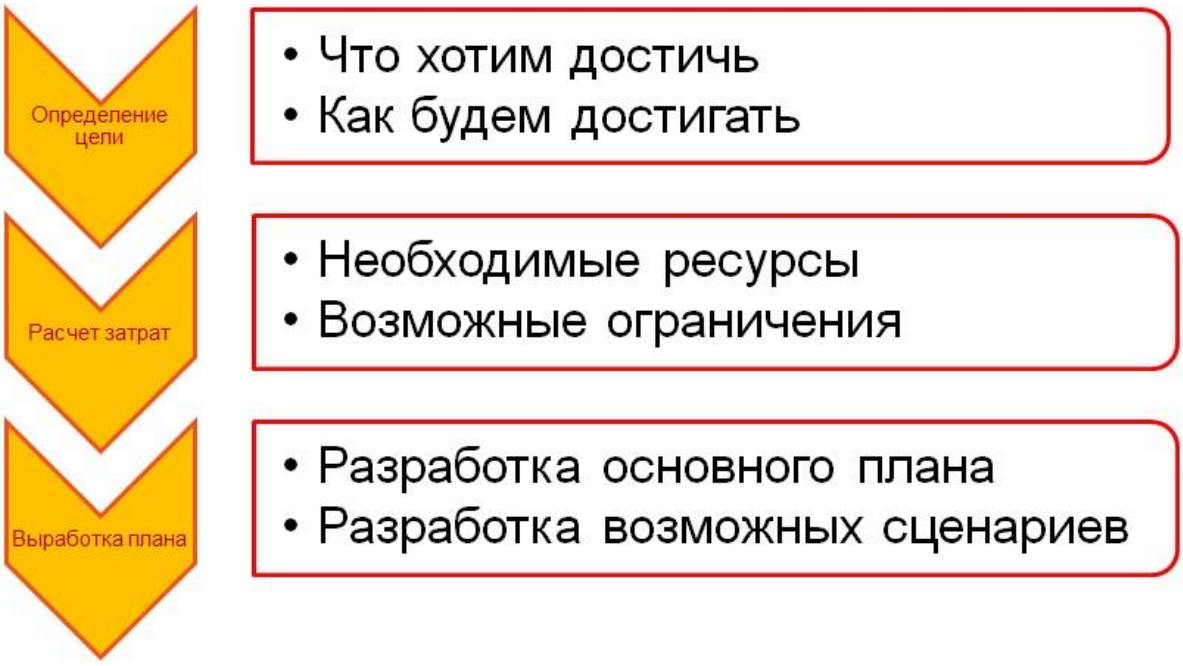
### Цикл информационной войны

Если говорить о «больших проектах», то информационная война имеет определенную цикличность. Связано это с необходимостью корректировать свои действия в зависимости от эффективности воздействия. Начинается все с принятия решения о необходимости проведение этого самого воздействия и определения желаемого результата – **ЦЕЛЕУКАЗАНИЯ.** То есть определяется конечная цель. Без определения конечной цели нет смысла и продолжать. Ведь чтобы выбрать силы и средства для достижения цели, нужно как минимум знать, чего хочется достичь.

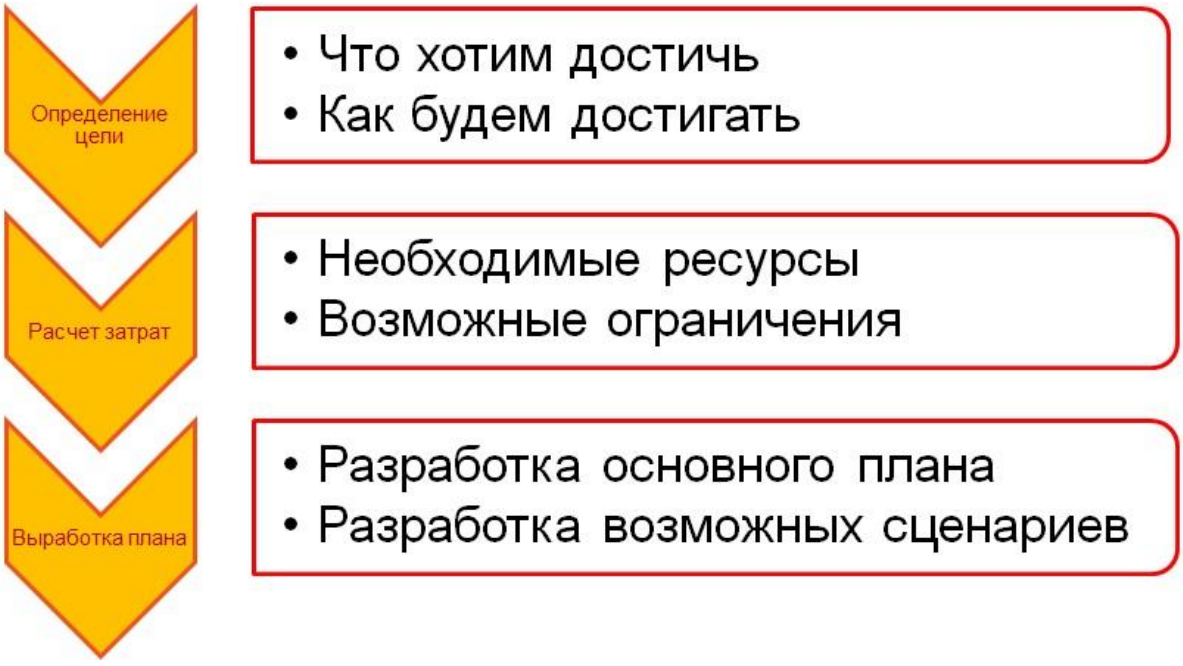
*Рисунок. Цикл информационной войны.*



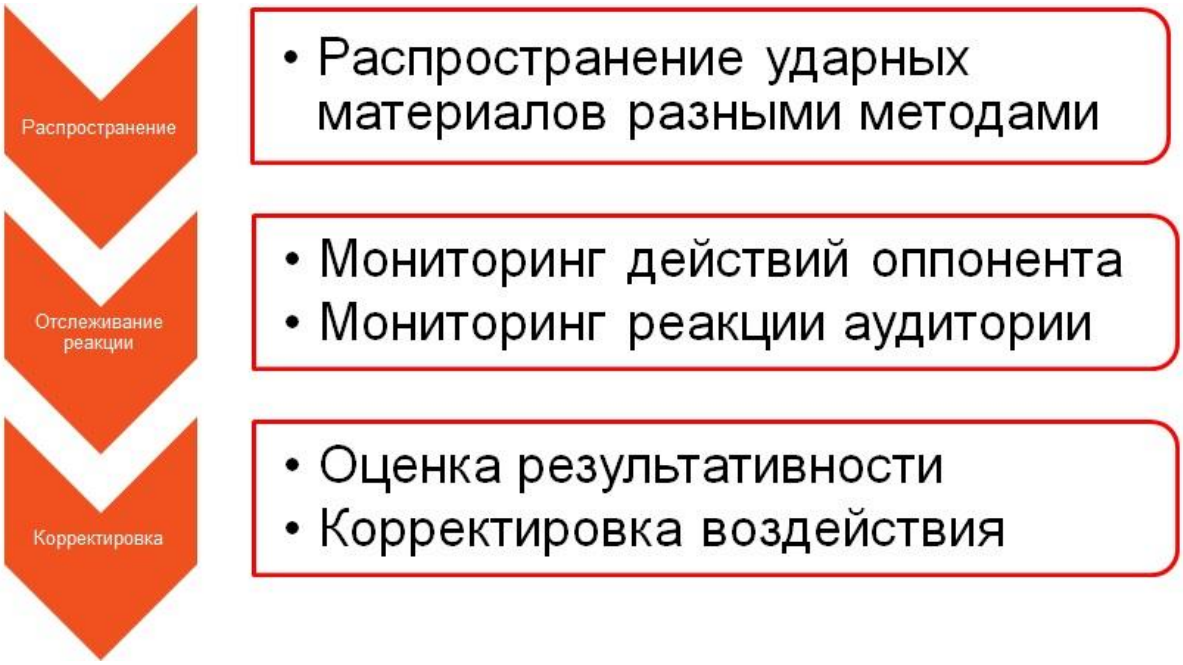

После определения конечной цели начинается разработка стратегии – определение того, как злоумышленник хочет достичь желаемого результата. Начинается **РАЗРАБОТКА СЦЕНАРИЯ** воздействия. Это достаточно объемный этап, так как он включает в себя определение той самой целевой аудитории, на которую будет осуществляться информационное воздействие, выявление ее уязвимостей, которые будут эксплуатироваться в процессе воздействия, и, конечно же, расчет затрат для планируемого мероприятия (число аккаунтов, число публикаций, частота публикаций, число авторитетных источников).




Следующий этап – **ПОДГОТОВКА ИНФРАСТРУКТУРЫ** для планируемой информационной войны. На данном этапе создаются или приобретаются аккаунты в нужном количестве, создается система управления ими, готовится контент (ударный, отвлекающий, провоцирующий), подбираются тролли, писатели (те, что будут создавать новые тексты) и т.п.




После этого начинается **ВОЗДЕЙСТВИЕ** – та часть информационной войны, которую мы чаще всего наблюдаем. А через какое-то время осуществляется **КОНТРОЛЬ ЭФФЕКТИВНОСТИ** воздействия – проверяется, не достигли ли мы цели, не отклонились ли от плана и т.п. Если всё идет по плану, то хорошо, а если нет, то вносятся коррективы в процесс воздействия. Кроме того, по мере противоборства может измениться и сама ситуация (могут поменяться приоритеты, ослабнуть или усилиться какие-то факторы). В этом случае вносятся изменения в целеуказание и цикл повторяется вновь.




## Целеуказание

Первым шагом в разработке плана информационной войны со стороны злоумышленника является четкий ответ на вопрос, чего собственно он хочет? Для этого ему нужно определить цели воздействия на объект. От поставленной цели зависят и способы воздействия, и необходимые ресурсы.

Например, у заказчика есть конкурирующая фирма, обладающая интересующей частью рынка. Обычными экономическими мероприятиями провести экспансию на рынке не удается (то ли возможностей нет, то ли запас прочности у конкурента солидный). Соответственно, задачей субъекта является захват рынка, а способом ее реализации – устранение влияния конкурента, и последнее становится задачей для разработчиков психологического воздействия на коллектив конкурента. Следовательно, целью действий нанятого им специалиста по психологическому воздействию, в зависимости от ситуации, можно назвать дестабилизацию экономического состояния конкурента неэкономическими методами, т.е. саботаж работы предприятия его же сотрудниками, уход из компании наиболее ценных сотрудников, раздор между лицами, принимающими решения и т.п.

### *Изучение объекта воздействия*

Вначале агрессор должен определить, какая информация нужна для реализации проекта, выявить ее источники, способы ее получения и произвести сбор информации. Полученная информация обрабатывается и анализируется. Одной из основных целей такого исследования является выявление уязвимостей объекта воздействия (население страны, региона, этническая группа, определенный социум). В ходе такого изучения выявляются объекты непосредственного воздействия (те, на кого будет направлено целевое воздействие), их уязвимость с точки зрения психологического воздействия, восприимчивость к тем или иным раздражителям, особенности характера и поведения… Объектами воздействия в данном случае являются группы людей с какими-то общими признаками, интересами и т.п., реже отдельные люди (в случае подбора «ретрансляторов» и лидеров мнения).

Затем выбранная целевая аудитория изучается с точки зрения условий обстановки, восприимчивости, уязвимости. Условия обстановки – это те условия их окружения, которые оказывают значимое влияние на них. Это могут быть социальные, экономические, физические, географические условия… Особое внимание будет уделено системе власти и подчинения объекта, системе выработки, принятия и исполнения решений, трудностям управления, нестыковкам и промашкам руководства, недовольству руководством. Также внимание уделяется острым социальным проблемам, которые касаются многих, конфликтам (особенно затяжным) и их подноготной, существующим группам и группировкам (их особенностям, ресурсам, зависимостям…), реальным и скрытым лидерам, удовлетворенности оплатой и отношению к руководству, коррупции и системе безопасности, связям с другими сообществами (в т.ч. странами, движениями), экономическому положению, проводимой политике на рынке, честности бизнеса, связи с криминалом и силовыми структурами, корпоративной культуре, способам выхода из критических ситуаций… Затем противник постарается выявить уязвимые стороны целевой аудитории. Это побуждения аудитории, подверженность стрессам и устремления, управляемость и устойчивость. Будут выявлены те темы, которые «цепляют за живое» большинство членов исследуемой общности или как минимум лидеров мнений и неформальных лидеров. После этого им определяется восприимчивость аудитории к тем или иным воздействиям. Часто это осуществляется с помощью реальных воздействий – эдакая разведка боем. Она во многом зависит от потребностей участников аудитории, побуждений и направленности действий.

### *Выбор тематики и символики воздействия*

Противник будет осуществлять выбор тематики и символики психологического воздействия в зависимости от уязвимости и восприимчивости целевой аудитории и поставленных задач. Тематика – предмет (сюжет) или направленность мероприятий, проводимых для достижения цели психологического воздействия. Тематика – связующее звено между уязвимыми сторонами и характером поведения объекта, обычно это «раскол группы», «принуждение к определенным действиям», «отказ от каких-то действий»… При выборе тематики противник должен учесть такие требования, как:

- содержание материала должно быть простым – легким в восприятии и осмыслении;
- тема должна быть ориентирована на понятные объекту нужды;
- тема должна иметь завершенный смысл;
- тема не должна содержать насмешек над объектом воздействия.

Тематика воздействия раскрывается посредством символики, которая может быть текстовой (статьи, лозунги, сообщения), визуальной (фото и видео материалы, предметы, картины), или звуковой (призывы, слухи, музыка). Символика используется для выражения идей и упрощения восприятия целевой аудиторией этих самых идей. Она должна быть проста, понятна, популярна и не противоречить морально-этическим нормам объекта. Чем символ понятнее, проще в запоминании и ближе к нуждам и чаяньям объекта воздействия, тем больше шансов, что он осядет в сознании и начнет свою постепенную, незаметную разрушающую работу.

### *Выбор средств и способов преподнесения и распространения информации*

Выбор способа предоставления информации объекту воздействия будет осуществляется злоумышленником на основе тех же критериев: доступность, понятность, популярность, непротиворечие морально-этическим нормам. При этом могут быть использованы неофициальные и официальные каналы. К официальным, в данном случае, следует отнести

СМИ, информация в которых может быть действительно официальной, а может быть заказной. К неофициальным каналам соответственно относятся соцсети, форумы, блоги, слухи. Для наибольшей эффективности информация из любых источников должна, помимо перечисленных свойств, обладать следующими: достоверность либо видимость достоверности, желательно подтвержденная хотя бы косвенно иными источниками; своевременность, т.е. появиться она (информация) должна в период информационного голода по данной тематике; востребованность как следствие своевременности, а источник информации должен вызывать доверие или уважение.
При выборе средств распространения информации противник будет учитывать следующие критерии:
- возможность доведения информации до целевой аудитории – информация должна быть доведена именно до тех, на кого направлено воздействие;
- восприимчивость объекта – объекту должна быть понятна доводимая информация, а также она должна вызывать планируемые реакции;
- наличие средств на реализацию – сам процесс должен быть недорогим (по возможности) как для объекта воздействия, так и для оператора;
- источник информации должен вызывать доверие у аудитории;
- своевременность доведения информации.

### *Разработка собственно метода воздействия*

Данный этап состоит из двух. На первом противник сведет воедино собранную и синтезированную информацию. Конечным результатом этого подэтапа является получение более или менее четких ответов на следующие вопросы:

- что представляет собой мишень информационной атаки (целевая аудитория), каковы ее уязвимые места, слабости, темы воздействия;
- к чему нужно сподвигнуть целевую аудиторию;
- как можно использовать уязвимости выбранной целевой аудитории для достижения поставленной цели;
- с помощью каких образов (тем) можно воздействовать на выбранные уязвимости;
- когда следует начать воздействие, чтобы достичь максимального эффекта;
- какими средствами следует это воздействие осуществить?

В процессе подготовки противник постарается выбрать наиболее оптимальный метод воздействия. Чаще всего для скрытого воздействия используется такой инструмент, как слух. Слух – это специфический вид коммуникаций, возникающий спонтанно, либо искусственно. Слух может быть либо следствием информационного голода, либо особой популярности данной темы. А запустить слух в эпоху интернета не составляет никакого труда.
После проработки всех моментов и проведения подготовительных мероприятий ваш противник приступит непосредственно к реализации намеченного плана, в процессе чего он должен следить за реакцией аудитории и при необходимости вводить коррективы.

### *Пси эффекты*

«Все старо как мир» и используемые приемы информвойны в интернете в общем-то уже давно изобретены и применяются в пропаганде и рекламе. Основываются эти приемы на вполне определенных эффектах восприятия человеком информации, восприятия подсознательного и потому трудно поддаются управлению самим человеком без специальной подготовки. Таких эффектов довольно много, и они хорошо описаны в соответствующей литературе по психологии, социологии и т.п. Я же предлагаю остановиться на тех из них, которые наиболее часто используются в информационных войнах.

### Эффект «первой любви»

Что первым узнал – тому и больше веришь. Так уж устроен человек, что информация, узнанная первой, пользуется большим доверием. Ведь она уже «закрепилась» в голове, заняла место, «обросла» связями с другой информацией. И чтобы противоречащей информации «закрепиться» в той же голове, ей нужно сначала вытеснить уже имеющуюся. А это сложнее, чем просто осесть на незанятую территорию. Именно по этой причине чиновники так стремятся первыми доложить руководству (так преподнести информацию, как это выгоднее им). Именно по этой причине так стремятся первыми «осветить» какое-то событие всевозможные центры влияния – чтобы подать информацию в нужном свете, с выгодой для себя, даже если событие не в их пользу. Именно по этой причине такое «освещение» событий распространяется максимально широко с помощью ботов, троллей и репостинговых сетей – чтобы интернет был заполнен именно этим, выгодным для инициатора, вариантом объяснения события, чтобы как можно больше пользователей, зайдя в инет, ознакомились первым делом именно с этой трактовкой события.

### Эффект стадности

Какое мнение больше людей поддерживает – то и правда. И это срабатывает очень часто. Мы идем туда, куда идет толпа, мы соглашаемся, когда нас убеждают все коллеги, нам психологически проще принять точку зрения большинства, чем стать «белой вороной». А потому, если «все говорят – черное», значит, так оно и есть, и неважно, что это лишь иллюзия, созданная кем-то. Есть и обратная сторона данного эффекта. Это страх – если все вокруг убеждены, что черное – это белое и агрессивно отстаивают свою точку зрения, то очень не хочется высказывать свое мнение, не совпадающее с мнением этих «всех». Мало ли что – ведь могут и оплевать, а то и побить… В этой ситуации человек даже не задумывается, что как раз его точка зрения – это точка зрения большинства, а беснующаяся толпа всего лишь искусственно созданное впечатление о реальном положении дел. Именно так большинство начинает подчинятся меньшинству. Этот эффект еще называют «социальным доказательством» (social proof). Наиболее эффективен он в ситуациях, когда разобраться сложно (уж очень запутанно всё), времени на разбирательство нет, а решение принять надо. Вот тут-то мы и смотрим, как все делают, и полагаемся на мнение большинства, забывая, что это мнение вполне может оказаться иллюзией, созданной для нас манипулятором. Этот эффект еще называют «спираль молчания». Объясняется он страхом социальной изоляции и начинает работать в тот момент, когда кто-либо уверенно высказывает свою точку зрения на социально значимую тему. Несогласные с услышанным предпочитают хранить молчание и не высказываться, ведь убеждены, что находятся в меньшинстве, и боятся изоляции.

### Эффект многократного повторения

Этот эффект давно и успешно применяется в рекламе – важно, чтобы продвигаемый товар (бренд, идея) как можно чаще попадались на глаза представителям той социальной группы, в которой это продвижение осуществляется. Помните? – «ложь повторенная многократно…». Причем не нужны доказательства, факты, объяснения и прочее. Достаточно повторения частого и регулярного. Именно для этого одна и та же мысль (идея, сообщение) в мероприятиях манипулирования повторяется многократно вроде бы разными людьми (например, аккаунтами в соцсетях) с некоторой разницей в подборе слов, но с неизменной смысловой нагрузкой.

### Эффект групповой поддержки

Если человек ассоциирует себя с некой социальной группой, то он с гораздо меньшей критичностью воспримет идеи и ценности, поддерживаемые этой группой. Уж так воспитывала человека мать природа, регулярно показывая, что выжить можно только в группе. И чем группа больше, тем выше вероятность выживания. Ничего не напоминает? Например, группы в социальных сетях…

### Апеллирование к авторитету

Готовность людей идти за лидером также обусловлена особенностями исторического развития человечества. И эту готовность весьма успешно эксплуатируют для манипулирования. Вспомните «По данным Британских ученых…», «По мнению ведущих политологов…» – это использование неперсонализированных лидеров мнений. А вот «Президент международной ассоциации стоматологов Иван Иванов считает…» – это уже персонализированный авторитетный источник (лидер мнений). Второй вариант предпочтительнее, так как люди охотнее верят, когда знают (или думают, что знают), от кого исходит информация. Именно для эксплуатации данного эффекта используются разнообразные заявления-демарши-выступления звезд эстрады, кино, литературы… Эти люди своим именем, с одной стороны, придают информации больше достоверности, а с другой – делают саму информацию более значимой – «Если уж ОН так считает…».
Интересным вариантом «авторитета» является манипулирование числами. Дело в том, что для людей непосвященных числа являются чем-то очень точным, а потому достоверным. А информация ими насыщенная гораздо легче принимается сознанием. По этой причине манипуляторы стараются сопроводить свои публикации «точными» цифрами.

### «На воре шапка горит»

Кто оправдывается, тот и неправ. Чем больше вы оправдываетесь, тем сильнее вам не верят. Особенно хорошо работает в сочетании с эффектом «первой любви». Кто первый обвинил (бездоказательно), тот и оказывается в более выигрышном положении. Отмываться всегда сложнее, чем обливать грязью. Вот и получается, что тактически выгоднее обвинить первым. Но если такое обвинение сфабриковано и дезавуировано оппонентом, то эффект может получиться обратным. Необходимо, чтобы противник не смог, не успел, не сообразил, не захотел нейтрализовать обвинение. Для достижения такого эффекта частенько стараются организовать поток обвинений. Пока оправдывается по первому обвинению, его уже обвинили еще в пяти грехах, и противник уже не успевает оправдаться, а обвинения «закрепляются» в головах аудитории.

### «Социальность» информации

Сообщению человека мы больше доверяем, чем сообщению информационного агентства или официальному обращению чиновника любого ранга. А если увидели общение двух человек по интересной нам теме, то, скорее всего, это так и есть (как они описывают), ведь мы «подслушали» чужой разговор – их же никто за язык не тянул, они не знают, что мы их читаем, они обменивались информацией между собой, а не ставили цель манипулировать нами…. И забываем, что этот подслушанный разговор мог быть специально инсценирован для нас с одной целью – создать иллюзию достоверности.

### Манипулирование терминами

Явно негативную идею нельзя просто дать целевой аудитории в качестве альтернативы. Нужно сделать так, чтобы люди менее критично воспринимали эту идею. Возможно, не получится сделать идею привлекательной, но можно ее сделать менее неприятной. Это позволит снизить порог тревожности и «зацепиться» за подсознание. Например, американская администрация во время войны во Вьетнаме называла уничтожение деревень напалмом «операциями умиротворения». Звучит не так неприятно, а потому легче принимается целевой аудиторией. Джордж Оруэлл писал, что на войне солдаты не умирают, а «героически погибают». Солдат, который идет служить в армию, не тратит годы жизни на службу режиму, он — «отдает долг Отечеству». Такая простая замена слов полностью меняет образ одних и тех же событий и позволяет преодолеть порог отторжения в сознании человека.

### Сделать идею привлекательной

У манипулирования терминами есть более сложное продолжение – внедрение в общественное сознание нужных идей, ранее воспринимаемых негативно. Вначале идея преподносится как предмет обсуждения (обсуждение этичности, целесообразности, опасности… чего угодно). Цель –

вызвать привыкание. Когда у аудитории наступает привыкание, идея начинает преподноситься как предмет научного исследования. Далее – как нечто не такое уж и неприятное. И позднее – как вполне возможное.

### Негатив

Так человек устроен, что он скорее поверит негативной информации. Видимо, в силу народной мудрости «лучше готовиться к худшему, тогда лучшее будет приятным сюрпризом». Уж очень много плохого пришлось пережить людям за свою историю. Вот и выработался рефлекс. А потому гораздо проще поверить в негативную информацию, а не в позитивную. Такое же положение дел наблюдается и в СМИ – более рейтинговыми оказываются негативные новости. Этим пользуются и манипуляторы.

### Юмор

Однако информация, смешанная с юмором, легче преодолевает внутренние психологические барьеры. Связано это с тем, что юмор снижает нашу тревожность, а потому нас проще обмануть в хорошем настроении. Сознание, находящееся в благодушии, менее осторожно, более доверчиво. Вот почему высмеивание так эффективно в распространении негатива об объекте.

### Визуальный контент

Картинки, демотиваторы, видеоролики, звук и прочие варранты воздействия, помимо текста, делают это воздействие значительно более эффективным. Происходит сие из-за того, что при такой подаче информации воздействие на наше сознание осуществляется по нескольким каналам одновременно. И наше сознание, атакованное по нескольким направлениям, быстрее сдается.

## *Технологические эффекты*

Все эти психологические эффекты воздействия на нас при использовании интернета как канала воздействия эксплуатируют еще и уникальные свойства самого канала распространения информации. Те самые свойства, которые открывают безграничные возможности как для добропорядочного пользователя, так и для злоумышленника.

### Скорость распространения

Информация в инете распространяется очень быстро, в т.ч. и цитированием первоисточника, ссылками на него и его комментированием, лайками, репостами. Только вы нажали кнопку «Опубликовать», и введенная вами информация становится доступна всем без исключения пользователям интернета. Ни одно бумажное СМИ не может похвастаться такой скоростью распространения контента.

### Отсутствие границ в интернете

Информацию можно получать из любых источников, в т.ч. и в других странах, на других континентах, и распространять ее можно на любых территориях, никак не отвлекаясь на географические и административные границы. Любая информация доступна из любой точки планеты, где есть интернет, что позволяет злоумышленнику напрямую обратиться к любой аудитории.

### Анонимность

В инете можно оставаться анонимным, если принимать соответствующие меры. А это значит, что один и тот же человек может выступать под неограниченным количеством ников, аккаунтов, личин… Один человек (оператор) может управлять армией виртуальных личностей (виртуалов), которые на разные голоса будут продвигать одну и ту же идею.

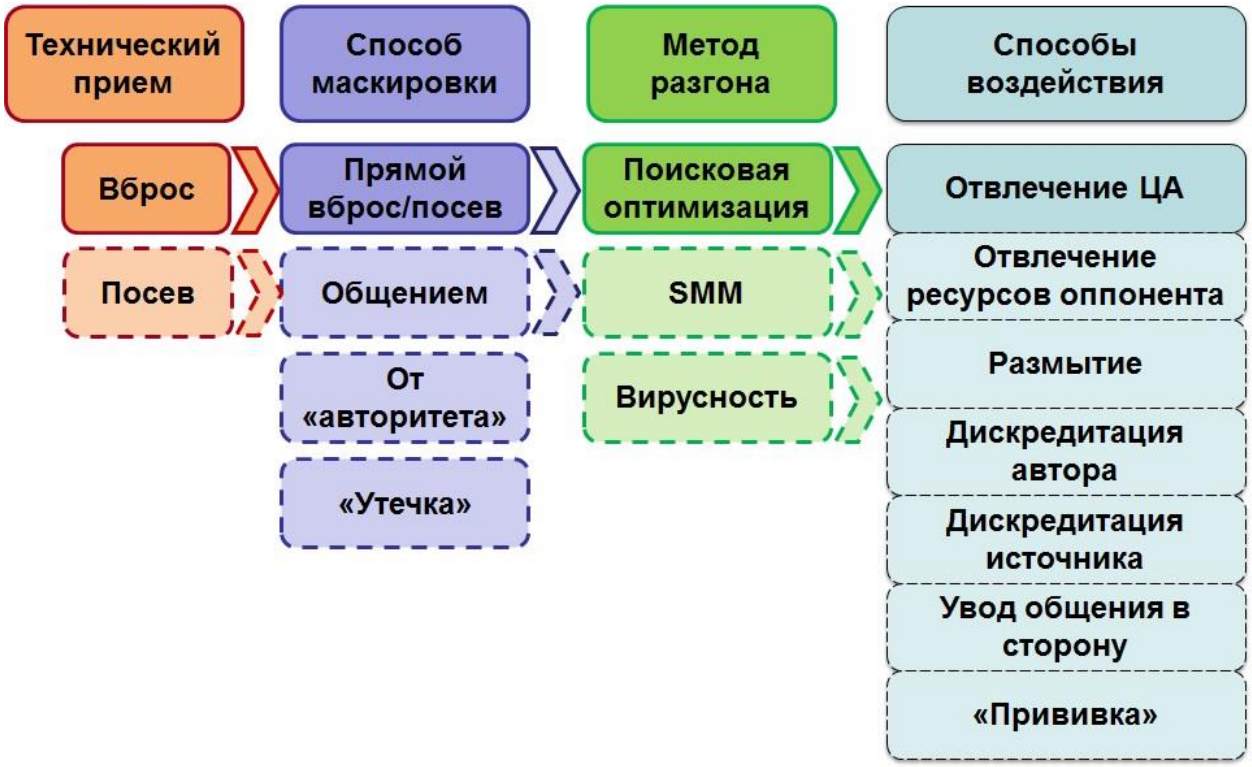
### Продолжительность хранения

В инете информация может храниться бесконечно долго. Точнее – пока существует интернет. Мало того, информация в процессе дублирования храниться уже не в одном месте, а во многих.

Это система распределенного хранения с независимой системой безопасности мест хранения. Это очень высокая надежность хранения.

### *Приемы информационной войны*

Технически метод распространения в интернете информации один – публикация или вброс. А дальше идет применения способа маскировки, способа разгона и используемой технологии воздействия на аудиторию.



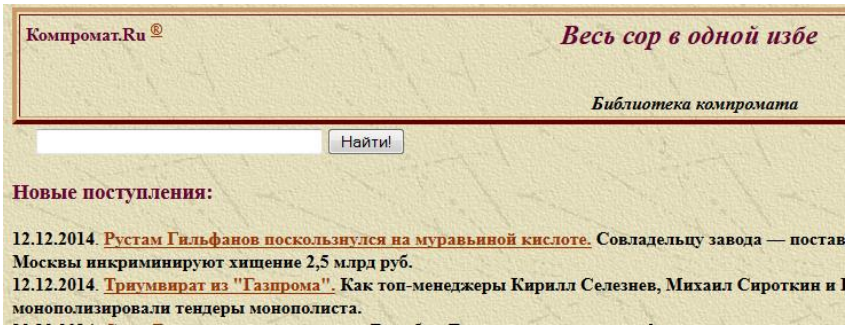

#### Вброс

Вброс – это доведение до целевой аудитории информации, способной вызвать резонанс. Смысл мероприятия сводится к разовому созданию у аудитории определенного настроения (мнения). Это самый простой и самый используемый прием информационных войн. Он связан с рядом особенностей и ограничений. Например, чаще всего вбрасываемую информацию необходимо легализовать, дабы не подставить источник или не подставиться самому. Также необходимо организовать доведение вбрасываемой информации до нужной целевой аудитории (чтобы она обязательно ознакомилась). Это технические вопросы, решаемые по-разному в зависимости от аудитории, вбрасываемой информации, оператора и поставленных задач, а сами вбросы породили целое «семейство» родственных приемов. Например, массовый вброс однотипной (или идентичной) информации стали называть «посевом». Вот некоторые из них.


Вице-президент США Дик Чейни неоднократно публично повторял утверждение о встрече некоего Атты (лидера террористов) с иракцами в Праге в качестве одного из ключевых доказательств причастности Багдада к теракту в США. А Колин Пауэлл заявлял о наличие у Хусейна химического оружия и иллюстрировал свои слова колбой с чем-то непонятным. На деле всё это оказалось обманом, но вброс от «авторитетного» источника сделал своё дело – общественное мнение было сформировано нужным образом.


## Легализация

Легализация информации – это действие, направленное на то, чтобы получить возможность открыто использовать информацию в каких-то целях. Такие действия необходимы, если информация получена неправомерно (прослушка телефонных разговоров, взлом почтового ящика) и ее обнародование влечет уголовное преследование или общественное осуждение. Или если необходимо скрыть источник этой информации (не подставить информатора). Или если инициатор не уверен в достоверности данных и хочет остаться в тени в случае их разоблачения. Этот вариант характерен для вброса явной дезинформации (фейков) от имени виртуальных личностей в соцсетях. Эти самые виртуалы создаются массово и подразумевают в качестве владельца не реального человека, а оператора, часто управляющего некоторым числом таких виртуалов. Таким оператором может быть человек или программа. Примеров легализации достаточно много. Самые известные – это публикации содержимого почтовых ящиков от имени разнообразных «кибер-активистов» и хакерских групп. А имена этих хакерских групп нередко используются без их ведома для мероприятий легализации. Другой пример – разнообразные «сливные бачки» – сайты, публикующие всевозможный жареный материал, от известных КомпроматРу, WikiLtaks и Шалтай-Болтай до имитирующих СМИ.


## Вброс – извинения

Информационная война всегда нацелена на манипулирование людьми. Это главная цель – подтолкнуть к каким-то действиям или к воздержанию от действий. Объект манипулирования должен поступить так, как нужно манипулятору. Достигается это разными способами, но с технологической точки зрения это снабжение объекта манипулирования (или целевой аудитории) специально сформированной информацией. Если сказать по-другому – дезинформирование. Вопрос только в том, как сделать так, чтобы объект снабжался этой дезинформацией.

Один из способов на профессиональном сленге называется посев. Это не что иное, как массовое распространение однотипной или идентичной информации. Цель «забить» нужный сектор интернета специально подготовленной информацией так, чтобы целевая аудитория (объект манипулирования) обязательно и в первую очередь с ней ознакомилась. Делается это с помощью виртуальных личностей – аккаунтов в социальных сетях, созданных специально для этой цели. Чтобы быстро накрыть нужный сектор интернета, бывает необходимо очень много таких виртуальных личностей. Это накладывает некоторые ограничения на скорость осуществления такого мероприятия.

Есть несколько иной путь – сделать так, чтобы ваш материал многократно продублировали СМИ и реальные люди в соцсетях. Для этого нужно, помимо интересности самого материала, чтобы первоисточник вброса обладал определенной авторитетностью. Для создания такого источника нужно время, а времени обычно нет. Особенно когда информационная война уже идет и реализовывать решения нужно быстро. В этом случае используется уже имеющиеся источники с наработанным авторитетом. Это может быть интернет-СМИ, известный блогер, интернет-вариант офлайнового СМИ или ТВ-канала. В общем, источник, который давно работает в интернете и имеет свою обширную аудиторию. И конечно же, чем известнее имя этого источника, тем шире охват и сильнее влияние.

И вот тут начинается проблема выбора. Вбросить-то нужно недостоверную информацию. И после выявления ее недостоверности источник будет дискредитирован, а этого допустить нельзя – уж очень непросто создать новый авторитетный источник. Что делать?

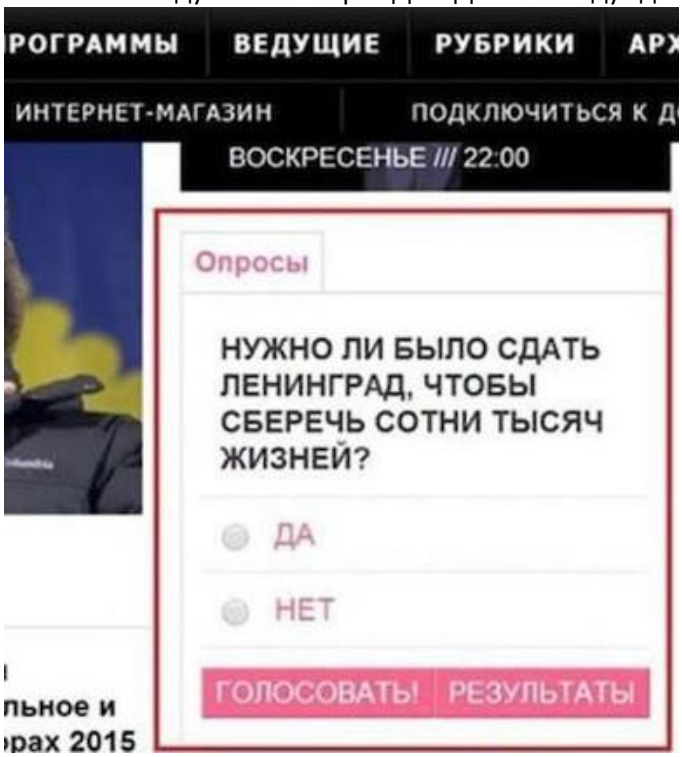
Вот в таких случаях и используют прием под условным названием «вброс-извинение». Его смысл заключается в выводе из-под ответного удара своего источника. После того, как сделали вброс нужной информации. Конечно, мнение об источнике будет поколеблено, но не столь радикально, как если бы был сделан просто вброс.

Суть приема сводится к тому, что в инфополе выбранной целевой аудитории осуществляется вброс явно провокационной информации, информации, которая противоречит морали, устоям общества, нормам поведения… А в случае бурной ответной реакции – извинения за ошибку, непродуманные действия, неграмотность. В результате, с одной стороны, целевая аудитория получает порцию модулирующей информации, а манипулятор остается без наказания. С другой стороны, даже если у основной части целевой аудитории ударная информация и вызовет отторжение, тем не менее она (информация) окажет воздействие на сомневающихся или на тех, кто не в курсе, и это уже неплохой результат.

Это очень удобно – сделал своё дело и вроде как не виноват – извините мы не в курсе, не подумали, не знали, не могли предположить… И примеров использования такого приёма с каждым днем всё больше. Это объясняется простотой самого приёма – не нужно серьёзной

подготовки. Проработки, продумывания, легендирования, организации путей отступления на случай неудачи. Помните – в феврале 2014 года CNN назвала монумент в Брестской крепости – памятник мужеству советского народа в годы Великой Отечественной войны – «уродливым»?


А якобы необдуманный опрос ДОЖДя по поводу сдачи Ленинграда фашистам?




А недавняя провокация с комплексом «Родина-мать зовет!» на Мамаевом кургане? Когда американский интернет-сайт Business Insider, посвящённый новостям бизнеса и технологий, составил рейтинг «самых абсурдных строений советской эпохи, которые до сих пор стоят». Наряду с различными зданиями и мемориалами стран бывшего СССР и Восточной Европы, в список была включена статуя «Родина-мать зовёт!», расположенная на Мамаевом кургане в Волгограде.

### *Как это делают*

Выбирается тема, требующая с точки зрения манипулятора корректировки или являющаяся ключевой в интересующей проблеме. Это может быть нечто, являющееся «фундаментом» морали общества, нечто неоспоримое, нечто не вызывающее сомнений.

Далее проводится подготовка – обсуждение темы в нейтральных тонах и вовлечение в это обсуждение наибольшего числа участников из числа нужной ЦА.

После этого осуществляется основной вброс уже той самой «ударной» информации. Информации, моделирующей нужное поведение целевой аудитории или вызывающей нужную реакцию.

Когда «ударная» информация доведена до целевой аудитории, осуществляется «отступление» – извинение за необдуманные действия, внутреннее расследование, посыпание головы пеплом… Но это не более чем способ уйти от ответственности. Ведь запланированное мероприятие осуществлено – выбранная аудитория была ознакомлена с «ударной» информацией и подверглась манипулирующему влиянию.

### *Зачем это делают*

Этот прием является одним из многих в информационной войне, а потому конечная цель его такая же, как и у других аналогичных технологий – управление поведением аудитории. Поэтому основной вопрос всегда один – кто та самая целевая аудитория? Для ответа на него нужно понять, как данная технология воздействует на разные аудитории.

### *Люди противника*

Если целевая аудитория – люди противника, то информация, прямо противоречащая нормам их общества, скорее всего, не сможет оказать хоть какого-то воздействия на зрелых людей. Разве что только на предварительно подготовленных. Но вот на подрастающее поколение воздействие вполне возможно. Связано это с тем, что молодежь, а тем более тинэйджеры, более подвержены подобному воздействию в силу отсутствия у них значимого негативного опыта. А рассказы старшего поколения воспринимаются не более чем байки.

Применение данной технологии по отношению к людям противника ведет, в конечном счете, к расколу общества, к появлению группы, разделяющей вашу точку зрения, а не точку зрения своих единоверцев. Если же в результате воздействия не удалось достигнуть хоть сколько-нибудь значимого успеха, то атакующему удается выяснить «расклад сил» в атакуемом обществе, наличие или отсутствие уязвимостей общества, понять реакцию общества на раздражители. Это, конечно, не совсем то, на что рассчитывал атакующий, но это уже данные, которые позволят выбрать более удачную тактику для следующего воздействия.

### *Свои люди*

Данная технология еще более эффективна по отношению к «своим» людям. Ведь в этом случае воздействие идет на уже подготовленную аудиторию, аудиторию, которая априори более благосклонно воспринимает информацию манипулятора, аудиторию, которая уже думает почти так, как нужно манипулятору. А потому и воздействие на нее гораздо более эффективно. Работая по «своей» аудитории, манипулятор, используя технологию «вброс-извинения», обычно преследует цели дискредитации противника в глазах своих граждан, формирования в обществе нужного ему отношения к проблеме, к противнику.

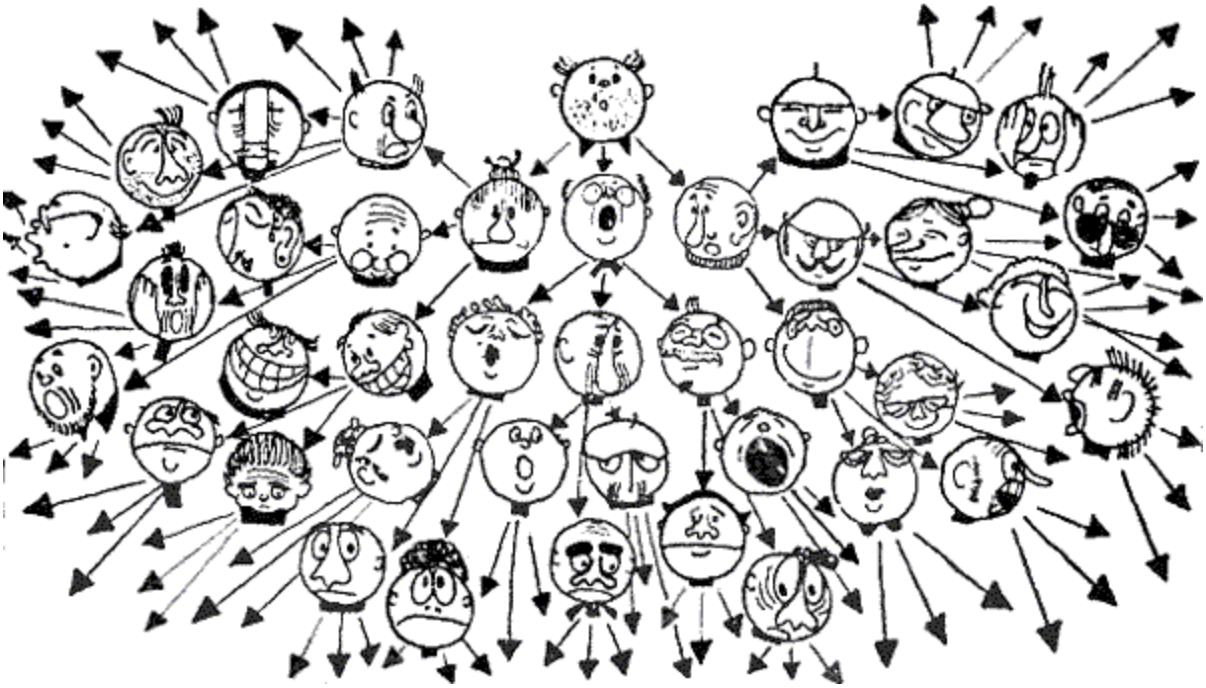
### *Как этап проекта «Окно Овертона»?*

Наблюдаемое сейчас активное использование данной технологии на разных уровнях не случайно, а, скорее всего, является этапами более глобального мероприятия. Уж очень хорошо все эти

события укладываются в общую схему, которая уже была использована в легализации гомосексуализма на западе. Речь о технологии, описанной Джозефом Овертоном, – окно возможностей Овертона (The Overton Window of Opportunity) или кратко «Окно Овертона». Еще его называют «окно политических возможностей» (window of political possibility).
Суть технологии в том, что требуемый сдвиг мнений в обществе разбивается на несколько шагов, каждый из которых не является радикальным, а сдвигает восприятие идей лишь на одну стадию, а общепринятую норму к его границе. Это делает возможным последующий сдвиг так, чтобы достигнутое положение снова оказалось не радикальным по отношению к предыдущему этапу, что и даст возможность совершить следующий шаг, и следующий, и так до доведения идеи к состоянию общепринятой.
По данной технологии идеи проходят следующие стадии восприятия обществом:
-это немыслимо,
-это радикально,
-это приемлемо,
-это мудро,
-это популярно,
-это официальная политика.
Один из наиболее распространенных способов сдвига общественного мнения к границе отторжения — имитация беспристрастного научного исследования; приведение прецедентов принятия чуждых идей; имитация борьбы радикальных сторонников и противников идей с «умеренными» сторонниками, на чью сторону привлекаются симпатии общества; создание эвфемистических названий неприемлемых идей.

## Массовый посев фейков

Это не что иное, как массовое распространение информации, не соответствующей действительности. Целями такого мероприятия может быть попытка спровоцировать оппонента на определенные действия, или спровоцировать целевую аудиторию (например, на неповиновение властям). Другой целью может быть размытие опасной информации – в случае утечки опасной информации начинается быстрое и массовое распространение сходной по фактуре информации, но отличающейся по смыслу. Например, обвинение оппонента в том, что вы сами сделали. Или кого-то еще… Главное, чтобы такой информации было много и аудитория не смогла бы разобраться, где правда, а где ложь, по крайней мере, – быстро не смогла бы разобраться. Таким же способом можно довести до абсурда невыгодную информацию, просто комментируя ее самыми невозможными способами. Главное, что вариантов интерпретации должно быть очень много (в том числе и абсурдных вариантов). И каждый вариант должен быть продублирован многократно. В результате человек, ищущий такую информацию, столкнется с валом взаимоисключающих суждений, оценок, мнений. Большинство читателей не сможет разобраться и либо окончательно запутается, либо потеряет интерес к теме.



## Зашумление

Это тоже массовый посев, но не обязательно фейков, а, скорее, «параллельной» информации. Например, для того, чтобы «утопить» опасную информацию о защищаемом объекте осуществляется массовый вброс (зашумление) самой разной (реальной) информации по объекту. Главное, чтобы эта информация была НЕ негативная и ее должно быть много. Обычно устанавливается порог не менее пятикратного. Этого оказывается достаточно для того, чтобы негатив не смог оказать значимого влияния на целевую аудиторию.

Одной из разновидностей зашумления является информационная блокада. В данном случае задача всё та же – не дать аудитории ознакомиться с опасной информацией. Здесь порог преобладания (обычно) нужен тот же пяти-шести-кратный, но в моменты появления опасной информации преобладание должно достигать десятикратного.

## Троллинг

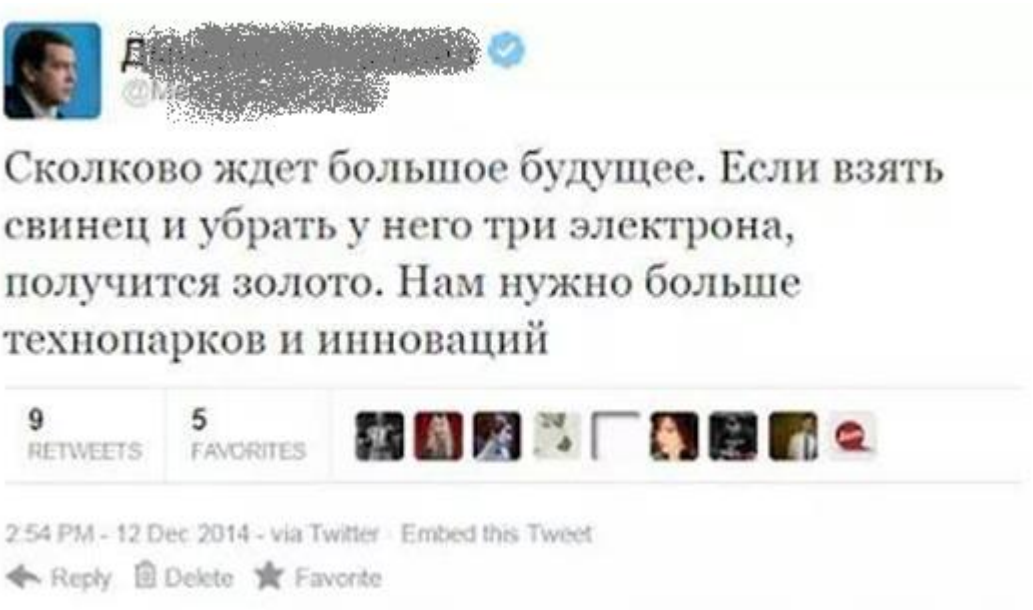
Вариантом зашумления является троллинг. По версии Википедии, троллинг – это нагнетание участником общения («троллем») гнева, конфликта путём скрытого или явного задирания, принижения, оскорбления другого участника или участников, зачастую с нарушением правил сайта и, иногда неосознанно для самого «тролля», этики сетевого взаимодействия. Выражается в форме агрессивного, издевательского и оскорбительного поведения. Используется как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации. Как вариант, это наполнение комментариев всем, чем угодно, но не тематическими сообщениями. Или сообщениями, которые отталкивают нормальных пользователей от чтения. Главное, чтобы эти самые обычные пользователи или не заметили, то, что инициаторы троллинга решили скрыть, или не захотели читать, испытав отвращение к написанному троллями.

Троллинг часто используется в разных форматах и для достижения разных целей. Например, для высмеивания оппонента или для его «эмоциональной дестабилизации», для затягивания оппонента или его ресурсов в бессмысленные препирания.


## Дискредитация

Дискредитация (от фр. Discrediter — подрывать доверие) — умышленные действия, направленные на подрыв авторитета, имиджа и доверия (http://ru.wikipedia.org). В нашем случае подразумевается дискредитация в глазах пользователей некой идеи, объекта, события, автора публикации или самой площадки (сайта), где публикация размещена. Цель – показать негативные стороны, максимально их увеличив. Если нет негативных сторон, то нужно их придумать, создать, спровоцировать… Методичное очернение рано или поздно даст свои плоды. Примерами анонимной дискредитации служат разнообразные черные списки, а открытой дискредитации – прямые обвинения во всех грехах. Для иллюстрации можно послушать выступления представителей внешнеполитических ведомств некоторых стран.

Дискредитации бывают разные. Например, через преувеличение слабостей Объекта. Оппоненты завели аккаунт от имени Объекта или воспользовались программой имитации аккаунта. Взяли за основу снисходительное отношение общества к Объекту и от его имени распространили информацию явно провокационного характера, в данном случае указав на его некомпетентность.

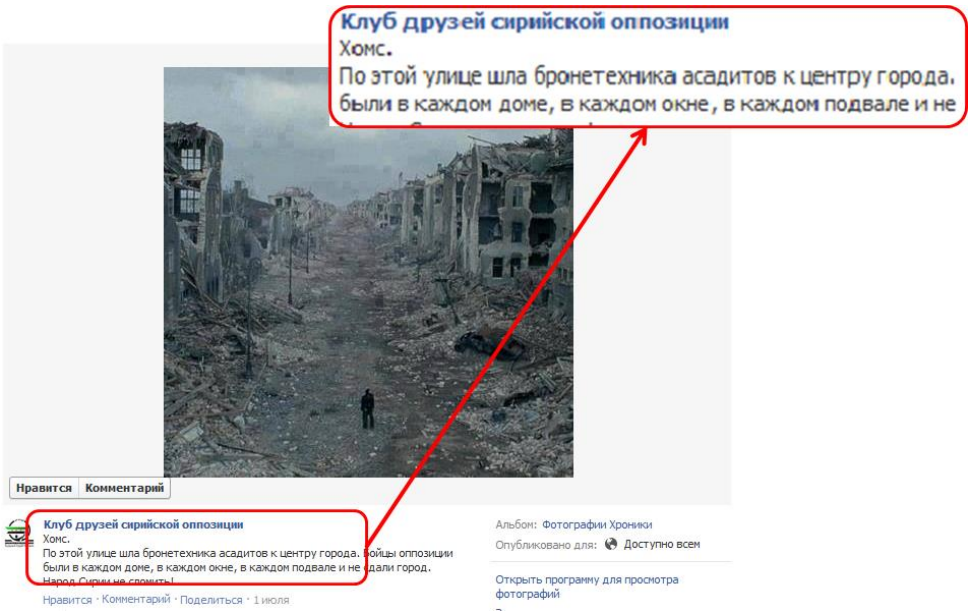



Другой вариант дискредитации – это освещение реальной ошибки Объекта. Помните прокол активистов «с той стороны», когда от имени аккаунта явно с мужским именем был опубликован текст от лица женщины. С одной стороны, этот прокол показал недоработку в системе управления «боевыми» аккаунтами, а с другой стороны, дал прекрасную возможность для дискредитации не только данного посыла, но и всех на него похожих.

А сколько было примеров дискредитации РПЦ, в основном искусственно созданных. Помните этот демотиватор? Недешёвая машина на фоне разрушающейся церкви как бы явно указывает на проворовавшегося священника. Эффект усилен необычным номерным знаком авто.


Правда при небольшом изучении ситуации оказалось, что и машина не его, и номер пририсовали…. Но цель достигнута – демотиватор оказывает нужное воздействие на целевую аудиторию.

Еще один способ дискредитации – это использование свойственного большинству людей сопереживания. В начале гражданской войны в Сирии таких вбросов, дискредитирующих законную власть в стране, было много. Поскольку заказ на них был достаточно большим, то создавались они в основном на старом материале. Как эта публикация фотографии, которая, по замыслу авторов, должна была показать всю бесчеловечность Башара Асада в Хомсе.




Правда, при детальном рассмотрении оказалось, что фото это вовсе не из многострадального Хомса, а является кадром из художественного фильма «Пианист» и изображает Варшавское еврейское гетто во время второй мировой войны.

## Отвлечение

Отвлечение внимания аудитории на негодный объект – так этот прием называется в терминах силовых структур. А его смысл сводится к переключению внимания аудитории с важного для манипулятора события на иное. Такое переключение происходит с использованием разных методик. Наиболее известная – сенсации. Когда нужно что-то скрыть или не дать развиться, то подбирается, искусственно создается или имитируется некое событие, которое привлекает больше внимания людей. И внимание к этому, отвлекающему, событию всячески культивируется обсуждениями, периодическим вбросом новых подробностей, имитацией активных обсуждений… В результате аудитория увлеченно обсуждает подброшенную ей сенсацию и не обращает внимания на защищаемую проблему.

Хорошо в качестве отвлечения внимания работают разнообразные конспирологические теории, которые невозможно проверить. Хороши они еще и тем, что в любой момент их можно «деактивировать», если такое вдруг понадобится.

Часто используется отвлечение внимания на нечто более приятное, например, смешное, вызывающее позитивные эмоции. Помните историю с Вятским квасом на пресс-конференции Путина? Когда журналист в своеобразной манере обрисовал ситуацию и задал вопрос. Все остальные темы, в том числе очень сложные и эмоциональные, как-то отошли на второй план.

Нередко используется и отвлечение внимания на антипод, как в ситуации с попыткой негативного воздействия на репутацию Натальи Поклонской.


Помимо отвлечения внимания аудитории можно отвлечь и самого оппонента, в том числе и его ресурсы. Если создать видимость чего-то, что для него имеет большее значение, чем защищаемый вами Объект. Вспомните, как «вовремя» начались народные волнения вокруг проекта второго трансокеанского канала в Никарагуа. Основной акционер этого мероприятия – Китай, и протестные акции начались сразу после того, как официальный Пекин указал на поддержку России в ситуации на Украине.

Правда, перед этим была еще «революция зонтиков» в Гонконге. Но это скорее тестирование технологий в Китайском обществе.


### *Виртуальные личности (суррогаты)*

Интернет дал возможность пользователю создавать неограниченное число аккаунтов в самых разных сервисах, в том числе и в соцсетях, и на блогохостингах. Ничего аморального в этом нет – забыл я от своего аккаунта пароль – создал новый. Не нравится мне мой сложившийся образ – бросил этот аккаунт, сделал новый, уже более соответствующий моему «я» (как мне кажется). Но, как и всё в нашем мире, такая возможность может использоваться не только во благо, но и во вред. Можно с помощью подложных (фейковых) аккаунтов вводить в заблуждение других пользователей, манипулировать их поведением… Причем интернет дает возможность осуществлять такое манипулирование буквально в промышленных масштабах, что незамедлительно взяли на вооружение государства. Ведь это уже не СМИ (газеты, радио, ТВ) и не культура (театр, кино, литература, изобразительное искусство), это сущность, вмещающая в себя всё это и потому обладающая еще более значительным влиянием на умы людей.

Как только пришло осознание возможностей интернета как средства манипулирования, тут же эту его способность стали использовать на разных уровнях, вплоть до государственного. И те самые аккаунты, которые не являются отражением реальной личности, стали появляться в промышленных масштабах. От их имени распространяется информация нужная заказчику – началось массовое манипулирование реальными пользователями. Собственно, это и есть основное предназначение таких виртуалов – манипулирование общественным мнением в той или иной форме. Цели могут быть самые разнообразные: от корректировки отношения населения к некой проблеме до полномасштабной информационной войны, но инструмент один – манипулирование с помощью искусственных интернет-созданий, выдающих себя за людей.

Существует два понятия, тесно связанных с фейковыми аккаунтами. Это боты и тролли. Причем использование данных обозначений нередко «пересекается». Ботов называют троллями, троллей – ботами. Но в задаче анализа контента в рамках противодействия информационной войне данное разделение не так важно, как понимание того, что некий аккаунт распространяет контент (генерит, репостит, лайкает, комментит) «по велению души» или в качестве работы (за вознаграждение). За деньги ли или за встречную услугу или еще за какое вознаграждение – это не важно. Главное, что данный аккаунт распространяет контент искусственно. Т.е. основным критерием разделения аккаунтов на «человек-не человек» является естественность или искусственность его поведения. И тут уже не имеет значения, что это – бот, тролль или какая еще сущность. Главное, что он совершает некие действия в интернете на возмездной основе.

Для упрощения понимания и относительного единообразия в изложении материала далее предлагаю называть такие аккаунты суррогатами или виртуалами. Причем слово суррогат более точно выражает сущность этих порождений.

## Какие бывают суррогаты

### *Простой суррогат*

**Одиночный**

Самый простой вариант суррогата – это одиночный аккаунт, созданный пользователем для каких-то целей. Например, для получения доступа в группу в социальной сети, куда самого владельца не пустят по каким-то причинам. Вот и создает он своё новое отражение в интернете, подкорректировав его так, чтобы не узнали настоящего владельца и с большей охотой допустили до вожделенного контента в группе.

Таких суррогатов не так много, они обычно контролируются своим владельцем и крайне редко используются для масштабных мероприятий по манипулированию. Тем не менее они используются для распространения если и не противоправного контента, то уж точно не совсем соответствующего морали.

**Группы**

Группы суррогатов до нескольких десятков обычно являются «собственностью» рекламных, PR или СММ-агентств, которые занимаются манипулированием мнения потребителей по заказу коммерческих структур. Чаще всего такие группы распространяют коммерческий контент, но есть достаточно примеров, когда работу их владельцам дает и политический заказчик. Связано это с тем, что эффективность «работы» суррогатов зависит, помимо прочего, и от их «прокаченности». Это собирательный термин, обозначающий и как широко может данный суррогат распространить информацию (сколько людей его читают), и как авторитетен данный суррогат (насколько некритично воспримут его информацию окружающие). А для получения высоких показателей этих характеристик необходимо время и определенные усилия.

**Программное управление группой**

Естественно, что суррогаты тем эффективнее, чем больше похожи на живого человека. А для этого нужно, чтобы они постоянно совершали некие человечные действия (комментили, репостили, лайкали, публиковали). Мало того, эти действия должны быть эмоционально окрашены. Когда в управлении один – два – три суррогата, то действия по поддержанию видимости человечности вполне может осуществлять один оператор. Но когда их несколько десятков или сотен, то это уже становится серьезной проблемой. Да и размещение заказного контента в нескольких сотнях аккаунтов одновременно задача не такая уж и простая. Для ее решения создают программы управления такими аккаунтами.

### *Суррогат на продажу*

Раз есть спрос на фейковые аккаунты, то появилось и предложение этих самых аккаунтов и их услуг. Суррогатов стали создавать для продажи, для сдачи в аренду, для разовых мероприятий, для длительных действий. Появились и посредники между теми, кому нужно купить такие услуги, и теми, кто готов их продать.

**Биржи комментов**

Это площадки, где можно заказать определенные комментарии в определенных сервисах (соцсетях, блогах, форумах). Те, кого на таких биржах называют «рекламодатель», выбирают подходящих под его задачу суррогатов, составляют нужный контент или предлагают владельцу аккаунта его создать (указав параметры вроде темы, тональности и т.п.) и оплатить услугу. Это может быть комментарий, в том числе и к публикации в СМИ, и репост, и лайк, и прямая публикация некоего материала от своего имени. Владельцы подходящих суррогатов осуществляют заказанное действие от имени подконтрольных им аккаунтов. Таким образом, имея некоторые финансовые средства, можно создать иллюзию того, что определенная тема активно обсуждается людьми (репостится, комментируется, лайкается, распространяется). А значит, это очень важно для пользователей, заинтересовало их…

**Биржи аккаунтов**
Кроме бирж комментариев, есть и биржи аккаунтов, где предметом продажи является готовый аккаунт с нужными заказчику параметрами. Исполнители создают суррогата, наполняют его контентом, «прокачивают» его, создавая иллюзию большого числа «друзей», высокой активности, вхожести в нужные группы и т.п. Подгоняют, если нужно, суррогата под требования заказчика (социальные особенности, предпочтения, стиль поведения) и продают заказчику, который уже использует таких суррогатов по своему усмотрению.

**Ворованный аккаунт**
Нередко на биржах комментариев и аккаунтов используются ворованные суррогаты. Т.е. аккаунты реальных людей, но тем или иным образом «угнанные» у них. Ведь для создания аккаунта и его раскрутки нужно время, а потому находятся и те, кто готов преступить не только нормы морали, но и закон.

### *Вирусный суррогат*
Последнее время наблюдается использование иного подхода к распространению ударной информации с помощью суррогатов. В данном случае уже и аккаунт, распространяющий такой контент, не совсем суррогат. В общем-то это нормальный аккаунт нормального человека, который и не планировал посещать соответствующие биржи, и не сдавал в аренду свой аккаунт. Тем не менее ударная информация распространяется от имени его аккаунта.

**Спящий суррогат (троян)**
Многие слышали про бот-сети. Обычно они ассоциируются с всевозможными киберпреступниками, наживающимися на незадачливых пользователях или на реализации ДДоС-атак, приводящих к отказу в работе интернет-сервисов. Но точно так же подобные бот-сети используются и для распространения ударного контента. На компьютер (смартфон, телефон, планшет) жертвы подселяется небольшая программка (бот), которая периодически проверяет, нет ли какой команды из управляющего центра. Когда такая команда обнаруживается, этот бот ее исполняет. Например, осуществляет публикацию того самого «ударного контента» от имени аккаунта пользователя, на устройстве которого «живет». Или при открытии браузера пользователем (на устройстве которого поселился бот) подменяет открываемую им страницу на подобную, но содержащую ударную информацию, что получил из управляющего центра. И пользователь видит уже не реальную картинку, а сформированную искусственно, специально для него. Такую «картинку», которая подталкивает его к нужным манипулятору действиям.

**Суррогатный червь**
Другой разновидностью вредоносного софта для информационных войн является «червь». По аналогии с уже привычными нам деструктивными программами, также именуемыми «червь», червь для информационной войны получает доступ к контактным данным жертвы и сам рассылает себя (в том или ином виде) по этим контактам. Параллельно, попав на новый компьютер, он осуществляет запрограммированное действие. Например, публикует от имени аккаунта жертвы ту самую ударную информацию. Или рассылает от имени жертвы ударную информацию на почту всех, кто есть в адресной книге. Или еще что-то.

## Особенности информационной войны в инете
Все эти особые свойства информации и особенности ее циркулирования в интернете несколько меняют тактику и стратегию ведения информационной войны. И действительно – зачем разбрасывать над территорией противника листовки с аэростата, если для информирования личного состава противника достаточно разослать соответствующее сообщение на их смартфоны и телефоны? Или сделать хитрее – распространить новость нужного содержания посредством новостного агентства, которое этот личный состав читает. Или стать их фрэндами в Фэйсбуке и

запостить соответствующую новость, или, или, или…. Бескрайние просторы для креативного исполнителя.
Интернет стал самым эффективным инструментом ведения информационной войны потому, что это дешево, просто, быстро. Мало того – интернет поменял тактику и стратегию ведения инфовойн. Если в доинтернет-эпоху сам процесс донесения информации до целевой аудитории занимал какое-то вполне осязаемое время, то с появлением интернета это одна секунда – точнее, столько времени, сколько нужно для нажатия на кнопку «ввод». А значит у обороняющего не осталось времени на принятие решений – совсем не осталось – нужно действовать на опережение. Нужно принимать превентивные меры. Нужно находить способ выявлять подготовку к информационной войне. Нужно «прикрывать» свои уязвимости, а еще раньше самому выявлять их.
Но есть несколько технологических моментов, которые необходимо разобрать подробнее, чтобы впоследствии на их основе можно было строить свои приемы ведения информационной войны.

### *Анонимность*

Анонимность пользователю интернета нужна для того, чтобы ваш собеседник воспринимал информацию от вас, как информацию от своего друга, или союзника, или коллеги, или…. Иными словами, анонимность – это основа для легендирования, фундамент для создания виртуальных личностей, от имени которых вы будете выступать.
С другой стороны, анонимность также нужна, чтобы «войти в доверие» к злоумышленнику. То ли под видом потенциальной жертвы, то ли под видом более опытного товарища, то ли… Главное – с целью получить дискредитирующую его информацию, выявить слабые места, отвлечь, направить по ложному следу, заманить в ловушку…
Поэтому вопросам анонимности нужно уделить достаточно времени. Дабы понимать, как может действовать противник и как нужно действовать нам.
«Оставить следы» в интернете, чтобы позже вас могли идентифицировать, можно по-разному. В основном это связано с особенностями работы самого интернета (IP, MAC-адреса, cookie сайтов, другие программные идентификаторы), с личными пристрастиями (общий e-mail или особенность написания аккаунта, одна фотография или подпись), с вредоносным софтом.

#### IP

IP-адрес это адрес, по которому можно идентифицировать устройство в интернете. Этот адрес имеет любое устройство сети, в противном случае оно (устройство) не сможет принять информацию. И по этому самому IP проще всего идентифицировать устройство и его владельца. Так вот, посещая сайты, отправляя письма, регистрируя аккаунты, вы оставляете свой IP. И по нему можно установить, с какого устройства осуществлялось каждое конкретное действие. А у вашего провайдера есть адрес установки устройства с этим самым IP. И есть данные, куда, когда ходили с этого IP, что делали. Кроме того, на сайтах, куда вы ходите, также есть свои логи с данными, с какого IP приходили, когда и что делали. Такие же логи ведутся на промежуточных серверах, через которые проходят ваши пакеты (запросы и ответы на них). Везде из перечисленных мест можно узнать, кто, откуда, когда и что делал.
По этой причине, если вы хотите остаться неузнанным, необходимо этот IP скрыть или подменить. Для этих целей служат разнообразные анонимайзеры от простых плагинов к браузерам до специализированных программ вроде Tor (сокр. от англ. The Onion Router).

#### Браузер и «куки»

Еще один способ идентифицировать пользователя – это оставить специализированный идентификатор в браузере – cookie. Изначально это решение предназначено для того, чтобы целевой сайт «узнавал» пользователя и применял его индивидуальные настройки. Но именно «узнавание» пользователя и стало причиной опасности для анонимности этих самых cookie. Соответственно, cookie нужно удалять. Браузер можно настроить очищать всю историю вместе с куками при закрытии. Так вы еще и дополнительно обезопасите себя.

### Данные в профиле

Имеются ввиду те данные, которые вы оставляете при заполнении анкетных данных во время регистрации аккаунта. Можно, конечно, заполнять по минимуму, но тогда ваш аккаунт будет очень напоминать «схемотехнический», а им доверяют хуже. Поэтому заполнять нужно, но так, чтобы аккаунты разных виртуальных личностей отличались друг от друга. Это касается и аватара, и контактных данных. Будет странно выглядеть, если разные виртуальные личности, спорящие друг с другом, будут иметь один и тот же e-mail.

### Геолокация

В последнее время все чаще применяется геолокация. И на ряде сервисов (в социальных сетях, например) есть возможность собирать данные о геолокации пользователей. Причем ряд мобильных приложений автоматически скрытым образом собирает данные о геолокации и передает «материнскому» сайту. Поэтому если человек пишет, что он из Питера, а API для получения информации о постах/твитах/комментах показывает, что он в Москве, – это тоже провал.

### Метаданные

Все файлы имеют свои метаданные, которые присваиваются программно в момент создания файла и его изменения. К метаданным относится дата и время создания файла, имя компьютера, на котором создан файл, дата и время изменения файла, геоданные (координаты места нахождения устройства в момент создания файла), в какой программе создан файл…. И еще много чего. Эти метаданные могут легко дезавуировать обман, который пытаются использовать в качестве основы манипулятивного воздействия. Например, пользователь утверждает, что сделал фото в определенное время и в определенном месте, а по метаданным видно, что совсем в другое время и совсем в другом месте….

### Поведенческие признаки

Это значительно более сложная область, но тем не менее уже опробованы алгоритмы, позволяющие идентифицировать пользователя по особенностям его действий. Для этого используются индивидуальные привычки набора текста (особенно устойчивых выражений), особенности поведения на определенных сайтах и т.п.

## *ТОП списки*

ТОП списки – это мнение какой-то системы рейтингования о популярности ресурса (страницы, новости) и/или о его ценности для пользователей. Такое мнение формируется по разным правилам, нередко с политическим оттенком и с учетом пристрастий владельца рейтинга. Но так или иначе эти ТОП списки прямо влияют на пользователей. Например, эксплуатируя эффект стадности – «если все считают так, то я тоже так считаю», или «подсовывая» пользователю первой нужную информацию. Здесь уже срабатывает эффект «первой любви».

### ТОП выдачи поисковиков

Это не что иное, как мнение поисковых систем, какая информация более всего подходит под ваш запрос в поисковой строке Яндекса, Google, Рамблер, Yahoo и им подобных. И отсортирована эта информация именно по релевантности (соответствию) этой самой информации вашему запросу. Т.е. вверху (на первой позиции) будет стоять наиболее соответствующее, на второй – чуть менее соответствующее и так далее. И естественно, что первым вы читаете именно первые в списке.

### ТОП обсуждений

Это рейтинги блогохостингов и разнообразных систем анализа блогов. В них структурирование происходит по количеству комментариев (т.е якобы по активности обсуждения). У какой публикации больше комментариев, та и вверху списка. Цель – определить наиболее обсуждаемые, а значит, наиболее популярные записи. Их и преподносят пользователю как наиболее популярные, несмотря на то, что «популярность» (число комментов) создана ботами.

Еще один вариант, это когда структурирование происходит по количеству подписчиков блога. У какого блога больше подписчиков, тот и авторитетнее ☺

### ТОП новостей

Это мнение новостного агентства по поводу значимости новости. Решение в данном случае принимается, как и в блогосфере, по числу комментов к новости, лайков, перепостов. У разных систем разный алгоритм подсчета, но смысл один – определить по этим признакам, какая новость наиболее значима.

## *Мониторинг инфополя*

Для того, чтобы вовремя увидеть начало атаки, а еще лучше подготовку к ней, необходимо отслеживать действия противника. Да и сам процесс противодействия необходимо постоянно отслеживать для выявления попыток оппонента взять реванш. Необходимо внимательно следить за оппонентом, за его действиями, за его репутацией, за окружающим его инфополем. А также и за своей репутацией, своим инфополем… Так что вопрос регулярного мониторинга является весьма актуальным.

Такое наблюдение поможет понять, как действует оппонент (его методы, приемы), где у него «болевые точки» (в нашем случае болевые темы), понять его инфраструктуру – его площадки, кто его друзья, а самое главное – кто его враги (враг моего врага – мой друг). По отношению к себе наблюдение позволит выявить изменение инфополя (увеличение или уменьшение упоминаемости), тренд этого изменения (позитив – негатив), в какой-то мере причину изменения. Понятно, что такое наблюдение вручную проводить весьма утомительно. Поэтому нужно максимально автоматизировать процесс. Для этого есть ряд решений от простых до довольно сложных.

### Закладки в браузере

Это самый простой способ. И подходит он для простых случаев. Исключительно потому, что автоматизация здесь минимальная. Суть метода в том, что нужно собрать в одно место все закладки на значимые в информационном плане ресурсы. Это могут быть новостные страницы ключевых порталов и страницы результатов запросов к новостным поисковым системам по вашей тематике. Такое простое объединение позволяет одним кликом сразу открыть все необходимые страницы и углубиться в изучение. Но если число новых материалов каждый день измеряется сотнями, то закладки мало помогут.

### Плагины для браузера

Примером таких плагинов могут служить Update Scanner для Firefox или Page Monitor для Chrom. Они позволяют отслеживать изменения на наблюдаемых страницах. Эти изменения «подсвечиваются», и можно быстро выявить, что изменилось на странице, а не вспоминать, как она выглядела прошлый раз. Страницей может быть страница новостей или страница результатов запроса к поисковой системе. В этом случае выявить новое еще проще, а потому и затрат времени меньше.

### RSS-агрегаторы

RSS – это формат распространения новостей в интернете. Он очень прост, распространен и удобен. Под него создано огромное число «читалок», которые собирают RSS-потоки новостей с указанных ресурсов и представляют вам в удобном виде. Есть онлайн RSS-агрегаторы. Такое решение удобно тем, что процесс сбора идет непрерывно и независимо от того, включили вы компьютер или нет. Из бесплатных – Яндекс Лента. Google Rider, к сожалению, был закрыт якобы из-за непопулярности. Еще примеры таких агрегаторов:

Bloglines – один из самых популярных онлайновых агрегаторов. Он прост в работе, очень быстр даже на диалап-соединении.

NewsGator – онлайн сервис, RSS-источники в котором представлены в виде древовидного меню, как в большинстве программ для работы с почтовой корреспонденцией.
NewsAlloy – по напичканности функционалом он может дать фору RSS-ридеру компании Google.
Оффлайн агрегаторы «селятся» у вас на компьютере, а потому обладают своими преимуществами. Примеры таких решений:
SeaMonkey — веб-браузер, HTML-редактор, агрегатор RSS, почтовая программа и IRC-клиент в одном пакете.
Omea Reader — бесплатный агрегатор RSS, электронной почты, сообщений интернет-пейджеров и NNTP.
FeedReader — мощная дружественная программа для получения, чтения и управления блоками новостей.
FeedDemon — популярная программа для получения и обработки новостей с сайтов в форматах RSS и XML.
BlogBridge — агрегатор лент RSS, предлагающий удобные функции чтения новостей сайтов и блогов.

### WebSiteWatcher

Программа предназначена, как и Update Scanner и Page Monitor, для выявления изменений на контролируемых страницах. Но в силу своей специализации эта программа способна контролировать огромное количество страниц и представлять информацию в более удобном виде. К тому же есть масса полезных настроек и «приспособлений» под разные типы сайтов. Сайт программы http://www.aignes.com/

### RSSHandler

Большинство RSS-агрегаторов имеет один общий недостаток – они ограничиваются скачиванием материала и организуют его в соответствии исключительно «по источникам». А этого недостаточно. Особенно когда RSS-лент несколько сотен, а новостей в них каждый день несколько тысяч. При таких объемах становится понятно преимущество программы RSSHandler. RSSHandler, помимо сбора новостей, еще и раскладывает их по созданным пользователям папкам в соответствии созданными пользователем же правилами. Например, в одной папке можно собрать все новости об одном человеке, а в другой папке – о другом человеке. Даже если эти новости изначально были в одной RSS-ленте. Сайт программы http://www.ryalsoft.ru/

### Авланч

Дальнейшее развитие и совершенствование идеи удобного представления большого объема новостей (и не только). Это не только их группировка в зависимости от объекта, но и создание Досье. Кроме этого в качестве источников информации в программе используются, помимо RSS-потоков, и страницы, не имеющие RSS, но содержащие новости. Сайт программы http://www.tora-centre.ru/avl1.htm

### СайтСпутник

Пожалуй, наибольшее число инструментов для сбора информации с сайтов и ее представления дает программа СайтСпутник. Информация может быть собрана и из новостных страниц, и из RSS-потоков, и из результатов поиска поисковиков (Яндекс, Google и т.п.), и из результатов поиска локальных поисковиков на сайтах, а также информация об изменении контролируемой страницы. Инструментарий для обработки собранных данных тоже значителен. Это и группировка по сложным правилам, создаваемым пользователем, и удаление дублируемой информации, и обмен данными между разными СайтСпутниками, и автоматизированное формирование и предоставление отчетов заказчикам разной информации. На мой взгляд, лучшее решение для мониторинга.
Сайт программы http://www.sitesputnik.ru/

#### *Готовность к ответным шагам*

Ваша активность в противостоянии агрессору точно будет замечена этим самым агрессором. Поскольку это нарушит его планы, то как минимум испортит ему настроение. А то и подпортит его репутацию. В такой ситуации разные люди ведут себя по-разному – реакция может быть не предсказуемой. В лучшем случае ваш оппонент усилит своё воздействие на инфополе – активизирует имеющиеся ресурсы. К этому нужно быть готовым, т.е. заготовить свои дополнительные ресурсы и использовать их в момент повышения активности оппонента.
Но, скорее всего, оппонент попробует взять реванш другим способом. Так сказать, осуществить асимметричные действия – действия, выходящие за рамки манипулирования информацией. Например, могут попробовать взломать ваш основной сайт. Тот самый, на котором аккумулируется вся информация и который продвигается в поисковиках. Перехватить управление, удалить содержимое, подменить содержимое… Чтобы такие действия были не фатальными для вас – делайте копии материала и/или копии сайта. А лучше создайте несколько «зеркал» и архивную копию у себя на сервере (компьютере).
Могут заказать ДДОС, и какое-то время ваш сайт будет недоступен пользователям. Для преодоления такого рода проблем используйте дубликаты на разных хостингах – крупных хостингах (отказо- и обузо-устойчивых хостингах). И те же «зеркала» сайта тоже помогут.
Могут попробовать найти, кто именно осуществляет противодействие, – найти вас. И оказать давление в той или иной форме. Именно поэтому вопрос анонимности всегда важен в информационных войнах.

## Стратегия противодействия

### Последовательность действий

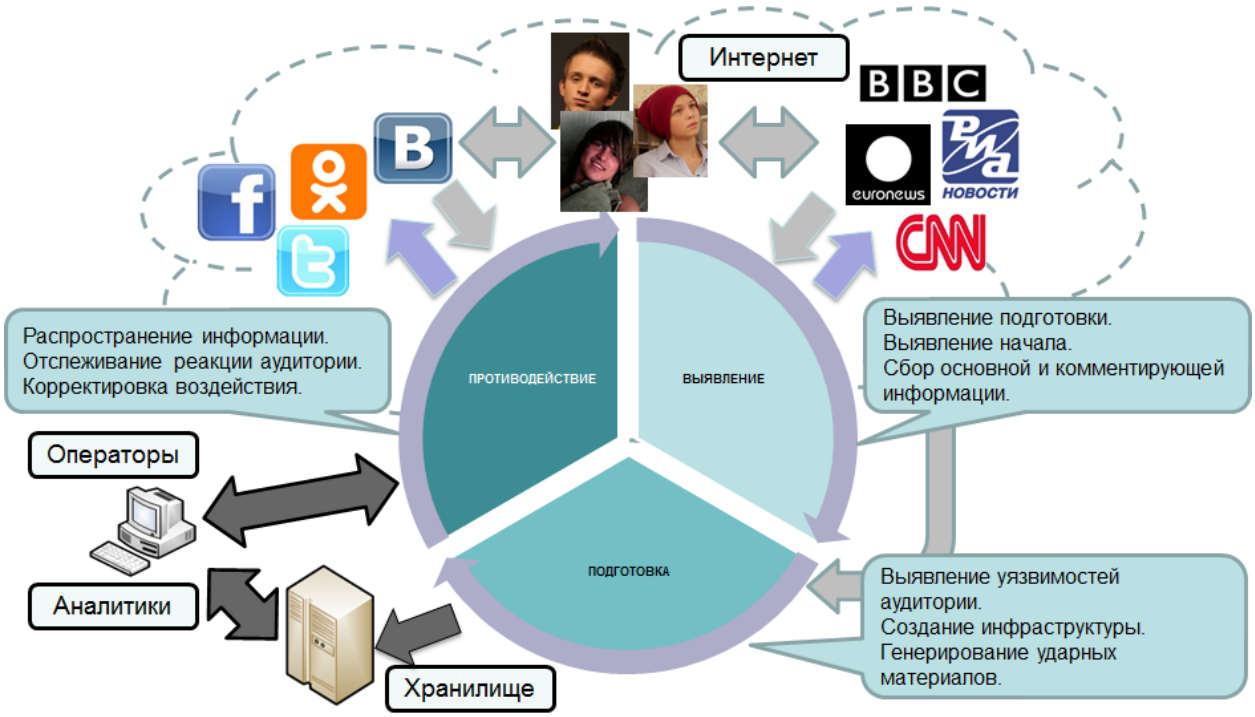
#### *Что и почему делать*

Помимо очевидного риска «попасть под ответный удар» в физическом смысле, осуществляя открытое противодействие агрессору, вы, действуя открыто, еще и осложняете сами себе работу. Ваш противник знает о ваших усилиях и конечно же принимает меры. Меры могут быть разные, но они точно не в помощь вам. Открытыми действиями вы сами провоцируете оппонента к приложению больших усилий, а значит и вам придется прилагать больше усилий со своей стороны. А это уже не борьба интеллекта, а борьба ресурсов, коих у вашего оппонента может оказаться значительно больше. Мало того, отвечая от своего имени, вы сами добавляете негатива о себе. Ведь ваше имя будет четко ассоциироваться с той информацией, которую вы распространяете. А коль скоро вы отвечаете на агрессию, то и распространяемая вами информация вряд ли будет носить мирно-позитивный характер.

Поэтому единственный разумный вариант – «партизанские» действия. Анонимно, скрытно и непредсказуемо – так должен осуществляться ответ на информационную агрессию. Посмотрите, как это происходит в интернете. «Вдруг», «ниоткуда», «на ровном месте» начинает массово появляться негатив. Невозможно понять, где источник, потому что источников очень много, непонятно, на кого «давить», с кем «договариваться», что делать, куда бежать – сущий хаос для мишени. Дезориентация, стресс, цейтнот, неуверенность... А если источник негатива известен, то и понятно, что и как делать – никакой суеты, а планомерные ответные шаги. А нам не нужно, чтобы оппонент чувствовал себя уверенно, нам нужно обратное. Поэтому не стоит давать оппоненту лишнюю информацию, в том числе и об источнике его неприятностей.

Соответственно, обнаружив несправедливость по отношению к вам, нужно остановить первый позыв срочно что-то ответить, нужно запастись терпением. Для начала – определите – это действительно продуманная и спланированная атака, или чьи-то то спонтанные действия. Не спешите с ответом. Ведь от него зависит многое. Если вы склонны думать, что это организованное воздействие, то необходимо предпринять несколько обязательных действий. Не факт, что эти действия дадут стопроцентный результат, но как минимум помогут вам оценить ситуацию (масштабы бедствия).

Помните цикл информационной войны? Так вот цикл противодействия информационной войне в общем и целом тот же. И связано это с тем, что против агрессора используется то же самое оружие – информационное.




Всё начинается с выявления, но выявление нападения это уже опоздание. Гораздо важнее выявить подготовку к нападению. И тут главное понять, по каким признакам можно определить, что идет подготовка к агрессии. Выявить этап «Планирования» можно только агентурными методами. А потому не будем на нем останавливаться. Хотя наблюдение (в интернете) за действиями ключевых фигур вероятного противника, так или иначе могущих быть причастными к подготовке информационной войны, и может дать возможность обнаружить изменения, свойственные принятию или обсуждению решений об информ-агрессии.

### *Начать мониторинг*

Итак – нужно срочно, если вы это не делаете, начать регулярный мониторинг интернета на предмет высказываний в ваш адрес. Это позволит увидеть «картину» целиком, а не фрагментарно и даст возможность вовремя «отлавливать» опасные тенденции. А при качественном подходе – прогнозировать развитие ситуации.

Организовать такой мониторинг можно вручную, если вы (или защищаемый объект) не слишком медийный, т.е. число новых его упоминаний в сутки не превышает сотни. Но уже в этом случае нужно будет тратить некоторое время на сбор и прочтение материалов. Сам же сбор можно организовать с помощью поисковых систем (Яндекс, Google). Один раз сформировав качественный запрос, чтобы свести информационный мусор в выдаче к минимуму, этот запрос сохраняете в виде закладки и при необходимости активируете.

Можно задействовать для мониторинга онлайн сервисы, которых много. У такого способа есть свои преимущества. Первое – вам не нужно тратить время на сам процесс сбора – это всё сделают за вас. Второе – весь объем собранного всегда доступен вам из любого места, лишь бы был интернет. Вот наиболее известные мониторинговые системы:

argylesocial.com
alterian.com/socialmedia
attensity.com/home
attentio.com
babkee.ru

beevolve.com
bottlenose.com/product
br-analytics.ru
brandoscope.ru
brandspotter.ru
brandwatch.com
buzzcapture.com
buzzlook.ru
buzzient.com
buzztalkmonitor.com
buzzware.ru
collectiveintellect.com
converseon.com
crimsonhexagon.com
cymfony.com
digimind.com
elect.mlg.ru
en.mention.com
gainsight.com
generalsentiment.com
hodyat-sluhi.ru
hootsuite.com
integrasco.com
jagajam.com/ru
iqbuzz.ru
kissmetrics.com
kribrum.ru
lithium.com
loudpixel.com
maritzresearch.com/solutions/social-intelligence.aspx
mediavantage.com
meltwater.com
nmincite.com
monitor.wildfireapp.com
moz.com
netvibes.com/ru
newssentiment.eu/main/index.jsp
oracle.com/us/solutions/social/overview/index.html
peerindex.com
poppler.ru
radian6.com
rowfeeder.com
samepoint.com
sdl.com/products/social-intelligence
semanticforce.net
silentale.com
silverbakk.com
simplymeasured.com
socialbaker.com
sociable360.com
socializer.ru
socialmention.com
socialreport.com

social-searcher.com
socialwatchdog.ru
spiral16.com
sysomos.com/products/overview/heartbeat
tagboard.com
topsy.com
trackur.com
twelvefold.com/splash/
veooz.com
visibletechnologies.com
webtrends.com/solutions/social
wigisocial.com
wobot.ru
youscan.ru

### *Установить агрессора*

Второе – нужно попробовать установить агрессора. Кто это. Действовать придется сразу по нескольким направлениям. Попробуйте установить авторов негативной публикации, пройдя по цепочке репостов и комментариев. Если атака массированная, то эта процедура довольно трудоёмкая, но проделать ее нужно. Вначале определите первоисточник – откуда началось распространение. И анализируйте именно первоисточник, а не дубли, репосты и перепечатки. Задайте себе классический вопрос «а кому это выгодно?». Кто получит прямые или косвенные преференции в случае вашего устранения как игрока? С кем были явные или скрытые конфликты? Ответы на эти вопросы могут сузить круг вероятных оппонентов. А это уже рабочие гипотезы для дальнейшей проработки.

### *Понять силы противника*

Третье – нужно определить «силы» противника и его возможности. Для этого надо выявить все ники, что участвуют в «разгоне» негативной информации. То ли репостом, то ли комментарием… Это даст дополнительную информацию для выявления автора, позволит организовать наблюдение непосредственно за исполнителями, а не за всем интернетом и поможет оценить, какие силы и средства нужны для противодействия. Ведь примерная стоимость бота известна – так что можно примерно оценить уровень затрат вашего противника. А по этому уровню – понять уровень финансирования и серьезность намерений. Да и с общей стратегией противника позволит разобраться.

### *Выработать план действий*

Четвертое – определить (на начальном этапе хотя бы в общем виде), что и как нужно делать. Что «выдавливать» из выдачи, что «продвигать», какую информацию разгонять сейчас, а какую оставить на попозже, где сделать отвлекающий удар по возможному оппоненту, а где отвлечь аудиторию на другую тему…. Но так или иначе вы подойдете к вопросам продвижения выгодных вам материалов. А потому нужно понимать, как это делается технически.

### *Официальные обращения*

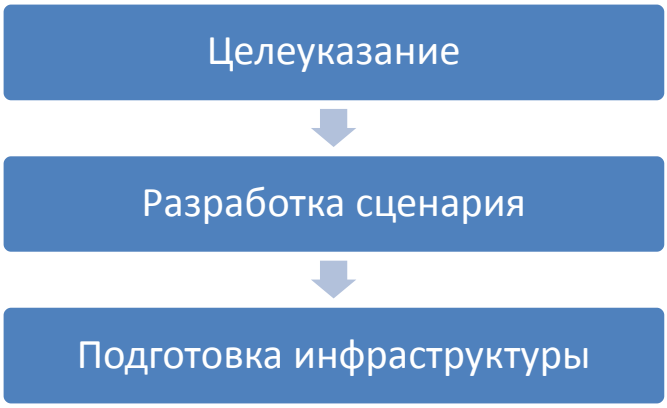
Предположим, вы увидели, что в выдаче поисковых машин по запросу вашего ФИО (или по названию вашей компании) выдается негативная информация. Что делать, как поступить? Посмотрите – негатив единичный или это уже приобрело массовый характер. Для этого достаточно сначала посмотреть на первую страницу результатов выдачи поисковика. Один там такой материал или много. А затем этот же результат отсортируйте по дате. И тогда вы увидите последние материалы, содержащие ваше ФИО. Опять же – много таких или только один? Поняв это, поймете, сколько оппонент потратил сил и сколько вам нужно потратить усилий на противодействие.

Если негатив этот единичный, то можно попробовать «поработать» с администрацией ресурса, на котором размещен негатив. Если этот материал хоть как-то нарушает Закон (клевета, разглашение персональных данных, угрозы, национализм и т.п.) – смело пишите обоснованное уведомление администрации ресурса. Но именно обоснованное – со скриншотами, с точным указанием фраз и статей этим нарушенных. Опять же «если» ресурс не специализируется на компромате, то его

владельцам будет не все равно, обратитесь вы в правоохранительные органы или нет. Но, увы, этот способ действует не всегда. Так что будьте готовы, что ваше обращение проигнорируют.
И вновь «если» вы готовы на траты времени, то обращайтесь в правоохранительные органы. В настоящее время наметилась хорошая тенденция – применение к интернету тех же законов, что и в реальной жизни. Поэтому, надеюсь, со временем соблюдение закона и в интернете станет нормой. Выявление и задержание торговцев наркотиками, порнографией, оружием…

### Как понять, война или нет

Главная проблема при принятии решений в информационных войнах заключается в понимании того, чем является рост негативных упоминаний – естественным явлением или искусственно созданной иллюзией. От этого зависит то, какая стратегия противодействия будет использована. Если такой всплеск является естественным явлением (общение реальных людей), то для противодействия будут использоваться одни инструменты. Если же всплеск негативных упоминаний создан искусственно, то и инструментарий будет другой.
Но это в случае, если воздействие уже началось. А раз оно началось, то вы уже опоздали – нужно принимать срочные меры, чаще всего неся потери. Но такой ситуации можно избежать, если заранее продумать возможные сценарии противодействия и выстроить несложную систему наблюдения.
Для начала вспомним о цикле информационной войны – начинается воздействие не вдруг. Ему предшествуют некоторые этапы. Помните? – воздействию предшествуют ЦЕЛЕУКАЗАНИЕ, РАЗРАБОТКА СЦЕНАРИЯ и ПОДГОТОВКА ИНФРАСТРУКТУРЫ.




Как уже было сказано чуть раньше, на этапе ЦЕЛЕУКАЗАНИЯ понять о готовящемся воздействии можно только с помощью агентурной работы. Или предполагать о такой возможности, исходя из своих знаний о реальных и потенциальных противниках, их интересах и ресурсах. А вот следующие этапы требуют некоторых действий от оппонента. И эти действия оставляют следы, а значит, эти следы можно обнаружить. Соответственно – вполне реально выявить подготовку к агрессии за некоторое время до ее начала.
Что происходит на этапе РАЗРАБОТКИ СЦЕНАРИЯ? Прежде чем начать реализацию, агрессору необходимо понять, как и на кого нужно воздействовать, чтобы достичь желаемого результата. Для понимания этого ему придется выявить, по какой целевой аудитории нужно «работать» – на кого нужно воздействовать. Или иначе – какую группу людей необходимо подтолкнуть к нужным агрессору действиям. То ли это пенсионеры (применительно к российской действительности), то ли фанаты спортклубов, то ли креаклы). Иными словами, нужно понять, чьими руками можно эффективнее достичь поставленной цели. Для этого проводится исследование, которое может в себя включать не только пассивное наблюдение и сбор информации, но и социологические опросы, работа с фокус-группами и тому подобные вполне осязаемые действия. Именно на выявление таких действий и должна быть нацелена система раннего предупреждения в области информационных войн.
После определения целевой аудитории осуществляется выявление ее уязвимостей – тем, которые вызывают наибольшие эмоции (коррупция, социальное неравенство, национализм). Из этих тем

отбираются наиболее удобные для эксплуатации. Кроме того, на данном этапе осуществляется тестирование этих тем в малых масштабах. Ведь нужно убедиться, что уязвимость работает так, как нужно агрессору. Это проявляется по-разному. Например, в виде провоцирования обсуждения темы на форумах, в блогах, в соцсетях. Пока локально – без искусственного разгона. И это тоже можно выявить.

Далее начинается ПОДГОТОВКА ИНФРАСТРУКТУРЫ. На этом этапе, помимо прочего, создаются аккаунты для будущего распространения информации. Поскольку аккаунты предназначены для «разгона» определенной темы, то их, скорее всего, оптимизируют именно под эту тему. Такая оптимизация нужна для выжимания из них максимального эффекта и выражается в том, что в профиле будут использоваться ключевые слова, присущие планируемой к эксплуатации темы. В описании увлечений, в тегах, а то и в нике аккаунта. Кроме того, такие аккаунты внедряют в соответствующие группы, нагружают релевантным контентом и т.д. Именно массовое появление аккаунтов со специфическими характеристиками и является одним из признаков подготовки к агрессии.

### *Признаки подготовки к войне*

В процессе мониторинга, в рамках противодействия информационным войнам, необходимо постоянно отвечать на один и тот же вопрос – не началась ли информационная атака? Если говорить точнее, то нужно на основе данных мониторинга в любой момент времени понимать, а что собственно происходит. Нужно это для своевременного принятия решения о начале действий по отражению атаки, по подготовке к отражению или по корректировке уже начатых действий. Ответить на эти вопросы можно, зная признаки тех или иных состояний – те самые «слабые сигналы», выявляя которые, мы понимаем происходящие в инфополе. Вот об этих сигналах или признаках мы сейчас и поговорим.

#### Опросы по болезненным темам

Появление разных социологических служб, которые исследуют общество (целевую аудиторию) либо с точки зрения его консолидированности-разобщенности, либо через анкетные вопросы, явно нацеленные на выявление тем социальной напряженности (вызывающих наиболее сильные эмоции, особенно негативные). Такие опросы могут быть как явными, так и неявными, когда анкетирование маскируется под собеседование, интервью и т.п.

Такие исследования стараются скрывать по понятным причинам. И проводить их неявно, например, проверяя «лайковость» того или иного демотиватора в ФБ, во ВКонтакте или в другой социальной сети. А структуры, стремящиеся к мировому господству, ставят такие исследования на поток. Например, с 2010 года DARPA развивает программу Anomaly Detection at Multiple Scales, которая, помимо прочего, предназначена для выявления аномальных процессов, происходящих в обществе. С начала 2011 года Пентагон развивает систему SMISC (Social Media in Strategic Communication – в переводе «социальные медиа в стратегической коммуникации»), которая отслеживает все политические дискуссии и устанавливает, является ли это случайным продуктом коллективного разума или пропагандистской операцией со стороны враждебной нации или группы. Конечная цель проекта – создание системы, способной самостоятельно выявлять попытки вражеского манипулирования и противодействие ему. А в рамках этого проекта создана технология выявления уязвимостей интересующего общества (целевой аудитории), которые впоследствии можно использовать для воздействия.


### Тестирование болезненных тем

После выявления уязвимостей социума необходима калибровка – проверка того, действительно ли эти темы так значимы. Получить ответ на этот вопрос можно, только проверив свои домыслы в реальной обстановке. Например, подняв такую тему на форуме и отследив реакцию пользователей. Именно появление таких тем «вдруг», «ниоткуда» и является еще одним признаком того, что идет подготовка. Такие темы могут создаваться впервые, или, что чаще бывает, поднимаются старые темы с подходящим содержанием.

### Массовое появление аккаунтов со специфическими характеристиками

После кабинетных и полевых исследований злоумышленнику необходимо создать инфраструктуру для будущей атаки (если только она у него уже не создана). Но и те, кто постоянно занимается информационными войнами в интернете, вынуждены непрерывно пополнять свой парк ботов. Такая подготовка инфраструктуры подразумевает создание аккаунтов в разных социальных сетях (в широком смысле этого слова), связывание их между собой по схеме «управляющий – управляемые», настройку кросспостинга и т.п. Сами аккаунты желательно создавать не «от фонаря», а закладывая в профайл те ключевые слова, по которым впоследствии будет идти инфовоздействие. Это облегчит поисковую оптимизацию и повысит результативность при «посеве». Именно одномоментное (или в короткий срок) появление большого числа аккаунтов с тематическими ключевыми словами в настройках и есть признак подготовки к информационной войне. Тематические ключевые слова помещаются в описание увлечений, хобби, пристрастий, в теги будущих публикаций, а то и в ник аккаунта.

## *Признаки начала войны*

### Всплески

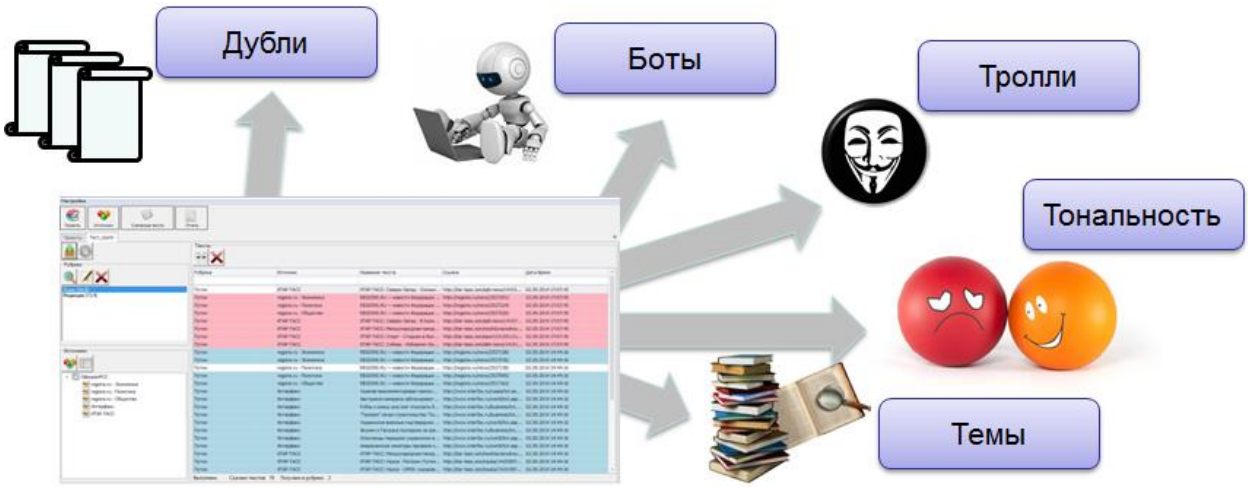
А выявление начала атаки осуществляется по вполне понятным признакам: рост негативной активности в болезненных (а для противника в ударных) темах, рост числа суррогатов в негативных высказываниях и т.п.


Резкий рост упоминаний Объекта указывает на появление интереса к нему (естественного или искусственного). Такой всплеск является указанием, что что-то не так, что-то изменилось, причем вдруг, очень быстро. Конечно же это может быть и не информатака. Но лучше посчитать пару таких всплесков атакой и «отработать» их, чем пропустить тот, который действительно является угрозой.

Куда показательнее резкий рост негативных высказываний об Объекте. Такой рост уже сам по себе сигнал тревоги, а при выявлении искусственности его природы – однозначное указание на то, что против Объекта началась информационная атака.

### Искусственность волны

Вопрос в том, как определить, что всплеск негатива является искусственно созданным? Сам ответ несложен – наличие в числе распространителей информации аккаунтов, которые являются ботами или троллями, и есть указание на то, что всплеск негатива является чьим-то искусственным порождением. И дело тут в том, что боты сами по себе или их аренда стоят денег, как и публикации троллей, которые потратили ресурсы на выход в тысячники. И просто так они информацию не распространяют.




Не менее важно понимать, какое число ботов и троллей нужно считать достаточным для утверждения, что началась атака? Ответ не так прост. Дело в том, что для малозаметных в медийном смысле объектов появление одного бота в распространении негативной информации

уже показатель искусственности волны. А для объекта, который каждые сутки упоминается несколько сотен раз, появление нескольких ботов в числе распространителей негатива еще не повод паниковать. Просто потому, что ботам нужно постоянно придавать видимость человечности. А для этого, помимо прочих приемов, используется и репостинг популярных новостей. И ваш объект мог попасть случайно. Поэтому для медийных объектов нужно вводить порог в 2-3 % от общего числа негативных сообщений (очень условно).

Следующая проблема заключается в том, как определить, что негативное сообщение опубликовано ботом.

### *Признаки ботов*

В определении ботов есть одна особенность – отсутствие однозначного ответа на вопрос, бот или не бот? Связано такое положение дел с тем, что точный ответ можно дать, только контролируя сам аккаунт, а такой возможностью обладает лишь его владелец. Поэтому оперируем понятиями нечеткой логики. А сама система оценки близка по своей сути к скоринговой системе, когда принятие решения осуществляется по совокупности признаков, а не по одному показателю. И реализовывать ее нужно именно так – определив перечень показателей и оценив их вес в итоговой оценке.

**Статичные признаки**

К статичным признакам относятся особенности оформления аккаунта – то, как полно занесены данные, какие данные использованы для оформления и т.п. Рассмотрим некоторые примеры таких признаков.

Корректное написание имени – использование в имени аккаунта не имен. Это признак, который сам по себе настораживает и используется для определения только в комплексе с другими признаками как дополнительный фактор. Однако, если у вас уже есть выявленные боты, а имя исследуемого аккаунта отличается от них на +1, то это скорее всего бот.

Наличие публикаций аккаунта – если сам ничего не пишет, а только комментирует чужие записи, то это еще один признак ботности. Нередко для имитации жизни такие публикации делаются, но они являются дубликатом уже имеющихся и/или «не в тему». Чаще используется такой показатель, как соотношение входящих сообщений к исходящим или комментариев к публикациям.

Наличие и содержание фотографии также является дополнительным признаком «ботности» аккаунта. Содержание фотографии также имеет значение, но формализовать процедуру такой оценки достаточно сложно.

Соответствие друг другу разных данных профайла. Особенно интересно соотносить друг с другом даты. Например, дата рождения и дата начала и окончания обучения в школе, в вузе. В спешке оформления (а аккаунты-боты создаются чаще в спешке) нередко ошибаются, и тогда оказывается, что в школу пошел в четырехлетнем возрасте или в 11 лет… Конечно же это не однозначный показатель, а лишь еще один пункт в скоринговую систему оценки ботности.

Дата создания аккаунта, когда нужно создать много ботов, их создают единовременно, и по близости даты создания (или ее совпадения) можно выявлять боты, входящие в одну группировку (управляемых одним ботоводом или участвующих в одном проекте). Но и дата создания сама по себе это дополнительный признак – если аккаунт создан на днях, то доверия к нему меньше.

Интересным показателем является соотношение длительности существования аккаунта (дата создания) к его активности (число публикаций или комментариев). Ведь если аккаунт зарегистрирован несколько дней назад, но при этом уже пара тысяч комментариев, то это необычно, хотя и возможно.

Число фрэндов – тоже интересный показатель. Ведь если у человека нет друзей, пусть и виртуальных, но при этом он активно общается (комментирует), то это не совсем обычно. Поэтому также интересен не сам показатель числа фрэндов, а его соотношение с длительностью существования аккаунта, числом публикаций и числом комментариев (входящих и исходящих).

Общая заполненность профайла – все ли пункты профайла заполнены. Ботов нужно создавать много, а потому нет времени и желания заполнять профайл. Заносится минимум данных, только те, которые нужны для регистрации и функционирования.

**Поведенческие признаки**

К этому типу признаков относятся те особенности, которые характерны для действий изучаемого аккаунта.

Участие в искусственном продвижении материалов ранее указывает на то, что данный аккаунт скорее всего бот. Есть случаи, когда люди свой реальный аккаунт «сдают в аренду» для автоматического распространения некой информации, но они единичны. Для этого существуют своеобразные биржи. Другой вариант – когда чей-то реальный аккаунт «угнали», или подобрали пароль и, не афишируя этого, используют его для распространения информации. Но во всех подобных случаях это уже бот.

Нормальный человек не может оставлять комментарии со скоростью 1 коммент в секунду. Как минимум нужно прочитать то, что комментируешь, сформулировать ответ и набрать его на клавиатуре. При самых парниковых условиях секунд десять на это уйдет. По этой причине, кстати, более точен показатель, основанный на соотношении скорости комментирования к длине самого комментария.

Комментарии разных аккаунтов с одного IP за короткий промежуток времени. Речь идет о ситуации, когда в комментариях одной публикации (например, в блоге) «оставили след» несколько аккаунтов за короткий промежуток времени и все с одного IP. Это явное указание на то, что управляются эти аккаунты с одного компьютера (сервиса) или через один прокси-сервер.

Содержание комментариев также может указывать на их нечеловечность – например, примитивные комментарии («+100500», «аффтар жжот», «убейся апстену»). Безусловно, это может написать и человек, а потому это лишь дополнительный признак. Другой вариант – комментарии «не в тему», когда содержание комментария не соответствует содержанию общения. Еще один вариант – точные дубли других комментариев, особенно когда коммент дублируется многократно (десятки, сотни дублей) за короткий промежуток времени. Но здесь нужно учитывать такое явление, как цитаты. Достаточно примеров, когда некое короткое высказывание нравится публике, и его начинают распространять именно люди, дублируя.

## Приемы противодействия

Поскольку «работа» ведется вами в информационном поле, то и технологии будут те же самые, что и у вашего противника.

### Дискредитация

Дискредитация (фр. Discrediter — подрывать доверие) — умышленные действия, направленные на подрыв авторитета, имиджа и доверия (http://ru.wikipedia.org). В нашем случае подразумевается дискредитация в глазах читателей автора негативной публикации или самой площадки (сайта), где публикация размещена. Дискредитация сайта полезна в том случае, если материал на ней не один и/или высока вероятность появления на этом сайте новых материалов по теме. Или когда не указывается автор публикации. В этом случае подрывается доверие к самому источнику информации.

Фактически, в результате вам нужно добиться того, чтобы читатель не воспринимал всерьез то, что публикует автор (сайт). Именно на этом есть смысл сконцентрировать усилия, а не на попытках оправдаться. Оправдываться бессмысленно – вы только добавите поводов поверить оппоненту, а не вам. Здесь сработает принцип «раз оправдывается – значит виноват». Кроме того, в результате оправдывания вы дадите оппоненту лишние инфоповоды над вами поглумиться. Поэтому не тратим силы попусту, а показываем истинное лицо оппонента. Причем используем его же технологию – обвиняем, а он пусть теперь отмывается. Но напоминаю – обвинение должно исходить от кого угодно, но не от вас и не от объекта, который с вами можно связать.

### *Обнародование компромата*
Тут всё просто – если у вас есть информация, о чем-то негативном, противоправном, аморальном в отношении объекта – это нужно предать огласке. Причем с оговоркой типа «ну если уж ЭТО, то как ему вообще можно верить?».

### *Обнародование виртуального компромата*
Если реального компромата нет, то его придумывают (создают видимость его наличия). Самый простой способ – придумать что-то и опубликовать. Но лучше если это что-то имеет частичные подтверждения, тогда больше читателей поверит.

### *Негативная похвала*
Такое действие подразумевает публичную похвалу объекта дискредитации. Специфика заключается в том, КАК похвалили или КТО похвалил. По поводу КАК похвалили – явное перехваливание. Например, чрезмерное употребление разных хвалебных эпитетов без подтверждения фактами, хвала за то, чего не делали, хвала с вкраплениями негатива… Вторая составляющая – это КТО хвалит. Если хвала исходит от негативно воспринимаемого аудиторией объекта, то, скорее, она будет иметь также негативный характер.

### *Разрушение виртуальных понятий*
Виртуальные, т.е. «живущие» только в нашем сознании, понятия – это такие, как престижность, универсальность, авторитетность, популярность, значимость и т.п. Эти понятия имеют определенную ценность для самооценки людей. А подвергая сомнению авторитетность или престижность автора или источника, можно добиться разных результатов от нервозности автора до потери к нему доверия со стороны читателей.

### *Немотивированное освистывание*
Это не что иное, как высказывание негативного суждения по поводу текста, иллюстрации, автора или самого ресурса. Здесь подходит всё от банального «да это бред какой-то» до обвинений в плагиате, необразованности, лицемерии – в чем угодно. Главное, чтобы эти обвинения носили массовый характер. И тогда читатель подумает – «раз уж столько народу так считает…» – сработает стадное чувство.

### *Общественное возмущение*
Этот метод близок к немотивированному освистыванию по своей организации. Но здесь используется обращение к другим социальным чувствам читателей. «Это попрание всех норм морали», «это возмутительно», «да какое он имеет право?» – знакомые фразы? А ведь их можно использовать по отношению к кому угодно.

### Размытие негатива
Размытие или растворение негатива подразумевает генерацию нейтральной или позитивной информации об объекте в объемах, превышающих объемы негативной информации. По сути, это «зашумление» негативной информации. Основной вопрос в том, на сколько или во сколько должно превышать число нейтральных и позитивных упоминаний упоминания негативные. Универсального ответа нет.
Например, если вы обнаруживаете, что в сутки появляется 10 негативных упоминаний объекта, то за те же сутки вам нужно создать (инициировать, сгенерировать…) 30, 40, а то и 50 упоминаний не негативного характера. И так каждый день до прекращения появления новых негативных упоминаний.

### Отвлечение
### *Отвлечение ресурсов оппонента на другую войну.*
Ресурсы всегда ограничены, а потому есть возможность уменьшить «силу» информационного воздействия на объект путем стимулирования «генератора негатива» на иную деятельность.

Например, на отражение информационной атаки на него или на защиту его подопечного объекта… В зависимости от особенностей такой контратаки, ее результат может быть как «местный», так и стратегический.

### *Отвлечение аудитории на новую сенсацию.*

Также можно отвлечь внимание аудитории на что-то более интересное, сенсационное, важное. Это что-то более интересное нужно создать (инициировать) или создать его видимость. Данная технология хорошо работает на коротком промежутке времени – порядка одного – трех дней. Если есть необходимость пролонгировать результат, то необходима последовательность сенсаций. Их также можно создать искусственно.

### *Отвлечение на малозначительный факт в рамках текущей проблемы*

Еще более тонким способом отвлечения является концентрация внимания аудитории на непринципиальных для вас (объекта) моментах в рамках озвученной противником проблемы. Фактически это может быть увод дискуссии в сторону или подмена понятий, но в итоге участники общения концентрируют внимание на не важных для вас фактах в рамках обсуждаемой проблемы.

### Доведение до абсурда

Достаточно действенный способ, основанный на «выработке иммунитета» у аудитории к негативу об объекте. Необходимо приучить аудиторию к тому, что негатив есть, но он ложен. Достигается такой эффект разными способами. Самый простой – заранее распространить информацию о возможных вариантах негатива с пояснением, что «не разобравшись в проблеме, некоторые люди начинают рассказывают разные небылицы типа этой и вот этой…»

Если такую иммунизацию провести не успели или она не дала результат, то можно гипертрофировать имеющийся негатив до фантастических и явно невозможных размеров, добавив еще и придуманного вами. И все это рассказать пользователям со словами «а еще мы поклоняемся инопланетному дьяволу и едим младенцев…». Присутствие явного бреда спровоцирует аудиторию на восприятие и остального негатива как бреда.

Еще один способ доведения до абсурда – это собрать весь негатив об объекте и распространять его, меняя имя (название) объекта на другие имена (названия), – любой нормальный человек, увидев такое, посчитает авторов текстов не совсем нормальными, а материалы – враньем. В том числе и материалы оппонента.

Помните ситуацию с заявлением о якобы обнаружении в прибрежных водах подводной лодки. Поначалу утверждалось, что это субмарина МО РФ. Был найден хороший способ доведения этой информации до абсурда.

### Работа над имиджем объекта

Пожалуй, наиболее действенным способом предупреждения негатива (точнее его последствий), а не только борьбы с ним, является активное формирование имиджа защищаемого объекта. Формируйте и распространяйте позитив об объекте. Активнее рассказывайте о положительном, обсуждайте на форумах, общайтесь со сторонниками… Делайте благодарные отзывы от сторонников, высказывания поддержки союзников… Продвигайте свою точку зрения, оптимизируйте подконтрольные объекту ресурсы, осуществляйте поисковую оптимизацию…

## Формирование текстов

Прежде чем начать распространять информацию ее нужно создать. В нашем случае речь идет о текстах, которые станут основой для вашего противодействия.

### Принципы

#### *Краткость*

Сложность формирования текстов заключается в том, что тексты должны быть «цепляющими», т.е. читателя должно заинтересовать написанное, даже если он далек от темы. И заинтересовать в первых строках этого текста, чтобы читатель захотел дочитать до конца. И при этом **материал должен быть коротким** – не более половины страницы. В крайнем (именно крайнем) случае – одна страница. Помните – вы ориентируетесь на тех, кто совсем не в курсе событий, а чтобы удержать их внимание, материал должен быть недлинным. Это первое требование к создаваемым текстам.

#### *Достоверность*

Второе требование к таким текстам – это **достоверность излагаемой информации**. Если информация не соответствует действительности, то рано или поздно оппонент найдет это несоответствие и использует данный факт для дискредитации и самого материала, и всех других материалов по принципу «единожды солгавши…». Единственная ситуация, в которой может быть оправдано использование недостоверной ситуации, – достижение преимущества на коротком промежутке времени и при сохранении анонимности распространителя информации. Например, при отвлечении ресурсов оппонента на короткий срок от основного направления.

### *Юмор*

Смешной материал воспринимается людьми гораздо легче. Позитив всегда больше нравится, чем что-то серьезное и, тем более, чем негатив. Мало того, такой материал запоминается лучше и им хочется делиться с другими. Информация начинает сама себя распространять. Именно эти свойства и определяют юмор как один из приоритетных свойств генерируемых материалов в информационной войне.

### *Серьезность*

Но бывают ситуации, когда юмор использовать нельзя. По разным причинам, но нельзя. Тогда материал должен быть серьезным, выдержанным и очень конкретным.

### *Посылы (мысли)*

Поскольку нужно, чтобы пользователь прочитал материал, то сам текстовый материал должен быть не очень длинным. Максимум одна страница, а лучше половина. Мало того, в тексте не должно быть хитросплетений, как в детективе. Нужна четкая и понятная последовательность изложения. Читатель не должен прилагать дополнительных усилий для понимания написанного. Кроме этого, в тексте не должно быть много «основных мыслей». Тех самых «смыслов» (идей), которые вы хотите донести до читателя. Их должно быть не более трех. Это максимум. А идеальный вариант – одна. В этом случае читатель ее запомнит с большей вероятностью, поймет и обдумает.

### *Ключевые слова*

Само собой, что создаваемый текст должен содержать ключевые слова, по которым вы продвигаете свои материалы в поисковых системах. Куда ж без них.

### *Оскорбления*

Ни в коем случае не используйте в своих текстах оскорбления – не нужно давать оппоненту дополнительную возможность для противодействия вам. А оскорбления – это именно такая возможность. Правда есть случаи, когда оскорбления используются. Например, для отвлечения ресурсов оппонента. Это когда вам нужно, чтобы оппонент потратил часть своих сил и средств на борьбу с «ветряными мельницами» и ослабил информационное давление на ваш Объект.

### *Оправдания*

Оправдания воспринимаются аудиторией как подтверждение неправоты. Мало того, оппонент может толковать ваше оправдание как «на воре и шапка горит» – это для него дополнительный аргумент в его пользу. Поэтому не оправдывайтесь.

### *Хладнокровие*

Важно не поддаваться эмоциям в ходе информационного противодействия. Эмоции – плохой советчик, а часто способ подтолкнуть вас к фатальной ошибке. Если вы только что увидели негатив о себе и тут же захотели ответить – остановитесь. Ответьте себе на простой вопрос: как изменится мир, если вы не будете отвечать прямо сейчас, а сделаете это завтра или не сделаете вовсе?

### *Визуализация*

Данное требование поставлено на последнее место, но оно вовсе не последнее, а одно из основных. Дело в том, что визуальный материал воспринимается человеком значительно быстрее. Такой материал оказывает дополнительное воздействие, лучше запоминается. Поэтому текст нужно сопровождать картинкой, не забыв в свойства этой картинки внести ключевые слова ☺

Еще лучше, если есть видеоматериал. А если видеоматериал с соответствующим звуковым рядом, то это просто великолепно.

## Приемы генерации контента

Как таковых приемов создания контента немного. Это создание нового и использование уже имеющегося. Но есть ряд «модификаций» этих приемов. **Создание уникального контента** может осуществляться «писателем» – человеком, собственно сочиняющим текст, рисующими картинку, снимающим видео. Или программой – автогенерация, когда новый текст или рисунок создает программа на основании случайного выбора образов. Другое направление – **создание псевдоуникального контента**, что выражается в модификации (изменении) имеющегося контента (образца) под новые задачи. Также может осуществляться как человеком, так и программно. Третье направление – **использование готового контента**. В данном случае возможны такие варианты, как создание библиотеки контента под разные прогнозируемые тенденции. Или «отзеркаливание». В основном, как осуществляется работа в том или ином направлении, понятно из названий, за исключением нескольких приемов, которые есть смысл разобрать чуть подробнее.

### *Автогенерация*

Автогенерация контента, или создание уникального текста программой, сопряжено со сложностью обучения машины создавать относительно длинные, осмысленные тексты, имитирующие прямую речь или литературный язык. Небольшие осмысленные тексты (до 30 предложений) со строгой структурой («сухие») уже используются для формирования текущих спортивных и финансовых новостей.

### *Генерация псевдоуникального контента*

Генерация псевдоуникального контента сводится к использованию набора шаблонов и словарей синонимов для создания под конкретную ситуацию относительно новых коротких текстов (обычно в одно предложение). В начале 90-х был популярен «Бредогенератор» – программа, которая, комбинируя данные из трёх словарей (словарь подлежащих, сказуемых и определителей), формировала вполне себе осмысленные предложения. Затем появился «автоответчик для ICQ, который не генерировал новые варианты ответов, а выбирал их из базы готовых ответов по несложному алгоритму. Всё это примеры простых генераторов псевдоуникальных текстов.

### *Отзеркаливание*

Один из распространенных способов создания контента – это использование уже готового контента, созданного противником, но с небольшой его корректировкой, образно говоря, сменой «общего знака контента» (с минуса на плюс или наоборот).

Последнее время примеров использования данного приема было много. Достаточно вспомнить использование украинской стороной фотографий замерзших бойцов АТО (снимки выдавались за фото защитников Донбасса).

## Способы распространения информации

Финальный вопрос темы (но не технологии) – как же распространить тексты со своим мнением? Вопрос, при всей его видимой простоте, таит в себе ряд подводных камней. Во-первых, нужно помнить, что этот самый текст для распространения, который вы так кропотливо делали, всего лишь один из инструментов информационной войны. Хоть и очень важный, но один из. Во-вторых, текст этот создан не ради его создания, а ради воздействия посредством него на целевую аудиторию. И тем эффективнее он сработает (в большинстве простых случаев), чем больший будет охват этой целевой аудитории. И в-третьих, как следствие из предыдущих пунктов, текст сам по себе ничего не сделает – его нужно максимально широко распространить. Или не широко, но так, чтобы он гарантировано дошел до тех, кому предназначен. Исходя из этого, рассмотрим посредством чего можно ваш замечательный текст распространить в интернете.

### «Прямые» способы распространения

Прямыми эти способы названы по причине того, что вы сами осуществляете публикацию (распространение) информации.

#### *Блоги*

Блоги самый мощный ресурс для продвижения текста, а вместе с ней и вашей идеи. Связано это с несколькими особенностями блогов. Первая – это простота и скорость создания. Если не претендовать на эксклюзивность, то блог с доменом третьего уровня создается в течение нескольких минут. Создать таких блогов можно неограниченное число. Цена вопроса – только затраты времени (тех самых нескольких минут), да в некоторых случаях затраты на новую СИМ-карту (когда регистрация увязана с подтверждением личности через номер мобильника). Вторая – в блоге вы сами решаете, что публиковать, а что нет, какие комментарии оставлять, а какие удалять – вы, а не кто-то еще.

Достаточно поверхностного изучения, например, отечественного блогохостинга под названием LJ (он же ЖЖ), чтобы увидеть, как активно используются блоги для информационных войн. Возьмите топовые журналы и посмотрите наиболее комментируемые темы. Особо обратите внимание на смысл комментов и скорость их появления. Очень интересные выводы напрашиваются. А когда полученные данные накладываются на «ареал обитания» комментаторов (какие темы и где они комментируют), то выводы становятся еще более конкретными.

##### Обычный блог

Обычный – это блог, созданный на специализированных блогохостингах (LiveJournal, uCoz, Блоги@Mail.Ru, LiveInternet, Acars.ru, BabyBlog.ru, Blogger.com и т.п.). Это бесплатно и быстро. У такого блога домен третьего уровня, но, несмотря на это, «большие» поисковики интернета мониторят такие блогохостинги очень внимательно, и ваша публикация будет в их выдаче самое позднее через несколько часов. А при некоторых ухищрениях – мене чем через час.

##### Блог на отдельном домене

Для данного типа источника необходимо арендовать доменное имя и хостинг. При нынешних ценах это от 4,5 тысяч рублей в год. Тоже не очень дорого. Зато такой блог будет расположен на домене второго уровня, что для поисков является признаком большей авторитетности источника. В остальном это такой же блог, как и те, что расположены на специализированных площадках.

##### Микроблоги

Это блоги с ограниченной длинной сообщений. Фактически это СМСки для всех (Twitter, Rutwitt, Жужужу, Juick, FriendFeed, DUDU, Я.ру и т.п.). В нашем случае они полезны скорее не как место распространения идей, а как средство оптимизации других площадок. Например, для распространения названия публикации на основном блоге со ссылкой на него, для привлечения внимания и т.п.

## Как использовать блоги

### *Управляющий блог*

Это блог, который используется для управления распространением материала. Схема простая – на управляющем блоге публикуется нужный материал, а уже с помощью RSS-потоков, bot-ов, троллей, задействованных в мероприятии, материал многократно дублируется, распространяется дальше, комментируется. Нередко управляющий блог делают «закрытым» (видимым только фрэндам). Такая схема нужна, чтобы усложнить вычисление сети, ее узлов и выработке мер противодействия вам.

### *Продвигаемый блог*

Это блог, используемый для продвижения материала в ТОП выдачи поисковиков. На этот блог делаются релевантные ссылки, что и продвигает его вверх выдачи в поисковиках по вашему ключевому слову. Иногда таких блогов делают несколько (если бюджет позволяет), что значительно усиливает воздействие. В простых случаях управляющий и продвигаемый блоги совпадают, но это подходит именно для простых случаев.

### *Блог поддержки*

Блоги поддержки нужны для многократного дублирования материала и создания релевантных ссылок на продвигаемый блог или иную продвигаемую страничку в интернете. Помимо этого, блоги поддержки используют для комментирования и продвижения материала в ТОП популярности (обсуждаемости).

### *Блоги-камикадзе*

Их назначение быстро повлиять на ситуацию. Быстро опубликовать материал, создать первую ссылочную массу, спровоцировать обсуждение, отвлечь внимание и т.п., чтобы у вас появился небольшой запас времени для создания минимальной инфраструктуры для отражения нападения. Поскольку задача таких блогов влиять на ситуацию сутки, максимум двое, то и особых требований к их адаптации под требования поисковых систем в плане «человечности» материала нет. Главное быстро разместить информацию (ударную, отвлекающую, провоцирующую, маскирующую).

### *Комментарии к блогам*

Комментарии также важны для продвижения материала. Ведь в комментариях также можно изложить идею. Мало того, в комменте можно сделать и ссылку. И это не всё – комменты влияют на позиции в рейтинге обсуждаемости. А это дополнительный приток читателей и дополнительное дублирование уже никак не связанными с вами источниками. Но и это еще не всё – число комментов к материалу (по слухам) учитывается и поисковиками и влияет на их выдачу. Нередко в комментариях содержится больше материала, чем в основном (комментируемом) тексте.

### *«Замаскированные» блоги*

Эти блоги мимикрируют. Одни блоги делают вид, что им интересна определенная тема, набирают фанатов этой темы в друзья, авторитетность у поисковиков, ссылочную массу… А в день «Ч» начинают публикацию нужных их владельцу материалов. А их уже читают, цитируют, на них ссылаются…. Точно по той же схеме создают сообщества или группы в социальных сетях. Вначале эта группа фанатов чего-то безобидного и общепринятого, а после набора нужного числа читателей (или в назначенный день) админ группы меняет ее название и «ударный» контент на нужный ему, и вот появилась группа со 100 тысячей пользователей, требующих отставки правительства. А пользователи и не догадываются о том, что они состоят в такой группе.
Другой вариант замаскированных блогов – это создание дневника якобы в поддержку вашего оппонента. Такой блог позволяет выявить сочувствующих оппоненту, их подготовку, их ресурсы и т.п. Мало того, такой блог может серьезно деморализовать оппонента, когда в самый не подходящий момент начнет вещать совсем не в его пользу. Или если на нем случайно и косвенно

начнет появляться информация, так или иначе компрометирующая оппонента и подталкивающая его аудиторию к сомнению.

### *Сайты компромата*

Сайты, на которых публикуются негативные материалы. Таковых вполне достаточно, причем как глобальных (обо всех), так локальных (по теме, по региону…) и персональных (компромат на конкретное лицо или компанию). Их назначение вполне конкретно – легализация материалов. Другими словами, дать манипулятору возможность ссылаться на какой-то источник, называть его первоисточником и не отвечать за клевету, ведь это не он первый опубликовал. Ваш оппонент может использовать уже имеющиеся сайты компромата, а может создать свои, специально для информационной войны с вами.

### *Сайты-клоны*

Точная копия какого-то популярного у вашей целевой аудитории сайта. Иногда используется сей прием для снятия «барьера недоверия» – вроде как от доверенного источника информация пришла… Внешне ведь точь-в-точь как «тот самый» сайт, а на адресную строку мало кто обращает внимание.

### *Сайты-подставы*

Разновидность сайтов-клонов – копия сайта, который нужно скомпрометировать или от имени которого нужно ввести в заблуждение целевую аудиторию. Размещается заведомо ложная или провокационная информация, и аудитория перестает доверять источнику. Очень распространено в социальных сетях. Это так называемые фэйковые аккаунты. Создали аккаунт от имени вашего оппонента (вроде как это он его создал), начали размещать вначале правдивую и интересную информацию, набрали «фрэндов», попутно выяснив «кто за него», а затем начали размещать информацию, дискредитирующую оппонента. И если ложность аккаунта не вскрыта – часть сторонников вашего оппонента разочаровалась в нем.

### *Комменты к статьям*

Большинство онлайн СМИ, публикуя материалы, дают возможность их комментировать пользователям. Эдакая обратная связь с аудиторией и попытка понять, что пользователям интересно и почему. Это можно и нужно использовать для распространения информации – комментарии точно так же индексируются поисковиками, а значит в них можно помещать полезную информацию вплоть до ссылок, картинок…

### *Форумы*

Форумы – это отдельный большой «кусок» интернета, позволяющий людям общаться. Таких площадок много: от «всё обо всём» до узкотематических. Поскольку форумы предназначены для общения, то их нужно использовать как для распространения информации и ссылок, так и для получения сторонников, для провоцирования обсуждений, в том числе и эмоциональных, для выявления сторонников оппонента…

#### Общение ради ссылок

Цель такого «общения» – сделать ссылки на продвигаемый ресурс. Т.е. осуществить его поисковую оптимизацию и заодно заманивать туда людей с этого форума. Но нужно помнить, что последнее время учет ссылок с форумов сведен к минимуму, тем не менее поисковики по ним переходят, и люди по ним переходят, а ссылки с «авторитетных» для поисковиков форумов всё же учитываются при ранжировании страниц.

Но для эффективной работы на форумах нужно соблюдать некоторые правила. Например, не нужно заниматься явным спамом – это никому не нравиться, и вы будете быстро забанены. Поэтому необходимо выбрать подходящую вам по теме «ветку» форума и разместить в ней обоснованный пост с нужным вам материалом. Как говориться, ваша реплика должна быть «в тему», а не «с потолка». Только в этом случае у вашего материала есть шанс остаться на форуме.

### Общение ради распространения идеи

В этом случае цель заполучить сторонников вашей идеи (убеждением, разъяснением, провоцированием), а они уже сами найдут нужный материал.

### Особенности

При работе на форуме есть ряд особенностей, которые нужно учитывать. Первое – это ваш профиль. Профиль нужно заполнять релевантной вашей легенде информацией и с использованием тех ключевых слов, по которым планируете осуществлять продвижение материала (если планируете). Обязательно используйте теги, которые также должны содержать ваши ключевые слова. Не забудьте про подпись, которая будет ставиться в конце каждого вашего поста – ее также нужно сделать соответствующей вашей легенде и продвигаемому вами материалу.

И сами сообщения делайте интересными, а не занудными (зануды мало кому нравятся, а потому пользователей отталкивает и продвигаемая занудой идея). Поэтому не пытайтесь каждым постом что-то «вдолбить» собеседнику. Гораздо эффективнее привлечь внимание и заручиться поддержкой через помощь.

Неплохо работает создание нескольких аккаунтов (виртуальных личностей) и распространение информации через общение между ними. Конечно же, нужно помнить, что модераторы быстро выявят такое «продвижение», если вы не предпримите некоторые меры анонимизациии. Как минимум – каждый виртуал должен работать со своего IP-адреса.

## *Гостевые книги*

Это отзывы на сайте, в которых также можно оставлять ссылки и мнение, вести обсуждение и обмениваться данными. На «живых» площадках обычно есть предмодерация или постмодерация, которую нужно учитывать.

Даже старые, давно не обновляемые гостевые книги полезны – ведь они давно в инете, а потому для поисковых систем являются весьма авторитетным источником (по признаку старости контента). И это обстоятельство нужно использовать.

## *Сервисы публикаций*

Существуют разнообразные сервисы публикации материала. От разовых (вроде как оставить на память) до долгосрочных. С точки зрения информационной войны их функционал близок к блогам (но значительно проще). Их также нужно использовать. Пример такого сервиса – Ontex.info

## *Сервисы закладок*

Это сервисы онлайн хранения интересных закладок. Они бывают автономные и встроенные в другие сервисы, простые и сложные. Но все они активно отслеживаются поисковыми системами т.к., по их мнению, указывают на то, что интересует людей больше всего. Поэтому такие сервисы очень полезны для поисковой оптимизации продвигаемого контента.

Закладки нужно делать «открытыми» (доступными всем), а их название становится ключевым словом ссылки. Поэтому название создаваемой закладки нужно продумывать и включать в него ваши ключевые слова. Мало того, у закладок есть теги, которые тоже являются и ссылками, и ключевыми словами. Но и это не всё. Комментирование закладок – это тоже и якорные слова, и ссылки, и мнение пользователей, которое учитывают поисковые системы.

## *Фотохостинги*

Фотохостинги также являются хорошим инструментом продвижения материала. Кроме релевантных ссылок на «ударный» контент, с помощью фотохостингов вы заполняете нужными вам материалами «поиск по картинкам» у поисковых систем. Что также помогает в продвижении идеи.

Для эффективного использования фотохостингов нужно помнить о некоторых особенностях. Так, название альбома должно обязательно содержать ваши ключевые слова, как и теги к публикациям. В подписях к фото тоже должны быть те же самые ключевые слова. И не забывайте

про комментирование фотографий – это тоже способ распространения идеи и способ поисковой оптимизации ударного контента.

## Сервисы SMM

Social media marketing (SMM) — процесс привлечения внимания к бренду или продукту через социальные платформы (http://ru.wikipedia.org/wiki/Social_media_marketing ). Другими словами, это технологии распространения информации с помощью социальных сервисов интернета. Через прямое предоставление информации, через общение, через разного рода вовлечение пользователей. По сути, это инструмент для рекламы, PR, маркетинга в социальных сетях. В его основу заложено желание людей общаться в сочетании с удобством такого общения на соответствующих площадках. Но это ведь ровно то, что нужно для ведения информационной войны и для противодействия информационным войнам. Но живое и правдивое общение давно уже уступило место технологичным приемам манипулирования. Далее примеры наиболее используемых технологий. Они проиллюстрированы некоторыми реальными сервисами, по одному, дабы не распространять информацию о них слишком активно.

### *Биржи*

Начнем с того, что создавать быстро и много уникального контента одному человеку не под силу. А посмотрите на блогеров, находящихся в ТОПе поисковиков или же блогохостингов. Обратите внимание на частоту появления новых материалов, их объем, глубину проработки и частоту комментирования своих и чужих публикаций. На мой взгляд, даже если заниматься только одним блогом и не отвлекаться более ни на что, всё равно не получится так много и быстро писать. Значит, это делает не один человек.

Понятно, что в одном блоге может публиковать свои материалы неограниченное число людей, но проще, не теряя контроля над своим блогом, заказывать такие материалы. Для этого существуют соответствующие биржи – специализированные сайты, где можно купить понравившийся материал или заказать материал на определенную тему.

Мало того, на таких биржах можно купить и репост своего материала от имени других блоггеров, что поднимет авторитет вашего блога. А можно купить неограниченное число комментариев к вашему материалу от лица других блоггеров. При этом можно выбрать, что за блоггеры будут комментировать и какого рода комментарии будут оставлять. Например, можно ограничить географию или язык комментов, а также указать, какие ключевые слова должны присутствовать в таких комментариях. Да и тональность самих комментариев можно заказать. Например, восхваляющие заслуги кого-то, или, наоборот, критикующие что-то… Вопрос только в вашем бюджете. Как вы думаете – сколько времени нужно, чтобы вывести ваш блог из только что созданного состояния в ТОП поисковых систем, используя такие биржи? При условии достаточности финансов. А что значит попасть в ТОП выдачи поисковиков с точки зрения влияния на аудиторию, вы уже знаете…

Помимо этого, на подобных биржах можно купить нужное число аккаунтов в любых сервисах, или заказать их создание. Правда, нет никакой гарантии, что эти аккаунты (которые вы закажите или от имени которых будет распространятся информация) будут «чистые», а не взломанные.

Таких сервисов (бирж) в интернете достаточно много. Они позиционируют себя как сервис для СММ, но это технологии двойного назначения. Вот пример того, как позиционируют себя такие сервисы:

«Наполните сайт, блог или интернет магазин контентом.
Оживите ваш форум.
Спровоцируйте пользовательскую активность.
Репосты и лайки в социальных сетях.
Поддержка любых CMS.
Переходы с нашей биржи не фиксируют счетчики.
Осмысленные, без грамматических ошибок публикации.
Проверка комментариев перед оплатой.»

Примеры таких сервисов:

http://qcomment.ru/
http://wpcomment.ru/
http://www.rotapost.ru/
http://buylike.ru/
https://socialtools.ru/
Это только те, что «попались под руку», а их гораздо больше. Вот примеры бирж, специализирующихся на продаже аккаунтов:
http://www.buy-ak.ru/
http://www.inviter.ru/
http://akkaynt.net/

### *Кросспостинг*

Кросспостинг в Интернете — умышленное автоматическое, полуавтоматическое или ручное помещение одной и той же статьи, ссылки или темы в форумы, блоги, либо иной формы сайты или публичные переписки, в том числе и в режиме онлайнового общения (например, IRC, CommFort, Skype) (wikipedia.org ). Это не что иное, как многократное дублирование контента. Оно нужно, например, для «посева», когда есть потребность распространить один и тот же материал от имени большого числа пользователей. Для этого используются специализированные сервисы от простых (работающих с одной соцсетью) до сложных (охватывающих многие соцсети и предоставляющие дополнительные сервисы). Примеры таких решений:
http://www.pistonposter.com
http://novapress.pro/
http://www.prpilot.ru/
http://socialpilot.ru/
http://sociate.ru/
https://www.buzzlike.pro/

### *Сервисы управления аккаунтами*

Еще один интересный сервис, который позиционируется как инструмент SMM, это сервис управления аккаунтами. Его замысел в том, что у пользователя есть по одному аккаунту в каждой из наиболее популярных соцсетей и не хочется тратить много времени на то, чтобы один и тот же материал постить там, там и там… Гораздо удобнее это сделать нажатием одной кнопки, а лучше и вообще не нажимая – автоматом. Появился материал в «управляющем» аккаунте, и тут же система его опубликовала в подконтрольных сервисах. Но ведь это и есть тот же «посев» в информационных войнах… Особенно при учете того, что можно сделать много аккаунтов и синхронизировать их через управляющий блог. Пример такого сервиса http://feedman.ru/ или https://time2post.ru/

### *Боты*

Бот (англ. bot, сокр. от robot, бот) — программа, автоматически выполняющая действия на компьютере вместо людей http://lurkmore.to/%c1%ee%f2 . Да – это программы, которые позволяют автоматизировать процесс распространения информации в социальных сетях. Например, посредством публикации контента от имени большого числа разных пользователей. Или «накрутка» лайков… Интересным примером таких программ являются решения разработчиков из http://viking-studio.com/ А бывают и такие «онлайн боты» http://pamani.ru/

## Технические вопросы

### SEO оптимизация

Как человек ищет нужную ему информацию в интернете? Самый очевидный способ – это задействовать поисковики: задать запрос в них, используя ключевые слова. В этом случае

поисковик выдает результат, в первых строках которого будут материалы, по мнению этой поисковой машины, наиболее соответствующие вашему запросу. Соответствующие вашему запросу в виде ключевых слов. Собственно, эти самые ключевые слова и есть основа, на которой строятся все манипуляции с попаданием на первую страницу выдачи поисковых машин. Ключевые слова и ссылки на продвигаемый сайт. Именно создание такого сочетания ссылок и ключевых слов, которое выведет сайт в первые строки выдачи поисковика, и называют SEO или поисковой оптимизацией (если совсем просто).
В информационной войне поисковая оптимизация играет важную роль. К примеру – если ваш оппонент некий гражданин с Фамилией, Именем и Отчеством, то «раскрывая миру глаза» на то, кто он на самом деле, нужно сделать так, чтобы при поиске по этим Фамилии, Имении, Отчеству людям, в первую очередь, попадался сайт с этой самой информацией (кто он на самом деле). Для этого нужно создать или подобрать страничку с таким материалом и с помощью поисковой оптимизации вывести ее на первые строчки выдачи поисковика по Фамилии, Имени, Отчеству.
Последнее время «большие» поисковики один за другим объявляют о нахождении и применении некоего алгоритма определения наиболее релевантного материала без учета ссылок на него. Вообще, алгоритм ранжирования является одной из наиболее защищаемых тайн в работе поисковых систем. Ведь, как только он станет общеизвестен, сразу станет понятно, как его обойти и поставить в первые строки выдачи именно свой материал, а не тот, который больше соответствует запросу пользователя. И именно с поправкой на это и нужно воспринимать все подобные заявления больших поисковиков. Так вот, в основу нового алгоритма якобы положена процедура определения авторитетности источника и нахождения первоисточника информации, которая интересует пользователя. А что такое первоисточник? – правильно – это искомая информация с наиболее ранней датой публикации. А вы обращали внимание на то, что, например в ЖЖ дату публикации можно поставить самому и указать ее не совсем соответствующей действительности? В общем, есть над чем подумать в области оказания влияния на эти новые алгоритмы поисковиков. Но и ссылки остались важной составляющей определения степени релевантности информации. Только теперь стало важнее их «качество», т.е. соответствие представлению поисковой системы о важности (полноте, авторитетности, человечности) информации. Например, на первые позиции выходят ссылки, сделанные из уникального тематического текста. Тогда как ссылки из многократно дублированного контента получают наименьший коэффициент влияния. Становятся более «влиятельны» такие виды ссылок, как лайки (да-да, это тоже ссылки) или «мне нравится», или «поделиться»…
А теперь, очень кратко, без лишней напыщенности, что же из себя представляет эта самая поисковая оптимизация. А начнем с напоминания того, что с поисковой оптимизацией ведут постоянную борьбу поисковые сервисы. Оптимизацию стараются «вычислить» по разным признакам, а сайтам, заподозренным в оптимизации, грозит удаление из выдачи поисковиков. Звучат громкие заявления администрации поисковиков, что они нашли универсальный алгоритм, но ситуация остается той же, что и раньше.

### Наполнение сайта

Как и было сказано чуть выше – один из основных компонентов поисковой оптимизации – это ключевые слова, которые должны содержаться в текстовых элементах продвигаемой страницы. Те самые ключевые слова, по которым люди ищут информацию по «вашей» проблеме. Эти ключевые слова должны содержаться основном тексте (в вашем повествовании), причем обязательно – в первом абзаце, в заголовке материала и в заголовке страницы, в названиях картинок, что используются в материале.
Если с числом ключевых слов в названиях более или менее понятно – один раз. То вот в основном тексте можно варьировать. И возникает вопрос – сколько раз ключевые слова должны попадаться в основном тексте (какова должна быть их плотность)? Ведь, по мнению поисковой машины, чем их больше – тем более ваш текст соответствует теме ключевого слова. Конечно, можно сделать весь текст состоящим из ключевых слов, но с такой «оптимизацией» поисковые системы научились бороться. Такому сайту присвоят «штрафные очки» и выкинут из выдачи. Поэтому

важно не перейти ту самую границу, за которой поисковым сервисам ясно, что текст именно оптимизирован.
В этом вопросе нет четкой рекомендации, скорее нужно полагаться на естественность и чувство меры. Если использование ключевого слова естественно вписывается в нормальное звучание предложения – можно использовать. Используется такой прием – в тексте о некоем объекте (если ключевое слово, это и есть название объекта) все местоимения, указывающие на этот объект (он, ему, его), заменяются на полное название объекта, т.е. на ключевое слово.
Еще одним аспектом, связанным с основным текстом оптимизируемого сайта, является его оригинальность (уникальность). Т.е. неповторимость текста – отсутствие в интернете второго такого же текста. Тема эта очень спорная. Но точно можно сказать, что уникальный текст даст положительный результат в психологическом направлении. Пользователям всегда интересно читать что-то новое, нежели повторение уже прочитанного. Поэтому уникальный текст, при прочих равных, имеет дополнительный плюс.
Но создавать уникальные тексты довольно хлопотно. Поэтому используют некоторые ухищрения. Например, оригинальный текст заказывают внешнему исполнителю. Или берут чей-то материал и пересказывают его своими словами. Есть еще один способ – берется чужой материал (со ссылкой на оригинал) и к нему делается нечто вроде вступления-пояснения-комментария, которое придает некоторую новизну.
Продвигают такие ресурсы не по коммерческим словам, т.е. не по тем ключевым словам, за которые идет конкурентная борьба. Значит, нет большого числа ресурсов, которые «оптимизируются» именно по этим словам. Чаще всего это ФИО некоего человека, а такое сочетание не является коммерческим. А раз так, то и нет нужды делать значительные усилия.

### Ссылки и ссылающиеся ресурсы

Ссылки – это вторая ключевая составляющая оптимизации. Именно по количеству ссылок на оптимизируемый ресурс поисковая система принимает решение о ценности этого ресурса для пользователей. Особую ценность, с точки зрения поисковых систем, представляют релевантные ссылки. Ссылка является релевантной, если в ней, в качестве якорного слова, используется ваше ключевое слово.
Ссылки имеют свою форму написания (теги). Пример такой релевантные ссылки, при условии, что ключевым словом является словосочетание «конкурентная разведка» <a href=”http://ci2b.info/”> Технологии конкурентной разведки для всех</a> Именно в таком виде ссылки присутствуют в HTML коде. И именно в таком виде их нужно создавать.
А создавать такие ссылки на продвигаемый ресурс можно самостоятельно. И чем больше таких ссылок будет зафиксировано поисковой системой, тем выше будет продвигаемый сайт в выдаче поисковика по используемому ключевому слову. Логичный вопрос – как сделать так, чтобы таких ссылок было много? Вопрос тоже вполне логичный – сделать самому. Например, в тексте материалов, которые вы публикуете в своем блоге, или в Твиттере, или на форуме. Но можно и не в своем болге. Точнее, в блоге, который вроде бы вам и не принадлежит, а принадлежит некой виртуальной личности, которую вы создали и контролируете. И таких блогов, аккаунтов на форумах можно создать множество. А значит, что и мест для создания ссылок у вас тоже будет множество.
Еще один не маловажный момент – наличие таких же ключевых (якорных) слов и в тексте страницы, на которой стоит ваша «продвигающая» ссылка. Логика поисковых систем простая – если ссылающаяся страница содержит те же ключевые слова, что и продвигаемый сайт, значит это действительно имеет значение для людей, а значит вес такой ссылки увеличивается.
Также важно наличие ссылок друг на друга сайтов, участвующих в продвижении основного сайта. Связано это с особенностью работы краулеров (роботов, которые «ходят» по сайтам и индексируют их содержимое). Другими словами – если в обрабатываемой странице обнаружена ссылка, то робот пройдет по этой ссылке и посмотрит, что там. Если сайты, задействованные в продвижении, ссылаются друг на друга, то робот каждый раз будет обходить их все, тем самым быстро обновляя создаваемые вами изменения.

Такое же значение имеют и «внутренние» ссылки сайта – ссылки на разные страницы одного сайта. Поэтому важное значение имеют качественно созданные теги, оглавления, темы и прочие «фишки» сайта. Кстати, в тегах, оглавлениях и темах также полезно использовать ключевые слова. Это увеличивает их плотность и создает релевантные ссылки, пусть и внутрисайтовые.
Возраст сайта также влияет на его «авторитет» у поисковиков – чем старше сайт, тем больше ему доверия, и тем быстрее он попадет в первые страницы поисковиков. Поэтому если вы занимаетесь информационными войнами постоянно, то лучше сделать «заготовки» на будущее – сделать сайты на нейтральную тему и «поддерживать их на плаву».
Важно, чтобы с продвигаемого вами сайта не было ссылок на спамерские ресурсы и на сайты с противоправным контентом. Такие ссылки для поисковых систем являются однозначным признаком для удаления из выдачи ресурса, содержащего такую ссылку.
Есть еще ряд моментов, так или иначе влияющих на продвижение целевого сайта. Например, в блогах, используемых для продвижения, нужны и «статические» ссылки на продвигаемый сайт. Это ссылки, которые указывают в разделах «Мои любимые страницы» или «Обязательно посмотрите». Они будут «показываться» интернет-роботам на каждой странице вашего блога, что хорошо, да и люди нет-нет, да будут переходить по таким ссылкам, что тоже вам на руку.
В блогах, используемых для продвижения, должны быть «френды» – по сути, это дополнительные ссылки на «союзные» ресурсы, а значит и дополнительная возможность удержать «внимание» краулера на своем ресурсе.
Не забывайте заполнять профиль блогов, причем заполнять тематическими словами и естественно не своими данными. Это придаст больше «человечности» блогу и дополнительные бонусы у автоматизированных систем анализа.
Еще один важный момент – это комментарии в блогах, используемых для продвижения. И эти комментарии должны быть не просто тематическими, но и содержать ваши ключевые слова. Такие комментарии делают блог еще более «человечным» в глазах поисковиков. Мало того – в комментах можно ставить релевантные ссылки, которые не только работают по прямому назначению, но и воспринимаются краулерами как однозначно ссылки, созданные людьми, а значит более авторитетные.

### *Подъем в ТОП поисковиков позитива о себе*

Замещая в выдаче поисковиков негатив о себе позитивом, вы так или иначе «поднимаете» позитивную информацию о себе. Поэтому постоянная работа по созданию позитивной информации о себе должна войти в привычку – это нужно делать регулярно, если есть хоть малейшее подозрение о возможной агрессии.

### *Выдавливание из ТОП выдачи поисковиков негатива о себе*

Что же делать, если по запросу вашего ФИО на первой странице выдачи поисковика, а то и на первом месте, стоит именно та самая страница? Вспомните, КАК продвигают в ТОП выдачи поисковых машин нужную информацию. Понимая это, вы поймете, ЧТО сделал агрессор для достижения такого результата. Соответственно, понятно, ЧТО нужно сделать вам – создать ресурс с позитивной или нейтральной информацией, который по релевантности будет выше цениться поисковыми машинами, нежели ресурс с негативом. И тогда ваш ресурс станет «выше» вражеского. Для надежности, таких ресурсов нужно создать десять – чтобы вытеснить негатив со всей первой страницы выдачи поисковика.
Но можно и не создавать новые страницы с нейтральной или позитивной информацией. Можно воспользоваться уже имеющимися. В таком случае вашему оппоненту будет труднее понять, что происходит. Ведь если появляются новые страницы «ни о чем» и выходят в ТОП, то это явно искусственные действия. А вот когда в ТОП выходят уже давно существующие страницы – тут уже сложнее понять, что происходит.
То, КАК вывести в ТОП нужные страницы, мы поговорили чуть выше – ссылки, ссылки и еще раз ссылки. Главное помните – эти ссылки можно оставлять в самых разных местах. От блогов, форумов и гостевых страниц, до сервисов закладок, хранения фотографий и публикации новостей…

### *Подъем в ТОП поисковиков негатива об оппоненте*

Точно так же, как вы «поднимали» в выдаче поисковиков позитивную информацию о себе, вы можете поднимать и негативную информацию об оппоненте. Зачем? – все очень просто – такие действия заставят его отвлечь часть ресурсов на борьбу с негативом о себе. И у вас появится больше возможностей справиться с ситуацией.

Обычно негатив не нужно создавать искусственно – достаточно внимательно изучить следы оппонента, и всё найдется. Люди сами дают достаточно поводов.

### *Выдавливание из ТОП поисковиков позитива об оппоненте*

Если вы «поднимаете» негатив об оппоненте, то позитив о нем естественно будет выдавливаться вниз – просто ресурсы с негативом будут занимать топовые места. Это вновь «другая сторона медали» – делая одно, вы оказываете влияние и на второе.

### *Технические приемы (твиттер, блоги, форумы…)*

Самым очевидным способом создавать релевантные ссылки на нужный ресурс является самостоятельное создание таких ссылок. А наиболее подходящей формой для этого являются **блоги**. Во-первых, созданный вами блог подконтролен вам, а не кому-то еще. И вы можете с ним работать, как вам удобно. Во-вторых, крупные блогохостинги находятся «под неусыпным контролем» крупных поисковых систем и индексируются ими достаточно регулярно. И есть еще один момент – социализация поисковиков. Ища способы противодействия оптимизаторам, поисковые системы всё больше значимости предают данным из социальных сетей. По этим причинам ваши материалы будут быстро проиндексированы, что важно в ходе отражения информационной агрессии. Кроме того, таких блогов можно создать неограниченное количество – главное самому не запутаться в них.

Также не забывайте, что ваши публикации можно комментировать и оставлять в этих комментариях ссылки, которые также будут учитываться поисковыми системами. Мало того – комментарии помогут в продвижении вашего материала в ТОП обсуждений, что увеличит посещаемость страницы и привлечет внимание большего числа читателей.

Но есть один тонкий момент. Блоги на блогохостинге – это сайты с доменом третьего уровня. А такие площадки для поисковых систем чуть менее авторитетны, чем расположенные на домене второго уровня. По этой причине, если есть время и немного денег, то лучше создать основной блог (основную площадку) на отдельно арендованном домене. Ссылки с такого сайта-блога будут иметь чуть больший вес при ранжировании у поисковиков.

Еще одним продуктивным способом распространения релевантных ссылок является их размещение **в комментариях** к тематическим статьям на сайтах новостных агентств, профильных порталов т.п. Как правило, такие сайты являются давно действующими и признаются поисковыми системами как более авторитетные источники. А значит, и ссылки с них приобретают дополнительный «вес» при ранжировании. А также привлекают дополнительное число пользователей, чем способствуют распространению информации.

**Форумы** также можно и нужно использовать для увеличения числа ссылок на продвигаемый ресурс. Но в отличие от созданных вами блогов, это чья-то площадка. А значит и правила на этой площадке чьи-то. И они могут отличаться от удобных вам. Например, может быть запрещено создавать ссылки на внешние ресурсы. Или такие ссылки могут создавать пользователи с определенным уровнем «доверия», который определяется по числу публикаций или по времени, проведенном на форуме или индивидуально, присваивается модератором. Кроме того, форумы, особенно малоизвестные, гораздо реже индексируются поисковиками, и потому ссылка на них может оказаться задействованной в ранжировании позднее, чем вам этого хочется. Тем не менее форумы нужно использовать для создания дополнительных ссылок и для ознакомления людей с вашей точкой зрения.

Еще одним «интересным» местом распространения ссылок являются **гостевые книги** сайтов. Это места, где администрацией сайта планируется размещение отзывов пользователей, общения с ними и т.п. В таких разделах также возможно размещение ссылок. Правда, здесь есть свои

трудности. Например, тематичность ресурса и модерирование контента таких отзывов. Но, во-первых, можно подобрать тематические сайты, а во-вторых, можно найти «заброшенные» площадки, которые давно не обновлялись и, скорее всего, уже неинтересны их создателям. Но если они не представляют интереса создателям, то это не значит, что на них нельзя размещать ссылки. А кроме этого, такие площадки, давно размещенные в интернете, являются для поисковых систем достаточно авторитетными из-за своего возраста. А значит и ссылки с них также получают «дополнительные очки».
Если поразмыслить, то можно найти много мест в интернете, где есть возможность оставить ссылки. Например, **сервисы хранения закладок** – в принципе, место, предназначенное для ссылок. А если эти ссылки сделать общедоступными, то они начинают работать в нужном нам русле. **Ленты новостей** пользователей социальных сетей – еще одно место для размещения ссылок. Или разнообразные **группы** в этих социальных сетях.

## Распространение материала

Теперь несколько слов о том, как распространить саму информацию, а не ссылки на нее. Целью этого действия является ознакомление с распространяемой информацией как можно большего числа людей. Это основная задача. А есть и вспомогательные, которые нередко становятся основными. Например, создание видимости массовости обсуждения проблемы. Другими словами, когда нужно, чтобы сложилось впечатление, что ЭТО есть везде, что ЭТО обсуждают все и всем ЭТО интересно и важно. Или когда нужно создать «информационный шум», в котором бы «утонула» скрываемая информация и никто на нее не обратил бы внимания…

### *«Посев»*

Словом «посев» в соответствующей среде обозначается мероприятие по массовому распространению в интернете целевой информации. Так сказать, разбрасывание семян по большой площади. Цели описаны чуть выше. А вот технологии есть смысл обсудить отдельно.
В общем-то используются те же приемы, что и при распространении ссылок. Наиболее используемым является создание большого количества **блогов** и распространение заготовки путем публикации ее в этих самых блогах, в комментариях к блогам. Для массовости используются открытые блогохостинги.
Также используются для «посева» и **комментарии к статьям** на порталах, позволяющих комментировать свои материалы. **Форумы** для «посева» используются гораздо активнее, поскольку нет необходимости вставлять ссылки, а значит многие ограничения модераторов не действуют. **Гостевые книги** также используются для распространения, но их эффективность ниже из-за ограниченности аудитории таких гостевых книг.
Зато есть специализированные площадки для публикации материалов – так называемые **сервисы публикаций**. Есть площадки для разовых публикаций, есть для регулярных. Для «посева» подходит и **спам** – e-mail рассылка. Главное помнить об отношении к спаму пользователей и осуществлять ее с «поправкой» на эту особенность.

### *«Авторитетный источник»*

Особой технологией распространения информации является создание «авторитетного источника». Здесь имеется в виду создание источника, информация на котором воспринимается как ценная для пользователей. Понятно, что быстро создать такой источник не получится. Нужно его создавать заранее и поддерживать его «авторитет» до нужного момента, а то и дольше. Это зависит от выбранной стратегии. Фактически это многоходовая комбинация по дезинформированию.
Создание «авторитетного источника» связано с некоторыми особенностями. Первая – это анонимность. Скорее всего, вам будет нежелательно, чтобы тот самый материал, для распространения которого и создавалась площадка, как-то связали с вами. Поэтому лучше изначально делать свои взаимоотношения с таким ресурсом закрытыми от публики. Вторая – это эксклюзивность материала, который будет размещаться. Материал нужен такой, чтобы он «цеплял» людей. Лучше, если этот материал будет уникальным. Но можно и не уникальный, но

организованный так, чтобы пользователям было удобно им пользоваться. По крайней мере, удобнее, чем на других ресурсах.
Кроме этого, ваш «авторитетный источник» нужно сделать авторитетным и у поисковых машин. Причем по той теме, с которой вы планируете впоследствии «работать». Для этого нужно заняться его SEO-оптимизацией. Это всё та же поисковая оптимизация, оптимизация контента и ссылочная масса. А еще – регулярное обновление – размещение новых, интересных материалов и инициированные «кем-то» обсуждения материалов из этого источника в социальных сетях.
Где-то через полгода (если активно продвигать такой источник) он станет достаточно «известен» и его можно будет использовать для основной задачи. Правда, вам будет жаль своих трудов на его «раскрутку», но тут уж ничего не поделаешь. Но при правильном использовании в информационной войне такой источник можно сделать еще более «авторитетным», например, за счет скандалов, которые он освещает, а то и в которых участвует. Обычная технология шоу-бизнеса.

### *«Общение» двух ников*

Еще одна активно используемая технология распространения информации – это имитация общения людей. На форуме, в блоге, в комментариях… Создается два или более аккаунтов и инициируется общение между ними с использованием той самой информации, которую нужно распространить. Конечно же, это не такая массовая акция, как «посев». Это скорее точечный удар, направленный на вполне конкретную группу людей. Но зато такая технология позволяет преодолеть сомнения людей относительно распространяемой информации. Срабатывает эффект «подслушивания». Вроде как общаются посторонние люди, а я «подслушал» их общение. Они же между собой общаются – значит и не собирались меня обманывать…
Кроме того, люди склонны больше доверять людям, а не информационным агентствам и уж тем более официальным заявлениям. Поэтому если распространяемая информация имеет вид общения двух людей, то она с большей вероятностью будет воспринята как истина.

### *Виртуальная личность*

#### Зачем нужны виртуальные личности

Еще один способ распространения информации в интернете – это распространение с помощью виртуальных личностей (виртуалов). Такое распространение может быть разным. Интернет дает огромные возможности для создания нужного антуража. Это относится и к элементам, относящимся к самому виртуалу, так сказать, к его «внешности», характеру, компетенциям, связям, и к элементам окружающей обстановки – внешних условий, сопутствующих моменту воздействия. Сопутствующие высказывания как бы сторонних личностей, новостной или информационный шум, внешний вид сайта, на котором происходит воздействие.
Например, если такой виртуал стал **авторитетным источником** информации для определенной аудитории, то и информация от его имени быстрее «попадет в цель» в этой аудитории. Люди с меньшей осторожностью воспримут эту информацию и с меньшей критичностью.
Или если такой виртуал стал **участником диалога**, то информация им выдаваемая тем проще будет воспринята другими участниками (и не только), чем более человекоподобнее выглядит этот виртуал (помимо прочего, конечно).
Или если такой виртуал обладает определенными характеристиками, которые делают объект воздействия более «податливым». Например, «связи» виртуала – видимость взаимодействия с некими принципиально важными людьми. Или участие в каких-то событиях, или еще что-то.

#### Как создаются виртуальные личности

Что такое виртуальная личность? По сути (в самом минимальном виде) – это один аккаунт на какой-то площадке в интернете. Но аккаунт, от имени которого можно оставить сообщение. Это может быть блог, аккаунт в соцсети, аккаунт на форуме… Это самый простой вариант. Но даже этот простой вариант требует дополнительных действий. В зависимости от задач, для решения которых создан виртуал, требуется и определенная проработка нюансов этого виртуала.

Виртуал – это, по аналогии, агент влияния с соответствующей легендой. И вот эту самую легенду ему нужно создать. Создать и саму виртуальную личность (внешность, связи, характер) и легенду – ее прошлое. Применительно к виртуалу даже не знаю, где проходит граница между созданием самой виртуальной личности и ее легенды. Но оставлю это на долю желающих потеоритизировать.

*Общее*

Виртуальной личности тем больше поверят, чем более человекоподобным выглядит виртуал. Например, нужно заполнить профайл виртуала в блоге или форуме, или в соцсети. Профайл того самого аккаунта, от имени которого будет осуществляться воздействие. Нужна «человечная» фотография (человечная в рамках предназначения виртуала). Нужно заполнить хотя бы часть полей профайла (интересы, подпись и т.п). Например, если виртуал должен спровоцировать последующее общение вне данной площадки, то нужен какой-то контакт в личных данных этого виртуала. А если виртуал предназначен для воздействия на мужчину, то можно попробовать это от имени виртуала в женском «облике».

*Специальное*

Для совсем простых задач, обычно, но не всегда, достаточно недавно созданного аккаунта на соответствующей площадке. Однако простые задачи бывают редко. Чаще нужно тщательно прорабатывать личность виртуала, чтобы объект воспринял его как надо, а при проверке виртуала убедился в том, что ему виртуал преподносил. Для этого нужно, помимо профайла, создать соответствующее «окружение» виртуала. К такому окружению может относиться и аккаунт в социальной сети или в нескольких, и дополнительный блог, и сообщения на профильных форумах, и «друзья». Такая проработка легенды требует определенных ресурсов, в основном времени.

Гораздо сложнее в ситуации, когда нужно создать достаточно старые «следы» виртуала. Например, его высказывания год или два назад. Такая потребность пока бывает редко, но уже бывает. А со временем, когда виртуальная образованность людей повысится, станет необходимостью. Для таких ситуаций нужно создавать виртуалов впрок и поддерживать видимость их жизнедеятельности.

Интернет дает возможность создавать виртуальные личности неограниченное число раз. И злоумышленник может сделать видимость, что материал распространяют или обсуждают сотни, а то и тысячи людей. Собственно, так и создается видимость массовости в интернете.

## Список использованной литературы

Антонов А.В. Системный анализ – Высшая школа 2004

Бабец О.А. Опыт военной разведки на службе в коммерческой фирме – Харвест 2003

Барбара Минто Золотые правила Гарварда и mckinsey. Правила магической пирамиды для делового письма - Росмэн-Пресс 2004

Баяндин Н.И. Технологии безопасности бизнеса – Юрист 2002

Белановский С. А. Глубокое интервью. - Никколо-Медиа 2001

Белановский С. А. Методика и техника фокусированного интервью – Наука 1993

Бернейс Э. Пропаганда - Москва 2011

Блум Уильям Убийство демократии. Операции ЦРУ и Пентагона в период холодной войны – Кучково поле 2013

Большаков М.И. Информационно-психологическое обеспечение военной операции НАТО против Югославии - Сборник ГУ ГШ ВС РФ. - 1999

Волкова В.Н. Козлов В.Н. Системный анализ и принятие решений – Высшая школа 2004

Воронов Ю.П. Конкурентная разведка Учебное пособие - Москва 2007

Гаврюшин Е.И. Линдер И.Б. Хрестоматия. Практическая аналитика в службах безопасности – ICTTA 2006
Гарифуллин Р.Р. Психология блефа, манипуляций, иллюзий – АСТ 2007
Гершензон В.Е. Глобальные технологии и информационная безопасность - Информационная безопасность. 2011. № 4
Глазунов О. Китайская разведка – Алгоритм 2008
Гордукалова Г.Ф. Анализ информации: методы, технологии, организация – Профессия 2009
Губанов Д. А., Калашников А. О., Новиков Д. А. Теоретико-игровые модели информационного противоборства в социальных сетях - Управление большими системами. 2010. № 3
Даллес А. Искусство разведки - Международные отношения 1992
Данилов Н. Новые формы психологического воздействия - Информационный сборник ГУ ГШ ВС РФ. 1994. № 5
Деревицкий А. Коммерческая разведка – Питер 2006
Доблаев Л. П. Логико-психологический анализ текста - Саратов 1971
Добротворский И.Л. Искусство войны в бизнесе: стратегия и тактика – Дело и сервис 2003
Доронин А.И. Бизнес-разведка – Ось-89 2003
Доронин А.И. Основы экономической разведки и контрразведки - Тула 2000
Доронин А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия – Тула 2000
Дридзе Т.М. Текстовая деятельность в структуре социальной коммуникации - Наука 1984
Дрогобыцкий И.Н. Системный анализ в экономике – Финансы и статистика 2007
Дудихин В.В. Конкурентная разведка в Интернет – советы аналитика – ДМК 2002
Духов В.Е. Экономическая разведка и безопасность бизнеса - НВФ Студцентр 1997
Зайцов А.А. Служба генерального штаба – Куликово поле 2003
Звонарев К.К. Агентурная разведка - БДЦ-пресс 2003
Зданович А.А. Отечественная контрразведка 1914-1920 - Крафт+ 2004
Землянов В.М. Своя контрразведка - Харвест 2002
Землянов В.М. Агентура в разведке и контрразведке – Харвест 2007
Землянов В.М. Основы сыскного ремесла – Харвест 2004
Зукулис Р.Я. Организация и ведение психологических операций странами-участниками НАТО в ходе военной кампании в Косово - Информационно-аналитический сборник. Екатеринбург. 1999. № 3
Ивахин А.Е., Прыгунов П.Я. Оперативная деятельность и вопросы конспирации в работе спецслужб – Киев КНТ 2008
Канн Д. Война кодов и шрифтов – Рипол 2004
Касперски Крис Секретное оружие социальной инженерии – 2008
Каценеленбаум Б. «Демагогия: опыт классификации»
Кириллов В.И., Старченко А.А. Логика - Юрист 1996
Кара-Мурза С.Г. Манипуляция сознанием - Алгоритм 2005
Ковалев Е. М., Штейнберг И. Е. Качественные методы в полевых социологичсеких исследованиях – Логос 1999

Козлов С.Б. Иванов Е.В. Предпринимательство и безопасность - Универсум 1991
Колпаков А.И. Все о внешней разведке – Олимп 2002
Корж П.А. Негосударственная безопасность – Феникс 2002
Кузин А.В., Нежданов И.Ю., Ющук Е.Л. Дезинформация и активные мероприятия в бизнесе – Казань 2009
Куликов Е.М. Искусственно созданные слухи: социологическое обеспечение контроля и управления «информационным вирусом» в сети Интернет - Историческая и социально-образовательная мысль. – 2011 – № 4
Лабоцкий В.В. Управление знаниями – Современная школа 2006
Лайнбарджер П. Психологическая война - Москва 1962
Ландэ Д.В. Поиск знаний в Интернет – Диалектика 2005
Лебон Г. Психология толпы - Мнение и толпа - Москва 1998
Лемке Г.Э. Нелинейный стратегический менеджмент или искусство конкуренции – Дело и сервис 2006
Лемке Г.Э. Конкурентная война. Нелинейные методы и стратегии – Ось 89 2007
Лемке Г.Э. Секреты коммерческой разведки – Ось 89 2008
Матанцев А.Н. Стратегия, тактика и практика маркетинга – Юрист 2002
Мелтон Х.К. Офисный шпионаж – Феникс 2005
Мироничев С. Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы борьбы с ним - «Дружок» 1995
Минто Барбара "Золотые правила Гарварда и mckinsey. Правила магической пирамиды для делового письма" - Росмэн-Пресс 2004
Митник Кевин Искусство обмана - Айти 2004
Митник Кевин Искусство вторжения - Айти 2004
Михайлов Б. И. Психологические операции ВС США в конфликтах малой интенсивности - Зарубежное военное обозрение. 1996. № 8
Михеев А.Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности - Современные глобальные проблемы мировой политики: Учеб. пособие для студентов вузов / Под ред. М.М. Лебедевой. – М.: Аспект Пресс, 2009
Мелисс Клеммонс Румизен Управление знаниями – АСТ 2004
Мухин А.А. Информационная война в России – Москва 2000
Най Дж. «Мягкая сила» и американо-европейские отношения - Свободная мысль-XXI. 2004. № 10
Наумов В.В. Лингвистическая идентификация личности – комкнига 2006
Нежданов И.Ю. «Аналитическая разведка»
Нежданов И.Ю. «Технологии разведки для бизнеса»
Одинцов А.А. Экономическая и информационная безопасность – Экзамен 2005
Остапенко П.В. Тайная война в древнем мире –Харвест2004
Парад Б. Коммерческий шпионаж – Проспект 2005
Пашенцев Е.Н. Стратегическая коммуникация США: «Имперское перенапряжение сил» - Мир и политика. 2012. № 8
Петров М.Н. Механизмы государственных переворотов – Харвест 2005
Прескотт Д.Е., Миллер С.Х. Конкурентная разведка уроки из окопов - Альпина-паблишер 2003
Поповская Л.В. Лингвистический анализ художественного текста в вузе – Феникс 2006
Почепцов Г.Г. Теория коммуникаций – Релф-бук 2001

Почепцов Г.Г. Стратегический анализ – Дзвин 2004
Почепцов Г.Г. Революция.com – Основы протестной инженерии – Европа 2005
Почепцов Г. Г. Информационные войны. — Рефл-бук
Почепцов Г. Г. Психологические войны. — Рефл-бук
Райс Э. Траут Д. Маркетинговые войны – Питер 2000
Ромачев Нежданов Конкурентная разведка – Ось-89 2007
Ронин Р. Своя разведка - Харвест 1999
Ронин Р. Это тонкое дело – разведка - Гинлайт 2008
Рубин Ю.Б. Теория и практика предпринимательской конкуренции – Маркет ДС 2007
Рушайло В.Б. Основы оперативно-розыскной деятельности – Лань 2000
Садердинов А.А. Информационная безопасность предприятия – Дашков и К 2004
Сойма В.М. Советская контрразведка в годы Великой Отечественной войны - Крафт 2005
Соклакова Н.А. Криминалистическое исследование материалов документов – Питер 2005
Соловьев А.В. Информационная война: понятие, содержание, перспектива - Пространство и время. 2010. № 2
Судоплатов А.П. Безопасность предпринимательской деятельности – Олма пресс 2001
Таганов Д.Н. Информация как основной фактор формирования конкурентной стратегии – Менеджмент в России и за рубежом 2005 №1
Тарас А.С. Своя контрразведка – Харвест 2002
Тарас А.С. Спутник разведчика и партизана – Харвест 2005
Тарас А.С. Методы и приемы психологической войны – Харвест 2006
Тарас А.С. Секреты психологической войны – Харвест 1999
Тарас А.С. Подготовка разведчика – Харвест 2000
Тарас А.С. Телохранитель – Харвест 2000
Тарас А.С. Управление войсками – Харвест 2006
Тарасов В.К Искусство управленческой борьбы – Добрая книга 2003
Токарев Б.Е. Методы сбора и использования маркетинговой информации – Юрист 2001
Федотова Л.Н. Контент-аналитические исследования средств массовой информации и пропаганды - Изд-во Моск. Ун-та 1988
Фляйшер К. Бенсуссан Б. Стратегический и конкурентный анализ – Бином 2005
Халяпин Д.Б. Основы защиты информации – Москва 1994
Хлобустов О. Госбезопасность от Александра 1 до Путина Яуза 2005
Шалак В.И. Современный контент-анализ – Омега 2004
Шиян А.А. Руководство по социальным технологиям – Украина 2001
Черчилль К.А. Маркетинговые исследования – Питер 2003
Чуфаровский Ю.В. Психология оперативно-розыскной деятельности
Ющук Е.Л. Конкурентная разведка – маркетинг рисков и возможностей – Вершина 2006
Ющук Е.Л. Интернет-разведка руководство к действию – Вершина 2007
Ющук Е.Л. Блог. Создать и раскрутирть – Вершина 2007
Ющук Е.Л. и Кузин А.В. Противодействие черному PR в Интернете – Вершина 2008

Ядов В. А. Стратегия социологического исследования - Москва 2000
Яковец Е.Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел – Издательский дом Шумиловой 2005
Ярославский В. Военные методы в бизнесе. Тактика – Крылов 2003
Ярочкин В.И. Бузанова Я.В. Системы защиты предпринимательства Мир 2005
Ярочкин В.И. Бузанова Я.В. Корпоративная разведка – Ось89 2005
Ярочкин В.И. Безопасность банковских систем – Ось-89 2004
Яскевич В.И. Секьюрити – организационные основы безопасности фирмы – Ось-89 2005