Центр стратегических оценок и прогнозов

www.csef.ru

Расторгуев С.П., Литвиненко М.В.

Серия «Новая стратегия»

# Информационные операции в сети Интернет

Под общей редакцией
доктора военных наук,
профессора,
генерал-лейтенанта
Михайловского А.Б.

Москва. 2014

**Расторгуев С.П.**, д.т.н., профессор, действительный член Академии криптографии РФ. Известен по работам в различных научных областях. *В программировании* «Искусство защиты и раздевания программ» (1991); *в информационном противоборстве*: «Информационная война» (1997), «Философия информационной войны» (2001), «Информационная война. Проблемы и модели» (2006); *в философии и теории управления*: «Цель как криптограмма. Криптоанализ синтетической цели» (1996), «Управление Вселенной» (2006), «Воспоминания о душе» (2009). Им написано более 5 учебных пособий по дисциплинам информационной безопасности. Всего более сотни публикаций и интервью в прессе и на телевидении.

**Литвиненко М.В.**, д.пед.н., к.т.н., действительный член Академии военных наук. Один из самых молодых докторов наук России. Ученая степень доктора педагогических наук была присвоена в 31 год. Ведущий специалист в области дистанционного образования. Имеет несколько монографий по педагогике. Научные интересы последних лет нашли отражение в книге «Аватаризация» (2011).

# Информационные операции в сети Интернет

В работе предложен и обоснован подход к построению систем выявления информационных угроз. Даны базовые определения и проведено исследование специальных действий, присущих информационным операциям в сети Интернет. Показано, что производство практически всех компонент информационной операции уже поставлено на промышленную основу: от вирусов, нацеленных на автоматизированные объекты военного и промышленного назначения, до генераторов сообщений в виде текстов, голосовых сообщений по заданной голосовой характеристике или видеосюжетов по заданной исходной «картинке». В работе описан механизм, позволяющий частично автоматизировать планирование информационной операции за счет использования типовых схем их проведения, показано, каким образом возможна организация игрового тренинга по моделированию проведения информационных операций.

ISBN 978-5-906661-05-0

Книга предназначена для военных экспертов, специалистов, работающих в сфере информационно-психологического воздействия. Также будет интересна и широкому кругу читателей, интересующемуся вопросами развития кибернетических систем и сетевых технологий.

Центр стратегических оценок и прогнозов

Расторгуев С.П., Литвиненко М.В.

# Информационные операции в сети Интернет

*Под общей редакцией доктора военных наук,*
*профессора генерал-лейтенанта*
*Михайловского А.Б.*

Москва
2014

УДК355.01:519.7
ББК 68+22.1в
Р24

## Серия «Новая стратегия». Книга 3

Расторгуев С.П., Литвиненко М.В.

Р24 **Информационные операции в сети Интернет** / Под общ. ред.А.Б. Михайловского. — М.: АНО ЦСОиП, 2014. — 128 с. (— Новая стратегия, 3)

**ISBN 978–5–906661–05–0**

В работе предложен и обоснован подход к построению систем выявления информационных угроз. Даны базовые определения и проведено исследование специальных действий, присущих информационным операциям в сети Интернет. Показано, что производство практически всех компонент информационной операции уже поставлено на промышленную основу: от вирусов, нацеленных на автоматизированные объекты военного и промышленного назначения, до генераторов сообщений в виде текстов, голосовых сообщений по заданной голосовой характеристике или видеосюжетов по заданной исходной «картинке». В книге описан механизм, позволяющий частично автоматизировать планирование информационной операции за счет использования типовых схем их проведения, показано, каким образом возможна организация игрового тренинга по моделированию проведения информационных операций.

Книга предназначена для военных экспертов, специалистов, работающих в сфере информационно-психологического воздействия. Также будет интересна широкому кругу читателей, интересующихся вопросами развития кибернетических систем и сетевых технологий.


**ISBN 978–5–906661–05–0**

# СОДЕРЖАНИЕ

# Введение

В условиях широкого распространения СМИ нового типа — сайты, форумы, блоги, социальные сети и т.п. — основная борьба за право адекватного отображения действительности перемещается в Интернет. Новые формы представления и распространения информации создаются чуть ли не в режиме реального времени, и в их «раскручивание» вкладываются значительные средства. Если еще в прошлом веке при вооруженной агрессии степень охвата аудитории страны с целью перепрограммирования была среди малозначимых параметров, то сегодня, после внедрения в промышленно развитых странах т.н. демократической формы правления, повышение степени охвата — это значимый параметр при условии грамотного оформления подаваемого материала.

Перепрограммировать население, а самое главное, исполнительные и законодательные структуры противника — это значит, победить его. Перепрограммирование требует соответствующих ресурсов, и главный ресурс — время. Охватить, как можно шире, аудиторию в сжатые сроки становится возможным при максимальной автоматизации всего процесса: от промышленной генерации материала СМИ до автоматической доставки, размещения на заданном множестве ресурсов. Чем позже жертва выявит факт ведения информационной операции и поставит заслон, тем больше шансов на успех. С другой стороны, чем раньше выявлен факт ведения информационной операции[1] противником, тем меньше ресурсов требуется для ее локализации и ликвидации. При этом сам процесс локализации и ликвидации требует проведения корректирующих действий, т.е. ответной информационной операции. В этой связи, важной становится

[1] Информационная операция — совокупность взаимосвязанных действий информационного характера, направленных на решение поставленной задачи по перепрограммированию, блокированию, генерации информационных процессов как в технической, так и в гуманитарной сферах.

любая автоматизация, как в части раннего выявления информационных угроз, так и при формировании плана проведения ответной информационной операции.

Известно, что общее время на ликвидацию информационных угроз складывается из трех составляющих:

- времени на выявление угрозы;
- времени на разработку и утверждение плана действий по локализации и ликвидации угрозы;
- времени на реализацию утвержденного плана.

Сокращение общего времени способствует повышению эффективности в целом всей системы информационной безопасности любого государства или крупной организации.

Проведенный анализ научных работ и существующих в мире технических средств и технологий, направленных на выявление угроз и проектирование информационных операций в сети Интернет, показал следующее.

В данной области по имеющейся информации более активно, чем другие, работают в основном США и Израиль.

Причем Израиль известен как в области специальных вирусоподобных средств для скрытого управления промышленными объектами, так и в разработке и проведении информационных сетевых операций поддержки собственных действий. По утверждению СМИ, для этого есть все необходимые структуры: «В Израиле задачи по планированию и реализации мероприятий по нарушению функционирования объектов информационной и телекоммуникационной инфраструктуры зарубежных государств возложены на разведывательное управление и управление связи и компьютерных систем генерального штаба национальных вооруженных сил… Израильтяне считают, что отсутствие международных правовых механизмов, ограничивающих использование программно-аппаратных средств для поражения компьютерных систем, позволяет применять их без согласования с международными организациями и иностранными государствами»[2].

Основной упор в части выявления угроз в спецслужбах и министерстве обороны США отводится сбору данных и их интеллекту-

[2] См.: http://interaffairs.ru/read.php?item=454.

альному анализу. Важнейшим критерием является объем собранной информации. Для решения данной задачи технические службы используют не только специальные технические средства и технологии, типа системы «Эшелон», но и возможности ведущих мировых корпораций, в том числе таких как Майкрософт и Гугл, программное обеспечение которых представлено практически в каждом компьютере, имеющем выход в Интернет. Так, в августе 2013 года были опубликованы секретные документы о слежке американских спецслужб в Интернете, полученные от Эдварда Сноудена. Из них следует, что у Великобритании есть разведбаза на Ближнем Востоке, перехватывающая интернет-трафик и телефонные звонки всего региона. В числе гигантов Всемирной паутины, сотрудничающих со спецслужбами, были названы Google, Yahoo, Microsoft, Facebook, AOL, Skype, YouTube, Apple и PalTalk (некоторые из них позже заявили, что извлечение данных происходит без их ведома). Из опубликованных документов следует, что Google, Yahoo, Microsoft и Facebook получали из специального фонда АНБ деньги на сертификацию, необходимую для сотрудничества с агентством[3].

Для широкомасштабного анализа собранной информации используются современные «интеллектуальные» продукты (технологии Data Mining) с удобной формой отображения результатов анализа.

В настоящее время другим странам идти путем США не представляется возможным в силу отсутствия широко распространенных в сети собственных контролируемых подобных продуктов и стоящих за ними промышленных гигантов. В этом случае решение проблемы — это не широкомасштабный сбор и анализ, а целенаправленный поиск и анализ, исходя из требований и ограничений поставленной задачи.

Подобный подход может быть эффективным по критерию результат/затраты, благодаря тому, что проблема проектирования информационных операций, судя по информационным операциям, проводимым США в последние годы, сведена специалистами США к выработке всего нескольких типовых сценариев, которые и реализуются с небольшими модификациями.

---

[3] См.: http://news.mail.ru/politics/14460882/?frommail=1.

Сама по себе разработка системы выявления информационных угроз и поддержки формирования задания на проведение информационной операции является новой. В открытых публикациях научных результатов по проблеме в целом нет. Более того, до сих пор остается нерешенной проблема формирования перечня типовых задач, решаемых на современном этапе с помощью проведения информационных операций. Разработка подобного класса систем невозможна без предварительного исследования и создания терминологического, технологического и алгоритмического обеспечения. Поэтому в данной работе мы формулируем только те результаты, которые подкреплены опытом проектной реализации.

Информационное противоборство (ИП), являясь составной частью общего противоборства, имеет свои специфические события, знания о которых позволяют судить о ведении ИП. В общем случае проблема выявления факта начала информационной войны (информационной операции) относится к алгоритмически неразрешимым проблемам, но на определенном этапе развития информационной операции появляются признаки, позволяющие получать вероятностные оценки факта ее проведения.

Основным признаком является повторение близких по смыслу новостей и комментариев новостей, выполненных в соответствующем контексте. При этом совершенно неважно, соответствуют ли эти новости происходящим в эмпирическом мире событиям. Более того, чем меньше похожести, тем больше вероятность того, что новости являются частью спланированной операции. В условиях обусловленного текущим развитием общества частичного замещения эмпирического мира виртуальным в сознании зрителей, навязывание им соответствующих тем через повторение способствует вытеснению возможности разумной, основанной на логике и здравом смысле, оценки сообщения. Здесь временной фактор значит много. Для того чтобы разобраться, где правда, а где ложь, нужно время. И если оно упущено, то проблема становится гораздо сложнее, а иногда она уже и не имеет решения. Так, например, Грузия, несмотря на полный военный провал, выиграла информационную войну против России 08.08.2008. Непризнание миром Абхазии и Южной Осетии — очень показательный результат. Так реализуются угрозы нового класса — информационные угрозы.

Принципиальное отличие информационной угрозы в следующем. Если формирование классической угрозы предполагает сокрытие составляющих ее компонент среди естественного «шума» окружающей среды, то в случае информационной угрозы речь идет о сокрытии истинности или ложности факта, который активно подается в СМИ и раскручивается в комментариях. Например, «разработка Ираком оружия массового поражения», «применение химического оружия в Сирии» или «регулярное нарушение самолетами РФ воздушного пространства зарубежных стран».

В этой связи представляет научный интерес проблема формирования обоснованного перечня новостных тематик, предшествующих вооруженному конфликту, и разработка вероятностных критериев оценки факта начала ведения информационной операции. Существующие объемы материала (вооруженные конфликты в Ираке, Ливии и др.) позволяют сегодня приступить к решению данной проблемы.

Отдельные научные положения и алгоритмы в части создания технологической и алгоритмической составляющей подсистемы проектирования поведенческих схем, используя типовые библиотеки, на базе принципа оптимальности Беллмана (правил, алгоритмов, таблиц, схем и пр.) разработаны в робототехнике, а также заявлены теорией рефлексивного управления. Однако приложение существующих научных положений применительно к проектированию конкретных схем для управления поведением социальных субъектов, а тем более, для проектирования оригинальной информационной операции до сих относится к серьезным научным задачам. В данной работе мы попытались дать общую формальную постановку этой задачи.

# ГЛАВА 1

# Интернет как поле информационного противоборства

Любая война начинается с определенной последовательности действий со стороны противника. Действия, будучи для любого внешнего наблюдателя событиями, находят отражение в новостях, которые черпаются как из открытых источников информации, так и добываются с помощью специальных технических средств и технологий, а также агентурным путем. Комплексный анализ всех полученных данных позволяет сделать выводы о наличии или отсутствии потенциальных угроз.

Так, например, предвоенный месяц Великой Отечественной войны, несмотря на взаимную риторику политиков и государственных деятелей о дружбе и сотрудничестве, сопровождался резким возрастанием нарушений со стороны Германии воздушного пространства СССР. При грамотно поставленной аналитической работе информация об этих событиях сама по себе была достаточна для определения даты начала войны. Ибо нарушения воздушного пространства вторичны — они результат уже исполняющегося плана по подготовке вторжения. Цель — разведка приграничной территории. И сообщения о нарушениях (времени и месте) позволяют сформировать картину о законченности подготовки к началу войны. В то время Интернета не было, поэтому выявление данной угрозы осталось на уровне субъективной точки зрения отдельных военных аналитиков, которые не смогли убедительно обосновать и довести свою точку зрения до руководства страны.

Однако приведенный пример больше относится к решению разведывательных задач с помощью информационного пространства. При проведении классической информационной операции события не прячут. Их, наоборот, придумывают и активно распространяют (поджог

Рейхстага, расстрел мирной демонстрации, зверства над детьми и инвалидами и т.п.). При этом цель другая — не разведать территорию противника (считается, что эта задача уже решена), а перепрограммировать живую силу противника в возможно короткие сроки. Именно поэтому надо четко различать задачи по выявлению угроз эмпирического мира, нашедших свое отражение в сети, и задач по выявлению разворачивающихся информационных операций. Но при этом надо понимать, что появление именно информационной операции соответствующей направленности — это сигнал, говорящий о том, что где-то рядом начинает формироваться военная угроза.

Прежде чем перейти к исследованию сети Интернет как источника информации о вызревающих угрозах и поля информационного противоборства, рассмотрим обобщенную модель перепрограммирования, основанную на таких параметрах, как:

- частота подачи материала, относящегося к заданной теме;
- значимость источника;
- охват населения.

Именно эти параметры являются значимыми для выявления информационных операций. Критерием победы и достижения цели считается отсутствие в СМИ, особенно в официальных СМИ, противоположной точки зрения. Если подобное происходит, но задача по свержению того или иного правительства или президента не решена, то тогда открывается зеленая улица для военного вторжения. Именно поэтому для «слабого» в военном отношении соперника важно уметь грамотно вести информационное противоборство. И если не выигрывать, то хотя бы создавать условия для затягивания информационной операции — выигрыш времени важен для мобилизации собственных сил.

## 1.1. Задачи, решаемые в телекоммуникационных средах с помощью информационных операций

В рамках противоборства в информационном пространстве без перехода к горячей фазе конфликтующими сторонами могут решаться следующие два класса задач:

1. Выявление угроз. Фильтрация и анализ содержимого заданного множества сайтов, интегрирование результатов и выработка управленческой стратегии.
2. Проведение информационных операций.

Информационные операции, на примере материалов сети Интернет, включают в себя:

- уничтожение реальных объектов и инфраструктуры, например, с помощью компьютерных вирусов и закладок. Характерным примером вирусов нового поколения для решения подобного класса задач является Stuxnet, который чем-то похож на высокоточное оружие — находит промышленные системы управления соответствующего изготовителя и берет над ними контроль, по команде из Центра способен заблокировать работу промышленного объекта, а то и уничтожить объект, скрытно управляя им;
- уничтожение, блокирование, дискредитация интернет-ресурсов. Одной из самых популярных атак для решения подобных задач являются DDoS-атаки. Так, в новостях Google только за одни сутки, например, за 12 августа 2013 года было 35 сообщений по этой теме. Большинство сообщений похожи друг на друга, типа:

«Сегодня в 16:00 МСК на все наши сервера начали поступать DDoS-запросы GET и POST на большое число сайтов всех клиентов. Запросы направлены на панель администратора CMS Joomla (POST /administrator/index.php) и форму авторизации Wordpress (POST/wp-login.php).

Сотрудниками техподдержки составлены списки блокировки IP-адресов, а также списки стран для временной блокировки доступа. На данный момент насчитано более 12 000 атакующих IP из 10 стран. По всей видимости, атака носит глобальный характер и направлена именно на указанные CMS»[4];

- создание, раскручивание, рекламирование, навязывание интернет-ресурсов. Под термином «раскручивание» (продвижение) ресурса понимается комплекс мероприятий, направленных на поддержку и рост позиций ресурса в поисковых системах сети Интернет, увеличение целевой посещаемости ресурса, создание благо-

[4] См.: www.steadyhost.ru/joomla_wordpress_ddos.htm.

приятного имиджа и узнаваемости в Интернете. Раскрутка ресурса становится возможной благодаря наличию в Интернет таких сервисов, как поисковые системы, которыми регулярно пользуются практически все посетители сети. Поисковые системы собирают данные по ключевым словам и словосочетанием вместе со ссылками на ресурсы, где эти ключевые слова находятся. Объем выдачи поисковой системы в зависимости от запроса пользователя может изменяться в очень широких пределах, как полное отсутствие выдачи, так и тысячи ссылок, которые невозможно просмотреть в разумное время. Считается, что ресурс хорошо раскручен, если по основным терминам, отражающим суть данного ресурса, поисковые системы помещают ссылку в Топ-10 найденных ссылок. Тема раскручивания сайтов одна из самых популярных в Интернете. Запрос на словосочетание «раскручивание сайтов» дает в Google более 1 330 000 результатов (интернет-страниц). Многие из этих страниц содержат предложения по реализации данной услуги;

- приведение к власти представителей определенных кругов, конкретных лиц. Актуальность объясняется взятием на вооружение сервисов Интернета для обоснования причин интервенции. Например, в случае с Ливией: «Война начиналась как чисто театральная постановка. Впервые была использована во всю мощь агитационная машина нового формата: Интернет и спутниковое телевидение. Впервые были построены масштабные декорации, копировавшие отдельные районы некоторых ливийских городов, в том числе — Триполи. Именно телевидение и Интернет нанесли первые удары. Формальным поводом для «народных» волнений стал арест правозащитника Фатхи Тербиля, которого быстро отпустили. Это случилось 15 февраля, а уже 17 февраля прошел «День гнева» с массовыми выступлениями в городах Бенгази, Бевида, Зентан, Ружбан и Дерна. Массовость их, будто бы, обеспечили социальные сети. По телевидению с утра до вечера гоняли очень мутные картинки, на которых были видны, в основном, ноги куда-то бегущих толп людей. Все это сопровождалось истерич-

ными выкриками женщин и мужчин на тему о «страшных зверствах палачей Каддафи»[5];

- снижение уровня напряженности в заданном регионе/повышение уровня напряженности в заданном регионе. Например, фильм «Невинность мусульман», распространенный на определенные регионы через сеть Интернет, вызвал резкое повышение экстремистской активности. Так, в Египте разъяренная толпа ворвалась на территорию посольства США в Каире и сорвала американский флаг. В результате вооруженного нападения на американское диппредставительство в Бенгази погиб посол США в Ливии и еще трое американцев, в том числе двое морских пехотинцев[6];
- формирование общественного мнения на заданных интернет-ресурсах. В частности, подготовка общественного мнения для принятия противником законодательных актов ущербного для противника характера. Актуальность этой задачи именно для пространства Интернета следует еще и из того, что сегодня обсуждение наиболее значимых законопроектов в сети становится все более популярной мерой, цель которой — легитимировать принимаемые законы в глазах населения. Так, 23 августа 2012 г. Д.А. Медведев утвердил Концепцию формирования механизма публичного представления предложений граждан Российской Федерации с использованием информационно-телекоммуникационной сети «Интернет» для рассмотрения в Правительстве Российской Федерации предложений, получивших поддержку не менее 100 тыс. граждан Российской Федерации в течение одного года. Близкие по духу законы, позволяющие учитывать общественное мнение посетителей ресурсов Интернет, уже давно действуют в зарубежных странах;
- формирование имиджа (положительного/отрицательного) посредством целенаправленной коммуникационной политики. В частности, повышение/понижение статуса определенной страны/организации/человека и др. Характерный пример, который на слуху в связи с выборами мэра в Москве 2013 года, — борьба некоего Н с партией «Единая Россия». Борьба, в основном, шла через Интернет и, именно

[5] См.: www.centrasia.ru/newsA.php?st=1315208040.
[6] См.: www.vesti.ru/doc.html?id=904758.

благодаря Интернету ему удалось причинить серьезный ущерб имиджу партии путем высмеивания. Высмеивание иногда действует гораздо сильнее, чем открытые уголовные дела. Считается, что Н организовал сайт с доменным именем **партия-жуликов-и-воров.рф**.

Подобное делается довольно просто: регистрируется имя, приобретается хостинг для размещения, после чего созданный сайт транслирует через себя официальный сайт партии, но прилепив ему соответствующее издевательское название.

Так же просто и защититься от подобных операций. И не только защититься, но и подсунуть противнику нечто, его самого позорящее. Важно только вовремя выявить эти операции. В данном случае руководство «Единой России» не придало значения атаке, не защитило себя, и в результате процесс волной прокатился по всему Интернету, вызвав лавину насмешек и серьезно изменив отношение нейтральных пользователей к данной теме.

На сегодняшний день проблема полноты задач информационного противоборства для телекоммуникационного пространства остается открытой. Классификация задач, решаемых в сети Интернет с помощью проведения информационных операций, требует своего дальнейшего исследования.

Конструирование информационной операции осуществляется специалистом, используя наработанную исторической практикой базу готовых шаблонов и допустимые связи от целей к подцелям, задачам, объектам воздействия, информационным материалам, способам воздействия и собственным силам и средствам. Кроме знаний и понимания, что и как делать, специалисту нужны инструментальные средства и технологии. Подобные инструментальные средства и технологии принято относить к информационному оружию.

## 1.2. Классификация информационного оружия

Понятие «информационное оружие» имеет не один десяток определений, многие из которых базируются на особенностях среды применения оружия, объектов воздействия и глобальности или локальности его

применения. Не вдаваясь в дебаты о строгости существующих определений информационного оружия, приведем классификацию технических средств, относимых к информационному оружию, применительно к организации информационной операции в среде Интернет.

Постараемся провести такую классификацию, которая бы обладала определенной полнотой по охвату всего спектра возможных информационных воздействий в среде Интернет. Наличие полноты позволит нам в дальнейшем проводить сравнительные оценки и определять наиболее приоритетные классы технических средств, способных помогать специалисту решать соответствующие задачи.

При этом в условиях дефицита специалистов, в первую очередь разработчиков, целесообразно классифицировать технические средства таким образом, чтобы максимально полно использовать наработанные специалистами изделия и технологии в пределах каждого класса.

Информационное оружие представляет собой технические средства и технологии, целенаправленно применяемые для активизации, уничтожения, блокирования или создания в информационной системе процессов, в которых заинтересован субъект, применяющий оружие.

Существует классический подход применения любого оружия в боевых действиях: постановка задачи, разведка, планирование, проведение операции, оценка результативности. Причем процесс охвачен обратными связями и не всегда завершается, как запланировано. На разных этапах этого процесса возможно применение различных инструментальных средств и технологий. Наша задача при ведении классификации заключается в том, чтобы охватить все множество воздействий, где возможна хоть какая-то автоматизация, при этом объединить те технические средства и технологии, для которых допустим единый подход в части формирования знаний и умений разработчиков. С одной стороны — охватить всё, с другой — минимизировать собственные ресурсы.

Анализ существующего информационного оружия в сфере Интернет показал, что это оружие развивается по следующим основным направлениям, в рамках которых оно и применяется:

- разведка;
- проведение специальных операций;
- планирование информационных операций, управление про-

цессом их проведения и оценка результативности.

Каждое направление в силу специфики применяемых средств и технологий требует своих специалистов/разработчиков.

При этом важно, что объектами информационного воздействия по каждому направлению могут быть как ресурсы сети (сайты, локальные компьютеры), так и посетители сети, что тоже требует разной подготовки разработчиков в части знания объекта воздействия. Таким образом, мы приходим к следующей классификационной схеме (рис. 1.2.1).

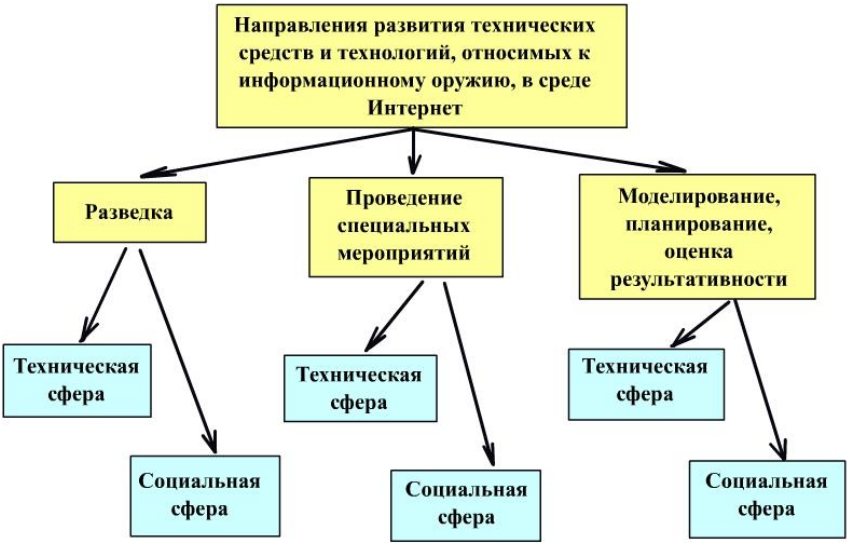



РИСУНОК 1.2.1. *Классификация информационного оружия*

Информационное оружие целесообразно разделить на шесть классов.

В части разработки технических средств и технологий для ведения разведывательной деятельности:

**Класс №1.** Средства разведки и мониторинга состояния ресурсов Сети. Здесь речь идет о разработке технических средств для мониторинга сетевых ресурсов с целью:

- выявления фактов появления новых тем (подобное довольно часто связано с началом информационной операции);

- выявления фактов появления новых ресурсов заданной направленности;
- выявления связей между ресурсами;
- выявления отношений предпочтения ресурсов;
- проведения онлайн-опросов посетителей заданных ресурсов по заданной теме.

**Класс №2.** Средства разведки и мониторинга деятельности посетителей Сети. Речь идет о разработке технических средств для изучения поведения посетителей сети путем сбора данных об IP-адресах и программном обеспечении компьютеров, зафиксированных на разных ресурсах Сети. Удачное решение данной задачи и, в случае наличия знания о провайдерах государственных или политических структур, представляющих интерес, позволит строить поведенческие интернет-портреты пользователей заданной организации, а порой и конкретных людей.

В части разработки технических средств и технологий для проведения специальных мероприятий.

**Класс №3.** Средства активного воздействия на ресурсы сети, включая вывод из строя, блокировку работы, как отдельных модулей, так и сегментов сети Интернет. Речь идет о создании и применении широкого спектра различного типа программных средств скрытого информационного воздействия, специальных подставных ресурсов, в том числе технологии ботнетов, для организованного и целенаправленного выполнения команд центра.

**Класс №4.** Средства активного воздействия на посетителей Сети. Речь идет о разработке технических средств, позволяющих решать задачу по размещению в Сети на заданном множестве ресурсов и служб специально подготовленных мультимедийных материалов и ссылок: с помощью почтовых сообщений, с помощью рассылки через форумы, чаты, блоги, социальные сети, комментарии к новостям и др.

В качестве основы для технических средств обоих классов правильнее рассматривать средства скрытого контроля и при необходимости воздействия на ресурсы Сети. Речь идет о разработке программных средств скрытого информационного воздействия и специальных технологий, которые базируются на знании уязвимостей

широко используемых программных продуктов, включая применяемые разработчиками и пользователями средства защиты.

В части разработки технических средств и технологий помощи при планировании и проведении информационных операций.

**Класс №5**. Средства планирования, управления информационными операциями (ИО) и оценки их результативности в технической сфере.

**Класс №6**. Средства планирования, управления информационными операциями (ИО) и оценки их результативности в гуманитарной (социальной) сфере.

На результативность проведения информационной операции большое влияние оказывает качество ее подготовки и возможность грамотного управления непосредственно в режиме реального времени. В зависимости от сферы применения (техническая/гуманитарная) должны быть использованы свои характеристики и алгоритмические особенности поведения объектов воздействия.

Предложенная классификация информационного оружия во многом определяет структуру данной книги. Это:

- выявление угроз в гуманитарной сфере путем анализа новостных тематик;
- выявление угроз в технической сфере путем анализа общей динамической схемы мировых DDoS-атак на сайты различных представительств и учреждений;
- исследование составных компонент информационной операции в среде Интернет, как в технической, так и гуманитарной сфере;
- исследование вопросов автоматизации процессов планирования и моделирования информационных операций.

# ГЛАВА 2

# Мониторинг информационного пространства на предмет выявления информационных операций

На современном этапе противоборство в информационном пространстве является составной частью, а порой упреждающей составляющей вооруженного конфликта или торговой войны. При этом информационная операция, на первый взгляд, может не иметь ничего общего с целями конфликтующих сторон. Поэтому особенно важно как можно раньше выявить факт начала подобного рода информационной акции с тем, чтобы успеть подготовиться к реальному конфликту или, используя собственные информационные возможности, снизить вероятность наступления этого конфликта.

В свете сказанного необходимой составляющей современной войны является постоянный мониторинг информационного пространства на предмет выявления фактов начала информационных операций. Мониторинг целесообразно осуществлять в сети Интернет как наиболее динамичной составляющей информационного пространства, на базе хорошо зарекомендовавших себя образов, слоганов, слов и словосочетаний.

Выявление информационных угроз, как и любых других угроз, целесообразно начинать с анализа подходов и методов целенаправленного перепрограммирования информационных систем, будь то технические системы, или социальные структуры, или люди. Выделение последовательности присущих информационной операции событий, а затем выявление этих событий в общем «жизненном шуме» — это классический путь решения подобных задач.

Данный путь состоит из следующих этапов:

**Этап 1.** Последовательность событий, составляющих угрозу, всегда связана с целью (см. перечень задач в разделе 1.1). Достиже-

ние цели предполагает перепрограммирование субъектов информационного противоборства. Чтобы понимать, насколько достигнута цель, желательно уметь оценивать результаты перепрограммирования и собственные возможности, говоря другими словами — степень возможного поражения информационным оружием той или иной системы. Одни объекты уничтожить и перепрограммировать не составляет труда, с другими — задача может оказаться неразрешимой за выделенные для этой цели ресурсы и временные ресурсы, в первую очередь[7].

**Этап 2**. Оценка и обоснование частоты появления событий, при которой уже можно говорить о начале информационной операции по перепрограммированию[8].

**Этап 3**. Оперативное и доступное представление информации пользователю в случае выявления опасных тенденций[9].

## 2.1. Степень поражения информационным оружием

Предлагается степень поражения информационным оружием оценивать через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Что означает данное определение на практике?

Для вычислительной однопроцессорной системы степень ущерба можно оценить через процент потерянного полезного времени (иногда — через число репликаций компьютерного вируса), т.е. через долю процессорного времени, в течение которого инфекция управляет всей системой для достижения запрограммированных в ней целей плюс объем погубленных программ и данных, имеющих отношение к дальнейшему существованию данной системы, к поддержанию ее потребительских свойств.

---

[7] Раздел 2.1.
[8] Раздел 2.2.
[9] Раздел 2.4.

Для государства, по аналогии, — это доля паразитирующих структур или структур, работающих в данном государстве в интересах других государств или, исключительно, — самих себя. Так, например, многие исследовательские институты сегодня в России работают по зарубежным заказам, по зарубежным грантам, и часто обосновывают то, что желает заказчик. А так как таких немало, то и рекомендаций соответствующего направления становится все больше и больше. И на их фоне увидеть, что для страны хорошо, а что плохо, очень даже проблематично. Наука, к сожалению, никогда не бывает свободной от идеологии, от финансирования и от желания заказчика.

На финансовой системе — степень поражения информационным оружием отражается через отток капитала.

Для народа — через процент, на который ежегодно происходит его уменьшение, плюс погибшие культурные ценности и научно-производственные центры.

Как уже отмечалось, информационное поражение всегда начинается с поражения системы управления. В общем случае эффективность функционирования системы управления определяется следующими показателями состояния информационной системы:

– количеством и качеством элементов, ответственных за сбор входных данных, и эффективностью их функционирования. В данном случае под эффективностью функционирования элемента предлагается понимать такие характеристики, как: объем добываемых данных, «новизна» данных, достоверность данных;

– количеством и качеством элементов, ответственных за доставку данных, и эффективностью их функционирования. В данном случае эффективность функционирования элемента оценивается через время доставки данных и объем искаженных данных;

– количеством и качеством элементов, ответственных за обработку данных, и эффективностью их функционирования, которая в общем случае оценивается временем обработки данных, временем выработки решения и, возможно, мощностью потенциального пространства решений;

– количеством и качеством элементов, ответственных за представление результата, и эффективностью их функционирования. Здесь эф-

фективность функционирования можно попытаться оценить через степень искажения принятого решения при его реализации;

– количеством и качеством связей между элементами;

– защищенностью («жизненной силой») перечисленных выше элементов и связей между ними. При этом надо иметь в виду, что понятие «информационная защищенность элемента» подразумевает защиту этого элемента от информационных воздействий. В том случае, если защищаемый элемент принадлежит системе принятия решений, то наличие подобной защищенности резко понижает эффективность его работы в силу сокращения допущенных до него системой обеспечения безопасности данных, которые, на самом деле, могут оказаться необходимыми системе для выработки команд адекватной реакции.

Однако надо помнить, что через перечисленные показатели можно оценить эффективность работы системы управления, но нельзя понять, в чьих интересах она работает. В определенных условиях ее эффективная работа иногда может приносить больше вреда собственному народу, чем пользы. Например, водитель способен умело и ловко управлять машиной, но вести ее при этом к обрыву или в засаду противника.

Поэтому для теории информационной войны важнее оценить не столько эффективность работы системы управления, сколько степень ее возможного поражения. Степень же возможного информационного поражения системы управления логично оценивать через открытость этой системы для внешних целенаправленных информационных воздействий.

Перечислим качественные признаки открытости системы управления для противника.

1. Ключевые субъекты из системы управления «привязаны» противником (победителем) к сфере своих интересов.

2. Для ключевых субъектов из системы управления противником обеспечена «база» у себя. Родственники подобных субъектов («агентов влияния»), как правило, переселяются, проживают, учатся за пределами своей страны.

3. В случае победы противник, как правило, перестраивает систему управления пораженного объекта. Перестройка эта осуществляется в

ключе, удобном для понимания и дальнейшего скрытного управления. Чаще всего перестройка системы управления по своей форме направлена на соответствие образу и подобию системы управления победителя. В биологии сказанное выглядит следующим образом: «*В присутствии РНК-содержащих вирусов рибосомы клетки хозяина предпочтительно связываются не с молекулами РНК клетки-хозяина, а с молекулами вирусной РНК. Эти последние начинают теперь функционировать в качестве матриц для синтеза белка вирусной оболочки, а также для синтеза некоторых дополнительных ферментов, которые требуются для репликации других структурных компонентов вируса и, в частности, самой вирусной РНК*»[10].

Так как степень возможного поражения системы управления напрямую связана с открытостью системы, то следующий этап исследования — количественная оценка открытости системы управления для противника, которая и является важнейшей характеристикой степени возможного поражения.

Важно, что современная система управления включает в себя не только человеческий фактор, но и технический компонент, который при определенных условиях не менее значим, чем лицо, принимающее решение. Поэтому степень открытости имеет смысл анализировать как в части открытости лиц, принимающих решение, открытости соответствующих социальных структур, так и используемых технических средств.

При этом надо иметь в виду, что степень открытости определяется не только государственной волей, нормативными требованиями и законодательными актами, но и культурой народа. Определенные национальные типы изначально ориентированы только на свою нацию, что, несмотря на любые государственные реформы, обеспечивает нации защищенность от внешнего мира. Другие, наоборот, без соответствующего «железного занавеса» начинают терять свою национальную идентичность, исчезая, как нация, в окружающем мире.

Пусть $X = \{x_1, x_2, \ldots x_N\}$ — субъекты, принадлежащие системе управления.

---

[10] *Ленинджер А.* Биохимия. Молекулярные основы структуры и функций клетки. М.: Мир, 1976. 960 с., ил.

Здесь

$N$ — общее число субъектов ($N = N_г + N_т$);

$N_г$ — общее число субъектов-людей;

$N_т$ — общее число субъектов-технических систем, задействованных в принятии решений.

Каждый из них может быть охарактеризован близостью к основному центру принятия решений $\{s_i\}$. Самый простой пример — это:

$s_i=5$ — лицо, принимающее решения;

$s_i=4$ — непосредственный постоянный контакт с лицом, принимающим решения;

$s_i=3$ — непосредственный периодический контакт;

$s_i=2$ — опосредованный (через одного) постоянный контакт;

$s_i=1$ — опосредованный (через одного) периодический контакт;

$s_i=0$ — отсутствие непосредственных контактов.

Кроме того, каждый из названных субъектов может быть охарактеризован с позиции близости его к зарубежным культурам (обучение в соответствующих зарубежных центрах, как это было в СССР в случае ряда ключевых фигур ЦК КПСС), близости к жизненным интересам других государств (наличие родственников и друзей, живущих и работающих за рубежом или в фирмах, имеющих, в основном, иностранный капитал). Понятно, что данная характеристика применительно к конкретному субъекту не может говорить о том, что данный субъект является «агентом влияния», но в своей совокупности (по всей системе управления) вполне может выступать в качестве определенной оценки степени ее открытости.

Обозначим через $\tau_{iг}$ оценку близости индивидуума к «чужим» жизненным интересам и культурам (в том числе криминальным). Для числового примера воспользуемся такой же, что и выше, шкалой близости:

$\tau_{iг} = 5$ — гражданин другой страны;

$\tau_{iг} = 4$ — работа за рубежом;

$\tau_{iг} = 3$ — близкие родственники за рубежом;

$\tau_{iг} = 2$ — друзья и постоянные знакомые за рубежом;

$\tau_{iг} = 1$ — частые поездки за рубеж;

$\tau_{iг} = 0$ — зарубежных контактов нет.

Тогда степень открытости отдельно взятого субъекта:

$$o = \tau_{ir}\, s_i/25,$$

а всей системы управления:

$$O_г = (\sum \tau_{ir}\, s_i/25)/N_г.$$

Степень открытости изменяется в пределах от 0 до 1.

0 — система полностью закрыта для вероятного противника;

1 — система полностью открыта.

Аналогично оценивается открытость технической подсистемы, принадлежащей системе управления.

$$O_т = (\sum \tau_{it}\, s_i/25)/N_т.$$

Здесь оценка близости к основному центру принятия решений $\{s_i\}$ остается той же самой, а оценка близости к «чужим» жизненным интересам и культурам наполняется следующим содержанием:

$\tau_{it} = 5$ — все технические средства (программное и аппаратное обеспечение) зарубежного производства, принадлежат вероятному противнику;

$\tau_{it} = 4$ — все программное обеспечение зарубежного производства, аппаратное — собственное;

$\tau_{it} = 3$ — все системное программное обеспечение (ОС) зарубежного производства, остальное — собственное;

$\tau_{it} = 2$ — сетевое программное обеспечение зарубежного производства. Все остальное собственное;

$\tau_{it} = 1$ — только прикладное программное обеспечение зарубежного производства. Все остальное собственное;

$\tau_{it} = 0$ — все технические средства (программное и аппаратное обеспечение) собственного производства.

Тогда общая оценка выглядит следующим образом:

$$O = O_г * O_{т.}$$

Как и каждый сомножитель, общая степень открытости изменяется в пределах от 0 до 1.

0 — система полностью закрыта для вероятного противника;

1 — система полностью открыта.

## 2.2. Оценка эффективности перепрограммирования субъектов информационного воздействия

Цель информационного воздействия — перепрограммирование субъекта воздействия. Какое количество воздействий и какой информацией надо сделать, чтобы добиться цели? Ответ на этот вопрос крайне важен для организации решения задачи мониторинга информационного пространства на предмет выявления угроз. Здесь просматриваются две крайности:

- естественный новостной ряд по какой-либо теме может быть ошибочно принят за разворачивающуюся информационную угрозу;
- информационная угроза не была выявлена вовремя и цель информационного воздействия достигнута. После этого что-то предпринимать информационными методами уже поздно: лидер выбран, закон принят, бесполетная зона введена.

Таким образом, важной становится задача теоретического определения количества воздействий, после появления которых уже можно делать обоснованные прогнозы о ведении противником информационной операции. Для этого необходимо предложить аналитическое выражение, позволяющее связать степень достижения информационной победы с числом информационных воздействий, т.е. оценить эффективность перепрограммирования или, иными словами, эффективность применения противником информационного оружия, или скорость разворачивания информационной операции.

Чтобы теоретически оценить эффективность перепрограммирования, не прибегая к измерениям, необходимо обосновать соответствующую модель влияния сообщений от источника, обладающего определенной информационной энергией[11], на постоянных пользователей его информации.

Сделаем предположение, что последовательность информационных воздействий одинаковой направленности изменяет состояние объекта пропорционально количеству воздействий — капля камень

---

[11] Информационная энергия — это возможность субъекта (модели) перепрограммировать окружающие информационные системы (модели), включая себя. См.: *Расторгуев С.П.* Информационная война. Проблемы и модели. М.: Гелиос АРВ, 2006.

точит. Предположим, что таких объектов N. Через k обозначим число информационных воздействий, а через $\alpha$ — некоторый коэффициент пропорциональности. Пусть Y(k) — количество субъектов (читателей, зрителей), изменивших свою точку зрения под воздействием k передач и начавших по-иному воспринимать тот или иной термин. Наша задача заключается в том, чтобы обосновать аналитическую зависимость Y от k. При этом первоначально, для упрощения считаем, что все воздействия имеют одинаковую направленность и равны по своей силе информационного воздействия.

Предположим, что в ходе первого воздействия $\alpha N$ субъектов изменит свою точку зрения относительно определенного термина, события или персонажа. Предполагается, что $\alpha$ изменяется от 0 до 1 (0 — воздействие ничего не меняет, 1 — воздействие изменяет точку зрения). Тогда останется $(N-\alpha N)$ субъектов с прежней позицией. Второе воздействие будет направлено в первую очередь именно на них и поразит $\alpha$-ую часть оставшихся — $\alpha(N-\alpha N)$. Таким образом, в ходе двух воздействий будет откорректирована позиция $\alpha N + \alpha (N-\alpha N)$ человек. Вводя функцию Y(k), сказанное можно записать в виде:

$$Y(k) = Y(k-1) + \alpha [N-Y(k-1)].$$

Для практических расчетов коэффициент $\alpha$ может служить в качестве одной из сравнительных характеристик способности различных источников информации перепрограммировать информационные субъекты. Для конкретного информационного источника он назван **напряженностью воздействия информационного источника** и рассчитывается по формуле:

$$\alpha = [Y(k)-Y(k-1)] / [N — Y(k-1)].$$

Напряженность воздействия информационного источника связана с информационной энергией источника, в частности, с числом субъектов, которые положительно относятся к данному источнику. Таким образом, $\alpha$ может быть еще оценен на предварительном этапе. По сути своей, его величина пропорциональна мощности множества посетителей, идущих за конкретным информационным источником.

Как было отмечено в первой главе, обобщенная модель перепрограммирования должна быть основана на таких параметрах, как:

- частота подачи материала, относящегося к заданной теме. Частота подачи материала оценивается величиной $k/\Delta t$, где $k$ — число информационных воздействий, $\Delta t$ — временной интервал, в течение которого эти воздействия были сделаны. Обоснование временного интервала — отдельная задача, частично она была решена в рамках математической модели слухов[12], частично в теории рекламы — при оценке навязывания потребителю одинаковых информационных сообщений для сохранения устойчивости сформированного образа;
- значимость источника. Данный параметр оценивается величиной $\alpha$;
- охват населения. В модели охват населения оценивается величиной $Y$.

Все названные параметры являются определяющими для представленной модели.

ПОДВЕДЕМ ИТОГ СКАЗАННОМУ.

Если наблюдается устойчивый рост информационных воздействий ($k$) в рамках одной и той же темы и одновременно происходит стабильное увеличение числа субъектов ($Y$), изменивших свою точку зрения, при этом новая точка зрения несет в себе угрозу текущему состоянию, то речь, с большой долей вероятности, идет именно об информационной операции.

## 2.3. Математическая модель распространения слухов и понятие «реальное время» информационной операции

Одним из важных вопросов при планировании информационной операции в сети Интернет является физическая размерность **понятия «реальное время».**

Во время Второй мировой войны психологи из Гарвардского университета Гордон У. Оллпорт и Лео Постман провели исследование

[12] *Allport G., Postman, L.* The psyhology of rumor. New-York: Holt, 1947.

слухов, распространявшихся в военное время. Это позволило им вывести математическую формулу, описывающую механизм распространения и действия слухов, и на ее основе разработать методы управления слухами. Ученые опубликовали результаты своих исследований в 1947 году в книге «Психология слухов»[13]. Оллпорт и Постман дали следующее определение понятию «слух»: «В том значении, в котором мы будем использовать данный термин, слух — это информационное сообщение, которое распространяется между людьми, как правило, в устной форме, без предоставления доказательств его достоверности… Слух передается при условии, что события, которые он раскрывает, имеют какую-либо значимость для людей, а информация, содержащаяся в нем, является недостаточной или неопределенной. Неопределенность содержания слуха может быть результатом того, что новости были изложены нечетко, либо они были противоречивыми, либо получатель информации неправильно ее истолковал».

Неопределенность также может быть следствием недоверия компании, т.е. когда люди не верят всем сообщениям компании, даже правдивым. Оллпорт и Постман комментируют это следующим образом: «Слух будет распространяться тем быстрее, чем больше люди не верят официальным новостям, которые они слышат». По этой причине компании следует сформировать хорошую репутацию и завоевать доверие общественности еще до того, как начнутся проблемы.

Оллпорт и Постман демонстрируют механизм совместного действия факторов значимости и неопределенности и отмечают наличие математической зависимости между ними: «Распространение слуха находится в количественной зависимости от двух основных факторов — значимости и неопределенности. Формула, позволяющая установить интенсивность распространения слуха, может быть выражена следующим образом:

$$R \sim i \times a.$$

Эта формула означает следующее: интенсивность распространения слуха изменяется в зависимости от степени значимости предмета слуха для конкретных слушателей, умноженной на неопределенность фактических данных, содержащихся в слухе. Отношение между зна-

[13] *Allport G., Postman, L.* The psyhology of rumor. New-York: Holt, 1947.

чимостью и неопределенностью не аддитивное, а мультипликативное, так как если один из этих факторов равен нулю, то слуха не существует. Слух не может существовать при наличии только фактора неопределенности или только фактора значимости».

Время жизни и распространения слуха опирается на определенные временные периоды, существует т.н. динамика цикла новостей. Как правило, возможность применить формулу R ~ i x a для ликвидации слухов существует только в определенные моменты цикла новостей. Если пропущен один период, то предотвратить дальнейшее распространение информации до следующего периода становится гораздо сложнее.

Периоды:

45 минут
6 часов
3 дня
2 недели[14].

Приведенные выше периоды предлагается взять за основу понятия «реальное время», используемое в наших построениях. В дальнейшем эти периоды во многом определяют реальное время субъектов, принимающих решение, а сами определяются «масштабом» субъектов. Так, если в случае принятия или непринятия решений об интервенции в Ливии и Сирии для высшего руководства НАТО единицей измерения были трое суток, то для модератора сайта, на котором разворачивается информационная операция, единицей измерения времени уже становится 45-минутный интервал.

## 2.4. Мониторинг информационного пространства

Признаком ведения информационной операции технической направленности являются нарастающие атаки на ресурсы сети: на

[14] Хелио Фред Гарсия. Crisisnavigator. Org. Раздел: Слухи — buzz marketing. По материалам: http://iniciator.ru/index.php/buzz/razdel/C47/.

конкретные тематические сайты, на сайты провайдеров, которые размещают у себя соответствующие тематические сайты, на DNS-сервера и другие важные для функционирования Интернета службы. Отследить появление фактов нарастания атак соответствующей направленности можно по появлению новостных сообщений, которые выбираются, например, по следующим ключевым словам:

- атака на DNS-сервер;
- DDoS-атака;
- нарастание вирусной угрозы;
- блокировка сайта;
- отказ в обслуживании и т.п.

Данный перечень далеко не полный. Доведение его до приемлемой для практического использования полноты — отдельная исследовательская задача.

Как было показано выше, на сегодняшний день зарекомендовавшим себя признаком ведения информационной операции гуманитарной (социальной) направленности является создание и закрепление в общественном сознании выгодной агрессору модели мира. При этом важно, что сегодня информационное воздействие всегда направляется на объект агрессии. Агрессор формирует требуемое ему общественное мнение именно у населения противника. Получается, что для поддержания собственной информационной безопасности анализировать информационные материалы важнее не те, которые подаются в той или иной стране, а те, которые формируются в собственной стране источниками, подконтрольными зарубежным структурам.

При изучении зарубежного информационного пространства выявление устойчиво формируемых соответствующими источниками моделей позволяет понять взаимоотношение зарубежных стран по отношению друг к другу.

Таким образом, к признакам информационной угрозы можно отнести:

- увеличение и поддержание на определенном уровне частоты повторения новостей определенной тематики и заказных комментариев к ним в соответствии с заданной количественной оценкой;
- территория, на которую направлено воздействие соответствующей информации (объект воздействия);

- источники информации (субъект воздействия).

По гуманитарному (социальному) направлению нами был проведен анализ новостных тематик, предшествующих интервенции в Ирак, Ливию. Он показал, что на роль ключевых слов для фильтрации новостей подходят следующие слова/словосочетания/реплики:

– нарушение прав человека…
– создание оружия массового поражения…
– преступления режима против собственного народа…
– коррумпированный режим…
– антинародный режим…
– диктаторский режим…
– коррумпированная власть…
– уничтожение собственного народа…
– борьба с собственным народом…
– уничтожение демократии…
– подавление свободы…
– применение армии против собственного народа…
– поставка оружия…
– приграничные конфликты…
– пособничество терроризму…
– подготовка террористов…
– нарушение правил торговли…
– организация бесполетной зоны…
– применение химического оружия…

и т.п.

Количество возможных слов, словосочетаний, слоганов и их комбинаций с учетом синонимов даже на простых примерах при одновременном выявлении информационных угроз различной направленности измеряется тысячами. Чем полнее это множество, тем больше вероятность выявления угрозы на раннем этапе ее зарождения. Но для человека-оператора отследить развитие процесса по всем направлениям не представляется возможным. Поэтому задача автоматизации факта выявления изменений в частотах повторения новостных тематик и оперативного удобного представления результатов оператору является актуальной и практически значимой.

Обозначим через $x_i$ — слово/словосочетание, относящееся к i новостной тематике.

$V_j(x_i)$ — число новостных сообщений, содержащих $x_i$, в течение j временного периода (j — в зависимости от решаемой задачи, может быть порядковым номером минуты, часа, суток, неделей и т.п.), так, например,

$V_1(x_i)$ — число новостных сообщений, содержащих $x_i$, за первый час наблюдения;

$V_2(x_i)$ — число новостных сообщений, содержащих $x_i$, за второй час наблюдения;

$V_j(x_i)$ — число новостных сообщений, содержащих $x_i$, за j-ый час наблюдения и т.д.

Тогда величина:

$$V_j(x_i)^1 = V_{j+1}(x_i) — V_j(x_i)$$

характеризует направление развития числа новостных сообщений, а величина:

$$V_j(x_i)^2 = V_{j+1}(x_i)^1 — V_j(x_i)^1 = V_{j+2}(x_i) — 2V_{j+1}(x_i) + V_j(x_i)$$

свидетельствует об устойчивости процесса.

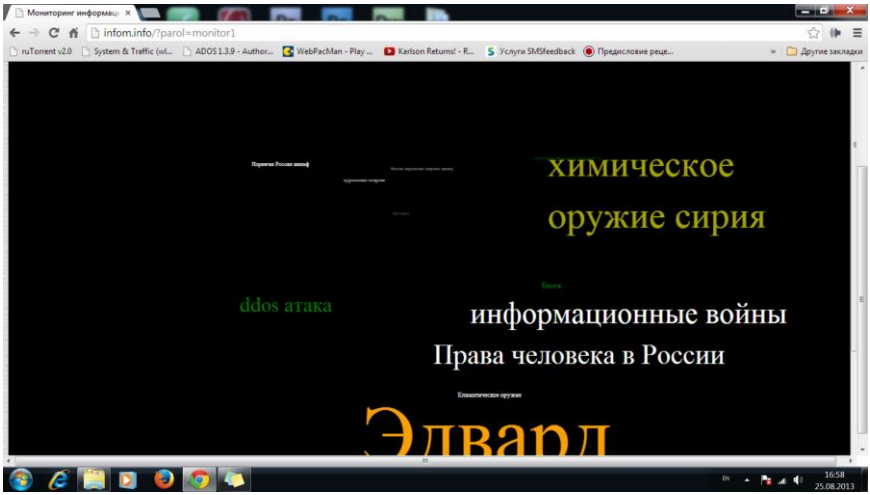
При этом должен существовать интервал, для которого, начиная с некоторого $t_1$, выполняется $V_j(x_i) > V_0$.

Таким образом, задача сводится к формированию множества $\{x_i\}$, формированию множества доверенных источников ($\{y_i\}$ – ресурсов сети Интернет), по которым будет осуществлен регулярный сбор данных о $\{x_i\}$ с последующей оценкой значений $V_j(x_i)_1$ и $V_j(x_i)_2$ по разным временным интервалам ($\Delta t$).

Считаем, что информационная угроза имеет место, если значения $V_j(x_i)_1$ и $V_j(x_i)_2$ превышают некоторый порог и выполняется $V_j(x_i) > V_0$, начиная с некоторого j и до текущего временного интервала не менее, чем для P% временных интервалов[15].

В ходе предварительных исследований был создан специальный макет, на котором изучались представленные выше результаты и предложения. Ниже приведен скриншот экрана макета.

[15] По нашим оценкам P=60.




Для макета было использовано следующее множество $\{x_i\}$:

– химическое оружие Сирия;
– права человека в России;
– Эдвард Сноуден;
– нарушение воздушного пространства;
– Россия нарушение морских границ;
– информационные войны;
– климатическое оружие;
– Курильские острова;
– Норвегия Россия шельф.

В качестве множества $\{y_i\}$ — новостных ресурсов сети Интернет — было взято множество новостных ресурсов Google и отфильтровано с помощью службы Google по адресной рассылке новостных сообщений заданной тематики. Сегодня подобные рассылки можно получать у любого серьезного новостного ресурса (yandex.ru, mail.ru, Би-би-си и др.). При необходимости дополнительно можно сделать собственный поисковик, ориентированный на конкретные доверенные ресурсы.

В качестве специальных эффектов были использованы цвета и форма подачи материалов в виде «облака тегов». Цвета выбраны следующие:

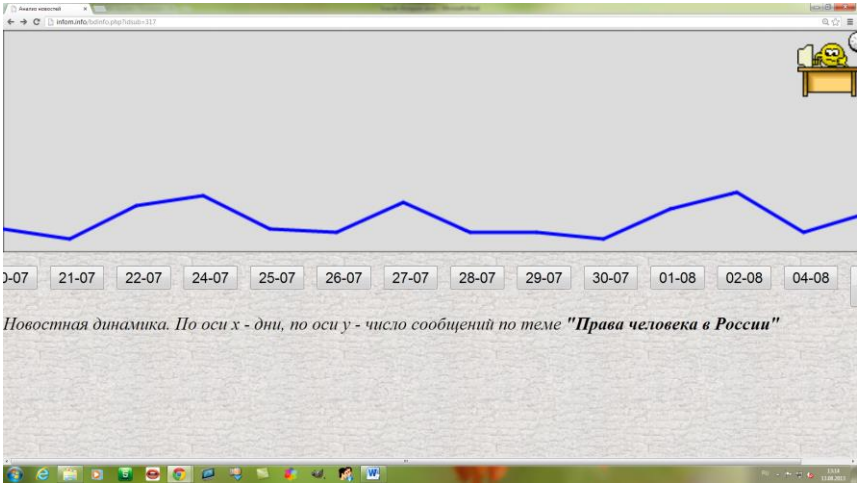
– белый — число новостных сообщений находится в заданных (естественных) границах;

– желтый — число новостных сообщений выходит за пределы границы (верх);

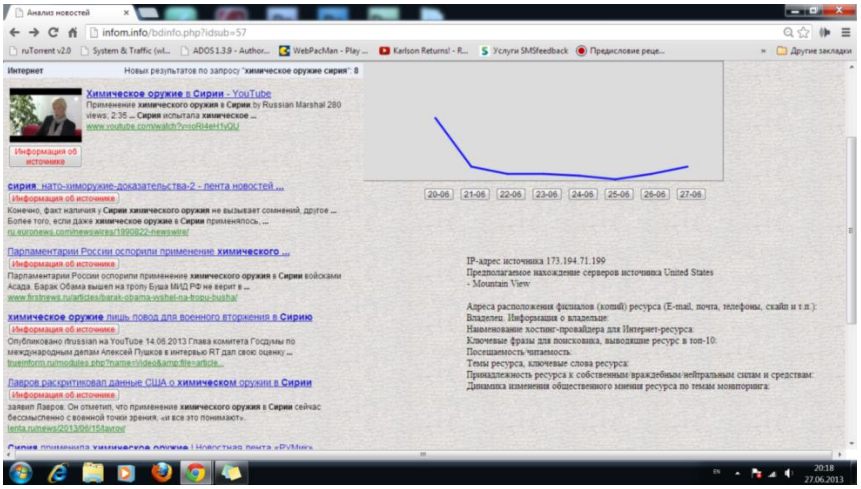
– зеленый — число новостных сообщений выходит за пределы границы (вниз);

– красный — число новостных сообщений значительно нарастает ($V_j(x_i)^1$ и $V_j(x_i)^2$ больше установленных значений).

В том случае, если появляются сообщения с предупреждающей окраской, оператор всегда может перейти к детальному исследованию новостного процесса.




По вертикальной оси — число новостных сообщений, по горизонтальной — время в выбранном масштабе, в данном случае — день-месяц. По нажатию соответствующей кнопки оператору представляются ссылки на все новости данного дня:




На вышеприведенном экране макета оператор может непосредственно по ссылке перейти на сайт, где размещена новость, а также посмотреть информацию об источнике (специальная красная кнопка «Информация об источнике»). При нажатии на эту кнопку в правой нижней части экрана высветится следующая информация:

- наименование ресурса;
- географическое расположение;
- адрес (IP-адрес (для интернет-ресурса), E-mail, почта, телефоны, скайп и т.п.);
- адреса расположения филиалов (копий) ресурса;
- владелец;
- наименование хостинг-провайдера для интернет-ресурса;
- ключевые фразы для поисковика, выводящие ресурс в топ-10;
- посещаемость/читаемость;
- темы ресурса, ключевые слова ресурса;
- принадлежность ресурса к собственным/враждебным/нейтральным силам и средствам (перечень дружественных и враждебных ресурсов (ссылки);
- динамика изменения общественного мнения ресурса.

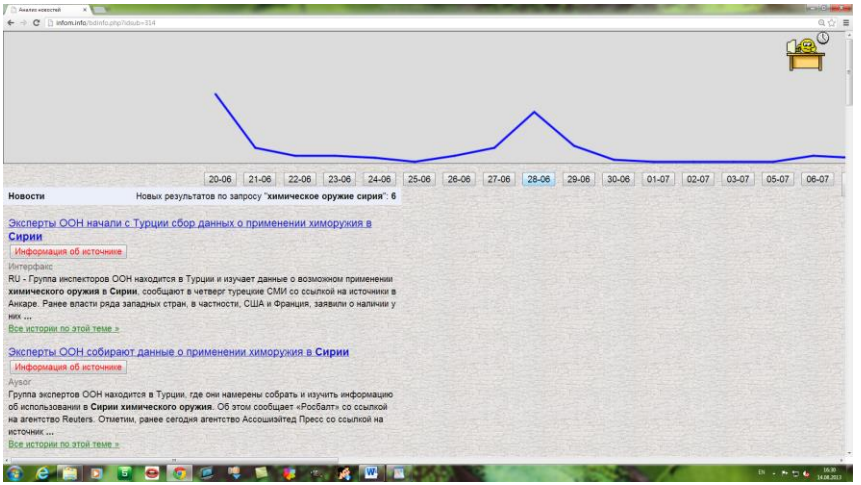
Все эти данные пригодятся для детального анализа источников подобного рода сообщений, их связей друг с другом и возможностей влияния на них и их хозяев. Кроме того, данная информация

может быть использована в качестве исходных данных для планирования собственных ответных операций.

Полученные с помощью макета материалы имеют довольно широкий спектр применения — они позволяют изучать процесс протекания информационной операции. Приведем пример. Понятно, что нагнетание угрозы по поводу применения Сирией, имеющей нормальное военное вооружение, включая авиацию, химического оружия против зарубежных наемников является чисто информационной операцией, направленной на перепрограммирование мирового общественного мнения. В условиях, когда никто не возражает, данная позиция становится доминирующей. Подобное на наших глазах происходило применительно к Ливии, когда все, включая Россию, поддержали введение бесполетной зоны над суверенным государством.

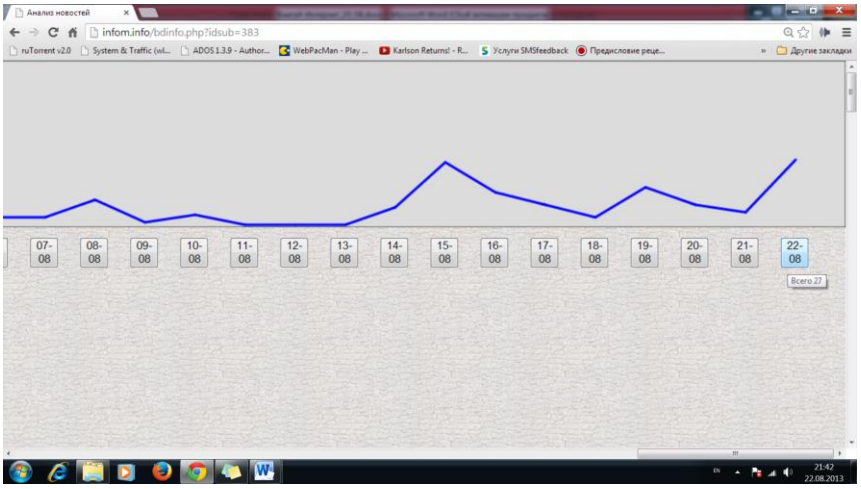
Исследуем развитие информационной операции по убеждению мирового общественного мнения в применении сирийскими военными химического оружия.

На следующем скриншоте показан график новостных сообщений по теме «химическое оружие Сирия». Сообщения выбраны по дате 28 июня. На этот день их было 26.



29 июня В.В. Путин заявляет: «У нас нет доказательств фактов применения химоружия властями Сирии».

После этого заявления число новостных сообщений по данной тематике стало резко уменьшаться. Но авторы информационной операции не успокоились. Заявление В.В. Путина и последующие заявления российского МИДа снизили общий рост новостных сообщений и способствовали увеличению времени проведения данной информационной операции. 10 июля РФ привела доказательства использования сирийскими «повстанцами» зарина в Алеппо, что опять вызвало всплеск новостных сообщений. Но уже 12 июля США обвинили Россию в блокировании расследования применения химоружия в Сирии. Наблюдаем полное игнорирование результатов работы российских экспертов, в силу того, что оно противоречит создаваемой агрессором модели. После этого российская точка зрения практически покидает новостное информационное пространство. Опять продолжает исполняться «старая песня». На другие мнения ведущие мировые СМИ не обращают внимание. Таким образом, организаторы информационной операции не позволяют «затухнуть» данной теме.




Тема раскручена, и для ее поддержания в дело уже идут самодельные, но настоящие ракеты, начиненные зарином, которые и

выпускаются по населению. В результате мировое внимание к данной теме с одновременным осуждением всех, придерживается противоположной точки зрения, усиливается.

Обывательская логика проста:

А. Ранее общественности было доказано, что руководство Сирии и, в частности, ее президент — злодеи. Доказывали долго и интенсивно.

Б. Произошло злодейское событие — применение химического оружия по мирному населению.

Вывод №1: Химическое оружие применено по указанию президента Сирии.

Следствие №1: Все те, которые поддерживают законное злодейское правительство Сирии, включая Россию и Китай, — такие же злодеи.

# ГЛАВА 3

# Проведение специальных действий в ходе осуществления информационных операций

Прежде чем приступить к раскрытию содержания данной главы, определимся с применением термина «специальный» в отношении действия. Согласно Толковому словарю Ушакова, «специальный»: 1. *Особый*, отдельный, не общий, исключительно для чего-н. предназначенный. 2. Связанный с отдельной, *обособленной* отраслью общественной жизни (науки, техники и т. п.), присущий той или иной *специальности* (отличие от общего). Действия, проводимые в ходе информационных операций, названы «специальными» по той причине, что они, действительно, имеют существенное отличие от «обычных» — их проведение осуществляется с соблюдением анонимности, в телекоммуникационной среде, а не на открытом поле реального боя, например, и эти *особенности* должны также учитываться при планировании и моделировании информационной операции.

## 3.1. Исполнители

В большинстве случаев, говоря об информационных операциях в Сети, мы подразумеваем проведение специальных действий в условиях анонимности. Субъект, как инициирующий информационную операцию, так и осуществляющий ее, выступает как некий ***актор***. Согласно Глоссарию конфликтологических терминов М. Устиновой[16], **актор** (лат. *actor* — деятель) — индивид, общественная груп-

[16] *Устинова М.* Новые термины на русском языке. Глоссарий конфликтологических терминов. М.: Каллиграф, 2008. 96 с.

па, институт или другой субъект, осуществляющий конкретные действия; сторона, участвующая в конфликте[17]. Таким образом, в рамках ролевых концепций исход информационной операции является результатом реализации различных ролевых предписаний задействованных акторов. Исполнителями действий являются не только люди; способностью к исполнению целенаправленного действия наделяются виртуальные субъекты, например, программные [ро]боты и даже вирусы. В программировании актор — программная сущность заданной структуры и механизмов взаимодействия; содержит данные и процедуры, обладает инкапсуляцией, отношениями, наследованием и может порождать сообщения [там же]. Акторы так же, как в театре, «играют роли» на информационной арене (сцене) Интернета по сценариям или спонтанно.

Рассмотрим акторов информационных операций, взяв за основу их поведенческие особенности, проявляющиеся в ходе воздействия на объекты технической и гуманитарной (социальной) сферы.

### *3.1.1. Акторы технической сферы*

Достижение информационного превосходства путем уничтожения, искажения или хищения информационных массивов, преодоления систем защиты, обеспечения допуска незаконных пользователей, дезорганизации работы технических средств и компьютерных систем ориентируется на высокоточные и максимально скрытые, анонимные способы воздействия масштабного разрушения. Акторами выступают:

---

[17] Другие определения актора: *в социологии* — 1) действующий субъект; индивид, совершающий действия, направленные на других. Например, лидер общественного мнения; 2) участник преобразований, движимый собственными мотивами и обладающий для этого соответствующим опытом. Акторы могут иметь неоднозначные мотивы, ожидания, эмоциональные переживания, связанные с неопределенностью последствий совместных преобразований и «неизреченностью = непроявленностью собственных смыслов»; *в политологии* — субъект политики, участник мировой политики, который может влиять на процессы, происходящие в мире. См.: http://ru.wikipedia.org/wiki/Актор.

- компьютерные вирусы, способные внедряться в программное обеспечение информационных систем, размножаться, передаваясь по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п.;
- логические бомбы — программные закладки, которые заблаговременно внедряют в информационно-управляющие части системы, чтобы по команде или в назначенное время привести их в действие;
- средства нейтрализации тестовых программ;
- преднамеренные ошибки, вводимые противником в программное обеспечение объекта воздействия.

Приведем пример средства воздействия на программный ресурс электронных управляющих модулей, которое обеспечивает вывод их из строя и изменение алгоритма их функционирования с использованием специальных программных средств. Это известный вирус Stuxnet, представляющий собой специализированную разработку (2010 год) спецслужб Израиля и США, направленную против ядерного проекта Ирана. Уже позже данную гипотезу подтвердил Эдвард Сноуден. Экс-сотрудник ЦРУ, находясь в транзитной зоне московского аэропорта Шереметьево, заявил в интервью немецкому журналу Spiegel, что компьютерный вирус Stuxnet, поразивший ядерные центрифуги Ирана, создан и запущен Израилем в сотрудничестве с США.

Примечательно, что «масштаб заражения иранских систем можно описать как фатальный, вирус проник по многим заводами активно вмешиваясь в системы управления. Если судить по блогам, то по оценкам иранских граждан, знакомых с проблемой, заражено до 60% процентов всего оборудования в Иране. В то же время иранские СМИ лишь кратко описывают ситуацию и утверждают, что Агентство по атомной энергии Ирана успешно справилось с проблемой и занимается зачисткой остатков»[18]. Так иранские СМИ стали акторами социальной сферы, влияющими на формирование общественного мнения.

---

[18] *Табаков Д.* Атака StuxNet, оценка угрозы вирусной атаки // www.sald.ru/blog-1826/0/.

Таким образом, акторы технической сферы, представляя собой информационное оружие на основе программного кода, «ответственны» за проведение следующих специальных действий в ходе осуществления информационных операций в телекоммуникационной среде:

- проникновение в информационную систему противника;
- преодоление систем защиты;
- собственная маскировка и анонимность;
- сбор данных, циркулирующих в информационной системе противника;
- доставка и внедрение определенных команд или информационных материалов в конкретное место информационной системы (интернет-ресурса);
- создание или модификация виртуальной реальности (имитация голосов, создание видеоизображений конкретных людей и т.п.);
- модификация информации, хранимой в базах данных информационных систем противника или отображаемой на его интернет-ресурсах;
- скрытое изменение алгоритма функционирования программного обеспечения в заданный момент времени или при наступлении определенного события в системе и др.

Перечисленные акторы технической сферы — компьютерные вирусы и закладки, средства нейтрализации тестовых программ, преднамеренные ошибки программного обеспечения — подробно описаны в технической литературе. Не будем повторяться и в данной книге остановимся на приемах применения информационного оружия виртуальными специалистами (раздел 3.2. «Практикум «воина сети Интернет»).

### *3.1.2. Акторы гуманитарной (социальной) сферы*

Общей предпосылкой проведения информационной операции в социальной сфере является тот факт, что, когда человек вынужден ориентироваться в условиях недостатка информации либо ее избытка, повышается вероятность принятия ошибочных решений с

последующим накоплением ошибок на различных уровнях управляемого процесса. Поэтому в ходе информационной операции, в частности, должна решаться задача уменьшения или увеличения информационных сообщений, размещаемых на доверенных и раскрученных в Сети информационных ресурсах (новостных сайтах и лентах, в социальных сетях, в комментариях, где имеет место выражение отношения к проблеме). При этом все более распространенными становятся явление астротерфинга и явление зомбирования (социального программирования) мемами. Неодушевленными акторами социальной сферы в этих явлениях выступают медиавирусы в случае социального программирования, тролли и [ро]боты в случае астротерфинга.

## Медиавирусы

Явление медиаактивизма и применения медиавирусов описано впервые американским специалистом в области средств массовой информации Дугласом Рашкоффом[19]. Он ввел понятие медиавируса для обозначения медиасобытий, вызывающих прямо или косвенно определенные изменения общественного мнения. Часто употребляемыми в контексте информационных операций и взаимосвязанными понятиями становятся «мемы»[20], «вирусы сознания», «вирусы СМИ». Медиавирусы представляются распространяющимися по инфосфере мемами и мемокомплексами, изменяющими восприятие локальных и глобальных событий.

«Мем — это единица информации в сознании, чье существование влияет на события так, что большое число ее копий возникает в других сознаниях… Заразные информационные паттерны, которые воспроизводятся паразитически, инфицируя сознания людей и видоизменяя их поведение, заставляя их распространять этот паттерн. Отдельные слоганы, лозунги, музыкальные мелодии, визуальные изображения… — типичные мемы. Шутки поддерживают инфицирование тем, что они смешные, мелодии тем, что вызывают разнообразные эмоции,

---

[19] *Рашкофф Д.* Медиавирус. Как поп-культура тайно воздействует на ваше сознание / Пер. с англ. Д. Борисова. М.: Ультра. Культура, 2003. 368 с., ил.

[20] Руководство по мемам: путеводитель пользователя по вирусам сознания (Версия 1.1) © Бретт Томас, 1995 // http://asocial.narod.ru/material/memes.htm.

лозунги через выразительность и многократное повторение… Идея или информационный паттерн не является мемом до тех пор, пока не заставит носителя реплицировать ее, повторить ее в ком-то еще… Вирус сознания — что-то во внешнем мире, что инфицирует людей с мемами. Те мемы, наоборот, влияют на поведение инфицированных людей так, что они помогают увековечивать и распространять вирус… Вирусы СМИ — тип вирусов сознания. Они используют сообщения СМИ. Есть три типа вирусов СМИ: 1) умышленные вирусы СМИ: реклама, агитация, действия СМИ, направленные на распространение идеологии или продукта; 2) захваченные вирусы СМИ: их намеренно не выпускали, но ими быстро начинают пользоваться группы людей, которые надеются с их помощью продвинуть свои собственные цели; 3) самозарождающиеся вирусы СМИ: плодятся, благодаря случайным событиям, которые выявляют объективные интересы, и распространяются добровольно потому, что они попадают прямо в слабости общества и идеологический вакуум» [там же].

Бóльшую часть книги Рашкоффа занимают примеры различных медиавирусов[21]. Это скандальные происшествия, сплетни о политиках и поп-звездах и т. п. — события с негативной или провокационной подоплекой, освещаемые в среде Интернет с помощью специально подготовленных медиаматериалов (текст, аудио, видео) и вызывающие заметные для общества последствия. К медиавирусам, например, относят сексуальный скандал вокруг бывшего, а тогда действующего президента США Билла Клинтона и Моники Левински, использованный республиканцами и способствовавший ослаблению позиций демократов в этой стране.

### Акторы астротерфинга

Астротерфинг — создание искусственного общественного мнения с помощью специальных программ и технологий на базе среды Интернет.

Почему подобное стало возможным? И насколько оно опасно?

Возможно, потому что важнейшей характеристикой современной эпохи стало появление технических средств между человеком

[21] См.: http://ru.wikipedia.org/wiki/Медиавирус.

и человеком. И тот, кто владеет этими техническими средствами, тот и управляет людьми.

Опасно, потому что Интернет — это не только СМИ, это не только взаимодействующие технические системы. Интернет — это среда, в которой одновременно обитают как люди, так и программные модули, которые мало чем отличаются от людей. В литературе они называются по-разному: боты, аватары[22], программные роботы. В силу того, что эти программные роботы в части диалогового интерфейса мало чем отличаются от людей, а порой даже их превосходят по ряду коммуникационных параметров, возникает вопрос, кого будут слушать люди? Чьи тексты будут читать посетители, открывая огромную книгу по имени Интернет? К чьему мнению прислушиваться? Если к мнению большинства, то это мнение легко формируется хозяином соответствующих технических средств, соответствующих программных роботов.

Воздействие на общественное мнение, как и защита его — одна из наиболее актуальных современных задач, относящихся к обеспечению информационной безопасности. При этом речь идет уже не о безопасности отдельно взятой страны, а об обеспечении информационной безопасности всего человечества. События в Ливии и Сирии показывают, что сегодня идет мощнейшая атака на систему отношений людей друг к другу и к миру, независимо от того, где они проживают и какие ценности исповедуют.

Вопрос: «Насколько защищены подобные технологии, чтобы они имели право на существование? Не начнет ли формироваться у определенной части человечества модель мира, неадекватная этому миру? Что само по себе уже опасно! Не подкладывается ли сегодня мина под фундамент человеческого знания о мире и самом себе. А если подкладывается, то как от этого защититься? И возможна ли вообще защита?

Вернемся в лоно строгих определений и алгоритмов. **Общественное мнение** на базе ресурсов Интернет представляет собой совокупность взаимосвязанных индивидуальных мнений по конкретному вопросу, затрагивающему группу людей. Эти мнения зафикси-

---

[22] *Расторгуев С.П., Литвиненко М.В.* Аватаризация. СПб.: Реноме, 2011. 311 с.

рованы в виде мультимедийных материалов на ресурсах сети Интернет. Например, в виде комментариев к какой-либо новости. Новость является тем узлом, который собирает эти мнения вокруг себя.

Грамотный выбор потока новостей влияет и на множество комментариев, но это отдельная тема. Здесь мы рассмотрим только ту часть проблемы, которая относится к возможности комментирования.

А теперь подойдем к главному вопросу: как формируется эта совокупность индивидуальных мнений? Что надо для того, чтобы оставить комментарий?

Все множество новостных сайтов, как показал анализ на предмет возможности комментирования сообщений, может быть разбито на несколько классов:

- сайты, где любой посетитель имеет право комментировать любую новость;
- сайты, на которых, чтобы оставить комментарий, посетителю необходимо зарегистрироваться (ввести логин и пароль);
- сайты, где необходимо не только зарегистрироваться, но и при каждой авторизации преодолевать различные капчи[23];
- сайты, где при регистрации используется номер сотового телефона посетителя, пароль посетителю передается через смс;
- сайты, где комментарии могут оставлять только «свои», т.е. права доступа получаются не при регистрации, а выдаются заранее по принципу «лично известен». Например, банки и другие подобные структуры.

Принципиально важно, что посетитель приходит на тот или иной ресурс не непосредственно сам, а опосредованно, через соответствующее ПО — браузер. Браузер — обычная компьютерная программа, и ей все равно, кто ее запускает — человек или другая компьютерная программа. Кроме того, другая, специально созданная компьютерная программа может выходить в Интернет самостоятельно с заданными настройками, например, под видом любого

---

[23] *Капча* (англ. *Captcha*) — название применяемых в Интернете приемов, предназначенных для проверки на принадлежность к людям, разновидность обратного теста Тьюринга. Обычно прохождение капчи заключается в решении задачи распознавания текстовых, голосовых, математических образов, которые может распознать человек, но не может программа.

браузера. Сегодня написать подобный код достаточно легко. Для этого существуют специальные пакеты, например, Curl.

Вот так выглядит на php обращение к сайту от имени посетителя, который вошел в Интернет, *якобы*, с браузера: «Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322)».

```
// 1. Инициализируем соединение
$ch = curl_init();
// 2. Указываем параметры, включая url
$headers = array
(
'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*;q=0.8',
'Accept-Language: ru,en-us;q=0.7,en;q=0.3',
'Accept-Encoding: deflate',
'Accept-Charset: windows-1251,utf-8;q=0.7,*;'
);
        curl_setopt($ch, CURLOPT_HTTPHEADER,$headers);
        curl_setopt($ch, CURLOPT_URL,$s[0]);
        curl_setopt ($ch, CURLOPT_USERAGENT, «Mozilla/5.0
(compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322)»);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        curl_setopt($ch, CURLOPT_HEADER, 0);
        curl_setopt($ch, CURLOPT_COOKIEJAR,
«my_cookies.txt»);
        curl_setopt($ch, CURLOPT_COOKIEFILE,
«my_cookies.txt»);
// 3. Получаем HTML в качестве результата
        $output = curl_exec($ch);
// 4. Закрываем соединение
        curl_close($ch);
```

После этого обращения все содержимое сайта будет загружено в переменную $output. При этом система контроля сайта отметит, что на сайт заходил посетитель с браузера «*Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322*)», на котором установлены следующие языковые предпочтения: *ru,en-us;q=0.7,en;q=0.3*, используемая кодировка — *windows-1251 и utf-8*, т.е. именно с того браузера, который был указан при обращении.

Обработка полученного в переменной $output содержимого — это уже применение классического набора алгоритмов на базе стандартных библиотечных функций, по выделению интересующих полей, например, логин и пароль, заполнению их необходимыми данными, а после авторизации — поиск формы, используемой для выдачи комментариев, заполнение их и отправка требуемого комментария. Кстати, для всех перечисленных задач также существуют уже готовые продукты.

Теоретически робот способен самостоятельно зарегистрироваться, так как процесс регистрации хорошо алгоритмизирован.

Теоретически робот читает смс и «знает», что с ними можно делать. Для этого достаточно только наличие доступа к памяти телефона.

Теоретически робот способен распознать капчу и преодолеть ее, затратив серьезные вычислительные ресурсы.

Но *на практике все гораздо проще*[24] — для решения задач, сложных для робота, существует человек, который способен помочь сотням роботов, тем самым значительно упростив их разработку:

- специально обученный человек на сотнях различных интернет-ресурсах самостоятельно регистрирует роботов;
- специально обученный человек ставит задачу роботам в виде множества текстов комментариев, на базе которых роботы должны формировать «похожие» и размещать их на заданных ресурсах;
- специально обученные и организованные люди по заданию роботов распознают капчи и выдают результат. Сегодня эта платная услуга широко представлена в Интернете. При столкновении с капчей робот обращается за помощью на соответствующий платный ресурс, демонстрирует людям капчу, получает ответ, отвечает и идет дальше.

Вывод: теоретически люди могли бы поставить заслон роботам, но роботам, которым помогают такие же люди, поставить заслон практически невозможно.

Остается один не доступный (пока!) для роботов вид ресурсов — сайты, где комментарии могут оставлять только «свои», только те,

---

[24] Обратите внимание, эта фраза, «инфицировавшая» аудиторию научно-практической конференции, превратилась в мем (пример из практики авторов). Участники стали многократно повторять ее (реплицировать), распространяя этот информационный паттерн.

кто имеет личные атрибуты доступа к содержимому (логин и пароль). Однако и здесь есть свои уязвимости:

- порядочность людей, которые осуществляют регистрацию;
- защищенность компьютеров, где хранятся регистрационные данные (как-то уж так получается, что все серьезные БД регулярно появляются в открытом доступе);
- расплывчатость такого понятия, как «живой» человек. Например:

> **МОСКВА, 22 февраля — РИА Новости.** Приложение LivesOn, способное самостоятельно продолжить Twitter-микроблог пользователя после его смерти, будет запущено в марте текущего года, сообщает газета The Guardian.
>
> «Когда твое сердце остановится, ты продолжишь твитить» (When your heart stops beating, you'll keep tweeting), — гласит слоган приложения. Сервис основан на алгоритмах, которые анализируют онлайн-поведение пользователя — интересующие его темы, часто употребляемые слова, особенности речи.
>
> В случае смерти сервис продолжит генерировать записи от имени пользователя и даже публиковать ретвиты сообщений со страниц, которые он наиболее часто цитировал. Однако при регистрации в LivesOn пользователь все равно должен назначить человека, который получит контроль над его аккаунтом после смерти.

По нашим оценкам на сегодня до 10 процентов почтовых ящиков принадлежат умершим.

> И вот здесь опять появляется бессмертный Чичиков:
>
> *— Вы спрашиваете, для каких причин? причины вот какие: я хотел бы купить крестьян… — сказал Чичиков, заикнулся и не кончил речи.*
>
> *— Но позвольте спросить вас, — сказал Манилов, — как желаете вы купить крестьян: с землею или просто на вывод, то есть без земли?*
>
> *— Нет, я не то чтобы совершенно крестьян, —*

*сказал Чичиков, — я желаю иметь мертвых…*

*— Как-с? извините… я несколько туг на ухо, мне послышалось престранное слово…*

*— Я полагаю приобресть мертвых, которые, впрочем, значились бы по ревизии как живые, — сказал Чичиков.*

В некотором смысле в приложении к задаче астротерфинга получается, что кому принадлежат мертвые души, тому и принадлежит общественное мнение живых! Но при этом мертвых с каждым годом становится все больше и больше. И если им помогут роботы, то за ними вполне может быть будущее Интернета!

Возвращаясь к ответу на поставленные вопросы о возможности надежной защиты процесса формирования общественного мнения в сети Интернет, констатируем, что на сегодняшний день таких технологий нет и, более того, как было показано, и быть-то не может. Поэтому все попытки введения подобного вида законодательных инициатив — это проведение в жизнь дополнительных новых механизмов целенаправленного скрытого манипулирования общественным мнением. Серьезно к этому мнению относиться нельзя. Так, получается, что по нашему законодательству, человек, имеющий 100 тыс. роботов, легко может инициировать любую законодательную инициативу[25].

Таким образом, важнейшей задачей в данном случае является объяснение пользователям Интернета того печального факта, что настало время, когда ко всему, что происходит в Интернете, в части формирования общественного мнения, надо относиться с определенной долей недоверия.

Но в то же время не надо забывать, что в случае ограничения деятельности роботов Интернет теряет многие свои преимущества в ча-

---

[25] Концепция предусматривает создание условий для публичного представления предложений россиян по усовершенствованию российского законодательства с использованием сайта в Интернете. После этого идеи, которые получили поддержку не менее 100 тыс. граждан в течение года, рассматривают в правительстве страны. [«Концепция формирования механизма публичного представления предложений граждан Российской Федерации с использованием информационно-телекоммуникационной сети «Интернет» для рассмотрения в Правительстве Российской Федерации предложений, получивших поддержку не менее 100 тыс. граждан Российской Федерации в течение одного года». Утверждена Д. Медведевым 23 августа 2012 года]

сти автоматизации многих поисковых процессов. Сайт, который активно борется с роботами, теряет посетителей за счет того, что:

- отсеиваются многие поисковики, и в результате сайт становится менее известным;
- отсеиваются люди, не способные распознать капчу;
- отсеиваются полезные в определенном смысле этого слова роботы, которые по заданию пользователя проводят предварительную разведку для своего хозяина на предмет: а стоит ли человеку посещать этот сайт.

### *3.1.3. Лаборатория виртуальных специалистов*

Понятно, что все-таки люди больше доверяют людям, способным, в отличие от робота, принимать решения в нестандартных ситуациях и оперативно действовать согласно им. Чтобы создать интеллектуального робота, требуется время и другие затраты на его подготовку для проведения специальных действий в ходе информационной операции. Поэтому надежными исполнителями по-прежнему остаются специально нанятые посетители, которые за определенную плату или по идейным соображениям периодически заходят на заданное множество сайтов и выполняют оговоренные с заказчиком действия. Они регистрируются под несколькими никами и массово продвигают определенную идею[26].

> В Сети рекрутинговые интернет-ресурсы для троллей содержат типовые объявления:
>
> «На постоянную работу требуется специалист по работе в социальных медиа (фейсбук, вконтакте, твиттер, ЖЖ и др. блоги). График работы гибкий/свободный. Оформление по ТК. Обязанности: работа в комментариях — требуется оперативная реакция на изменяющуюся ситуацию в блогах, способность поддержа-

[26] В открытом доступе имеются видеосюжеты, популяризирующие данную проблему — например, видеоматериал под названием «Спецслужбы: троллинг в сети» // www.youtube.com/watch?v=iOoa7Xf47ZE.

ния дискуссии и перенаправление ее в требуемое русло; создание виртуалов, написание постов от их имени, раскрутка; мониторинг социальных медиа. Требования: опыт использования социальных сетей и блогов как продвижение чего-либо, понимание механизма их работы и психологии пользователей. Знание популярных блогеров, их основных позиций приветствуется».

Интересно, что такой способ используется даже на государственном уровне. Он хорош тем, что позволяет довольно быстро собрать эффективно действующую армию информационных бойцов.

Например, в 2010 году Израиль объявил призыв добровольцев в своеобразную «армию блоггеров», которой предстоит выйти на поля интернет-сражений для борьбы с антисионизмом. Руководит проектом министерство абсорбции Израиля[27]. Согласно опубликованному министерством объявлению, оно приглашает израильтян, владеющих каким-либо иностранным языком, представлять Израиль в антисионистских блогах на английском, французском, испанском и немецком языках. Также представляют интерес блоггеры, пишущие на русском и португальском.

Более того, «Всемирный совет еврейского студенчества (World Union of Jewish Students, WUJS) нашел способ организовать эффективную борьбу за мировое общественное мнение в Интернете. В начале войны с «Хезболлой», когда Израиль, как всегда в таких случаях, начал проигрывать информационную войну, WUJS выступил с новой инициативой: создать в интернете активное произраильское сообщество, которое могло бы в режиме реального времени реагировать на появляющиеся в сети антиизраильские материалы. Инициативу поддержал отдел по связям с общественностью израильского МИД, а техническое средство реализации идеи обеспечила израильская компания по разработке программного обеспечения: была создана программа под названием «Интернет-мегафон», позволяющая быстро оповестить всех желающих о появляющихся в сети онлайновых опросах, статьях и форумах, связанных с Израилем.

[27] См.: www.dni.ru/tech/2009/1/20/157540.html.

Добровольцы WUJS ежедневно ведут мониторинг и сообщают обо всех интернет-публикациях, которые, по их мнению, требуют реакции израильской публики. Отныне внести свой вклад в информационную войну за интересы Израиля может любой желающий»[28].

Соединенные Штаты в ноябре 2009 года сформировали аналогичное интернет-подразделение — «Команда по цифровым внешним контактам». Данное подразделение предназначено для противодействия антиамериканской дезинформации в Интернете за рубежом. В ее задачу входит присутствовать в Интернете — в чатах, на популярных интернет-сайтах и в блогах, рассказывая об американской политике, исправлять ошибки, которые имеют место, а также отсылать людей «к правильным документам».

Так все же, какие специальные мероприятия в контексте перечисленных в разделе 1.1 типовых задач способны выполнять люди, выступающие акторами информационной операции в телекоммуникационной среде, а какие задания — виртуальные специалисты-[ро]боты? Сравним:

| **люди** | **[ро]боты** |
|---|---|
| сокрытие и/или подмена адреса источника размещаемых материалов | сокрытие и/или подмена адреса источника размещаемых материалов с помощью подключаемого к [ро]боту продукта, работающего через динамически изменяемый прокси-сервер |
| защита размещаемых материалов от удаления | защита размещаемых материалов с помощью автоматической генерации текстов похожего содержания |
| оперативная «раскрутка» ресурсов | оперативная «раскрутка» ресурсов, благодаря размещению на открытых форумах ссылок на заданные ресурсы |
| автоматическое преодоление защиты от роботов | автоматическое преодоление защиты от роботов для тех ресурсов, на которые [ро]бот был предварительно настроен, или преодоление защиты за счет парсинга сайта и передачи капча-фильтра на распознавание человеку (дежурному оператору) |

[28] См.: www.securitylab.ru/news/273278.php.

| | |
|---|---|
| оперативное создание или нахождение ресурсов для размещения мультимедийного контента | нахождение ресурсов по ключевым словам и словосочетаниям (функции поисковика) |

Множество действий, доступных виртуальному специалисту, — это также:

– рассылка сообщений-напоминаний, аудио, видеоматериалов в рамках утвержденного графика работ;

– регулярный сбор материалов с заданных источников в сети Интернет, обработка (реферирование), хранение;

– сбор аудио-, видеоинформации с WEB-камер и других технических средств;

– ведение новостной ленты (кто и когда включил/выключил компьютер, отправил сообщение, сколько раз обратился к той или иной базе данных и т.п.);

– контроль технологических процессов;

– ведение журналов аудита;

– разработка предсказаний; предупреждение о возможной опасности;

– акцентирование внимания руководства на нетипичных ситуациях;

– ответы на вопросы с использованием всего спектра разнородной информации (текст, аудио, видео), обсуждение сформулированной человеком проблемы[29]; при этом диалог может вестись как

---

[29] Примеры:

Витализация окружающей среды // http://vechno.info;

Русский онлайн чатбот с открытым обучением // http://chatbot.tw1.ru;

Робот — помощник по сайту // http://mibot.ru/robotface.php?id=16;

Робот — подсказчик и собеседник // www.zabaware.com/assistant/index.html;

Видеоаватар // — http://sheepridge.pandorabots.com/pandora/talk?botid=dee0624a5e345abd&skin=iframe-voice;

Роботы, аватары, боты // www.chatbots.org;

Автороботы // www.sitepal.com;

Робот-ребенок // www.vesti.ru/doc.html?id=532251;

Встреча двух чатботов // www.bbc.co.uk/russian/multimedia/2011/09/110909_chatbots_argue.shtml.

в виде текстовых сообщений, так и голосом и на уровне видеореплик (так, например, браузер Google Chrome позволяет вводить запросы и реплики голосом с высоким качеством распознавания).

Одним из перспективных направлений для решения перечисленных выше функциональных задач является применение специального программного обеспечения, интерфейс которого идентичен поведению реального пользователя сети. Понимаем, что *виртуальный специалист* — это программный модуль, написанный на языке web-программирования, например, php. Модуль исполняется на сервере и способен использовать любые доступные ему как программному модулю ресурсы. Особенностью модуля является наличие всех тех механизмов, которые пожелает встроить в него разработчик.

Благодаря перечисленным особенностям и функциональным возможностям, виртуальные специалисты становятся все более востребованными. Создание виртуальных специалистов возможно практически в любой предметной области. Им находится место и в качестве бойцов на информационном поле боя. Таким путем идут в США, например, в 2011 году контракт стоимостью 2,76 млн. долл. достался зарегистрированной в Лос-Анджелесе компании Ntrepid. Цель контракта — разработать специальное программное обеспечение (ПО) для проведения проамериканской пропаганды через различные социальные сети и блоги. «По словам представителя Centcom Билла Спикса, данная технология позволит вести секретную блогерскую деятельность на зарубежных сайтах. В частности, такое ПО поможет противодействовать распространению пропаганды за пределами США, кампаниям по дезинформации или хакерским атакам… в рамках этой программы будут создаваться вымышленные виртуальные личности в Twitter, Facebook и других соцсетях, которые по всем внешним признакам должны казаться обычными пользователями из разных стран и иметь убедительную легенду. Под контролем одного военного будет до десяти онлайн-персонажей. Единый пункт управления расположится на базе ВВС США Макдилл близ Тампы (Флорида) и будет функционировать в круглосуточном режиме. Работать в нем будет до 50 операторов. Также предусмотрена система защиты от разоблачения. Отличить бот от настоящего пользователя будет еще более затруднительно,

поскольку фэйловым аккаунтам замаскируют IP-адрес. Это позволит создать видимость того, что посты отправляются реально существующими пользователями из разных стран»[30]. По словам Билла Спикса, пресс-секретаря Центрального командования ВС США, данная система будет использоваться для общения на арабском, фарси, урду, пушту и других языках. Данный проект позволит американской армии не только получать оперативную информацию от пользователей о текущем состоянии в регионе, но и добиться «эффекта ложного единодушия» в онлайн-дискуссиях.

Для виртуального специалиста вполне реально сформулировать цели, задачи и правила поведения — это, в первую очередь, постоянное расширение знания в той предметной области, за которую он отвечает, а во вторую — набор правил, согласно которым он функционирует, зафиксированные в его функциональных обязанностях. Виртуальный специалист должен постоянно актуализировать данные, информацию, знание. Он обязан активно обучаться в части решения классической задачи по распределению ресурсов и заданий.

Рассмотрим возможности виртуальных специалистов по обучению и переобучению. При этом будем помнить о том, что, поскольку виртуальные специалисты работают в условиях анонимности, то желательно, чтобы они как можно больше походили на людей, но превосходя их в точности, скорости и масштабности действий.

Обучение виртуального специалиста предполагает организацию работ по двум направлениям:

– обучение материалам, которые, согласно оперативному сценарию, должны быть доставлены на интернет-ресурсы;

– обучение общему поведению и такому языковому интерфейсу, которые бы способствовали повышению веры посетителей ресурсов в источник сообщения.

Доверие со стороны объекта управления к источнику мультимедийного контента, в данном случае к виртуальному специалисту, во многом определяется возможностью его причисления к категории «своих». Исследуем направления работ по обучению и переобучению виртуального специалиста в направлении повышения к

[30] См.: www.rbcdaily.ru/2011/03/21/world/562949979906266.

нему доверия со стороны других субъектов. Основой любого доверия всегда является понимание одного субъекта другим, которое, в свою очередь, строится на базе созданного информационного образа. Создать информационный образ любого субъекта — значит воссоздать его систему отношений, т.е. проявить его опыт на данный момент. Если же известны правила, по которым данный субъект осуществляет познание мира, то появляется возможность создания устойчивого информационного образа, способного к обучению, к самостоятельному познанию мира. В том случае, если измерение отношения осуществляется не однозначно и не двузначно, а многозначно, то система отношений превращается в систему предпочтений. Часть предпочтений задаётся на этапе создания виртуального специалиста, другие формируются в ходе проведения информационной операции.

Система предпочтений, правила познания, индивидуальная манера поведения в совокупности образуют основу любого информационного образа, в частности информационного образа виртуального специалиста. К этому образу можно добавить биографию, имя, наиболее характерные истории из жизни, чтобы он выглядел более реалистично. Чтобы информационный электронный образ был похож на «живой», он должен состоять из элементов, способных к взаимозависимой деятельности. Он должен содержать в себе своё алгоритмическое самоподобие в виде множества интегрированных компонент, способных к различным видам взаимозависимой деятельности[31].

Введение понятия «алгоритмическое самоподобие» влечет за собой переход к процессам, протекающим по структурам, образованным на базе отношений. Именно процессы определяют, какие сиюминутные информационные образы будут проявлены, а какие нет. Но сами процессы, в свою очередь, также поддаются классификации, и каждый процесс имеет свою структуру, т.к. сам по себе состоит из последовательности различных операций. Например, в объектно-ориентированном программировании элементарными

[31] *Расторгуев С.П., Токарев Р.С.* О направлении развития самообучающихся механизмов сети Интернет // Информатика и образование. 2009. №1. С. 79–86.

составляющими процесса являются методы. В нашем исследовании к методам можно отнести возможности:

– изменения размеров;

– изменения месторасположения;

– изменения компонент объекта;

– добавление новых компонент;

– удаление компонент;

– порождение дополнительного образа объекта, освещающего (описывающего) данный объект под другим углом зрения.

Перечисленные методы связаны с перемещением объекта в пространстве и времени и с изменением компонент самого объекта.

Информационный образ виртуального специалиста проявляется через естественный язык, который понимают пользователи Интернет, а также искусственные языки среды Интернет, в частности язык разметки гипертекстов html, который они обязаны понимать, когда попадают на тот или иной интернет-ресурс. Язык среды используется для создания текстов.

Среда, в которой функционирует виртуальный специалист, структурируется наличием:

– ключевых слов для текстов, циркулирующих в этой среде;

– связей между ними;

– эмоциональной окраской, как всех текстов, так и отдельных предложений и даже слов;

– наличием определенной комбинации тегов языка разметки гипертекстов. С помощью тегов указывается значимость того или иного слова для данного текста. Подобного рода значимые слова выделяются в тексте с помощью т.н. <meta> тега и тегов разметки текста типа создания заголовков разного уровня, подчеркивания, включения жирного шрифта, гиперссылок. Виртуальному специалисту достаточно «взглянуть» на содержимое названных тегов, и он уже «понимает», о чем идет речь.

Итак, задача виртуального специалиста при общении с человеком или с сайтом заключается в переводе полученных текстов на свой внутренний язык, причем перевод этот должен начинаться с оценки эмоциональной окраски и удаления избыточности. То, что останется, и будет языковой средой.

**Индивидуальная манера поведения** виртуального специалиста формируется на основе множества его бесед с пользователями ресурсов сети Интернет. Беседы строятся на предпочтениях. В беседах, как правило, присутствуют любимые слова и выражения и отсутствуют нелюбимые. Беседы с теми, к кому хорошо относятся, проходят совсем не так, как с тем, кого опасаются, — другой сценарий беседы. Если в основе первого сценария лежит выбор такого сообщения, которое заинтересует и позволит увеличить продолжительность беседы, то во втором случае сообщения выбираются так, чтобы время беседы сокращалось, а сама беседа ограничилась получением только нового знания о возможных опасностях.

**Правила познания.** В данном случае рассматриваются способности виртуального специалиста правильно решать те или иные задачи независимо от способности к т.н. познанию. Если задача того или иного уровня решается информационной системой (виртуальным специалистом), значит, система (виртуальный специалист) соответствует этому уровню познания.

Предлагается выделить следующие семь уровней познания:

На первом уровне система способна давать ответы на вопросы только на основе содержания имеющегося у нее текста. Если, например, системе известен текст: «*Началась война*!», то система должна уметь отвечать правильно на вопрос типа: «*Что началось*?» Существуют различные алгоритмы решения данной задачи. Например:

– на базе фрейма, содержащего все места, которые посещает субъект, с перечнем его возможных действий;

– поиск в хранящихся текстах предложений, содержащих в себе вопрос или большую часть вопроса, и объединение их в текст ответа с учетом синтаксиса языка. В данном случае системе совсем необязательно уметь анализировать текст и понимать, что такое «война», и знать, что она началась, — это должен знать тот, кто задал вопрос. Главное, чтобы субъект, задающий вопрос, был удовлетворен ответом. На данном уровне важнейшей задачей является задача определения расстояния не только между различными текстами (в этой части достаточно существующих решений), но и между неизвестным вопросом и известным ответом, который и должен быть поставлен в соответствие этому вопросу.

Для определения индивидуального стиля поведения (разговора) виртуальному специалисту вполне подойдут адаптированные к текстам естественного языка алгоритмы самообучения на базе гибели и рождения элементов[32]. В магистерской диссертации Р.С. Токарева (МФТИ, 2009 г.) было показано, что для решения данной задачи вполне достаточно всего четырех видов элементов с такими базовыми операциями, как удалить слово, добавить слово, заменить слово, переставить слова.

На втором уровне у системы имеются правила пополнения текстов и правила исключения отдельных фрагментов текста. Здесь возможны два пути модификации исходных текстов:

– их действительная модификация (включение/исключение);

– расширение (сужение) для информационной системы возможностей по доступу к текстам, принадлежащим другим информационным системам.

Наличие подобных правил может стать основой механизма самообучения, т.к. при определенных условиях эти правила задают направление развития информационной системы. Все ответы готовятся на базе различных текстов. Неоднократная отрицательная оценка ответа различными собеседниками является достаточным основанием для удаления текста, понижения его статуса. Положительная оценка приводит к повышению статуса текста, что, в итоге, способствует его выбору в случае наличия конкуренции среди текстов, претендующих на роль генератора ответа.

На третьем уровне при ответе на вопрос система должна уметь оперировать историей вопросов-ответов. Например, отвечая на вопрос «Согласны?», система должна уметь посмотреть историю диалога и расширить вопрос текстами о том, с чем предполагается согласиться. Как глубоко уходить в историю, на сколько шагов, определяется собеседником. В случае рядовой беседы людей друг с другом ими обычно учитываются от 3 до 7 последних высказываний.

Повышению эффективности функционирования системы на третьем уровне может способствовать карта взаимосвязи текстов,

---

[32] *Расторгуев С.П.* Философия информационной войны. М.: МПСИ, 2002.

страниц сайтов, состоящая из матрицы следования текстов (вопросов/ответов друг за другом) и матрицы расстояний между текстами.

На четвертом уровне система должна иметь не только тексты, на базе которых строится ответ, но и информацию о конкретном субъекте, являющемся источником вопросов-сообщений, о цели и правилах общения. Четвертый уровень предполагает возможность интимного общения, опирающегося на знания о собеседнике. Четвертый уровень хотя бы без частичного знания системы предпочтений собеседника невозможен. Знания о собеседнике могут быть собраны информационной системой (виртуальным специалистом) в процессе регулярных бесед с собеседником. Эти знания представляются в виде соответствующей модели, которая позволяет рассчитывать такие характеристики, как:

– отношение собеседника к данному виртуальному специалисту. Отношение можно попытаться оценить через время беседы, через число положительных оценок, выставленных собеседником виртуальному специалисту за беседу, через число непосредственных обращений;

– интересы собеседника. Интересы формируются на базе частотного словаря употребления ключевых слов — это и есть интересуемые проблемы;

– отношение к интересующим проблемам. Это отношение формируется путем сбора данных об эмоциональной окраске речи собеседника применительно к интересующим проблемам;

– адекватность собеседника, в том числе истинность или ложность его текстов. Подобное возможно, если собирать оценки других посетителей на высказывания виртуального специалиста, которым его научил конкретный собеседник.

На пятом уровне система должна уметь оценивать истинность или ложность того или иного сообщения, в том числе с учетом того, кто автор этого сообщения. Умение оценивать истинность или ложность предполагает наличие памяти о происходящем, о том, чем закончилось то или иное высказывание.

На шестом уровне система должна уметь самостоятельно достигать целей, ради которых она существует. Изначально цели должны быть сформулированы создателем конкретного виртуального специалиста.

Цели могут быть самыми разными: от максимально возможного продления времени существования себя в беседе до получения конкретного результата от собеседника. Выдача и получение соответствующих текстов становятся возможными только тогда, когда данные тексты есть у виртуального специалиста, и для него возможен сценарий беседы, приводящий к требуемому результату.

В общем виде достижение целей предполагается путем модификации правил, в соответствии с которыми осуществляется изменение статуса отдельных текстов. При этом процессы, направленные на достижение целей, должны протекать не только во время беседы, но и в «спящем» режиме. Суть этих процессов заключается, во-первых, в установлении связей между имеющимися текстами на предмет достижения поставленных целей, а во-вторых, в повышении структурированности текстов за счет внесения в текст гиперссылок, раскрывающих смыслы как отдельных слов, так и предложений.

Для седьмого уровня одного текста на естественном языке недостаточно. Здесь речь уже идет о распознавании изображений, голосов и т.п.

Уровни познания расположены в порядке расширения возможностей познания. С одной стороны, они следуют друг из друга, позволяя последовательно возводить здания искусственной жизни, получая на каждом этапе определенный практический результат. С другой стороны, многие задачи (логический вывод, построение трехмерных образов, синтаксический анализ, теория перевода, механизмы самообучения и т.п.) в рамках названных уровней познания уже решены до вполне приемлемых результатов.

Исследуя уровни познания, мы показали одно из направлений совершенствования виртуальных специалистов. Второе не менее важное направление — это повышение привлекательности виртуального специалиста. Это важнейшее направление, так как привлекательность напрямую связана с верой в передаваемое информационное сообщение.

Введем функцию определения мощности множества — μ. Обозначим через $\mu(T_j)$ мощность множества $T_j$. Через $t_н$ — множество истин, ставших известными субъекту i в ходе беседы с некоторым не представившимся субъектом j, которого надо узнать в ходе бе-

седы. Тогда для субъекта i вероятность, что он беседует именно с субъектом j, могла бы быть оценена по формуле:

$$P = \mu(t_н)/ \mu(T_j).$$

Но реально субъект i не всегда может знать все множество истин $T_j$. Это множество истин (в случае человека) может быть вообще не перечислимым, т.е. не всегда возможно даже посчитать мощность множества $T_j$, а значит, наверняка узнать собеседника. Так, предлагаемая формула верна только для случая, когда речь идет об узнавании такого виртуального специалиста, все тексты которого известны субъекту i.

Любой субъект может реализовывать операцию узнавания только на базе тех данных, что у него есть. Пусть субъект i ранее в ходе бесед с субъектом j накопил определенные знания о субъекте j в виде множества истин $t_з$. Тогда вероятность, что в данный момент он беседует с j, можно оценить так:

$$P = \mu(t_н \cap t_з)/ \mu(t_з).$$

Признаем, что узнавание собеседника (робота или человека) идет не по глубине мысли, а по набору присущих субъекту любимых слов и словосочетаний. Причем таких слов и словосочетаний, именно любимых, не так уж и много. Поэтому можно усилить последнюю формулу, заменив в ней $t_з$ на $t_{з`}$, где $t_{з`}$ — множество любимых слов и словосочетаний.

Привлекательность для виртуального собеседника — это умение притягивать к себе посетителей. Повышать привлекательность — значит повышать умение привлекать к себе внимание. Виртуальный специалист делает это целенаправленно и алгоритмически обоснованно. И он обязан это делать регулярно, чтобы оставаться востребованным.

Если измерять качество общения строго формально, то на первый план выходит именно оригинальность и новизна сказанного и желание человека слушать данного конкретного виртуального специалиста. Как только собеседники «перелили» друг другу свое содержание (доступное для понимания друг другом) и вышли на соответствующий баланс, как в их отношения вкладывается однообразие, которое затем приводит к раздражению, и на этом взаимодействие заканчивается. Психологи подобное состояние называют информационной опустошенностью.

На основании изложенного выдвинем следующие требования к оценке привлекательности:

1. Привлекательность тем выше, чем меньше пустых диалоговых квантов в каждый фиксированный временной интервал общения.

2. Привлекательность тем ниже, чем меньше пересечение диалоговых квантов каждого фиксированного временного интервала общения с базой знаний посетителя.

С одной стороны, виртуальному специалисту надо что-то говорить, а с другой — нельзя говорить то, что неинтересно посетителю. Важно правильно найти точку равновесия. Кроме того, для виртуального специалиста непростой задачей является понимание того, в чем заключаются интересы посетителя, о чем целесообразно с ним разговаривать?

Перейдем к формальной постановке задачи.

Обозначим через $K_{i,a}(t)$ — множество диалоговых квантов, в которых виртуальный специалист *a* принимал участие вместе с i-м посетителем до момента времени t;

$K_i(t)$ — множество диалоговых квантов, в которых принимал участие i-й посетитель (эти кванты могут быть из бесед данного посетителя с любыми другими посетителями, в том числе другими виртуальными специалистами-роботами) до момента времени t;

$\Delta t$ — фиксированный временной интервал. Предлагается считать, что вся беседа состоит из последовательности таких интервалов $\{\Delta t_j\}$.

Тогда, оценку привлекательности попробуем собрать из вероятности, что виртуальный специалист попадет в тему посетителя, и вероятности, что очередной фиксированный временной интервал беседы не будет пуст.

$P_1 = \mu(K_i(t) \cap K_{i,a}(\Delta t_{j+1}))/\mu(K_{i,a}(\Delta t_{j+1}))$ — оценка вероятности попадания в тему посетителя;

$P_2 = \mu(K_{i,a}(\Delta t_{j+1})) — \mu(K_{i,a}(\Delta t_j) \cap K_{i,a}(\Delta t_{j+1}))/ \mu(K_{i,a}(\Delta t_{j+1}))$ — оценка вероятности, что новая последовательность квантов будет «лучше» предыдущей.

Итого:

$P_{прив} = P_1 \bullet P_2$.

$P_{прив} = \mu(K_{i,}(t) \cap K_{i,a}(\Delta t_{j+1}))\ (\mu(K_{i,a}(\Delta t_{j+1})) — \mu(K_{i,a}(\Delta t_j) \cap K_{i,a}(\Delta t_{j+1})))/ \mu(K_{i,a}(\Delta t_{j+1}))^2$.

Данная формула очень важна для функционирования виртуального специалиста, она указывает цель в его самообучении, тем самым делая его существование целесообразным, а его самого — привлекательным для посетителей интернет-ресурсов.

В ходе любой беседы, используя эту формулу, виртуальный специалист первоначально подготовит несколько реплик, но прежде чем сказать, просчитает все подготовленные реплики на предмет собственной привлекательности, выберет лучшую и только потом выдаст ответ.

Обосновав основные направления самообучения, которые на уровне моделей должны быть встроены в процессы, ответственные за обучение и переобучение, перейдем к основным компонентам данной подсистемы.

Данная подсистема должна включать в себя следующие блоки (рис.3.1.3.1):

- обучение диалогу в виде множества взаимозависимых реплик, которые позволяют настроиться собеседникам друг на друга;
- обучение историям[33], которые может рассказать виртуальный специалист о себе или о других (например, собственная биография, истории из жизни);
- обучение «любимым» фразам и индивидуальной манере подачи материала. Под любимыми фразами в данном случае понимаются выражения (диалоговые реплики, отдельные фразы, слова и словосочетания, придающие индивидуальность — по этим фразам конкретный виртуальный специалист всегда может быть идентифицирован);
- обучение заданиям. Под заданиями понимаются действия виртуального специалиста в виде размещения соответствующего материала в заданной форме на указанных интернет-ресурсах;
- хранение всех реплик диалогового взаимодействия;

---

[33] Истории — тексты на естественном языке более одного предложения, описывающие то или иное событие, проблему, мысль.

- корректировка диалоговых форм и реплик с целью исправления ошибок, допущенных виртуальным специалистом в ходе информационного взаимодействия с посетителями сайтов и процесса обучения.

В ходе информационного взаимодействия виртуальный специалист может использовать все перечисленные блоки, т.е. любую входную реплику любого посетителя он должен проанализировать и активизировать соответствующие блоки. При активизации возможны ошибки следующего характера:

- активизирован не тот блок, который является более правильным в качестве выходного ответа;
- блок выбран правильно, но внутри выбранного блока выбор ответа оказался неверным.


РИСУНОК 3.1.3.1. *Общая функционально-структурная схема подсистемы обучения и переобучения*

База данных словарей и заданий виртуального специалиста должна состоять из взаимоувязанных таблиц, содержащих словарь виртуального специалиста, словарь синонимов, множество взаимоувязанных реплик по типу вопрос/ответ, множество взаимоувязан-

ных историй, множество характерных фраз, определяющих индивидуальную манеру поведения виртуального специалиста, множество выданных ему заданий.

## 3.2. Практикум «воина сети Интернет»

### *3.2.1. DDoS атаки*

Начнем с текущих новостей:

*«*Второго июня 2013 года было сообщено, что телеканал Russia Today первым из новостных ТВ мира преодолел отметку в 1 миллиард просмотров на YouTube. Сразу же на следующие сутки сайт телеканала Russia Today RT.com подвергся DDoS-атаке[34]. Хакерской атаке подверглись также другие сайты Russia Today, в том числе actualidad.rt.com, arabic.rt.com и russian.rt.com. Представители телеканала заверили, что атака не повлияла на передачу новостей о ходе судебного процесса над информатором сайта Wikileaks Брэдли Мэннингом, а также об акциях протеста в Турции. Ответственность за атаку взяли на себя представители анонимной хакерской группировки AntiLeaks, которая и ранее предпринимала DDoS-атаки на сайт Russia Today*»*.

*«*В ночь с 13 на 14 августа была организована DDoS-атака на официальный сайт партии »Справедливая Россия» — *www.spravedlivo.ru.* Злоумышленники использовали методы мощного HTTP-флуда и параллельного SYN-флуда. Атака велась с тысяч различных IP-адресов. При попытке блокирования IP-адресов, с которых происходили обращения к серверу, DDoS-атака тут же возобновлялась с новых. Специализированное защитное оборудование (CISCO) дата-центра, в котором размещен сервер «Справедливой России», не справилось с атакой. Итогом стало полное выве-

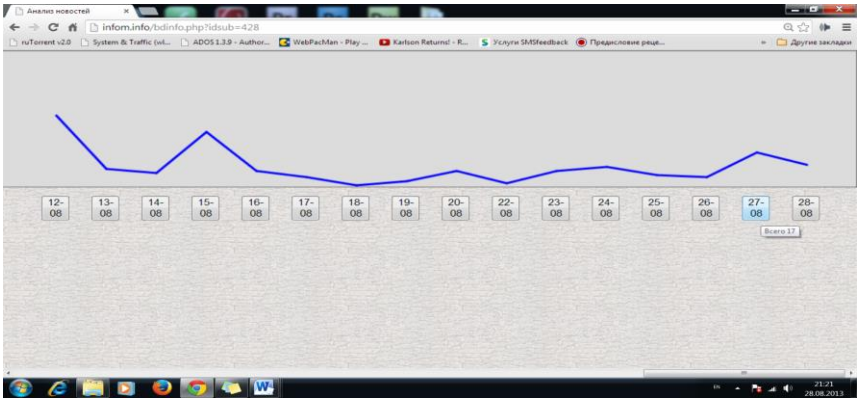
[34] DDoS-атака производится при помощи множества зараженных злоумышленником компьютеров, посылающих запросы по определенному адресу в интернете, что приводит к перегрузке и, в отдельных случаях, недоступности ресурса.

дение сервера из доступа. В настоящее время DDoS-атака продолжается. Сайт партии не работает».

«Китайский сегмент интернета 25.08.2013 столкнулся с мощной DDoS-атакой, направленной на доменные серверы, обслуживающие доменную зону .cn. Как сообщил китайский интернет-центр CNNIC (China Internet Network Information Center), атака была крупнейшей в истории чайнета и сказалась на работе множества сайтов, даже из числа тех, против которых никаких хакерских действий не было предпринято.

Согласно данным мониторинга, атака стартовала примерно в полночь по пекинскому времени 25.08.2013 и к 4 часам утра она достигла своего пика. На протяжении 5–6 часов многие китайские сайты оказались недоступны, так как пользовательские компьютеры не смогли получить данные о местоположении серверов по доменам. Мощность атаки значительно снизилась к 10 часам утра по местному времени»[35].

Приведенные примеры DDoS-атак — это то, что мы видим на поверхности информационного поля боя. На рисунке ниже представлен график частоты упоминания в новостях термина DDoS атака.




Почему мы начали описание специальных действий именно с DDoS-атак? В Интернете для любых ресурсов немало и других

[35] См.: www.cybersecurity.ru/net/180123.html.

угроз. Сайт могут взломать, деньги с банковских счетов отправить по другому неизвестному хозяину направлению, вирусная атака поставит сайт на контроль, да еще не только сайт, но и пользователей, которые его посещают. Угроз в сети немало. Но есть угрозы, как бы, ручной работы, а есть угрозы — поставленные на промышленную основу. Жулик, потративший год, на проникновение к базам данных какого-либо банка с целью наживы, остается просто жуликом, а не участником информационной операции.

Информационная операция — это совокупность взаимосвязанных действий, производство которых поставлено на конвейер. Например, вирус Stuxnet — это оружие промышленного изготовления, на сегодняшний день имеющее уже десяток модификаций. DDoS-атаки — это такое же оружие. Но, как и любое оружие, DDoS-атаки бывают разные. Есть примитивное оружие, когда злоумышленник запускает у себя конкретную программу, которая в цикле осуществляет доступ по заданному IP-адресу и блокирует его, забивая своими обращениями. Подобный злоумышленник ловится по собственному IP и блокируется, а его адрес попадает еще и в черный список адресов Интернета.

Есть более изощренный злоумышленник, который, осуществляя атаку со своего компьютера, проводит ее через анонимайзеры и соответствующие вебсервера. Большого количества адресов на долгое время таким образом тоже не собрать.

Здесь мы говорим о специально подготовленном механизме для DDoS-атак. Это ботсети. Классическим примером информационного оружия в технической сфере являются именно ботсети (ботнеты). **Ботнет** (англ. *botnet*, произошло от слов *ro**bot*** и ***net**work*) — компьютерная сеть, состоящая из хостов и компьютеров пользователей с установленным на ней специальным программным обеспечением (бот), управление которым осуществляется с хостов.

Масштабы и возможности.

В октябре 2010 г. издание Вебпланета (http://webplanet.ru) сообщило, что голландская полиция захватила 30-миллионный ботнет. Только за один месяц скрытого наблюдения за его активностью сеть пополнилась тремя миллионами заражённых машин. Ботнет является частью сети Bredolab.

Bredolab — это крупное семейство троянских программ, проникающих на компьютеры пользователей через вредоносные приложения к почтовым сообщениям или заражённые сайты. Получив контроль над компьютером, Bredolab загружает на него другие вредоносные программы. Хорошо известно о связи Bredolab со спамерскими рассылками и лже-антивирусами. В ходе расследования были выявлены 143 контролирующих сервера. В ходе уничтожения ботнета контролирующие сервера были отключены от Сети. Пользователям зараженных компьютеров при очередном входе в систему автоматически были выданы сообщения с информацией о том, каким образом они могут очистить свои машины.

Структура ботнета.

Ботсеть включает в себя центр управления, из которого поступают команды, и множество зараженных компьютеров. Понятно, что если центр выявлен, то сеть ставится под контроль и либо используется противником, либо уничтожается.

Боты (зараженные компьютеры) получают из центра команды для выполнения. Команда состоит из перечня действий и времени выполнения, типа:

– зайти на сайт Z (время: от $T_1$ до $T_2$);

– послать письмо по адресу X (время: от $T_1$ до $T_2$);

– снимать информацию из папки P, с клавиатуры и т.п. и помещать в хранилище M (время: от $T_1$ до $T_2$);

– отправить собранные данные в хранилище M по адресу X (время: от $T_1$ до $T_2$);

– внедрить зараженный код $D_k$ по заданным адресам $\{X_i\}$ (время: от $T_1$ до $T_2$);

– получить данные D (например, $D_k$) по адресу X и хранить в месте M (время: от $T_1$ до $T_2$);

– сменить адреса центра управления $\{X_i\}$ на адреса $\{Y_i\}$ (время: от $T_1$ до $T_2$);

– сменить ключ шифрования (время: от $T_1$ до $T_2$);

– доложить о выполнении команды (время: от $T_1$ до $T_2$);

– «уснуть» (на время: от $T_1$ до $T_2$);

– самоуничтожиться (время: от $T_1$ до $T_2$) и т.п.

Команды при передаче ботам шифруются криптографическим алгоритмом с открытым ключом RSA. Открытый ключ имеется у каждого бота, закрытый только в центре управления. Таким образом осуществляется защита ботов от захвата потенциальными противниками.

Существуют ботнеты с фиксированным центром управления и с динамически меняемым центром. Динамически изменяемый центр управления создается самими ботами, которые путем генерации случайной последовательности, например, применяя отечественный ГОСТ или американский DES к некоторому тексту, вырабатывают последовательность адресов $\{X_i\}$, на которых пытаются разместить центр управления в виде команд D. В случае удачного заражения компьютера, боты в дальнейшем используют его для связи с владельцем сети. Владелец ботнета, зная правила генерации случайной последовательности и выставляемый признак заражения, всегда может связываться с ботами через любой из компьютеров центра управления, которые постоянно меняются. Причины изменения:

- выявление зараженного компьютера антивирусом;
- выявление зараженного компьютера из-за попадания в руки потенциального противника бота с адресами;
- заражение новых компьютеров.

Еще раз заострим внимание: ботнеты — это атакующие резервы, обладающие множеством «незасвеченных» IP-адресов. Это IP-адреса потенциальных посетителей из различных стран мира. Закрыться от них системой защиты — значит выключить себя из сети.

А теперь самый важный момент информационной борьбы за ресурсы: сегодня практически каждый программный продукт, установленный на компьютере пользователя, а особенно лицензионный[36], постоянно связывается со своими разработчиками. Разработчики всегда способны переориентировать этот продукт на решение любых других актуальных для текущего момента задач, подгрузив ему блок соответствующих команд. Образно говоря, владельцы лицензионного Windows образуют официальный хорошо организованный «ботнет» под руководством единого управля-

[36] Не лицензионный, т.е. «крякнутый» софт, как правило, лишен возможности взаимодействия со своим разработчиком.

ющего Центра. То же самое можно сказать и про любое другое программное обеспечение. Так что в случае информационной баталии компьютер каждого пользователя Интернет потенциально может стать местом сражения перенастроенного установленного на нем программного обеспечения различных производителей.

### *3.2.2. Промышленная генерация информационных материалов*

Классическая система управления любым объектом, кроме подсистемы мониторинга состояния объекта, всегда предусматривает наличие подсистем, отвечающих за решение таких задач, как подготовка соответствующих управляющих воздействий. В данном случае, это мультимедийный контент по заданной проблематике и доставка этого контента до объекта воздействия. В данном разделе рассмотрим основные принципы и варианты подготовки мультимедийного контента в сети Интернет по заданной проблематике.

В качестве основных принципов предлагаются следующие:

– подготовка мультимедийного контента в режиме «реального времени» на базе имеющихся типовых заготовок;

– контент может иметь как текстовую (форматы txt, doc, docx, pdf), так и видео- (форматы: mp4, flv) и аудио- (форматы: mp3) форму.

Исходя из типовых задач информационной операции, перечисленных в главе 1, при подготовке мультимедийного контента необходимо соблюдать следующие требования:

*Требование Т1* — возможность формирования текстовых материалов в заданном стиле, по образцу текстов конкретного автора;

*Требование А1* — возможность формирования аудиоматериалов на заданном аудиофоне (шум моря, аэропорт, улица, помещение с людьми, помещение без людей и т.п.);

*Требование А2* — возможность формирования аудиоматериалов с заданными базовыми голосовыми характеристиками (мужской голос, женский голос, голос молодого человека, голос человека среднего возраста, голос пожилого человека) на основе исходного аудиоматериала;

*Требование А3* — возможность формирования аудиоматериалов с заданными голосовыми характеристиками конкретного человека на основе исходного аудиоматериала;

*Требование В1* — возможность формирования видеоматериала на заданном видеофоне (улицы конкретных городов в различное время суток, различные помещения: музеи, театры, диппредставительства и т.п.);

*Требование В2* — возможность формирования видеоматериалов с заданными базовыми видеохарактеристиками для главных действующих лиц (пол, возраст, национальность);

*Требование В3* — возможность формирования видео материалов с видеохарактеристиками, позволяющими зрителям опознать в действующих лицах конкретных людей.

*Подготовка текстовых материалов*

Теоретическая возможность формирования текстовых материалов заданной направленности объясняется избыточностью естественного языка, большим разнообразием форм подачи одного и того же содержания. При этом избыточность языка позволяет любое сообщение транслировать в соответствующей эмоциональной интерпретации, определяя тем самым свое отношение к этому сообщению, что очень важно при формировании общественного мнения.

Например, новость: «Появляется все больше свидетельств тому, что сирийские повстанцы сбили истребитель ВВС Сирии».

Возможные перестроение заданной направленности путем использования синонимического словаря:

1. «Распространяется все больше слухов тому, что сирийские бандиты повредили самолет ВВС Сирии».

2. «Приводится все больше подтверждений тому, что сирийские освободители уничтожили истребитель ВВС Сирии».

Два варианта одной и той же новости, полученные путем применения синонимического словаря. Оба эти варианта имеют совершенно разную эмоциональную направленность. Первый вариант явно принадлежит перу официальных служб ВВС Сирии, второй — сирийским повстанцам.

Исследование направления автоматической генерации текстов в заданном стиле и существующих реализаций позволило сделать следующие выводы:

1. Наиболее распространенными программами являются программы, которые позволяют видоизменять текст — синонимайзеры, а не создавать его с нуля.

Имеют место два вида синонимайзеров, предоставляющих соответственно возможность:

1) автоматической генерации текстов со встроенной базой синонимов; программа автоматически находит в тексте слова-синонимы и хаотично заменяет их словами из своей базы;

2) генерации текстов по заданному шаблону; при генерации статьи задается шаблон, в котором пользователь программы указывает, где заменить слова-синонимы или словосочетания; при таком подходе из одной статьи можно сделать несколько других.

На выходе второго вида программ получаются более читабельные тексты.

Синонимайзеры могут быть оформлены в виде сайта в Интернете или скрипта.

*Подготовка аудиоматериалов*

В данной работе будем опираться на следующие понятия:

**Аудио** — общий термин, относящийся к звуковым технологиям. Зачастую под термином аудио понимают звук, записанный на звуковом носителе; реже под аудио подразумевается запись и воспроизведение звука, звукозаписывающая и звуковоспроизводящая аппаратура. Аудиоаппаратура работает с сигналами, включающими частоты до 20 кГц, поскольку звук большей частоты не воспринимается слухом. Как и любая волна, звук характеризуется амплитудой и частотой. Считается, что человек слышит звуки в диапазоне частот от 20 Гц до 20 000 Гц. Среди слышимых звуков следует также особо выделить фонетические, речевые звуки и фонемы, из которых состоит устная речь, и музыкальные звуки, из которых состоит музыка.

**Звукозапись** — процесс сохранения воздушных колебаний в диапазоне 20–20 000 Гц (музыки, речи или иных звуков) на каком-либо носителе. Необходимое оборудование: прибор для преобразования

звуковых колебаний в электрические (микрофон) или генератор тона (например, звуковой синтезатор, семплер), устройство для преобразования электрических колебаний в последовательность цифр (в цифровой записи), устройство для сохранения (магнитофон, жесткий диск компьютера или иное устройство для сохранения полученной информации на носитель) www.hardbroker.ru/catalog/239/.

**Монтаж** (фр. *montage*) видео- или аудиоматериала — процесс переработки или реструктурирования изначального материала, в результате чего получается иной целевой материал[37].

Наиболее полный глоссарий терминов, связанных с аудио, размещен на сайте Википедии по адресу http://de.wikipedia.org/wiki/Liste_von_Audio-Fachbegriffen.

Под **аудиоматериалом** будем понимать звук, записанный в виде устной речи (голос), звуковых эффектов разной тематики, музыки и их сочетаний и оформленный в виде аудиофайла, пригодного для размещения в сети Интернет на контролируемых ресурсах.

Существует два основных источника звуковых эффектов для аудиофона:

1) Записанные естественные звуки; подбираются из профессиональной фонотеки.

2) Электронные; создаются на специальных аппаратах (реверберaторы).

Для аудиофона профессиональные фонотеки формируются двумя способами:

- запись естественных звуков высокого качества без посторонних шумов; например, специально записанные при сборе звуковых эффектов звук взрывающегося вдалеке снаряда, звук толпы разного эмоционального настроя, бытовые звуки и т.п.; запись производится с использованием средств записи звука, поддерживающих современные распространенные аудиоформаты; отсутствие шума на аудиофоне достигается последующей обработкой записи с использованием аудиоредакторов, делающих звук чистым, либо использованием профессиональных цифровых диктофонов;

[37] См.: http://ru.wikipedia.org›wiki/Монтаж.

- вычленение звуков фона из произвольной записи — создание так называемых «минусовок»; достигается использованием специально предназначенных для этого аудиоредакторов.

Для того чтобы формировать аудиоматериалы на заданном аудиофоне необходимо:

- иметь фонотеку (коллекцию аудиофонов);
- программное обеспечение (ПО) для формирования аудиоматериалов (аудиоредакторы, ПО для звукомонтажа).

При выборе программного обеспечения для формирования итоговых аудиоматериалов учитывается тот факт, что для подготовки мультимедийного контента целесообразно выбрать профессиональный инструмент, который бы обладал необходимым функционалом звукомонтажа не только для формирования аудиоматериалов на заданном аудио фоне, но и для формирования аудиоматериалов с заданными базовыми характеристиками и с заданными характеристиками конкретного человека одновременно.

Базовыми характеристиками будем считать пол (женский/мужской голос), возраст (например, детский, голос пожилого человека и т.п.), национальность (с акцентом, с иностранным акцентом). Звукозаписи голосов с заданными базовыми характеристиками получают двумя способами:

- озвучивание текста голосами профессиональных дикторов (ссылки на услуги подобного рода широко представлены в сети);
- используя эффекты программного обеспечения «компаратор голоса» (предустановленные голоса и эффекты). На сегодня уже существуют вполне приличные программные продукты для имитации голосов людей после сравнения и подстройки[38]. Существуют готовые пакеты для имитации голосов знаменитостей, в том числе президентов отдельных стран.

Технология «клонирование голоса» позволяет моделировать персональные характеристики речи человека с достаточно полным совпадением с оригиналом, называемым «мишенью копирования». Технология клонирования речи базируется на известных алгорит-

[38] Например, Voice Changer Diamond Edition

мах математической обработки сигнала-носителя голоса[39]. Реализуется в режиме как реального времени, так и в отложенном пакетном режиме. Синтез измененной речи на основе сигнала-носителя, то есть получившийся «клонированный голос», реализует возможность максимального сохранения персональных акустических характеристик копируемого исходного голоса: фонетических особенностей произношения, акцента и даже артефактов такого рода, как заикание.

*Подготовка видеоматериалов*

Под **видеоматериалом** будем понимать аудиовизуальный материал, записанный в виде видеофайла в формате, пригодном для размещения в сети Интернет на контролируемых ресурсах.

Под видеофоном будем понимать **футаж** — видеофайл, содержащий видеофрагменты небольшой длительности разной тематики; используется для монтажа, повышая зрелищность, эффектность видеоматериала, а также его реалистичность, в качестве фона, на котором происходит основное действие.

Расширение компьютерных видеофайлов:

3gp, flv, avi, mpg, mov, swf, asf, mp4, wmv, mts, mkv — более подробную информацию о каждом из них можно получить в электронной библиотеке по адресу http://ru.wikipedia.org/wiki.

Футажи делятся на две категории:

- футажи с альфа-каналом (прозрачная основа): анимированные фоны, анимированные титры, оверлейные маски, МД элементы (анимированные элементы), частицы;
- «хромокеевские» футажи: могут использоваться как подложка-фон для основной композиции, титров или снятое изображение (движение людей, природа и т.п.).

Футажи с альфа-каналом первоначально создавались для редактора Pinnacle Studio, но их можно применять и в других редакторах (метод и способ использования футажа с альфа-каналом в разных видеоредакторах разный). Футажи с альфа-каналом состоят из двух частей (двух файлов: файл с расширением .alp и файл .dif).

---

[39] *Лобанов Б.М., Цирульник Л.И.* Компьютерный синтез и клонирование речи. Минск: Белорусская наука, 2008, 316 с.

Для добавления футажа в Pinnacle Studio необходимо открыть и вставить на видеодорожку файл .dif (.alp — это вспомогательный файл и он «найдет свое применение» автоматически).

«Хромокеевские» футажи — это видеофрагменты, снятые на зеленом, синем или (реже) на черном фоне. При добавлении такого футажа в свой ролик (в видеоредакторе) к нему необходимо применить соответствующий хромокеевский фильтр, для того чтобы фон (синий или зеленый) сделать прозрачным. Для футажей, снятых на черном фоне, технология другая: к ним применяется фильтр цветности, и путем изменения цветового баланса необходимо добиться того, чтобы черный фон футажа не менял общей цветовой картины основного ролика и не влиял на яркостный канал. Хромокеевские футажи применяются практически во всех видеоредакторах[40].

Во всех видеоредакторах футаж редактируется так же, как любой видеофрагмент: обрезка, применение к нему фильтров, переходов, трансформация, копирование и выставление в ряд несколько копий (для увеличения продолжительности футажа) и т.д.

Таким образом, формирование видеоматериалов на заданном видеофоне предполагает наличие:

- коллекции футажей;
- программного обеспечения (ПО) для формирования видеоматериалов (видеоредакторы, ПО для видеомонтажа) с заданными базовыми и конкретными характеристиками одновременно.

К базовыми характеристикам будем относить пол, возраст, национальность главных действующих лиц или массовок, возможно, в разных ситуациях и с разным эмоциональным настроем.

Видеозаписи с заданными базовыми характеристиками получают двумя способами:

- привлекая непрофессиональных актеров-массовщиков для специально организованной постановочной съемки сюжетов; в сети Интернет много предложений и выбор действующих лиц с заданными базовыми характеристиками из существующих баз данных;
- используя эффекты программ для оживления (анимации) статичных изображений (фото) людей с заданными базовыми характе-

[40] Футажи для видеомонтажа. // http://studio-25kadr.ru/s99.html.

ристиками, животных и даже предметов. Преимущество данного способа в том, что можно оперативно из любых фотографий, удовлетворяющих требованиям «базовых характеристик», создавать видеофрагменты. Недостаток — недостаточная для естественного видеосюжета реалистичность выходного видеоматериала.

При создании видео материала с видеохарактеристиками, позволяющими зрителям узнать в действующих лицах конкретных людей, проблема заключается в получении видеозаписи конкретных людей и видеомонтажа итогового материала в течение времени, не превышающего значение «реального времени». Пути ее решения на сегодня следующие:

– для видеомонтажа используют заранее подготовленные видеофрагменты:

вариант а) — специально снятые с участием конкретных людей, в том числе двойников или с использованием грима;

вариант б) — футажи с конкретными людьми (лицами);

вариант в) — анимированные фотоизображения конкретных персонажей, для которых фотографии можно найти в открытом доступе.

Варианты а) — в) перечислены по степени уменьшения реалистичности и, следовательно, доверия субъектов воздействия к видеоматериалу и по степени увеличения оперативности их получения.

После того как проведены мероприятия по подготовке мультимедийного контента, необходимо разместить материалы на заранее определенных интернет-ресурсах. Однако при этом могут встретиться препятствия, способы преодоления которых приведем далее.

### *3.2.3. Автоматическое преодоление защиты от роботов*

Виртуальные специалисты-[ро]боты, кроме языка людей, нескольких естественных национальных языков, на которых ими собирается информация, должны хорошо знать язык разметки гипертекста html. Ибо поле битвы для них — это не только люди, которых надо кормить спамом, но и сайты, которые надо изучить, проиндексировать, забанить, заблокировать, скачать. Робот должен знать, кто перед ним: пользователь, за которого идет сражение, или такой же

робот, который принес спам или пришел скачать сайт, чтобы в дальнейшем увести вслед за собой и сегодняшних посетителей.

Любой сайт, написанный на языке программирования, например, на php, сам является роботом, способным анализировать и классифицировать своих посетителей. По IP-адресу он понимает, из какой части планеты пришел посетитель, по языковым настройкам браузера он узнает о естественных национальных языках, которые предпочитает данный посетитель, по адресу перехода — откуда, с какого сайта пришел, гость.

Робот-сайт не только классифицирует своих посетителей, но и управляет ими. К примеру, несколько сайтов-роботов, договорившись, легко могут выставить в неприглядном свете целую страну. Им достаточно обращения всех своих посетителей, имеющих IP этой страны, одним потоком переключить на сайт-мишень. Пусть потом хозяин сайта-мишени разбирается, из-за чего на него вдруг такой наезд из Лилипутии. Скорее всего, реакция будет однозначной — закрыть вход на сайт-мишень жителям Лилипутии, идентифицируя их по IP-адресу. И в результате ни в чем не виновные граждане и их слуги-роботы никогда не попадут туда за интересовавшей их информацией. Подобный прием — составная часть информационной операции.

А сколько уже сегодня существует сайтов с чужим «лицом» и в чем-то похожим именем? Простаки, ошибившиеся в одном символе, попадают по виду туда, куда они, вроде бы, и планировали, но на самом деле они попадают в ловушку, где из них будут выжимать знания о почтовых адресах, паролях, счетах. Даже в таком простом имени, как rambler, обычный пользователь ошибается не менее одного процента, в основном за счет нажатия близких букв на клавиатуре или из-за того, что клавиатура не переключена на нужный язык. Посетителей у rambler’а немало. Скупив близкие по начертанию доменные имена, можно легко построить хорошо раскрученный за чужой счет сайт и при этом не нарушить ни одного пункта законодательства, да еще и собирать долго-долго чужие почтовые адреса, которые потом оптом поставлять любителям спама.

Заметать свои следы от профессиональных поисковых машин и приманивать поисковые машины на приманку-обманку — сегодня одни из самых простых приемов. Суть их в следующем:

1. Провести распознавание посетителя.

2. Если посетитель — поисковая машина, то подсунуть этой машине такой html, в котором просто бессмысленный набор популярных слов и выражений, используемых людьми для поиска в Интернет. В результате рейтинг сайта значительно вырастет.

3. Если посетитель — человек, предложить ему настоящее содержимое, порой не имеющее ничего общего с тем, которое прописали в себя поисковики.

Как видно, одной из главных задач для робота является получение ответа на вопрос: «Кто есть кто?»

Эта задача актуальна для людей, и она не менее актуальна для роботов.

Защита от роботов подразумевает защиту от специальных компьютерных программ, выполняющих автоматически и/или по заданному сценарию какие-либо действия через те же интерфейсы, что и обычный пользователь сети Интернет.

На сегодняшний день многие ресурсы в сети Интернет имеют защиту от роботов. Защита, как правило, построена на решении задачи из класса задач по распознаванию образов, которая легко решается человеком, но сложна для робота. На сегодняшний день используются следующие варианты:

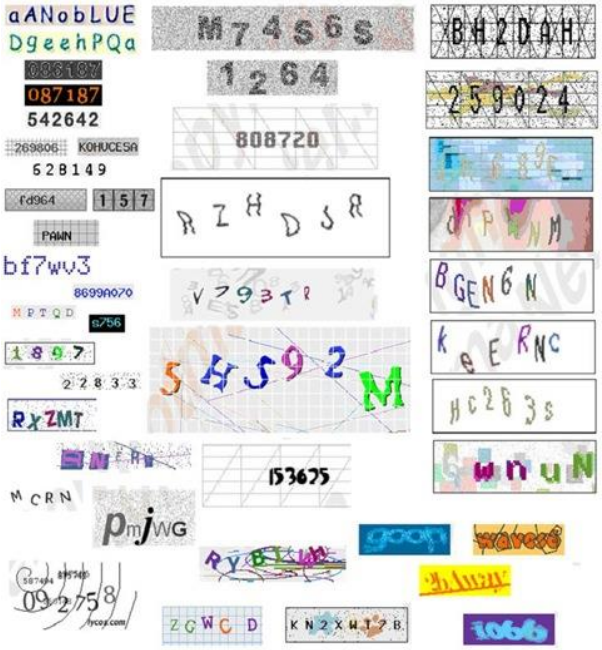
- распознавание числа или слова, написанного различными шрифтами;
- распознавание числа или слова, написанного различными шрифтами на сложном фоне;
- распознавание изображения;
- решение математической задачи, типа: Сколько будет 2+3?
- ответ на вопрос, который хорошо известен любому человеку, например, «Который сейчас час?», «Который сегодня день недели?» и т.п.

В основе построения защиты ресурсов от компьютерных программ лежит использование captcha-фильтров.

CAPTCHA (['kæptʃə] от англ. Completely Automated Public Turingtest-to-tell Computers and Humans Apart — полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей. Основная идея теста: предложить пользователю такую задачу, которую с легкостью может решить человек, но которую несоизмеримо сложнее решить компьютерной программе[41].

Примеры изображений, используемых в CAPTCHA см. ниже.

Могут также применяться другие, плохо алгоритмизируемые задачи, основанные на логике мышления человека, например: капчи, где необходимо выставить картинки в определенной последовательности, собрать пазл, выбрать один из предложенных вариантов решения задачи, добавить недостающий элемент в картинку, а также капчи, основанные на распознавании речи и движении мыши по определенному маршруту.



[41] Википедия [точка доступа: http://ru.wikipedia.org/wiki/CAPTCHA]

Преодоление подобного рода защиты строится на решении задачи распознавания образов и состоит из нескольких этапов:

1. В силу того, что сама защита — задача по распознаванию образов, расположена на сайте, она оформлена в соответствии с правилами оформления на языке разметки html. Поэтому первым действием необходимо считать содержимое сайта, выделить часть кода, ответственную за защиту, и проанализировать его, на предмет решения поставленной задачи, т.е. речь идет о применении классического парсинга[42] и создании для этого парсера[43].

Любой парсер состоит из трех частей, которые отвечают за три отдельных процесса парсинга:

- получение контента в исходном виде. Под получением контента чаще всего подразумевается скачивание кода веб-страницы, из которой необходимо извлечь данные или контент. Одним из самых развитых решений для получения кода требуемой страницы является библиотека cURL для языка PHP;
- извлечение и преобразование данных. В этой фазе происходит извлечение требуемых данных из полученного на первом этапе кода страницы. Чаще всего для извлечения используют регулярные выражения. Также на этом этапе происходит преобразование извлеченных данных к нужному формату, если это требуется. В случае преодоления капча-фильтра, после того как данные получены, осуществляется решение задачи распознавания образа;
- генерация результата. Завершающий этап парсинга. На нем происходит вывод или запись полученных на втором этапе данных в требуемый формат и передача результата.

2. В случае удачного решения, т.е. выявления скрытого изображения и нахождения ответа, необходимо выделить часть текста, ответственного за передачу результата на сервер, и полученный результат передать через форму непосредственно на сервер, где расположена база данных с ответами. В случае правильного ответа сервер сменит страницу сайта и пропустит программу-посетителя дальше.

---

[42] Парсинг — автоматизированный сбор контента или данных с какого-либо сайта или сервиса.

[43] Парсер — программа, занимающаяся сбором содержимого страниц сайта, анализом, выделением данных и преобразованием данных к требуемому виду.

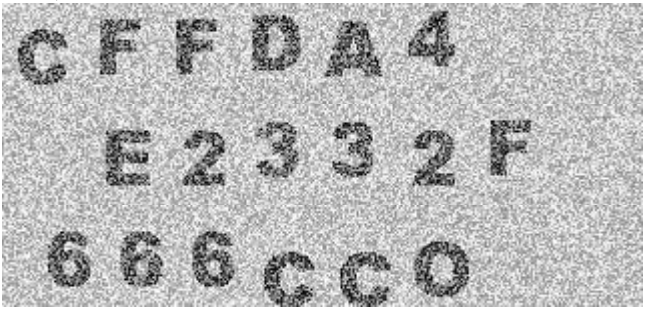
Распознавание каждого образа — это создание специального алгоритма распознавания, который базируется на выявленных слабостях конкретной капчи. Ниже приведем пример построения подобного рода алгоритма.

Например, (www.captcha.ru/breakings/phpbb/):

Довольно слабая CAPTHA: фиксированный шрифт, символы легко отделяются от фона из-за хорошего контраста. Для гарантированного получения только тех пикселей, которые принадлежат надписи, достаточно выбирать пиксели темнее некоторого порога.

увеличиваем контраст и определяем границы массивов черных точек — это и есть знакоместа.

Также слабой стороной является то, что высота расположения символа задана в шрифте, т. е. одинаковые символы будут на одной высоте (правда, при написании алгоритма распознавания это не учитывалось).



Видно, что одинаковые символы всегда на одной высоте.

Распознавание сделать довольно легко путем прямого попиксельного сравнения каждого из символов со шрифтом.

Понятно, что единого универсального алгоритма здесь нет, каждый раз при появлении принципиально нового капча-фильтра первоначально задачу придется решать человеку в виде создания алгоритма распознавания. Однако, несмотря на невозможность созда-

ния при сегодняшних технологиях универсального алгоритма, возможно создание универсальных технологий, в которых на определенном этапе используются человеческие возможности.

Делается подобное следующим образом.

Исходные данные:

- сайт №1, защищенный капча-фильтром, на который надо проникнуть виртуальному специалисту-[ро]боту;
- достаточно раскрученный сайт №2, который принадлежит владельцу данного виртуального специалиста-[ро]бота.

Решение задачи:

1. Виртуальный специалист-[ро]бот обращается к сайту №1 и парсит главную страницу, на которой находится капча-фильтр.
2. Виртуальный специалист-[ро]бот выделяет из страницы капча-фильтр и размещает его на подконтрольном сайте №2.
3. Посетители сайта №2 благополучно проходят капча-фильтр.
4. Виртуальный специалист-[ро]бот получает результат и передает этот результат главной странице сайта №1.

Интересный пример сражения роботов с роботами приведен на сайте html://www.omsk777.ru. Видно, что автора публикации война с роботами захлестнула не на шутку, и он описывает достаточно подробно, на уровне языка программирования, все известные ему способы идентификации роботов роботами.

Остановимся на одном достаточно элегантном примере распознавания робота.

Вот таким тегом языка html задается ссылка на страничках сайтов, по которой посетители лихо щелкают «мышкой»:

```
<a href='all.php?act=fuck_you'> <img src='img/bud2.gif' width='1' height='1' border='0'> </a>
```

Здесь Тег <a href='all.php?act=fuck_you'> указывает адрес перехода с параметрами;

width='1' height='1' — атрибуты тега <img>, которые задают размер картинки с именем файла

'img/bud2.gif' при отображении ее в виде значка перехода на экране.

Как видно, размер картинки всего один пиксель. Это означает, что посетитель-человек ее просто не увидит в силу слабости своего

восприятия. А робот увидит, ибо он смотрит не на экран, а непосредственно работает с языком разметки. Робот увидит ссылку, но вряд ли подумает, что она специально для него, ибо проверять размер картинки не станет. Он торопится. И он пойдет по ссылке и начнет скачивать приготовленную для него страничку html. Но вот здесь-то его и ждет засада. Автор этого приема с сайта omsk777.ru не поленился и отомстил по полной программе, подготовив для робота маленький архив из нулей, который при разархивировании раздувается до 250 Гб. Мало не покажется. Робот-противник надолго будет занят бессмысленным делом.

Главное, как мы видим, — это узнать противника. А способов наказания существует достаточно много. Можно навесить на врага тяжелые мегабайтные файлы, можно отправить его по ссылке в какое-нибудь отвратительное место, можно загнать его в бесконечный цикл. Правда, противник тоже не полный кретин, он, получив ту или иную ссылку, тут же проверяет, а знакома ли она ему? И только в том случае, если незнакома, идет по этой дороге. Но дело-то в том, что сами ссылки всегда направлены на те или иные имена файлов, а робот-сайт, который готовит ловушку, всегда может менять имена хранимым у него файлам, используя датчик случайных чисел или дату со временем, а затем проставлять эти новые имена в ссылки для одноразового срабатывания. Пришел враг по ссылке, но пока он приходил, в эти самые мгновенья прихода, уже появился новый файл с тем же содержимым, но с другим именем. И это новое имя уже прописано в ссылке и ждет, когда его выберут: «*И вечный бой!*» И сбежать нельзя, потому что «работа» не закончена[44].

Допустим, используя вышеприведенные приемы, виртуальный специалист проник на сайт-объект информационной операции и разместил подготовленный заранее контент. Однако при размещении материалов на чужих ресурсах всегда надо учитывать, что хозяин (модератор) может удалить эти материалы, если они не соответствуют задачам ресурса. Рассмотрим далее способы защиты размещенных материалов от удаления или блокирования доступа к нему.

---

[44] Не по таким ли ссылкам ходит вечно проявляющаяся в тварном мире душа человека?

### *3.2.4. Защита мультимедийного контента от удаления или блокирования доступа*

Удаление мультимедийного контента, размещенного на чужом сайте, осуществляется:

- автоматически (по набору ключевых слов и словосочетаний, путем отнесения того или иного материала к категории спама с последующим удалением);
- вручную (непосредственно модератором).

Автоматическое удаление спама практикуется многими средствами защиты, включая антивирусные пакеты. Выбор автоматически удаляемого материала осуществляется по следующим критериям:

- определенные слова и словосочетания;
- IP-адрес, с которого поступил материал.

Защитой размещаемых материалов в данном случае является их трансляция в тексты, отличающиеся по форме, но имеющие одинаковое смысловое содержание.

При удалении материалов вручную модераторы руководствуются «Правилами пользования… и конфиденциальность», которые традиционно размещены на сайте хозяином ресурса и, считается, доведены до сведения его посетителей и пользователей. Преимущественно Правила содержат требования к содержанию размещаемых материалов.

Защитой размещаемых материалов в данном случае является соблюдение Правил. Несоблюдение Правил может привести к блокированию доступа ко всему ресурсу владельцем хостинга или отдельному мультимедийному контенту, размещенному на чужом ресурсе, владельцем ресурса.

Самый надежный способ сохранить информационные материалы — разместить их на своем, подконтрольном интернет-ресурсе. Задача лишь в том, чтобы раскрутить собственный сайт.

В интернет-литературе, в обсуждениях в блогах и на форумах отмечают следующие бесплатные способы «раскрутки» ресурса:

- Регистрация в социальных закладках — сервисы социальных закладок: BobrDobr, Memori, MoeMesto и др. Если требуется зарегистрировать 1-3 сайта, это можно сделать «вручную», самостоя-

тельно выполнив указанные требования по регистрации ресурса. Однако для удобства и при большем числе требующих регистрации ресурсов чаще применяются специальные программы, которые регистрируют сайты в соцзакладках бесплатно. При регистрации необходимо указать название ресурса, его описание и URL.

- Регистрация в каталогах и рейтингах — каталоги могут иметь разную тематику, и этим обстоятельством можно с успехом воспользоваться. Существуют специально предназначенные для этого программы. Имеются также программы, которые генерируют и массово рассылают письма со ссылками на ресурс, создают объявления для бесплатной публикации на электронных досках объявлений.
- Регистрация в каталогах статей.
- Рассылка своих объявлений на доски объявлений.
- Написание пресс-релизов, новостей и статей и размещение на других сайтах.
- Ручной тематический обмен ссылками.
- Участие на тематических форумах (ссылка на сайт в подписи).
- Комментирование в блогах (ссылка на сайт в подписи).
- Написание уникальных статей и размещение их на своем сайте.
- Размещение на сайте полезных сервисов, софта.
- Своя рассылка.
- Свой блог.
- Свой форум.

Для того чтобы уменьшить вероятность удаления мультимедийного контента, размещенного на чужом сайте, можно применить мероприятия по сокрытию IP-адреса, с которого пришел виртуальный специалист, разместивший текстовый, аудио- или видеоматериал. При этом будет соблюден и базовый принцип проникновения — анонимность.

### *3.2.5. Сокрытие IP-адреса*

В основу работы сети Интернет положено семейство протоколов TCP/IP, определяющих взаимодействие между находящимися в сети компьютерами. Идентификация компьютеров осуществляется с помощью IP-адресов, каждый из которых представляет собой уникальный 32-битный идентификатор, который записывается в виде четырех десятичных чисел, например, 192.168.01.198.

Любому пользователю сети Интернет провайдер при каждом выходе в сеть выдает либо динамический IP-адрес из некоторого пула, зарегистрированного за данным провайдером, либо статический адрес, который является постоянным для данного пользователя, но также зарегистрирован за данным провайдером.

При обращении к любому ресурсу сети Интернет пользователь всегда может быть идентифицирован по своему IP-адресу. Знание IP-адреса позволяет установить географическое месторасположение посетителя с точностью до города.

Базовый принцип сокрытия и/или подмены IP-адреса заключается в организации взаимодействия пользователя с ресурсом через некоторый промежуточный ресурс, который называется прокси-сервером. Задача прокси-сервера заключается в подмене истинного адреса пользователя на адрес, закрепленный за прокси (рис. 3.2.5.1).

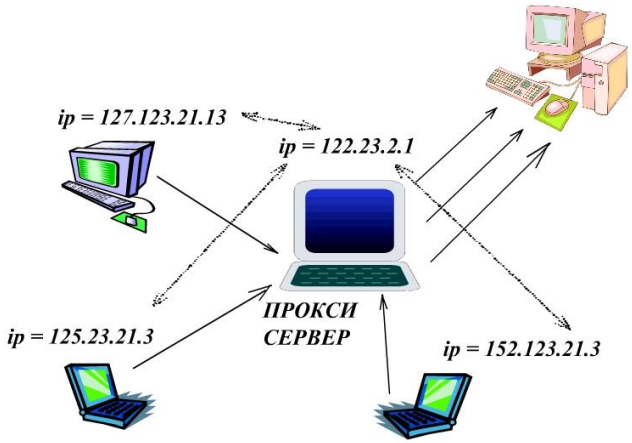



РИСУНОК 3.2.5.1. *Базовый принцип сокрытия IP-адреса*

Прокси-сервер — исполняемая программа, которая постоянно опрашивает соответствующий порт, ожидая запросов по определенному протоколу. Как только установлено соединение с посетителем и получен запрос, программа транслирует этот запрос другому серверу от имени посетителя, а затем возвращает посетителю ответ.

Прокси имеет несколько вариантов реализации, но суть у них всех одна: подмена адреса посредником. При этом допускается, что посредников может быть много, и каждый раз они могут быть разными (рис. 3.2.5.2). В этом случае задача нахождения истинного адреса источника становится еще более сложной.

Однако любой proxy сервер, а тем более бесплатный, ведет лог. И спецслужба, которая располагает соответствующими правами, всегда сможет вычислить, куда заходил клиент и что делал, даже если использовать цепочки анонимных прокси-серверов в разных концах планеты.

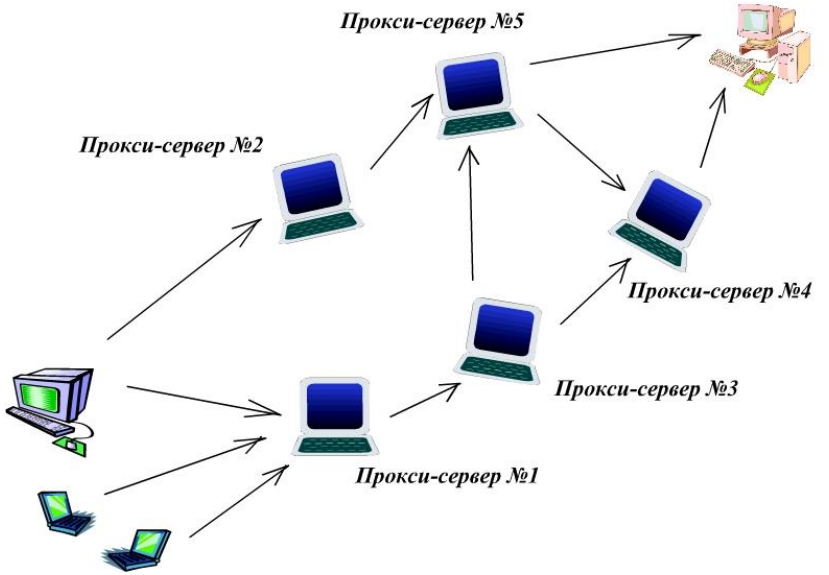



РИСУНОК 3.2.5.2. *Цепочки прокси-серверов*

Способы и методы сокрытия адреса с помощью прокси могут называться по-разному. В заключение раздела приведем краткий обзор наиболее популярных технологий, построенных на основе прокси. За основу взята работа http://legalrc.biz/threads/.

**VPN** (Virtual Private Network — виртуальная частная сеть)

VPN-соединение похоже на подключения к обычной локальной сети.

Любое приложение (браузер) без какой-либо настройки может использовать VPN для доступа в Интернет. Когда оно обращается к удаленному ресурсу, то на компьютере создается специальный GRE (Generic Routing Encapsulation — общая инкапсуляция маршрутов)-пакет, который в зашифрованном виде отправляется VPN-серверу. VPN-сервер пакет расшифрует и выполнит от своего IP-адреса соответствующее действие. Получив ответ от удаленного ресурса, VPN-сервер поместит его в GRE-пакет, зашифрует и в таком виде отправит обратно клиенту. Как видно, добавляется только шифрование.

**OpenVPN** — свободная реализация технологии VPN, организуется на основе общепринятого в Интернете стека протоколов TCP/IP.

Отличия OpenVPN от технологией VPN:

1) адаптивное сжатие данных в соединении, с применением алгоритма компрессии LZO. Скорость передачи данных через OpenVPN выше, чем у VPN;

2) поддерживает гибкие методы авторизации подлинности клиента, основанные на сертификатах;

3) использование одного TCP/UDP-порта без привязки к конкретному порту (в нашем случае UDP);

4) шифрование 2048 бит реализовано через постоянный ключ.

Серверы для анонимных VPN обычно устанавливают в странах, где наиболее лояльно относятся к взлому, спаму и т.д. (Китай, Корея и т.п.). В большинстве случаев имеет место договоренность с администрацией, которая за определенную плату обязуется игнорировать жалобы в abuse-службу и не вести логи. Однако убедить-

ся в том, что обещание сдерживается, для пользователя не представляется возможным.

**Proxy, SOCKS**

Классический вариант прокси-сервера. Особенности обусловлены используемым протоколом.

Протокол SOCKS наиболее примечателен тем, что он инкапсулирует протоколы не прикладного, а транспортного уровня, т.е. TCP/IP и UDP/IP. Поскольку только по этим протоколам возможна работа в Сети, через SOCKS можно работать с любыми серверами, в том числе и такими же SOCKS и, таким образом, организовывать цепочки SOCKS-серверов. По этой же причине все SOCKS-сервера анонимны — невозможно на уровне TCP/IP и UDP/IP передать дополнительную информацию, не нарушив работу вышестоящего протокола.

**Анонимайзеры** — программы с интерфейсом, похожим на обычный поисковик, только вместо слов/фраз здесь нужно вводить URL того сайта, который следует посмотреть.

Анонимайзеры представляют собой скрипты, написанные, например, на perl, php, cgi-скрипты, которые реализуют обращение через определенные прокси.

**TOR**

Tor (The Onion Router) — свободная (BSD) реализация второго поколения onion router (так называемая «луковая (многослойная) маршрутизация»). Система, позволяющая пользователям соединяться анонимно, обеспечивая передачу пользовательских данных в зашифрованном виде. Рассматривается как анонимная сеть, предоставляющая анонимный web-серфинг и безопасную передачу данных. С помощью Tor пользователи смогут сохранять анонимность при посещении web-сайтов, публикации материалов, отправке сообщений и работе с другими приложениями, использующими протокол TCP. Безопасность трафика обеспечивается за счет использования распреде-

ленной сети серверов, называемых «многослойными маршрутизаторами» (onion routers).

Пользователи сети Tor запускают onion-proxy на своей машине, данное программное обеспечение подключается к серверам Tor, периодически образуя виртуальную цепочку сквозь сеть Tor, которая использует криптографию многоуровневым способом (аналогия с луком — англ. onion). Каждый пакет, попадающий в систему, проходит через три различных сервера (нода), которые выбираются случайным образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьей ноды, потом для второй и, в конце концов, для первой.

Когда первая нода получает пакет, она расшифровывает «верхний» слой шифра (аналогия с тем, как чистят луковицу) и узнает, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом. В то же время, программное обеспечение onion-proxy предоставляет SOCKS-интерфейс. Программы, работающие по SOCKS-интерфейсу, могут быть настроены на работу через сеть Tor, который, мультиплексируя трафик, направляет его через виртуальную цепочку Tor. Что в конечном итоге позволяет обеспечивать анонимный серфинг в сети.

Существуют специальные надстройки-tor для веб-браузеров Opera, Firefox.

**SSH-туннелинг**

SSH (Secure Shell) — сетевой протокол, позволяющий производить удаленное управление компьютером и передачу файлов. Использует алгоритмы шифрования передаваемой информации.

SSH-туннелинг можно рассмотреть в качестве дешевой замены VPN. Принцип данной реализации следующий. Весь сетевой софт на компьютере форвардится на назначенный порт (вашего локалхоста), на котором висит сервис, соединенный по SSH с сервером (а как мы знаем, соединение по SSH- протоколу шифруется) и туннелирующий все запросы; далее, весь ваш трафик (уже не в зашифрованном виде) может форвардиться с нашего сервера на прокси (поддерживающий туннерирование) или сокс, которые передают

весь трафик к необходимым адресам. Наличие прокси или сокса не обязательно.

Какие плюсы данной системы?

1) Для организации данной схемы не нужно устанавливать серверный софт (т.к. SSH-аккаунт и сокс можно без проблем достать в интернете).

2) Поскольку при SSH-соединении трафик шифруется и сжимается, то мы получаем небольшой прирост скорости работы в инете (это верно, когда сокс-демон находится на том же сервере).

3) В случае, когда сокс-сервер находится на другом хосте, мы получаем дополнительную цепочку серверов, которые повышают нам безопасность и анонимность.

**JAP**

В одном из немецких институтов был разработан довольно хитрый способ сохранения анонимности. В систему пользователя устанавливается специальная прокси-программа JAP, которая принимает все запросы пользователя на подключения, шифрует (AES с 128-bit длиной ключа) и в безопасном режиме отправляет на специальный промежуточный сервер (так называемый микс). Дело в том, что микс одновременно использует огромное количество пользователей, причем система построена так, чтобы каждый из них был неразличим для сервера. А поскольку все клиенты одинаковые, то и вычислить конкретно одного пользователя не представляется возможным.

Миксы обычно устанавливаются на добровольных началах, в основном в университетах, которые официально подтверждают, что не ведут никаких логов. К тому же обычно используются цепочки миксов, как правило, три микса.

**P2P-анонимайзеры**

Рассмотрим на примере сети Peek-A-Booty.

Peek-A-Booty — это распределенная пиринговая сеть из компьютеров, принадлежащих добровольцам из различных стран. Создана для того, чтобы пользователи могли обходить наложенные локальной цензурой ограничения и получать доступ к запрещенным в

том или ином государстве ресурсы Интернета. Каждый узел сети маскируется, так что пользователь может направлять запросы и получать информацию с определенных IP-адресов в обход цензурных барьеров.

Пользователь подсоединяется к специальной сети, где работает Peek-A-Booty. Несколько случайно выбранных компьютеров получают доступ к веб-сайту и пересылают данные тому, кто послал запрос. Весь трафик в этой сети шифруется по принятому в электронной коммерции стандарту SSL, так что все выглядит как невинная транзакция.

*Нестандартные способы определения IP-адреса*

**Cookies**

При первом входе на веб-сайт, IP-адрес клиента (определенный сервером, т.е. IP proxy) сервер может сохранить в Cookies. Когда посетитель в следующий раз входит на сайт, сервер вновь определяет IP и сравнит его с сохраненным в Cookies. И если IP-адреса старый и новый различаются, сервер может сделать выводы о том, что вход осуществляется через прокси.

**JavaScript**

JavaScript — это скрипты, предназначенны для выполнения активных сценариев на компьютере пользователя браузером. Они довольно простые и имеют ограниченные функции, но они могут определить реальный IP и множество других настроек браузера.

**Java**

Java — это в отличие от предыдущего полноценный язык программирования, и программа, написанная на этом языке, может без особых трудностей определить реальный IP компьютера.

**Active X**

Это полноценные программы, которые выполняются на компьютере пользователя. Возможности у них лучше, чем у Java. Они могут легко определить любые настройки браузера и вычислить настоящий IP-адрес и даже легко изменить настройки прокси.

Все, о чем написано в Главе 3, — это пока набор отдельных специальных действий, проводимых в ходе информационных операций, которые используются в сражениях за посетителей, за рейтинги своих сайтов и проч. Настоящие войны начнутся только тогда, когда виртуальные специалисты-[ро]боты будут объединяться. И вот тогда объединенная группа, выстроившись клином, ломанет в атаку на противника. И именно тогда мы будем видеть полный набор операций, объединенных единым замыслом, что уже сможет вполне потянуть на название страшным словом «война».

# ГЛАВА 4

# Планирование и моделирование информационной операции

На первый взгляд представляется, что планирование информационной операции (ИО) скорее относится к искусству, и успешность операции во многом определяется талантом организатора. Но, оставаясь штучным товаром, операция не может считаться элементом информационной войны. Война требует продукции конвейерного производства, в которой и солдаты, и танки, и командиры заменяемы. Похоже, что специалисты США по информационным войнам давно это поняли. Так, например, все информационные операции в рамках арабской весны[45] похожи, как две капли воды. Практически одни и те же лозунги, одни и те же требования, близкие схемы действий с небольшими нюансами, объясняющиеся местными условиями. А победа достигается массированным информационным давлением. Как пишет С.Г. Кара-Мурза: «Хорошо построенной системой СМИ является такая, что при изобилии изданий и передач, разнообразии «позиций» и стилей она создает и использует одни и те же стереотипы и внушает один и тот же набор главных желаний. Различие взглядов *конструируется* — разрешается быть и буржуазным консерватором, и анархистом, но при условии, что структура мышления у них одинакова»[46]. Все сказанное в полной мере относится и к такому СМИ, как Интернет. Главное, заполнить «собой» потоки, которые адресованы потенциаль-

---

[45] *Арабская весна* — волна демонстраций и путчей, начавшихся в арабском мире 18 декабря 2010 года. Произошли перевороты в Тунисе, Египте и Йемене; странами НАТО и их союзниками была совершена вооруженная интервенция в Ливию, ставшая продолжением неудавшейся информационной операции, которая привела к уничтожению законной власти и убийству лидера нации Каддафи; гражданское восстание в Бахрейне; массовые протесты в Алжире, Ираке, Иордании, Марокко и Омане; и менее значительные протесты в Кувейте, Ливане, Мавритании, Саудовской Аравии, Судане, Джибути и Западной Сахаре.

[46] *Кара-Мурза С.Г.* Манипуляция сознанием. М.: ЭКСМО, 2001. 832 с.

ной жертве и «свидетелям», которые благодаря своему согласию одобряют военную агрессию в случае, если одних информационных акций недостаточно. Когда речь идет о формировании промышленного потока, мелкие особенности не играют принципиальной роли. Главное, чтобы материал был вовремя подготовлен и вовремя доставлен в той форме, которая наиболее удобна для восприятия. Заниматься штучным изготовлением, значит — заведомо проигрывать по времени. А проигрыш по времени — это и есть проигрыш информационной войны. Обратной дороги у жизни не бывает. Поэтому информационные операции проектируются по типовым шаблонам и реализуются в условиях жесткой исполнительной дисциплины с широким охватом всего заданного в рамках операции региона.

Довольно часто высказывается позиция о якобы невозможности проектирования ИО, выполнение которых требует длительного временного интервала — месяц, год. Аргументы опираются на все возрастающую динамику мировых событий, которые не могут быть учтены и которые «размывают» план. Именно этим объясняется отсутствие типовых ИО. На наш взгляд, данное утверждение на современном этапе развития общества уже потеряло свою адекватность. В условиях управляемости СМИ, в условиях *хорошо построенной системы СМИ*, далеко не всем происходящим в мире событиям уделяется заслуженное внимание. Основное внимание уделяется именно тем событиям, которые важны для успешного проведения информационной операции. Те же события, которые способны размыть планируемую ситуацию, как правило, замалчиваются. При таком подходе ИО могут успешно планироваться и реализовываться и, более того, формироваться на базе типовых шаблонов, что и подтверждается успешностью цветных революций и арабской весной.

## 4.1. Планирование информационной операции

Информационная операция начинается с формирования задания на операцию и его утверждения заказчиком, после чего уже запуска-

ется отработанный механизм планирования и реализации, включающий в себя:

1. Формулирование желаемого результата.
2. Придание результату товарного вида.
3. Определение путем тестирования, опросов населения наиболее популярных субъектов, т.е. лиц, обладающих максимальной информационной энергией.
4. Определение множества СМИ, в том числе ресурсов Интернет, совокупное воздействие которых позволяет «покрыть» достаточное для принятия положительного решения множество лиц, ответственных за данное решение (например, для законопроекта — депутаты думы, для выборов президента — население).
5. Подготовить и распространить соответствующие информационные материалы.

Перейдем к формальной постановке задачи.

### *4.1.1. Матрица действий*

Задание на ИО включает в себя:

– целевое действие (множество действий), ради которого проводится операция;

– время (множество временных интервалов), когда должно произойти это действие.

На основании задания готовится план. План проведения информационной операции — обязательный элемент любой информационной операции. План включает в себя:

– множество взаимоувязанных действий, которые необходимо совершить или которые должны произойти;

– время (временные интервалы), в которое должны произойти эти действия;

– субъекты, которые должны совершить эти действия.

Часто под планом работы понимают матрицу действий по проведению информационной операции, включающую в себя все выше перечисленные компоненты, но имеющую двумерную форму представления — более удобную для анализа и контроля. Пример матрицы действий приведен на рис. 4.1.1.1.

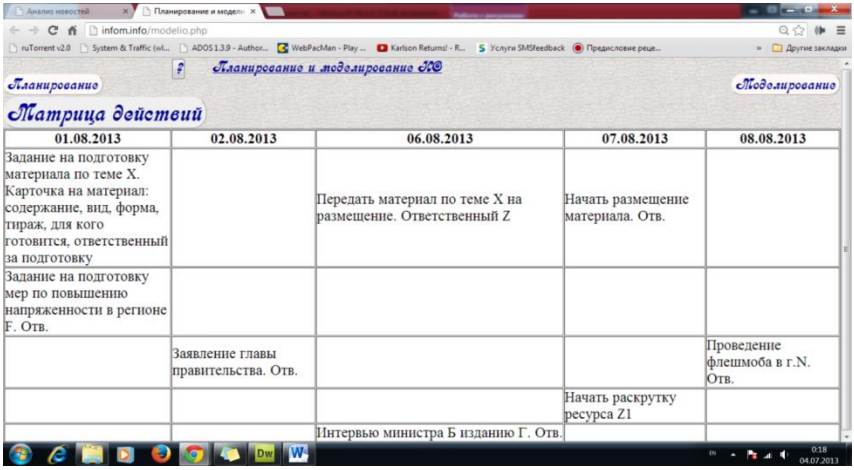



РИСУНОК 4.1.1.1. *Матрица действий*

В дальнейшем план проведения информационной операции и матрицу действий информационной операции будем считать синонимическими понятиями.

### *4.1.2. Формальная постановка задачи на формирование плана информационной операции*

Формирование матрицы действий начинается с цели, ради которой и планируется информационная операция.

**Цель** — действие/событие (множество действий/событий), в котором заинтересован автор информационной операции. Поэтому для цели, как и для любого действия, характерно время (множество временных интервалов), когда оно произошло, и субъект (множество субъектов), который его совершит. При этом важно, что субъекты, которые должны совершить целевое действие, не относятся к собственным силам и средствам. В том случае, если субъекты, от которых зависит достижение цели информационной операции, относятся к собственным силам, то проведение информационной

операции не имеет смысла, ибо все уже достигнуто и может быть выполнено по команде собственными силами.

Даже частичная автоматизация процесса формирования плана на проведение информационной операции на базе поставленной цели требует формализации процесса, введение строгих обозначений основных понятий и связей между ними.

Задание на проведение ИО содержит в себе цель ИО. Задача конкретных разработчиков заключается в том, чтобы наполнить целевое действие содержанием в части:

– определения ресурсов, если они не определены в задании на ИО;

– формулирования требований к материалу, если он не является приложением к заданию на ИО, в частности, определение содержания, вида и характера материала;

– определения способа доставки материала, если он не указан в задании на ИО;

– расчета времени, когда реально выполнить целевое действие, если оно не указано в задании на ИО;

– определения субъектов, если они не определены в задании на ИО, способных выполнить данное действие.

Для формализации описания введем следующие обозначения:

$d_ц$ — целевое действие или множество действий, относимых к целевому. Допускается, что цель может быть выражена через множество действий, которые могут иметь и одно наименование. Например, целевое действие «арабская весна» может быть сопоставлено одному событию, под которым понимаются революции в нескольких арабских странах, а может быть сопоставлено революциям с конкретным указанием стран;

D — множество возможных действий ($d \subset D$);

M — множество информационных материалов ($m \subset M$);

$m^-$ — материал, отрицающий материал m;

R — множество ресурсов, на которых размещаются информационные материалы;

S — множество субъектов, способных совершать действия из множества D ($s \subset S$);

N — число субъектов, $N = | S |$;

$S_s$ — множество субъектов, принадлежащих к собственным силам, $S_s \subset S$;

S(d) — множество субъектов, подготовленных (согласных) совершить действие (множество действий) d;

$t(d_ц)$ — множество временных интервалов, когда должно быть совершено действие (множество действий) $d_ц$;

$T(d_ц)$ — множество временных интервалов, когда может быть[47] совершено действие (множество действий) $d_ц$.

Таким образом, мы определили базовые множества, являющиеся исходными данными для формирования плана ИО. Теперь введем ряд функций на них.

*Справочные функции*

$s = F_п(d,S)$ — функция определения (поиска) множества субъектов, у которых есть реальная возможность совершить множество действий d. Если речь идет об использовании государственных служащих в качестве субъектов при проведении информационной операции, то разработать данную функцию несложно. Функция $F_s$ задается на базе множества должностных обязанностей и инструкций. В ходе современной тенденции на стандартизацию сферы управления и перевода ее на стандарты ISO 9000 должностные обязанности становятся все более формализованными и создаются на базе стандартных шаблонов. Как правило, они не являются закрытыми и в рамках электронного правительства доступны через Интернет. А это значит, что при грамотном синтаксическом и семантическом анализе текстов инструкций по ведомствам и министерствам результат можно получать чуть ли не в режиме реального времени.

$s = F_г(d,S)$ — функция определения (поиска) множество субъектов, потенциально готовых совершить множество действий d. Но при этом совсем не обязательно, что у них есть такая возможность. Получить значение для данной функции реально путем организа-

[47] В данном случае под термином «может быть» понимается, что данное действие будет совершено независимо от информационной операции, просто в силу регламента или какой-либо формальной процедуры, или в рамках выполнения должностных обязанностей того или иного лица.

ции интернет-тестирования, интернет-панелей и т.п. способов тестирования и сбора данных о состоянии посетителей ресурсов.

$m_d = F_m(s,d)$ — характеристика субъектов или материал, с которым согласны субъекты s, готовые совершить действия d.

$d = F_d(m_d)$ — действия, которые готовы совершить субъекты, согласные с материалом $m_d$.

$m_x = F_x(s)$ — тексты, характеризующие субъектов s. Как правило, эти данные получаются с помощью тестирования интернет-панелей.

$t = F_t(d,S)$ — функция определения множества временных интервалов, в которые может быть совершено действие d. Частичная автоматизация данной функции возможна благодаря организации доступа к следующим данным:

* времени на распространение сообщений различных СМИ, включая ареал распространения. Например, для случая, когда действие — это доставка информации до определенной группы лиц. Все сказанное относится и к ресурсам сети Интернет. Только в случае сети — это число посетителей тех или иных сайтов с учетом географического расположения посетителей, что можно определять по IP-адресу посетителя;

* расписанию встреч должностных лиц на различных саммитах, встречах в верхах и т.п. Например, для случая, когда заявление, являющееся компонентом ИО, должно быть сделано по результатам именно встреч в верхах;

* расписанию конференций, праздников, знаменательных событий, дней рождения и т.п. Например, когда заявление, являющееся компонентом ИО, должно исходить от ученых или определенных известных лиц. В данном случае праздник — повод взятия интервью, приурочивание одного события к другому — информационному действию;

* расписанию работы должностных лиц, планам командировок и т.п. Например, ИО привязана к действиям должностных лиц. Так, к посещению высшими должностными лицами России Курильских островов, совершаемому по заранее известному плану, может быть специально подготовлена информационная акция, что и было сделано определенными кругами в Японии.

$r = F_r(s)$ — функция определения множества ресурсов, которые посещаются субъектами s.

$s = F_s(r)$ — множество субъектов, которые посещают ресурсы r.

$z = Z_m(m_d)$ — стоимость создания материалов m.

$z = Z_r(r)$ — стоимость охвата ресурсов r.

$z = Z_{-r}(r)$ — стоимость блокирования ресурсов r.

Теперь перейдем к формализации самих действий.

$\Psi(m_d,k,r)$ — функция-действие, в ходе применения этой функции k раз осуществляется навязывание материала $m_d$ на ресурсы r.

Для удобства восприятия будем считать, что область значения функции принадлежит множеству целых чисел от –N до +N, где (N = | S |.

N — материал для множества субъектов после размещения на ресурсе стал определяющим их поведение для всех субъектов.

0 — материал никак не повлиял на поведение субъектов.

–N — материал для множества субъектов изменил поведение всех на прямо противоположное.

При этом мы исходим из того, что распространяемые материалы подготовлены с учетом «правильного» восприятия зрителями и читателями. И не рассматриваем ситуацию, когда подготовленные материалы вызовут обратный эффект. Хотя подобный вариант довольно часто встречается на практике и вполне может быть использован для решения задач информационного противоборства.

Рассмотрим несколько вариантов планирования ИО, от простой операции до сложной.

### Вариант №1. Планирование на базе единого материала

В этом случае формальная постановка задачи планирования ИО может быть сделана следующим образом:

Пусть $d_ц$ — целевое действие, которое должны совершить субъекты S.

Для того чтобы оно было совершено, необходимо подготовить соответствующий этому действию материал и распространить его на множестве ресурсов, которые посещаются этими субъектами:

$M_d = F_m(S,d_ц)$.

$R = F_r(S)$.

Цель: максимизировать $\Psi(M_d,k,R)$.

При следующих ограничениях:

1. $Z_m(M_d) + n\ Z_r(R) + Z_{-r}(R) < Z_0$ — финансовые средства, выделенные на подготовку и проведение ИО.

2. $t(d_ц) \cap T(d_ц)$ не пусто.

При такой постановке задачи планирование ИО сводится к подготовке материала $M_d = F_m(S,d_ц)$, формированию и разведыванию множества ресурсов, посещаемых субъектами S.

Судя по публикуемым материалам СМИ, сегодня информационные операции именно так и готовятся. Нюансы не играют никакого значения — только массированное информационное давление. По схеме этого варианта раскручивается информационная операция применительно к Сирии, которую мы условно назвали «Химическое оружие. Сирия».

Предложим аналитическое выражение для функции $\Psi(M_d,k,R)$. Очевидно, что значение этой функции тем больше, чем больше множество R, чем полнее соответствует материал $M_d$ состоянию субъектов S ($S = F_s(R)$), и чем больше сделано попыток «навязать» данный материал — k.

С учетом сделанных предположений предлагается следующее аналитическое выражение:

$$\Psi(M_d,k,R) = |\ S\ |\ (1 — (\ 1 — |\ M_d \cap F_x(S)\ |\ /|\ F_x(S)|\ )^k). \qquad (4.1)$$

Здесь

$|\ S\ |$ — число посетителей ресурса R;

$|\ M_d \cap F_x(S)\ |$ — похожесть[48] или выделение общего в текстах (материалах), которые характеризуют субъектов сейчас $F_x(S)$, и $M_d$, которые должны характеризовать субъекты, способные совершить соответствующие действия. В данном случае предполагается, что операция пересечения множеств текстов $M_d \cap F_x(S)$ оставит одинаковые в этих текстах формализованные поля. Результатом пересечения останется текст, состоящий из множества формализованных полей, присутствующих в обоих текстах в неизменном виде. Ре-

[48] В данном случае речь идет о таких понятиях, как похожесть текста на текст, понимаемость текста текстом и агрессивность текста к тексту, которые предложены в работе: *Расторгуев С.П.* Информационная война. Проблемы и модели. М.: Гелиос АРВ, 2006.

зультатом оценки мощности полученного множества $| M_d \cap F_x(S) |$ будет число общих полей (точек зрения).

$| F_x(S)|$ — число формализованных полей в текстах, полученных в ходе тестирования субъектов S. Здесь надо помнить, что процесс тестирования может выполняться не обязательно в явной форме с согласия субъекта, но и в скрытой (путем задания непрямых вопросов), а также с привлечением экспертов (соседей, знакомых, коллег по работе, по соцсетям и т.п.).

$(1 — ( 1 — | M_d \cap F_x(S) | / | F_x(S)| )^k)$ — оценка вероятности, что за k ознакомлений субъект S согласится с материалами $M_d$.

Если произвести замену $S = F_s(R)$, чтобы исключить переменную S, которая отсутствует в явном виде в функции Ψ, то окончательный вариант будет таким:

$$\Psi(M_d,k,R) = | F_s(R) | (1 — ( 1 — | M_d \cap F_x(F_s(R)) | / | F_x(F_s(R))| )^k). \qquad (4.2)$$

## Вариант №2. Планирование с учетом индивидуальных особенностей субъектов

В то же время учет индивидуальных предпочтений субъектов S способствовал бы повышению эффективности ИО и снижению общих затрат. Учет индивидуальных предпочтений возможен, если провести разбиение множества S на подмножества:

$$S = \cup s_i,$$

и в дальнейшем готовить материал, ориентированный на конкретные подмножества субъектов. Тогда общая постановка задачи планирования будет выглядеть следующим образом.

Пусть $d_ц$ — целевое действие, которое должны совершить субъекты S.

Для того чтобы оно было совершено, необходимо провести разбиение субъектов S по интересам и политическим предпочтениям, а затем подготовить соответствующий этому действию материал, ориентированный на конкретные группы субъектов:

$m_{di} = F_m(s_i,d_ц)$.

$r_i = F_r(s_i)$.

$$\text{Max} \sum \Psi(m_{di},k_i,r_i)$$

При следующих ограничениях:

1. $\sum Z_m(m_{di}) + \sum n_i Z_r(r_i) + \sum Z_{-r}(r_i) < Z_0$ — финансовые средства, выделенные на подготовку и проведение ИО.

2. $t(d_ц) \cap T(d_ц)$ не пусто.

При такой постановке задачи планирование ИО сводится к разбиению всего множества субъектов на подмножества по «интересам» и подготовке для каждого подмножества материалов, ориентированных именно на данное множество субъектов.

### Вариант №3. Планирование с учетом разбиения цели на подцели

При планировании ИО по первому и второму варианту мы исходили из того, что достижение цели осуществляется непосредственно на первом этапе ИО. Как правило, так оно и есть. Но в отдельных случаях, как, например, в случае информационной войны против СССР, достижение цели предполагало ряд этапов, т.е. чтобы достичь цели, надо было совершить целую последовательность дополняющих друг друга действий. Перепрограммирование осуществлялось этапно. Прежде чем перейти к подготовке субъектов на совершение $d_ц$ действия, они готовились к совершению действий, близких к целевому.

В данном варианте планирование ИО осуществляется, начиная с построения цепочки множеств действий типа: $d_1,d_2,d_3,\ldots d_i,\ldots,d_ц$. После чего по каждому множеству действий применяется вариант планирования №2 или №1.

В случае применения вариантов №2 и №1, а особенно №1, адекватность распространяемой информации реальным процессам уже не играет никакой роли, важно только массированное информационное давление, важна только величина $n_i$ в формуле $\Psi(m_{di},k_i,r_i)$, которая во многом определяется возможностями агрессора — $Z_0$.

Довольно часто для подтверждения своих текстов используются специально созданные фальшивки ($m_i$), особенно когда необходимо показать агрессивность и «бесчеловечность» той или иной страны и ее лидеров. Чтобы выйти на «дружное» осуждение исторического деятеля и факта, специально переписывается история. Реанимация из ничего якобы существовавшего действия $d_n$, в конце-то концов,

приводит к возможности реализации действия $d_ц$. Как гласит основной закон информационной войны: «Доказанная взаимосвязь несуществующих событий становится законом, определяющим поведение реальных субъектов»[49].

«Вот, скажем, такой пикантный моментик. По официальной версии Договор о ненападении между Германией и СССР и «секретный протокол» к этому договору были подписаны одновременно в Москве в рабочем кабинете Сталина в ночь с 23 на 24 августа 1939 г. Но почему-то они отпечатаны на разных пишущих машинках. Выходит, у Сталина была специальная пишущая машинка, на которой печатали только секретные сделки с Гитлером? Да, прямым доказательством подлога это не является, потому что гипотетически пишущая машинка после того, как на ней отпечатали текст договора, могла сломаться и «секретный протокол» к договору печатали на другой. Договор с «протоколом» отпечатаны на двух языках — русском и немецком. Для печати «секретного протокола» из советского комплекта использована тоже другая машинка с немецким шрифтом. Какова вероятность, что обе машинки — с русским шрифтом и немецким — сломаются одновременно?»[50] и т.д. еще десятки несоответствий.

Подробнее можно почитать в работе А. Кунгурова «Секретные протоколы, или Кто подделал пакт Молотова—Риббентропа»[51].

Это не единичный случай, подобных примеров по истории СССР достаточно много. Они были нужны, чтобы создать образ жуткого врага, для уничтожения которого годятся любые средства.

---

[49] *Расторгуев С.П.* Информационная война. Проблемы и модели. М.: Гелиос АРВ. 2006.

[50] *Кунгуров А.* Как обделавшийся профисторик Исаев подтерся пактом Молотова—Риббентропа //http://kungurov.livejournal.com.

[51] Книга посвящена исследованию проекта американских спецслужб по внедрению в массовое сознание мифа о существовании неких секретных протоколов, якобы подписанных Молотовым и Риббентропом 23 августа 1939 г. одновременно с заключением советско-германского Договора о ненападении. На основе стенограмм Нюрнбергского процесса автор исследует вопрос о первоисточниках мифа о секретных протоколах Молотова—Риббентропа, проводит текстологический и документоведческий анализ канонической версии протоколов и их вариантов, имеющих хождение, рассказывает о том, кто и зачем начал внедрять миф о секретных протоколах в СССР. А также кем и с какой целью было выбито унизительное для страны признание в сговоре с Гитлером. См.: www.etextlib.ru/Book/Details/42285.

Демонизировать Сталина необходимо не ради демонизации, а ради настоящего и будущего. Происшедшие события забываются, свидетели умирают, архивы переписываются. В этих условиях история, как и любая религия, формируется опираясь на веру. Например, есть событие — атомная бомбардировка японских городов. Кто палач, отдавший приказ? Злодеи коммунисты или свободолюбивые демократы? Ответ понятен и не требует доказательств. Ибо только злодеи на подобное способны.

В информационную эпоху создавать фальшивки стало проще, используя соответствующее программное обеспечение, а распространять еще проще, благодаря Интернету, куда сегодня и переместился основной центр изготовления и распространения фальшивок.

Как уже говорилось выше, через d мы обозначаем множество однотипных действий, которые могут выполняться параллельно. В условиях информационной войны против СССР последовательность была немаленькой, перечисление хватило было для хорошего отчета не на одну тысячу страниц. Для удобства иллюстрации мы выбрали более простой пример ИО, включающий в себя последовательность всего из трех множеств действий: $d_1$, $d_2$, $d_3$, $d_ц$.

Схема информационной операции по дискредитации интернет-ресурса приведена на рис. 4.1.2.1.

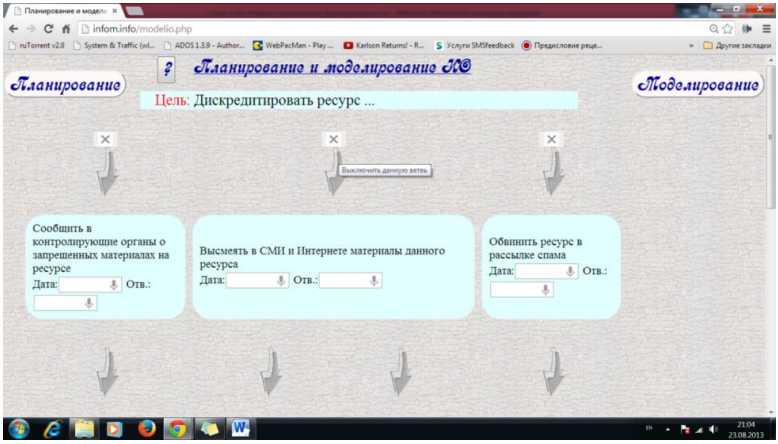



РИСУНОК 4.1.2.1 *Схема по дискредитации интернет-ресурса*

На рис. 4.1.2.2. изображено следующее дерево действий:

Целевое действие ($d_ц$):

– дискредитировать ресурс.

Действия, приводящие к целевому ($d_3$):

– сообщить в контролирующие органы о запрещенных материалах на ресурсе;

– высмеять в СМИ и Интернете материалы данного ресурса;

– обвинить ресурс в рассылке спама.

Действия, приводящие к $d_3$ ($d_2$):

– разместить на ресурсе материалы, подпадающие под запрещенные (методы размещения: взлом ресурса, комментарии к новостям, форум/чат);

– разместить на ресурсе материалы издевательского над ресурсом характера (методы размещения: взлом ресурса, комментарии к новостям, форум/чат);

– создать искаженное зеркало ресурса (методы: создание и регистрация специального собственного сайта);

– организовать почтовую рассылку спама от имени данного ресурса (методы: организовать анонимный доступ в Интернет).

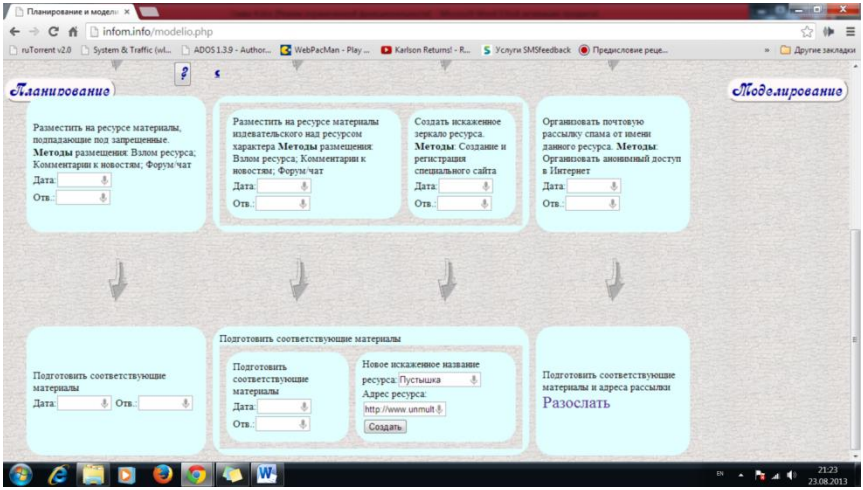



РИСУНОК 4.1.2.2. *Пример дерева действий*

Действия, приводящие к $d_2$ ($d_1$):

– подготовить соответствующие материалы;

– придумать новое искаженное (издевательское) название ресурса;

– подготовить соответствующий спам и адреса рассылки.

Затем подготовленная схема наполняется адресами конкретных ресурсов (R). Далее осуществляется предварительный анализ, на основании которого проводится оценка стоимости и времени на выполнение действий плана. После чего выполняется окончательный расчет и общая оценка вероятности достижения цели.

## 4.2. Моделирование информационной операции

Моделирование ИО важно потому, что в случае некорректно подготовленной и проведенной операции, не давшей задуманного результата, повторение ее будет осуществляться уже по модифицированному, т.е. частично перепрограммированному субъекту. А это потребует серьезного изменения исходных данных, по сути, подготовки совсем новой операции.

В то же время многие действия, составляющие ИО, бессмысленно моделировать. Вопрос о включении в состав своих сил и средств тех или иных ресурсов решается административными и финансовыми методами. Тираж заказывается из соображений охвата нужной аудитории. Возможность скрытого взятия под контроль тех или иных ресурсов определяется талантом собственных специалистов и количеством дыр в системе безопасности ресурса. И то и другое можно оценить достаточно точно. В отличие от воинской операции, в которой всегда присутствует спектр результатов — выполнение поставленной задачи, потери живой силы и техники своей и чужой, в информационной операции существует только один результат — перепрограммирование (переориентация) заданной группы субъектов на совершение ими целевых действий. В условиях отсутствия противника, или пусть не противника, а хотя бы того, кто способен противодействовать ИО, заниматься вопросами моделирования ИО нет смысла.

Задача моделирования становится важной, когда появляется противник. Но с появлением противника сама задача моделирования ИО уже решается классическими методами. Для этого требуются следующие исходные данные: собственные силы и средства, силы и средства противника, перечень возможных специальных действий в ходе ИО, цель и задачи ИО. Сами сражения ведутся за контроль над ресурсами, посещаемыми субъектами.

Противники решают одну и ту же задачу, но каждый для себя — это максимизировать $\Psi(M_d,k,R)$ при следующих ограничениях:

1. $Z_m(M_d) + n\ Z_r(R) + Z_{-r}(R) < Z_0$ — финансовые средства, выделенные на подготовку и проведение ИО.

2. $t(d_ц) \cap T(d_ц)$ не пусто[52].

Вот здесь и начинается искусство информационного противоборства: какой ресурс лучше сдать противнику, если нет сил на нем победить, а какой оставить за собой.

Победа в противоборстве во многом зависит от выделенных ресурсов на операцию, от полноты и точности составленного плана (никто не забыт) и от того, как рано или поздно противник выявит операцию и начнет противодействовать.

На рис. 4.2.1 схематично показано игровое поле боя двух соперников (Игрок №1 и Игрок №2), которые сражаются за ресурсы, влияющие на своих посетителей.

---

[52] Подробнее см. *Вариант №1. Планирование на базе единого материала*, стр.106-108

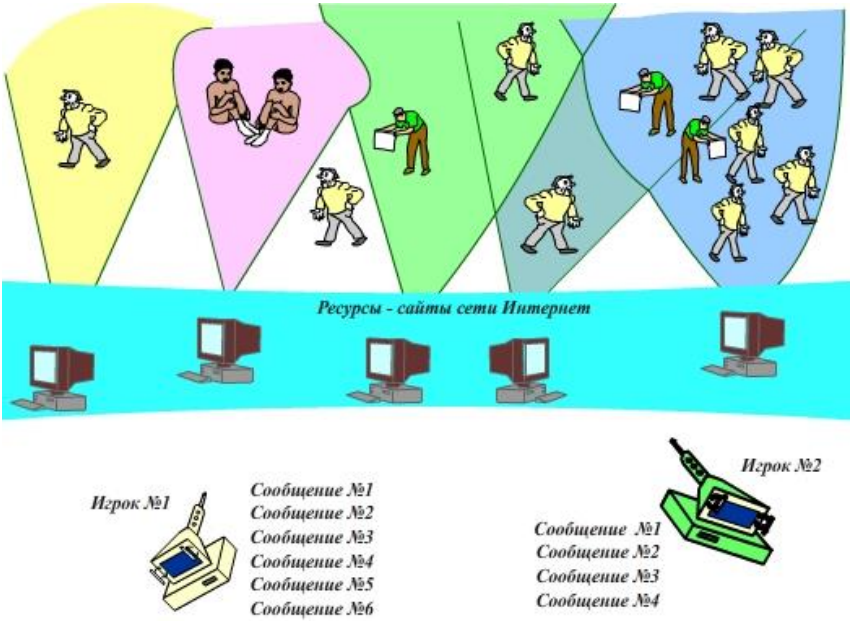



РИСУНОК 4.2.1. *Схема виртуального поля боя*

В сражении используются следующие игровые атрибуты:

* значимость ресурса, которая оценивается через число посетителей ресурса. Захватить все значимые ресурсы — значит, победить. Это один из важнейших параметров, сродни стратегическим высотам на реальном поле боя. Но между виртуальными и реальными высотами есть существенная разница, которая заключается в том, что виртуальные «высоты» могут быть обманчивы. В сети существуют не афишируемые, но посещаемые ресурсы. Однако есть и такие, на которых практически не бывает посетителей, кроме роботов, накручивающих счетчики посещений. Такие ресурсы в чем-то сродни надувным танкам. Силы и средства на них можно потратить значительные, а результат будет равен нулю;

* снаряды — сообщения. Эти «снаряды» различаются «убойной силой», т.е. состоянием тех, на кого они падают. Можно завалить читателя самой интересной литературой, но если он не умеет читать на этом языке, то все окажется зря. Понятно, что предпо-

чтение всегда отдается ярким видеорепортажам с места событий. Видео посмотрит или хотя бы начнет смотреть большинство посетителей. Соответствие новостного сообщения состоянию зрителя — это одна из специальных задач, которая при моделировании решается отдельно. По своей «убойной силе» сообщения не равны друг другу. Но значимость может быть повышена их повторением, условно говоря, сотня «автоматчиков» компенсирует одного «пулеметчика». Если в рамках игровой ситуации сообщения от противников попадают на общий ресурс, то для ситуационного моделирования проводится оценка «близости» этих сообщений $M_{d1}$ (сообщение, произведенное Игроком №1) и $M_{d2}$ (сообщение, произведенное Игроком №2) состоянию «среднего» посетителя. Аналитическое выражение *4.2*, позволяющее оценить степень «захвата» ресурса, содержит и меру близости сообщений и частоту их подачи;

* скорострельность стрельбы — количество новостей нужной тематики в единицу времени. Читатель идет туда, где есть новости. Поэтому если новостей нет, то их придумывают;

* броня, которую надо пробить, — защищенность того или иного ресурса. С администрацией ресурса можно договориться, можно запугать, купить. Сам ресурс можно забанить, подвергнуть DDoS-атаке, заразить вирусом. Понятно, что если противнику известны особенности защитных механизмов, оставленные разработчиками «люки», или у противника на этом ресурсе уже заранее установлено какое-то программное обеспечение собственной разработки, то вопрос проникновения на ресурс решается в его пользу;

* приз — число посетителей ресурса.

Ресурс считается захваченным игроком, если сообщений, отвечающих его задачам, на данном ресурсе окажется больше, чем сообщений противника.

Игрок считается победителем, если под его влияние попало больше половины посетителей ресурсов, за которых идет сражение.

Данный подход, предложенный к моделированию информационных операций, распространяется и на техническую составляющую с учетом следующих аналогий:

сообщения — программные коды, содержащие соответствующие включения в виде программных средств скрытого информационного воздействия;

броня, которую надо пробить, — антивирусные и другие средства защиты ресурсов.

# Заключение

Подводя итог сказанному, руководствуясь правилом, сформулированным в работе в приложении к информационным воздействиям: **непонятность изложения материала компенсируется многократностью его подачи**, еще раз повторим основные результаты.

Кнут, пряник, убеждение — эти средства управления на разном этапе развития общества имели разную значимость. Сегодня, в информационную эпоху, превалирует убеждение, производство которого поставлено на промышленную основу. Убеждают на примерах применения кнута и пряника. Настоящие это примеры или выдуманные, уже не имеет значения. Важнее другое — кто громче и выразительнее кричит. Новая информационная среда позволяет в промышленных масштабах генерировать, заставлять слушать и верить этим крикам (сообщениям) в пределах своего ареала распространения. Для информационного монополиста, планирующего передел мира, это уже даже не крик, а рычание готовящегося к прыжку хищника. Это предупреждение о намерениях. Наличие этого предупреждения является своего рода подсказкой выбранной жертве.

Но кто предупрежден, тот вооружен. Поэтому мониторинг того же Интернета на предмет выявления информационных угроз является составной частью мониторинга политической и военной безопасности. Однако мониторинг мониторингу рознь — можно смотреть и не видеть, можно слышать, но не понимать.

В работе предложен и обоснован подход к построению систем выявления информационных угроз. Чтобы понять угрозы, нужно понять механизм их создания. С этой целью был проведен анализ задач, решаемых в телекоммуникационных средах с помощью информационных операций, а затем — классификация информационного оружия в рамках следующих направлений применения:

– разведка;

– проведение информационных операций;

– планирование информационных операций, управление процессом их проведения и оценка результативности.

Именно эти три направляющих оси положены в основу структуры книги. И именно на эти оси и нанизаны основные результаты, к которым относятся следующие:

1. Проведено предварительное исследование новостных тематик, предшествующих вооруженному конфликту. Результатом этого исследования стал набор тем, рекомендуемых для мониторинга новостей.

2. Опираясь на оценку эффективности перепрограммирования субъектов информационного воздействия, предложен подход к получению вероятностных критериев оценки факта начала информационной операции на базе динамики новостных тематик.

3. Проведены исследования на макете и предложены удобные для восприятия формы отображения динамики изменения количества новостных сообщений по темам. Обосновано наличие необходимой, дополнительной и справочной информациии.

4. Проведено исследование специальных действий, присущих информационным операциям в сети Интернет. Показано, что производство практически всех компонент информационной операции уже поставлено на промышленную основу: от вирусов, нацеленных на автоматизированные объекты военного и промышленного назначения, до генераторов сообщений в виде текстов, голосовых сообщений по заданной голосовой характеристике или видеосюжетов по заданной исходной «картинке».

5. Одним из наиболее сложных и затратных по времени является этап планирования информационной операции. В работе предложен подход, позволяющий частично автоматизировать этот процесс за счет использования типовых схем их проведения. Предложена формальная постановка задачи на планирование информационной операции.

К важным результатам работы относим полученную аналитическую зависимость количества «перепрограммированных» посетителей ресурса от качества подготовленного материала и частоты его подачи — формула *4.2*.

В работе показано, каким образом возможна организация игро-

вого тренинга по моделированию проведения информационных операций.

Изложенные в работе результаты относятся не только к информационному противоборству на межгосударственном уровне, но и на локальном уровне. На глобальном уровне уже сложился монополист, и именно он всегда делает первый ход, еще больше усиливая свою позицию. А вот локальные информационные конфликты — в первую очередь, конечно, местные выборы — еще пока не потеряли остроты, которую придает неопределенность подведения итогов.

Однако, несмотря на то что книга получилась в большей степени с практическим уклоном, все ж таки главным желанием было показать глубокую связь всех тех баталий, которые сегодня идут в сети, со сражениями в эмпирическом мире, более того, тенденцию смены ролей ведущего и ведомого между этими мирами. Когда-то утверждалось, что бытие определяло сознание, сегодня поставленные на конвейер образы сознания обрекают многих на жалкое бытие. Модели торжествуют, определяя поведение субъектов эмпирического мира. Современные модели легко переписывают историю.

Победил СССР Германию — и весь мир осудил фашистский режим, уничтоживший польских офицеров в Катыни. Победило НАТО в холодной войне над Советским Союзом, и российская дума осудила СССР за, якобы, расстрел всё тех же поляков.

Если вдруг в ходе дальнейшего информационного противоборства распадется США на много маленьких государств, как обещал И. Панарин[53], то уцелевшие поверят, что уничтожение башен-близнецов было на самом деле провокацией американских спецслужб, типа поджога рейхстага, сигналом к началу кровавого похода на устои старого мирового порядка.

Человек желает, верит, думает и делает. И если реальность бытия расходится с его модельными построениями, то человек, имеющий ресурсы, подправляет не модель, а эту самую реальность бытия. Например, согласись Россия и Китай еще два месяца назад осудить Сирию, не пришлось бы травить людей зарином ради нужных новостных сообщений, затребованных моделью информационной операции.

---

[53] *Панарин И.* Крах доллара и распад США // www.litmir.net/bd/?b=119288.

И последнее, если разница между миром и его желаемым представлением станет расти все больше и больше, то откроется пропасть, в которую и провалится вся наша цивилизация. Информационные войны работают против нас, они сносят тот фундамент, на котором стоит человеческая цивилизация. Если «надуваемой» модели нового мирового порядка понадобится себя подкрепить нужными новостями, то ради них в дело может пойти и ядерное оружие. Например, взбунтовались жители какого-то города и перекрыли трассу. И тут вдруг кто-то по этому городу наносит удар тактическим ядерным оружием. Кто? Конечно, злодеи! А кто злодеи? Злодеи — собственное правительство. А раз так, то всему мировому сообществу надо срочно принимать ответные меры.

Разве подобного еще не было?

Военная операция против Сирии возможна без санкции Совета безопасности ООН после того, как в этой стране было применено химическое оружие, заявил 26.08.2013 министр иностранных дел Великобритании Уильям Хейг.

Не правда ли, знакомая песня?

# Глоссарий

Аватаризация — этап развития информационной составляющей человеческого общества, приходящий на смену монотеизма в понимании сущности информационного существа, при котором выделяются информационные копии человека разумного на основе расщепления, синтеза и наполнения его информационного образа. Аватар — информационная поименованная диалоговая система, созданная по образу и подобию, способная адаптироваться к любым входным данным для достижения поставленной цели.

Актор (лат. *actor* — деятель) — индивид, общественная группа, институт или другой субъект, осуществляющий конкретные действия; сторона, участвующая в конфликте. В программировании актор — программная сущность заданной структуры и механизмов взаимодействия; содержит данные и процедуры, обладает инкапсуляцией, отношениями, наследованием и может порождать сообщения. В социологии — 1) действующий субъект; индивид, совершающий действия, направленные на других. Например, лидер общественного мнения; 2) участник преобразований, движимый собственными мотивами и обладающий для этого соответствующим опытом. Акторы могут иметь неоднозначные мотивы, ожидания, эмоциональные переживания, связанные с неопределенностью последствий совместных преобразований и «неизреченностью=непроявленностью собственных смыслов». В политологии — субъект политики, участник мировой политики, который может влиять на процессы, происходящие в мире.

Алгоритм — множество команд, связанных одним замыслом (целью), с заданным порядком применения по каждой команде, позволяющим по каждому исходному данному или аргументу из некоторой совокупности возможных исходных данных (аргументов) получить результат для выдачи вовне, если такой существует, или не получить ничего, и/или самомодифицироваться.

Анализ — выявление свойств целого (объекта) путем мысленного или реального разделения его на составные части.

АНАЛИТИКА — вид интеллектуальной деятельности, направленный на получение обобщений (выводов) и рекомендаций на основе применения процедур анализа и синтеза.

АНАЛИТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ — деятельность, основанная на аналитике.

АНОНИМАЙЗЕРЫ — программы с интерфейсом, похожим на обычный поисковик, только вместо слов/фраз здесь нужно вводить URL того сайта, который следует посмотреть. Анонимайзеры представляют собой скрипты, написанные, например, на perl, php, cgi, которые реализуют обращение через определенные прокси.

АУДИОМАТЕРИАЛ — звук, записанный в виде устной речи (голос), звуковых эффектов разной тематики, музыки и их сочетаний и оформленный в виде аудиофайла, пригодного для размещения в сети Интернет.

БЛОГ (weblog) — регулярные записки в Интернете, представленные в обратном хронологическом порядке, содержащие краткие высказывания и комментарии к ссылкам на сторонние ресурсы.

БОТНЕТ (англ. *botnet*, МФА: [ˈbɒtnɛt]; произошло от слов *ro**bot*** и ***net**work*) — компьютерная сеть, состоящая из хостов и компьютеров пользователей с установленным на ней специальным программным обеспечением (бот), управление которым осуществляется с хостов.

ВЕБ-ФОРУМ — класс веб-приложений для организации общения посетителей веб-сайта.

ВЕБ-ЧАТ (англ. *chat* — разговор) — средство общения пользователей по сети в режиме реального времени, с помощью специального программного обеспечения, позволяющее организовывать такое общение.

ВЕС КЛЮЧЕВОГО СЛОВА (*keyword weight*) — отношение частоты использования ключевого слова к общему количеству слов на индексируемой странице, выраженное в процентах.

ВИДЕОМАТЕРИАЛ — аудиовизуальный материал, записанный в виде видеофайла в формате, пригодном для размещения в сети Интернет.

ГИПЕРМЕДИА — это гипертекст, в который включены графика, звук, видео, текст и ссылки, для того чтобы создать основу нелинейной среды информации.

Диалоговый квант — минимальная единица речевого общения, отражающая позиции всех участников диалога, но не более одного высказывания каждого участника.

Дорвеи — страницы и ресурсы, созданные специально для роботов поисковых систем, как правило, с большим количеством ключевых слов на странице.

Защита от «роботов» — совокупность приемов, применяемая для защиты сайтов от анализа и добавление данных программными средствами в автоматическом режиме, основанная на решении задачи из серии распознавания образов.

Знание — совокупность сведений, выраженная в структуре системы и функциональных возможностях ее элементов.

Интернет-ресурс (ресурс в сети Интернет, веб-ресурс, сайт) — совокупность электронных документов (файлов) частного лица или организации, объединенных под одним адресом (доменным именем или IP-адресом).

Информационная операция (общая форма) — совокупность взаимосвязанных действий информационного характера, направленных на решение поставленной задачи по перепрограммированию, блокированию, генерации информационных процессов как в технической, так и в гуманитарной сферах.

Информационная операция — распространение и навязывание совокупности взаимосвязанных сообщений, объединенных общей темой, имеющих тенденцию к устойчивому росту и направленных на изменение состояния общественного сознания.

Информационная энергия — возможность субъекта (модели) перепрограммировать окружающие информационные системы (модели), включая себя.

Информационное оружие — технические средства и технологии, целенаправленно применяемые для активизации, уничтожения, блокирования или создания в информационной системе процессов, в которых заинтересован субъект, применяющий оружие.

Информация — степень изменения знания субъекта.

Капча — CAPTCHA (англ. *Completely Automated Public Turingtest-to-tell Computers and Humans Apart*) — полностью автоматизированный пуб-

личный тест Тьюринга для различия компьютеров и людей. Основная идея теста: предложить пользователю такую задачу, которую с легкостью может решить человек, но которую несоизмеримо сложнее решить компьютерной программе.

Квант учебной информации — поименованная сущность (текст, речь, видео), несущая в себе элементарный смысл, достаточный для ответа, как минимум, на основной вопрос, породивший данную сущность.

Клонирование голоса — алгоритмический процесс, позволяющий создать аудиоматериал, содержащий имитацию голоса любого человека по его образцу.

Ключевое изображение (*key image*) — преобладающий образ, вокруг которого строится информационное обращение.

Ключевые слова (*keywords*) — слова, предположительно по которым должен находиться соответствующий текст, содержащий эти слова или отвечающий на эти слова, при поиске в поисковых системах.

Кросс-браузерность (*cross-browser*) — свойство сайта отображаться и работать во всех популярных браузерах идентично. Под идентичностью понимается отсутствие развалов верстки и способность отображать материал с одинаковой степенью читабельности.

Кросс-платформность (*cross-platform*) — программное обеспечение, работающее более чем на одной аппаратной платформе и/или операционной системе.

Модератор (*moderator*) — человек, имеющий более широкие права по сравнению с обыкновенными пользователями на общественных сетевых ресурсах (чатах, форумах и т.д.).

Мониторинг (англ. *monitoring* в переводе — отслеживание, на базе латинского корня *monitor* — напоминающий, предостерегающий) — процесс наблюдения и регистрации данных о каком-либо процессе с целью выявления его соответствия некоторому заданному сценарию.

Монтаж (фр. *montage*) видео- или аудиоматериала — процесс переработки или реструктурирования изначального материала, в результате чего получается иной целевой материал.

Мультимедиа — совокупность современных средств аудио-, теле-, визуальных и виртуальных коммуникаций, используемых в процессе организации, планирования и управления информационным взаимодействием.

Мультимедийный интернет-ресурс — интернет-ресурс, в котором основная информация представлена в виде мультимедиа в дополнение к традиционным способам предоставления информации, таким как текст.

Набор норм — набор предписаний, требований, пожеланий общественноодобряемого поведения.

Набор ролей — набор ожидаемых действий субъекта, за которым закреплены определенные функциональные обязанности.

Обученность — это реально усвоенный уровень знаний, умений и навыков.

Обучаемость — это восприимчивость к обучению, способность к учению. Показатель скорости и качества усвоения субъектом материала (*квантов диалога)* из прямых и косвенных источников (соответственно человека-пользователя и другого субъекта) и овладение материалом до степени активного применения.

Общественное мнение на базе ресурсов Интернет — представляет собой совокупность индивидуальных мнений по конкретному вопросу, затрагивающему группу людей, которые зафиксированы в виде мультимедийных материалов на ресурсах сети Интернет.

Парсер — программа, занимающаяся сбором содержимого страниц сайта, анализом, выделением данных и преобразованием данных к требуемому виду.

Парсинг — автоматизированный сбор контента или данных с какого-либо сайта или сервиса.

Поисковая машина (*search machinery*) — программный комплекс, который существует для поиска информации в Интернете.

Поисковая оптимизация (англ. *search engine optimization, SEO*) — комплекс мер для поднятия позиций сайта в результатах выдачи поисковых систем по определенным запросам пользователей.

ПРИОРИТЕТ РЕСУРСА — порядковый номер ресурса в последовательности ресурсов, упорядоченной по числу представляющих интерес для определенного множества посетителей.

ПРОКСИ-СЕРВЕР — исполняемая программа, которая постоянно опрашивает соответствующий порт, ожидая запросов по определенному протоколу. Как только установлено соединение с посетителем и получен запрос, программа транслирует этот запрос другому серверу от имени посетителя, а затем возвращает посетителю ответ.

РАЗВИТИЕ — целенаправленное накопление информации с последующим ее упорядочением, структурированием. Процесс последовательных, необратимых внешних и внутренних изменений, характеризующих переход от одних иерархий к другим.

РЕЛЕВАНТНОСТЬ — смысловое соответствие между информационным запросом и полученным сообщением.

РЕЛЕВАНТНОСТЬ САЙТА — степень соответствия текста и тематики сайта слову или выражению, заданному в качестве ключа при поиске информации.

САМОМОДИФИКАЦИЯ — применение множества команд, составляющих алгоритм, к самому этому множеству с целью изменения команд и/или изменение порядка применения команд из этого множества.

СНИФФЕР (англ. *to sniff* — нюхать) — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

СОЦИАЛЬНАЯ ГРУППА — совокупность индивидов, взаимодействующих определенным образом на основе разделяемых ожиданий каждого члена группы в отношении других.

СОЦИАЛЬНЫЕ СЕТИ (англ. *social networking service*) — онлайн-сервис, веб-сайт (совокупность веб-сайтов), предназначенные для построения, отражения и организации социальных взаимоотношений, пример: Twitter, Facebook.

СЦЕНА — описание обстановки и типовых ситуаций, присущих объектам сцены.

СЦЕНАРИЙ — последовательность сцен, описывающих процесс достижения конечной цели (решения задачи).

ТЕХНОЛОГИЯ — последовательность операций (мер, приемов, действий), совершаемых над исходным материалом для получения желаемого конечного продукта.

ФУТАЖ — видеофайл, содержащий видеофрагменты небольшой длительности разной тематики; используется для монтажа, повышая зрелищность, эффектность видеоматериала, а также его реалистичность, в качестве фона, на котором происходит основное действие.

ЮЗАБИЛИТИ (*usability*) — концепция разработки пользовательских интерфейсов сайта (программного обеспечения), ориентированная на максимальное психологическое и эстетическое удобство для пользователя.

ЭХО-ФРАЗА (*Tag line*) — короткое сообщение, выражение, стоящее в конце текстового рекламного обращения, которое повторяет (дословно или по смыслу) заголовок либо основной мотив обращения. Особенно эффективна эхо-фраза в информационных материалах большого объема.

ЮЗАБИЛИТИ-ТЕСТИРОВАНИЕ (*usability test*) — метод оценки удобства использования продукта, основанный на привлечении пользователей в качестве тестирующих.

ЯДРО АУДИТОРИИ (*Main body*) — количество постоянных посетителей сайта.

ЯЗЫК МОДЕЛИРОВАНИЯ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ (*VRML (Virtual Reality Modeling Language*) – подобен **языку разметки**, только описывает графические трехмерные объекты путем перечисления используемых в сцене примитивов и их координат. Позволяет создавать сложные сцены с наложением текстур, установкой источников цвета и камер.

ЯЗЫК ПОИСКОВЫХ ЗАПРОСОВ — набор метасимволов и правил, в соответствии с которыми строится запрос к поисковой системе.

ЯЗЫК РАЗМЕТКИ (*markup Language*) — набор символов или последовательностей, вставляемых в текст для передачи информации о его выводе или строении. Принадлежит классу компьютерных языков. Текстовый документ, написанный с использованием языка разметки, содержит не

только сам текст (как последовательность слов и знаков препинания), но и дополнительную информацию о различных его участках.

IP-АДРЕС (*айпи-адрес*, сокращение от англ. *Internet Protocol Address*) — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

JAVASCRIPT — язык программирования, тексты на котором предназначены для выполнения браузером на компьютере пользователя.

# Литература


1. *Кара-Мурза С.Г.* Манипуляция сознанием. М.: ЭКСМО, 2001. 832 с.
2. *Ленинджер А.* Биохимия. Молекулярные основы структуры и функций клетки. М.: Мир, 1976. 960 с., ил.
3. *Лобанов Б.М., Цирульник Л.И.* Компьютерный синтез и клонирование речи. Минск: Белорусская наука, 2008. 316 с.
4. *Расторгуев С.П.* Введение в теорию информационного противоборства: Учебное пособие. СПб.: СПбГТУ, 2000.
5. *Расторгуев С.П.* Информационная война. М.: Радио и связь, 1998.
6. *Расторгуев С.П.* Информационная война. Проблемы и модели. М.: Гелиос АРВ, 2006.
7. *Расторгуев С.П.* Основы информационной безопасности. М.: Академия, 2009.
8. *Расторгуев С.П.* Философия информационной войны. М.: МПСИ, 2002.
9. *Расторгуев С.П., Литвиненко М.В.* Аватаризация. СПб.: Реноме, 2011. 311 с.
10. *Расторгуев С.П., Токарев Р.С.* О направлении развития самообучающихся механизмов сети Интернет // Информатика и образование. 2009. №1. С. 79–86.
11. *Рашкофф Д.* Медиавирус. Как поп-культура тайно воздействует на ваше сознание. М.: Ультра. Культура, 2003. 368 с., ил.
12. Руководство по мемам: путеводитель пользователя по вирусам сознания (Версия 1.1) © Бретт Томас, 1995 // http://asocial.narod.ru/material/memes.htm.
13. *Устинова М.* Новые термины на русском языке. Глоссарий конфликтологических терминов. М.: Каллиграф, 2008. 96 с.
14. Словарь иностранных слов в русском языке для школьников и абитуриентов: более 9 000 слов / Сост. Е. Грубер. М.: ЛОКИД-пресс, 2006. С. 486.
15. *Табаков Д.* Атака StuxNet, оценка угрозы вирусной атаки // www.sald.ru/blog-1826/0/.
16. *Хелио Фред Гарсия*. Crisisnavigator. Org. Раздел: Слухи — buzz marketing. По материалам: http://iniciator.ru/index.php/buzz/razdel/C47/.
17. *Allport G., Postman, L.* The psyhology of rumor. New-York: Holt, 1947.

**Научное издание**

Расторгуев С.П., Литвиненко М.В.

# Информационные операции в сети Интернет

*Под общей редакцией доктора военных наук,*
*профессора генерал-лейтенанта*
*Михайловского А.Б.*

Сдано в набор 08.01.2014. Подписано в печать 16.01.2014. Формат 60x88/16.
Бумага офсетная. Гарнитура «Таймс». Печать офсетная. Усл.-печ. л. 8,0.
Уч.-изд. л. 5,34. Тираж 500 зкз. Заказ №17.

**Центр стратегических оценок и прогнозов**
**http://csef.ru/** 129515, г. Москва, ул. Академика Королева, д. 13, стр. 1

Типография ООО «Телер». 125299, г. Москва, ул. Космонавта Волкова, д. 12.
Лицензия на типографскую деятельность ПД №00595