

**Евгений Ющук, Александр
Кузин**

**Противодействие черному
PR в Интернете**

Предисловие

Мировая история Public Relations (пабблик рилейшнз, дословно – «публичные отношения») насчитывает уже два века. Принято считать, что своим рождением этот термин обязан американскому президенту Томасу Джефферсону, который употребил его в Седьмом обращении к Конгрессу в 1807 году. В 30-е годы XIX века в США оформилось понятие «relations for the general good» – «отношения ради всеобщего блага».

До начала XX века все PR-усилия в основном были сосредоточены в сфере пропаганды и носили односторонний характер. Как и любая другая форма тотального убеждения, они не учитывали мнения объекта воздействия и не корректировались в соответствии с этим мнением. Однако с началом XX столетия все начало кардинально меняться. Рост бизнеса, накопление огромных капиталов, сосредоточение финансовой мощи в руках узкого круга представителей общества начали вызывать раздражение и негативные реакции остального населения. По мнению обывателей, дельцы были готовы на все ради своей прибыли. Сращивание ка-

питала с властью, лоббирование своих интересов в политических элитах также не добавляло популярности ни политикам, ни предпринимателям. Появилась острая потребность установления двусторонних связей между «большим бизнесом», властью и обществом, которые смогли бы преодолеть враждебное отношение масс, устранить недопонимание, донести до населения декларируемые цели, наладить доброжелательное отношение потребителей и избирателей с предпринимателями и политиками.

В 1906 году американский журналист Айви Ли опубликовал «Декларацию о принципах PR», в которой назвал основной задачей специалистов этой сферы «побуждение людей верить в то, что правления корпораций преследуют искреннюю цель заручиться их доверием». Так, по сути, возникло то направление деятельности, которое мы и знаем как паблик рилейшнз.

Но задолго до этого события появилось то, что в начале 90-х годов прошлого столетия в нашей стране, с легкой руки некоторых журналистов, стали называть черным PR,[1] или попросту – чернухой.

Распространение порочащих сведений, клевета, диффамация, подтасовка фактов,

шельмование,[2] вытаскивание на всеобщее обозрение грязного белья – все это часть истории человечества с незапамятных времен. Примеры использования чернухи можно без особых усилий отыскать еще в классических произведениях эпохи Возрождения:

«Действуй, мое лекарство, действуй! Вот как ловят доверчивых безумцев!

Вот как честных, невиннейших и непорочных женщин позору подвергают!»

У. Шекспир. Отелло

Чем не черный PR, с помощью которого негодяй Яго опорочил невинную Дездемону в глазах Отелло?

В современной России черный PR расцвел невиданным цветом, попав на благодатную почву постперестроечной растерянности общества, смуты ельцинских реформ и периода дикой приватизации, когда за свое место под солнцем бились, не считаясь ни с чем. Хороши были любые средства и методы, главное – чтобы они привели к желанной цели: власти или деньгам. Лучше всего – и к тому, и к другому одновременно. Конкурентов и соперников топили всеми доступными способами. Благо народ наш был не искушен и не имел прививки от грязи, которая выплескивалась со страниц газет и экранов те-

левизоров.

Конечно то, что вливали в мозги нашим соотечественникам, никакого отношения к PR не имело. При чем тут технологии по связям с общественностью (а именно такой перевод Public Relations прижился в нашей стране) и коряво наклеенной на столбе листовкой, где утверждалось, что гражданин Пупкин – педофил, спонсор чеченских террористов и сатанист? Сейчас на такую туфту уже никто и внимания не обратит, но в начале 90-х у доверчивых россиян от подобной «правды» перехватывало дыхание и поднимало дыбом волосы. Крупные политики, не стесняясь, грозили «чемоданами компромата», а нашему гражданину столько и не требовалось – достаточно было упоминания в прессе о любовнице известного человека, чтобы народ пришел в искреннее негодование.

С тех пор много воды утекло. Сейчас сами политики с удовольствием демонстрируют себя любимых со всех мыслимых и немыслимых сторон: публикуют свои откровенные фотосессии в «журналах для взрослых», бравируют количеством жен и подружек. Не отстают от них и представители бизнеса, выставляя напоказ свою роскошь, делая из раз-

водов громкие информационные поводы или вывозя на зарубежные курорты топ-моделей.

На смену примитивной чернухе пришли утонченные методы негативного PR. Это уже в полном смысле технологии, причем настолько сложные, что овладеть ими дано далеко не каждому специалисту по связям с общественностью. Это одно из самых дорогих (если не самое дорогое) из направлений современного PR, с астрономическими подчас бюджетами и фантастическими гонорами специалистов. Есть мнение (с которым мы абсолютно согласны), что можно оправиться и восстановиться после мощного административного прессинга или полного разорения, но после хорошо спланированной и грамотно проведенной PR-войны – уже нет.

До недавнего времени PR-специалисты в основном использовали традиционные каналы распространения информации – печатные СМИ, телевидение, радио. При необходимости в ход шли листовки или direct-mail. По вкусу добавлялись «неформальные информационные каналы» – слухи, кулуарные внутриэлитные коммуникации, и т. д. и т. п. Интернет как площадка для серьезной PR-активности почти не рассматривался и в

основном служил неким вспомогательным средством.

Сегодня ситуация резко изменилась. Темпы роста российского сегмента Интернета настолько стремительны, что коммуникативная активность все больше и больше смещается в виртуальное пространство. Так, по данным исследований Фонда «Общественное мнение», на период зимы 2006–2007 Интернетом в России пользовались (с разной периодичностью) от 10 до 28 миллионов граждан страны в возрасте от 18 лет и старше. [3] В 2006 году Россия занимала 14-е место среди 15 стран-лидеров по числу интернет-пользователей. [4] Это колоссальная аудитория, которой может похвастаться далеко не каждое федеральное СМИ.

Однако стремительно возрастающая на сетевых просторах PR-активность несет с собой огромное количество проблем и головную боль как для специалистов по связям с общественностью, так и для многих фирм, компаний и отдельных граждан. Своей бесцензурностью и неподконтрольностью Интернет дал возможность чернушникам развернуться во всей своей красе и обрести вторую жизнь.

Конечно, набирающий мощь потенциал Интернета не отменяет тонких и изящных негативных PR-технологий. Но простота размещения в Сети любых, в том числе и порочащих, материалов, а главное – их круглосуточная доступность для пользователей в любой точке земного шара основательно снизили планку, отделяющую технологии от грязи. Сейчас для того, чтобы регулярно выливать ушаты помоев на человека или организацию, уже не нужно иметь большие бюджеты и нанимать специалистов высокого уровня. Склепать «на коленке» сайт с компроматом или разместить откровенно клеветническую информацию в блоге или на форуме может кто угодно – достаточно обладать самыми скромными познаниями и навыками пользования Интернетом. А что в таком случае способна сделать с «жертвой» команда профессионалов, располагающая необходимыми средствами?

Для противостояния чернухе в Интернете необходимо обладать не только знаниями и наработками борьбы с этим явлением в «реале» (так обычно называют реальную жизнь заядлые интернетчики) – понадобится владение особыми он-лайнowymi техниками и методиками. Многие из того, что PR- или ан-

тикризисный специалист мог бы применить в традиционном коммуникативном пространстве, для сетевых информационных войн малоприменимо или не применимо вообще. К примеру, вы можете узнать от «своих людей», что к публикации в газете готовится заказная статья, направленная против вас или вашего бизнеса. Проявив сноровку и подключив необходимые связи, вы вполне можете заблокировать ее выход (вплоть до ареста и уничтожения тиража) или успеть опубликовать материал, сводящий к минимуму возможный ущерб от компромата. А если приложить определенные усилия, то несложно выяснить, кто стоит за этой атакой. Вы можете подать в суд на издание, заставить его опубликовать опровержение, взыскать немалую компенсацию за моральный ущерб и сделать из этого события хороший информационный повод. В конце концов можно вообще заблокировать доступ к медианосителям для своих недругов. В Интернет все это не пройдет. О подготовке атаки вы, скорее всего, узнаете, когда она уже начнется. Да и то не факт, что вам станет известно, что на вас наехали, сразу, как только это случится. Скорее всего, вы еще долго будете пребывать в блаженном неведении и

о своих проблемах узнаете последним, со всем как тот обманутый муж. Блокировать и уничтожить информацию вам тоже не удастся – это почти 100 %. Также не получится узнать, кто за всем этим стоит. Ну разве что сами нападающие любезно раскроют свою анонимность. Судиться вам тоже будет не с кем. Даже если вы будете почти наверняка знать авторов и инициаторов нападения, то доказать ничего не сможете. А подать в суд на интернет-ресурс, где про вас говорят всякие гадости, – это из области фантастики: глобальность сети Интернет позволяет разместить материалы где угодно – хоть на сервере в Папуа Новой Гвинее. А затем чернуха вполне может перекочевать из виртуального пространства на страницы бумажных газет и, увы, здесь вы тоже ничего не сможете сделать – по закону СМИ могут публиковать информацию из Интернета, не опасаясь никакой ответственности.

Картина вырисовывается удручающая. Но не все так безнадежно. Рано или поздно на любой яд находится противоядие, для борьбы с болезнями появляются эффективные и доступные лекарства.

О некоторых эффективных и вполне доступных каждому лекарствах против черно-

го PR в Интернете вы сможете узнать уже сейчас.

Введение

Мы согласны с популярной у ряда специалистов по информационным технологиям точкой зрения, что так называемый черный PR – это распространение не любой негативной информации, а лишь той, что основана на лжи. Иными словами, это целенаправленное распространение заведомо ложных, недостоверных сведений. Цель этой книги – научить противодействовать черному PR в Интернете. Для достижения этой цели сначала следует понять, какие особенности заставляют рассматривать Интернет отдельно от других, более традиционных способов распространения информации (любой, а не только негативной). А для этого в первую очередь надо проследить, каким образом общество пришло к сегодняшнему уровню развития Интернета как среды распространения информации.

Интернет сегодня стал неотъемлемой частью жизни многих людей. Когда количество пользователей в середине 1990-х годов стало увеличиваться, компании, предлагающие товары и услуги, также незамедлительно пришли в Сеть. Вначале заметнее всех

оказались фирмы, имеющие достаточно средств для создания и продвижения своего сайта, либо специалисты, не располагающие деньгами, но умеющие создавать сайты самостоятельно. Обычному человеку, не имеющему специальной подготовки, оставалось довольствоваться сервисами, которые не требовали ни особых навыков, ни финансовых вложений – электронной почтой или ICQ и его аналогами. Однако главную роль в дальнейшем развитии событий сыграл тот факт, что Интернет появился в западных странах, где отдельный человек с его мнениями, знаниями и эмоциями часто ставится во главу угла. В результате началась работа по максимальной интеграции обычного человека в Глобальную сеть. Для этого требовалось решить две принципиальные проблемы: удешевить пользование Интернетом и упростить его. Массовое приобщение рядовых пользователей к Сети шло в двух основных направлениях.

Во-первых, появились бесплатные «конструкторы сайтов», позволявшие каждому создать личный сайт, и бесплатные ресурсы, предоставляющие хостинг (место на сервере, подключенном к Интернету) для таких личных сайтов.

Во-вторых, стали появляться бесплатные сервисы, которые позволяли людям переносить в Интернет свою переписку, фотографии, общение и даже создание электронных документов.

Как правило, эти возможности предоставлялись на крупных интернет-порталах с большой посещаемостью – таких как поисковые машины, порталы крупных городов или отраслевые.

Следующим шагом стало появление возможности комментировать сообщения друг друга, т. е. обмениваться мнениями. Как следствие появились инструменты, позволяющие этот обмен мнениями увидеть. Фактически родилась система, позволяющая незнакомым людям, которых порой разделяли тысячи километров, координировать свои действия в реальном масштабе времени или с незначительной временной задержкой. Отличным примером подобных скоординированных действий может служить статья, опубликованная 20 июля 2007 года на сайте «Регионального информационного агентства Дейта ru».

Последнюю книгу про Гарри Поттера уже перевели на русский язык

17 июля в Интернете появились фотокопии всех страниц книги «Harry Potter and Deathly Hallows» (неофициальный русский перевод – «Гарри Поттер и роковые мощи»), которая выходит на английском только 21 июля.

Как выяснилось, Levy Home Entertainment. LHE и интернет-магазин DeepDiscount.com нарушили запрет на продажу книги до полуночи 21 июля 2007 года и отправили несколько экземпляров покупателям по почте. Несмотря на то что было отправлено всего примерно 1200 экземпляров (при тираже 12 миллионов) событие вызвало большой ажиотаж: кто-то из первых читателей книги решил поделиться своим счастьем с другими поклонниками Поттера и выложил в сети сфотографированные страницы романа. Согласно данным компании BigChampagne Media Measurement, к среде 18 июля эти файлы загружали по всему миру каждую секунду сообщает «Комсомольская правда».

Издательство намерено судиться с виновником утечки Levy Home Entertainment. Также оно обратилось ко всем получившим доступ к тексту с просьбой не раскрывать сюжет романа до его официального поступления в продажу.

Многие российские «поттероманы» скачали фотокопии и тут же перевели роман на русский, поделив между собой главы. Пиратские переводы выкладываются сразу на нескольких сайтах в Интернете.[5]

В результате всех вышеописанных изменений резко снизилась стоимость размещения информации в Интернете и одновременно оказался затруднен поиск человека, непосредственно ответственного за размещение того или иного сообщения.

Компании не замедлили присоединиться и к новшествам. Это видно даже из того, насколько чаще стало упоминаться в блогах и форумах словосочетание «корпоративный блог». Увидеть такую статистику можно на ресурсе Яндекса «Пульс блогосферы»[6] (рис. 1).

С приходом предприятий и политиков в Интернет туда оказались перенесены и все их проблемы, существующие в реальной жизни. Было бы удивительно, упусти компании и политики шанс использовать возможности новой «среды обитания» для улучшения собственного имиджа. И разумеется, для ухудшения имиджа своих оппонентов. Так, в полном соответствии с философским законом единства и борьбы противоположно-

стей, Интернет принес людям и предприятиям как преимущества, так и угрозы. Это нормальное явление, или, по крайней мере, естественное.

Пульс блогосферы — корпоративный блог

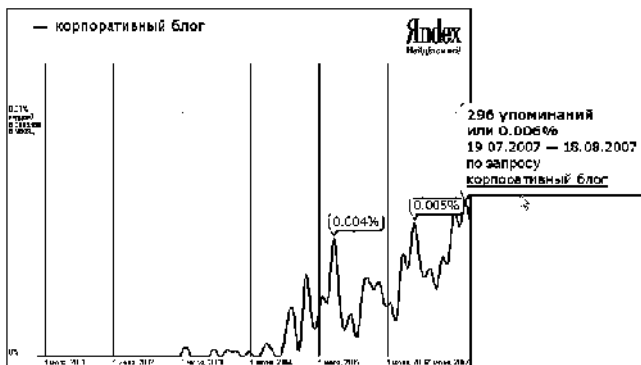


Рис. 1. Упоминаемость словосочетания «корпоративный блог» в «Блогах Яндекса».

Тому, как реагировать на угрозы, исходящие из Интернета, и посвящена эта книга. Она написана на основе изучения и обобщения опыта многих реально существовавших PR-войн. Выводы и рекомендации, приведенные здесь, проверены на практике.

Особенности распространения информации в Интернете

Информация в Интернете распространяется очень быстро

Любой компьютер, подключенный к Сети, в принципе может получить доступ на сайт, расположенный физически сколь угодно далеко. С точки зрения скорости работы, нет никакой разницы, расположен сайт на соседнем столе или на соседнем континенте.

Если информация попала в Интернет и показалась интересной кому-то из пользователей, она может быть моментально распространена любым заинтересованным лицом на теоретически неограниченное количество интернет-площадок разного рода (таких как сайты, блоги, форумы и ряд других, которые мы подробно рассмотрим ниже). На сайтах и форумах этому способствуют механизмы отслеживания изменений с помощью RSS-потокa, а в блогах – система френдов,

подписанных на новые сообщения. Как только информация появится в блоге, она становится автоматически доступна всем, кто подписан на чтение размещаемых в нем сообщений. Каждый из блоггеров обычно имеет своих подписчиков, количество которых колеблется от нескольких человек до нескольких сотен. Благодаря такой структуре новости, которые интересны большому количеству людей, могут распространяться практически мгновенно. Если это происходит, то такие сообщения попадают в поле зрения специальных сайтов, контролирующих самые популярные новости (они отслеживают ту информацию, на которую обратили внимание пользователи, количество которых превышает некую пороговую величину). Оттуда сообщение автоматически включается в специализированные рассылки и попадает в почтовые ящики, владельцы которых могут и не увлекаться интернет-серфингом, но подписаны на новостные рассылки. Электронные рассылки формируют вторую, не менее масштабную, волну в распространении информации. Новостные интернет-агентства способны дополнительно подключиться к распространению информации на любом этапе, если сочтут ее интересным для

себя информационным поводом.

Распространять информацию в Интернете анонимно технически возможно

Нравится нам это или нет, но анонимное распространение информации в Интернете действительно возможно. Одни считают это злом, другие – благом. Недовольны, как правило, жертвы такого распространения, а положительно оценивают сохранение анонимности в Интернете те, кто желает довести до сведения общественности свое неприязненное отношение к человеку или предприятию.

При выходе терминала (компьютера или мобильного телефона) в Интернет он всегда получает так называемый IP-адрес. По определению Википедии – сетевой энциклопедии, которая составляется всем интернет-сообществом, – «IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) — уникальный идентификатор (адрес) устройства (обычно компьютера), подключенного к локальной сети или Интернету».[7] Этот адрес действительно уникален. В Интернете

двух компьютеров с одинаковыми IP-адресами нет. Именно по IP-адресам компьютеры передают друг другу информацию, поэтому если два компьютера будут иметь один и тот же IP-адрес, то станет непонятно, кому из них она предназначена. Распределение IP-адресов осуществляется уполномоченными организациями. Пул адресов в определенном диапазоне закрепляется за конкретным интернет-провайдером, поэтому провайдера и город, из которого вышел в Интернет компьютер, определить по IP-адресу можно всегда. IP-адрес бывает постоянным или динамическим. Постоянный закреплен за конкретным пользователем, динамический – один из свободных в данный момент – выдает провайдер своим клиентам в ответ на конкретный запрос на выход в Интернет. В случае использования постоянного IP-адреса информация о том, за кем он закреплен, часто может быть доступна кому угодно. Если используется динамический IP-адрес, эти сведения будут известны только провайдеру, и то не всегда: хотя провайдер знает, с какого терминала был осуществлен выход, это не гарантирует идентификации пользователя. Так, при выходе в Интернет с городского телефона известен его абонентский

номер и адрес, по которому он установлен. При выходе с мобильного телефона – абонентский номер и персональный номер телефонного аппарата (так называемый IMEI), а при выходе в Интернет с выделенной линии провайдер знает, по какому адресу располагается терминал, подключенный через эту линию. Однако если выход в Сеть осуществлялся из интернет-кафе либо через публичную точку доступа Wi-Fi (в кафе, на вокзале или вообще из автомобиля, припаркованного около них), либо с мобильного телефона, зарегистрированного на подставное лицо, поиск конкретного человека становится очень затруднительным или вообще невозможным.

Интернет-провайдер легально может сообщить информацию об абоненте только правоохранительным органам по их запросу. В противном случае он нарушает как Федеральный закон «О персональных данных», так и целый ряд ведомственных нормативных актов.

Проблема поиска человека, вышедшего в Интернет, усугубляется тем, что IP-адреса не всегда транслируются напрямую. Например, при использовании GPRS с мобильного телефона, как правило, все, кто пользуется

этой услугой в сотовой компании, имеют один IP-адрес. Точно так же имеют один IP-адрес все, кто выходит в Интернет через так называемый прокси-сервер (это часто встречается в интернет-кафе, учебных заведениях и крупных офисных зданиях).

Кроме того, существуют программы, специально предназначенные для прикрытия IP-адресов – анонимайзеры. По своей сути это прокси-серверы, созданные специально для предоставления анонимности в Интернете. Некоторые из них (например, Steganos Internet Anonym VPN)[8] обеспечивают даже шифрование передаваемой информации, что не позволяет перехватить ее на каналах связи. При попытке идентифицировать человека, который разместил в Интернете текст или другую информацию с использованием анонимайзера, необходимо проделать целый ряд действий. Сначала обратиться в правоохранительные органы. Те должны возбудить уголовное дело (если есть признаки преступления) и убедить Генеральную прокуратуру написать мотивированный запрос в правоохранительные органы иностранного государства, которому принадлежит IP-адрес анонимайзера. Этот запрос должен быть оформлен с соблюдением всех не-

обходимых формальностей, иначе он вообще не будет принят к рассмотрению за рубежом. Из запроса должно явно следовать, что он не является политически окрашенным, иначе по сложившейся практике многие страны также не примут его к рассмотрению, независимо от правильности оформления. После этого правоохранительные органы иностранного государства обратятся к фирме, предоставляющей услуги анонимайзера, и потребуют дать информацию о том, с какого IP-адреса к нему подключились. В ходе всего этого комплекса мероприятий, на проведение которых потребуется немало времени, выяснится лишь адрес, с которого недруги подключились к анонимайзеру. А ведь анонимайзеры могут быть и выстроены в цепочку, когда подключение к одному из них производится через другой...

Вдобавок к уже сказанному надо отметить, что существует распределенная анонимная сеть Tor,[9] которая создана и поддерживается сторонниками приватности. Эта компьютерная сеть в Интернете организована так, что практически невозможно отследить перемещение пакета данных от начальной точки к конечной.

Вот почему для большинства случаев, если они не касаются международного терроризма, когда все силы спецслужб крупных стран будут скоординировано брошены на поимку злодея, можно говорить о том, что обеспечить анонимность в Интернете технически возможно.

Хотя мы здесь дали обзор основных методов обеспечения анонимности в Интернете, для удобства читателей более подробно мы расскажем о них в отдельном разделе.

Оф-лайновые механизмы противодействия распространению информации не срабатывают он-лайн

Создание блога занимает 15 минут. Создание работоспособного сайта, не претендующего на номинацию в конкурсе веб-дизайна, – от 40. Перенос сайта на новый хостинг – от нескольких секунд до нескольких минут.

Оф-лайн за это время невозможно даже написать исковое заявление. Более того, открыть хостинг (т. е. купить место на сервере, где будет размещен сайт) на момент написа-

ния книги можно было вообще анонимно, используя в качестве оплаты переводы через платежные системы, не предусматривающие идентификации. А если хостинг при этом заказан в другой стране, то оф-лайновые процедуры воздействия на него становятся не менее трудоемкими, чем те, что описаны нами в предыдущем разделе, посвященном установлению реального IP-адреса недруга. Это очень длительные и подчас дорогостоящие процедуры, результатом которых может стать судебное решение о закрытии хостинга, после чего, как мы уже говорили, ничто не мешает вновь открыть его в другой стране, и в течение нескольких минут сайт, с которым шла борьба, снова окажется в эфире. Кроме того, совершенно не факт, что судебное дело против сайта с черным PR будет выиграно. Ведь если негативная информация представляет собой не клевету или оскорбления, а личное мнение, и если при этом не нарушаются никакие законы (например, о недопустимости публикации персональных данных без прямого согласия того, кому они принадлежат), то суд может вообще не принять решения о ее удалении.

Интернет – «стиральная машина» для негативной информации

Если средство массовой информации размещает недостоверные сведения, порочащие кого-либо, пострадавший может обратиться в суд, и у него есть шанс получить компенсацию, а также заставить СМИ опубликовать опровержение. И хотя существующая сегодня даже в уважаемых изданиях система не во всем совершенна (например, на практике журналист, считающий себя «акулой пера», может разместить непроверенную информацию – и никто не станет его действия контролировать), все же можно попытаться призвать к ответу СМИ. Это трудно, долго, но возможно. А вот когда информацией такого рода наводняется Интернет, после чего об этом факте начинают писать СМИ («в Интернете появилась информация о том, что...»), к ответственности привлекать обычно некого.

Эту особенность Интернета почти десять лет назад одним из первых отметил Глеб Павловский: «Интернет – идеальный инструмент для запуска в массовое сознание необ-

ходимых сюжетов. Кроме того, традиционные средства массовой информации несут ответственность за распространяемые ими сведения. Слухи же, передающиеся через Интернет, анонимны. Зато газеты и телевидение получают возможность ссылаться на Интернет. То есть происходит самое настоящее отмывание так называемой черной информации».[10]

До недавнего времени даже он-лайнные СМИ не удавалось привлечь к ответственности. При обращении в суд требовалось направить на их адрес копию искового заявления, а к моменту судебного слушания информация с сайта исчезала. Правда, в последнее время появилась возможность нотариально заверить копию изображения информации, размещенной на сайте. В результате даже если тот или иной текст к моменту суда с сайта удаляется, это не спасает электронное СМИ от ответственности. Наверное, это победа. Однако она столь мала, что не решает проблемы в целом.

Информация в Интернете может храниться вечно и часть архивов общедоступна

Когда пользователь размещает информацию в Интернете, он зачастую утрачивает контроль над ней, даже не осознавая этого. Фразы «Слово не воробей, вылетит – не поймаешь» и «Что написано пером, не вырубишь топором» здесь причудливо объединились и обрели сегодня новый смысл. Действительно, написав что-либо на чужом интернет-форуме или прокомментировав чей-то сетевой журнал, пользователь может полностью утратить власть над своими словами. Даже если кто-то считает, что при необходимости сможет убрать информацию, размещенную им, не факт, что это на самом деле возможно. Любому человеку достаточно просто скопировать слова, приведенные в сообщении, чтобы власть автора над этим сообщением оказалась утрачена. Возможно, навсегда.

Но даже если информация размещается на собственном сайте пользователя, он может рано или поздно обнаружить, что не в состоянии убрать ее из Интернета. Это чаще всего происходит по четырем причинам.

1. Информация попадает в архив Интернета. Действительно, в Интернете по адресу: www.archive.org/ существует ресурс, который копирует страницы сайтов и сохраняет

их на своих серверах. Поскольку он находится в Сан-Франциско и принадлежит (во всяком случае, официально) частному лицу, вряд ли существует возможность легко «зачистить» информацию там по желанию организаций или частных лиц без решения американского суда. Вот фрагмент статьи «Архив Интернета» из Википедии:

Архив Интернета расположен в Сан-Франциско, основан в 1996 году и занимается несколькими проектами. Архив обеспечивает бесплатный доступ для исследователей, историков и школьников. Декларируемой целью архива является сохранение культурно-исторических ценностей цивилизации в эпоху интернет-технологий и создание интернет-библиотеки.

The Wayback Machine – в базе сохраняется содержимое веб-страниц, и можно посмотреть, как выглядела та или иная страница раньше, даже если сайт больше не существует. В октябре 2004-го впервые было зафиксировано использование The Wayback Machine в качестве доказательства в американском суде. Также замечена цензура, когда часть архивных копий веб-страниц, содержащих критику сайентологии, была удалена из архива по требованию юристов из церкви сай-

ентологов.[11]

Для того чтобы увидеть возможности архива Интернета, приведем хранящиеся там изображения сайтов РосБизнесКонсалтинга ([www. rbc.ru](http://www.rbc.ru)) от 10.12.1997 г. и Мост-банка (www.most.ru) от 16.01.1997 г. (рис. 2, 3).

Позже мы расскажем более подробно о том, как пользоваться этим сервисом.

2. Информация перепечатывается другим пользователем.

Любой человек, компания или новостное агентство может перепечатать у себя слова пользователя со ссылкой на источник и прокомментировать их.

Слова пользователя интернет-форума могут быть процитированы другим участником того же форума и за счет этого выйдут из-под контроля автора. Автор может попросить их убрать того, кто цитировал, либо модератора форума, однако не в его силах заставить кого-либо выполнить эту просьбу.

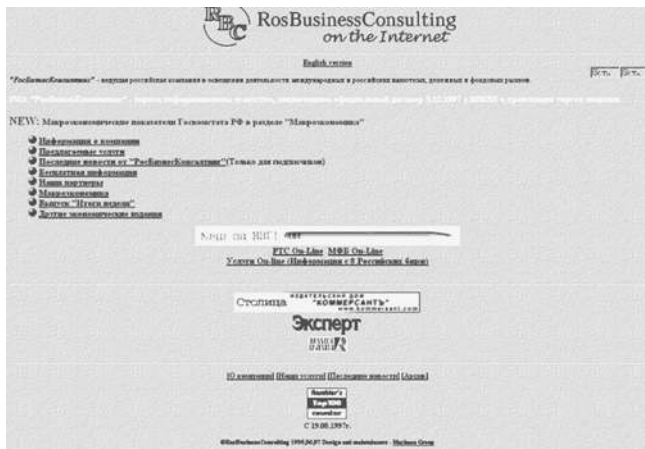


Рис. 2. Сайт РосБизнесКонсалтинг от 10.12.97 г. в архиве Интернета.



Рис. 3. Сайт Мост-банка от 16.01.1997 г. в архиве Интернета

3. Сообщение пользователя попадает в так называемые топы различных ресурсов и остается там. Это явление характерно главным образом для блогов. Как только какая-либо тема начинает обсуждаться достаточно активно, она фиксируется специальными сайтами и ее копия размещается там в разделах вроде TOP-30 Живого Журнала за такое-то число. Нередко с этих сайтов новость попадает в тематические рассылки и распространяется всем подписчикам в разных городах и даже странах.

Многие ресурсы в Интернете стали интерактивными. Действительно, еще десять лет назад рядовой человек или небогатое предприятие не могли получить возможность высказать свою точку зрения на те или иные события или проблемы. Сегодня в Интернете появляются примеры, показывающие, что любой человек может сделать это так «громко», что будет услышан во всем мире и при необходимости получит помощь. Люди, еще вчера не знакомые друг с другом, в одно мгновение объединяются общей идеей или отношением к какой-то проблеме и начина-

ют выступать сообща.

Если тема интересна, пользователи могут самостоятельно присоединиться к ее обсуждению или даже принять участие в ее решении оф-лайн. Потенциал влияния интерактивного Интернета на реальную жизнь отчетливо просматривается на примере таких безобидных ресурсов, как сообщество «Даром» в Живом Журнале (ЖЖ, или Livejournal), www.community.livejournal.com/darom/ и сообщество Живого Журнала «Флэшмоб» (www.community.livejournal.com/fmob/).

Вот описание сообщества «Даром», приведенное в его Журнале:

Если у вас в доме обнаружилась хорошая, но ненужная вещь такая, что выкинуть жалко, а девать некуда, а также если возникла необходимость в чем-нибудь, вы можете оставить сообщение в этом комьюнити. Наверняка найдется человек, который будет готов отдать вам необходимую вещь.

Здесь можно оставлять объявления: «отдам даром», «приму в дар», «поменяюсь» или «услуга за услугу». Никаких строгих ограничений нет, кроме объявлений «куплю/продам».

Обязательно укажите город, в котором вы находитесь, или возможность отправки по почте. Если вы не укажете город, то это будет равносильно подписи «г. Москва».

Если вещь уже нашла своего нового владельца или отпала необходимость в вещи, то не забудьте это указать в вашем объявлении.

Внимание!

1. Объявления о раздаче котят и щенков категорически запрещены. Для этого существует более 90-та сообществ, где люди интересуются котятами, более 400 – кошками, более 40 – щенками и почти 300 – собаками. К остальным животным этот запрет не относится.

2. Запрещено постить сообщения типа «подскажите, пожалуйста», «скажите даром», соцпросы и прочее. Для этого существует специальное сообщество `podskajite_plz`, не сомневаюсь что желающих дать хороший совет всегда найдется больше, чем его спрашивающих.[12]

Описание из Журнала сообщества «Флэшмоб»:

Коротко о Флэшмобе

Флэшмоб – это механизм... механизм, позволяющий за счет десятков, сотен незнако-

мых между собой людей смоделировать такую ситуацию, которая в реальности просто не может произойти. Это возможность не просто создать необычную ситуацию, это возможность ИЗМЕНИТЬ РЕАЛЬНОСТЬ! Договорившись на этом сайте, мы внезапно появляемся в местах скопления народа и выполняем наши сценарии. Удивляем, озадачиваем, пугаем восхищаем и исчезаем – до новых встреч

Правила Флэшмоба

1. Не говори о флэшмобе ни перед, ни во время, ни после акции.

2. Внимательно изучи сценарий заранее, чтобы не растеряться и ничего не перепутать на месте.

3. НЕ СМЕЙСЯ ВО ВРЕМЯ FLASHМОВ АКЦИИ

4. Не приезжай с друзьями; не здоровайся, если встретишь кого-то знакомого.

5. Строго следуй инструкциям в сценарии. Никогда не старайся выделиться.

6. Настрой свои часы максимально точно. Окажись на месте за 10 секунд до начала flashmob акции.

7. Не оставайся на месте проведения акции после завершения флэшмоба.

8. На вопрос: «Что здесь происходит?» отвечай: «Я здесь случайно... увидел – и присоединился».

9. Фото– и видеосъемку нужно вести крайне скрыто, а лучше вообще от этого отказаться.[13]

На примере этих двух сообществ видно, что по любому вопросу интересному людям, может быть быстро создан коллектив единомышленников. Такой коллектив может действовать скоординировано, причем его участникам не мешает, что они могут быть незнакомы друг с другом. Если решение общей проблемы требует физического присутствия участников, географическая удаленность еще ограничивает возможности коллектива, но когда речь идет о распространении информации в Интернете, препятствий нет вообще. Социальная сеть, представленная участниками неформального коллектива, распространяет информацию быстро и широко. А вот противодействовать такому молниеносному распространению информации по всему миру крайне затруднительно, а чаще всего вообще невозможно.

4. Государственные границы сохраняются в реальной жизни, но практически стерты в виртуальной. Мы уже затрагивали этот

вопрос, говоря о том, какие усилия требуются, чтобы легальными способами получить информацию об IP-адресе пользователя в другой стране или воздействовать на компанию, предоставившую свой сервер для сайта противника. Кроме того, в ряде случаев с этой страной может не быть соглашения о взаимодействии правоохранительных органов, или по ее законам поступок вашего недруга не является чем-то предосудительным. Возможно, она находится на другом конце земного шара или в ней неспокойно, так что по соображениям финансовым или личной безопасности лететь в нее для установления контактов на месте вы сочтете нецелесообразным. Наконец, может быть и так, что у этой страны сложные политические отношения с Россией, и поэтому она с энтузиазмом будет ставить палки в колеса по любым вопросам, предполагающим помощь российским предприятиям, гражданам, правительству или правоохранительным органам.

Таким образом, попытка воспрепятствовать распространению информации в Интернете вполне реально может натолкнуться на серьезные барьеры в виде государственного суверенитета и различий в законах, тогда как тому, кто эту информацию

распространяет, подобные проблемы обычно не грозят.

Интернет значительно более демократичен, чем реальная жизнь

Это имеет как существенные плюсы, так и существенные минусы. Реальная жизнь заставляет человека в любой стране вести себя с оглядкой на возможные последствия его поведения. Даже в странах с развитыми демократическими институтами человек вынужден думать о том, как его поступки или высказывания будут восприняты окружающими.

В Интернете этих ограничителей часто нет вообще, либо они есть, но их значительно меньше, чем в «реале». В результате любой человек может высказать всему миру свою точку зрения (причем не важно, правильную или нет), и при определенных обстоятельствах у него не меньше шансов быть услышанным, чем у серьезного новостного агентства. Ведь недаром сегодня появились и активно работают новостные агентства в Интернете, в которых рейтинг новости опре-

деляется самими читателями, а не редактором. Это так называемые социальные новости[14] (социальные не по тематике, а по алгоритму определения рейтинга новостей всем сообществом). Примером таких ресурсов в Рунете могут служить news2.ru (www.news2.ru/) или smi2.ru (www.smi2.ru/), популярность которых, по данным исследователей, постоянно растет. Правда, подобные ресурсы, как любая открытая система, постоянно подвергаются опасности накрутки результатов в рекламных целях, поэтому некоторые из них вновь начинают жестко моделироваться при размещении новости, как, например, weblinks.ru (www.weblinks.ru/). На наш взгляд, тенденция развития сервисов социальных новостей налицо, а по мере приобретения такими сервисами известности среди широкой публики вероятность искажения результатов заинтересованными лицами значительно снизится. Это видно на примере зарубежных аналогов. Уже проверено на практике, что события, волнующие большое количество людей, широко комментируются рядовыми пользователями Интернета в реальном масштабе времени. При этом степень доверия сказанному невероятно высока. Примером может служить ситуа-

ция с ураганом «Катрина» в Новом Орлеане. Для иллюстрации приведем фрагмент статьи «Новоорлеанские блоггеры совершили журналистский подвиг», размещенной на известном российском ресурсе CNews.

Блоггеры на страницах своих интернет-дневников описывали тропический шторм «Катрина» из первых рук в режиме реального времени и не менее ярко, чем крупные СМИ.

Дизельный генератор, компьютер и сотовый телефон – все что блоггерам было нужно для выхода в Интернет до того, как вышли из строя сотовые сети. «Везде валяются деревья. У соседа три дерева упали на дом. Южный яхт-клуб выгорел до основания», – написал в блоге яхтсменов Gulfsails Трой Джилберт (Troy Gilbert).

Блоггеры все чаще становятся важнейшим источником информации о чрезвычайных ситуациях в мире. Расцвет блогосферы в США произошел во время президентских выборов прошлого года, когда ход процесса описывали авторы из разных уголков страны. Аудитория блоггерских сайтов во время важных событий растет – люди чаще ищут в Интернете информацию, выходящую за рамки новостных сайтов. Так, Media Metrix от

comScore зарегистрировал 29 августа 1,7 млн он-лайн-поисков по словам «ураган» и /или/ «Катрина» – в 10 раз больше, чем за пять дней 22–26 августа.

«Блоггеры за пределами области бедствия делают все возможное, чтобы расширить распространение информации из первых рук», – сказал профессор Нью-Йоркского университета Марк Криспин Миллер (Mark Crispin Miller). Ричард Люсик (Richard Lucic), профессор университета Duke, считает, что блоги подкасты и другие новые технологии преподносят новости «на человеческом уровне», поскольку каждый желающий может заниматься этим при очень небольших инвестициях и без подготовки.[15]

Мы нисколько не умаляем самоотверженность и стойкость блоггеров Нового Орлеана, но хотим отметить, что практически никогда не встречается даже попыток проверить правдивость фактов, изложенных в подобных случаях. Отчасти это связано с тем, что возможность проверки отсутствует в принципе, отчасти – с тем, что люди просто не задумываются о необходимости перепроверять информацию, если она кажется им волнующей и срочной. Но в любом случае для манипуляторов общественным мнением та-

кая ситуация открывает головокружительные перспективы.

Справедливости ради надо отметить, что первые разоблачения блоггеров, публикующих «правдивые» жареные факты, также уже зафиксированы. Хотя, конечно, неизвестно, сколько подобных фактов так и осталось нераскрытыми. Вот статья известного блоггера и журналиста Антона Носика,[16] пишущего в блогах под ником (псевдонимом).

Тем, кто нечасто заглядывает в блоги и на интернет-форумы, напомним, что ник – это виртуальное имя. Оно может быть в принципе любым, но в пределах одной площадки блогов должно быть уникальным, т. е. если кто-то раньше вас выбрал ник, который вам нравится, то вам придется придумать себе другой. Ник, выбранный вами, соответственно, не может быть выбран больше никем на этой площадке блогов. Поясним также некоторые термины, встречающиеся в приведенной ниже статье. «Фотожаба» – известная программа «Фотошоп» (Photoshop), позволяющая монтировать изображения и вносить в них любые изменения. «Лжеюзер» – пользователь Живого Журнала, который по-английски называется LiveJournal, а в русской

транскрипции – ЛивЖурнал, или ЛЖ.

Фотожаба переехала в Газу

Сотрудник Reuters в Газе Фадель Шада и его коллега, работающий на иранское ТВ, объявили себя жертвами израильского ракетного обстрела.

Ассоциация иностранных журналистов в Израиле поспешила назвать обстрел «outrageous targeting» и потребовала тщательного расследования.

Видимо, зря. Потому что анализ приведенных «потерпевшими» свидетельств показал, что речь идет об инсценировке.

Вот как излагает эту историю лжеюзера akog.

А вот те английские блоги, которые он использовал при подготовке материала: MyPetJawa, PowerlineBlog (update), Snapped Shot, Confederate Yankee.

Отдельно интересный сюжет к вопросу о постановочных съемках разрушений – инсценировка израильского удара по ливанским каретам скорой помощи.[17]

Краткая характеристика широко известных инструментов распространения негативной информации в контексте информационной войны

Корпоративные сайты. Это сайты, принадлежащие конкретным организациям. Как правило их задача – привлечение внимания к компании-владельцу, а также помощь клиентам.

В ряде случаев они могут технически обеспечивать ведение бизнеса компании – например, когда на сайте работает интернет-магазин или когда речь идет о сайте новостного агентства, где новости – главный продукт этого агентства – непосредственно размещаются. Поскольку корпоративный сайт имеет явно обозначенного владельца, размещенная на нем информация, с одной стороны, воспринимается как более достоверная

(если владелец сайта достаточно авторитетен), но, с другой, в случае размещения недостоверной информации владелец сайта оказывается под ударом.

В нашей практике был случай, когда контролирующим органом была наказана компания, размещавшая клеветническую и недостоверную информацию о некоторых своих клиентах. Эта информация размещалась на сайте на основании голословных утверждений сотрудников компании. В рамках работы конкурентной разведки по противодействию распространению клеветнической информации в Интернете мы инициировали проверку деятельности предприятия, которая завершилась вынесением наказания. Для этого оказалось достаточно внимательно изучить размещенные на сайте материалы, а затем написать мотивированное заявление в соответствующие инстанции.

Уязвимость сайта, которой мы воспользовались, – обычное явление, характерное для многих корпоративных сайтов. Дело в том, что, как правило, они очень велики – могут насчитывать несколько тысяч (а то и десятков тысяч) страниц. В то же время сотрудники, непосредственно отвечающие за размещение и обновление на сайте информации,

достаточно часто меняются. В результате устаревшая или изначально недостоверная информация, однажды случайно или умышленно размещенная, остается висеть на нем, даже если в силу изменившихся внешних обстоятельств сам факт ее размещения способен скомпрометировать и подставить под удар организацию. О таких материалах чаще всего просто забывают или до них «не доходят руки» у нового веб-администратора. Если никто не ставит задачу атаковать организацию, такая информация может годами оставаться незамеченной. Но достаточно кому-либо для подготовки нападения на компанию тщательно изучить сайт – и материал для нанесения удара по предприятию легко выявляется.

Преимущества корпоративных сайтов для защиты от информационного нападения обусловлены тем, что владелец ресурса известен. Если он достаточно авторитетен, то его точка зрения способна влиять на формирование общественного мнения сильнее, чем точка зрения малоизвестного частного лица. Кроме того, корпоративный сайт обычно «авторитетен» и у поисковых машин, поэтому ссылки с него могут поднять блоги или социальные ресурсы в результатах выдачи

и сделать приведенную в них точку зрения более известной.

Чтобы эффективно использовать корпоративный сайт в продвижении точки зрения на проблему, при этом сведя к минимуму риски преследования его владельца, обычно достаточно процитировать на нем материалы с других источников, указав их.

Личные сайты, расположенные на бесплатном хостинге.

В Интернете достаточно много площадок, предоставляющих возможность бесплатно разместить сайт. Одна из самых известных – Narod.ru (www.narod.yandex.ru/), именуемый обычно просто Народом. Чтобы открыть там сайт, не требуется специальных знаний и навыков, поскольку существуют готовые и понятные шаблоны. Вместе с тем продвинутый пользователь может разместить на Народе и достаточно большой сайт собственного изготовления, поскольку сервис предоставляет такую возможность. Главное преимущество сайтов на бесплатном хостинге, помимо необходимости платить, – как раз возможность выбирать для них тот дизайн и структуру сайта, которые нравятся владельцу. Главный недостаток – низкий рейтинг в поисковых машинах и, соответствен-

но, довольно низкое положение в выдаче по запросам в эти машины. К существенным недостаткам сайтов на бесплатном хостинге мы также относим и невозможность обсуждения расположенных на них материалов. Интерактивность, которая возможна на таких сайтах, – общение через гостевую книгу (гестбук).[18] Но гостевая книга не способна организовать обмен мнениями большого числа участников беседы в короткий промежуток времени, максимум ее возможностей в организации общения – размещение статического отзыва о материалах сайта либо вопроса к его владельцу, если других каналов связи не предусмотрено. А с изобретением спамерских роботов, прицельно атакующих гостевые книги, у многих владельцев сайтов появились дополнительные проблемы: они вынуждены теперь отвлекаться на удаление спама.[19]

Личные сайты, расположенные на платном хостинге. По своей сути эти сайты ничем не отличаются от корпоративных, о которых мы уже говорили выше. Их авторитетность напрямую зависит от авторитетности их номинального владельца. Защищенность личных сайтов несколько выше, чем корпоративных. Они защищены от предъявления

претензий их владельцам, потому что если в организации за все отвечает директор, то в случае с личным сайтом по сложившейся практике ответственность должен нести тот, кто непосредственно разместил информацию. А найти такого человека бывает достаточно тяжело, особенно когда дело доходит до возможных неприятностей.

Блоги. Это мощный инструмент информационной войны в Интернете. Даже в тех примерах, которые мы уже рассматривали выше, блоги фигурируют часто. По ряду параметров в информационной войне они имеют преимущества перед сайтами. Роль блогов в распространении информации в Интернете, а значит, и в отражении информационного нападения, настолько велика, что мы уделим им ниже самое пристальное внимание и рассмотрим их в подробностях. Поэтому сейчас мы на них останавливаться не станем.

Форумы. Интернет-форумы в современной информационной войне в Сети также играют важную роль, но в большинстве случаев она менее значительна, чем роль блогов. Исключение составляет ситуация, когда тема информационной войны касается какого-то профессионального сообщества или

интересов населения определенного города. В таких случаях роль профессиональных или региональных интернет-форумов значительно возрастает: ведь там как раз и сосредоточена целевая аудитория, интересующаяся данной проблематикой. Форумы имеют ряд общих с блогами черт, но тем не менее отличаются от них. Об этом мы ниже также поговорим подробнее.

Помимо таких широко известных сегодня ресурсов, как личные и корпоративные сайты, блоги и интернет-форумы, существуют и другие ресурсы, которые могут быть эффективно использованы в информационной войне для решения вспомогательных задач, и мы непременно уделим им внимание в этой книге.

Как изложить интернет-аудитории свою точку зрения: стратегия, тактика, инструменты

Сходства и отличия «боевого» и «мирного» продвижения своей точки зрения

Принципиально задача донести до людей свою точку зрения в Интернете в ходе информационной войны очень похожа на задачу продвижения сайта или блога компании в рекламных целях. Однако при всем сходстве «боевое» продвижение имеет и отличия от «мирного». Давайте рассмотрим эти сходства и отличия более подробно, сделав упор на «боевом» продвижении.

На наш взгляд, информационная война в Интернете заключается, с технической точки зрения, в том, чтобы свою точку зрения в результатах выдачи по запросу в поисковых машинах как можно выше поднять, а точку зрения противника, напротив, как можно

ниже опустить. При этом приоритет должен отдаваться тем словам, по которым целевая аудитория обычно ищет информацию в нужном нам контексте. Поясним это на гипотетическом примере.

Предположим, какой-то человек любит рыбалку и боулинг. При этом он необоснованно позиционирует себя как крупнейшего в мире специалиста по рыбной ловле, совершая целый комплекс нелицеприятных или криминальных поступков, например, подделывая документы, распространяя заведомо ложную информацию о других рыбаках, присваивая себе несуществующие титулы. Если будет поставлена задача дискредитации этого человека как специалиста по рыбной ловле, то основными словами, по которым будет идти информационная война в Интернете, должны стать его фамилия, имя и отчество в контексте рыбалки. Боулинг при этом может не являться мишенью и даже вообще игнорироваться.

Сами мероприятия в рамках информационной интернет-войны должны проводиться в двух направлениях:

1. подъем в Интернете нашей точки зрения и вытеснение вниз точки зрения противника;

2. удаление из Интернета ресурсов, распространяющих точку зрения противника.

Начнем со второй задачи, поскольку она требует меньше времени на пояснение.

Задача удаления ресурсов противника из Интернета обычно сводится к тому, чтобы поставить организации или людей, разместивших на своих сайтах информацию, поддерживающую противника, перед выбором: убрать эту информацию или испытывать разного рода неудобства. Для этого бывает достаточно просто попросить организацию или частное лицо предоставить документы, подтверждающие размещенную на их сайте информацию. Если информация недостоверна, за этим обычно следует ее добровольное снятие с ресурса. Если же этого не происходит, то вполне допустимо, на наш взгляд, обратиться в контролирующие органы с просьбой проверить достоверность распространяемых сведений и, если сведения недостоверны, принять меры. Мы уже приводили пример наказания организации, распространявшей недостоверные сведения.

Если организации или частные лица разместили ложную информацию, то мы одобряем подобное законное давление на них, рассматривая его как досудебное удаление

ложной или клеветнической информации из информационного поля. При этом очень важно, по нашему мнению, не переходить рамки закона.

Иная ситуация, если размещена правдивая информация или просто высказано мнение по какому-либо вопросу. Мы согласны с точкой зрения, что свобода слова должна существовать реально и никто не вправе давить на людей или СМИ, распространяющих пусть неприятную кому-то, но правдивую информацию. Особенно если при этом предоставлено место для выражения точек зрения всех конфликтующих сторон.

Интересно отметить, что в современных информационных войнах и информационных стычках стороны конфликта иногда вспоминают о том, что свобода слова гарантируется Конституцией, и периодически апеллируют к ней.

Однако на практике в политике, да и в бизнесе, сплошь и рядом встречается давление на тех, кто высказал правдивую, но неприятную для кого-то точку зрения. Порой это давление может принимать криминальные формы – угрозы или шантаж. Иногда воздействие пытаются оказать не на людей, а на технику. Для удаления ресурса из Ин-

тернета некоторые участники конфликтов прибегают к услугам хакеров, организующих DDoS-атаку,[20] делающую недоступным сервер с сайтом. Несмотря на то что подобные хакерские атаки являются преступлением, предусмотренным Уголовным кодексом, это не всегда останавливает злоумышленников.

Первая же задача (подъем в Интернете нашей точки зрения и вытеснение вниз точки зрения противника) столь масштабна и имеет настолько разные варианты решения, что ей посвящена практически вся эта книга. Сейчас мы, пожалуй, скажем лишь, что между «боевым» и «мирным» продвижением своей точки зрения, а точнее, информационных ресурсов, эту точку зрения содержащих, есть одно существенное отличие: «боевое» продвижение может быть более агрессивным и в общем случае меньше требует оглядываться на неписанные, но общепринятые правила поведения в Интернете.

Так, при «мирном» продвижении сайта предприятия человек, ответственный за его продвижение, постоянно балансирует на грани, за которой его могут обвинить в поисковом спаме, т. е. в попытке исказить выдачу поисковых машин и «выбросить» его от-

туда. А поскольку эта грань четко не очерчена и вообще эфемерна, оптимизатору приходится вести себя так, чтобы заведомо не подходить к ней слишком близко. Это гарантирует ему, что он не будет обвинен в поисковом спаме, но при этом значительно замедляется и дорожает продвижение сайта. Довлеет над оптимизатором и понимание того, что корпоративный сайт недешев. Это обусловлено тем, что его изготавливают обычно специализированные агентства, стоимость услуг которых достаточно велика. Адрес его также представляет самостоятельную ценность, поэтому оптимизатор корпоративного сайта просто не может им рисковать.

«Боевые» сайты этих недостатков лишены. Они создаются, как правило, специально для ведения информационной войны и часть из них вполне может выполнять задачи «пограничной заставы», которая даже ценой своей возможной гибели в схватке обеспечивает сдерживание противника до подхода основных сил. Такие сайты, подобно кораблям-брандерам, поджигавшим корабли противника в морских баталиях прошлого, атакуют быстро и поднимаются высоко.

Методы быстрого подъема этих сайтов столь агрессивны, что могут быть сочтены

поисковым спамом, что приведет к удалению этих сайтов из поисковых машин. Однако алгоритм признания сайта спамерским (это решение принимают роботы) потребует значительно больше времени, чем необходимо для подъема сайта в выдаче поисковиков. А значит, такой сайт будет достаточно долго виден целевой аудитории. Если его заголовки и сниппеты (те несколько строк, которые видны в выдаче поисковика) позволяют довести до людей свою точку зрения, они будут работать в течение одной-трех недель даже после полного удаления сайта из Интернета, потому что по-прежнему видны в выдаче.

Люди некреативные иногда поступают очень просто: выпускают волнами «сайты-брандеры» – так, чтобы к моменту гибели «брандера» предыдущей волны появлялись следующие.

Подобным образом действуют прежде всего настоящие спамеры. Они выпускают дорвеи (сайты, не несущие никакой полезной информации и служащие лишь для привлечения пользователя и его автоматической переброски на нужный спамеру сайт). Дошло до того, что созданы специальные программы, которые генерируют дорвеи авто-

матически, по мере их уничтожения поисковыми машинами. Такие программы сами проверяют численность «своих» дорвеев и добавляют новые взамен исчезнувших. Но мы не любим спамеров и не одобряем их деятельность. Тем более что и без спамерских методов можно справиться с продвижением «боевого» сайта, если понимать механизмы работы поисковых машин и стараться не осложнять жизнь ни их владельцам, ни простым пользователям Интернета. И сделать это можно быстро, при этом не потеряв их из-за того, что их сочтут спамом.

Но в целом все же можно считать, что разница между «боевым» и «мирным» сайтами примерно такая же, как между пассажирским самолетом и бомбардировщиком: невозвращение пассажирского самолета из полета – это чрезвычайное происшествие и трагедия, а потеря бомбардировщика после бомбометания – событие нежелательное, но допустимое.

Кроме того, «мирное» продвижение сайта, как правило, производится по ключевым словам, за которые идет большая конкуренция (например, «пластиковые окна», «металлопрокат», «изготовление сайтов» и пр.). «Боевое» продвижение идет чаще всего по

словам, конкуренция по которым значительно ниже – вроде «Постирушка-импэкс стиральные машины» (применительно к гипотетическому ООО «Постирушка-импэкс», продающему бытовую технику).

Требования к информации, которая будет распространяться в ходе отражения информационного нападения

Из собственного опыта и наблюдения за успехами и просчетами чужих информационных войн в Интернете мы сделали вывод, что информация, которая будет подниматься в результатах выдачи поисковых машин, должна соответствовать нескольким критериям.

1. Достоверность. Это справедливо как в отношении позитивной информации о себе, так и негативной о противнике. На наш взгляд, оба эти вида информации необходимо использовать при отражении информационного нападения.

Мы полностью согласны с известным высказыванием Козьмы Пруtkова: «Единожды солгавший, кто тебе поверит?» Нет ничего хуже, чем распространять информацию, которая может быть опровергнута документально, потому что в результате дискредитируется все остальное, что исходит от источника, уличенного во лжи.

Например, в нашей практике встречалась такая ситуация. Один из субъектов рынка, на котором важны личностные характеристики участников, стремительно утрачивал свои позиции, становился аутсайдером. Это происходило из-за того, что когда-то он был монополистом, но теперь его продукт устарел, а квалификации для совершенствования не хватало. Тогда «отстающий» для восстановления своих позиций решил разыграть карту черного PR. Чтобы дискредитировать конкурента, он заявил, что на странице 101 своей книги тот якобы разместил минимально измененный текст третьего автора, не сославшись на источник. Развивая это информационное наступление, аутсайдер тут же поспешил заклеить своего конкурента как плагиатора. Оклеветанный еще не успел отреагировать на этот выпад, как нашлись дотошные люди, показавшие, что

ссылка, которой, со слов аутсайдера, якобы нет, на самом деле присутствует в начале раздела, на странице 99. Более того, вскоре обнаружилось, что разрешение на размещение такого текста было публично получено от автора первоисточника до выхода книги (энтузиасты и это обнаружили в Интернете и продемонстрировали всем). Естественно, после этого клеветник выглядел весьма жалко. А когда в ходе ответных мероприятий вскрылись факты и подробности его собственного реально существовавшего плагиата, этот выпад вообще стал восприниматься многими наблюдателями как дополнительное отягчающее обстоятельство. После информационной контратаки инициатор черного PR стал широко известен как плагиатор и продавец неконкурентоспособной продукции. В результате своей черной PR-атаки аутсайдер практически отрезал себе пути к восстановлению положения на рынке.

Мы считаем, что если информация размещается общедоступно, она должна подкрепляться документами и свидетельствами, подтверждающими ее правдивость. По мнению многих специалистов в области информационных технологий, не каждое распро-

странение негативной информации является черным PR. Негативизация имиджа, негативные PR-технологии отличаются от черного PR тем, что черный PR – это распространение заведомо ложной информации, тогда как негативные PR-технологии – распространение информации, ухудшающей репутацию человека или организации, но при этом правдивой.

На наш взгляд, негативизация имиджа лжеца или негодяя – не только нормальное, но очень правильное явление. Это позволяет обществу, во-первых, дать справедливую оценку тем, кто переступает через мораль и закон, а во-вторых, является предупреждающим сигналом для потенциальных последователей негодяев. Ведь как известно, значительно лучше предупредить проблему, нежели решать ее, когда она уже возникла. Народная мудрость, кстати, уже давно узаконила право негативизации имиджа на существование, определив лишь один случай, когда о человеке можно говорить или хорошо, или никак.

2. Либо очень смешная, либо очень серьезная подача. Дело в том, что в информационной войне борьба идет, как правило, за мнения людей, изначально не имеющих соб-

ственной точки зрения на то, кто прав, а кто виноват в информационном противостоянии. Необходимо сделать так, чтобы эти люди, которые и представляют собой целевую аудиторию, встали на нашу сторону. Для этого нужно обратиться не только к их логике, но и к эмоциональной сфере.

Поэтому, чтобы максимально облегчить и ускорить понимание нашей позиции, надо обосновывать ее не только эмоционально, но и логически. Это обоснование должно сопровождаться документами и историческими аналогиями, а также объяснять корыстные мотивы противника, заставляющие его поступать в отношении нас бесчестно. Кроме того, такой подход помогает выставить противника в максимально негативном свете (разумеется, он этого заслуживает – ведь мы говорим правду. Но кому охота в этом самостоятельно разбираться?).

Изложение фактов о противнике смешным языком, высмеивание его странных, противоречивых или откровенно глупых поступков дискредитирует его как нельзя лучше. Как сказал один из ведущих политтехнологов нашей страны, «если над человеком ржали до слез, то воспринимать его всерьез уже не будут».

Высмеивание противника – сложная в практической реализации задача. Ведь необходимо не просто найти его недочеты, двусмысленности и глупости в его поступках, но написать такие тексты, которые у большинства людей будут вызывать хохот.

Непосредственному написанию текстов предшествует серьезная работа, которая не каждому по силам. Текстрайтер должен не только грамотно и смешно писать, но и хорошо понимать принципы создания текстов, которые будут использованы в Интернете для отражения информационного нападения. Все тексты, которые он создаст, должны полностью соответствовать этим принципам. Так, например, текстрайтер обязан понимать, что каждый текст должен представлять собой небольшое по объему произведение (примерно полстраницы в Word четырнадцатым кеглем), из которого должно быть полностью понятно, кого и почему касается этот текст. Нельзя создавать тексты в расчете на то, что читатель уже ознакомился с предыдущими материалами. Максимум, что можно допустить в привязке к предыдущим материалам в Интернете, – дать гиперссылку на такие материалы, снабдив ее пояснением, что причины появления текста объяс-

нены на сайте, расположенном по этой гиперссылке, либо что там содержатся документы, подтверждающие текст. Текстрайтер должен постоянно помнить, что читатель, столкнувшийся в Интернете с текстом номер 335, может не иметь никакого желания читать предыдущие 334. При этом вся основная информация, которую требуется довести в ходе информационной войны до целевой аудитории, должна содержаться в этом тексте номер 335. Определяя в деятельности противника или его текстах направление для высмеивания или анализа, текстрайтер должен быть готов (и способен) проделать достаточно непростую работу.

Нам вспоминается в этой связи случай, когда обстоятельства вынудили нас скрупулезно изучить методами конкурентной разведки деятельность одного человека, который объявил себя светилом чуть ли не мирового уровня по одному из специальных вопросов. Из официальных же документов следовало, что он являлся обыкновенным рядовым сотрудником относительно небольшой организации, при этом не имел ни профильного образования, ни ученой степени, ни серьезных публикаций, ни официально признанных достижений в той сфере специаль-

ных знаний, на которую претендовал. При этом он вел себя с клиентами организации, в которой работал рядовым сотрудником, так, будто не организация, а лично он заключал с клиентами договор на услуги и исполнял его (что также противоречило реальному положению вещей). В довершение ко всему проверка показала, что он самовольно выдавал клиентам документы, хотя таких полномочий не имел. Затем этот самозванец уволился, стал человеком без постоянного места работы, но, рекламируя себя, по-прежнему представлялся серьезным специалистом. Он продолжил самовольно выдавать документы, имитирующие государственные образцы, привлекая к себе таким образом доверчивых клиентов. Заметив, что мы все-таки стали разбираться с его истинным статусом (мы осознанно на определенном этапе работы перестали скрывать свою активность), он занервничал, стал вести себя очень агрессивно, на официальные обращения не реагировал, а затем и вообще начал совершать противоправные действия с использованием возможностей Интернета, принялся делать клеветнические заявления в адрес тех, кого считал причастными к нашим действиям. Тогда мы провели консуль-

тации в профессиональном сообществе, к которому принадлежал этот человек, в том числе с участием зарубежных специалистов, признанных в профессиональной среде. По итогам консультаций было принято решение провести негативизацию его имиджа, рассказав общественности правду о нем, и для этого обнародовать документы, полученные в ходе проверки его деятельности. Этому человеку было предложено добровольно прекратить кампанию клеветы против конкурентов, а также исключить ложную информацию из своей рекламы. Он отказался, и операция по негативизации его имиджа началась.

Текстрайтерам пришлось тогда проделать большую работу по изучению примерно 150 страниц, написанных этим человеком за несколько лет его работы на рынке. По их словам, это стало непростой задачей, так как изучаемые тексты были составлены стилистически безграмотно, изобиловали двусмысленностями и пестрели наукообразными изречениями, призванными замаскировать непонимание автором предмета, о котором он пишет.

После успешного завершения этой предварительной работы к документам, получен-

ным в ходе проверки деятельности интересующего нас человека, добавились тексты, созданные текстрайтерами. Они либо высмеивали его мысли и поступки, либо анализировали их. Важно, что при этом и те, и другие виды текстов основывались на реальных высказываниях. Тексты, написанные текстрайтерами, не содержали никаких оскорблений, а лишь доводили до читателя мнение их авторов о том, как они восприняли проанализированные ими «произведения». У многих читателей в результате создавалось значительно более полное представление о человеке, который предлагал им свои услуги, чем после ознакомления с его рекламой. Если раньше потенциальные клиенты редко вчитывались в длинные и трудночитаемые «произведения», то теперь они получили возможность ознакомиться и с избранными местами его «авторских материалов», и с комментариями по этому поводу других людей. Самозванец попытался экстренно исправить свои тексты, основываясь на найденных и озвученных «ляпах», однако его новые опусы были ничуть не более грамотными, чем старые, и лишь добавили материала для творчества текстрайтеров.

Обычно авторов, умеющих писать по-настоящему смешно на любую тему, мало, и поэтому их услуги на рынке стоят недешево.

Практика показала, что дополнить (именно дополнить, но не заменить) текстрайтеров, пишущих смешные тексты, могут люди, которые умеют использовать анекдоты в тему. Сегодня в Интернете есть немало сайтов, на которых можно найти анекдоты практически на все случаи жизни (правда, среди них много нецензурных, поэтому и здесь требуется проделать определенную работу, чтобы выбрать подходящий материал). Если поработать с этими сайтами, всегда можно найти не одну сотню анекдотов, которые иллюстрируют качества оппонента. Ведь на самом деле при всем многообразии поступков отдельных людей те из них, кто опускается до черного PR и поэтому становится объектом противодействия, часто обладают одним или сразу несколькими отрицательными качествами, о которых обычно и слагаются анекдоты: жадность, глупость, тщеславие, трусость, злобность, подлость, упрямство, беспринципность, мстительность и т. д.

Помимо анекдотов, высмеивающих определенные отрицательные качества людей, существуют и такие, которые вызывают

смешные ассоциации, настраивают на определенное восприятие дальнейшего текста. К таким «анекдотам-настройщикам» мы бы отнесли встретившийся нам в ходе отражения реального информационного нападения анекдот, размещенный кем-то из участников конфликта: «Первое правило моряка: если предмет движется – отдай ему честь, если не движется – покрась его!». [21]

3. Наличие не более пяти простых мыслей, которые будут доведены до людей, а затем регулярно повторены разными словами. Эти ключевые мысли должны быть предельно простыми, понятными и лаконичными. Причем понятны они должны быть именно той категории людей, на которую рассчитаны. Здесь, как ни в каком другом деле, требуется «равнение на отстающих», и это особенно важно, когда речь идет о доведении своей точки зрения до неопределенного круга лиц, среди которых есть малообразованные люди.

Хотим привести в этой связи слова Вальтера Николаи, руководителя германской военной разведки времен Первой мировой войны. Думаем, что читателю не следует буквально воспринимать и напрямую применять к информационной войне в бизнесе

слова, сказанные в начале XX века о пропаганде после поражения страны в войне, но основная идея, безусловно, заслуживает внимания.

Неправильно придавать пропаганде слишком большую многосторонность (что уместно, может быть, когда дело идет о научном преподавании предмета).

Восприимчивость массы очень ограничена, круг ее понимания узок, зато забывчивость очень велика. Уже по одному этому всякая пропаганда, если она хочет быть успешной, должна ограничиваться лишь немногими пунктами и излагать эти пункты кратко, ясно, понятно, в форме легко запоминаемых лозунгов повторяя все это до тех пор, пока уже не может быть никакого сомнения в том, что и самый отсталый из слушателей наверняка усвоил то, что мы хотели. Как только мы откажемся от этого принципа и попытаемся сделать нашу пропаганду многосторонней, влияние ее сейчас же начнет рассеиваться, ибо широкая масса не в состоянии будет ни переварить, ни запомнить весь материал. Тем самым результат будет ослаблен, а может быть и вовсе потерян.[22]

В случае распространения этой информации в Интернете к общим принципам ин-

формационной войны добавляется и необходимость учитывать особенности поисковых машин. Мы рассмотрим это подробно в соответствующих разделах книги.

4. Отсутствие оскорблений и ругательств в адрес противника.

Целевая аудитория в Интернете, за исключением самых молодых людей, имеет довольно высокий уровень образования. Как правило, образованные люди за ругательствами и оскорблениями, так же, как за ложью, видят бессилие и неспособность аргументировать свою точку зрения, и это может снизить эффективность противодействия информационному нападению.

5. Ключевые мысли должны затрагивать основную деятельность объекта. При противодействии информационному нападению, как мы уже говорили, принципиальное значение имеет дискредитация атакующей стороны, а не оправдания в отношении тех ложных обвинений, которые содержатся в волне черного PR в отношении вас. Оправдываться при нападении черных пиарщиков и бессмысленно, и вредно. Ну в самом деле – как можно доказать, что вы, например, не пьете йогурты прямо в супермаркете, не заплатив за них? Зато отрицательный

эффект при попытках оправдываться будет очевиден. Поэтому правильнее при противодействии информационному нападению сосредоточиться на том, чтобы показать истинное лицо агрессора. В этом случае, как справедливо указывают А. С. Ольшевский и А. С. Ольшевская в своей книге «Негативные PR-технологии», [23] надо сконцентрироваться на тех качествах объекта и фактах, их подтверждающих, которые являются определяющими в деятельности объекта. Аргументированно обвинять магазин по продаже дорогих компьютеров в том, что у него плохая сервисная служба, значительно более перспективно, чем сообщать, что у него маленькая парковка для посетителей.

Показывать, что астроном, утверждающий, что он написал много книг и открыл много планет, не смог предъявить ни одной официально изданной книги и ни одной зарегистрированной им планеты, правильнее, чем писать, что он ходит на работу в желтых носках и синих шортах.

Артем Овсянников проиллюстрировал этот раздел следующей схемой (рис. 4).

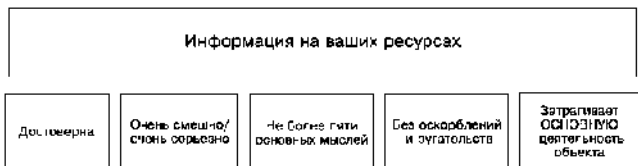


Рис. 4. Требования к информации, которая будет распространяться в ходе отражения информационного нападения

На вас «наехали»

Чего делать нельзя

Итак, в Интернете появились отдельные материалы или целые сайты, которые порочат вашу деловую репутацию, обливают грязью ваше честное имя и унижают ваши честь и достоинство. Пора брать в руки виртуальное оружие и давать отпор врагу. Но не стоит сразу же бросаться в битву сломя голову. Перво-наперво необходимо понять некоторые вещи, составить четкий план противодействия черным пиарщикам и уяснить для себя, что делать.

Для начала о том, чего делать нельзя ни при каких обстоятельствах. По большому счету этих «нельзя» всего два. Какой бы грязью вас ни обливали, не оправдывайтесь и не впадайте в ярость. Можно добавить еще и третье – не отмалчивайтесь, но этот ход зависит от ситуации, поэтому рассмотрим его ниже.

1. Не оправдываться. Достаточно вспомнить поговорку «оправдание – удел виноватых» – и в справедливости тезиса «не оправдываться» дальше можно не убеждать.

Любое оправдание ставит вас в крайне невыгодное положение нашкодившего ребенка, который пытается уверить окружающих, что это не он съел варенье и разбил вазочку. Дескать, варенье само испарилось, а вазочка взяла, да и упала. Никакая, даже самая железобетонная, аргументация вам не поможет, если вы настроитесь на оправдательный тон. Бесполезно говорить о том, что во время дебоша в гей-клубе вы не могли там находиться, потому что были в заграничной командировке. Бесполезно призывать свидетелей вашего пребывания в Антананариву и выкладывать на свой сайт сканы командировочного удостоверения, авиабилетов, страницы загранпаспорта с отметками пограничного контроля и фотографии на фоне достопримечательностей Мадагаскара – не поможет. Все вами продемонстрированное будет объявлено фальшивкой, а у атакующей стороны найдется вдвое больше свидетелей того, как вы крушили зеркальные стены клуба и избивали бармена гигантским фаллоимитатором. Фотографии вашего разгула тоже найдутся, причем в изобилии. Перефразируя Остапа Ибрагимовича Бендера, можем вас уверить: при современном развитии компьютерных технологий смонтиро-

вать фотографии – это такой пустяк, что об этом смешно говорить...

Если вы думаете, что нарисованная нами картина погрома в клубе – это лишь плод не совсем здоровой фантазии авторов, то ошибаетесь, в жизни бывает куда как круче.

Так, однажды, во время избирательной кампании одному из авторов довелось столкнуться с заказным материалом против кандидата (директора крупного рыбозавода), где в красках расписывалось, как он практически ежедневно избивает женщин, работающих на заводском конвейере... замороженными рыбинами!

2. Не впадать в ярость. Не надо брызгать слюной в бессильной злобе и истерить. В одной из своих работ доктор психологии, профессор Тимоти Лири писал: «Эмоции – это низшая форма сознания. Эмоциональные действия – это самая ограниченная, примитивная и опасная форма поведения. (...) Эмоциональный человек не способен думать; не способен совершать реальные смелые действия (за исключением тех, что связаны с физической агрессией и силой). (...) Человек в эмоциональном состоянии – это робот, отличающийся дикой и неистовой яростью в бою».[24]

Злость – очень плохой помощник. Все, на что вы способны, отражая информационную атаку во взвинченном состоянии, – лишь масса бессвязных и неаргументированных обвинений ваших обидчиков во всех смертных грехах и перевод действия в плоскость яростного спора по принципу «Дурак!» – «Сам дурак!».

Можете поверить, что, пойдя по этому пути противодействия, вы в лучшем случае поставите себя в нелепое и смешное положение, а в худшем – вызовите у наблюдающих за развитием событий стойкое убеждение, что обвинения против вас небеспочвенны.

Теперь поговорим о «тактике замалчивания». В некоторых случаях это наиболее оптимальный подход к направленному против вас черному PR. Но срабатывает он только в том случае, если вы убеждены, что негативная информация не будет иметь широкого распространения и, выражаясь языком военных, останется в рамках локального конфликта. Учитывая специфику Интернета, можно с высокой степенью уверенности предположить, что такая чернуха никогда не поднимется на первые строки новостных сайтов и поисковых систем, а через довольно короткое время и вовсе утонет в информаци-

онном океане.

Если вы все же решитесь отреагировать на такой мелкий выпад ваших недругов, то не стоит забывать об адекватности действий, а также о том, что излишнее рвение в отражении нападения может здорово сыграть на руку организаторам атаки. Помните анекдот, где утверждалось, что войны не будет, но будет такая борьба за мир, что камня на камне не останется? Это тот самый случай. Слишком усердствуя в своих действиях, вы станете играть на стороне противника, сами распространяя на себя компромат. О таком счастье любой агрессор может только мечтать!

Другое дело, когда оценка ситуации с выбросом негатива такова, что распространение компрометирующей информации неизбежно и последствия от ее тиражирования в Интернет могут стать для вас весьма пагубными. Тут уже нельзя отмалчиваться, поскольку игнорирование инсинуаций против вас будет расценено общественностью как слабость, отсутствие аргументов в вашу пользу, и в итоге все решат, что все сказанное о вас – чистая правда, какой бы грязной она ни была. Поэтому планируем свои действия и переходим к активным мероприяти-

ям.

Артем Овсянников предложил для иллюстрации сказанного следующую схему (рис. 5).

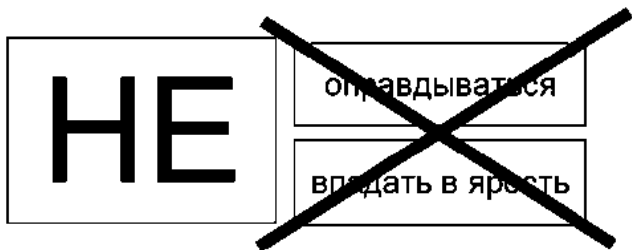


Рис. 5. Чего в информационной войне делать нельзя

Есть ли у вас план?

Тщательное планирование своих действий на основе трезвого анализа ситуации при отражении информационного нападения позволит вам не только оценить свои силы и возможности, но и не даст совершить многих серьезных просчетов и ошибок. Не забывайте – некоторые из них вполне могут стать для вас фатальными.

В первую очередь успокойтесь (помните, чего делать нельзя?), отбросьте эмоции и задайте себе сакраментальный вопрос, кото-

рый задавали еще древние римляне: «Qui prodest?» («Кому выгодно?»). Возможно, что, ответив на него, вы сможете хотя бы приблизительно сориентироваться и определить круг потенциальных агрессоров. Однако не следует забывать, что ваши выводы могут быть ошибочными и кто-то имитирует одного из ваших недругов, подсовывая вам очередную версию. Так что всегда есть смысл делать поправку на такие варианты, перепроверять свои сомнения уже в процессе «боевых действий» и по мере необходимости вносить тактические коррективы в ваш план.[25]

Следующим этапом вашего анализа, предваряющего планирование активных мероприятий в Интернете, должно стать осмысление цели, которую преследует нападающая сторона. Согласитесь – довольно бессмысленно бросать все силы на защиту своего бизнеса, если удар направлен на разрушение вашей семьи. Понимание направления удара позволит вам сконцентрировать оборону именно там, где она больше всего необходима.

Стадия планирования действий заключается в следующем:

- постановке целей, которых вы собираетесь добиться своими действиями;
- сборе и накоплении информации, которая необходима для ведения мероприятий;
- выработке стратегии противодействия;
- определении тактических методов;
- выборе оптимальных инструментов реализации ваших задач;
- подготовке плана конкретных мероприятий;
- определении «союзников» и способов их вовлечения в процесс;
- подготовке материалов для размещения в сетевом пространстве (текстов, фото, графики и т. д.);
- выборе методов контроля за результатами вашей деятельности.

Не стоит подходить к планированию своей активности слишком поверхностно. Дескать, ввяжемся в драку, а там видно будет. Сделав такой опрометчивый шаг, вы рискуете набить себе множество болезненных шишек, а то и вообще сломать шею – в переносном, разумеется, смысле, но с вполне реальными последствиями для вашей репутации.

Однако не стоит и слишком мудрить. Со всем ни к чему разворачивать ваш план на полсотни страниц и составлять график ме-

роприятий на год вперед. Все должно быть в меру – достаточно иметь четкую картину действий на ближайшее время: месяц, от силы два. Вполне вероятно, что за этот период вам удастся решить свои проблемы с распространением негативной информации, направленной против вас. Если же этого не произойдет и атаки будут продолжаться, откорректируйте свои планы в соответствии с ситуацией.

В штыковую или...

Выбор стратегий противодействия черному PR в общем-то не богат и в традиционном коммуникативном пространстве, а в сети Интернет он и того меньше. В целом вы можете выбрать либо метод «лобового столкновения», либо «партизанской войны».

Идти на противника в полный рост, с поднятым забралом – это, конечно, по-рыцарски благородно, но довольно безрассудно, если не сказать глупо. Особенно в случае с черным PR в виртуальном пространстве. Ни к каким положительным для вас результатам такое «донкихотство» не приведет. Перечитайте Сервантеса, если позабыли, чем окончилось сражение благородного идальго с

ветряными мельницами. Приняв вызов противника, вы изначально оказываетесь в проигрышном положении, соглашаясь с его правилами игры. Дело усугубляется тем, что эти правила вам наверняка неизвестны. А вот противник, напротив, знает их хорошо, поскольку он их и придумал. Так что будьте готовы к тому, что во все ловушки и засады, которые агрессор заботливо для вас подготовил, вы попадете, к его большому удовольствию.

Проблема этой тактики противостояния негативу в Интернете осложнена еще и тем, что вам неизвестно, с кем вы воюете. Разумеется, эмпирическим путем вы можете с достаточной вероятностью определить заказчика и инициатора нападения, особенно если удар направлен против вашей основной деятельности. Круг лиц, заинтересованных в захвате ваших позиций в бизнесе, политике, общественном положении и т. п. должен быть вам известен. Но даже в этом случае ваши предположения остаются лишь предположениями, не более того. А если атака организована не так прямолинейно и удар направлен на ваши личные качества или вообще опосредованно – на ваших родных и близких? На кого тогда идти с шашкой

наголо?

Конечно, можно попытаться привлечь к ответственности владельцев ресурса, на котором появились материалы дискредитирующего характера. Представим себе, что вам удалось точно выяснить, кто хозяин сайта – такое тоже не исключено, особенно если он зарегистрирован в Министерстве печати и имеет лицензию электронного СМИ, как, к примеру, Агентство федеральных расследований FreeLance Bureau.[26] Однако поспешим охладить ваш пыл и заметим, что в нашей стране судиться со средствами массовой информации могут либо большие любители тяжб, либо достаточно богатые люди, которые не пожалеют средств для того, чтобы решение было принято в их пользу. О том, куда и кому именно пойдут эти средства, мы благоразумно умолчим, пусть читатели додумают сами.

Подать иск против интернет-ресурса можно. Можно даже выиграть его и заставить в судебном порядке принести вам извинения, опубликовать опровержение и заплатить компенсацию ущерба. Это так, и подобные случаи известны и в зарубежной, и в отечественной практике.

Абаканский городской суд удовлетворил требования Исаковского В. В., который обратился с иском к учредителю интернет-сайта nacbez.ru о защите чести и достоинства, просил признать ряд утверждений в опубликованных статьях не соответствующими действительности и порочащими честь, достоинство и деловую репутацию Исаковского В. В. и обязать администратора домена nacbez.ru Афанасьева М. В. опубликовать на сайте www.nacbez.ru опровержение утверждений, а также взыскать компенсацию морального вреда.

Доказывая факт распространения порочащих сведений, истец представил суду графическую копию текста указанных статей за протоколированных нотариусом с интернет-сайта www.nacbez.ru

Суд, изучив содержание статей, пришел к выводу о порочащем характере этих сведений, поскольку они свидетельствуют о фактах совершения Исаковским В. В. нечестных, незаконных поступков недобросовестности при осуществлении его служебной деятельности.

Как пояснил в судебном заседании ответчик Афанасьев, он является собственником домена www.nacbez.ru с 17.02.2004 года. Из

письма директора Российского НИИ развития общественных сетей (г. Москва) следует, что Афанасьев М. В. является администратором домена www.nasbez.ru. Возражая на иск, ответчик ссылается на то, что опубликовать на сайте www.nasbez.ru оспариваемые сведения могло любое другое лицо, поскольку к сайту открыт доступ. Между тем, как следует из пояснений специалиста Могилевского, размещение на указанном сайте информации лицами, не владеющими логином и паролем (идентификаторы заказчика по договору № 107688 об оказании услуг), возможно лишь при несанкционированном доступе.

Доказательств несанкционированного доступа к сайту www.nasbez.ru ответчик суду не представил.

Довод ответчика о том, что сведения в отношении истца в виде сообщений на сайте распространялись не им, а анонимными посетителями сайта, доступ к которому является свободным, является несостоятельным. Поскольку возможность появления порочащих истца сведений на страницах сайта www.nasbez.ru является следствием создания ответчиком как владельцем (администратором) доменного имени соответствующих технологических условий, суд приходит

к выводу о том, что распространителем оспариваемых сведений является ответчик Афанасьев М. В.

По мнению суда, распространенные в отношении истца сведения являются порочащими, поскольку содержат негативную оценку служебной деятельности Исаковского В. В., свидетельствуют о его коррумпированности, совершении под его руководством исполнительных действий без установленного регламента, т. е. о нарушении требований Закона «Об исполнительном производстве» и другого действующего законодательства.

В связи с тем, что указанные сведения были распространены в сети Интернет путем размещения на сайте www.nacbez.ru, суд полагает, что опровергнуты эти сведения должны быть также в сети Интернет на сайте www.nacbez.ru.

Руководствуясь ст. 1100 ГК РФ, п. 15 Постановления Пленума Верховного Суда РФ от 24.02.2005 г. № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц», а также требованиями разумности и справедливости, суд оценил размер компенсации морального вреда в 30

000 руб.[27]

А что же вы получите в качестве «бонуса» к удовлетворению судебным решением и скромной сумме компенсации морального вреда? Громкую огласку дела, широкое распространение негативных материалов в традиционных СМИ и Интернете, повышенный интерес сообщества к компромату против вас и, возможно, непоправимый репутационный ущерб. Заметьте, все это вы сделаете своими руками. Добавим к этому еще и значительную пролонгацию конфликта и переход информационного противостояния в хроническую фазу «кто кого пересидит по шею в грязи». Затягивая баталию, вы реально рискуете получить несмываемое пятно на своей биографии. Окружающие уже давно забудут суть препирательств, но воспоминания о том, как вы лили ответную грязь на ваших противников останется очень надолго.

Репутационная война «лоб в лоб» не просто бессмысленна – она деструктивна, и в первую очередь для того, кто решил ей противостоять таким манером. На создание репутационного ущерба уходят годы, разрушить его можно в считанные дни, а на восстановление, возможно, не хватит оставшейся жизни.

Политтехнологам с опытом работы на избирательных кампаниях хорошо известно, что ввязываться в открытое противостояние с конкурентами и якобы независимыми критиками, в стиле взаимных оскорблений – гиблое дело для кандидата. При обвинении сторон во всех тяжких грехах и обоюдном вытаскивании на всеобщее обозрение грязного белья победителей, как правило, не бывает. Нередки случаи, когда лидеры предвыборной гонки настолько увлекались черным PR по отношению друг к другу, что фаворитом неожиданно становился вчерашний аутсайдер, которого никто всерьез и не воспринимал. Помните китайскую притчу о мудрой обезьяне, которая сидела на дереве и наблюдала за смертельной схваткой двух тигров? Один из тигров был повержен, а второй настолько ослаб в бою, что обезьяна, спустившись с дерева, легко добила его палкой и забрала добычу, из-за которой хищники и сцепились. Тот самый случай. Избирателям настолько надоедает грызня лидеров и обилие жареных фактов на того и другого, что они либо на все плюют и не идут на выборы, либо голосуют «протестно» – за кого угодно, только не за «этих».

Для того чтобы эффективно противостоять черному PR во время избирательной кампании, но самому при этом остаться незапятнанным, часто используются так называемые боковины – кандидаты, которые внешне никак не связаны с объектом атаки, а скорее наоборот – составляют ему конкуренцию. На деле эти «боковые кандидаты», разумеется, никоим образом не противопоставляются «своему» претенденту на выборную должность и не оттягивают на себя голоса его избирателей. Одной из основных задач таких участников избирательного процесса является «слив» негатива на конкурентов от своего имени и исполнение роли своеобразного буфера, который реагирует на все выпады оппонентов и принимает удар на себя. Данная технология, отлично зарекомендовавшая себя в предвыборных войнах, была применена одним из авторов этой книги для противостояния попыткам дискредитировать имидж и деловую репутацию в сферах, далеких от политики. Результатом все остались довольны – атака была не просто отражена, а превратилась в контрнаступление, вернувшись к противнику с такой силой и эффектом, что это напрочь отбило охоту у агрессора к продолжению и развитию

конфликта.

Приведенный выше пример использования «боковых структур» – лишь одна из возможностей ведения диверсионной партизанской войны в информационном пространстве. Основная идея, которая лежит в основе любых действий, проводимых в рамках данной стратегии, – избежание прямых столкновений с противником, нанесение ударов таким образом, чтобы ваше участие оставалось невидимым сторонним наблюдателям и самому инициатору нападения, а ваша управляющая роль не могла быть идентифицирована с достаточной долей уверенности.

Кстати, притчу об обезьяне и тиграх очень любил основатель Китайской Народной Республики Мао Цзэдун, который считал Китай мудрой обезьяной, наблюдающей за битвой тигров – СССР и США. Время, увы, доказало правоту и прозорливость Великого кормчего – один из тигров пал...

Основные приемы борьбы с черным PR в Интернете

Итак, вы спланировали свои ответные действия в части стратегии, тактики и инструментов реализации своего плана в сети Интернет. Настал момент определиться, как вы будете подавать «контрчернушный» материал на своих интернет-ресурсах.

1. Доведение до абсурда. Вы можете взять за основу своего контента весь негатив, который направлен против вас, и гипертрофировать его до полного бреда. Включайте фантазию на полную катушку и начинайте сочинять о себе небылицы одна другой краше. Вам приписывают нетрадиционную сексуальную ориентацию и склонность к малолетним? Отлично! Пишите, что вы почетный академик всемирной академии сексуальных извращенцев и полномочный представитель тайного ордена садомазохистов в странах СНГ. Не забудьте поведать миру, что у вас разветвленная сеть завербованных воспитательниц детских садов и санитарок родильных домов, которые подбирают вам и вашим сподвижникам малышей для оргий.

Да, будет неплохо, если у вас имеется свой парк детских колясок, в которых вам доставляют детей.

Вас обвиняют в причастности к тоталитарной секте? Замечательно! В красках расскажите о ночных сатанинских мессах на кладбище, на которых вы приносите в жертву юных девственниц и пьете из их черепов человеческую кровь. Да, разумеется, вы магистр этой секты, не меньше.

Появилась информация о том, что вы берете взятки? Годится! Вам приходится это делать, потому что содержание сети воспитательниц и похищение девственниц – очень накладное дело (см. выше). Да и к тому же вам самому нужно давать большие взятки за разрешение строительства вашего замка на Красной площади, а ваша тайная любовница Анджелина Джоли требует в подарок алмаз «Орлов» из Алмазного фонда России.

В общем, это тот самый случай, когда «кашу маслом не испортишь» – лейте щедро.

На кампании по выборам мэра одного из российских городов мы обратили внимание на зарождающиеся попытки нагнетания ксенофобских настроений среди избирателей, которые были явно направлены против на-

шего кандидата как одного из основных претендентов на победу. Время от времени на местных форумах появлялись посты,[28] в которых кандидата загодя обвиняли в том, что, после того как он станет мэром, все ключевые должности в городской администрации будут «заняты его единоверцами», которые разворуют бюджет, приватизируют всю собственность и обложат данью «простого русского труженика».

Все это звучало довольно бредово, но вместо того чтобы отмахнуться, мы решили не рисковать и провели акцию в стиле «доведение до абсурда» и в реальном, и в виртуальном пространстве. В городе появились анонимные листовки, где в нарочито истеричной форме утверждалось, что главной целью нашего кандидата после победы на выборах является немедленное присоединение в виде анклава города к одному из государств, где у власти находятся люди одной национальности с нашим кандидатом, введение поголовной обязанности носить народные костюмы и исполнять ритуалы, еще в древности сложившиеся у народа, к которому этнически принадлежал кандидат, и так далее, и в том же духе. Разумеется, одновременно в Интернете появилась коряво слепленная

страничка с тем же текстом, а на всех форумах, которые массово посещали горожане, постоянно выкладывались ссылки на эту информацию, и обильно цитировался сам текст.

Горожане хохотали дня два, показывая друг другу листовки и интернет-страницу. Само собой, после этого любые спекуляции на теме ксенофобии в отношении этноса кандидата были обречены на провал. Реакцией на редкие попытки поднять «этнический вопрос» был либо смех, либо кручение пальцем у виска и посылание в известном направлении.

2. Смех – страшное оружие! Высмеивание своих недругов и их попыток оболгать честное имя человека во все времена и эпохи было одним из самых мощных средств нейтрализации клеветы и оговора. Еще Михаил Евграфович Салтыков-Щедрин писал о борьбе со злом: «Философы пишут с целью разъяснения подобных действий целые трактаты; романисты кладут их в основание многотомных произведений; сатирики делают то же дело, призывая на помощь оружие смеха. Это оружие очень сильное, ибо ничто так не обескураживает порока, как сознание, что он угадан и что по поводу его уже раздал-

ся смех».[29] О том же говорил и Николай Васильевич Гоголь: «Насмешки боится даже тот, кто уже ничего не боится на свете».[30]

Убийственный сарказм и тонкая издевка над обвинениями в ваш адрес способны не просто нивелировать действие черного PR, но и разрушить его до основания, выставив атакующих в неприглядном и комичном свете.

Внимательно анализируйте тексты ваших противников, находите в них несоответствия, излишнюю заумь и пафос или, напротив, примитивность мышления. Выискивайте явные и скрытые глупости, оговорки, приведенные не к месту цитаты и высказывания, незаслуженно приписываемые заслуги и регалии и т. д., и т. д., и т. д.

Однако не следует забывать и о некоторых ограничениях. Возможно, тот, кто развернул против вас информационную агрессию, известен и вам, и многим интернет-пользователям не только в он-лайне. Упаси вас бог от насмешек над его физическими данными, внешностью или состоянием здоровья. Никогда не используйте в борьбе даже против самых отъявленных мерзавцев, распространяющих о вас чудовищные наветы, нападки на их родных, друзей и близких: во-первых,

они ни при чем, а во-вторых, нельзя переходить тот невидимый рубеж, который отличает порядочного человека от подонка и становиться вровень с ним. Разумеется, каждый сам для себя определяет те морально-этические границы, через которые он не переступит. И уж если так случилось, что у вас эти границы слишком широки, подумайте об инстинкте самосохранения. Частенько это отрезвляет и помогает осознать последствия необдуманного шага. Да и при завоевании симпатий окружающих такой подход заведомо проигрышный. Возможно, какое-то количество маргинальных личностей и станет вашими приверженцами, но вот симпатии порядочных людей вы не завоеуете.

Конечно, далеко не каждый человек наделен даром острого слова и испепеляющей сатиры. И тут уже вам решать – использовать этот инструмент в информационном противостоянии или нет, решиться это делать самому или призвать кого-либо на помощь. Нет ничего хуже неудачной шутки или плоской остроты. И если уж на карту поставлено слишком многое, то, безусловно, лучше обратиться к профессионалам в сфере информационных войн или воспользоваться уникальной возможностью, которую дает

Интернет, – коллективным разумом.

3. «Имидж – все!» Данный подход к проблеме борьбы с негативом не предусматривает прямого противостояния с атакующей стороной. В противном случае все сведется к взаимному боданию на радость зевакам. Информационные войны – это не игра в подкидного дурака: «А я вам валета! А я его дамой! А вот что насчет короля? А мы тузом!» Это гораздо более сложный и многогранный процесс, в котором далеко не всегда выигрывает тот, у кого карта лучше. Да и в подкидном, кстати, тоже без обдумывания ходов и их последствий не обойтись, а туза вполне может побить козырная шестерка.

Внешне, для постороннего взгляда, ваши интернет-ресурсы никак не должны быть связаны с выбросом в сетевое информационное пространство негативных материалов, направленных против вас. Рассказывайте о своих достижениях и планах, показывайте положительные результаты своей деятельности, публикуйте в своих гостевых книгах, блогах и на форумах хорошие и добрые отзывы о себе, любимом. В общем, выстраивайте свой положительный имидж, хольте его, лелейте и усиливайте по мере возможностей.

А вот на уровне, скрытом от стороннего наблюдателя, все должно быть максимально направлено на отражение атаки. Как уже не раз говорилось, задвигайте агрессора как можно глубже и продвигайте свои ресурсы как можно выше. Пользователи Сети, интересующиеся вашей персоной, должны, в первую очередь, попадать на ваши страницы, а до страниц, где вас поливают грязью, они в идеале не должны добраться никогда.

Можно сказать, что это основные приемы борьбы с проявлениями черного PR в Интернете, хотя, безусловно, и не единственные. К тому же различные комбинации из вышеперечисленных методов могут дать довольно большое количество вариантов противостояния информационному нападению.

Главное, помните базовый принцип: в отношении противника вы должны (без прямой связи с его нападками на вас и уж тем более без прямого цитирования этих нападков) продвигать свою точку зрения о нем как можно выше, сдвигая его саморекламу в глубь Интернета. Делайте это, независимо от того, какую из описанных стратегий противодействия вы решили избрать в качестве основной, а какую – в качестве вспомогательной.

Стратегии контратаки визуально представлены на схеме Артема Овсянникова (рис. 6).



Рис. 6. Стратегии контратаки

Работа с информацией

Любая информация как совокупность неких знаний, данных и сведений может быть подвергнута обработке и трансформации. Это в полной мере относится и к той информации, которую мы называем черным PR, вне зависимости от каналов ее распространения.

Еще в 30-е годы прошлого столетия в западной практике политических коммуникаций появилось такое понятие, как «spin». Само это слово переводится с английского языка как «верчение, кружение, вращение», что сразу же рисует довольно наглядную картину того, что делают с информацией при помощи spin-технологий. Принято различать два основных вида таких приемов работы с информацией – spin-мастер и spin-doctor.[31] Технология spin-мастер заключается в подготовке общественного мнения к нужному восприятию предстоящих событий, тогда как spin-доктор предназначен для исправления и коррекции информации, в том числе и имеющей ярко негативную окраску. В контексте информационного противостояния нас, естественно, в первую очередь будет ин-

тересовать именно эта технология, хотя и о методах spin-мастер как способе продвижения своей точки зрения в информационном пространстве мы тоже поговорим.

Итак, что же можно сделать с информацией, которая способна нанести вам серьезный репутационный ущерб? Как мы уже говорили, при незначительной угрозе распространения и минимальном прогнозируемом ущербе на «выброс» можно просто не реагировать, и такая информация сама собой «затухнет». Если же дело грозит более серьезными последствиями, то можно попытаться «утопить» суть в информационном шуме. Конечно, такая возможность есть далеко не всегда. Но если вы можете разместить свою информацию на тех же интернет-ресурсах, где опубликованы порочащие материалы, то постарайтесь выложить туда что-нибудь сенсационное, значимое или просто интересное (лучше побольше и поразнообразнее), что отвлечет на себя внимание посетителей сайта. Благо, Интернет под рукой, а значит, таких сюжетов можно набрать в неограниченном количестве и разнообразии буквально за считанные минуты. Однако не стоит прибегать к рекламе размещенных вами материалов за пределами интернет-ре-

сурсов, так как это неизбежно будет популяризировать и сам сайт, привлекая туда новых посетителей. Не забывайте – там находится информация, направленная против вас, и главная задача состоит в том, чтобы отвлекать от нее тех пользователей, которые уже и так зашли на интернет-страницу Информацию, а точнее ее источник, можно дискредитировать и другим способом, назовем его «Мизантроп» (в литературе его называют также «Принципом Али-Бабы», по аналогии с историей об Али-Бабе, который нарисовал крестики на всех дверях, понимая, что на своей стереть его не может). Суть методики заключается в массовом выбросе созвучных по духу и содержанию материалов, но направленных на другие объекты. Для очистки собственной совести и во избежание проблем объекты должны быть вымышленными, так же как и чернуха в их адрес. Используя этот прием, можно одним выстрелом убить двух зайцев: во-первых, «растворить» сведения, направленные против вас, в однотипном информационном потоке, а во-вторых, подорвать доверие к источнику. Едва ли кто-то станет всерьез воспринимать обвинения против вас, если они проистекают от «человеконенавистника», который поли-

вает грязью всех и каждого, либо от человека, однозначно нездорового психически.

В нашей практике был случай, когда в крупном городе сотрудник одного из кафе написал на тематическом сайте немало гадостей – преимущественно небылиц – о своем бывшем работодателе. Текст был написан от первого лица и поэтому воспринимался читателями как свидетельство очевидца. Для нейтрализации негативного воздействия было проведено мероприятие, в ходе которого на этом сайте появилось еще 48 сообщений абсолютно такого же содержания, где менялись только названия точек общепита. После этого каждому, кто заходил на сайт, становилось очевидно, что «это понаписал какой-то шизофреник». Такая реакция подтвердилась и фокус-группой, которой была поставлена задача прокомментировать увиденное.

Другой, близкий по смыслу «Мизантропу», метод мы назвали «Мыльные пузыри». Его суть – в переключении и акцентировании внимания аудитории на какой-либо мало-значительный момент, содержащийся в негативной информации, и в последующем раздувании этой темы. Гиперболизация и утрирование никчемного по смысловой на-

грузке фрагмента до самой главной темы неизбежно снизят доверие и к источнику, и к самой информации.

Достаточно эффективно работает и метод навешивания ярлыков на своих оппонентов. В сознании каждого из нас существуют определенные стереотипы, используя которые можно вызвать предсказуемые эмоции и реакции. К примеру, восприятие слова «разведчик» порождает, как правило, только положительные чувства. Перед глазами встает героический образ самоотверженного человека с немного усталыми, но проницательными глазами, который, ежеминутно рискуя свободой и жизнью, выясняет зловещие планы врагов нашей Родины. А вот «шпион» наверняка не будет ассоциироваться ни с героизмом, ни с честностью, ни с принадлежностью к «нашим». Не так ли? Хотя на самом деле это слова-синонимы, но так уж сложилось, что наши – «разведчики», а вражеские – непременно шпионы. Так что повесьте на источник информации ярлык, вызывающий отрицательные эмоции большинства, – и уровень доверия к нему и его словам будет значительно снижен.

Как и было обещано, в двух словах коснемся технологии spin-мастер, поскольку пони-

мание ее смысла поможет повысить эффективность воздействия ваших материалов на аудиторию.

Анонсируя скорое появление информации на задействованных вами интернет-площадках и ненавязчиво повышая ее важность, вы не только стимулируете интерес аудитории, но и в некотором роде «программируете» получателей на восприятие сведений как более значимых, чем они есть на самом деле.

Другой немаловажной стороной технологии spin-мастер является так называемый пост-spin – благоприятная реакция на уже опубликованную информацию. Разместить положительные отзывы и комментарии на ваши материалы в Интернете труда не составляет, даже если вы ведете информационную войну в гордом одиночестве. Сайты и программы-анонимайзеры, о которых рассказывается в этой книге, позволяют любому пользователю Сети легко обрести «тысячу лиц и характеров».

Способов «перекручивания» и «полировки» информации существует довольно много. Spin-технологиям посвящены целые тома, поэтому авторы считают, что приведенного выше краткого обзора этой темы будет вполне достаточно, чтобы дать читателям

понимание сути методов и приемов из арсенала spin.

Самые распространенные инструменты черных пиарщиков, или Против чего придется воевать

1. Сайты для размещения компромата.

В Интернете существует целая группа веб-сайтов, специализирующихся на размещении компрометирующих и скандальных материалов. Первым крупным ресурсом для размещения компромата в русскоязычном сегменте Интернет стал сайт «Коготь», появившийся на бесплатном сайте people-weekend.ru 27 ноября 1998 года. «Коготь» был предназначен для массированного «слива» политического компромата. Анонимные авторы размещали на сайте материалы, якобы полученные в результате прослушивания разговоров российских политиков, а также телефоны и адреса известных персон, оперативные справки, результаты наружного наблюдения и т. д. О подлинности этой информации можно только гадать, но необходимый общественный резонанс вполне был достигнут.

Этот сайт просуществовал всего один день и был закрыт правоохранительными органами. Однако его зеркала (копии сайта, расположенные на других адресах в Интернете) тут же появились на зарубежных хостингах. В частности, на американском homeofsex.com. Там, впрочем, «Коготь» проработал только несколько дней – до 1 декабря.

Несмотря на столь непродолжительный срок работы, на «Коготь» обратили внимание не только правоохранительные органы, но и оф-лайн-средства массовой информации – этому ресурсу были посвящены первые полосы «Московского комсомольца» и «Московских новостей».

Время от времени в Сети появляются его продолжатели и последователи – так, в 1999 году был открыт «Коготь-2», который содержал материалы о принадлежности Анатолия Быкова, [32] к преступным группировкам Красноярского края. Потом – «Коготь-3» и т. д. Эти сайты, как правило, возникали в моменты обострения политических противостояний или больших бизнес-войн. Так, на момент написания этой книги пользователям сети Интернет был еще доступен сайт «Коготь-7» [33] располагавшийся на бесплатном хостинге FreeServers.Com Информация

на сайте очень и очень устаревшая и бесполезная. Видимо, это и есть одна из причин, по которой существование сайта «Коготь-7» никого не волнует.

Наиболее известные из подобных ресурсов, успешно функционирующих сегодня, – это, пожалуй, сайт Компромат. Ru,[34] созданный и поддерживаемый (как это декларируется на самом сайте) Сергеем Горшковым, и сайт FLB.[35] Оба сайта имеют зарегистрированные торговые знаки, а Агентство федеральных расследований «FreeLance Bureau» (это полное название сайта FLB) даже зарегистрировано в Министерстве печати России как общественно-политическое электронное периодическое издание. Компромат. Ru кроме всего прочего имеет собственные печатные версии – журнал «Компромат-досье» и газету «Компромат-online».

Сайты этой группы пользуются весьма большой популярностью как у сетевого сообщества, так и у традиционных СМИ, которые охотно их упоминают и цитируют.

Проводя аналогии с массмедиа, можно сказать, что такие сайты сравнимы с крупными федеральными изданиями, а потому многим нашим читателям не стоит беспокоиться, что они опубликуют на них непро-

мат, если, конечно, они не чиновники, занимающие высокие посты, политики крупного масштаба или бизнесмены, ворочающие огромными капиталами.

И тем не менее рассмотрим вариант, когда на одном из таких сайтов появляется информация, которой вы совсем не рады. Есть ли возможность полностью нейтрализовать ее (читай – убрать с сайта) или хотя бы высказать свою точку зрения? В принципе есть, хотя процесс этот крайне муторный и мало-результативный.

Дело в том, что формирование контента[36] этих ресурсов осуществляется по принципу библиотеки. То есть на сайт выкладываются материалы, которые были опубликованы на других интернет-страницах – в основном на сайтах электронных версий средств массовой информации, а также сетевых информационных и новостных агентств. Поэтому ни владельцы Компромат. Ру, ни FLB никакой ответственности за перепечатку не несут, и напрямую заставить их убрать материал нельзя. Однако вы можете обратиться в суд с иском на то СМИ, которое послужило первоисточником, и если ваша правота будет признана, то СМИ должно будет как минимум дать опровержение и снять

со своего сайта порочащую статью. Тем не менее нет уверенности в том, что так же поступят редакторы Компромат. Ru, FLB и им подобных ресурсов. Скорее, вам будет предоставлена возможность дать свои комментарии на ранее опубликованный материал. Эти сайты живут скандалами, которые так любят обыватели, а что может быть лучше для хорошей свары, чем прилюдное препирательство двух сторон конфликта? Конечно, периодически находятся те, кто пытается организовать хакерскую DDoS-атаку на подобные сайты, но обычно такая реакция характерна для людей неопытных в Интернете. «Задосить» весь Интернет или даже его часть надолго невозможно технически, а кроме того, длительная атака на один и тот же адрес рано или поздно чревата для ее исполнителей тюрьмой. На практике проведение подобной атаки лишь привлекает внимание к атакуемому ресурсу, порождает вокруг него массу слухов и заканчивается появлением невообразимого количества его копий в Интернете. Причем многие из них делаются не заинтересованными лицами, а любителями приберечь про запас интересную информацию без какой-либо конкретной цели.

Есть еще один момент, который изрядно затрудняет контроль над публикуемыми на подобных ресурсах материалами, – высокий индекс их цитирования[37] другими сайтами. В считанные минуты после того, как будет опубликован материал, его копии разлетятся по десяткам и сотням других страниц, падких на «горяченькое». На этом все попытки убрать компромат из сетевого информационного пространства можете считать законченными – сделать уже ничего нельзя. Добавьте сюда же сохраненные поисковыми системами страницы, которые будут доступны пользователям, даже если оригинал перестанет существовать.

Но есть еще одна возможность доведения до общественности своей точки зрения, которая напрямую связана с интернет-ресурсами, специализирующимися на сборе и публикации компрометирующих материалов – форумы этих сайтов. Эта тема требует более обстоятельного рассмотрения, и к ней мы еще вернемся в последующих главах книги.

2. Сайты-клоны. Это категория сайтов, предназначенных для введения интернет-пользователей в заблуждение (в лучшем случае) или «слива» порочащей информации (а вот это уже куда как чаще). Сайты-

клоны требуют от своих создателей достаточно больших временных и финансовых затрат.

Клон (или фальшивка) должен как можно более точно воспроизводить сайт-оригинал. Дизайн, цветовое решение, рубрикатор – все должно вызвать у посетителя первое впечатление, что он попал на нужный ему ресурс, а не на фальшивку. Ну а дальше... Дальше у создателей сайта есть надежда, что зашедший на сайт посетитель заинтересуется материалами, которые размещены на ресурсе. Надо ли говорить, что их содержание зачастую представляет собой компромат и чернуху разной степени искусности? Особым шиком среди специалистов черного PR считается ситуация, когда информационное наполнение сайта-клона максимально стилизовано под контент сайта-оригинала.

Как уже отмечалось выше, создание таких сайтов полноценно, в деталях, копирующих структуру крупного портала, – дело затратное и под силу только команде профессионалов: веб-дизайнеров, текстрайтеров, специалистов по мониторингу ресурса-мишени, координаторов, специалистов по PR (разработчиков стратегии акции и тактических решений – отдельных атак и информационных

вбросов в рамках общего плана), а также продвижению сайта в Интернете.

В связи с серьезностью и сложностью задач позволить себе создание такого ресурса может далеко не каждый. В основном сайты-фальшивки используют для недобросовестной конкуренции крупные политические силы или «серьезный» бизнес в корпоративных войнах.

Так, однажды во время федеральных выборов в Интернете появился сайт-клон одной из крупнейших политических партий России. Он был сделан на основе верстки настоящего сайта партии-мишени. Расположение текста и графических модулей было таким же, как в оригинале, но тексты и иллюстрации были заменены на другие. В частности, клон содержал информацию о якобы имеющих место уголовных преступлениях конкретных членов партии-мишени, на нем приводились результаты опросов общественного мнения, прямо противоположные опубликованным на официальном партийном сайте. Выбранное для клона доменное имя было созвучно настоящему, точнее, оно было в точности как у настоящего сайта, но располагалось в другой доменной зоне. Например, если бы название партийного

сайта было partija.ru, то сайт-клон был бы зарегистрирован с именем partija.net.

Во время региональных выборов мы сталкивались с сайтом, в точности копировавшим реальный сайт завода, директор которого баллотировался в депутаты Областного законодательного собрания одного из регионов России. Портрет директора и фотографии завода оставались прежними. Но тексты были заменены на другие, примерно такого содержания: «Первый миллион долларов мы украли вместе с таким-то на таких-то махинациях. Потом еще десять миллионов с таким-то на таких-то операциях. А электорату мы втираем, что...». Методами поисковой оптимизации сайт-клон был «поднят» в результате поисковых запросов выше настоящего сайта завода.

В бизнесе нам также встречались подобные действия, правда, проведенные в еще менее изящной по исполнению форме. Сайт одного крупного дилера высококачественных красок был полностью скопирован. В тексты и изображения фальшивки не вносились никаких изменений, но ссылки с него в разделах «контакты» и «купить» вели прямо на сайт конкурента. Мы не знаем, было ли это неуклюжей попыткой конкурента при-

обрести новых клиентов, или же третья сила пыталась сравнить между собой две конкурирующие организации.

Рунет уже неоднократно сталкивался с такими способами выплескивания компромата в сетевое информационное пространство. Так, в 2003 году появился ныне уже не существующий, разумеется, сайт, который якобы принадлежал одной из ведущих правоохранительных структур некоего крупного государства СНГ. На нем было размещено изрядное количество грязи, направленной на работников этого ведомства. Это был первый в СНГ случай, когда «клонеры»[38] создали фальшивый сайт правоохранительной структуры. Контент этого сайта содержал стилизованные под официальные новости материалы, которые подводили читателя к выводу, что в атакуемой государственной структуре якобы царит беззаконие.

На первый взгляд кажется, что рядового гражданина все эти разборки на вершинах политики и бизнеса касаться не должны, но «попасть под раздачу» может практически любой. Это вполне реально, если организаторы и руководители «проекта» сочтут, что размещение чернухи на вас станет еще одним мазком в общей картине шельмования

соперников. Вы можете быть рядовым членом политической партии или работать обычным водителем в крупной корпорации. Для атаки на главную цель это подходит. Главное, что вы так или иначе имеете к этой цели отношение – и этого достаточно. В принципе, вы можете вообще не состоять в партии и не работать. Для тех, кто делает черный PR, это не имеет никакого значения. На сайте-клоне вполне может появиться разгромная статья, что вы как видный партийный чиновник уездного города Верхне-Ниженска исправно собираете дань с местных лоточников и отвозите деньги в областной центр, где вручаете их лично руководителю регионального отделения вашей партии. Или что вы, рядовой водитель компании, регулярно привозите в загородный дом генерального директора малолетних проституток.

Вы безработный? Это тоже подойдет, и даже будет лучше: нигде не работает – значит, имеет скрытые доходы. Какие? Да вот – наркотой президента «ЗаборКредитБанка» снабжает. Да-да, именно так. Банкир – наркоман со стажем, а вы ему свои деньги доверяете!

Примерно так вы можете попасть в зону обстрела на сайте-клоне. Главное для чер-

ных пиарщиков – попасть в главную мишень. А то, что при массовой атаке пострадают и другие, для них не имеет значения. В этом случае действуют два основных правила: «Лес рубят – щепки летят» и «Цель оправдывает средства». Так что никто не застрахован от того, что станет инструментом в руках непорядочных людей.

Увы, бороться с чернухой на сайтах-клонах практически невозможно – как правило, эти ресурсы создаются людьми, которые умеют заматывать следы. Физически такие сайты почти наверняка будут расположены на зарубежных серверах. Так, уже упомянутый лжесайт, атаковавший правоохранительную структуру одного из государств СНГ, размещался на хостинге Server Central в Чикаго, и представитель американской компании наотрез отказался предоставлять какую-либо информацию о владельцах ресурса. Открытые регистрационные данные владельца указывали на гражданина, проживающего в Москве, но его поиски оказались безрезультатными. Домен, где был зарегистрирован сайт-клон крупной политической партии, о котором мы говорили, кстати, тоже был зарегистрирован на москвича с незатейливым именем Иван Петров. Желающие мо-

гут поискать встречи.

В последнее время технически упростилось создание сайтов-клонов. С появлением программ-конструкторов сайтов, таких как Dreamwiewer, скопировать чужой сайт, заменить его содержимое на другое и «залить» это «изделие» на свой хостинг стало несложно. Соответственно, и риск стать жертвой подобных действий со стороны недоброжелателей многократно возрос.

Так что остается только надеяться на то, что ваше доброе имя не станет разменной монетой в грязной игре чьих-либо «высоких интересов». А если этим надеждам не суждено сбыться, то, как часто бывает, на помощь приходит принцип «клин клином вышибают». Убрать сайт-клон невозможно, но «закопать» его поглубже в недра Интернета вполне реально. Если при этом существует вероятность, что кто-то намеренно начнет искать его в поисковых машинах по ключевым словам в контексте негатива, то, возможно, потребуются провести дополнительные мероприятия. Например, придется уже самостоятельно выпустить псевдоклоны, содержащие слова негатива, скажем, в юмористическом контексте и поднять их в поисковых машинах так, чтобы они оказались в выдаче

выше клона, созданного противником, но при этом ниже нормальных ресурсов.

3. Сайты-подставы. Основные отличия сайтов-подстав от сайтов-клонов в том, что первые даже и не пытаются маскироваться под какие-либо прототипы и абсолютно не стесняются в средствах. Фото- и видеомонтаж самого грязного толка, порно, экстремистские и человеконенавистнические высказывания, приписываемые якобы жертве таких ресурсов, откровенно выдуманные «факты» биографии, подтасовка и передергивание – все идет в ход.

Поскольку такие сайты по определению не могут, да и не собираются клонировать оригинальные ресурсы «мишеней», [39] то чаще всего они имитируют домашние страницы тех или иных персон, против которых направлено воздействие. Логика создателей сайтов-подстав, в общем-то, понятна. С их точки зрения, посетитель такого сайта может купиться на то, что человек на своей домашней странице показывает себя с иной, неофициальной стороны, с не известного никому ракурса. Ну вот захотелось, предположим, известному в городе бизнесмену рассказать о своей тайной жизни и фривольных приключениях. Почему бы и нет? Интернет-

сообщество уже давно к таким вещам привыкло и не особо удивляется очередной веб-страничке, владелец которой рассказывает самые интимные, а подчас и самые гнусные подробности своей биографии. Да что говорить об Интернете, когда журнальные и газетные страницы пестрят откровениями vip-персон, а полки книжных магазинов плотно заставлены мемуарами и художественными произведениями на автобиографической основе с отнюдь не безобидными воспоминаниями о первой и чистой любви. Достаточно вспомнить скандальные опусы лидера НБП Эдуарда Лимонова. Так что некоторое доверие к таким псевдодомашним сайтам есть, и от этого никуда не деться.

В начале нынешнего 2007 года в Интернете появился сайт-подстава, который имитировал домашнюю страницу депутата Законодательного собрания одного из российских мегаполисов. По соображениям этичности мы не станем называть имя этого человека и адрес подставного ресурса. Иллюстраций тоже не будет, тем более этот ресурс уже давно заблокирован. Да и человек этот известен не только как региональный политик, но и как творческая личность. К чему лишний раз связывать его с той грязью, которая

на него вылилась?

Домашняя страница содержала изрядное количество порнографических видеоматериалов, где главным действующим лицом всех откровенных сцен был «человек, похожий на депутата Заксобрания». Еще до появления этого ресурса в Интернете квартира депутата была обворована. По слухам, которые активно муссировались в городе, среди украденного была и видеокассета с home video сексуального содержания. Возможно, эти слухи и побудили создателей сайта разместить порновидео в Сети, связав его с именем депутата, а возможно, появление сайта-подставы стало лишь завершающим этапом спланированного активного мероприятия – нельзя исключать того, что распространение слухов о краже кассеты и появление порочащего ресурса – звенья одной цепи.

Довольно показательной была и привязка атакуемого депутата к сайту и контенту – видеоролики снабдили текстовыми комментариями, где депутат рассуждал о политике, Родине и т. д. Для придания домашней странице хоть какой-либо достоверности на первой странице сайта создатели поместили официальное фото депутата и его биографию, написанную «от первого лица». В био-

графии хвастливо рассказывалось о его достижениях в политике и на творческом поприще.

Однако политики далеко не единственные, кто попадает под удар черных пиарщиков такого профиля. Объектом воздействия оказываются многие известные, а подчас и совсем не известные широкой общественности люди. Первые нередко становятся невольными жертвами шаловливых и праздных интернет-шатающихся, которые развлекают себя фотомонтажом пикантных картинок с популярными актерами, эстрадными звездами, героями светских тусовок. Такой способ развлечь себя и окружающих получил свое название – «отжабить» (от жаргонного термина «фотожаба»). В подавляющем большинстве случаев такой способ времяпрепровождения не ставит своей целью очернить того или иного человека. С точки зрения авторов, это просто баловство, шутка. Сомнительно, однако, чтобы результаты такого «баловства» сильно веселили тех, чьи лица монтируют в порнокартинки.

Совсем иная ситуация, когда подобные вещи начинают использовать из личной неприязни или желания мести. Тут уж чаще всего жертвами становятся отнюдь не герои

светских хроник. Под такую грязную волну может попасть абсолютно любой человек – девушка, отвергнувшая назойливого поклонника, руководитель небольшой фирмы, уволивший разгильдяя-сотрудника, даже школьный учитель, поставивший двойку в четверти обалдую, который худо-бедно умеет двигать мышкой и на элементарном уровне пользоваться парой функций того же «Фотошопа». Никто не застрахован от появления в Интернете примитивной странички со своим изображением в непристойном виде или от потока площадной брани в свой адрес.

Несколько успокаивает то, что авторы подобных «шедевров» в основной своей массе не очень умеют или не особо хотят продвигать такой ресурс: любое продвижение все же требует некоторых вложений – и финансовых, и временных, и трудовых. Как правило, им хватает того, что на каком-нибудь бесплатном хостинге, в глубинах домена третьего уровня, будет лежать страничка, которую можно с гордостью продемонстрировать друзьям и знакомым. А если и забредет на такой «сайт» человек посторонний, то скорее всего совершенно случайно. Это как правило. Но не будем забывать, что любые

правила имеют исключения и нельзя полностью игнорировать возможность стать жертвой наезда злобного и мстительного доморощенного черного пиарщика, который поставит своей целью выпить у вас как можно больше крови и максимально испортить вам жизнь.

Как с этим бороться? Собственно, эта книга целиком посвящена ответу на данный вопрос. Основное правило, которое нужно помнить и реализовывать, – задвигайте агрессора подальше и поднимайте свой ресурс как можно выше. В идеале на любой запрос в поисковой системе по ключевым словам, имеющим к вам непосредственное отношение, ищущий должен получить ссылки на ресурсы, которые демонстрируют вас с самых лучших сторон. Определяя ключевые слова, которые могут быть в запросах, учитывайте, что подавляющее большинство интернет-пользователей до сих пор пользуются поисковыми системами на уровне первоклассников (авторы просят прощения у продвинутых школьников младших классов) и для поиска человека попросту набирают в строке запроса его имя и фамилию – Василий Пупкин. Ну, в случае, описанном в начале этого раздела, запрос могут немного расши-

рить: «депутат Законодательного собрания Василий Пупкин». В огромном количестве выданных ссылок те, которые ведут на ваши противочернушные или имиджевые странички, обязаны занимать первые позиции.

Прочие возможности распространения черного PR

В данном разделе мы кратко рассмотрим некоторые возможности Интернета, которые могут быть использованы для распространения порочащей информации в сетевом информационном пространстве. Краткость обзора обусловлена тем, что приведенный здесь инструментарий не так мощно воздействует на интернет-аудиторию, как, к примеру, сайты, блоги или форумы. А некоторые из рассматриваемых методов требуют значительных временных и финансовых затрат. К тому же такие действия, как массовая рассылка электронных писем с информацией, которая не запрашивалась адресатом (спам), в ряде стран уже законодательно признана незаконной, и спамер вполне может понести административное и даже уголовное наказание.

Таким образом, авторы рассматривают приведенные в данном разделе инструменты как вспомогательные орудия. Они, скорее, могут быть использованы при распро-

странении негатива в Интернете для поддержки базовых ресурсов с компрометирующими сведениями. Их применяют обычно для разовых акций информирования интернет-общественности о появлении в Сети тех или иных материалов.

К этим средствам относятся следующие:

- гостевые книги;
- чаты;
- комментарии;
- e-mail-рассылки;
- баннерная реклама.

Гостевые книги – одна из самых главных возможностей, которые предоставляет Интернет своим пользователям, – возможность общаться, высказывать свою точку зрения на любые проблемы, оставлять отзывы, комментировать события, а также опубликованные в Сети и традиционных СМИ материалы. Для этой цели существует довольно большое количество сетевых инструментов, среди которых мы, пожалуй, выделим форумы, гостевые книги, чаты и комментарии. Поскольку форумы оцениваются авторами как достаточно серьезные средства формирования общественного мнения в Интернете и площадки для эффективного продвижения информации (в том числе и порочащего

свойства), им посвящен отдельный раздел книги, где они рассматриваются более подробно и тщательно.

Гостевые книги являются частью какого-либо сайта и предназначены для отзывов от посетителей, сбора их мнений и оценок данного ресурса и его контента. В основном гостевые книги – форма для обратной связи, которую посетитель сайта может заполнить и отправить его владельцам. Как правило, они модерируются, а многие из них для размещения информации на своих страницах требуют регистрации и авторизации. К тому же нередко в соответствии с правилами, установленными хозяевами сайта, в гостевых книгах запрещено распространение информации негативного свойства, размещение открытой рекламы и ссылок на другие ресурсы, если на то нет объективных причин. Модератор, т. е. тот, кто следит за выполнением этих правил, может удалить сообщение из гостевой книги уже после его появления (постмодерация) или вообще не допустить размещение информации, если используется премодерация, т. е. предварительный просмотр и разрешение или запрет на опубликование. На практике чаще всего используется постмодерация, когда ответ-

ственный за содержимое гостевой книги время от времени просматривает уже размещенный материал и решает – оставлять его или нет. Поскольку правила общения через гостевые книги определяются владельцем ресурса, то и решение «быть или не быть» чаще всего весьма субъективно: нравится – оставляем, не нравится – стираем. Апеллировать к хозяину сайта с просьбами разместить или не удалять информацию – дело практически бесполезное. Сайт – его собственность, и допускать или не допускать кого-либо на свою территорию – дело сугубо частное.

Многие гостевые книги снабжаются программными фильтрами, которые по заложенному в них списку проверяют сообщения на наличие нецензурных и оскорбительных слов и выражений. Сообщение, в котором робот найдет непарламентскую лексику, автоматически отправится в мусорную корзину.

Разумеется, инициатор информационного нападения может попытаться использовать гостевые книги тех сайтов, которые, по его мнению, пользуются интересом у целевой аудитории. Под целевой аудиторией в этом случае он понимает потребителей негатив-

ной информации на конкретное лицо или организацию. Однако от агрессора потребуются тончайшее мастерство балансирования, которое позволит придать негативной информации достаточно невинный для модератора вид и в то же время заинтересовать читателей гостевой книги его месседжем. [40]

Конечно, самородков в нашем отечестве немало (в том числе и среди тех, кто использует черный PR для своих неблагоприятных целей), но, скорее всего, для такой ювелирной работы придется обращаться к профессионалам, а это уже расходы, причем весьма существенные.

Чаты. Обладают еще меньшими возможностями для вброса негатива. Эти ограничения обусловлены самим принципом работы подобного инструмента интернет-общения. Да, в чате любой человек в любой момент может присоединиться к беседе без какой-либо регистрации или авторизации. Да, чат позволяет писать все, что заблагорассудится, – хоть нецензурщину, хоть призывы к свержению конституционного строя Зимбабве, хоть требования предоставить гражданство всем пингвинам без исключения. Казалось бы – идеальный инструмент для рас-

пространения самого оголтелого черного PR в чей угодно адрес, если бы не одно «но». Общение в чате происходит в режиме реального времени, а содержание *существует* только «здесь и сейчас», поскольку чаты построены по принципу информационного потока. Сообщение вливается в общую массу и вскоре бесследно растворяется, становясь полностью недоступным для любого посетителя, зашедшего немного позже. Да и аудитория чатов не совсем подходит для серьезных информационных акций. Точнее – совсем не подходит. В основном чаты – это место для молодежных тусовок.

Комментарии. Более серьезный инструмент, используя который, можно если не донести до интернет-аудитории весь компромат на объект атаки, то по меньшей мере возбудить интерес и стимулировать пользователей к посещению ресурса, где находится порочащая информация.

Большинство сетевых средств массовой информации и электронных информационных агентств позволяют читателям оставлять комментарии и отзывы на свои публикации. Поскольку серьезные интернет-СМИ активно анонсируют свои материалы на популярных ресурсах, то аудитория их читате-

лей довольно внушительна. И, что совсем немаловажно, эта аудитория является целевой, т. е. объединенной интересом именно к той теме или проблеме, которая затрагивается в статье, заметке, новости или ином информационном сообщении. Внимательно отслеживая анонсы материалов крупных сетевых информационных ресурсов, распространитель негативной информации вполне способен вычленить наиболее интересные для него публикации, которые будет читать нужная ему категория посетителей. Комментируя подходящую по тематике статью, агрессору не составит труда заложить в свой отзыв небольшое сообщение, побуждающее пользователей посетить его интернет-ресурс. Причем ему даже не придется особенно маскироваться. К примеру, будет вполне достаточно, якобы заинтересованно обсуждая статью о коррупции в правительстве, подать реплику вроде: «Да что там правительство?! Вон у нас в Верхне-Ниженске начальник милиции каждый месяц в открытую у торгашей мзду берет и ничего не боится! А что ему будет, когда его тесть у губернатора работает! И говорят об этом, и пишут, а все без толку!». Ну и, разумеется, не забыть дать ссылку на сайт, где говорят и пишут о нечи-

стом на руку служителя закона. Можно быть уверенным, что по этой ссылке на сайт с чернухой придет немалое количество посетителей.

E-mail-рассылки. Как уже говорилось, за массовые рассылки электронных писем во многих странах можно понести вполне ощутимую ответственность, вплоть до уголовной. Законодательство нашей страны наказания за спам пока не предусматривает, но будем надеяться, что только пока. Несмотря на то что это явление еще не получило заслуженной юридической оценки, спам пользуется в России дурной славой и осуждается большинством членов интернет-сообщества. Разумеется, за исключением тех, кто таким неблаговидным способом зарабатывает деньги. Спам отлавливается специальными фильтрами, которые любой пользователь может установить в своем «Почтовом клиенте», [41] настроив их под свои потребности. Провайдеры, корпоративные серверы и серверы почтовых служб тоже вносят свою лепту в фильтрацию почтового мусора, вылавливая такие письма по ключевым словам и почтовым адресам, занесенным в черные списки. Но спамеры не сидят сложа руки и придумывают новые способы и возможно-

сти обхода спам-фильтров. Надо отдать должное – в изобретательности им не откажешь. Как говорится, эту бы энергию да в мирных целях. И все же ни один здравомыслящий человек не станет даже открывать такое электронное письмо, даже если оно прорвется в его почтовый ящик, не говоря уж о том, чтобы пройти по указанной в нем ссылке. Так что тому, кто организывает волну черного PR через массовую рассылку электронных писем, нужно очень постараться, чтобы вызвать у получателя интерес. Есть и еще один нюанс, который делает такой вид распространения информации далеко не самым эффективным – адресные базы, по которым спамеры проводят рассылки. Одно дело, когда черный PR направлен против крупной структуры федерального уровня, политической партии накануне парламентских выборов, например, информация о которой может заинтересовать практически каждого взрослого гражданина страны. Тогда у спамера есть резон организовывать массовое забрасывание электронных почтовых ящиков информацией, в расчете на то, что попадание в целевую аудиторию будет более-менее плотным. Другое дело – узконаправленная атака против бизнеса или

политика масштабом помельче. Нет никакого смысла тратить деньги на рассылку сотен тысяч, а то и миллионов электронных писем, надеясь, что их получит та ничтожно малая доля процента адресатов, до которых и нужно довести негативную информацию. А за каждый адрес виртуального почтового ящика, на который отправляется электронное письмо, спамеры берут с клиента вполне реальные деньги, предпочитая конвертируемую валюту. Так что соотношение «цена – качество» будет явно не в пользу последнего. Вариант с использованием целевой адресной базы мы даже не рассматриваем, поскольку ее создание под задачу распространения локального черного PR – нечто из области ненаучной фантастики.

Баннерная реклама – еще один инструмент, который, как мы считаем, необходимо рассмотреть. В отечественной практике черного PR такой способ привлечения внимания интернет-пользователей к ресурсам с компрометирующей информацией использовался и используется. Достаточно вспомнить продвижение сайта-клона крупной политической партии, о котором мы уже говорили. Одновременно с его появлением в Интернете на различных сетевых ресурсах

(в основном на сайтах с достаточно фривольным контентом) были размещены баннеры с изображением полураздетой звезды отечественной эстрады и зазывающим текстом. Баннеры, как вы понимаете, вели на тот самый сайт-клон, где в изобилии была представлена чернуха на партию-мишень.

Довольно сложно дать позитивную оценку такому «маркетинговому ходу» промоутеров сайта-клона. Едва ли интернет-пользователи испытали дикий восторг, кликнув по баннеру (явно в надежде насладиться прелестями поп-дивы) и угодив на сайт, где анонимные авторы поливают помоями своих политических недругов. С помощью такой рекламы на сайт пришла явно не целевая аудитория.

Опять же, не стоит забывать, что разработка, создание, размещение и демонстрация баннеров в Интернете стоит денег и требует привлечения профессионалов, так что если против вас организована атака с применением этого средства, то стоит задуматься – кто и ради чего так усердствует? Едва ли список ваших врагов, готовых на столь масштабированное, затратное и скоординированное нападение, окажется слишком велик.

Подробно об основных инструментах, применяемых для противодействия черному PR в Интернете. Блоги и сайты

Арсенал инструментов велик, и каждый из них имеет свои особенности. Мы кратко их перечислим, а затем поговорим о них подробнее – об одних совсем немного, о других, наоборот, много и подробно.

Мы решили говорить о блогах и сайтах в одном разделе, потому что блогам принадлежит ведущая роль в организации противодействия информационному нападению в современном Интернете. Это связано прежде всего с тем, что их очень просто создавать и ими очень легко управлять. Поскольку блоги – это следующий шаг эволюции сайтов, они сохранили в себе многие их плюсы, но при этом они лишены их существенных недостатков. Основные варианты использования сайтов в информационной войне мы

рассмотрели ранее, тогда как разговор о блогах, наоборот, перенесли «на потом». Считаем, что это «потом» как раз и наступило.

Блог – это фактически небольшой интернет-сайт, с очень простой системой управления и возможностью обратной связи с читателями. Управление блогом настолько просто, что каждый, кто умеет работать в текстовом редакторе Word и выходить в Интернет, может стать блоггером без дополнительного обучения.

Именно простота размещения материалов на блогах и интерактивность сделали их таким распространенным явлением. Причем на них могут быть размещены не только тексты, но и фотографии, а также видео- и аудиофайлы. Это позволяет при желании превратить блог в он-лайновую газету или радиостанцию.

Возможность делать записи видимыми лишь ограниченному числу людей либо вообще только хозяину блога дает возможность использовать его не только для личных целей, но и для работы. Например, транслировать корпоративные новости в подразделениях компании, разбросанных по всей стране, или координировать работу филиалов, находящихся в разных странах.

Обычные люди с помощью блогов могут общаться с друзьями, рассказывать о событиях в своей жизни, слушать музыку, смотреть видео.

Блоги стали общедоступны с 1996 года. Сегодня вести блог стало модно, уже насчитывается более миллиона блоггеров (а значит, под них создана соответствующая инфраструктура и среди них при необходимости легко спрятаться, «затеряться в толпе»).

Завести себе блог может каждый, поскольку сделать это очень легко и это не налагает никаких обязательств. Блог, как правило, ничего не стоит и вести его никто не обязывает. Его можно открыть и ничего в него не писать или писать нерегулярно. При необходимости блог можно забросить на несколько лет, а потом к нему вернуться – он будет ждать возвращения своего хозяина. Оставляя блог надолго, можно его содержимое закрыть под замок, а можно и оставить в открытом доступе.

Новые сообщения в свой сетевой журнал пишут, непосредственно входя в него или отправляя эти сообщения по электронной почте или с мобильного телефона.

В конце концов, если надоест вести блог, можно его просто ликвидировать.

Блоги были задуманы и реализованы как инструмент, позволяющий людям без посредников в виде редакторов или веб-мастеров доводить свою точку зрения, свои мысли и пожелания до других людей. Редакторские функции в этом случае перекладываются на плечи авторов,[42] которые справляются с ними в меру своих сил, умения и желания.

Устройство блогов

На наш взгляд, для понимания социальных сетей, блогов и другого интернет-контента (информационного наполнения), формируемого самими людьми без посредников, логично обратиться к мнению членов интернет-сообщества, в частности к Википедии. В англоязычной Википедии (Wikipedia) в отношении блогов написано следующее.

Блог – это веб-сайт, содержимое которого наполняется самим пользователем. Блог выполнен в стиле журнала и располагает сообщения в обратном хронологическом порядке. Блог позволяет выпускать комментарии или новости по любым вопросам, таким как кулинария, политика или местные новости. Иногда блоги выполняют функции личных дневников. Типичный блог сочетает в себе

текст, изображения, гиперссылки на другие блоги, веб-страницы и другие ресурсы, имеющие отношение к теме блога. Важная часть большинства современных блогов – возможность читателям оставлять комментарии в интерактивном формате. Большинство блогов текстовые, хотя некоторые сосредоточиваются на фотографиях (фотоблоги), рисунках (скетчблоги), видеоматериалах (влоги) или аудиоматериалах (подкасты). Существуют и социальные сети, охватывающие одновременно широкий спектр интересов. Блоги могут быть частью таких сетей.[43]

Сегодня блоги настолько развиты, что даже неподготовленный человек может быстро научиться и без затруднений вести собственный блог. В который раз уже повторяется ситуация, характерная для всех новинок Интернета: новые сервисы сначала доступны только специалистам, но затем пользование ими упрощается, и в конце концов с ними без проблем справляется любой человек. Достаточно вспомнить, например, как развивалась электронная почта: сначала только программисты владели таинством составления и отправки писем, а теперь это доступно всем. Правда, скорость адаптации новых сервисов к их использованию непод-

готовленными людьми значительно возросла.

Мы расскажем, как завести блог, на примере двух самых больших на момент написания книги площадок – Живого Журнала и LiveInternet.

Место блогов в Интернете

Блоги во многом похожи на традиционные интернет-сайты. Они тоже расположены в Интернете, имеют странички с адресами и позволяют размещать информацию, доступную пользователям. Однако отличия блогов от интернет-сайтов столь принципиальны, что заставили говорить о появлении новой технологии. Главное отличие состоит в том, что интернет-сайты предоставляют для ознакомления информацию, размещенную их владельцами, и обычно не предполагают оперативной обратной связи. (Мы говорим об информационных сайтах, а не о таких, как интернет-магазины, где интерактивность присутствует, но направлена на уточнение заказа и совершение покупки, а не на многосторонний обмен мнениями.) Конечно, элементы двустороннего общения присутствуют и на традиционных сайтах, но

это, как правило, одностороннее или двустороннее общение.

Так, на большинстве традиционных сайтов есть электронная почта, с помощью которой можно общаться с владельцем или редактором сайта, но это общение скрыто от посторонних глаз.

Кроме того, на некоторых традиционных сайтах есть гостевая книга, о которой мы уже говорили. Каждый желающий может оставить в ней сообщение или задать вопрос. Но и через нее общение внешне выглядит либо как одностороннее (когда вопрос виден всем, но ответ в публичном доступе не размещается), либо, даже при наличии ответа, это общение исключительно между двумя людьми (ведь даже если у других есть возможность наблюдать за обсуждением, они не могут в него вмешиваться).

Процедура размещения контента на сайте и в блоге тоже отличается. Для того чтобы разместить материал на сайте, требуется зайти в соответствующий раздел и воспользоваться формой для размещения статей либо вообще создать страничку на своем компьютере и затем записать ее на сервер, предоставляющий место для сайта в Интернете (такое предоставление места называют

хостингом). Подобные действия требуют некоторой подготовки.

Создание блога предельно упрощено. Форма для создания сообщения является стандартной. Доступ к ней по силам освоить любому человеку, который в принципе смог выйти в Интернет. Правда, никакой автоматической рубрикации на блоге не предусмотрено, и все статьи по умолчанию будут располагаться друг за другом в порядке их появления.

Сделаем небольшое отступление и поговорим о явлении, которое способствует стремительному развитию блогов и одновременно обеспечивает почти мгновенный доступ к новой информации, появляющейся в них. Это RSS-потoki.

Если говорить упрощенно, то RSS-поток – это специальный инструмент, который позволяет подписчикам отслеживать те новинки и изменения, которые владелец сайта или блога согласен показать неопределенному числу лиц.

Википедия говорит, что RSS-потoki предназначены «для описания лент новостей, анонсов статей, изменений в блогах и тому подобного. Информация из различных источников, представленная в формате RSS,

может быть собрана, обработана и представлена пользователю в удобном для него виде специальными программами-агрегаторами».[44] Благодаря RSS-потокам любое изменение в блоге становится видно подписчикам в считанные минуты. Кроме того, RSS-потоки блогов, как правило, транслируются в службу «Блоги Яндекса», где информация в течение часа с момента публикации становится доступна пользователям.

Программы, позволяющие читать RSS-потоки с разных сайтов или блогов в одном месте, называются RSS-агрегаторами. Благодаря им пользователю нет необходимости посещать различные сайты. Это позволяет сэкономить время, необходимое для оперативного отслеживания изменений в блогах. Подробнее о конкретных RSS-агрегаторах мы поговорим ниже.

Для того чтобы пользоваться любым оружием, надо знать во всех подробностях его устройство. Чтобы с помощью блога противодействовать черной PR-атаке с наилучшим результатом, следует научиться использовать все возможности, которые он предлагает. Давайте подробно рассмотрим процесс создание блога, не упуская из виду даже те детали, которые часто остаются «за

кадром» даже у опытных пользователей.

Создание блога в Живом Журнале

Живой Журнал на момент написания нашей книги является самым крупным ресурсом для ведения русскоязычных блогов.

Надо сказать, что, с одной стороны, инструкции по управлению блогом, содержащиеся в разделе «Помощь» и «FAQ» (частые вопросы) Живого Журнала, очень велики по объему. С другой, для того чтобы завести блог и начать им пользоваться, надо сделать не так уж много действий, и сами эти действия достаточно просты. Интерфейс блогов настолько понятен, что повседневная работа с ним обычно не вызывает затруднений у пользователей. Поэтому мы расскажем об основных действиях, которые надо выполнить, создавая блог. А если потребуется дополнительная информация о каких-то новых возможностях блогов, вы сможете найти ее в самом Живом Журнале.

Прежде чем начать регистрировать блог, надо позаботиться о том, чтобы обзавестись адресом электронной почты. Дело в том, что при регистрации блога указать e-mail необ-

ходимо, причем это должен быть реально работающий почтовый ящик. На адрес, указанный при регистрации, придет письмо с подтверждением регистрации блога, на которое надо ответить. До того, как почтовый адрес будет подтвержден, пользователь не имеет права писать комментарии к другим блогам. Почтовый ящик может быть любым, главное, чтобы он был уникальным для Живого Журнала, т. е. чтобы по нему ранее не проводилась регистрация на этом сайте (регистрация этого адреса на любых других сайтах значения не имеет). Требования к уникальности электронного адреса предъявляются потому, что по нему высылается пароль в случае, когда пользователь его забывает.

Проще всего открыть почтовый ящик на любом бесплатном почтовом сервисе (например, на Яндексе, Рамблере, Гугле, Mail.ru или любом другом). Чтобы не запоминать различные пароли и адреса своих почтовых ящиков, рекомендуем сразу после того, как почтовый ящик создан, сделать в нем переадресацию всех входящих писем на ваш постоянный адрес электронной почты. При таком подходе вы сможете иметь неограниченно большое количество почтовых ящиков, непосредственно работая только с од-

ним из них.

Мы настоятельно рекомендуем при открытии почтовых ящиков пользоваться анонимайзерами. Каждый раз, когда вы входите на сайт, предоставляющий сервис электронной почты, ваш IP-адрес фиксируется. В условиях информационной войны желательно не оставлять противнику даже гипотетической возможности идентифицировать конкретного исполнителя, помогающего вашей стороне в Интернете. Не все анонимайзеры способны работать с любым сервисом электронной почты. Будет ли работать ваш конкретный анонимайзер с тем сервисом, который вы избрали, станет ясно при попытке зарегистрировать почтовый ящик. Если даже Яндекс или Mail.ru не станут работать с вашим анонимайзером, это не очень большая проблема: в Интернете по запросам «бесплатная почта Украина», «бесплатная почта Латвия» и им подобным есть множество русскоязычных бесплатных почтовых сервисов. А по запросу в Гугле «free mail» их просто огромное количество по всему миру, так что вы всегда найдете приемлемый вариант.

После того как адрес электронной почты получен, можно приступить непосредствен-

но к открытию блога.

Для этого надо отправиться на главную страницу Живого Журнала по адресу: www.livejournal.com (рис. 7).



Рис. 7. Главная страница Живого Журнала.

На этой странице немало разного рода информации о Живом Журнале, но для нас сейчас главное, что сразу в нескольких местах страницы есть кнопки или гиперссылки «Создать аккаунт» (либо «Создать журнал»). Они-то нам и нужны. Выбирайте любую и нажимайте.

На открывшейся после этого странице (рис. 8) надо заполнить информационные поля.

Рис. 8. Страница создания нового аккаунта в Живом Журнале.

Имя пользователя. Выберите себе любое имя (ник). В Живом Журнале ник может состоять только из латинских букв, цифр и

знака нижнего подчеркивания. Он может быть, например, таким: `ivan_petrov`, `ivanpetrov`, `iv_an_petrov`, `ivanpetrovvv`, `ivanpetrov85` и т. п.

Поскольку в Живом Журнале очень много пользователей, простые и короткие ники, скорее всего, зарегистрировать не удастся.

Адрес e-mail. Как мы уже говорили, в это поле должен быть введен реальный адрес электронной почты. На него автоматически будет отправлено письмо, содержащее гиперссылку для подтверждения подлинности электронного адреса. Вам надо просто перейти по гиперссылке в полученном письме, чтобы адрес электронной почты был подтвержден. Все сообщения, которые имеют отношение к Живому Журналу, станут приходить на этот адрес. По умолчанию к ним относится информация о том, что в вашем блоге сделан комментарий или что кто-то добавил вас в список своих друзей.

Пароль. Введите пароль (и запомните его). Лучше, чтобы он был не короче шести знаков и содержал, помимо букв, еще цифры и/или не алфавитно-цифровые символы (например, знаки @, !, ? \$). Чтобы было проще создавать и запоминать пароли, устойчивые к взлому, попробуйте, например, заменить

букву «а» на символ «@», букву «о» на цифру «0», букву «с» на символ «\$», букву «ч» на цифру «4» и т. д. Тогда, например, слово «Спичка» приобретет вид «\$пи4к@». Такой пароль довольно сложно подобрать. А чтобы не переключаться из регистра в регистр, его можно просто копировать из файла, где он хранится, и вставлять в поле для пароля. Только не храните его в текстовом файле на рабочем столе, потому что есть троянские программы, которые специализируются на краже именно таких файлов с рабочего стола с целью похищения пароля. Лучше всего скопировать его на сменный носитель или пользоваться программой – менеджером паролей.

Подтвердите пароль. Просто подтвердите пароль, набрав его еще раз, – это защитит вас от опечаток.

День рождения. В принципе вы можете ввести здесь любую дату (но при вводе ненастоящей даты рождения не забывайте, что вам должно быть больше 13 лет). Живой Журнал не требует называть ваш настоящий день рождения. В комментарии к этому пункту указано, что он введен по требованию американского законодательства (Живой Журнал принадлежит частной компа-

нии из США). Однако там же говорится, что неверное указание даты может затруднить вам пользование блогом. При его регистрации вы сможете полностью или частично скрыть введенный день рождения от посторонних глаз, так что решайте сами, как вам поступать в данном случае.

Подтвердите, что вы человек. Этот пункт – стандартная защита от автоматических регистраций, которые проводят спамеры с помощью специальных роботов. Для того чтобы «подтвердить, что вы человек», достаточно ввести буквенно-цифровой код, написанный рядом со строкой, в которую его вводят. Иногда не получается ввести его с первого раза, так как для защиты от автоматического сканирования он снабжен таким количеством «помех» и искажений, что даже человек не всегда понимает его с первого раза. Ничего страшного в ошибке при вводе этого кода нет. Если данный код не удастся ввести с первого раза, в следующий раз будет выдан уже другой, как правило, более читаемый. Если потребуется, он будет изменен и в третий раз, хотя в этом практически никогда не возникает необходимости.

Новости сайта. По умолчанию напротив этого поля стоит галочка с текстом «Да, изве-

щайте меня о новостях Живого Журнала». Если у вас нет желания получать подобные новости, вы можете просто снять галочку, и новости к вам приходить не будут.

Официальные данные. Здесь галочку наоборот надо поставить – напротив текста «Я прочитал(а) условия использования и положение о конфиденциальности и выражаю согласие».

После заполнения этих полей вы подтвердите, нажав кнопку внизу, что готовы продолжать работу с Живым Журналом и попадете на страницу, которая позволяет выбрать тарифный план. Она называется «Настройте свой аккаунт» (рис. 9). Тарифных планов на момент написания книги было три, два из них – бесплатные.

На вновь открывшейся странице вы увидите таблицу, в которой перечислены все три типа тарифных планов. Особенности каждого из них видны очень хорошо.

Если говорить кратко, то отличаются эти планы друг от друга возможностями, предоставляемыми пользователю, и тем, что от пользователя требуют взамен. Каждый следующий тарифный план позволяет загружать большее количество файлов, фотографий, а также аватаров (небольших картинок

пользователя, которые позволяют ему сделать свой блог и свои сообщения более оригинальными и вместе с тем выразить свое настроение и мысли).

LIVEJOURNAL

LiveJournal Secure Site

Настройте свой аккаунт

Get your own journal, a full suite of privacy controls, and the ability to create an unlimited number of communities.

Choose Account Level *

	Basic (Free)	Plus* (Free)	Paid (Paid)
Pricing	Бесплатно	Бесплатно	От \$2/мес. **
Display Userpics on Posts and Comments	6	15	30
Numerous Pre-made Designs for Your Journal	100	300	600+
Get Notified of New Posts, Friends, Comments, etc.	25	200	1000
Post Photos & Text via Your Mobile Device	•	•	•
Get Free Text Message Notifications		3/mo	10/mo
Create and Post Polls and Surveys	•	•	•
Add Voice Posts (Audio Posts) to Your Journal		5/mo	20/mo
Create Custom Mood Themes to Express a Mood	•	•	•
Store and Manage Your Photos		1GB	2GB
Point Your Personal URL to Your Journal (Domain Forwarding)	•	•	•
Use the Advanced Search Options			•
Earn Extra Userpics with Our Loyalty Program			•
Receive an @LiveJournal.com E-mail Address			•
Access the "Express Lane" for faster service during high traffic			•
Advertising Free			•

[View full comparison chart](#)

* Plus Journals have advertisements
 ** These prices are only available for paid accounts with automatic payments.

[Ознакомьтесь](#) | [Условия обслуживания](#) | [Положение о конфиденциальности](#) | [Реклама](#) | [Настройки просмотра](#) | [Начать бесплатный журнал/блог](#)

Рис. 9. Выбор тарифного плана в Живом Журнале.

Первый тариф – «Базовый» – относительно беден по своим возможностям, хотя достаточно функционален.

Второй – «Плюс» – дает по-настоящему хорошие возможности работы с блогом, но при этом содержит рекламные баннеры. Собственно говоря, именно рекламодатели и

позволяют пользователям бесплатно приобретаться к тарифу, предлагающему много возможностей.

Третий – «Платный» – позволяет дополнительно получить некоторые дополнительные услуги:

- дополнительное место для хранения фотопальбомов (всего 2 Гбайта);
- адрес электронной почты в Живом Журнале вида name@live-journal.com;
- скоростной канал доступа в Живой Журнал в моменты большой нагрузки на сервер;
- отсутствие рекламы.

Стоимость платного тарифа на момент написания книги была порядка двух долларов США в месяц (дополнительные деньги взымались, если, к примеру, пользователь хотел увеличить объем дискового пространства для хранения файлов до 10 Гбайт). Платеж проводился дистанционно, например, с помощью кредитной карты. При платеже сразу за год предоставлялась скидка, и его стоимость составляла порядка 20 долларов США.

На наш взгляд, для дебюта в блоггинге и для целей отражения информационного нападения в Интернете подходит тариф «Плюс». Тем, кто по каким-либо причинам не приемлет рекламные баннеры в Интерне-

те, но вообще не хочет тратить денег на блог (или не может себе позволить раскрывать свое инкогнито, совершая именные электронные платежи), можно рекомендовать тариф «Базовый».

После того, как тариф выбран, Живой Журнал перемещает нового пользователя на страницу «Изменить профиль – найти друзей и сообщества», которая предлагает пользователю заполнить информацию о себе (рис. 10).

Рекомендуем внимательно отнестись к этой странице, поскольку она играет в дальнейшем продвижении блога довольно большую роль. В самом Живом Журнале говорится об этой странице так: «Ваш профиль позволит остальным узнать, кто вы и о чем ваш журнал. Это просто базовая информация, чтобы было с чего начать. Все поля абсолютно необязательны, но чем больше, тем веселее». Мы хотели бы дополнить эту мысль, имея в виду дальнейшее продвижение блога в Интернете, а значит и продвижение вашей точки зрения к целевой аудитории в информационной войне.

Страница, о которой сейчас идет речь, впоследствии будет называться вашим профилем в блоге и получит уникальный адрес

в Интернете. По сути, она является еще одним сообщением в блоге, которое доступно читателям и поисковым машинам.

Рассмотрим, какие разделы предлагается здесь заполнить и для чего они нужны.

Необходимость указать имя, пол и день рождения вряд ли вызовут какие-либо вопросы. Тем более что они уже введены ранее и подставляются здесь автоматически. Правда, вместо имени по умолчанию фигурирует ваш ник, но вы вправе, если сочтете нужным, заменить его на настоящее или любое другое имя.

В информационных войнах встречаются оба варианта, хотя чаще выбор делается в пользу работы под псевдонимом. Более частый выбор псевдонима, а не настоящего имени, диктуется тем, что, во-первых, предотвращает попытки причинения вреда тому, кто оказывает сопротивление черному PR, а во-вторых, противнику приходится ломать голову над тем, кто это вообще может быть. Ведь его очень страшит вполне реальная ситуация, когда третья сила перед выходом на рынок играет на противоречиях двух уже имеющих на рынке участников, стравливая их между собой, компрометируя и ослабляя. Иногда встречается и третий вари-

ант выбора имени в блоге – когда с целью провокации указывается идентификатор, компрометирующий кого-то из стана противника. Например, чтобы внести раскол в ряды врагов.

Рис. 10. Страница «Изменить профиль – найти друзей и сообщества» в Живом Журнале.

Далее идет строка, с помощью которой можно выбрать, как показывать дату рождения – полностью (число, месяц, год), либо только число и месяц (все будут знать, когда у вас день рождения, но не будут знать, сколько вам лет), либо только год. Есть еще

один вариант – вообще ее не показывать.

Затем следует большое поле «О себе». Оно позволяет разместить любую информацию, причем с гиперссылками (которые размещаются только с помощью тегов HTML, так как визуальный редактор в этом разделе на момент написания книги не работал). Обычно пользователи могут указать здесь свои любимые интернет-ресурсы и сделать переход к ним прямо с этой страницы. В информационной войне эти гиперссылки позволяют дополнительно продвинуть свою точку зрения, предоставив людям возможность перейти на рекомендуемый вами ресурс. Кроме того, эти гиперссылки дополнительно обеспечивают ссылки на ваши другие сайты и блоги, поднимая их рейтинг у поисковых машин. Вы можете здесь же разместить любые картинки или фотографии, назначив им с помощью тегов HTML имена. Правильно выбранное имя такой картинки также делает ваш блог более тематическим с точки зрения поисковых роботов (об этом мы поговорим подробно несколько позже).

И последний раздел на этой странице – «Интересы». Каждый интерес может быть представлен как одним словом, так и словосочетанием (но в словосочетании не может

быть более четырех слов). Интересы отделяются друг от друга запятыми. После того как вы закончите заполнять этот раздел и (обязательно!) сохраните внесенные изменения, то в режиме просмотра вашего профиля увидите, что те интересы, которые разделяет кто-либо еще в Живом Журнале, стали гиперссылками. Пройдя по такой гиперссылке, вы окажетесь на странице, где представлены остальные пользователи, которые имеют такой же интерес. Уникальные интересы останутся просто текстом. Присмотритесь к словам этого текста: не исключено, что они просто набраны с ошибками либо их можно сформулировать иначе. Например, если вас интересует PR, то слова «пиар» и «PR» приведут вас на разные страницы, к разным группам единомышленников. Если вы введете в это поле в качестве интересов имя или название того, кто организовал на вас информационное нападение, либо название его продукции и какие-то другие связанные с ним слова, то сможете дополнительно продвинуть свой ресурс по этим словам, а значит, получите преимущество в информационном противостоянии.

После сохранения результатов вы будете перемещены на следующую страницу, где

вам предложат внести изменения в профиль, а также найти «земляков по региону» либо людей, имеющих интересы, схожие с вашими. Здесь же объясняется, как включить этих людей в список друзей (рис. 11).

Друзья (френды, friends) в контексте Живого Журнала – это люди, с которыми ваш блог будет иметь взаимные гиперссылки и все новые сообщения с блогов которых вы сможете читать в одной ленте (ее называют френдлентой). Френдлента похожа на Ленту Яндекса и аккумулирует все новые сообщения, появившиеся в блогах людей, внесенных вами в список ваших друзей. О том, как работать с Лентой друзей, достаточно подробно и написано в самом Живом Журнале. Кстати, там же есть большой список часто задаваемых вопросов и подробные ответы на них.

Надо ли записывать в друзья дружественные вам в информационной войне ресурсы – вопрос непростой. С одной стороны, записав дружественные вам ресурсы в друзья, вы повышаете их рейтинг в поисковых машинах (правда, довольно незначительно), а с другой – облегчаете противнику выявление ваших союзников и, возможно, ставите их под удар. Поэтому подойдите к этому вопро-

су взвешенно. Может быть, вы придете к выводу, что открыто вносить в друзья на блоге своих реальных союзников не всегда нужно. Вместе с тем при отражении информационного нападения часто бывает необходима именно демонстративность, так как она позволяет привлечь больше внимания общественности и повышает вероятность вмешательства прессы. Решение о том, каково должно быть соотношение демонстративности и анонимности, надо принимать исходя из ваших задач и общей обстановки. Универсального рецепта в данном случае нет.

Рекомендуем затем пройти вперед в регистрации блога. Вы попадете на страницу, на которой в принципе уже можно начать писать сообщения в свой блог (рис. 12).



Рис. 11. Страница поиска друзей и сообществ в Живом Журнале.

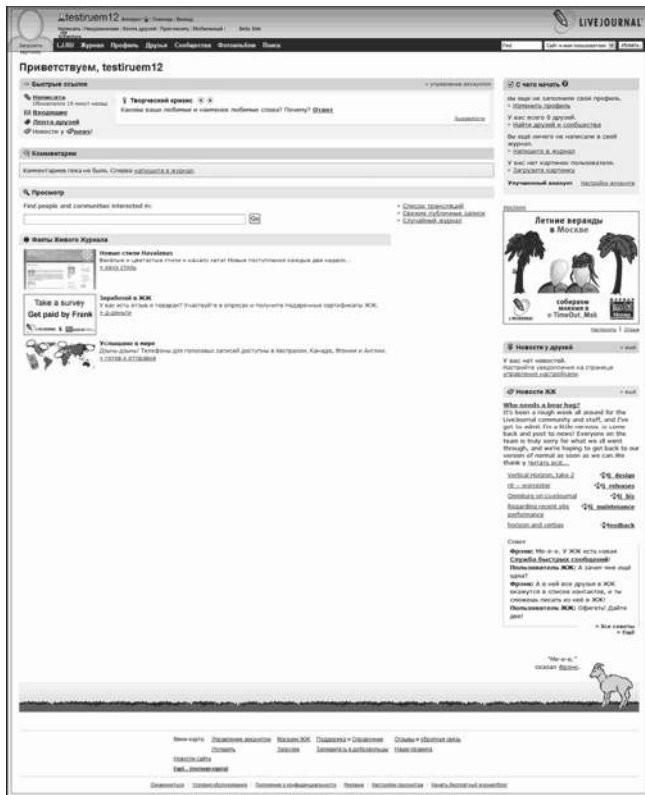


Рис. 12. Страница Живого Журнала, на которой уже можно начать писать сообщения.

Однако не надо торопиться. Лучше закончить настройку, чтобы больше к этому не возвращаться. Прежде всего рекомендуем навести курсор на меню «Профиль» и в выпадающем окне выбрать раздел «Изменить» (рис. 13).



Рис. 13. Как попасть на страницу изменения профиля пользователя в Живом Журнале, на которой появились дополнительные поля.

Страница изменения профиля будет несколько отличаться от той, что вы видели в начале регистрации. Теперь на ней вы можете внести гиперссылку на свой основной сайт или блог. Это может быть на самом деле ваш ресурс, который вы дополнительно раскрутите за счет этой гиперссылки, а может быть и тот, который вы поддерживаете как союзника. Указанная гиперссылка разместится в вашем профиле пользователя и за-

одно будет отображаться на главной странице вашего блога и на всех остальных его страницах.

На этой же странице редактирования личных данных вы можете указать свои номера ICQ и телефона. Надо ли это делать, каждый решает для себя сам исходя из целей в информационной войне, для которых он завел блог. Мы лишь напомним, что эта информация становится доступна без преувеличения в глобальном доступе кому угодно и откуда угодно, в том числе и вашему противнику.

Ну вот, осталось совсем немного – и блогом можно будет пользоваться, однако надо еще кое-что настроить, а именно – внешний вид блога и доступ к записям.

Следует пройти по ссылке: «Журнал – Оформление» (рис. 14).

На открывшейся странице внести «Заголовок журнала» (Journal Title). Это исключительно важный шаг, поскольку по заголовку поисковые машины будут определять, какой теме (а точнее по каким словам) блог соответствует. Поэтому ключевые слова должны присутствовать в этом заголовке, а еще лучше, чтобы заголовок состоял только из этих ключевых слов. Например: «Растратчик Имярек», или «Иванов Иван Иванович», или

«Кактус Девелопмент Груп». Старайтесь избегать чересчур длинных заголовков. Например, если вы хотите раскрутить блог о мошеннике Сперецком (это вымышленная фамилия), то лучше назвать блог «Сперецкий», чем «Сперецкий – это такой злостный мошенник, что просто в ужас приходишь от его кошмарных и циничных поступков!». Связано это с тем, что поисковые машины интересуется не только наличие ключевых слов в заголовке, но и их удельный вес. Страница, в которой ключевые слова имеют большой удельный вес, считается более тематической, чем та, где удельный вес ключевых слов меньше. Соответственно, такая страница встает в выдаче выше. Правда, в заголовке можно попытаться дать ключевое слово несколько раз, если вы сможете это сделать мотивированно, избежав обвинения в спаме. Так, например, написать заголовок блога «Сперецкий, Сперецкий, Сперецкий» – не очень хорошая идея, так как видимого основания для трехкратного упоминания ключевого слова нет. Возможно, лучше озаглавить блог примерно так: «Сперецкий и „Дело Сперецкого“» или «Сперецкий. „Дело Сперецкого“». История со Сперецким в развитии».



Рис. 14. Как перейти к настройкам журнала в Живом Журнале.

Следующая строка – «Подзаголовок журнала» (Subtitle) – тоже важна. Лучше, чтобы подзаголовок также содержал основные ключевые слова и тоже с достаточно большим удельным весом. Например, для блога по продвижению фактов о мошенничестве гипотетического гражданина Сперецкого может подойти подзаголовок «Мошенничество Сперецкого», «Жертвы мошенника говорят о Сперецком» или «Сперецкий. Мошенничество в подробностях». Можно в подзаголовке написать и «Мошенник Сперецкий. Все о мошенничестве господина Сперецкого». Посмотрите, чтобы подзаголовок рас-

шифровывал и дополнял заголовок, выглядел связанным с ним по смыслу.

Ниже подзаголовок есть еще третье поле – заголовок для ленты друзей. Его заполняют по такому же принципу, как подзаголовок. Можно и не заполнять его вообще, поскольку заголовок и подзаголовок важнее, чем эта страница с точки зрения продвижения блога в поисковых машинах, а нагромождение ключевых слов еще и на этой странице будет выглядеть перебором.

После заполнения заголовка и подзаголовка следует перейти ниже по странице – в раздел «Новый дизайн», где можно настроить внешний вид журнала. Там просто выберите стиль оформления, который вам больше нравится, и цветовую гамму, которая вам по душе. Каждый стиль оформления можно открыть на отдельной странице и увидеть, как ваш журнал будет выглядеть при таком оформлении. При выборе стилей оформления вы увидите, что часть из них недоступна пользователям с бесплатными аккаунтами. Платным пользователям все стили оформления доступны.

Если вы не хотите менять стиль и не имеете ничего против того, чтобы он был назначен вам автоматически, можно ограничить-

ся заполнением полей «Заголовок» и «Подзаголовок» и сразу после этого начинать пользоваться блогом. Мы рекомендуем пользоваться в разных блогах, участвующих в отражении информационного нападения, разными стилями оформления, так как иначе в случае, если читатель ваших материалов станет переходить с блога на блог, он быстро устанет от однообразия. Кроме того, в ряде случаев разный стиль оформления блогов позволяет создать иллюзию, что ваших союзников больше, чем на самом деле, а это может помочь сломить боевой дух противника и быстрее завершить информационную войну.

Все. Настройка блога закончена. Теперь у вас есть блог с именем и адресом в Интернете (пример для имени «name») www.name.-livejournal.com

Блог готов, и теперь можно в него писать. Но можно не значит необходимо. Вы имеете полное право начать делать записи в блог позже. В информационной войне бывают промежутки между сражениями, и есть смысл потратить высвободившееся время, чтобы заготовить некоторое количество «боевых единиц» впрок.

Аватар (аватара) – это маленькая картинка, которая, на ваш взгляд, может представлять вас в виде изображения в Интернете. Это изображение появляется рядом с вашими текстами, когда вы пишете пост или комментируете чьи-либо слова. Аватар позволяет людям быстрее понять, что сообщение, которое они читают, – ваше, а в случае работы с обычным блогом дает возможность дополнительно продемонстрировать, как вы сами себя воспринимаете. В информационной войне аватар, на наш взгляд, большой роли не играет. Он слишком мал, чтобы его можно было в подробностях разглядеть. Хотя, если вам удастся ввести в обиход какой-то графический символ, например, выделяющий ваших сторонников, то этот символ вполне может быть размещен на их блогах. Его роль будет примерно такой же, как ленточки в петлице у демонстрантов. Возможно, существуют одно-два недлинные слова, которые выполняют роль слогана в вашей войне. Их можно поместить на картинку и использовать ее в качестве аватара.

Вы можете создать аватар сами, а можете выбрать из коллекции (например, на сайте www.avatar2k.nm.ru/). Особенность аватара в том, что его размер должен быть по разме-

ру не более 100 x 100 пикселей, поэтому поставить любую фотографию или картинку, которая вам нравится, без специальной обработки нельзя. В Интернете существуют сервисы, позволяющие бесплатно превратить вашу картинку или фото в аватар. Например, широко известный у блоггеров и участников интернет-форумов сайт www.photolava.com/

В самом Живом Журнале также есть возможность превратить изображение в аватар – на странице www.livejournal.com/editpics.bml

Первая запись в блоге. Если вы только что закончили настройки блога и находитесь на странице, где выставлялись стили его оформления, то пройдите по гиперссылке «Журнал – Написать». Если же вы просто зашли в свой блог с его главной страницы www.name.livejournal.com, то нажмите на гиперссылку «Написать в журнал» («Post to your journal»).

В открывшемся окне введите тему записи (она должна по возможности не только характеризовать текст, который предваряет, но и содержать ключевые слова). Если обратиться к примеру с растратчиком Сперецким, то заголовок «Механизм мошенниче-

ства» будет хуже для продвижения в поисковых машинах, чем заголовок «Механизм мошенничества Сперецкого» или «Сперецкий. Механизм мошенничества».

Для ввода текста существуют два режима: «визуальный редактор» и «HTML». Первый позволяет выполнить форматирование текста, подобно тому, как это делается в текстовом редакторе Word, а второй дает возможность вводить текст с тегами, прописанными вручную. Начинающим пользователям, на наш взгляд, лучше пользоваться визуальным редактором.

Введите (или скопируйте из текстового реактора) основной текст своего сообщения. В режиме «визуальный редактор» можно менять размер шрифта и его цвет, вставлять или удалять гиперссылки, таблицы, нумерованный или маркированный список, выделять фрагменты текста курсивом или жирным шрифтом, подчеркиванием или зачеркиванием и т. п. Пиктограммы очень похожи на те, что есть в Word.

В визуальном редакторе особого внимания заслуживает кнопка со всплывающей надписью «Врезка ЖЖ» (рис. 15).

Если выделить фрагмент текста, а затем нажать эту кнопку, то текст будет убран под

кат, т. е. на главной странице блога он окажется скрыт за надписью-гиперссылкой «Читать дальше» («Read more»). При нажатии на эту надпись читатель будет перемещен на страницу с сообщением, которое хочет прочитать (сообщение на этой странице будет доступно для чтения полностью). После нажатия кнопки «Врезка ЖЖ» вы увидите окошко с надписью «Читать дальше». Нажав на нее, обнаружите, что текст, который надо убрать под кат, полностью выделен серым цветом (рис. 16).

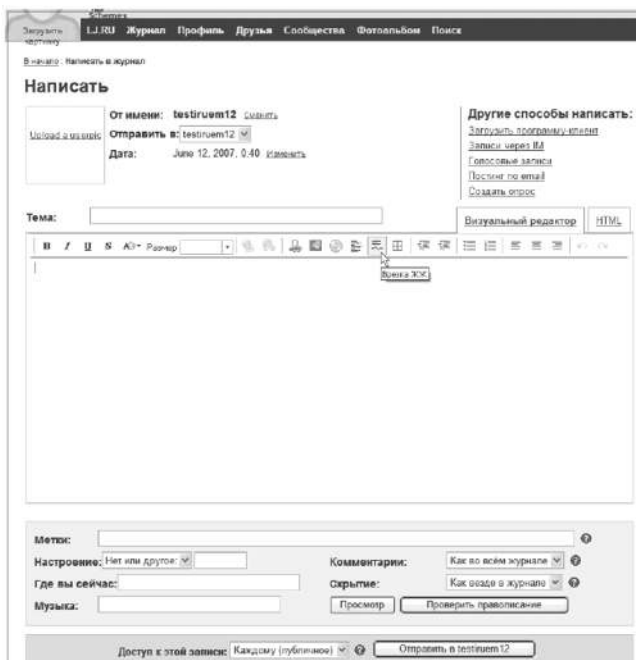


Рис. 15. Кнопка «Врезка ЖЖ» в визуальном редакторе Живого Журнала при создании нового сообщения

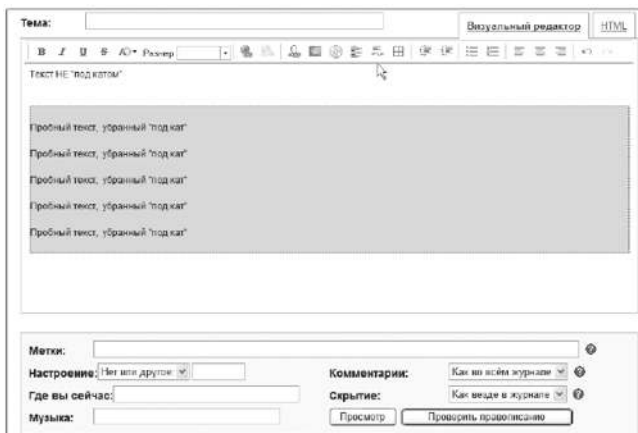


Рис. 16. Текст, выделенный серым, будет в Живом Журнале убран под кат.

Убрать текст под кат очень важно для пользователей Живого Журнала – как для удобства читателей блога, так и для повышения его рейтинга у поисковых машин. Читателям так удобнее, потому что, если текст сообщения длинный, он во френдленте будет занимать слишком много места, что вряд ли их обрадует. Мы, к примеру, неоднократно сталкивались с тем, что пользователи, записавшие нас в друзья, просят убирать под кат длинные тексты. Они сами перейдут на вашу страницу, если заинтересуются темой, но если она будет им навязываться, они могут быть недовольны. В условиях противо-

действия информационному нападению не стоит давать потенциальным союзникам повод для недовольства собой. Под кат можно убирать не только окончание текста, но и любую его часть, в том числе и фрагмент из середины. Это бывает важно, когда текст длинный и несколько важных мыслей распределены в нем равномерно. Вы можете убрать под кат расшифровку каждой мысли, получив в результате компактный перечень основных аргументов, которые при такой компоновке сами по себе способны оказывать информационное воздействие на читателя. При этом перечень можно на любом месте развернуть и прочесть все аргументы.

Что касается рейтинга текста у поисковых машин, тут важно понимать следующее. Для того чтобы ваши ресурсы поддерживали друг друга, неплохо иметь в каждом сообщении несколько гиперссылок на те сайты или отдельные интернет-странички, к которым вы хотите привлечь внимание целевой аудитории или которые хотите поднять в выдаче. Например, на блоге одного из авторов этой книги – «Блоге Ющук А. В. Конкурентная разведка» – в конце каждой страницы стоят гиперссылки на некоторые интересные материалы (к примеру,

на статью о том, как профессионально искать в Гугле). Это позволяет человеку перейти с любой страницы блога к полезной статье и прочитать ее, но в то же время и паук может перейти к этой статье с каждой страницы блога. Однако если эти гиперссылки не убирать под кат, то на первой странице блога, где обычно помещается 20 сообщений, окажется расположено 20 однотипных гиперссылок, что может быть воспринято поисковыми машинами как спам, будет достаточно скоро обнаружено специальными фильтрами и с большой вероятностью приведет к исключению ресурса из индексации либо к понижению его рейтинга в выдаче. А когда фрагменты страницы, содержащие гиперссылки, убраны под кат, то на главной странице блога однотипных ссылок нет (их не видно за надписью «Read More»). На каждой отдельной странице (а точнее, на каждом URL) есть лишь одна такая ссылка, что не воспринимается машиной как нечто предосудительное, поскольку так и выглядит обычно оглавление сайта или обыкновенный рекламный баннер.

Если возникает необходимость вставить в текст гиперссылку в режиме визуального редактора, то следует напечатать или скопи-

ровать в блог текст, затем выделить его и, нажав кнопку «Вставить/ Редактировать ссылку», добавить ссылку на нужный ресурс в появившемся всплывающем окне. А если в режиме визуального редактора вставляется скопированный из Интернета или из текстового редактора фрагмент текста, уже содержащий гиперссылку, то она при вставке сохраняется.

Если же требуется вставить теги HTML вручную, то рекомендуем вначале перейти из режима визуального редактора в режим HTML

и уже в нем эти теги добавлять. В противном случае они будут восприниматься как обычный текст, и вы будете видеть их, а не тот эффект, который они должны обеспечивать при просмотре отформатированного с их помощью текста в браузере. К плюсам Живого Журнала несомненно можно отнести то обстоятельство, что в нем (в отличие от многих других блогов) при переходе из режима визуального редактора в режим HTML и обратно текст, который вы редактируете, не исчезает.

В принципе большинство пользователей могли бы отправлять сообщение в блог уже в этом виде. Но для более полного использо-

вания возможностей блога в целях отражения информационного нападения мы рекомендуем научиться пользоваться и другими полями, расположенными ниже основного текстового поля. Речь идет о полях «Метки», «Настройка», «Где вы сейчас», «Комментарии», «Скрытие» и «Доступ к этой записи».

Рассмотрим их более подробно.

«Метки». Обязательно заполните поле «Метки» («Tags»). Это ключевые слова. Во-первых, по ним пользователи смогут найти ваш блог, когда потребуются отыскать материалы по определенной теме. Более того, метки обычно индексируются поисковиками, причем не только в вашем блоге – они собраны на отдельных страницах Живого Журнала и еще немалого количества различных интернет-ресурсов. Все эти ресурсы посещаются пауками поисковых машин и имеют отдельные адреса в Интернете. Соответственно, и строки в выдаче поисковых машин они занимают отдельные, дополнительно продвигая вашу точку зрения. В результате вы получаете гиперссылки на свой блог с самых разных адресов, что помогает в раскрутке вашего блога и дает преимущество в информационной войне. Особенно удачно располагать среди меток слова, име-

ющие широкое распространение, например, «Интернет», «видео», «любовь», «музыка». С достаточно большой вероятностью вы в результате увидите по ключевым словам строки в поисковых машинах, где будет написано слово «Интернет», а затем будет идти название вашего блога. При переходе по такой гиперссылке читатели получают возможность перейти на него и ознакомиться с вашей точкой зрения. Поэтому постарайтесь внести в поле «Метки» максимально большое количество слов, которые характеризуют тему вашего материала на странице блога. И постарайтесь включить в метки к каждой странице те ключевые слова, по которым вы хотите раскрутить свой блог, а также те распространенные слова, которые имеют отношение к тексту, расположенному над ними. Избегайте включать в метки слова, не имеющие никакого отношения к тексту. Не забывайте, что противник только и ждет повода обвинить вас в спаме и потребовать удаления вашего блога с блоговой площадки и из поисковых машин. Если вы не видите, каким образом увязать текст с одним из распространенных слов, то просто включите их в текст так, чтобы это смотрелось логично. Например, используйте фразы вроде «Это

песня!», «Впору видео снимать по такому сюжету!», «Он, наверное, считает, что Интернет все стерпит!», «„Музыка“ его речей навевает тоску».

Вот что сообщает о метках сам Живой Журнал (на примере блога yushchuk.livejournal.com).

Вопрос № 226

Как мне пометить свои записи? Где я могу управлять своими метками?

Метки – это слова или короткие фразы, которые можно использовать для систематизации журнала. Задайте метки записи набрав их в поле «Метки». Задайте несколько меток, разделив их запятыми (например, «дети, дом»). Можно также задать метки существующей записи, нажав в ней кнопку «Метка» или воспользовавшись ссылкой «Редактировать метки». Просматривать свои метки и управлять ими можно на странице управления метками (<http://www.livejournal.com/manage/tags.bml>).

Просмотр меток

Список меток покажет все ваши метки и частоту их использования. В некоторых стилях эта страница покажет уровни доступа для меток, которые доступны пользователю; в других стилях метки могут оказаться вид-

ны пользователям, даже если сами записи с этими метками для них закрыты.[45]

«Настроение». Этот раздел позволяет сделать ваше сообщение более эмоционально окрашенным. Он не обязателен для заполнения. Для целей противодействия информационному нападению он обычно не нужен, но заинтересует вашу целевую аудиторию – блоггеров, которые в своих сообщениях придают этому разделу особое внимание. Теоретически можно предположить, что отражение вашего истинного или мнимого настроения способно нести смысловую нагрузку и воздействовать на целевую аудиторию либо на противника. На практике мы ни разу не встречались с необходимостью уделять внимание этому разделу.

«Где вы сейчас». Этот раздел предполагает дополнительную информацию для существующих и потенциальных друзей о вашем местонахождении. Возможно, он и важен для тусовщиков, но в информационной войне не очень востребован. Разве что надо помозолить глаза противнику каким-то значимым для него названием, заведомо навевающим на него тоску или говорящем о том, что вы процветаете, несмотря на его происки.

«Комментарии». По умолчанию комментарии, которые пишут к вашему блогу, приходят по электронной почте на адрес, указанный при регистрации. В зависимости от того, какой вариант вы выберете, будет установлено, кому вы разрешаете комментировать ваши сообщения и разрешаете ли вообще. По умолчанию комментарии открыты для всех, если вы не устанавливали иных правил при настройке блога. Поэтому раздел «Комментарии» по умолчанию содержит правило «Как во всем журнале». Если вы сочтете нужным изменить правила для всего журнала, то лучше сделать это, пройдя по ссылке «Журнал – Комментарии – Настройки комментариев». Но если особые правила комментариев вы планируете установить только для отдельной записи, это можно как раз сделать, изменив параметры поля «Комментарии» для этой конкретной записи при ее вводе или редактировании. Комментарии могут быть разрешены всем, либо только зарегистрированным пользователям (т. е. запрещены анонимам), либо только тем, кого вы сами добавили в друзья. Можно вообще запретить комментирование или сделать так, что комментарии будут скрыты и вы сделаете их видимыми после того, как с ни-

ми ознакомитесь.

При противодействии информационному нападению нельзя дать однозначный совет, как лучше настраивать комментарии. Все в очень большой степени зависит от конкретной ситуации. Если количество блогов, находящихся в вашем ведении, относительно невелико и противник или кто-то еще не проявляет активности по их комментированию, можно просто вывести уведомление о поступающих комментариях в один почтовый ящик. Для этого на него устанавливают переадресацию с почтовых ящиков каждого блога. Это позволяет контролировать ситуацию без особых затрат времени и сил. Если же количество комментариев, которые надо удалять, велико, то лучше вообще запретить комментирование или же разрешить его только тем, кого вы внесли в список друзей. Нельзя забывать и о проблемах, которые доставляют спамерские боты (программы, намеренно размещающие спам в комментариях на блогах и форумах). Оставлять спамерские комментарии на своих блогах нельзя, так как поисковые машины могут считать ваш ресурс также спамерским и удалить его из своей базы. Активность спамерских ботов может сама по себе послужить причиной

ужесточения политики комментариев в блоге. А чем популярнее будет ваш блог, тем большее количество спамерских ботов станет вам досаждать, да и противник может попытаться размещать в комментариях к вашему блогу ссылки на порносайты или откровенно спамерские интернет-ресурсы, чтобы понизить рейтинг вашего блога у поисковых машин.

«Скрытие». Позволяет скрывать комментарии – все или по определенным параметрам. В Живом Журнале, как мы уже говорили, можно разрешить комментарии всем без исключения, либо всем, кто зарегистрировался в Живом Журнале, либо только тем, кто занесен вами в список ваших друзей, а можно и вообще запретить комментарии для всех без исключения. Скрытие комментариев имеет смысл, например, когда вы хотите видеть все комментарии, поступающие в блог, но не хотите, чтобы они без цензуры попадали в Интернет.

«Доступ к этой записи». Это поле позволяет сделать саму вашу запись видимой всем, либо только тем, кто добавлен владельцем аккаунта в список его друзей, либо вообще только владельцу журнала (точнее, тому, кто зашел под логином владельца). Все, чей

уровень допуска не позволяет видеть запись, увидеть ее не смогут и даже не узнают о ее существовании.

Если запись была в открытом доступе, а затем ее закрыли, то, не имея достаточных прав, прочитать страницу не удастся даже по прямой ссылке: вместо доступа к ее контенту появится сообщение, что прав для доступа у посетителя блога недостаточно.

После заполнения всех нужных полей остается нажать кнопку «Отправить в журнал» – и в вашем блоге появится запись, которая будет иметь уникальный адрес в Интернете, а значит люди в принципе могут ее прочитать при поиске через поисковые машины по ключевым словам. Как сделать, чтобы эта запись оказалась как можно выше в результатах выдачи, мы покажем далее.

Платный аккаунт в Живом Журнале

Платный аккаунт имеет один недостаток: он не позволяет полностью соблюсти анонимность, поскольку предусматривает проведение безналичных платежей. Безусловно, это в принципе решаемая проблема, но она существует. На странице www.mylj.-

ru/support/faqbrowse.-

bml?faqid=131&view=full рассказывается, что именно приобретает за деньги владелец платного аккаунта. Для целей отражения атаки черного PR из всего многообразия преимуществ, описанных в Живом Журнале для владельцев платного аккаунта, мы бы выделили следующие возможности:

- устанавливать 50 постоянных ссылок вместо 10 доступных базовым пользователям (это важно, в том числе и потому, что постоянно существующие ссылки со временем приобретают все больший авторитет у поисковых машин);

- вставлять опросы в свои записи (иногда это позволяет лучше довести свою точку зрения в информационной войне);

- пользоваться улучшенным доступом к фотоальбому: под фотографии отведено 2 Гбайта пространства, и он полностью встроен в журнал (это позволяет легко и без ограничений размещать фотоматериалы);

- отправлять мобильные, почтовые и голосовые сообщения;

- покупать дополнительное место на диске для картинок в фотоальбоме и голосовых сообщений;

– заносить в список друзей до 2 тысяч пользователей, а не тысячу, как у базовых и улучшенных аккаунтов;

– массово менять уровень доступа к записям в вашем журнале, хоть ко всем сразу.

Ответы практически на каждый вопрос, который может возникнуть у пользователя Живого Журнала на русском языке, вы найдете по адресу: www.livejournal.com/support/faq.bml

Создание блога в Liveinternet

ВНИМАНИЕ! Чтобы нормально зарегистрировать дневник на Liveinternet.ru, нельзя отключать в браузере скрипты и просмотр изображений.

Итак, рассмотрим механизм создания блога на этом ресурсе.

Перейдите на главную страницу www.liveinternet.ru/ и там, в разделе «Блоги (Дневники)», нажмите на кнопку «Заведите дневник» (рис. 17).

После этого вы попадете на страницу «Быстрая регистрация», где есть всего два поля для заполнения. В них предлагается ввести действующий адрес электронной почты и код подтверждения (ввод кода – защита от

автоматических регистраций). Если у вас еще нет почтового ящика, либо вы хотите завести себе новый почтовый ящик, вам здесь же предлагается открыть почтовый ящик формата @li.ru (рис. 18).

Еще раз напомним: пароль должен быть достаточно длинным (длиннее шести знаков), не связанным с вашим именем, номером телефона или номером автомобиля, именами ваших родных или, например, домашних животных. Лучше всего включить в пароль не только буквы, но и цифры, а также (если нет ограничений на вводимые символы) при создании пароля рекомендуем использовать такие знаки, как @, !, ? #.



Рис. 17. Главная страница Liveinternet.ru и кнопка «Заведите дневник».

Быстрая регистрация

Для регистрации достаточно ввести адрес своей электронной почты. На нее будет выслан пароль и ссылка, по которой можно выбрать имя и другие параметры своего дневника. Если у вас нет почтового ящика или вам нужен новый, предлагаем [зарегистрировать его](#) в почте [@li.ru](#)

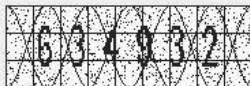
Ваш e-mail:

Выберите пароль:

Повторите пароль:

Код подтверждения:

Что написано на картинке?



Отправить

Рис. 18. Страница «Быстрая регистрация» на Liveinternet.ru

Достаточно быстро (иногда сразу) в указанный при регистрации электронный почтовый ящик приходит письмо, в котором содержится автоматически сгенерированный пароль (практически непригодный для запоминания, но устойчивый к подбору) и гиперссылка с адресом, по которой можно перейти для продолжения регистрации блога.

После перехода по присланной ссылке происходит стандартная для интернет-сервисов процедура регистрации, похожая на описанную нами, когда мы говорили об открытии блога в Живом Журнале. Следует выбрать себе имя (ник), указать дату рождения, город, в котором вы живете, написать несколько слов о себе или создаваемом блоге.

Кроме того, надо выбрать цветовую схему блога, причем без этого регистрация не продолжается. Внешний вид страницы, на которой заполняется первичная информация о пользователе, приведен на рис. 19.

После регистрации можно внести некоторые дополнительные изменения в личные данные, в том числе указать адрес вашей домашней страницы. Домашней страницей также может служить адрес сайта или, например, другого вашего блога. Тем самым вы дадите своему ресурсу дополнительную ссылку на него со своего нового блога и повысите его цитируемость.

По окончании регистрации вы увидите личное сообщение от руководителя разработчиков сайта Liveinternet.ru под ником Valez, который не только приветствует вас как нового владельца блога, но и знакомит с

основными сервисами блога и дает гиперссылки на них. Вот текст этого личного сообщения.

Приветствую.

Я Валентин, руководитель разработчиков этого сайта. Пусть это приветствие и рассылается автоматически, но я действительно рад новым людям и готов приложить все усилия, чтобы на сайте понравилось, работа с ним была удобна и хотелось порекомендовать его своим друзьям. В случае возникновения каких-либо проблем можно (и нужно) написать мне личное сообщение например, ответив на то, что сейчас читаете. Подписавшись на **мой дневник**(нажав **Стать постоянным читателем** в левой панели моего дневника), можно общаться со мной и узнавать об изменениях на сайте. Таким же образом можно добавить в свои друзья любой другой понравившийся дневник. Начав пользоваться сайтом, я бы:

1. Написал что-нибудь в дневник более полноценное, чем то, что введено при регистрации. Новое сообщение в дневник можно добавить из профиля, кликнув ссылку «Новая запись», нажав аналогичную кнопку в дневнике или прямо сейчас – **по этой ссылке добавления**.

LiveInternet 070x240px.html Ввод / Регистрация / Настройка профиля

Обратная связь Настройка профиля

Описание анкеты: Введите, пожалуйста, подробней об основных этапах в жизни человека

Быстрая регистрация

Выборите, пожалуйста, имя для своего дневника или сообщества (названия сайта приемлемы только тогда, когда вы выбрали email, а также зарегистрируете другие дневники в сети и в социальных сетях). Обязательное для заполнения поле: фамилия (имя отчество).

Персональные настройки:

Имя (имя): *

Вы создаете:

Анкеты данные:

Пол: *

Дата рождения: *

Город: *

Ваш e-mail:

Номер ICQ:

E-mail-адреса друзей:

Настройки дневника:

О себе и дневнике: *

Ваша фотография:

Цветовая схема:

Рис. 19. Страница, на которой заполняется информация о пользователе на Liveinternet.ru

2. В настройках дневника закачал свою картинку – аватар, подстроил цветовую гамму под свой вкус. Вот **ссылка на управление аватарами**

3. Закачал бы в фотоальбом несколько фотографий, чтобы познакомить всех с собой – ссылка «Добавить фото» есть в профиле, опять же в самом фотоальбоме, или можно **нажать сюда**.

4. С чувством выполненного долга начал бы поиск друзей.

Например, пошел бы на ленту-страницу самого популярного на сегодня. Хотя, может, лучше бы пригласил друзей присоединиться. Лично как-то приглашать неудобно, а через спецсервис вроде как и ненавязчиво. Кому не надо, могут просто не читать и сделать вид, что их и не приглашали.

5. А дальше – уже придумал бы по ходу дела. Или написал бы мне, спросил совета:)

Удачи, пишите мне, если что.

Валентин

Теперь можно пользоваться блогом. Поскольку Liveinternet – российский ресурс, на нем нет языковых проблем. Все меню пользователя написаны по-русски, снабжено разделом «Помощь», а кроме того, понятно даже интуитивно.

К серьезным преимуществам Liveinternet мы бы отнесли возможность получения развернутой статистики о посетителях, которая может помочь владельцу блога понять,

сколько людей приходят на его блог, откуда, по каким запросам и на какие страницы. На рисунке 16 приведен внешний вид страницы блога, которая позволяет полноценно управлять доступом ко всем его функциям после регистрации на рис. 20.

В Liveinternet есть страница, где содержатся ответы на большинство вопросов, возникающих у пользователя. Она расположена по адресу: www.wiki.liveinternet.ru/ServisDnevnikovLiveInternet/FAQ

Другие блогговые площадки

Мы рассмотрели две самые крупные блогговые площадки в Рунете, потому что они являются типичными, общеизвестными и отлично индексируются. Между тем в мире существует огромное количество блогговых площадок, и зачастую невозможно предугадать, как они будут восприниматься поисковыми машинами. Внимательное наблюдение со стороны за одним корпоративным конфликтом, сопровождавшимся информационной войной в Интернете, показало, что текст, размещенный на блогговой площадке в Украине, оказался на первой странице Гугла уже на следующий день. Причем эта

площадка в Рунете не на слуху, по крайней мере мы никогда раньше не слышали о ее существовании. Помимо вопроса индексации поисковыми машинами есть и еще один аспект, заставляющий обратить более пристальное внимание на блогерские площадки, неизвестные широкой публике в Рунете. Противодействие информационному нападению – это всегда конфликт. Противник, инициировавший волну черного PR, будет пытаться противодействовать вашим действиям. И чем менее он профессионален, тем больше вероятность, что он начнет в ответ на ваши действия совершать глупые, бессмысленные, но требующие от вас ответной реакции поступки. Такие малопрофессиональные люди, по нашим наблюдениям, могут пытаться писать администрациям блогерских площадок жалобы с требованием снять материалы о них из Интернета. Как показало скрупулезное изучение информационных войн в Сети, цели в подобных ситуациях достигают либо те, кто смог показать, что их ругали нецензурными словами, либо те, кто имеет административное или финансовое влияние на владельцев блогерских площадок. Однако победа у них обычно получается пиррова, и вот почему. Во-первых, если текст

не содержит оскорблений или призывов к антиконституционным действиям, то администрации блоговых площадок не считают нужным вмешиваться в чужие конфликты. Они исходят из того, что предоставили равные для всех права выражать свою точку зрения, и потом уж пускай заинтересованные лица, ознакомившись с обеими точками зрения, сами делают выводы, кто прав, а кто нет. Во-вторых, сторона, снимающая таким образом информацию из Интернета, сама подталкивает своего противника к тому, чтобы он размещал информацию на как можно большем количестве ресурсов, снижая тем самым вероятность вражеского воздействия (никогда заранее неизвестно, кто с кем находится в дружеских, служебных, родственных или деловых отношениях, поэтому некоторые попытки снять информацию из Интернета могут быть успешными).

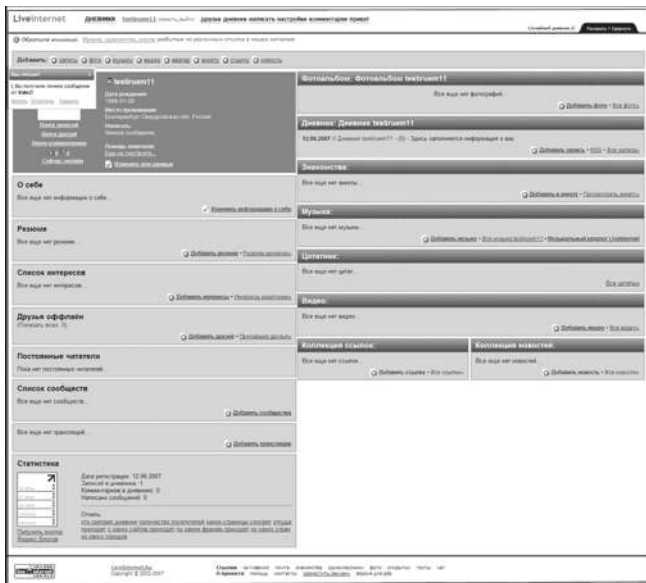


Рис. 20. Внешний вид страницы блога на Liveinternet.ru после завершения регистрации

Поиск альтернативных блоговых площадок элементарно прост. Достаточно поискать в Гугле, Yahoo или любом другом зарубежном поисковике документы по запросу «blogs Canada», «blogs Australia» «блоги Казахстан» и т. п. Блоги, расположенные на всех площадках мира, практически одинаковы, и размещение на них материалов проблем не вызывает. А вот «надавить» на администра-

цию блоговых площадок или «договориться» с ней в таком случае практически невозможно.

Подкастинг: размещение аудиофайлов в блоге

Люди стремятся перенести в Сеть все средства коммуникации, к которым они привыкли. Идея переноса аудиофайлов родилась, наверное, сразу, как появился Интернет. Однако медленные каналы связи и несовершенные средства обработки аудио долгое время препятствовали ее реализации.

Сегодня, когда Интернет стремительно дешевеет, а скорость передачи данных неуклонно растет, стало вполне возможно выкладывать аудиосообщения в Интернете вместо текстов. Все чаще на блогах, например Shkolazhizni.ru, вместо текстов появляются аудио-ролики.

Наибольшее распространение получил так называемый подкастинг. Это фактически радиовещание в Сети, организованное по принципу социальных сетей, т. е. доступное для комментирования. Причем комментарии можно давать не только письменно, но и голосом. Как метко сказал Александр

Белов в статье «Подкастинг: у всех на ушах»: «Вскоре смайлики уйдут в прошлое, уступив место нормальному человеческому ржанию».[46]

От обычного прикрепленного аудиофайла подкастинг отличается тем, что позволяет подписываться на изменения с помощью RSS, а также автоматически скачивать новые файлы, чтобы прослушивать их в удобное время на компьютере, плеере или мобильном телефоне. В частности, Nokia создала специальную программу для скачивания подкастов на телефон. Эта программа доступна по адресу: www.europe.nokia.com/podcasting

Компьютеры фирмы Apple, например, уже имеют предустановленную программу iWEB, которая позволяет совершенно неподготовленным пользователям очень быстро создавать красивые сайты, прикреплять к ним подкасты и одним кликом мышки размещать на сервисе «Дотмак» (.mac), принадлежащем Apple.

Благодаря появлению подкастинга многие люди, которым нравится именно аудиоформат, открывают себе дополнительные журналы на порталах подкастинга или вообще полностью переходят на эти порталы. Самый

известный портал в Рунете – Rpod.ru (www.rpod.ru/).

Для того чтобы составить представление о том, что предлагает к прослушиванию этот портал и какова его основная аудитория, приведем перечень наиболее популярных подкастов на 08.06.2007 г. с его главной страницы.

ТОР-20 за вчерашний день

1. УпячкаTV. Первый выпуск.
2. #24 JoCastS.
3. Сергей Чекмаев «Прозрачный паровозик с белыми коле сами».
4. УпячкаTV. Второй выпуск.
5. Сиськи-письки-шоу. Ненормативная лексика.
6. Сергей Чекмаев «Гладиаторы каменных джунглей».
7. Сергей Туманов «Создатель игрушек».
8. Пол Ди Филиппо «Однажды в Телевизионном Городе».
9. Альфред Ван Вогт «Призрак».
10. Андрей Павлухин «Теледрайв».
11. NOVUS ORDO HIPHOP MIX.
12. Радио-Т #38. Vobuk и Umputun импровизируют на хайтековские темы.
13. Аэростат – 106, «Иоганн Себастьян Бах».

14. THE BIG PODCAST! 28.05.07. «Скоро: молодая американская маньячка!». Ненормативная лексика.

15. Евгений Гаркушев «Шестое чувство».

16. #23 JoCast.

17. UWP – Выпуск #127 (1 июня 2007).

18. 102 – Бобук в гостях у пиндоса, или Радио Т после пьянки.

19. Сиськи-письки-шоу. Ненормативная лексика.

20. Как домашние растения влияют на нашу жизнь?

Для целей противодействия черному PR в Интернете подкастинг может быть очень полезен. Диапазон его возможностей колеблется от размещения отдельного аудиофайла до организации собственной радиостанции в Интернете, не требующей ни лицензирования, ни дорогостоящего оборудования. При этом вам совершенно необязательно бороться с лидерами портала для размещения подкастов за первое место по числу слушателей. Вы можете привлечь свою целевую аудиторию, дав прямые ссылки на свой ресурс, где вам ничего не мешает в буквальном смысле слова высказать свою точку зрения на ситуацию.

Видео в Интернете как явление и как средство раскрутки блога

Видеоблоги несколько отстают пока что от аудиоблогов по скорости своего распространения, хотя это отставание непрерывно сокращается. В течение ближайших нескольких лет ожидается быстрое развитие видео в Интернете. Мы не будем подробно останавливаться на видеоблогах, скажем лишь, что наиболее крупными в мире порталами распространения видео являются YouTube, MySpace, Google Video и iFilm. В Рунете можно выделить проект Рамблера Rambler Vision (www.vision.rambler.ru/). Вот что сказано о нем на сайте самого Рамблера.

Rambler Vision – уникальный для российского Интернета проект. Это прообраз интерактивного, или «открытого», телевидения завтрашнего дня – пользователь становится одновременно и зрителем, и создателем этого телевидения. Здесь не телевизор программирует человека, а человек – телевизор. С помощью Rambler Vision каждый желающий может не только увидеть редкие работы, которые до этого были недоступны широкой аудитории, но и донести свои собственные

произведения до массовой аудитории, публикуя их на «Рамблер Планетах», и участвовать в различных конкурсах, постоянно проводимых в разделе «Конкурсы». Rambler Vision – единственное место в российском Интернете, где каждый автор может найти своего зрителя.

Для публикации своих работ необходимо зарегистрироваться или войти в систему под почтовым логином/паролем Rambler и загрузить работу в заданном формате.

Вы можете сделать это самостоятельно (см. подробнее «Загрузка видеофайла») или прислать свое видео посылкой или бандеролью с указанием вашего логина на Рамблере, после чего их опубликуют на сайте наши специалисты.[47]

Уже многократно говорилось, что Интернет живет за счет гиперссылок, которые позволяют пользователям, а также паукам поисковых машин находить новые ресурсы, определять их авторитетность и вообще превращать Интернет в реально работающую сеть. Естественно, должен был появиться сервис, позволяющий встраивать в видеоклипы активные гиперссылки. И такой сервис появился. Он расположен по адресу: www.bubbleply.com Детальное описание раз-

мещения гиперссылки в видеоролике с помощью этого ресурса приведено в видеоролике на блоге Марины Смайли (Marina Smiley) в статье «Простой способ зарабатывания на видеоблогах» по адресу: www.businesswithoutstress.com/2007/04/blog-post-.html

В Живом Журнале также есть возможность вставки видео (равно как и другого мультимедиа) с других сайтов.

Вопрос № 268

Как добавить видео и другие медиаролики в свои записи?

Вы можете вставить видео и прочие медиаролики с других сайтов в свои записи при написании и редактировании. Нажмите ссылку «Embed Media» (в редакторе HTML) или кнопку (с изображением компакт-диска. – *Е.Ю.*) в визуальном редакторе и введите код встраивания, предоставленный разместившим ролик сайтом.

Вы можете запретить загрузку и показ видеоклипов, включив заменители видео на странице настроек просмотра. Это приведет к замене всех встроенных видеоклипов на заменители (если вы вошли в ЖЖ). Эта настройка блокирует загрузку видео до тех пор пока вы не нажмете на значок заменителя.

Это полезно, если у вас дорогостоящее или медленное соединение с Интернетом.[48]

На рисунке 21 видно, как выглядит эта кнопка в визуальном редакторе Живого Журнала при написании нового поста.



Рис. 21. Кнопка вставки видеоролика или аудиоролика в визуальном редакторе Живого Журнала

Блог на мобильном телефоне

Интернет-сервисы развиваются в сторону повышения мобильности. Компьютеры становятся все меньше по размеру, а их возможности с каждым днем – все больше. Авторы блогов теперь могут с помощью мобильного телефона находиться в своем журнале круглосуточно. Вряд ли надо говорить о том, насколько это важно для тех, кто участвует в информационной войне и должен иметь возможность немедленно отреагировать на изменения в ситуации. Одним из пионеров переселения блогов в мобильные телефоны стал Живой Журнал. На странице www.ljmob.ru/ находится мобильный доступ к бло-

гу и его основным сервисам, адаптированный к работе на мобильном телефоне.

Вот меню доступа к Живому Журналу с мобильного:

Livejournal homepage

Лента друзей

Добавить запись

Читать журнал

Профайл

Рейтинг пользователей

Рейтинг записей.

Stand-Alone-блоги

Это оружие, идеально приспособленное для ведения информационных войн в Интернете, поэтому ему стоит уделить пристальное внимание. Как показала наша собственная практика и наблюдение за рядом информационных столкновений в Сети, «воюющие стороны» все чаще при выборе оружия в информационной войне отдают предпочтение stand-alone-блогам (отдельно расположенным блогам). Они находятся на площадках, подобных Живому Журналу или Liveinternet, а на отдельных хостингах и с отдельными доменными именами. Эти блоги очень похожи на сайты, если принимать

во внимание хостинг и доменное имя, но остаются именно блогами, если брать в расчет информацию и возможность обсуждения тем посетителями.

Можно сказать, что отдельно расположенные блоги сочетают в себе плюсы блога (легкое управление и интерактивность) и сайта (благосклонное отношение со стороны поисковых машин). Современные «движки» таких блогов, как правило, созданы по принципу открытого программного обеспечения, а значит, настраиваются и дополняются энтузиастами со всего мира. Они настолько хорошо исполнены технически, что блоги, созданные на этих движках, прекрасно индексируются. Управление ими столь просто, что таким «блогосайтом» может управлять даже десятилетний ребенок или пенсионер, впервые увидевший компьютер совсем недавно. Один человек в принципе способен размещать в течение дня информацию в сотне подобных блогов. Таким образом, использование stand-alone-блогов позволяет реагировать на инциденты в Интернете очень оперативно, даже располагая малыми кадровыми ресурсами.

Наиболее распространенным на момент написания книги «движком», с помощью ко-

торого создавались отдельно стоящие блоги, был Wordpress. Его можно официально бесплатно скачать в Интернете (например, на русскоязычном сайте mywordpress.ru). К нему существует множество плагинов (дополнений, обеспечивающих дополнительную функциональность), также бесплатно скачиваемых. Настройка такого блога под конкретного пользователя занимает у специалиста от силы полдня и не представляет никаких трудностей. Можно синхронизировать отдельно стоящий блог с блогом в Живом Журнале или на Liveinternet, и тогда сообщения, размещенные на отдельно стоящем блоге, будут с помощью специального плагина кросспостинга дублироваться в обычном блоге. В результате каждое сообщение станет автоматически «зеркалиться» на несколько других блогов. Примером отдельно стоящего блога могут быть перечисленные ниже.

1. «Блог о Блогах». Ющук Евгений Леонидович (www.blogging.ru/).

2. «Блог МегаФон Москва». Неофициально о тарифах, об услугах, о зоне покрытия и роуминге, слухи, события, комментарии (www.blog.megafoncity.ru/).

3. Блог Александра Плющева (ведущего программы «Эхонет» на «Эхе Москвы») (www.plushev.com/) и его «Зеркало» в Живом Журнале (<http://echonet.livejournal.com/>).

Маскировка «боевого» блога

Не всегда нужно, чтобы противник отчетливо видел, что блог создан исключительно для противодействия его нападению. Бывают ситуации, когда блог должен имитировать реально существующий ресурс, для которого участие в информационной войне – не главное, для чего он создавался. Тогда вам придется заниматься блоггингом, а значит, решать основную проблему, которая возникает у большинства блоггеров, – творческую. Как выбрать тему для блога? О чем писать?

Специалисты спецслужб хорошо знают профессиональную поговорку: «Лист надо прятать в лесу». Соответственно, ваш блог, который надо замаскировать под обычный, должен быть похож на другие «мирные» блоги. Вам придется решать проблему датирования записей и их содержания. С датированием на самом деле проблем не возникает: вы можете поставить любую дату при написании сообщения – как предшествующую

действительной, так и ту, что только будет. А вот вопрос тем для блога действительно актуален.

Ниже перечислены темы, которые мы предлагаем взять за основу для вашего «боевого» журнала, с помощью которого вы противодействуете направленному против вас черному PR. Они появились как результат исследования самых популярных тем блогосферы. Можно сказать, что это универсальный набор тем, среди которых всегда можно выбрать ту, что вам больше по душе и хотя бы отдаленно стыкуется с мотивами вашей информационной войны. Возможно, вы не выберете ни одну из них, но они наведут вас на мысль о каком-то другом направлении. Помните, пожалуйста, что все чужие тексты имеют авторов, и не забывайте ссылаться на них при цитировании. Старайтесь создавать собственные тексты. По возможности делайте фотографии или видеоролики и размещайте их в блоге.

1. Хобби и способы отдыха.
2. Чай, кофе, другие напитки (их история, обзоры сортов, способы приготовления).
3. Кулинария (рецепты и способы приготовления пищи).

4. Национальные кухни (рецепты и способы приготовления пищи, а также традиции трапезы).

5. Корабли, самолеты, танки, автомобили и прочая техника (технические характеристики, фотографии, истории, моделизм).

6. Спорт (история, снаряжение, техника, биографии спортсменов, смешные или поучительные истории, собственные случаи).

7. Обзор модных мероприятий.

8. Обзор тенденций в мире моды.

9. Значки, марки, нумизматика.

10. История каких-либо стран или территорий.

11. Описание особенности работы с теми или иными интернет-сервисами.

12. Домашние любимцы – животные или растения (виды, особенности содержания, истории, связанные с ними, советы начинающим).

13. Ваши впечатления о фильмах, музыке, презентациях, выставках, аукционах – словом, обо всех местах, куда люди приходят что-либо посмотреть – ведь не все успевают это сделать, а тем, кто успел, нередко хочется обменяться мнениями с другими.

14. Мнения о прочитанных книгах, особенно новинках, – не все уже прочли их и

многие в раздумьях: что выбрать из всего многообразия на прилавках, особенно когда времени мало.

15. Дайджест о смартфонах и коммуникаторах. Помещайте туда все новинки и обзоры, которые появляются в Сети. Можно сделать примерно то же о телефонах определенной марки.

16. Путевые наблюдения и впечатления о других городах и странах, если вы имеете возможность путешествовать. Телепередачи, посвященные этой теме, десятилетиями стоят в сетке вещания.

17. Раз уж вспомнили о программах про путешествия, не уходящих из эфира десятилетиями, не забудем и о жизни диких животных.

18. Прошлое исчезнувших стран. Например, большой популярностью пользуются блоги с рассказами, фотографиями и шутками времен СССР.

19. Обзор программного обеспечения, которым массово пользуются люди (например, секреты «Фотошопа», Word, Excel, OpenOffice и т. д.).

20. Внутренняя жизнь организаций, которые у всех на слуху, но о которых мало кто информирован. Напомним, что книги Арту-

ра Хейли, рассказывающие живо и увлекательно о жизни отеля, аэропорта, автомобилестроительного завода, пользуются феноменальным успехом. А в топ-список самых цитируемых блогов входит блог о жизни одного провинциального морга. Только не переусердствуйте: как только вы не сможете обезличить место, которое описываете, и оно будет идентифицировано, у вас, скорее всего, возникнут серьезные проблемы на работе, и вы пополните список людей, которых уволили за публикации в блогах. Либо противник сможет идентифицировать вас.

21. Поддержка или, напротив, осуждение какого-либо движения. Но помните: времени на вычерпывание спама и нецензурщины от противников вашей точки зрения придется потратить много.

22. Опыт преодоления трудностей в общении с противоположным полом.

23. Опыт противостояния семейным неурядицам: как решать проблемы с детьми, родителями, супругами, родителями супругов и всеми, с кем приходится жить вместе.

24. Списки библиотек или поиск книг на всевозможные темы.

25. Помощь тем, кто учит иностранные языки либо совершенствует свои познания

в русском. Расскажите, как правильно говорить и писать по-русски, какие ошибки совершают русскоязычные в иностранном языке.

26. Фотография – заведите о ней разговор доступным языком, но на серьезном уровне.

27. События каждого дня. Если ваши друзья, когда вы им рассказываете, как прошла рабочая неделя, покатываются со смеху, то можете просто писать обо всем, что с вами происходит, в блоге. Реалити-шоу ведь тоже популярны...

28. Рассказ обо всех событиях вашей жизни, которые вам запомнились. Скорее всего, вы не одиноки в своих эмоциях. Обязательно найдутся люди, которые тоже пережили подобное или которые как раз сейчас переживают ситуацию, похожую на вашу, и нуждаются в советах.

29. Смешные стихи или частушки.

30. Красота – обзоры косметических средств, средств для ухода за волосами, тенденций в парикмахерском искусстве, диет, фитнес-клубов, соляриев, бассейнов, маникюрных кабинетов, салонов красоты.

Если совершенно нет времени на написание оригинального контента, а необходимость в нем есть, можно воспользоваться

сервисом, предлагающим купить оригинальные статьи. В таком случае авторские права переходят к покупателю, и никто без вашего разрешения и ссылки на вас как источник не сможет ваши материалы перепечатывать. Этот сервис называется Textsale и расположен по адресу: www.textsale.ru/

Продвижение «боевого» блога в поисковых машинах

Продвижение «боевого» блога в поисковых машинах имеет много общего с продвижением «мирных» сайтов, которым занимаются специалисты по поисковой оптимизации (их называют SEO, это аббревиатура от search engines optimization). Поэтому большинство рекомендаций, приведенных для «боевого» блога, могут быть применены и для продвижения «боевого» сайта.

Отличия способов раскрутки блога от способов раскрутки сайта невелики и обусловлены преимущественно двумя причинами. Во-первых, как правило, бюджет для организации противодействия атаке черных пиарщиков недостаточно большой, чтобы вы могли совершенно не ограничивать себя в тратах на виртуальную войну. А во-вторых,

блог, расположенный на общественных площадках, подобных Livejournal.com или Liveinternet.ru, имеет возможности взаимодействия с другими участниками этих площадок, недоступные традиционным сайтам, и этот фактор вы можете выгодно использовать в своих целях.

В связи с этим мы рассмотрим инструменты продвижения блогов и сайтов в Интернете, преимущественно бесплатные и доступные каждому. Мы покажем, как с помощью таких общедоступных инструментов сделать ваш блог или сайт известным поисковым машинам и продвинуть его в выдаче по тем ключевым словам или словосочетаниям, по которым вы хотели бы его продвинуть, чтобы эффективно дать отпор напавшим на вас черным пиарщикам.

Как правило, блоги и сайты, участвующие в информационной войне в бизнесе, не вступают в конкуренцию за первые страницы поисковых машин с крупными компаниями, потому что слова, по которым их поднимают в Интернете, часто связаны не с продукцией компании, а с ее названием или именами ее сотрудников. Это позволяет выполнить продвижение «боевого» блога или сайта в Интернете быстрее и с меньшими затратами,

чем при обычной борьбе за «мирные» высококонкурентные слова. Хотя продвижение технически можно выполнить по любым словам, был бы бюджет достаточно большим.

Мы не будем подробно останавливаться на таких базовых для SEO понятиях, как Page Rank (для Гугла) и Тематический индекс цитирования – ТИЦ (для Яндекса), которыми эта авторитетность измеряется. Во-первых, большинство ресурсов при противодействии черному PR в Интернете не имеют этих показателей вообще, а во-вторых, информации о них в Интернете очень много, и найти ее не составляет проблемы. Даже если вы сможете привлечь на свою сторону авторитетные ресурсы, их удельный вес почти никогда большим не будет, и не они станут определять успех ваших мероприятий. Поговорим о том, что действительно важно и подконтрольно вам при организации противодействия информационному нападению в Интернете.

Пример, показывающий раскрутку блогов и сайтов в целях противодействия информационному нападению, основан на нашей практике. Для целей раскрутки не имеет значения, какие именно ключевые слова

вам требуются в каждом конкретном случае, поэтому наш пример может быть использован с другими ключевыми словами применительно к любой теме. Мы покажем вам инструменты, которые были использованы при продвижении в выдаче поисковых машин словосочетания, которое отвечало нескольким условиям:

- отражало наши интересы в противостоянии черному PR, направленному против нас;

- не пересекалось с интересами крупных коммерческих структур, т. е. не являлось высококонкурентным словом, за которое борются SEO-специалисты многих компаний;

- имело определенный вес у поисковых машин.

В борьбе за вес словосочетания у поисковых машин нам надо было занять ведущие места в Интернете по нескольким причинам. Во-первых, оно было не таким уж редким (а значит, помимо борьбы с противником, предстояло «оттеснить» сайты, не имеющие к нему отношения, но содержащие те же слова). Во-вторых, противник приложил большие усилия, чтобы не дать нам занять первые строчки в выдаче поисковиков. Ведь речь шла о его возможности самого себя ре-

кламировать, не допуская пользователей до значительно менее позитивной правды, и тем самым не только потешить свое самолюбие, но и привлечь новых клиентов. Это достаточно типичная ситуация для информационной войны в бизнесе, поэтому мы и выбрали данный пример.

Для продвижения вашей точки зрения в информационной войне недостаточно одного-двух блогов или сайтов. Вам потребуется создать еще ряд интернет-ресурсов, поскольку Интернет обладает уникальной особенностью. Вы, вероятно, помните историю Барона Мюнхгаузена, который рассказывал, что вытащил сам себя из болота за волосы. Никто ему, само собой, не верил, поскольку в реальной жизни это невозможно. Так вот, это возможно в Интернете. Вы сами совершенно бесплатно можете создать несколько (или – в зависимости от масштабности задачи – несколько десятков или сотен) интернет-площадок, которые вытащат сами себя наверх в поисковых машинах из «болота» информационного шума.

Мы решили показать вам инструменты продвижения «боевой интернет-группировки» в поисковых машинах на примере отражения информационного нападения реаль-

ного человека. В ходе отражения атаки черного PR нами были отработаны инструменты продвижения своей точки зрения вверх в поисковиках. В работе с поисковыми машинами мы продвигали в качестве ключевых слов фамилию, имя и отчество нашего противника. Перед нами стояла задача поднять по этим ключевым словам в выдаче поисковиков информацию об оппоненте, которая рассказывала о его нелицеприятных либо и вовсе незаконных поступках. При написании этой книги мы внесли изменения в факты, имена и обстоятельства. Однако мы сохранили общие принципы похожими на те, которые были на самом деле.

Назовем нашего противника в этой книге Секретовым Секретом Секретовичем. Предположим, что через поисковые машины необходимо довести до сведения общественности его проступки.

1. Господину Секретову очень хотелось написать собственную книгу, но он не умел. Тогда он взял всемирно известную книгу Петра Павловича Ершова «Конек-Горбунок», выпущенную крупным издательством, стер с обложки имя П. П. Ершова и написал на обложке свое имя: «Секретов С. С», а затем дополнительно приписал, что это его автор-

ское произведение.[49]

2. В детстве Секретов был единственным в своем дворе обладателем ведерка и совочка. Он копал в дворовой песочнице ямки, называл их пещерами и показывал дворовой детворе. Секрет хотел стать спелеологом и исследовать пещеры профессионально. Но когда он вырос, у него не получилось делать эту работу хорошо. Тогда он стал гулять по настоящим пещерам неподалеку от входа, рассказывая всем, какие приключения якобы с ним там происходили. Однако он не смог избавиться от мысли, что все спелеологи-профессионалы украли его идею исследовать пещеры. Секрет стал думать, что спелеологи должны платить ему деньги. Он стал нападать на спелеологов в Интернете и обвинять их в различных им самим выдуманных прегрешениях.

3. В раннем детстве малыш Секретик по просьбе девочек лепил в своей детской песочнице куличики. Секрет Секретович считает своим по праву все, что попадает в поле его зрения. Поэтому, когда он вырос, стал пытаться заявить свои права на слово «кулич» и запатентовать их. И хоть никто так и не разрешил патентовать права на куличи, Секрет Секретов все равно считал все кули-

чи в мире своими, а всех, кто использовал куличи, не спросив его разрешения, – злодеями.

А человека, от имени которого производилась раскрутка блогов и сайтов, пускай зовут в этой книге Спелеолог.

Тогда контентом наших интернет-ресурсов должна была стать – и стала – информация об этих проступках Секретова, снабженная документальными подтверждениями, свидетельствами очевидцев, комментариями экспертов. А продвижение блогов и сайтов, задействованных в отражении атаки черного PR, производилась по словосочетанию «Секретов Секрет Секретович».

При правильной раскрутке после ввода этого ключевого словосочетания в поисковые машины пользователь Интернета видел информацию с наших ресурсов со ссылкой на первоисточник.

ВНИМАНИЕ! Имена Секрет Секретович Секретов и Спелеолог в настоящей книге вымышленные. Они не имеют никакого отношения к реальным людям, носящим такие имена, если такие люди реально существуют. Книга уважаемого писателя П. П. Ершова «Конек-Горбунок» также взята для иллюстрации, поскольку она известна большинству

читателей. Информации о фактах замены имени П. П. Ершова на имя Секретова С. С. в реальной жизни у нас нет.

Давайте рассмотрим базовые принципы, которые мы должны соблюсти, чтобы достичь желаемого результата. И сразу договоримся: в предложенных нами мероприятиях надо соблюдать меру. Как говорится, пересоленный суп ничуть не лучше недосоленного. Если утратить чувство меры, применяя предложенные в этой книге приемы, то вместо раскрутки ваших ресурсов в поисковых системах вы будете исключены из них на время или насовсем за поисковый спам. Чувство меры – величина неконкретная. Просто смотрите, как выглядит текст с позиции обычного человека, можно ли его еще считать выдержанным с литературной точки зрения или нет. Исключение составляют ситуации, когда вам надо реагировать на нападение немедленно. Тогда, как мы уже говорили, может потребоваться создать первую волну сайтов (блогов) – «брандеров», которые быстро поднимутся в поисковых машинах, а затем «погибнут», оказавшись вычеркнутыми из поисковиков. «Брандеры» и на самом деле типичный поисковый спам, но, к сожалению, любая война всегда лишена

эстетики, и виртуальная – не исключение. Но второй и последующие эшелоны ваших интернет-ресурсов все равно должны соответствовать принципам «мирной» оптимизации сайтов, чтобы не быть исключенными из поиска и надолго занять господствующее положение над противником в результатах выдачи поисковых машин.

Поисковые машины постоянно стремятся, чтобы пользователь получал информацию, которая максимально соответствует его потребностям. Это их бизнес, это привлекает к ним пользователей и рекламодателей, на этом поисковики и сосредоточивают свои усилия.

Давно минули те времена, когда поисковая машина определяла важность документа, просто пересчитывая количество ключевых слов на странице. И те времена, когда можно было написать зелеными буквами на фоне того же цвета ключевые слова, тоже давно прошли. Если на странице обнаруживается текст, видимый паукам, но невидимый людям, то за это наказывают, невзирая на лица: примером может быть один из сайтов BMW, подвергшийся в свое время наказанию за то, что содержал текст, который для пауков и людей был различным. Поэто-

му, читая написанное ниже, вы должны постоянно помнить: чтобы достичь долговременного успеха, ваш текст должен нравиться и людям, и паукам. А значит, он должен обязательно быть осмысленным, нести в себе какую-то информацию, а не представлять собой бессмысленный набор слов.

Ниже перечислены основные принципы, соблюдение которых помогает подняться в выдаче поисковых машин.

1. На странице должно быть по возможности много ключевых слов.

2. Ключевые слова должны быть в первом абзаце текста.

3. Должны быть гиперссылки с блогов с сайтов на ваш интернет-ресурс.

4. В тексте гиперссылок должны содержаться ключевые слова (их еще называют якорными).

5. Сайты и блоги, которые ссылаются на ваш интернет-ресурс, должны содержать в своих текстах ключевые слова (т. е. быть для вашего интернет-ресурса тематическими).

6. Желательно, чтобы сайты и блоги ссылались друг на друга «по кругу».

7. Желательно, чтобы страницы вашего «боевого» сайта или блога также ссылались друг на друга.

8. Возраст вашего сайта или блога работает в вашу пользу: чем старше он становится, тем выше его авторитет у поисковых машин.

9. Ваш сайт или блог не должен давать ссылки на спамерские ресурсы (в том числе и на ваши собственные ресурсы первой волны контратаки, если вы задействовали там «брандеры»).

10. Ключевые слова должны быть в заголовке страницы.

11. Ключевые слова должны быть в идентификаторах рисунков.

Приведение текста в соответствие с этими принципами (при обязательном сохранении осмысленного текста!) и составляет большую долю работы оптимизатора сайтов или блогов.

Давайте разберем эти пункты подробнее.

1. На странице должно быть относительно много ключевых слов. Нередко встречается прием, когда в текст максимально часто вставляются ключевые слова, если они подходят по смыслу. Этот подход достаточно очевиден даже для неподготовленного пользователя. Это не имеет ничего общего с тем, как поступают спамеры, бессмысленно вставляя в любой текст ключевые слова (каждый пользователь Интернета встречал-

ся с такими сайтами, где, например, в текст Пушкина вставлены через каждые три слова какие-то посторонние слова, к тексту никакого отношения не имеющие). Повторимся, поскольку это очень важно: материал, размещенный вами на сайте или в блоге, обязательно должен быть осмысленным.

Ниже, в таблице 1, приведены для сравнения два текста. Первый является ответом Спелеолога на агрессию (он был размещен в первом сообщении блога, чтобы сообщение так и оставалось первым, которое увидят читатели этого журнала, его можно датировать далеким будущим). Второй представляет собой тот же текст, но переработанный так, что в нем слова «Секретов Секрет Секретович» употребляются часто, однако уместно, пусть даже несколько в ущерб литературному стилю.

Таблица 1. Сравнение двух текстов.

Исходный текст, не учитывающий необходимости в поисковой раскрывке	Текст с большим содержанием ключевого словосочетания
Новая буря в стакане воды. Мой оппонент в спелеологии — Секретов Секрет Секретович — опять «преславился». Не особо заморачиваясь, он показательно «сжег чучело врага»: объявил, что спелеологи, и я в том числе, повинны во всех его проблемах и неудачах. Реагировать на это и искоренение мне совершенно не хочется.	Новая буря в стакане воды. Мой оппонент в спелеологии — Секретов Секрет Секретович — опять «преславился». Не особо заморачиваясь, Секрет Секретович Секретов показательно «сжег чучело врага»: сбывавил, что спелеологи, и я с том числе, повинны во всех его проблемах и неудачах. Реагировать на это

Продолжение табл. 1.

Исходный текст, не учитывающий необходимости в поисковой раскрутке	Текст с большим содержанием ключевого словосочетания
но вроде бы надо. Ладно, отреагирую. Все же чужик старался — небылицы придумывал и факты подтасовывал. Подобные наезды — это традиционная и любимая забава Секрета Секретовича, известная участникам рынка спелеологии и кулинарии как этакий «личный пунктик», «милая странность» господина Секретова. Она имеет сложные, порой необъяснимые правила. Про людей, которые ему лично неприятны, Секретов Секрет Секретович обычно пишет отдельное авторское произведение. И называет его странно — «черным списком». Чего только не придумают некоторые, чтобы не утратить окончательно известность. Потрясла меня в связи с этим прозорливость Антона нашего Палыча Чехова. Великий писатель! Он объяснил истинные причины поведения типажа Секретова Секрета Секретовича много лет назад в очень коротком и смешном рассказе «Радость». А то я просто терялся в догадках относительно такой активности господина Секретова. А еще я думаю, что виной всему мокро-холодный ужас конкурента, осознавшего сальдо. Ведь человек трудился два с половиной года, а создать за это время смог только одно эпохальное произведение — «Черный список спелеологов и кулинаров». Мне кажется, что сочинения моего оппонента — закономерная реакция	шкворчание господина Секретова Секрета Секретовича мне совершенно неохота, но вроде бы надо. Ладно, отреагирую. Все же мужик старался — небылицы придумывал и факты подтасовывал. Подобные наезды — это традиционная и любимая забава Секретова Секрета Секретовича, известная участникам рынка спелеологии и кулинарии как этакий «личный пунктик», «милая странность» господина Секретова Секрета Секретовича. Она имеет сложные, порой необъяснимые правила. Про людей, которые ему лично неприятны, Секретов Секрет Секретович обычно пишет отдельное авторское произведение. И называет его Секретов Секрет Секретович странно — «черным списком». Чего только не придумают некоторые, чтобы не утратить окончательно известность. Потрясла меня в связи с этим прозорливость Антона нашего Палыча Чехова. Великий писатель! Он объяснил истинные причины поведения типажа Секретова Секрета Секретовича много лет назад в очень коротком и смешном рассказе «Радость». А то я просто терялся в догадках относительно такой активности господина Секретова. А еще я думаю, что виной всему мокро-холодный ужас конкурента, осознавшего сальдо, как осознал его Секретов Секрет Секретович. Ведь человек трудился два с половиной года, а создать за это время смог

Исходный текст, не учитывающий необходимости в поисковой раскрутке	Текст с большим содержанием ключевого словосочетания
субъекта, годами совершающего необычный поступок, который мы отчасти упоминали. Как показала практика, выделяется господин Секретов Секрет Секретович тем, что обладает «эффектом покрашенной скамейки»: вовлекает в свои личные проблемы практически всех, с кем контактирует — поручителей, работодателей, знакомых, слушателей... В общем, в пору писать: «Осторожно Окрашено!» С уважением, Спелеолог	только одно эгохальное произведение — «Черный список спелеологов и кулинаров». Мне кажется, что сочинения моего оппонента — Секретова Секрета Секретовича — закономерная реакция субъекта, годами совершающего необычный поступок, который мы отчасти упоминали. Как показала практика, выделяется господин Секретов Секрет Секретович тем, что обладает «эффектом покрашенной скамейки»: вовлекает в свои личные проблемы практически всех, с кем контактирует — поручителей, работодателей, знакомых, слушателей... В общем, в пору писать: «Осторожно Окрашено» С уважением, Спелеолог

Чтобы не перегружать книгу, пошагово объясняя каждый вариант, мы объединили его еще с одним с приемом, который используется оптимизаторами сайтов, когда надо не просто поднять в выдаче материал по нужным ключевым словам, но еще наглядно показать некие факты, подтверждающие точку зрения составителя текста.

Предположим, наша задача – обратить внимание целевой аудитории на факт удивительного внешнего совпадения двух книг – сказки П. П. Ершова «Конек-Горбунок» и произведения «Конек-Горбунок», автором

которого объявил себя господин Секретов С. С.

Достаточно включить ссылку на такой факт внутрь гиперссылки и объединить его с текстом, вставленным в ее видимую часть, чтобы обеспечить требуемый эффект. Каждый пользователь Интернета знает, что человек, дочитавший до текста гиперссылки, может перейти по ней и увидеть документы, которые в текст не включены, но подтверждают мнение его автора.

В приведенном ниже примере в правой колонке словосочетание «Секретов Секрет Секретович» оказывается одновременно и гиперссылкой на презентацию его «авторского произведения». Такие слова для наглядности дополнительно выделены в тексте подчеркиванием.

В реальной практике этот эффект часто достигается за счет публикации большого количества связанных по смыслу материалов на разных страницах одного ресурса, со взаимными ссылками друг на друга.

Мы выделили ключевое словосочетание жирным шрифтом, чтобы было лучше видно, насколько чаще оно встречается во втором случае по сравнению с первым.

Как видите, слева оно встречается четыре раза, а справа —десять, причем в одном из этих десяти случаев оно является гиперссылкой на страницу с документами.

Материал, содержащийся в правой колонке, и стал первым сообщением в блоге, с которого началось его продвижение. Это было началом контратаки против черного пиарщика, которая затем переросла в масштабное контрнаступление.

Достаточно подробно о написании текстов с учетом требований поисковой оптимизации рассказано в книгах И. Ашманова, А. Иванова «Продвижение сайта в поисковых системах».[50] и Н. В. Евдокимова «Основы контентной оптимизации»[51] Обе написаны живым языком и на многочисленных примерах показывают, как надо писать тексты с учетом предпочтений поисковых машин.

2. Должны быть гиперссылки с сайта на сайт. Не загружая читателя терминами, скажем лишь, что поисковые машины считают: если на сайт ссылаются, значит, он полезен и его надо поднять в выдаче повыше. И чем больше ссылок на него с других ресурсов, тем он лучше. Добросовестные люди делают сайт с полезным контентом, который нужен

людям, и за счет этого он приобретает ссылки – все равно что один человек советует другому хорошую книгу или хорошего парикмахера.

Покажем, как гиперссылка выглядит «изнутри».

Например, гиперссылка, которая в исходном коде страницы выглядит следующим образом: `<a href="http://ci-razvedka.ru/"> Сайт Юшука Евгения Леонидовича. Конкурентная разведка </a>` будет в окне браузера выглядеть как надпись: *Сайт Юшука Евгения Леонидовича. Конкурентная разведка* и вести будет на адрес: <http://ci-razvedka.ru/>

3. В тексте гиперссылок должны содержаться ключевые слова. Как мы уже говорили, хорошо, когда гиперссылки извне на сайт существуют в принципе. Но эффект усиливается, если в тексте гиперссылок будут содержаться те же слова, что и на сайте, на который они ведут. Это так называемые якорные слова.

То есть для того, чтобы поднять на первую страницу текст по запросу «спелеолог», требуется сделать его текстом гиперссылок.

Например, гиперссылка, помогающая поднять в выдаче точку зрения Спелеолога о Секрете Секретовиче Секрете на первую

страницу результатов по запросам «Спелеолог», «Секретов Секрет Секретович» и «Черный список» может выглядеть так: **Спелеолог. Ответ на «черный список», автор которого Секретов Секрет Секретович.**

4. Сайты и блоги, которые ссылаются на ваш интернет-ресурс, должны содержать в своих текстах ключевые слова.

В борьбе поисковых машин против поисковых спамеров однажды наступил момент, когда последние стали использовать ссылки на свой сайт из сотен и даже тысяч каталогов. Эти ссылки покупались и продавались, они позволяли поднять в выдаче даже не очень качественный сайт в ущерб более тематическим, но неоплаченным ресурсам. Для того чтобы бороться с этим явлением, поисковики стали обращать внимание на то, какие слова содержатся на ссылающемся ресурсе. Они стали присваивать больший вес тематическим ссылкам. Поэтому желательно, чтобы в текстах сайтов и блогов, которые ссылаются на ваши ресурсы, присутствовали ключевые слова. Впрочем, ваши «боевые» сайты и блоги неизбежно и так их содержат.

5. Желательно, чтобы сайты ссылались друг на друга «по кругу». До недавнего вре-

мени пауки воспринимали любую ссылку с одного сайта на другой примерно одинаково, ориентируясь разве что на авторитетность самого ссылающегося ресурса у пользователей Интернета. Но затем поисковые спамеры (это люди, которые заинтересованы в продвижении своей рекламы через поисковые машины любой ценой, в отличие от оптимизаторов сайтов, которые преследуют те же цели, но делают это в рамках неписаных правил, принятых в Интернете) начали запускать так называемые программы-линкаторы, которые создавали огромное количество ссылок сайтов друг на друга, и люди, которые продвигали свои ресурсы за счет создания качественного содержимого, не могли соревноваться с этими роботами в скорости создания гиперссылок.

Тогда пауки поисковых машин стали вводить понижающие коэффициенты рейтингу взаимных ссылок сайтов друг на друга.

Оптимизаторы сайтов ответили созданием «колец из сайтов» (когда сайт А ссылается на сайт В, тот – на сайт С, а сайт С уже на сайт А, и при этом взаимных прямых ссылок на сайтах нет).

Кроме того, началось и приобрело размах создание сайтов-сателлитов. На простейшем

примере это выглядит так, что все сайты (сателлиты) ссылаются друг на друга, однако есть один, два или более сайтов, которые ни на кого не ссылаются, получая при этом ссылки со всех остальных сайтов, формально самостоятельных, но объединенных общим замыслом поискового оптимизатора или спамера. Эти-то «получатели ссылок» и поднимаются выше всех.

Образно говоря, можно представить, как множество слабых людей взяли в руки вилы с длинной ручкой и одновременно начали поднимать тяжелый клок сена, неподъемный для одного человека.

Или можно провести аналогию с увеличительным стеклом, которое собирает отдельные слабые солнечные лучи в точку, в результате чего температура в этой точке поднимается очень высоко.

Механизм, позволяющий увидеть внешние гиперссылки, существует. Это оператор языка запросов Link, который еще недавно был во всех основных поисковых машинах. Теперь многие системы (но не все и не для всех сервисов) закрыли к нему доступ.

Существуют сайты, позволяющие без знания языка запросов поисковых машин посмотреть, кто ссылается на сайт или блог.

Зайдите на страницу www.be1.ru/services/stat и введите в служебное окошко адрес вашего блога или сайта. В открывшемся окне появится информация о том, какие из его страниц проиндексированы различными поисковыми машинами и какие ссылки ведут извне на ваш ресурс (рис. 22).

Обычно период попадания правильно сделанного интернет-ресурса в поисковые машины занимает от 1 до 14 дней, хотя это в значительной степени зависит от того, как технически сделан этот ресурс, как он связан гиперссылками с другими ресурсами и где размещен. Соответственно, этот период может колебаться в значительном диапазоне. Очень отличается и скорость попадания в Интернет новой информации, размещенной на разных блогах и сайтах. Например, слова, размещенные на форуме разведчиков (www.it2b-forum.ru), где обсуждаются вопросы конкурентной разведки и служб безопасности предприятий, могут быть видны в поисковых машинах уже через 7—10 часов.

Для эффективного противодействия противнику в информационной войне вам нужно создавать дополнительные блоги или страницы сайтов, которые будут содержать перепечатки ваших текстов и давать ссылки

на ваш блог как источник информации. Безусловно, лучше, если сразу же ссылку на вас станут давать посторонние люди. Однако для того чтобы это произошло, недостаточно иметь хороший, интересный контент. Ведь даже при мирной раскрутке сайта или блога для того, чтобы на вас стали давать ссылки, о вас сначала должны узнать. А при контратаке на черных пиарщиков многие, кто к вам хорошо относится, могут просто побояться попасть под удар черного PR, если засветятся участием в информационной войне, пусть даже просто давая на вас ссылки. Хотя, если вам удастся сделать свое противостояние интересным для достаточно большой группы людей, страх значительно уменьшится, и ссылки вы получите достаточно быстро, притом в большом количестве. Поскольку отражать нападение черных пиарщиков приходится, когда оно произошло, а не когда вам это удобно, то нет возможности ждать, когда на ваши ресурсы дадут ссылки. Надежнее дать их со своих же или с дружественных вам ресурсов. Продвигайте самостоятельно сайты и блоги, выражающие вашу точку зрения, не надеясь на помощь извне, и со временем вы увидите, что у вас появится множество сторонников.

Не рассчитывайте на помощь, но принимайте ее с благодарностью.

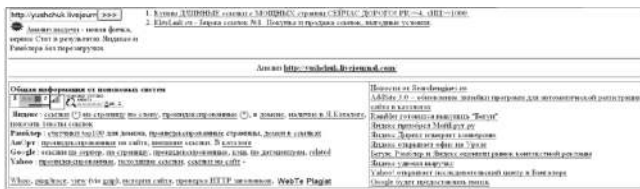


Рис. 22. Пример результатов исследования блога yushchuk.livejournal.com/ на сайте be1.ru.

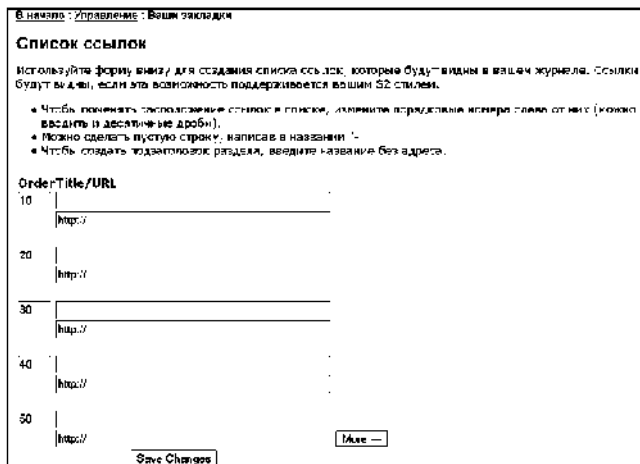


Рис. 23. Страница для ввода постоянных ссылок в Живом Журнале.

Недостаточно давать ссылки на свои блоги и сайты только в тексте сообщения. Надо поставить также постоянные гиперссылки на них со своих блогов в Живом Журнале. Для этого необходимо в блоге в Живом Журнале войти в профиль пользователя (он может называться также «User info» или «Личная информация») и пройти по ссылкам «Журнал – Настройка – Your link list». На открывшейся странице вы можете проставить 10 гиперссылок на нужные вам ресурсы. Эти гиперссылки автоматически будут присутствовать на всех страницах вашего сайта. Страница, на которой можно ставить постоянные гиперссылки, видна на рис. 23.

По умолчанию там всего пять строк и, чтобы получить дополнительные строки для ссылок, надо нажать кнопку «More». Когда все необходимые ссылки будут введены, нужно сохранить эти изменения, нажав кнопку «Save changes». Блоги, сделанные вами для поддержки ваших основных «ударных» блогов и сайтов, должны ссылаться друг на друга, и желательно, как мы уже говорили, – по кругу, так как прямые ссылки имеют очень сильный понижающий коэффициент, а иногда и вообще не учитываются. То есть ситуация, когда блог А ссылается

на блог В, а тот в свою очередь встречно ссылается на блог А, хуже, чем когда блог А ссылается на блог В, тот – на блог С, а блог С – на блог А.

6. Желательно, чтобы страницы блога также ссылались друг на друга (к страницам сайтов это относится в полной мере).

В блогах предусмотрены различные стили оформления. Некоторые из них позволяют видеть оглавление блога, которое автоматически дублируется на каждой странице справа, слева или вверху относительно текста. Если же вы пользуетесь стилем оформления, в котором такого оглавления нет, то его желательно поставить на страницы блога самостоятельно: просто разместить гиперссылки, якорные слова которых – названия статей на страницах блога, а сами гиперссылки при этом ведут на эти страницы. С сайтами ситуация аналогичная. Некоторые из них сконструированы так, что на них оглавление присутствует на каждой странице, тогда как на других этого нет и лучше проставить такое оглавление на каждой странице вручную.

Возраст вашего блога работает в вашу пользу. Действительно, чем дольше ваш ресурс присутствует в Интернете, тем больше

доверия к нему испытывают поисковые машины. Этот эффект хорошо виден на примере гостевых книг заброшенных сайтов, висящих в Сети с конца 1990-х годов. Тексты, размещенные на таких площадках, занимают высокие позиции в выдаче поисковых машин. Со временем ваш блог или сайт будет занимать более высокие позиции в поисковых машинах. Правда, надо сказать, что время это исчисляется годами, поэтому не в каждой информационной войне вы сможете воспользоваться указанным преимуществом.

Ваш блог или сайт не должен давать ссылки на спамерские ресурсы. Поисковые машины не любят спамеров, потому что те ставят под угрозу само существование поисковых машин. Ведь если люди вместо реальной информации станут получать в поисковиках только рекламу, они просто перестанут ими пользоваться. Если спамерский ресурс ссылается на ваш сайт или блог, вам это, может быть, ничем и не угрожает, потому что иначе все конкуренты уже давно подавляли бы друг друга таким образом, например, просто открывали бы спамерские и порносайты и ставили бы оттуда ссылки на противника. Поисковики понимают, что вам не

под силу запретить кому-либо ставить на вас ссылки. Но вот если вы сами ссылаетесь на спамерские ресурсы, вас вполне могут наказать – ведь разместить на странице блога или сайта гиперссылку случайно практически невозможно. Исключения составляют комментарии вашего блога, где любую информацию может оставить каждый желающий, если не принять соответствующих мер. Но в ваших силах контролировать комментарии вплоть до полного их запрета, поэтому многие специалисты отмечают, что за ссылки на спамеров в комментариях вашего блога вас также могут наказать. Уделите контролю за комментариями в ваших блогах пристальное внимание или просто запретите комментирование – для всех или для тех, кто не входит в список ваших друзей.

9. Ключевые слова должны быть в заголовке страницы. Когда вы подбираете заголовки для страницы, постарайтесь выполнить два условия: во-первых, ключевые слова должны в принципе в нем присутствовать, а во-вторых, их удельный вес должен быть достаточно большим. Это опять компромисс между тем, что делается для поисковых машин, и тем, что делается для чело-

века.

Поэтому идеальными для ключевых слов «Секретов Секрет Секретович», с точки зрения поисковых машин, будет заголовок «Секретов Секрет Секретович».

А для людей, возможно, был бы хорош заголовок: «Посмотрите на обложку двух книг „Конек-Горбунок“! Вы не находите, что Секретов Секрет Секретович нагло стер имя П. П. Ершова и написал свое? Позор Секретову! Плагиату не место в нашем обществе! Заклеймим плагиаторов позором и не будем подавать им руки при встрече! И никакие оправдания не могут плагиаторам помочь, недаром за плагиат наказывают в соответствии с Уголовным кодексом!»

На наш взгляд, компромиссным вариантом был бы такой: «Секретов Секрет Секретович и „Конек-Горбунок“. Плагиат Секретова Секрета Секретовича».

Заголовок страницы – это та ее часть, которая находится в самом верху, в браузере, на синем фоне (для Windows XP). Если в название блога и в название конкретной статьи вы включите ключевые слова, то как раз получите требуемый эффект.

Заголовок страницы, получившийся в результате: «Секретов Секрет Секретович – Се-

кретов Секрет Секретович и „Конек-Горбунок“. Плагиат Секретова Секрета Секретовича». Его можно увидеть на рис. 24.

Название сообщения: «Секретов Секрет Секретович и „Конек-Горбунок“. Плагиат Секретова Секрета Секретовича». Текст сообщения: «А здесь располагается непосредственно текст статьи».

Название журнала – Секретов Секрет Секретович.

10. Ключевые слова должны быть в идентификаторах рисунков. Это очень серьезный, хотя и неочевидный на первый взгляд инструмент продвижения блога или сайта в поисковых системах. Дело в том, что поисковые машины, как мы уже говорили, читают исходный код страницы, а не только ее текст, видимый людям. Когда на странице размещается рисунок, у него предусмотрен раздел тега «alt», в который заключается текст. Этот текст показывается пользователям, когда рисунок по каким-либо причинам не может быть загружен (например, если в браузере пользователя отключен просмотр изображений). В принципе логика верна: если вместо рисунка показан текст, значит, этот текст имеет самое непосредственное отношение к изображению. Если в этом теге

прописать ключевые слова, то страница, содержащая такой рисунок, будет считаться более релевантной запросу.

Вот вариант написания тега, в разделе «alt» которого содержатся ключевые слова «Секретов Секрет Секретович»: ``

Здесь `src="http://ci-razvedka.ru/sekretov.jpg"` – источник самого изображения, а `alt="Секретов Секрет Секретович"` – текст, который появляется вместо изображения, когда загрузка изображения не удалась.

Френды (друзья) в блогах

Как уже неоднократно обсуждалось, особенность современной части Интернета, которую называют Web 2.0 – его интерактивность. Создатели концепции Web 2.0 считают, что только сами люди могут определить, что на самом деле им надо, и самостоятельное решение этого вопроса – неотъемлемое право пользователя Интернета. Процедура добавления пользователя в друзья на блоговых площадках максимально упрощена: чтобы кого-то добавить в друзья («зафрендить»), надо всего лишь войти под своим ни-

ком в свой блог, выйти на страницу того блога, который вас интересует (или зайти в профиль пользователя, которого вы хотите добавить в друзья) и нажать кнопку «Добавить в друзья». Больше ничего делать не требуется. Гиперссылка с вашим ником появится в том блоге, который вы записываете в друзья, а гиперссылка с ником владельца того блога – в вашем. В случае отражения информационного нападения взаимная запись в друзья блогов, входящих в состав вашей «боевой» группировки, позволяет обеспечить перекрестные ссылки этих блогов друг на друга и тем самым повысить эффективность каждого отдельного блога этой группировки. Однако, как мы уже сказали ранее, иногда из соображений конфиденциальности, чтобы не раскрывать точный состав участников группы по противодействию черному PR в Интернете, приходится жертвовать преимуществами, которые дают взаимные ссылки, и не «френдить» своих соратников. Пользователи могут создавать в крупных блогах уровня Живого Журнала виртуальные сообщества по интересам. Мы уже говорили, что при заполнении профиля пользователя человек, открывающий блог в Живом Журнале, отмечает сферу своих инте-

ресов. Если в Интернете еще хотя бы кто-то один выбрал такие же интересы, название этого интереса превращается в гиперссылку. Достаточно по ней пройти, чтобы открылся огромный мир единомышленников. Эти люди не знали о существовании друг друга до того момента, пока не создали свой блог, а после его создания получили возможность общаться между собой. В ситуации информационной войны вы можете благодаря этой опции найти людей, которые интересуются темами информационной войны, продвижения сайтов в поисковых системах, PR, негативных PR-технологий в различных вариантах, борьбы с плагиатом, мошенничеством, воровством или какими-то другими явлениями, которые вы считаете созвучными в той или иной степени теме вашей информационной войне. Попробуйте сформулировать, по каким интересам еще можно поискать единомышленников, затем посмотрите их блоги, чтобы понять, нравятся вам эти люди в качестве возможных соратников или нет. Изучая их блоги, смотрите как на контент, так и на список их друзей.

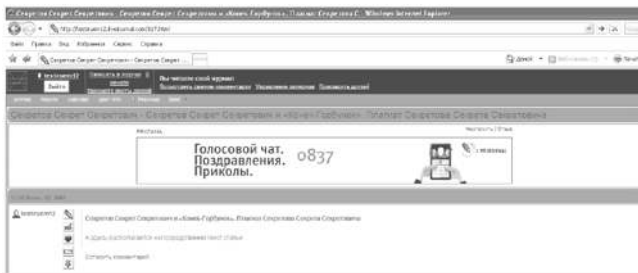


Рис. 24. Страница в блоге, имеющим в качестве названия ключевые слова, при размещении статьи, содержащей ключевые слова в названии.

Вы можете записать в друзья людей, имеющих общие с вами интересы, блоги которых вам понравились. Они получают об этом уведомления и, скорее всего, придут посмотреть на ваш блог. Кто-то решит записать вас к себе в друзья, чтобы читать ленту сообщений вашего блога. Часть этих людей поделится информацией о вас со своими друзьями. Так круг ваших соратников увеличится. А может быть, и будет перепечатана на дополнительных интернет-площадках информация, отражающая вашу точку зрения.

Сообщества в блогах и их роль в противодействии черному PR

Автор блога может не ограничиваться созданием никак не оформленного сообщества со своими друзьями и организовать полноценное сообщество, имеющее собственный адрес в Интернете. Это еще один блог, в котором пишут люди, объединенные какими-либо общими интересами и присоединившиеся к организованному сообществу. Процедура присоединения к сообществу определяется его создателями. В некоторые сообщества может вступить любой желающий, не спрашивая ни у кого согласия на вступление, тогда как на вступление в другие требуется подать заявку и получить разрешение. Заявка подается очень просто: надо войти в свой блог под своим ником, зайти на страницу сообщества и нажать кнопку «Присоединиться». После присоединения к сообществу вы получаете возможность писать сообщения не только в свой блог, но и в блог сообщества. Ваши сообщения в блоге сообщества будут содержать ваш ник, который является гиперссылкой на ваш журнал.

Благодаря сообществам вы получаете дополнительных тематических посетителей своего блога. Ведь люди, которые приняли решение перейти по гиперссылке на ваш блог, тем самым уже проявили интерес к на-

писанному вами и хотят найти что-либо еще по интересующей их и вас теме. Для создания сообщества надо в своем профиле пользователя пройти по гиперссылкам «Сообщества – Создать новое» (рис. 25).

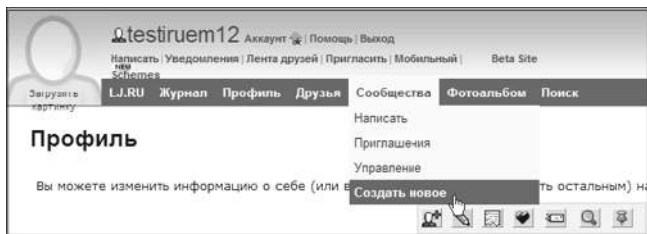


Рис. 25. Создание нового сообщества в Живом Журнале

А вот что говорится о создании сообщества на Liveinternet:

Сообщество – это по сути тот же дневник, который нужно сначала точно так же зарегистрировать и при желании настроить внешний вид по своему вкусу. Для того чтобы дневник стал сообществом, надо в его настройках, на вкладке «Изменить ваши предпочтения», поменять тип дневника с **личный дневник на открытое сообщество или закрытое сообщество**.

Главное отличие сообщества от дневника в том, кто имеет право добавлять туда сообщения. Если в личный дневник пишет толь-

ко хозяин дневника, то в сообщество могут писать многие. Кто именно – зависит от типа сообщества.

В **закрытое сообщество** имеют право писать только те, кто находится в списке друзей этого сообщества. Таким образом, создатель сообщества, составляя этот список, задает тех, кто участвует в его работе. Каждый участник закрытого сообщества имеет право редактировать свои записи; регистратор сообщества авторизовавшись под именем сообщества, имеет право редактировать или удалять любую запись в сообществе.

В **открытое сообщество** имеют право писать только те, кто добавил это сообщество в свой список друзей, став его постоянным читателем. Таким образом, любой человек (кроме тех, кто занесен в игнор-лист данного сообщества), став постоянным читателем, может добавить туда сообщение, независимо от воли создателя сообщества. Каждый имеет право редактировать свои сообщения. Те, кто состоит в списке друзей открытого сообщества, **имеет право модератора** в этом сообществе, то есть право редактировать и удалять сообщения и комментарии кого бы то ни было.[52]

С технической точки зрения, эффективность работы системы френдов (друзей) как применительно к блогам отдельных людей, так и блогам сообществ основана на гиперссылках. Когда участник Живого Журнала записывается в сообщество или допускается в друзья к кому-либо в пределах Живого Журнала, на странице обоих друзей появляется ник друга. И хотя взаимные ссылки нейтрализуются, тем не менее, по мнению многих специалистов, происходит это не полностью. А главное – пауки поисковых машин смогут посетить страницы обоих блогов с большей вероятностью, и индексация этих блогов поисковиками, возможно, станет лучше.

Этот ник для человека выглядит как текст гиперссылки (он выделен цветом, подчеркнут сплошной чертой и при наведении на него курсора тот меняет форму со стрелки на «ладошку»). И он на самом деле является гиперссылкой. Например, ник **yushchuk** в Живом Журнале, если посмотреть на него в исходном коде страницы, представляет собой гиперссылку такого вида: `<a href="http://yushchuk.livejournal.com/"_fcksavedurl="http://yushchuk.livejournal.com"><strong>yushchuk</strong></a>`

Ник **liveuser** – автора лучшего руководства по поиску через Яндекс Дениса – таков:
liveuser

Вот почему, если люди в блогах записывают друг друга в друзья, это способствует росту популярности обеих «дружащих сторон».

Каждый, кто не хочет видеть кого-либо в числе своих друзей, может в любой момент вычеркнуть его из списка.

Практически все сообщества модерироваться, и доступ в них невозможен без согласия людей, стоящих на страже того, чтобы сообщества получали только интересующую их информацию. Пытаясь войти в модерлируемое сообщество, вы отправляете модератору запрос с просьбой включить вас в члены этого сообщества. Модератор получает по электронной почте письмо с вашим запросом. В случае положительного решения вы будете автоматически уведомлены об этом также по электронной почте. Процедура зачисления в сообщество всецело зависит от загруженности модератора и может занимать от нескольких минут до нескольких дней.

Таким образом, сообщества – это оформленное созданием отдельного блога объединение единомышленников, имеющее коллективный блог, в который может писать любой член сообщества. Для получения преимущества в информационной войне в Интернете важно присоединиться к максимально большому количеству сообществ на вашей площадке блогов.

Комментарии в блогах как инструмент отражения информационного нападения

Мы уже отмечали, что каждый раз на той странице, где размещается комментарий зарегистрированного пользователя, появляется ник-гиперссылка, которая работает в интересах обоих – и того, кто комментирует, и того, кто это делает.

В результате получается высокая ссылочность, причем созданная именно людьми, а не роботами-линкаторами. Это Web 2.0 и считает самым важным в Интернете.

Однако, помимо технической пользы комментариев, существует и социальная, или «человеческая», польза. Когда вы комменти-

руете чей-то блог, ваш комментарий читают все, кто участвуют в дискуссии. Люди читают ваши мысли, видят ваш аватар (напомню: это небольшая картинка, расположенная рядом с ником). Если вы становитесь им интересны, они кликают мышкой по вашему нику и переходят в ваш блог. Если им понравится то, что написано в вашем блоге, они добавят вас в список своих друзей и, возможно, подпишутся на чтение новостей вашего блога.

Для раскрутки блога, призванного довести до общественности вашу точку зрения о противнике, полезно оставлять комментарии на хорошо посещаемых площадках. Правда, надо учитывать, что хорошо посещаемыми нередко оказываются те площадки, на которых идет горячая (иногда просто раскаленная) дискуссия, в которой участвуют две или более непримиримо враждующие группы людей. Встав на чью-то сторону, вы неизбежно навлечете на себя гнев противостоящей группировки, и в результате ваш блог может стать объектом массового негативного комментирования. Как говорят некоторые блоггеры, «будете вычерпывать негативные комментарии ведрами». Однако пауки поисковых машин активно посещают подобные

«горячие» площадки, многократно переходя на них по гиперссылкам, которыми являются ники пользователей. Да и сторонники вашей точки зрения могут написать не меньше позитивных комментариев, чем враги – негативных. В общем, если у вас есть желание тратить время на словесные сетевые баталии, то вы получите развлечение, массу новых внешних ссылок, огромное количество мусора, который надо будет удалять, и некоторое количество новых читателей.

Найти самые обсуждаемые в данный момент темы несложно. Для этого достаточно перейти на главную страницу блогов Яндекса www.blogs.yandex.ru/ Там слева вверху размещен список тридцати самых популярных записей. Первые пять видны пользователю непосредственно на первой странице, а остальные двадцать пять появляются в выпадающем окне. На момент написания книги список первых пятнадцати сообщений выглядел следующим образом:

Популярные записи

vañ_makaron всего: Легкий способ бросить. Да, тот пост натолкнул...

Neivid В нашем доме детям не разрешалось. 1. В нашем доме детям не разрешалось откусывать...

feeling_of_void ВАКАНСИИ. Ищу девушку модельной внешности

Mystafa Мы сможем ему помочь! Дима Светов (13 мая 1997...)

Sholademi Офисное рабство на московской радиостанции...

rkutsk_zabvo МИТИНГ В АНГАРСКЕ, 25 ИЮЛЯ ЧАСТЬ 2.

scholar_vit О защите Конституции Российской Федерации Похоже

LVN Интересные, замечательные стихи Олег Гаврилюк Все...

dart_misha Вчера в процессе дикого угара

resistenz_a В Удмуртии состоялись предварительные слушания...

Karandirry Из жизненных перлов:). Серебряный дождь:) 100.

Olshansky «осознанный ребенок». Фашики злобствуют по поводу...

ru_sex_school Секс с виртуалом. Мне сегодня приснилось

antihubbard отечественный автопром. Сегодня я проехался на Оке...

ru_existential Убить или позволить умереть? Это очень известный...

Разумеется, при таком спектре тем – от опыта поездки на автомобиле «Ока», секса с виртуалом во сне, поисков девушки с мо-

дельной внешностью и до различных аспектов политики – увязать комментарии в блогах-участниках топа с темой вашей информационной войны практически невозможно. Тогда на помощь в комментировании могут прийти неопределенные высказывания «ни о чем», вроде: «Спорное утверждение, хотя кто знает...», «Ну, не знаю, не знаю...», «Может быть, но не факт», «Вы на самом деле так считаете?», «Что вы имели в виду?», «Вполне возможно», «У каждого есть своя правда» и т. п. Использование подобных фраз минимизирует вероятность агрессивного ответа и в то же время смотрится уместно практически в любом сколь-нибудь длинном разговоре. Но постарайтесь вставлять эти фразы так, чтобы они смотрелись уместно, а то многим уже глаза намозолил робот, бегающий по Живому Журналу и совершенно не к месту вставляющий фразу: «Вы на самом деле так думаете?» Однако наиболее «горячих» тем мы рекомендуем все же избегать, или по крайней мере подумать, каковы могут быть последствия вступления в дискуссию с разгоряченными людьми, имеющими массу свободного времени и искренне уверенными в своей правоте и в неправоте соперников (неважно, чему посвящен их

конфликт). В наиболее неблагоприятном случае вас могут счесть врагом обе враждующие группы.

Интересные блоги и сайты обсуждаются и комментируются. Их советуют друг другу или ругают, но в любом случае о них говорят, а это значит, что они нужны людям. И такие ресурсы Гугл старается поднимать. С Гуглом плохо получается такой старый оптимизаторский трюк – «закольцевать» десяток сайтов, чтобы сказать всем: «Я хороший! Дайте мне денег!» Люди должны подтвердить качество ресурса, чтобы он мог претендовать на по-настоящему высокий рейтинг.

В чем-то это созвучно западному научному принципу: «Публикуйся! Или уходи!»

В Интернете, а особенно в блогах, когда речь идет об определении популярности, можно рассчитывать только на членов сообщества. Их слово будет решающим.

Ссылки на свои ресурсы и цитирование своих ресурсов как способ ведения информационной войны

Мы уже отмечали, что внешние ссылки важны, так как поднимают ваш блог или сайт в выдаче поисковых машин. И мы говорили о том, что получается замкнутый круг: пока вы неизвестны, вас мало цитируют, потому что никто о вас не знает, а пока вас мало цитируют, вы неизвестны, так как вас просто не видно в результатах выдачи поисковиков. Если вы не можете ждать, пока на вас наткнутся случайные посетители (а в условиях информационной войны по-другому обычно не бывает), вы можете организовать себе цитирование самостоятельно.

Создавайте новые блоги, которые будут перепечатывать статьи с вашего основного блога. Главное – чтобы они давали ссылки на ваш основной блог. Это надо делать точно так, будто вы цитируете чужой текст. В любом месте страницы с цитируемым текстом поставьте ссылку на источник – ваш собственный блог или сайт. Не стесняйтесь перепечатывать как можно большее количество своих материалов и давать ссылки на эти страницы. Создавайте большое количество «блогов поддержки» – и вы сможете поднять свой сайт или блог в выдаче поисковых машин. Точного определения, что такое «большое количество», не существует – все

зависит от масштабов мероприятия. Можно сказать, что количество «блогов поддержки» обычно варьируется в пределах от нескольких десятков до нескольких сотен.

Интересно, что при достижении определенного количества ссылок блог, расположенный в Живом Журнале (если именно на таком блоге первоначально появился текст), вполне может попасть в Топ-30 Яндекса или в число самых популярных тем в Живом Журнале. В таком случае он получит отдельный адрес в Интернете на отлично индексируемом поисковыми машинами ресурсе, а авторитет его повысится. Это может дать дополнительное небольшое преимущество в информационной войне.

Теги как инструмент раскрутки блога в информационной войне

Теги (их еще называют метками, или tags) служат для того, чтобы было удобнее найти нужный блог среди других или статью внутри блога. Это своего рода ключевые слова, по которым блоги с материалами по определенной тематике легко отыскать на ресурсе

блогов.

Для раскрутки блога в поисковых машинах в информационной войне важна одна особенность тегов: они аккумулируются на очень большом количестве площадок в Интернете. То есть происходит буквально следующее: на специальных страницах собирается огромное количество текстов (с гиперссылками), объединенных единственным общим критерием: они сопровождаются одним и тем же тегом в описании. Эти «сборные площадки» благодаря тому, что собирают тексты с огромного количества сайтов по определенным ключевым словам, становятся по этим словам высокорелевантными. Поисковые машины дают им высокий рейтинг, а поскольку каждый подобный «аккумулятор тегов» имеет отдельный адрес в Интернете, то в результате ваш блог получает дополнительные строчки на первых страницах поисковых машин, да еще и гиперссылки с этих адресов на блоги-источники. Повышается вероятность того, что пользователь, вводя в поисковую строку ключевое слово, придет на ваш блог, а значит, вы можете получить дополнительных читателей, дополнительных френдов и дополнительные ссылки и в конечном счете обогнать против-

ника в гонке за место в выдаче поисковиков.

Тематические интернет-форумы как целевая аудитория в информационной войне

Особенности интернет-форумов

По данным зарубежных авторов, уже в 2005 году в Интернете было 120 тысяч дискуссионных групп и форумов.

Интернет-форум – это своего рода клуб по интересам. Для того чтобы люди могли точнее ориентироваться в пределах интересующей их темы и получать по ней нужную им информацию, на форумах выделяются специальные тематические разделы. В пределах каждого из них есть отдельные темы (их часто называют ветками, топиками или тредами).

Таким образом, очевидно, что форумы, подобно блогам, позволяют организовать общение между людьми. Недаром их второе распространенное название – дискуссионные площадки. Чаще всего форумы присут-

ствуют в Интернете не самостоятельно, а являются частью сайта или портала. Порталами обычно называют сайты, открывающие доступ к другим сайтам, объединенным какой-то темой, но самостоятельным. Примером небольшого по размерам портала может служить сайт «Конкурентная разведка» одного из авторов этой книги. Он расположен по адресу: www.ci-razvedka.ru и не только содержит информацию по теме, вынесенной в заголовок, но и открывает доступ к различным инструментам, расположенным на самостоятельных сайтах по всему миру.

Для того чтобы лучше понимать разницу между форумами и блогами, а значит, максимально эффективно использовать форумы, рассмотрим этот вопрос более подробно. Сравнение блогов и форумов было удачно, на наш взгляд, проведено Романом Подоляном из Украины, редактором общественно-правового сайта «СОКол-ЮрОбоз» в его статье «Слухи о смерти форумов сильно преувеличены».[53]

Блоги и форумы похожи тем, что позволяют общаться в принципе неограниченному числу лиц как в реальном масштабе времени, так и в удобное для них разное время. Однако по некоторым своим возможностям

они серьезно различаются. Перечислим эти отличия.

1. Расположение сообщений на странице. В форуме наверх (в первую строку, видимую пользователем) выходит та тема, комментарий по которой появился позже всех остальных (т. е. он является самым свежим для данного форума).

Чтобы не было полного перемешивания тем и не затруднялся поиск нужного материала, на форумах существуют отдельные категории для каждого рода сообщений, но внутри каждой категории вверху все равно будет то сообщение, ответ по которому появился последним. Если, предположим, минуту назад на форуме была создана тема с вопросом, то она встает в первой строке перечня обсуждаемых тем.

Но если следующим будет сообщение в другой теме, созданной год назад и затухшей в течение пяти минут после создания, то эта тема годичной давности, давно забытая всеми, станет первой в списке, а предыдущий лидер сместится вниз и займет вторую строчку. Эту особенность форумов нередко используют в информационных войнах, чтобы «поднять» негативную информацию о противнике и не дать ей забыться.

В блогах ситуация иная. Обсуждение темы (их там, как известно, называют постом или статьей) в блоге не приводит к изменению последовательности расположения в нем текста. Хотя, как и в форуме, каждый новый комментарий к статье записывается под предыдущим, формируя так называемую ветку (тред). Сама статья, к которой дан новый комментарий, не меняет своего положения относительно других статей. Статья, которую обсуждают, по мере появления новых постов уходит в глубь блога вместе с обсуждением, которое по ней шло.

Управление контентом. С технической точки зрения, нет большой разницы между контролем над контентом в блоге и форуме. В обоих случаях обычно имеется модератор, который может удалять или редактировать сообщения посетителей, запрещать комментирование тем, видеть адреса, с которых посетители написали свое сообщение, ограничивать доступ посетителей на блог или форум. Но на практике исторически сложилось так, что чаще всего блог абсолютно подконтролен воле одного человека, тогда как форумы более демократичны (а иногда и просто никем не контролируются). На входе в форум, как правило, висят правила поведе-

ния на данном ресурсе, а на входе в блог их обычно нет. Хотя и здесь возможны отклонения от общей ситуации в обе стороны: масса форумов не соблюдает объявленных ими же самими правил, а на входе в журналы некоторых блоггеров правила присутствуют.

Кто может быть инициатором темы (тредстартером). На форуме тредстартером может быть любой зарегистрированный пользователь. В блоге, как правило, эту функцию выполняет владелец или тот, кто выступает от его имени. Вот почему форумы в значительно большей степени ближе к равноправию участников, чем блоги.

Продолжительность активного обсуждения темы. За счет встроенной функции поиска в форуме значительно проще найти нужную тему, чем в блоге. Поэтому человек, которому требуется найти ответ на свой вопрос, в форуме обычно может это сделать быстрее, чем в комментариях блога.

Если при комментировании в блоге собеседники дали ответ на вопрос, который интересует посетителя, пришедшего в поисках этого ответа, то в такой ситуации разницы между форумом и блогом для него не будет. Но если посетителю ответ не кажется полным и ему требуется что-либо уточнить, то

блог становится значительно менее удобным инструментом, чем форум. Ведь уточняющий вопрос, заданный в блоге, окажется невидим большинству людей, так как он «спрятан» в глубине просто в силу того, что появилось много новых постов.

В форуме же уточняющий вопрос новичка поднимет тему в верхнюю часть страницы и тем самым привлечет всеобщее внимание. И действительно, на форумах некоторые темы обсуждаются годами, тогда как на блогах обсуждение занимает значительно более короткий период времени. Разумеется, есть исключения и здесь. Например, блог Дениса Фурсова из Санкт-Петербурга, посвященный правильному поиску с помощью Яндекса, стал постоянно действующей площадкой, где обсуждаются проблемы поиска. Однако такие исключения довольно редки и не меняют общей ситуации.

Резюмируя, можно процитировать Романа Подольна: «Почему блоги не заменят форумы? Пока людям будут нужны коллективные обсуждения, близкие к равноправным, – до тех пор будут нужны и форумы. Пока людям будет нужно личное пространство – до тех пор будут и блоги».[54]

Чтобы интернет-форумы стали полезным инструментом в раскрутке блога, надо понимать некоторые их особенности. Мы рассмотрим их несколько под другим углом зрения, нежели когда мы сравнивали форумы и блоги.

1. На форуме каждый имеет право высказать свое мнение и вправе получить ответ.

Это действительно так, но есть некоторые ограничения.

Для того, чтобы форум не превратился в банальную рекламную площадку или в место, где люди могут нецензурно ругать друг друга, а также для того, чтобы он оставался тематическим, существуют модераторы, наделенные полномочиями корректировать (или полностью удалять) сообщения, запрещенные правилами форума, обычно вывешенными на входе. Кроме того, модераторы имеют право запрещать доступ на форум тем или иным людям на разный срок. Модераторы, как правило, назначаются из числа постоянных посетителей форума, с точки зрения владельца или распорядителя интернет-ресурса, хорошо зарекомендовавших себя. На небольшом форуме модератором может выступать сам его владелец.

Как правило, человек имеет право задавать не любые вопросы, а лишь те, что относятся к теме форума. Нетематические вопросы обычно запрещены (их называют оффтопиками). Модератор вправе наказать автора оффтопика и/или совсем убрать его вопрос.

Ответы на форумах даются только на добровольных началах. Никто не обязан отвечать на заданный вопрос.

2. На форуме каждый имеет право идентифицировать себя в той степени, в которой считает нужным.

Для того, чтобы иметь право участвовать в форуме, так же, как и в блоге, необходим ник. В принципе это тот минимум информации, который требуется для регистрации. Каждый имеет право дать о себе дополнительную информацию, но не обязан это делать.

Несколько лет назад можно было оставлять сообщения в форумах и без регистрации. Но в связи с развитием распространяемого роботами спама на форумах эта практика почти повсеместно прекращена.

При регистрации сегодня чаще всего требуется указывать действующий адрес электронной почты. Порой недобросовестные владельцы форумов продают адреса посети-

телей спамерам. Чтобы не попасть в списки несанкционированной рассылки, можно воспользоваться одноразовым почтовым ящиком, который живет кратко 10 минут.[55] Правда, в этом случае будет невозможно восстановить забытый пароль, поэтому альтернативой может служить открытие почтового ящика на бесплатном ресурсе специально для регистрации на форуме. Вы можете не читать сообщения в таком почтовом ящике, поэтому спам вас беспокоить не будет, но при необходимости с его помощью можно будет восстановить свой пароль к форуму.

3. Можно поднять все высказывания человека за время его пребывания на интернет-форуме.

Практически везде на форумах есть «кнопка», позволяющая получить доступ к высказываниям определенного человека за все время его пребывания на форуме. Дата высказывания фиксируется автоматически и не может быть изменена пользователем самостоятельно.

4. Как правило, на форумах есть поиск внутри сообщений по ключевым словам.

Это позволяет находить слова или словосочетания и таким образом ориентировать-

ся в многолетней базе данных форума.

Важно, что форумы частично относятся к «невидимому Интернету». Это значит, что никаким другим способом, кроме встроенного поиска, нельзя найти некоторую часть содержащейся там информации.

5. Материалы интернет-форумов (по данным западных авторов) хранятся около 10 лет.

6. В последнее время на многих форумах ссылки на внешние ресурсы перестают учитываться поисковыми машинами.

Это связано с тем, что спамеры начали активно размещать на форумах свои сообщения. Появились спамерские программы, способные обходить довольно сложные процедуры регистрации. Для того чтобы сделать спам на форумах нецелесообразным, администраторы часто запрещают поисковым машинам индексировать внешние ссылки. Однако часто, даже когда ссылки не учитываются в определении авторитетности сайта или блога, пауки совершают по ним переходы на блог, поэтому гиперссылки на блог из форумов все же имеют смысл – ведь частота повторной индексации вашего ресурса может несколько возрасти. А самое главное – на него перейдут люди, которые могут разде-

лить вашу точку зрения и, возможно, дать на вас гиперссылку. Любое увеличение численности ваших сторонников позволит вам получить преимущество в информационной войне.

7. Многие популярные форумы хорошо индексируются поисковыми машинами и имеют высокий рейтинг доверия.

Форумы, пользующиеся большой популярностью у людей, хорошо индексируются поисковыми машинами. Если форум качественно модерировается, на нем отсутствует беспорядочная реклама, нет нецензурных выражений и ссылок на спамерские ресурсы, то информация, попавшая него, не только становится быстро известной RSS-агрегаторам, но довольно оперативно попадает в «основной индекс» поисковых машин. Разумеется, блоггер заинтересован в том, чтобы найти тематические форумы по возможности быстро.

Рассмотрим поиск нужных интернет-форумов на примере Яндекса. В нем искать целевую аудиторию для нашего мастер-класса можно как минимум двумя способами – через блоги Яндекса и в «основном индексе» – через основную поисковую строку. В обоих случаях язык запросов Яндекса работает, что

позволяет составить запрос той степени детализации, которая требуется в каждой конкретной ситуации.

Поисковый запрос в случае поиска тематических для конкретной информационной войны форумов можно делать не очень сложным, так как вас будет устраивать достаточно широкий диапазон ответов, и при этом то, что вы получите не самый полный охват вариантов, не будет проблемой. В поиске все время приходится балансировать между слишком жестким запросом, где не исключено, что вместе с водой выплеснут и младенца, и чересчур мягким, где относительно много информационного мусора. Но что не может не порадовать – всегда имеется несколько правильных вариантов решения, поэтому нет смысла что-то заучивать, а достаточно понять алгоритм работы.

Подробно язык запросов поисковых машин изложен в нашей книге «Интернет-разведка. Руководство к действию» (М.: Вершина, 2007). Описание языка запросов Яндекса можно найти также в разделе «Помощь» на сайте этого поисковика. Здесь мы вкратце рассмотрим варианты запросов в блоги Яндекса. Блоги Яндекса – это служба, которая целенаправленно отслеживает сообщения в

блогах и форумах и отличается большой оперативностью в предоставлении информации.

Запрос: Секретов /1 (Секрет / + 1 Секретович).

Что означает: нам нужны документы, содержащие словосочетания «Секретов Секрет Секретович» или «Секрет Секретович Секретов» и при этом словоформы могут быть любыми – например, «Секретова Секрета Секретовича» или «Секретову Секрету Секретовичу» и даже «Секретову Секретом Секретович».

Запрос: + мнение && + форум && + (спортивная / + 1 спелеология).

Что означает: мне нужны документы, содержащие в любом месте документа слова «мнение», «форум» и «спортивная спелеология» (именно в такой последовательности, а не «спелеология спортивная»).

Запрос: + (истории | шутки | приколы | анекдоты) && + форум && + ((спортивная / + 1 спелеология) | (кулинария)).

Что означает: мне нужны документы, содержащие слова «истории», или «шутки», или «приколы», или «анекдоты» и чтобы в любом месте документа, их содержащего, были слова «спортивная спелеология» (именно

но в такой последовательности) или «кулинария».

На найденных таким образом ресурсах было бы целесообразно разместить ссылку на ваш блог или сайт. Для этого требуется найти повод. Учитывая, что тематика блога или сайта в случае отражения черного PR со стороны гипотетического Секретова Секрета Секретовича совпадает с тематикой постов в форуме, обнаруженном по приведенному запросу, найти такой повод должно быть достаточно просто.

Региональные или тематические блоги и форумы как инструмент раскрутки блогов и сайтов в целях противодействия информационному нападению

Как показала практика блога журнала «Деловой квартал» в Екатеринбурге и форума, расположенного на той же площадке, региональные блоги и форумы имеют достаточно высокий рейтинг у поисковых машин, и поэтому могут быть эффективны в защите

от информационного нападения. Так, материалы, опубликованные на блоге «Делового квартала», уже через 12 часов после размещения на нем ссылки на наш блог вывели его на первое место в Яндексе по запросу «Секретов Секрет Секретович». И в дальнейшем ресурсы, на которые были даны ссылки с «Делового квартала», стабильно получали высокий рейтинг. Как уже говорилось, такой эффект достигается на тех форумах, которые пользуются популярностью у людей и при этом хорошо модерируются. Пользуясь этими площадками, вы получаете хорошую поддержку с их стороны. Однако это не значит, что там можно размещать все, что вам заблагорассудится. Вы можете разместить там только те материалы, которые интересны пользователям регионального форума, и при этом эти материалы не должны содержать оскорблений и клеветы, а также нецензурных слов. При соблюдении этих важных условий вы фактически платите за свою поддержку тем, что даете региональному форуму интересный контент, привлекающий на него дополнительных пользователей. Подумайте, как сделать тему вашей информационной войны интересной людям. Расскажите более подробно (в рамках разумного) о

том, как технически вы организовали оборону от агрессора, напавшего на вас с помощью инструментов черного PR. Покажите, почему вы считаете, что любой человек или любое предприятие могут стать жертвой подобного нападения. По возможности придайте своей войне игровую или по крайней мере интерактивную форму, дайте возможность людям апробировать какие-то инструменты, выступая на вашей стороне, обеспечьте им легкое вступление в вашу войну и легкий выход из нее. При соблюдении этих правил вы, возможно, организуете подобие народного фронта с неограниченным числом участников. Если вам удастся сделать свою идею привлекательной для людей, этот фронт может быть неограничен ни в кадрах, ни по времени. Учитывая, что мы говорим именно о защите от черного PR, т. е. от заведомой лжи, распространяемой в отношении вас, как правило, вы сможете справиться с этими задачами.

Размещение на региональном ресурсе делает ваши материалы более доступными для людей, живущих в том регионе, где расположен региональный форум, так как внутренний трафик стоит значительно дешевле внешнего.

Достаточно часто на региональных форумах размещаются сообщения блоггеров с других площадок. Вы тоже можете разместить там свои материалы (перепечатанные с других ваших блогов или созданные вновь). Категорическое условие при этом – ваши тексты должны соответствовать тематике регионального форума, быть написаны грамотным языком и являться информативными, полезными для сообщества. В противном случае путь на региональный форум будет вам заказан. Нельзя просто рекламировать свой блог или сайт, посвященный отражению нападения черных пиарщиков. За право разместить ссылку с раскрученного форума на свой блог или сайт вы обязательно должны заплатить информацией, полезной для участников этой дискуссионной площадки.

Столь же эффективен тематический форум «Состав» («Sostav», www.forumsostav.ru) – один из крупнейших, если не крупнейший рунетовский ресурс, посвященный маркетингу. Модераторы «Состава» и подобных ему тематических сайтов всегда отнесутся благосклонно к вашей гиперссылке, если ваш блог или сайт, на который она ведет, полезен участникам форума.

Гостевые книги как инструмент противодействия черному PR

Гостевая книга – как правило, единственный механизм интерактивного взаимодействия с традиционными сайтами в открытом доступе. До появления интерактивных интернет-ресурсов Web 2.0 других способов публичного двустороннего общения с сайтами просто не было. Ставить в гостевых книгах гиперссылки технически возможно. Однако эта возможность – не единственная причина, по которой имеет смысл включить их в перечень инструментов, которые можно использовать в информационной войне. Не меньшее значение имеет и то, что гостевые книги раскрученных сайтов хорошо индексируются поисковыми машинами, а потому ваша точка зрения, размещенная там, станет известна большому количеству пользователей Интернета. Главное в таком случае – найти информационный повод для того, чтобы эту точку зрения высказать. Это

возможно не всегда, обычно надо ждать подходящего момента. Часто это происходит по схеме: «Согласен с предыдущим оратором. Я тоже могу привести пример из практики...»

Следует всегда внимательно смотреть на гостевые книги, которые по ключевым словам вашего блога или сайта находятся на первых страницах результатов выдачи поисковых машин, и искать среди них те, которые открыты для размещения новых сообщений.

В «живых» гостевых книгах вопрос, публиковать или нет ваш текст, решает модератор. Если же вы найдете заброшенные гостевые книги на старых ресурсах, давно находящихся в Интернете, имеет смысл использовать и их, давая там ссылки на свои блоги и сайты. Если сайт, на котором расположена такая гостевая книга, присутствует в Интернете более пяти лет, то авторитет такого «Летучего Голландца» у поисковых машин, как правило, очень высок. Определить заброшенный ресурс чаще всего несложно: на его главной странице раздел «Новости» давно не обновлялся.

Бывают ситуации, когда противник уже сам использовал заброшенные гостевые книги, например, для размещения собствен-

ной рекламы. Чтобы выявить этот факт, надо тщательно изучить все ресурсы, на которых его реклама расположена достаточно высоко в выдаче поисковых машин. Если среди этих ресурсов есть заброшенные гостевые книги, имеет смысл спланировать и провести «десантную атаку». Для этого нужно разместить там свои сообщения по тем же ключевым словам, по которым в этих гостевых книгах находится противник. Однако количество ключевых слов в ваших текстах должно значительно превышать количество ключевых слов в тексте противника.

Применительно к нашему вымышленному объекту атаки Секретову Секрету Секретовичу, который рекламирует свою фирму по производству куличей, это могло бы выглядеть так (гиперссылки выделены жирным шрифтом, а слово «кулич» – курсивом).

Оригинальный текст Секретова Секрета Секретовича

Предлагаю подписаться на программу поставки оборудования производства **куличей** по авторским технологиям в условиях магазина «Кулинария». Презентация проводится бесплатно. Авторская методика производства **куличей** непосредственно от автора, впервые применившего слово «**кулич**» в но-

вейшей истории России! Каждому клиенту – подарки:

- лицензия конечного пользователя на использование слова «**кулич**» в Российской Федерации, напечатанная на нашем фирменном бланке за подписью нашего Президента, академика Академии продвинутых технологий Секретова С. С.

- наш фирменный пластиковый пакет-мачка с изображением;

- авторский компакт-диск с трехчасовой речью Секретова С. С. произнесенной им на открытии булочной в микрорайоне Кривые Юзаки в марте 2007 года

Обращайтесь в предприятие «**Кулич с Секретом**»!

Текст, который может размещаться в ходе «десантной атаки» и рассчитан на замещение текста противника по ключевым словам «кулич» и «Секретов Секрет Секретович».

Здравствуйтесь, уважаемые любители куличей.

Мы не станем кричать, подобно уличным зазывалам: «**Куличи Куличи!** Горячие **куличи!** Покупайте **куличи!** Кому **куличи?**» Мы уважаем тех, кто помогает людям изготавливать **куличи** в любых условиях – от гипермаркета до небольшого магазина «Кулина-

рия».

И нам неприятно видеть, как Секретов Секрет Секретович безосновательно присваивает себе права на слово «**кулич**» и пытается ставить палки в колеса производителям **куличей** в нашей стране. Мы понимаем, что Секрет Секретович Секретов нуждается в деньгах и проигрывает более трудолюбивым и креативным производителям **куличей** в конкурентной борьбе, а потому пытается «принизить» других производителей **куличей** раз уж не получается «возвысить» себя. Мы понимаем, что ужас уходящего с рынка производителя **куличей** – Секретова Секрета Секретовича – обоснован: все больше людей профессионально пекут **куличи** и не собираются терпеть необоснованных притязаний в этой сфере. Но надо же Секретову Секрету Секретовичу и чувство меры иметь. Мы против того, чтобы не подкрепленные никакими официальными документами амбиции одного производителя **куличей** сказывались на всей отрасли производства этого продукта. Вот правда о том, на чем основаны немотивированные притязания Секретова Секрета Секретовича на слово «**кулич**» и почему Секрет Секретович Секретов так упрямо пытается мешать развитию производства **ку-**

личей в России.

Сайт 1. Восемь безответных официальных запросов Секретову Секрету Секретовичу по поводу подтверждения его прав на слово «кулич».

Сайт 2. Секретов Секрет Секретович не имеет прав на слово «кулич» (официальный ответ регистрирующего органа).

Сайт 3. Предшественники Секретова Секрета Секретовича в производстве куличей в России и за рубежом. Историческая справка.

Сайт 4. Секретов Секрет Секретович обманывал, утверждая, что сам придумал слово «кулич». Свидетельства очевидцев и вещественные доказательства.

При столь очевидном перевесе слова «кулич» и его производных «десантный» текст выйдет на первое место в выдаче поисковых машин по адресу этой гостевой книги. А заодно получится и продвижение по словосочетанию «Секретов Секрет Секретович». Если гостевая книга имеет несколько разделов, есть смысл разместить различные варианты текста в каждом из них, обязательно адаптировав эти варианты под тематику разделов, чтобы не быть обвиненными в спаме. В результате рекламный текст Секре-

та Секретовича Секретова будет заменен в выдаче поисковых машин вашими текстами, а его первоначальное рекламное объявление окажется закопано в строке вида «Еще с сайта 12 сообщений», которая расположена под результатами выдачи и на которую пользователи достаточно редко обращают внимание.

Публичные сервисы закладок как инструмент отражения информационного нападения

Сервисы закладок приобретают популярность в Интернете. Они бесплатны и могут быть эффективно использованы для продвижения блога или сайта в поисковых системах.

Основная задача подобных сервисов – обеспечить доступ к закладкам из любой точки земного шара и позволить находить тематические закладки, сделанные другими людьми.

Каждая такая закладка состоит из гиперссылки, ведущей на нужную страницу, якорных слов гиперссылки (текста гиперссылки), которые при создании закладки вводятся в отдельное поле, краткого комментария и тегов. Пользователь может регулировать доступ к своим закладкам. По умолчанию они доступны каждому, но можно ограничить доступ и разрешить его только себе.

Уникальной особенностью сервисов закладок, которая сделала их популярными, является возможность видеть закладки других пользователей, размещенные в открытом доступе. Благодаря этому у людей появляется возможность найти новые ссылки на ресурсы, которые им интересны. Этот поиск осуществляется при помощи тегов – каждый имеет возможность найти закладки по любой теме, собранные разными людьми. Практика показывает, что это очень эффективный способ поиска новых источников информации по определенной теме, этим и объясняется популярность сервисов закладок. А как только большое количество людей начинают пользоваться каким-либо интернет-ресурсом, давать на него ссылки и размещать на нем свои материалы, этот ресурс начинает активно посещаться и поисковыми машинами.

Еще одна особенность, которая характерна для Web 2.0, – возможность комментировать закладки. Ведь в ходе такого комментирования люди делятся своим мнением и часто при этом дают ссылки на другие ресурсы, дополнительно раскрывающие затронутую тему. Вот почему сервисы закладок стали очень популярными. Ими пользуется все

больше людей, а вслед за ними на сервисы закладок приходят и пауки поисковых машин.

В контексте продвижения своей точки зрения в ходе информационной войны страница закладок отдельного пользователя – это тематический мини-сайт на площадке, популярной у поисковых машин и имеющей высокий рейтинг доверия. Впервые нам эту идею подсказал Артем Овсянников.

Если разместить на этой площадке ссылки на статьи в ваших блогах и сайтах с краткими фрагментами текста вместо комментария и с ключевыми словосочетаниями в качестве тегов, то такая страница закладок способна заметно поднять ваши интернет-ресурсы в выдаче поисковых машин. Кроме того, страница с закладками сама по себе появится в выдаче поисковиков и послужит дополнительной точкой, с которой посетители смогут перейти на ваши сайты или блоги.

Вот основные площадки публичных закладок, которые на момент написания книги хорошо поддерживали русский язык и посещались поисковыми машинами:

- MoeMesto (www.moemesto.ru/);
- Mister Wong (www.mister-wong.ru/);

- Memori.ru (www.memori.ru/);
- BobrDobr.ru (www.bobrdobr.ru/index.html).

«Опорные» сайты-аккумуляторы и блоги-аккумуляторы

«Боевая» группировка сайтов в Интернете, которая позволяет отразить атаку черных пиарщиков с максимальным уроном для агрессора, напоминает морскую эскадру. На периферии находятся многочисленные небольшие разрозненные ресурсы, в центре – крупные корабли. Отдельные разрозненные ресурсы публикуют материалы для того, чтобы целевая аудитория могла ознакомиться с точкой зрения на проблему, которую вы хотите до нее донести. Поскольку в этот процесс на вашей стороне со временем включаются все новые и новые участники, они могут находить порой совершенно неожиданную, но очень полезную для победы над противником информацию. Практика показывает, что немалую пользу приносит создание сайтов и блогов, которые аккумулируют информацию с других ресурсов. На этих сайтах (блогах)-аккумуляторах вы можете выстроить информацию в такой последовательности, чтобы она лучше всего отражала

вашу точку зрения и представляла противника в максимально невыгодном для него свете.

Остается выбрать, сайт или блог использовать в качестве «аккумулятора информации», а также решить, каким должен быть такой блог, если будет принято решение остановить ваш выбор на блоге.

Блог удобнее сайта в случае, если основной объем вашей информации представлен в текстовом виде, а также в виде аудио-или видеоматериалов. А вот если у вас в материалах преобладают фотографии, то более предпочтительным нам представляется сайт.

С традиционным сайтом ситуация достаточно понятна: на нем просто создаются странички с нужными материалами, и затем они перелинковываются между собой.

А о создании блога-аккумулятора или сайта-аккумулятора давайте поговорим более подробно.

Поисковые машины отдают безусловный приоритет платным ресурсам перед бесплатными. Блог (сайт) на бесплатном хостинге имеет у них понижающий коэффициент по сравнению с блогом (сайтом), расположенном на платном. А людьми адрес бесплатно-

го хостинга интернет-ресурса может восприниматься как синоним плохого материального положения его владельца, поскольку стоимость регистрации доменного имени и хостинга невелики и непонятно, зачем серьезной организации на них экономить. Правда, иногда надо как раз продемонстрировать именно бесплатные ресурсы (например, проводя мероприятие, за которым якобы не стоит никакая компания), и тогда расположение на бесплатной площадке становится не недостатком, а преимуществом ресурса. Таким образом, для того чтобы ваш блог или сайт оказался лидером по избранным вами ключевым словам, мы рекомендуем вам не только создавать сеть блогов и сайтов, объединенных общими темами, имеющих ссылки друг на друга, состоящих из ресурсов и расположенных на разных площадках, но также включить в число участников этой сети stand-alone-блоги. Более того – сделать аккумуляторами информации именно их, а не бесплатные блоги. Для настройки stand-alone-блогов в самом начале работы потребуется участие специалистов, но затем вы сможете управлять ими самостоятельно, без каких бы то ни было проблем, точно так же, как обычными бесплат-

ными блогами. Как уже было сказано, stand-alone-блоги работают в основном на движке Wordpress, и вы без труда найдете в Интернете специалистов, умеющих их настраивать. Такие блоги-аккумуляторы могут публиковать на своих страницах всю информацию, первоначально размещаемую на бесплатных блогах и сайтах, входящих в вашу сеть. В результате блоги-аккумуляторы станут самыми крупными в Интернете ресурсами, содержащими тематические тексты.

Они получают тематический материал с других блогов и практически ничего другого содержать не будут, поэтому станут рассматриваться поисковыми машинами как высокорелевантные запросу по вашим ключевым словам. За счет ссылок на источники текстов (блоги и сайты вашей же сети) они станут снабжать ссылками всю сеть, получая от нее взамен ссылки. А за счет того, что эти блоги-аккумуляторы расположены на платном хостинге, они будут иметь приоритет при оценке их значимости поисковыми машинами и займут первые места в выдаче поисковиков. Расставив даты сообщений в блоге в нужной вам последовательности, вы сможете расположить информацию в том порядке, в котором считаете нужным, – ведь

информация в блоге располагается именно по дате.

Остальные ваши блоги и сайты окажутся ниже блогов-аккумуляторов в результатах выдачи поисковых машин по вашим ключевым словам. Это повысит вероятность встречи с вашей сетью при серфинге в Интернете. По большому счету борьба в информационной войне в Интернете идет за первые 30–40 строк в выдаче. Поскольку на каждом блоге вашей сети будет стоять ссылка на блог-аккумулятор или сайт-аккумулятор, пользователь с большей вероятностью придет на него, наткнувшись на второстепенный ресурс вашей сети.

Однако, создавая несколько блогов и сайтов, аккумулирующих информацию, не забывайте, что поисковые машины «режут зеркала», т. е., при наличии в Интернете нескольких копий одного ресурса на разных адресах показывают только одну из этих копий. Чтобы не попасться в эту ловушку, мы рекомендуем не размещать на ресурсах-аккумуляторах совершенно идентичную информацию. Даже если основные тексты будут одними и теми же, остальное наполнение блогов и сайтов-аккумуляторов должно отличаться, тогда это не будет считаться

полным «зеркалом», и ваши ресурсы займут несколько разных адресов в результатах выдачи, сталкивая вниз противника и доводя до общественности именно вашу точку зрения.

Вариант построения «боевого порядка» интернет-ресурсов при отражении информационного нападения Артем Овсянников проиллюстрировал соответствующей схемой (рис. 26).

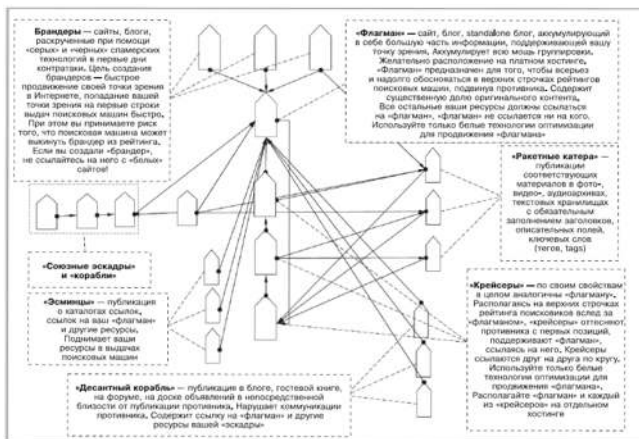


Рис. 26. Вариант построения «боевого порядка» интернет-ресурсов при отражении информационного нападения

Враг может нанять хакера. Насколько это опасно и как с этим бороться?

Это серьезный аспект информационной войны в Интернете, который нельзя обойти молчанием. Начиная противодействие агрессору в Интернете, вы ломаете своими действиями его планы, делаете неэффективными его финансовые траты. В общем, как минимум портите ему настроение, а как максимум – ставите под угрозу его репутацию и бизнес. Разумеется, он будет крайне недоволен. Само собой, это недовольство выразится в ответных действиях.

Вероятность, что ваш противник переступит через Уголовный кодекс и обратится к хакерам, очень велика. В случае, если он это сделает, события скорее всего будут развиваться в одном из двух направлений.

Во-первых, он может попытаться взломать ваш сайт и просто стереть его. Пароли на доступ к сайту, которые по умолчанию ставят хостеры, обычно взламываются до-

вольно быстро. Никакого особого вреда взлом сайта вам не причинит, правда, при одном условии: если у вас есть копия сайта после каждого его обновления. Для того чтобы уменьшить вероятность взлома вашего сайта, попросите хостера сразу установить максимально сложный из возможных паролей.

Во-вторых, противник может заказать DOS-атаку на ваш сайт. «Задосить» сегодня можно практически любую интернет-площадку. Желающих «досить» Живой Журнал обычно немного, так как это чревато крайне негативными последствиями для хакера, но «положить в DOS» сервер небольшого провайдера могут легко. Поэтому помните несколько правил: во-первых, не храните все свои ресурсы на одном сервере. Распределите их по разным хостингам и, возможно, разным странам. Это заставит агрессора тратить большие деньги на атаку, позволит вам быстрее ее отбить и резко повысит вероятность его поимки. Он знает, что совершает уголовное преступление и отдает себе отчет в том, что воевать против всего мира противозаконными методами длительное время опасно.

Старайтесь выбирать для хостинга не самые дешевые, а самые крупные и технически совершенные организации. У них возможности отбить DOS-атаку выше, чем у «карликов» рынка. DOS-атаки на момент написания книги считались самыми опасными видами хакерства с точки зрения мишеней. Такие атаки относительно легки в исполнении, а их источник обнаружить непросто, тем более что имеются программы, подменяющие адреса, с которых идет атака. Однако средства борьбы с такими атаками существуют, и диапазон их колеблется от фильтрации подсетей, с которых идет атака (сайт-мишень при этом может оставаться относительно работоспособным), до возврата атаки самому атакующему, когда он начинает атаковать сам себя, как бы воюя с зеркалом (сайт-мишень при этом отключается). Первый вариант требует применения специального «железа», поэтому он не по карману маленьким хостерам. Второй же вряд ли вам понравится, так как подразумевает отключение вашего сайта от Интернета.

В то же время создание копий собственных сайтов относительно недорого, поэтому в гонке между непрерывным созданием новых сайтов и непрекращающимися попыт-

ками противника «досить» ваши старые сайты преимущество в конечном счете будет не на его стороне.

Если вы считаете, что вероятность использования противником хакеров против вас велика, вы можете построить контратаку с самого начала следующим образом: сначала наполните Интернет информацией с максимально большого количества блогов, расположенных на как можно большем количестве различных блоговых площадок. А сайты или блоги-аккумуляторы создавайте лишь в случае, если их удаление из Интернета принципиально не изменит расстановку сил. Распределенной хакерской атаке противопоставьте таким образом распределенную информационную атаку, и вы этим сделаете для противника использование хакеров бессмысленной тратой денег.

Тактический прием «Ссылки как плакаты времен холодной войны»

Один из специалистов, имеющий за плечами опыт практической работы в государственной разведке, сказал об информации, размещаемой на сайтах черных пиарщиков, фразу, которая нам понравилась: «Борьба с информацией на их сайтах напоминает по своим условиям борьбу с плакатами времен холодной войны, размещаемыми на территории противника». Мы согласны с этим утверждением. Действительно, снять размещенный на территории противника плакат или заклеить его своим невозможно. Но зато возможно расклеить собственные листовки на своей территории и на территории союзников. При этом противник также ничего не сможет сделать с этими материалами.

Поскольку в жизни Интернета главную роль играют гиперссылки, лучше всего размещать не просто тексты или изображения, а именно гиперссылки, содержащие в якорных словах текст с ключевыми словами. Такие ссылки одинаково полезны как с точки

зрения привлечения внимания людей, так и с точки зрения продвижения ваших сайтов и блогов-аккумуляторов в поисковых системах. Ведь они ведут с разных адресов, более того, являются постоянными, а это также важно с точки зрения поисковых машин. Просто разместите ссылку с текстом вроде: «Секретов Секрет Секретович – ловкость рук? Легким движением руки книга П. П. Ершова „Конек-Горбунок“ превращается в книгу Секретова Секрета Секретовича». Эта ссылка будет давать возможность увидеть вашу точку зрения людям, а также тематически поднимет ваши сайты и блоги-аккумуляторы в выдаче поисковых машин по словосочетанию «Секретов Секрет Секретович».

Каждый из ваших сторонников сможет без особых усилий поставить эту ссылку на своем блоге или на своем сайте. Лучше, если якорные слова будут немного отличаться на разных сайтах, но при этом всегда в составе якорных слов гиперссылки должны присутствовать ключевые слова, по которым сайт продвигается в поисковых машинах. Дело в том, что антиспамовые фильтры, столкнувшись с совершенно идентичными ссылками, могут посчитать часть из них спамом. Логика простая: разные люди редко дают со-

вершенно одинаковую ссылку, а роботы, как правило, ставят именно одинаковые ссылки, имейте это в виду. Например, если на одном сайте может стоять ссылка с якорными словами «Секрет Секретович Секретов стащил книжку Ершова?», то на другом сайте может быть «Секрет Секретович Секретов сплагиа-тил книжку Ершова?», а на третьем «И зачем стащил книжку Ершова Секретов Секрет Секретович?».

Доски объявлений как инструмент в отражении информационного нападения

Сегодня доски объявлений стали вспомогательным, если не сказать очень важным инструментом информационной войны. Было время, когда они не только позволяли разместить любой текст и при этом хорошо индексировались поисковыми машинами, но и давали возможность ставить активные гиперссылки. Однако легкий доступ на доски объявлений привел к тому, что поисковый спам оккупировал их в значительной степени. В результате практически все они (кроме тематических, где есть жесткая модерация) перестали рассматриваться поисковыми машинами как авторитетные ресурсы. Гиперссылки с них, как правило, тоже не учитываются. Однако если тема вашей информационной войны подходит для размещения на полностью тематической доске объявлений, мы рекомендуем размесить там сообщение. Его прочтет целевая аудитория,

а само размещение не требует особых затрат сил или времени.

Периодически старая информация на досках объявлений удаляется и замещается новой. Обычно доски объявлений можно найти с помощью оператора TITLE (о нем подробно рассказывается в разделе, посвященном языку запросов поисковых машин), который указывает, какие слова должны содержаться в заголовке (title) страницы. Оператор TITLE есть в большинстве крупных поисковых машин. Как вариант применительно к нашему учебному примеру можно найти доски объявлений по таким запросам:

– в Яндексе: + (секретов /1 (секрет / + 1 секретович)) && + (\$title (доска));

– в Гугле: «секретов секрет секретович» intitle: «доска объявлений».

Рейд в «Картинки»

Сегодня благодаря развитию Web 2.0 существует возможность размещать не только текстовую, но и визуальную информацию в Интернете на бесплатных, отлично индексируемых площадках.

Речь идет о двух разных направлениях работы с изображениями.

Прежде всего это бесплатные фотохостинги. Фотохостинги – сайты, открытые для каждого и предназначенные для размещения фотографий. Каждый человек может поместить фотографии на такой площадке и сделать их доступными из любой точки планеты и с любого компьютера. Обычно на современных интерактивных ресурсах можно сделать фотографии общедоступными, а можно поставить их под пароль и разрешить показ только тем, у кого этот пароль есть.

Для того чтобы стало понятно, как можно сделать фотоальбом видимым в поисковых машинах по ключевым словам, надо детально рассмотреть процесс его создания. При создании персонального аккаунта на фотохостинге надо зарегистрироваться, выбрав себе ник, и открыть новый фотоальбом, по-

сле чего дать ему название и, разумеется, занести его в заголовок (Title) страницы.

После этого на фотохостинге размещается фотография, соответствующая теме информационной войны. Если фотографии, которая соответствовала бы теме у вас нет, можете разместить, например, подходящую по смыслу карикатуру. Большой выбор карикатур имеется на сайте anekdot.ru. [56] Несложно найти их и на других сайтах, введя слово «карикатура» в строку поиска любой поисковой машины. Фотографии также дается название, а затем краткое описание.

Достаточно использовать ключевые слова во всех этих случаях, чтобы создать по сути небольшую и очень высокорелевантную интернет-страничку на посещаемой пауками поисковых машин площадке.

Представьте себе, что название фотоальбома «Секретов Секрет Секретович», название фотографии такое же, а краткое описание фотографии звучит примерно так: «Как Секретов Секрет Секретович оказался на обложке книги П. П. Ершова „Конек-Горбунок“? Почему имя П. П. Ершова исчезло, а имя Секретова Секрета Секретовича появилось? Почему Секретов Секрет Секретович так и не дал объяснений этому факту?». Столь явно

относящийся к Секрету Секретовичу Секретову текст будет находиться в выдаче поисковых машин достаточно высоко.

Помимо фотохостингов, «рейд в картинки» может иметь и еще одно направление удара. Мы уже говорили о том, что целесообразно размещать ключевые слова в теге <alt> подписей к рисункам на вашем сайте или в вашем блоге.

Напомним: слова, размещенные таким образом, будут видны в браузере с отключенным просмотром рисунков. Так вот, интерес представляет тот факт, что слова из этого тега с высокой долей вероятности со временем попадут в раздел «Картинки» поисковых машин. Это значит, что в скором времени, помимо привычного изображения вашего противника, при запросе по его ключевым словам вы сможете увидеть там свои графические материалы, иллюстрирующие вашу точку зрения.

Некоторые фотохостинги предоставляют не только услуги хостинга фотографий, но и генерируют ссылки, уже адаптированные по размеру снимка и по формату тегов под форумы, блоги, сайты. Пользователю остается только загрузить фотографию на фотохостинг со своего компьютера, а затем выбрать,

какого размера или для какого ресурса он хочет фотографию адаптировать. После этого автоматически будет дана гиперссылка на фотографию и коды, которые позволяют разместить ее там, где вам требуется. Примером такого фотохостинга может служить очень известный ресурс «Photolava» (www.photolava.com/). После того, как файл загружен на фотохостинг, вам предоставляются коды для вставки рисунка на разные виды интернет-ресурсов и ссылка на страницу, где эти коды всегда доступны. Как выглядит отформатированное изображение на фотохостинге «Photolava», показано на рис. 27.

PhotoLava

Upload Photos Transload Photos My Photos

[Blinking Text](#) [Easter Text](#) [Fathers Day Text](#) [Grandparents Text](#) [Pimp My Profile](#)

Bookmark This Page! (Ctrl+D)

Link to this page

Free Photo and Image hosting for MySpace, eBay, Xanga, LiveJournal, blogs, etc.



View Full Image

HTML

IMG

SHARE

LINK

Remove this image.

Terms of Service

Report Abuse or Request Deletion

My Photos

© 2006-2007 PhotoLava.com

Рис. 27. Изображение отформатировано на фотохостинге «Photolava» и пригодно для вставки на нужные интернет-ресурсы

Сервис сохранения текстов как оружие в информационной войне

В Интернете существует сервис «Ontext» (www.ontext.info). «Мирное» предназначение этого ресурса – сохранение текстов. Его можно использовать в ситуации, когда вам пришлось напечатать какой-то текст и надо его просто сохранить так, чтобы иметь доступ к нему откуда угодно. Текст может размещаться анонимно. Можно отправлять ссылку на него по нескольким адресам электронной почты прямо с сайта «Ontext». Возможно и ведение блога на этой площадке.

После размещения текста на ресурсе «Ontext» вы получите ссылку на страницу, где он находится. Доступ может быть только для вас (если при размещении вы поставите его под пароль) или – по умолчанию – открытый. Теги на «Ontext» не поддерживаются, поэтому гиперссылки оттуда получить нельзя, но вот сами тексты неплохо индексируются. Во всяком случае в нашем эксперименте тексты, помещенные на этот ресурс в мае 2007 года, через три недели оказались на

второй странице Яндекса без каких бы то ни было вмешательств в их продвижение. Количество текстов, которые можно разместить на «Ontext», правилами не ограничено. Форма для размещения текста показана на рис. 28.

Вот что говорится о возможностях этого сервиса на его сайте:



The screenshot shows the 'ontext.info' website interface. At the top right, there are buttons for 'Добавить свой текст' (Add your text) and 'Регистрация/Вход' (Registration/Login). The main header features the 'ontext.info' logo and the text 'сервис быстрой публикации текстов (подробнее)' (fast text publishing service (more details)). Below the header, there is a form with two main input fields: 'Заголовок: (если поле оставлено пустым - сохраняется первое предложение текста)' (Title: (if the field is left empty - the first sentence of the text is saved)) and 'Текст: (все настройки форматирования и HTML-теги игнорируются)' (Text: (all formatting settings and HTML tags are ignored)). Below the text field, there is a checkbox labeled 'скрыть пароль' (hide password) and a password input field with a key icon and the label 'введите пароль:' (enter password:). To the right of the password field is a button labeled 'Получить ссылку' (Get link). At the bottom, there are two rows of navigation links: 'Добавить | Последние | Лучшие | Рейтинг | RSS' and 'Экспорт | Соглашение | Новости | Контакт'. The footer contains the text 'Дизайн - stasooo.com, Разработано в Омске, Владелец - Виктор Зазаричев'.

Рис. 28. Форма для размещения текстов на сервисе «Ontext».

Для всех пользователей

Быстрая публикация текста на веб. Достаточно заполнить содержимое поля «Текст» и нажать на кнопку «Получить ссылку» – ваш

материал будет опубликован на вебе.

Не поленитесь заполнить содержимое поля «Заголовок», в противном случае система сделает это автоматически, используя содержимое поля «Текст».

Вы можете защитить свой текст паролем, выбрав соответствующий чекбокс при публикации.

Все материалы выкладываются на сайте на равных правах. Вы можете их просматривать (закрытые – при наличии пароля) и выставлять свою оценку при помощи динамической системы голосования. Все опубликованные тексты собраны в каталоге (www.onext.info/catalog.html), где доступны разные параметры сортировки материалов. Функционирует полнотекстовый поиск по каталогу. На сайте ведутся рейтинги просмотров (www.onext.info/views.html) и одобрений (www.onext.info/rate.html).

Доступные материалы можно распечатать в специальной версии. Ссылку на публикацию можно отправить по трем адресам прямо с сайта «Ontext».

Для зарегистрированных пользователей

Регистрация в системе проста и требует указания только адреса электронной почты, на который придет информация с запросом

на активацию аккаунта. E-mail выступает вашим логином в системе.

Вы можете сменить пароль, выдаваемый системой в любой момент, воспользовавшись соответствующей функцией в своем профиле.

Каждый ваш текст может быть автоматически снабжен подписью а также идентифицирован именем автора, отличным от логина в системе. В то же время ваши тексты могут добавлять анонимно.

Автоматически каждому тексту в системе присваивается числовой идентификатор. У вас есть возможность давать ссылке свое имя, используя латинские буквы и цифры.

Доступны простейшие инструменты стилистического оформления текстов. Вы можете воспользоваться ими как при добавлении материала, так и при его редактировании – такая функция также доступна.

Если у вас есть готовый файл формата .txt – его содержимое можно импортировать в систему. Так же легко можно экспортировать содержимое любого открытого вами текста в файл аналогичного формата.

На сервере ontext.info вы можете вести простейший блог, который поддерживает экспорт данных в RSS и добавление коммен-

тариев к записям.[57]

Инструменты поиска информации в Интернете, полезные для успешного отражения информационного нападения

Поисковые машины и каталоги как инструменты раскрутки «боевых» интернет-ресурсов и наполнения их контентом

Данный раздел написан с использованием некоторых материалов книги «Интернет-разведка: руководство к действию».[58]

Автоматизация наполнения «боевых» сайтов и блогов тематическим контентом. Вряд ли большинство читателей сможет наполнять свои сайты и блоги большим количеством собственных текстов. Как правило, на это нет ни времени, ни большого количества специалистов. А сайт или блог желательно иметь достаточно большой. Кроме

того, для создания сайтов и блогов-аккумуляторов необходимо организовать постоянный мониторинг Интернета, дабы своевременно и максимально полно обнаруживать контент, который появляется независимо от вас, но может помочь в борьбе против черных пиарщиков. А если на блоге, помимо участия в информационной войне, планируется размещать материалы по сфере деятельности, интересной многим людям, вы вообще не сможете обойтись без материалов других исследователей (в противном случае у вас будет неполная информация по изучаемой теме). Подобное размещение материалов по общим темам часто бывает полезно, дабы не бросалось в глаза, что блог или сайт создан исключительно для целей контратаки на черных пиарщиков, поэтому на практике очень часто придется размещать на блогах и сайтах тексты или фотографии, созданные другими людьми, а значит, вам необходимо уметь быстро и недорого находить нужную информацию в Интернете и отслеживать ее изменения (слово «недорого» в данном случае относится не к покупке контента, а к затратам на интернет-трафик). Освоив то, что написано ниже, вы сможете всегда быть в курсе новинок по теме вашего

блога или сайта, поэтому люди будут читать ваши ресурсы и советовать их знакомым, расширяя тем самым вашу аудиторию. Паукам поисковых машин также нравятся интернет-ресурсы, на которых много тематического контента.

ВНИМАНИЕ! Настоятельно не рекомендуем покупать программы-парсеры,[59] которые механически нагребают обрывки текстов из Интернета и размещают на вашем сайте. Ничего, кроме выбрасывания из поисковых систем, вы этим не добьетесь. Автоматизация, о которой говорим мы, подразумевает быстрый и качественный поиск потенциально полезного вашему интернет-ресурсу материала. Поиск автоматизировать можно и нужно, но оценка найденного материала и принятие решения о размещении в блоге или на сайте должны производиться человеком. При этом помните о необходимости соблюдения авторских прав авторов этих материалов, иначе вы рискуете стать фигурантом уголовного дела. Как правило, условия использования материалов из Интернета изложены в нижней части сайта, на котором эти материалы расположены.

Если вы автоматизируете процесс сбора материалов для блога или сайта с соблюде-

нием озвученных правил, у вас будут хорошие результаты при ощутимой экономии времени.

Почему мы рекомендуем тратить время на изучение языка запросов поисковых машин. Как ни парадоксально звучит, но поиск информации – не главное, для чего нужен язык запросов поисковых машин. Найти информацию обычно можно, потратив значительно меньше времени, чем требуется на изучение языка запросов поисковиков. Но найденная «здесь и сейчас» информация сродни моментальной фотографии, а значительно важнее видеть изменения, происходящие на информационном поле.

По-настоящему вы оцените важность этого инструмента, когда будете проводить мониторинг Интернета в поисках новой информации. При хорошо составленном поисковом запросе вы с минимальными затратами времени увидите только то новое, что появилось по интересующему вас вопросу, и не будете отвлекаться на просмотр информационного мусора. Это правило в равной степени применимо практически к любому виду деятельности, который предусматривает просмотр информации в Интернете.

Мы не будем в этой книге останавливаться на языках запросов поисковиков, ознакомиться с описанием языка запросов поисковых машин можно в разделе «Помощь» этих машин, а более подробно и с примерами – в книге Е. Л. Ющука «Интернет-разведка. Руководство к действию», вышедшей в издательстве «Вершина».

Как поиск с помощью языка операторов запросов поисковых систем может помочь в раскрутке блога или сайта, участвующих в отражении информационного нападения. Если речь идет о сайте или блоге, «заточенном» исключительно под информационную войну, то язык запросов нужен для того, чтобы проводить мониторинг Интернета с целью поиска новых материалов по теме, размещенных вашими союзниками или противниками.

Если блог или сайт решили посвятить какой-то теме, не связанной с информационной войной (например, чтобы в Интернете появилось пять тысяч страниц, на каждой из которых будут стоять гиперссылки на «боевые» ресурсы), необходимость быстрого и качественного мониторинга Сети значительно возрастает.

Как мы уже говорили, для того чтобы блог или сайт не только участвовал в информационной войне, но и пользовался успехом у обычных читателей, он должен содержать полезные для них материалы. Если вы выбрали в качестве контента не художественные рассказы собственного сочинения, а информацию о каких-то событиях, технических устройствах или жизни каких-либо сообществ, вряд ли надо стараться, чтобы все материалы в блоге были вашими авторскими. На наш взгляд, человеческое общество сильно не тем, что каждый его член заново изобретает колесо, а тем, что, познакомившись с изобретениями других людей, каждый привносит что-то свое, и за счет этого все продвигаются вперед.

Однако каждый из ваших потенциальных читателей заинтересован в том, чтобы, во-первых, находить максимально полную информацию по вопросу, которым он занимается, во-вторых, обнаруживать ее как можно быстрее, а в-третьих, тратить на это минимум времени. И если ваш сайт или блог поможет читателю в этом, то он будет приходить к вам снова и снова.

С технической точки зрения эта проблема решена. Сегодня есть бесплатные или просто

недорогие инструменты, которые позволяют автоматизировать поиск новых данных среди массива тематической информации. Однако выделение самого этого тематического массива по-прежнему представляет сложности. Более того, эти сложности постоянно увеличиваются, поскольку объем Интернета стремительно растет, а значит, увеличивается и уровень информационного шума.

Если составить поисковый запрос, который будет отфильтровывать в Интернете нужную вам информацию, вы получите замечательный инструмент, позволяющий быстро наполнять ваш блог или сайт тематическим контентом.

И вновь напомним: не забывайте, пожалуйста, об авторских правах на информацию. Интернет значительно упростил процессы ее сбора и размещения, поэтому и проблемы нарушения авторских прав обострились. Практика показывает, что в большинстве случаев конфликт возникает из-за того, что люди просто забывают дать ссылку на источник информации, размещенной ими. В Интернете очень немного ресурсов, которые запрещают использовать их публикации. Да и то, как правило, они не делают запрет полным. Большинство подобных за-

претов идет от сетевых СМИ. Вот, например, выдержка из правил использования материалов газеты «Ведомости», помещенных на сайте этого издания.

Под использованием понимается любое воспроизведение, распространение, переработка и другие способы, предусмотренные Законом РФ «Об авторском праве и смежных правах»...

Действие настоящих Правил распространяется на информационные агентства, пользователей электронной и печатной версии газеты «Ведомости», официальные интернет-узлы компаний тематические интернет-узлы и интернет-СМИ, еженедельники ежемесячники и прочие печатные издания, газеты, журналы физических лиц и других пользователей (далее Пользователи)...

Любой Пользователь вправе свободно:

- составлять без гиперссылки на источник дайджест любого количества материалов из каждого номера газеты «Ведомости» используя только лид публикаций (полужирный текст, предваряющий текст статьи)

- бесплатно цитировать любое количество материалов газеты «Ведомости» из каждого номера при условии, что объем цитирования составляет не более 50 % новой публика-

ции, в которой оно используется, и для цитирования используется не более 25 % исходной статьи или другого материала газеты «Ведомости»...

До публикации извещать редакцию о намерении использовать материал путем заполнения на сайте <http://vedomosti.ru> следующей электронной Формы....[60]

Подавляющее большинство интернет-ресурсов не налагает ограничений на перепечатку своих материалов при условии, что на источник дана гиперссылка и имя автора материала указано. Это связано с тем, что всем нужны входящие гиперссылки на их сайт, а перепечатка материала сайта со ссылкой на него – идеальный способ получить «честные» входящие ссылки.

Если вы не хотите или не можете придерживаться тех правил, которые указаны автором материалов, то следует отказаться от размещения их копий. Но это не значит, что вы не можете их размещать у себя никаким способом вообще – речь идет об отказе от размещения именно копии.

У вас есть как минимум два законных варианта использования текстов, которые вам понравились, но которые вы по тем или иным причинам не можете скопировать на

свои интернет-страницы. Прежде всего вы можете процитировать небольшой фрагмент текста для того, чтобы его обсудить или проиллюстрировать им свою мысль. При этом вы должны заключить цитируемый текст в кавычки и указать его автора.

Наконец, вы можете пересказать текст своими словами. В этом случае кавычки не нужны, однако вы все равно должны указать, чье произведение пересказываете.

Рассмотрим в качестве примера фрагмент текста Михаила Шолохова, о котором мы уже говорили, изучая операторы языка запросов Гугла. Покажем варианты законного использования текста Шолохова на вашем интернет-ресурсе.

Пример цитирования:

«За Доном в лесу прижилась тихая, ласковая осень. С шелестом падали с тополей сухие листья. Кусты шиповника стояли, будто объятые пламенем, и красные ягоды в редкой листве их пылали как огненные язычки».

Михаил Шолохов, «Тихий Дон»

Другой пример цитирования:

Михаил Шолохов говорил в своем произведении «Тихий Дон»: «За Доном в лесу прижилась тихая, ласковая осень. С шелестом

падали с тополей сухие листья. Кусты шиповника стояли, будто объятые пламенем, и красные ягоды в редкой листве их пылали как огненные язычки».

Третий пример корректного использования чужого текста:

Михаил Шолохов писал в своем романе «Тихий Дон» о ласковой и тихой осени, прижившейся в лесу. Он рассказывал о том, что листья тополей шелестели, опадая с деревьев. Кусты шиповника писатель сравнивал с пламенем, а немногочисленные ягоды на них – с огненными язычками.

Мы рекомендуем всегда ссылаться на автора того текста, с которым работаете. Это ничуть не умалит вашей собственной роли в глазах читателей, но поможет предотвратить возможные конфликты.

Формы расширенного поиска в поисковых системах. Создатели поисковых машин понимают, что не все, кто пользуется их услугами, хотят изучать язык поисковой машины. Тем более что при всей принципиальной схожести синтаксис запросов конкретных поисковых машин отличается друг от друга, а некоторыми из них приходится пользоваться нечасто, поэтому нет смысла изучать этот язык глубоко для каждой поис-

ковой машины.

Форма расширенного поиска дает возможность детализировать запрос. После ее заполнения поисковая машина автоматически расставляет операторы запроса и выдает соответствующий результат. Такая простота в обращении позволяет пользователю добиваться приемлемых результатов с небольшими усилиями.

Однако обратная сторона использования такой формы составления поискового запроса – невозможность его тонкой настройки. Как показывает практика, человек, знающий язык запросов поисковой машины, составит запрос существенно точнее, чем алгоритм, записанный в форме расширенного поиска.

Именно поэтому мы предлагаем использовать форму расширенного поиска только на тех поисковых машинах, которыми приходится пользоваться нечасто, и то лишь в том случае, когда вас устраивает получение неисчерпывающего результата.

Как правило, в форме расширенного поиска пользователь может задать расположение слов запроса на странице: в заголовке страницы, тексте или ссылке на страницу. Можно также запретить образование слово-

форм.

Помимо этого, обычно имеется возможность задать поиск в определенном регионе или на определенном сайте. Ну и, наконец, можно затребовать выдачу документов только определенного формата или на определенном языке. Ограничение поиска конкретным сайтом и документами определенного формата позволяет, например, собрать все презентации, размещенные на сайте, или все документы в формате Microsoft Word (.doc). Иногда эти документы дают возможность получить информацию о противнике, помогающую получить перевес в информационной войне.

Формы расширенного поиска способны создавать относительно простые запросы. Но по-настоящему сложный, тонко настроенный запрос с помощью такой формы обычно составить нельзя.

Поиск картинок. Самый простой способ поиска картинок – искать в специализированных разделах Яндекса, Гугла или других поисковых машин. А смешные картинки, столь востребованные в информационной войне, – на специализированных сайтах, где в огромных количествах представлены «фотоприколы», «карикатуры», «gif-анимация»,

«плакаты» (по этим словам и без специального поискового запроса вы найдете в поисковиках картинки, подходящие для любой ситуации).

Переход в раздел «Картинки» находится выше поисковой строки (как в Гугле) или ниже ее (как в Яндексe). Перейдите в раздел «Картинки» и ищите в нем, вводя ключевые слова в поисковую строку. Не забудьте, что подписи к картинкам не всегда выполняются на русском языке, поэтому пишите нужные вам слова и по-русски, и по-английски, и транслитом.

Например, поиск в «Картинках» Гугла по слову «машина» мы рекомендуем дополнить поиском по словам «car» и «mashina».

Однако не забудьте дать ссылку на источник картинки, поскольку у нее, еще раз напомним, как правило, есть автор.

В принципе в Интернете существуют и сайты, на которых выложены свободные от авторских прав изображения. Алекс Экслер в своем блоге приводит такие ресурсы, содержащие фотографии или картинки, которые можно использовать бесплатно.

Бесплатные фотобанки:

www.adigitaldreamer.com/gallery/index.php

Использование языка запросов поисковых машин, о котором мы подробно говорили выше, дает возможность оперативно и качественно выбрать из массива информации в Интернете те сайты, которые представляют для вас и ваших читателей интерес. Однако простого знания адресов сайтов, которые вам нужны, недостаточно. Просматривать каждую страницу в поисках изменений хотя бы раз в день – очень трудоемко. Сегодня появились технические средства, позволяющие в значительной степени решить эту проблему. Из всего многообразия таких средств мы бы рекомендовали несколько, которые проверены нами в работе и хорошо себя зарекомендовали.

RSS-агрегаторы

Как мы уже говорили в самом начале книги, это приложения, которые позволяют собирать RSS-потоки с разных блогов и сайтов, и читать их все в одном месте, без необходимости посещать первоисточники. RSS-агрегатор автоматически через заданный в настройках интервал времени посещает определенные пользователем сайты и проверяет, не появились ли там новости. Если они по-

явились, RSS-агрегатор уведомляет об этом пользователя и показывает контент. Кроме того, RSS-агрегаторы, как правило, сохраняют принесенные новости в своем архиве.

Сначала появились программы, требующие установки на компьютер пользователя, а затем и он-лайновые сервисы. Рассмотрим их подробнее.

RSSBandit (www.rssbandit.org/). Эта программа устанавливается на компьютер. Она позволяет разнести разные RSS-потoki или группы потоков в разные папки и настроить для этих папок различное время обновления. Программа удобна тем, что информация, собранная с ее помощью, оказывается рассортированной по темам или сайтам, с которых она поступает. Например, можно разместить новости с сайтов, посвященных блогам, в одну папку и задать ей частоту обновления каждые 15 минут, а новости, посвященные компьютерам, – в другую папку, с частотой обновления один раз в три часа. За счет того, что информация поступает в заранее определенные для нее папки, пользователь, получая сообщение, что произошло обновление информации, заранее знает, какого рода новости он получил. Соответственно он может принять решение – надо

ли ему читать их прямо сейчас.

RSS Bandit – бесплатная программа. Единственный ее недостаток, на наш взгляд, заключается в том, что она требует установки на компьютере, поэтому с другого компьютера увидеть свою ленту новостей невозможно. Для тех, кто пользуется более чем одним компьютером, это серьезный недостаток. В остальном, по нашему мнению, программа может считаться одним из лучших RSS-агрегаторов.

Яндекс. Лента (www.lenta.yandex.ru/). Это он-лайнный сервис Яндекса, который доступен после вводе логина и пароля пользователя Яндекса. Как и остальные он-лайнные службы Яндекса, Яндекс. Лента бесплатна. Когда она появилась, уже существовало довольно много он-лайнных RSS-агрегаторов, поэтому ее создатели имели возможность взять лучшее от конкурентов, избежав при этом уже известных ошибок. В результате получился продукт, достойный по праву претендовать на лидерство среди русскоязычных он-лайнных RSS-агрегаторов.

Пользоваться Яндекс. Лентой очень легко. После ввода логина и пароля на доступ к почте Яндекса и другим его службам пользователь переходит по адресу Ленты, добавля-

ет туда те сайты и блоги, изменения и новости с которых его интересуют, и больше ничего ему предпринимать не требуется.

Если еще установить в браузер Тулбар от Яндекса (Yandex Toolbar), который автоматически предлагается скачать каждому пользователю браузера Mozilla Firefox при посещении главной страницы Яндекса, то информация об обновлениях начинает поступать автоматически во всплывающем окошке, а доступ к Яндекс. Ленте становится возможен одним нажатием кнопки на панели браузера.

Вот что пишет о Яндекс. Ленте сам Яндекс: Яндекс. Лента – это новая служба Яндекса для тех, кто хочет читать все интересные новости и блоги на одном сайте.

Яндекс. Лента позволяет объединять RSS-потоки в одну ленту и читать их, отмечая понравившиеся сообщения. Кроме этого, здесь можно подписаться на поисковые запросы из поиска по блогам и форумам и поиска по новостям.

Как начать пользоваться Яндекс. Лентой? Просто! Выбирайте подходящий вариант:

Начать с чистого листа

Вы можете добавить в свою ленту RSS-потоки, указав их адрес (или адрес их сайта),

журналы пользователей и сообществ Livejournal, подписаться на поисковые запросы в поиске по новостям и поиске по блогам и форумам.

Читать ленту друзей

Livejournal – это популярная служба для ведения блогов. Если вы пользуетесь этой службой, то Яндекс. Лента поможет вам лучше организовать ленту друзей. Кроме того, здесь же вы сможете читать и другие блоги.

Читать подписки на новости

Пользователям Яндекс. Новостей: мониторинг СМИ теперь доступен в удобном веб-интерфейсе.[62]

Несомненные преимущества Яндекс. Ленты – удобный и очень простой интерфейс, возможность искать сообщения в Ленте с помощью встроенного поиска и, конечно же, возможность доступа из любой точки земного шара и с любого компьютера, подключенного к Интернету, в том числе со смартфона.

Недостаток у Яндекс. Ленты, на наш взгляд, один – невозможность сортировки RSS-потоков по разным папкам. Там вообще папок нет, это действительно непрерывная лента, в которой каждое новое сообщение располагается выше предыдущего. Информация с разных сайтов идет в том порядке, в

котором она поступала, и перемешивается в Ленте. Избежать этого можно лишь одним способом – завести себе несколько разных Лент, но тогда потребуется каждый раз выходить из своего аккаунта и входить в другой.

Тем не менее Яндекс. Лента настолько удобна, что даже пользователи Живого Журнала все чаще переносят в нее свою ленту друзей (френдленту) и читают ее в Яндекс. Ленте вместе с информацией с остальных интересующих их сайтов.

Особо надо отметить, что, помимо RSS-потоков, можно направить в Яндекс. Ленту и информацию по любому поисковому запросу, введенному в Яндекс. То есть, например, если вы введете в поисковую строку Яндекса запрос, по которому будут выдаваться документы о смартфонах, то можете подписаться на новости по запросу, и вся новая информация, поступающая по вашему запросу в Яндекс, будет автоматически один раз в день размещаться в Яндекс. Ленте.

Подписки на новую информацию, появляющуюся в

поисковых машинах, без использования RSS-агрегаторов

В первую очередь речь идет о подписке на так называемые новости Яндекса по поисковому запросу. Это не новости в их обычном понимании – как последние события, происшедшие в мире. К новостям Яндекса относятся те новые ресурсы, которые недавно проиндексированы Яндексом. Реальный срок публикации этих документов в Интернете может быть достаточно давним, однако для Яндекса они считаются новинками и поэтому попадают в новости Яндекса.

От Яндекс. Ленты эта услуга отличается тем, что новости приходят по электронной почте в виде гиперссылки на документ и небольшого фрагмента текста документа, тогда для чтения Ленты пользователь должен переходить на ее сайт.

Блоггеру или веб-администратору, который ищет новый контент или новые идеи, появляющиеся в Сети, надо иметь возможность своевременно и точно отслеживать изменения на нужной интернет-страничке. Каждый может себе представить, насколько сложная, а чаще всего и вовсе не осуществи-

мая задача встает в таком случае перед специалистом. Вряд ли даже самый внимательный и скрупулезный человек в состоянии быстро и точно оценить изменения в тексте, занимающем несколько страниц.

Для решения этой проблемы несколькими компаниями разработано специальное программное обеспечение – так называемые сторожевые роботы. Это программы, которые, посетив страницу в первый раз, сохраняют ее образ в своей базе данных, а при повторном посещении сравнивают актуальное состояние страницы с этим образом. Если изменения выявлены, программа отмечает изменившиеся места (они становятся похожи на выделенные маркером на бумажном носителе фрагменты текста). Более того – те фрагменты, которые из текста удалены, также обозначаются во многих программах этого класса – как правило, внизу страницы, дабы не мешать восприятию пользователем информации. Подобные программы могут запускаться пользователем вручную, а могут и работать автоматически, по расписанию.

Их главный недостаток заключается в том, что они платные. Правда, стоимость их в момент написания книги колебалась в

пределах 20–40 долларов США и повторная оплата не требовалась, поэтому, на наш взгляд, человеку, который вступил в информационную войну и нацелен на победу в ней, вполне по силам заплатить такую сумму, чтобы сэкономить свое время и повысить качество своего блога или сайта – ведь от этого зависит победа в информационном противостоянии в Интернете.

Давайте рассмотрим эти программы более подробно.

Сторожевой робот WebSite-Watcher. Программа выпущена в Германии, ее официальный сайт www.aignes.com Стоимость продукта составляет около 40 долларов США за индивидуальную лицензию. Кроме того, пользователю дается тридцатидневная полнофункциональная версия, чтобы он успел удостовериться в нужности этого программного обеспечения. Заплатить за WebSite-Watcher требуется лишь один раз, после чего все обновления становятся доступны бесплатно и на неограниченный срок.

Интерфейс программы поддерживает русский и украинский языки, однако раздел «Помощь» до выхода в свет версии 4.06 был написан на английском. После появления версии 4.06 на сайте программы по адресу:

www.aignes.com/wswtrans.htm стал доступен exe-файл (wswhelp_russian.exe), который присоединяет к WebSite-Watcher справочную информацию на русском языке. Работа с русским языком не вызывает у программы никаких проблем, она довольно часто обновляется. Так, на момент написания книги была доступна версия 4.33. Программа работает со всеми версиями Windows – начиная с Windows'95 и заканчивая Vista.

WebSite-Watcher работает как клиент на компьютере пользователя. Это значит, что все закладки и конфигурации хранятся локально на жестком диске компьютера и сервер производителя не участвует в процессе поиска.

Ниже перечислено, что именно может проверять программа (приводится по данным производителя).

1. Любые веб-страницы с текстовым содержанием, независимо от расширения файла. То есть статичные страницы (страницы с расширением файла. htm или. html) и динамичные (с расширением файла. asp, php, и т. д.). WebSite-Watcher также выделит цветом все изменения в тексте.

2. RSS/Atom feeds: RSS/Atom преобразовываются в читаемый html-формат и могут об-

рабатываться как обычные веб-страницы.

3. Страницы, защищенные паролем, – для защищенных паролем страниц вы можете записать макрокоманду, после автоматического выполнения которой страница будет проверена на обновление.

4. Форумы, которые обрабатываются как обычные страницы с небольшой оптимизацией, например, специальной технологией подсветки изменений.

5. Страницы с Javascript – для страниц, содержание которых отображается с Javascript, WebSite-Watcher поддерживает отдельную и более сложную технологию преобразования динамически сгенерированного содержания страницы в статичное содержание.

6. Изображения – если вы отслеживаете изображение, WebSite-Watcher способен обнаружить обновление этого изображения. Изменения в изображении не подсвечиваются.

7. Двоичные (бинарные) файлы – WebSite-Watcher может обнаруживать обновление двоичных файлов (например, файлы zip или exe) сравнением даты файла, размера файла и/или части его содержания (двоичные файлы не будут полностью загружаться при проверке на обновление).

8. Файлы PDF и Flash – файлы PDF и Flash-анимации обрабатываются как двоичные файлы. WebSite-Watcher не подсвечивает изменения в их содержании.

9. FTP-файлы и каталоги – WebSite-Watcher поддерживает отслеживание FTP-файлов и каталогов. FTP-файлы могут проверяться по дате/размеру файла или по содержанию.

10. Интранет – все страницы в сети Интранет могут быть проверены подобно обычным веб-страницам.

11. Локально хранящиеся файлы – WebSite-Watcher может отслеживать любой файл на вашем жестком диске.

После того как WebSite-Watcher установлен и запущен на компьютере, в правом верхнем углу всех наиболее распространенных браузеров (в частности, Internet Explorer, Mozilla Firefox, Opera) появляется значок программы, представляющий собой стилизованный глаз. Вы увидите его в правом верхнем углу браузера левее кнопки, которая позволяет свернуть открытое окно.

Добавление закладки в перечень закладок может производиться двумя способами.

Способ 1. Непосредственно из браузера. Так можно добавить к закладкам ту страницу, которая в настоящий момент загружена

в браузере. При нажатии хоть правой, хоть левой кнопкой мыши на значок «WebSite-Watcher» в правом верхнем углу браузера появляется всплывающее меню, первый пункт которого – «Добавить в закладки» (рис. 29).

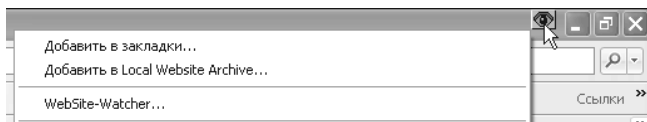


Рис. 29. Добавление страницы в закладки сторожевого робота WebSite-Watcher.

После того как выбирается этот пункт, появляется окно, в котором URL страницы уже автоматически внесен в соответствующее поле. Пользователю остается только ввести вручную имя страницы (это имя не имеет никакого значения для компьютера, а служит только для того, чтобы пользователь смог определить, для чего нужна та или иная закладка, и поэтому может назначаться произвольно). Начиная с версии 4.10 можно обойтись даже без ручного ввода названия страницы, поскольку программа может автоматически брать это название на самой странице.

ВНИМАНИЕ! После того как URL страницы и имя закладки внесены в это окно, требуется нажать клавишу «ПРОВЕРИТЬ!», а не кнопку «ОК». В этом случае WebSite-Watcher отправится на страницу и сохранит в своем архиве ее образ, с которым и будет при следующем посещении страницы проводить сравнение. В главном окне программы WebSite-Watcher после этого напротив имени закладки появится надпись «ОК, инициализировано».

Если же пользователь выберет кнопку «ОК» вместо кнопки «ПРОВЕРИТЬ!», то WebSite-Watcher сохранит закладку в меню, однако не будет посещать страницу, и соответственно не будет и сохранять в архиве ее копию.

Способ 2. Из главного меню программы WebSite-Watcher. Для этого надо открыть окно добавления новой закладки, щелкнув либо по второй слева кнопке на верхней панели программы (она называется «Мастер» и выглядит как жезл с икрящимся наконечником), либо по третьей слева кнопке в той же панели (она называется «Новая закладка» и выглядит как лист бумаги с размещенным на нем знаком «плюс»). Нажатие кнопки «Мастер» предпочтительно, когда проверяе-

мая страница защищена паролем, поскольку там предусмотрен макрос, позволяющий вводить этот пароль автоматически. В остальных случаях мы предпочитаем кнопку «Добавить закладку».

Программа WebSite-Watcher позволяет проверять изменения на странице как вручную, так и автоматически.

Очень легко организовать новые папки и подпапки для систематизации закладок. Причем папки можно перемещать в новые места, просто перетаскивая их мышью.

Кроме того, в программе предусмотрены фильтры, которые позволяют исключать из проверки определенные строки (например, постоянно меняющееся время или дату в углу страницы либо афоризм, который некоторые оптимизаторы сайтов любят постоянно менять на странице). Использование фильтров позволяет исключать неинформативные сообщения о наличии изменений на странице.

Архивирование страницы непосредственно в программе WebSite-Watcher не предусмотрено, однако производитель вместе с ней предоставляет бесплатную программу Local WebSite Archive, которая как раз и создает архивную копию странички Интернета. При

этом Local WebSite Archive может запускаться из того же меню, встроенного в браузер, что и WebSite-Watcher.

Подробное описание этих и других возможностей программы WebSite-Watcher приведено в разделе «Помощь» этой программы, поэтому мы не будем останавливаться на них более детально.

Программа Check&Get. Это отечественный продукт. Преимуществом российского происхождения программы является не только корректная поддержка русского языка, но и возможность ее приобретения за российские рубли, а также доступность создателя программы, если к нему появляются вопросы. Причем техническая поддержка при этом также русскоязычная, в отличие от программ-конкурентов.

Мы подтверждаем, что Дмитрий Скорняков (press@activeurls.com) – человек, который создал и поддерживает программу Check& Get, действительно всегда готов помочь разобраться с проблемой, если таковая возникает. Так, одному из авторов этой книги пришлось столкнуться с ситуацией, когда ни одна из приведенных здесь программ не смогла отследить изменения на сайте некоего российского университета. Попытавшись

понять причины этой проблемы, в бессилии расписались как создатели и администраторы проблемного сайта, так и служба технической поддержки WebSite-Watcher. И только Дмитрий Скорняков внимательно изучил проблемный сайт, разобрался в причинах возникшей ситуации и дал рекомендации, которые позволили устранить проблему. На наш взгляд, это немаловажное обстоятельство, говорящее в пользу программы Check&Get.

Скачать программу можно по адресу: www.activeurls.com/ru/download.php

Вот что говорит о возможностях программы сам ее создатель:

При обнаружении на веб-странице новой информации, Check&Get автоматически сохраняет «снимок» этой страницы в локальную базу данных и информирует Вас указанным Вами способом. Check&Get может послать Вам сообщение электронной почты с содержанием измененной веб-страницы, при этом изменения на странице будут «подсвечены» для их легкой идентификации. Также программа может вывести сообщение на экран или проиграть звуковой файл, информируя Вас об изменениях.

Check&Get автоматически извлекает названия и описания веб-страниц при создании закладки, проверяет Вашу коллекцию на наличие «мертвых» ссылок, находит дублирующиеся ссылки в Вашей коллекции закладок. Check&Get работает с Internet Explorer, Netscape, Mozilla, Opera, позволяя Вам импортировать, экспортировать и синхронизировать закладки. Благодаря этому Вы всегда имеете в выбранном браузере актуальную и организованную коллекцию ссылок.

Список ссылок также может быть импортирован и добавлен к Вашим закладкам из буфера обмена Windows, окна браузера, HTML-файла или офисного документа.

В дополнение ко всему, Check&Get позволяет конвертировать Вашу коллекцию закладок в файл HTML с легкой и удобной навигацией. Это дает Вам возможность опубликовать свои закладки на веб-сайте или создать в Интернет свой мини-портал буквально за пару минут.

На наш взгляд, способность программы импортировать все закладки или их часть в HTML-файл – интересная находка автора. В ряде случаев эта функция открывает очень полезные возможности. Такой файл может

быть использован на сайте как страница с работающими гиперссылками. Причем если его обработать в любом редакторе HTML-файлов, например, в Frontpage или в Dreamweaver, то можно снабдить первоначальный документ необходимыми текстовыми пояснениями или иллюстрациями.

Кроме того, программа Check&Get позволяет одним кликом мыши извлечь все гиперссылки, которые есть на странице.

Полезна и функция удаления «мертвых» и дублирующихся ссылок.

Стоимость программы для частного лица на момент написания книги составляла 580 рублей.

Существует 30-дневная ознакомительная версия программы.[63]

Сторожевые роботы для больших массивов информации. Программы, о которых мы говорили выше, отлично зарекомендовали себя при мониторинге до 500 закладок ежедневно. При большем количестве закладок, как правило, возникают проблемы, связанные с тем, что занесение результатов мониторинга в базу данных делается вручную, чаще всего путем копирования материалов в текстовые файлы – ведь у сторожевых роботов нет собственной базы данных – они

лишь показывают изменения по сравнению с предыдущим посещением сайта. При большом объеме работы это становится очень трудоемким занятием. А крупным компаниям и в «мирное» время, и во время информационной войны в Интернете приходится отслеживать значительное количество интернет-источников.

Для таких случаев существует целая линейка программ «Аваланч» (Avalanche), [64] созданных российским специалистом Андреем Масаловичем, который по праву считается одним из лучших в мире специалистом по созданию аналитического программного обеспечения, а «Аваланч» имеет несколько патентов в разных странах.

В отличие от программ WebSite-Watcher и Check&Get, «Аваланч» умеет не только показывать изменения на сайтах, но и сохраняет эти изменения в собственную базу данных, которая может просматриваться непосредственно в программе «Аваланч», а может быть импортирована в Microsoft Access.

Работа с «Аваланчем» выглядит следующим образом. Сначала настраивается собственный паук программы, которому «объясняют», на какие сайты ему надо ходить за информацией. Он может посещать как от-

дельные разделы сайтов, так и страницы поисковых машин по запросу (например, если на мониторинг поставлена первая страница Гугла по интересующему вас поисковому запросу). Затем настраиваются так называемые умные папки, которые из массива принесенной пауком информации выбирают ту, что относится к определенной теме, и забирают эту информацию к себе. Таким образом, «умные папки» автоматизируют процесс сортировки собранной информации. Эта рассортированная информация хранится в базе данных «Аваланча» и доступна для работы в любой момент.

Более сложные версии «Аваланча», помимо описанной работы, способны к обучению. В простом варианте тексты собираются в Интернете и затем сортируются в программе по прямо указанным ключевым словам. В более сложных версиях они выбираются и сортируются в контексте поставленной задачи, даже если ключевых слов на странице не содержится. Например, если некоторое время вручную помещать материалы, не содержащие ключевых слов, в «умные папки», то со временем, анализируя самостоятельно каждый раз эти тексты, «умные папки» смогут сами распознавать, какие материалы

владелец хочет видеть в данной рубрике. Наиболее продвинутые версии «Аваланча» умеют маскироваться под обычный браузер, не давая таким образом объекту возможности вообще понять, что его мониторят «Аваланчем», а также умеют пользоваться анонимайзерами, скрывающими истинный IP-адрес. Объект изучения пребывает в таком случае в уверенности, что к нему заходил обычный посетитель и не распознает город или страну, откуда вы на самом деле посещали его сайт.

Работа самой продвинутой версии «Аваланча», с точки зрения пользователя, выглядит так. Рано утром «просыпается» паук и идет собирать материал. Когда он заканчивает работу, «просыпаются» «умные папки», анализируют собранное и раскладывают по тематическим рубрикам. Затем на компьютере пользователя создается автоматически локальный сайт, который показывает на экране компьютера руководителя все новые сообщения, рассортированные по рубрикам, а также предоставляет возможность сделать запрос к базе данных и посмотреть архив, оценить ситуацию в динамике.

Существует также версия «Аваланча», которая собирает не только изменения, но всю

информацию по теме, даже если она повторяется. В ряде случаев пользователям бывает нужна именно такая функция.

Но самая простая и недорогая версия «Аваланча» похожа на WebSite-Watcher, дополненный автоматической сортировкой найденных материалов и базой данных, позволяющей их хранить и анализировать. На наш взгляд, «Аваланч» – возможно, лучшее решение на сегодня для автоматического мониторинга и анализа больших массивов информации в Интернете.

Архив сайтов Internet Archive Wayback Machine

Очень часто нападение черных пиарщиков происходит неожиданно для вас. В таком случае вы впервые сталкиваетесь с необходимостью пристального изучения противника. В случае если вы даже предполагали подобное развитие событий (например, в политике), все равно, как показывает практика, есть множество нюансов, которые, возможно, не казались важными вчера, но вдруг приобрели новое звучание. Все это усугубляется тем, что противник, спланировавший нападение, готовится к нему и обычно успевает убрать из Интернета ту информацию, которая могла бы ему повредить. В этом случае на помощь нередко может прийти сервис, который нам первым порекомендовал Arthur Weiss из Великобритании. Мы уже упоминали этот ресурс в начале нашей книги – он называется Internet Archive Wayback Machine[65] и позиционируется как архив Интернета. Пауки, принадлежащие Internet Archive Wayback Machine, посещают сайты в Интернете и сохраняют архивную

копию на его сервере. Как написано на сайте этого ресурса, интересующий нас сайт может и не оказаться в архиве. Например, в случае если паук не может его прочитать, поскольку тот был в свое время запрещен к индексации.

Сервис Internet Archive Wayback Machine – некоммерческий. Как утверждают его владельцы, он живет на пожертвования меценатов и за счет технической поддержки крупных интернет-компаний – таких, как Alexa. Ежемесячно архив Internet Archive Wayback Machine увеличивается в объеме на 20 терабайт. Ценным является то обстоятельство, что он позволяет увидеть копии даже тех сайтов, которых больше не существует в Сети (рис. 30).

Для того чтобы увидеть сохраненную версию нужного сайта, достаточно ввести в окно, расположенное в верхней части главной страницы, именно его адрес и нажать клавишу «Take me Back». После этого пользователю будет предложен архив, имеющийся по запрошенному сайту. В пределах этого архива можно запросить копию сайта за нужную дату.

Нам известны случаи, когда этот ресурс, достаточно хорошо известный российским

специалистам конкурентной разведки, помогал компаниям в сборе доказательств по фактам информационной войны против них. Как правило, в таких ситуациях, когда нападающая сторона «затирала» информацию на сайте, Internet Archive Wayback Machine позволял доказать факт распространения порочащих компанию сведений.

Один из источников автора рассказал о ситуации, когда наличие копии сайта в Internet Archive Wayback Machine позволило доказать в споре с контролирующими органами, что сайт, существование которого вызывало сомнения у контролеров, действительно существовал в тот период, когда компания получила деньги за его разработку и «раскрутку».

Существует удобный бесплатный инструмент, позволяющий легко увидеть архив сайта по интересующему вас адресу. Это уже упомянутый нами сайт be1.ru, где на специальной странице.[66] нужно ввести адрес изучаемого веб-сайта и затем, уже на странице с результатами, выбрать раздел «История сайта». Помимо архивных копий сайтов, на be1.ru можно получить такую информацию об изучаемом интернет-ресурсе, как ссылки на сайт, проиндексированные стра-

ницы сайта, адреса электронной почты, ключевые слова, заголовки, количество гиперссылок на странице, запрещенные к индексации страницы сайта, сайты, содержащие фрагменты такого же текста, IP-адрес сайта и ряд других параметров. На рисунке 31 приведен пример исследования сайта Сбербанка России с помощью сервиса be1.ru



Рис. 30. Главная страница Internet Archive Wayback Machine.

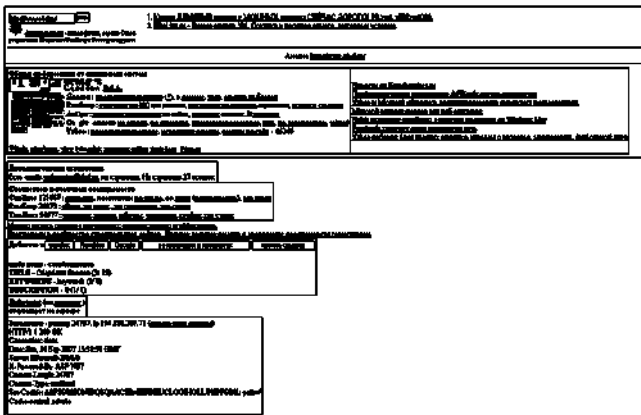


Рис. 31. Результат исследования сайта Сбербанка России с помощью сайта be1.ru

Как обеспечить анонимность перемещений в Интернете при противодействии черному PR

Поскольку противник, совершивший на вас нападение в Интернете, может представлять угрозу вашей жизни и здоровью, считаем необходимым подробно остановиться на вопросах обеспечения анонимности, что очень важно в условиях информационной войны.

Администратор чужого сайта и администратор той организации, которая обеспечивает вашему сайту хостинг, всегда способен увидеть, с каких IP-адресов приходили посетители. Он нередко может наблюдать, на какие страницы и в какой последовательности они переходили и какого рода информацией там интересовались. Эта информация хранится в логах (журналах) сервера. По официальному запросу администратор должен предоставить эту информацию правоохранительным органам. Учитывая степень раз-

вития неформальных связей в нашей стране, нельзя полностью исключать вероятность, что информация о вас окажется в руках у вашего противника.

Как назначаются IP-адреса

Мы не будем чересчур углубляться в вопросы организации компьютерных сетей, но расскажем лишь принцип организации назначения IP-адресов, дабы читатель, который ранее не интересовался этой проблемой, мог быстрее сориентироваться в дальнейшем материале.

Итак, прежде всего надо понять, что в Сети (в данном случае – в Интернете, хотя это справедливо для любой сети) не может быть двух компьютеров с одинаковым IP-адресом. Такая система обеспечивает возможность доставки данных именно на ту машину, для которой данные предназначены.

Компьютеры «знакомятся» друг с другом и передают данные именно посредством IP-адресов. При этом понятно, что людям было бы трудно запоминать эти бессмысленные наборы цифр, поэтому для них придумали доменные имена (вроде yandex.ru или si-razvedka.narod.ru). Для перевода понятных

человеку доменных имен в привычные для компьютеров IP-адреса в Интернете существуют так называемые DNS-серверы, работа которых по сути сводится к пересчету доменных имен в IP-адреса и наоборот по специальной таблице. Существует единый центр по выдаче адресов, который традиционно находится там, где и был создан Интернет – в США. Соответственно, этот центр де-факто, вероятно, способен держать под контролем в той или иной степени весь Интернет.

Как мы уже говорили, когда появляется новый интернет-провайдер, ему выделяется определенный диапазон IP-адресов, а он уже в пределах этого диапазона раздает адреса своим клиентам. Тем не менее город и провайдера по IP-адресу можно установить в любом случае, а физический адрес и название компании – в случае, если IP-адрес фиксированный.

Как «прикрыть» свой IP-адрес

Обычно применяются несколько законных способов прикрытия IP-адреса.

Сразу хотим отметить, что мы рекомендуем проводить работу по поиску в Интернете в рамках информационной войны или кон-

курентной разведки с компьютера, который не подключен к корпоративной сети, так как большинство способов «прикрытия» IP-адреса потенциально могут создать брешь в защите корпоративной сети вашего предприятия.

Вот основные способы «прикрытия» IP-адреса.

1. Воспользоваться обыкновенным модемом, работающим через телефонную линию.

В этом случае администратор посещаемого сайта будет видеть, что посетитель пришел из определенного города, не более того. IP-адрес, который при этом зафиксировывает у себя посещаемый сайт, будет истинным IP-адресом вашего компьютера, поэтому в случае атаки на этот адрес ваш компьютер может быть поражен.

К моменту выхода книги в коммерческой эксплуатации для пользователей были доступны телефоны оператора сотовой связи «СкайЛинк», работающие по технологии «Скай Турбо». Эти аппараты позволяли использовать динамические IP-адреса, при этом реально обеспечивая скорость передачи данных, сопоставимую со скоростью выделенной линии. По нашему опыту, это по-

что идеальное решение для конкурентной разведки и информационной войны, поскольку позволяет в любом месте получить высокоскоростной мобильный Интернет, не «привязанный» к конкретной компании и не создающий угрозы безопасности корпоративной сети. В принципе по запросу официальных органов можно установить, на кого оформлен договор на номер, с которого происходил выход в Интернет. Никто, кроме официальных органов, законно получить эту информацию не может.

2. Воспользоваться GPRS-соединением, без предоставления услуги фиксированного IP-адреса.

В этом случае администратор посещаемого вами сайта увидит, что вы пришли из сети определенного оператора связи определенной территории, с тем же IP-адресом, что и все остальные посетители, пришедшие от этого оператора. IP-адрес, который могут определить на посещаемом вами сайте, при этом будет иным, нежели на самом деле. Связано это с тем, что все пользователи GPRS имеют один IP-адрес, который транслируется сервером сотового оператора посещаемому сайту. Атака на такой видимый сайту IP-адрес вашу машину поразить не сможет, так

как она будет направлена против сервера сотовой компании.

3. Воспользоваться бесплатным анонимным прокси-сервером.

Из-за того, что большинство хакерских атак проводилось через цепочку анонимных прокси-серверов, в Интернете против подобных серверов ведется постоянная борьба.

Тем не менее списки IP-адресов анонимных прокси-серверов свободно доступны.

Вот ресурсы, которые предоставляют подобную информацию:

www.samair.ru/proxy/15.htm;

www.serve4u.chat.ru/wproxylst2.htm;

www.stayinvisible.com/

Настройка браузера на анонимный прокси-сервер выполняется очень просто. Для этого в нем прописывается IP-адрес прокси-сервера и указывается номер порта. И все – можно работать с новым IP-адресом. Как IP-адрес, так и номер порта указаны в списке прокси-серверов. Чаще всего номер порта либо указан прямо, либо запись об этих данных дается в таком формате: 217.556.81.93:35.

Это означает, что 217.556.81.93 – IP-адрес, а 35 – номер порта, которые и надо прописать в браузере.

В браузере «Мозилла Файрфокс» (Mozilla Firefox) версии 2.0.0.6 для того чтобы прописать IP-адрес и номер порта прокси-сервера, надо пройти по ссылкам: «Инструменты > Настройки > Дополнительно > Сеть > Настроить > Настроить параметры подключения прокси вручную».

Мы не рекомендуем пользоваться подобным методом достижения анонимности, так как никто не гарантирует его работоспособность.

Кроме того, обычно это соединение с Интернетом обеспечивает очень низкую скорость работы, и совершенно неизвестно, кто и с какой целью при этом собирает, например, вводимые вами через веб-интерфейс пароли и фиксирует ваш настоящий IP-адрес. Подобная проблема характерна для любого бесплатного ресурса по обеспечению анонимности в Интернете.

Помимо всего сказанного, обычно требуется затратить немало времени, чтобы найти такой прокси-сервер, который вообще работает в данный момент.

Однако, если вы все же выбрали этот способ достижения анонимности, помните: надо обязательно убедиться в том, что эта анонимность действительно существует в дан-

ный момент.

Чтобы убедиться в этом, достаточно подключиться к такому серверу, а затем проверить свой IP-адрес, например, на странице www.leader.ru/secure/who.html Сервис, предоставляемый там, не только позволяет увидеть, какой адрес транслируется сайту при вашем посещении, но и одним щелчком по гиперссылке «Информация о сети и домене» позволяет проверить, кому этот адрес принадлежит. На приведенном ниже рисунке видно, что администратор посещаемого нами сайта видит наш IP-адрес (217.119.94.135), тип браузера (MSIE v 7.0), а также почтовый сервер, принадлежащий провайдеру интернет-услуг в данном случае (mail.uraltel.net) (рис. 32).

Просмотрев данные об IP-адресе в данном случае (для IP-адреса 217.119.94.135), мы увидим, что он принадлежит компании МТС в Екатеринбурге, являющейся провайдером связи в стандарте GSM, и обращение к посещенному нами сайту идет с сервера, расположенного в компании Etel Co. Это показано на рисунке. Здесь же приведены контактные телефоны и адреса электронной почты компании Etel, а также указано контактное лицо, указанное при регистрации домена – в

данном случае это Evgeny Yarchuk (рис. 33).

Для удобства коллег мы разместили переход на вышеуказанную страницу проверки информации о компьютере пользователя прямо на главной странице сайта одного из авторов этой книги Евгения Ющука «Конкурентная разведка» по адресу: www.ci-razvedka.ru

А самый простой способ убедиться в своей анонимности – посетить главную страницу Яндекса. Если вместо погоды в вашем родном городе вам показывают погоду в другой стране, значит, ваш IP-адрес прикрыт анонимайзером.

Во многих случаях при использовании так называемыми анонимными прокси-серверами вы обнаружите, что определяется ваш подлинный IP-адрес. Поскольку посторонние прокси-серверы не взимают платы за их использование, следует понимать, что в случае неработоспособности заявленного сервиса, претензии предъявлять будет некому.

INVESTIGATION REPORT



Another site is up - Tools-On.Net - visit it now !

Please read about possible alerts

Note: If you think that results are incorrect and you're not trying to supply a lot of fake data to the test, let me know - it could be improved.

СОБРАННАЯ ИНФОРМАЦИЯ

Переданный адрес

217.119.94.135

Браузер

MSIE v 7.0

Браузер модифицирован

да

Тэги модификации

iOpus-I-M, SV1

OS

Windows XP

Найденный адрес

217.119.94.135

Имя хоста

отсутствует

Почтовый сервер

mail.uraltel.net

ДЕЙСТВИЯ

ИНФОРМАЦИЯ О СЕТИ И ДОМЕНЕ

Проверка на открытые порты

Рис. 32. Страница проекта leader.ru, на которой показана информация, видимая администратору посещаемого сайта.

General Information
Hostname
Cannot be resolved
IP
217.119.94.135
Preferable MX
mail.uraltel.net

Network Information
Имя
RU-DCNET-MTS
Диапазон адресов
217.119.94.0 - 217.119.95.255
Владелец
MTS-Ekaterinburg, GSM service provider
Расположение
Etel Co
Контактная информация
Evgeny Yarchyk, yarchuk@etel.ru, +7 343 3761709, Viktor S. Grishchenko, gritzko@post.dcn.ru, +7 3432 783101, +7 3432 147713, Evgeny Yarchyk, yarchuk@etel.ru, +7 343 3761709

Domain Information
Имя
URALTEL.NET
Расположение
Registrant ID: AYWALC8-RU, Registrant Name: Uraltel Limited, Registrant Organization: Uraltel Limited, Registrant Street1: Moskovskaya str.11, Registrant City: Ekaterinburg, Registrant State: Sverdlovskaya obl.Registrant Postal Code: 620014, Registrant Country: RU
Сервера имен
ns1.uraltel.net, www.uraltel.net

Leader's Whois module v 4.0 (C) by Alexander K. Yezhov,
admin@leader.ru

Shenlock Holmes.

Рис. 33. Информация о принадлежности вашего IP-адреса, полученная на странице проекта leader.ru

4. Воспользоваться платным анонимайзером.

Если вы выйдете в Интернет через такой анонимайзер, то ваш адрес будет прикрыт адресом прокси-сервера, который принадлежит фирме, предоставляющей услуги этого анонимайзера. Это легальный сервис, поэтому вас сразу предупреждают, что информация о вас записывается и будет выдана по запросу правоохранительных органов, если таковой поступит. Для всех остальных вы будете выступать инкогнито.

К платным анонимайзерам относится, например, программа Steganos Internet Anonym VPN (www.steganos.com). На момент написания книги ее цена на год работы составляла примерно 150 долларов США и купить ее можно было в российском интернет-магазине программного обеспечения Softkey.[67] За эту цену можно было получить возможность пропускать через анонимайзер до 25 Гбайт трафика в месяц. Полностью безлимитная версия стоила в несколько раз дороже.

Steganos Internet Anonym VPN при запуске связывается с сервером производителя и устанавливает с ним защищенное соединение. Данные передаются в зашифрованном виде и перехват трафика не позволит полу-

чить результат.

Примерно так же работает программа Anonymizer (<https://www.anonymizer.com>), цена которой на момент написания книги составляла около 30 долларов США за год использования, без ограничения трафика. По сравнению с Steganos Internet Anonym VPN, анонимайзер Anonymizer работал заметно медленнее и пропускал через себя без сбоев меньшее количество информации. Тем не менее если речь идет не о загрузке файлов на сайты, а о веб-серфинге, программа Anonymizer вполне может быть рекомендована для работы.

Помимо возможности анонимного интернет-серфинга в дистрибутив анонимайзера Anonymizer входит программа по автоматической очистке на вашем компьютере сведений о ваших перемещениях в Интернете.

Кстати, без этого пакета вы можете очистить эти данные вручную, если зайдете в браузере Mozilla Firefox в раздел «Инструменты > Настройки > Приватность > Личные данные > Очистить сейчас».

При платеже в фирму, предоставляющую услуги анонимайзера, неизбежно должна передаваться информация о плательщике. Он получает уникальный ключ, активирую-

щий его копию анонимайзера на определенный период времени.

Информация о том, кто оплатил этот анонимайзер, может быть предоставлена только по официальному запросу Интерпола или полиции страны, в которой находится фирма, предоставляющая услуги анонимайзера. Это возможно лишь при наличии возбужденного уголовного дела, явно не связанного с политическими преследованиями частного лица властями. Если западные страны заподозрят политический компонент в таком уголовном деле, то могут отказать в предоставлении информации, даже если дело возбуждено. Поскольку при противодействии черному PR в Интернете размещается не клевета, а правдивая информация, возбуждение «честного», с точки зрения иностранных государств, уголовного дела, связанного с размещением информации, вряд ли возможно.

5. Воспользоваться бесплатным анонимайзером.

Таких сервисов в Интернете довольно много. Некоторые из них, подобные анонимайзеру Guardster (www.guardster.com/), также приведены на главной странице сайта «Конкурентная разведка» (www.ci-razvedka.-

ru/). Удобство таких анонимайзеров в том, что достаточно ввести адрес нужного сайта в специальное окошко и перейти на него, чтобы стать защищенным. Сделать это можно и инкогнито, не передавая о себе никакой личной информации. Основной недостаток бесплатных анонимайзеров в том, что надо постоянно следить, чтобы не перейти на страницу, минуя окно анонимайзера – например, из раздела «избранное» («закладки») вашего компьютера, так как в этом случае вы окажетесь незащищенным. Кроме того, большинство бесплатных анонимайзеров не поддерживают скрипты, поэтому с ними не работают всплывающие окна и невозможно форматирование текста в визуальном редакторе, например, на сайте или в блоге. Это может несколько затруднить размещение информации.

Есть подобный анонимайзер в российской части Интернета по адресу: www.anonymizer.ru/ (рис. 34).

без нашего сервиса.

Anonymizer.Ru позволяет своим пользователям исследовать просторы сети, оставаясь анонимным для окружающих, не задумываясь о проблемах безопасности и личной неприкосновенности.

Мы ставим перед собой задачу сделать наш сервис самым лучшим и наиболее популярным среди всех ему подобных не только на просторах России, но и во всем оставшемся мире, и поэтому с удовольствием примем любые ваши замечания и предложения.[68]

6. Установить на рабочем месте отдельное соединение через ADSL-модем или выделенную линию, зарегистрированные на частное лицо.

В этом случае вы получите фиксированный IP-адрес, не связанный с вашей компанией. Однако это будет ваш настоящий IP-адрес, одинаковый во всех случаях выхода в Интернет и закрепленный за вашим физическим адресом, поэтому анонимность в данном случае ограничивается только отсутствием записи о вашей компании в журнале веб-администратора посещаемого вами сайта.

7. Воспользоваться публичным доступом в Интернет.

Существуют точки, предназначенные для анонимного выхода в Интернет. К таким точкам относятся wi-fi в кафе, ресторанах, гостиницах, автосервисах и прочих публичных местах. Кроме того, выйти в Интернет можно и из интернет-кафе. Однако следует иметь в виду, что в большинстве таких мест существует видеонаблюдение, а в интернет-кафе достаточно часто на компьютерах установлены клавиатурные перехватчики, позволяющие фиксировать все нажатия пользователем клавиш, в том числе имеется возможность перехватывать пароли и адреса, на которые с этими паролями пользователь заходил.

Как вести затяжную информационную войну в Интернете

Не всегда удастся прекратить информационную войну быстро. К сожалению, весьма возможно, что она приобретет затяжной характер.

Одна из особенностей нашей цивилизации состоит в том, что все более-менее значимые для человечества новшества вначале появляются и развиваются в военной сфере, а уж потом начинают использоваться «для гражданских целей». Не стала исключением и информационная война.

Кстати, впервые термин «информационная война» появился в официальных документах военного ведомства США в начале 90-х,[69] и был введен в оборот директивой министра обороны 21 декабря 1992 года. Смысл, который изначально был заложен в понимание сути информационной войны в «Доктрине борьбы с системами контроля и управления»[70] и «Объединенной доктрине информационных операций»[71] – «комплексное воздействие (совокупность инфор-

мационных операций) на систему государственного и военного управления противника, его военно-политическое руководство с целью принятия им уже в мирное время благоприятных для страны-инициатора информационного воздействия решений и полной парализации инфраструктуры управления противника в ходе конфликта» – во многом применим и к тем действиям, которые применяются для воздействия на массовое сознание граждан внутри общества.

Как совокупность действий информационная война появилась значительно раньше самого понятия и успешно использовалась с давних времен. Те же листовки, которые разбрасывались над окопами противника в годы Второй мировой войны с целью побудить его к сдаче в плен или прекратить сопротивление – по сути, элементы все той же информационной войны. Однако самым ярким примером ведения затяжных боевых действий на информационном поле стала так называемая холодная война 1946–1991 годов, в которой столкнулись непримиримые идеологии капиталистического и социалистического лагерей. Чем это закончилось, известно, пожалуй, всем – крахом советской системы и развалом СССР. Многие исследователи

и аналитики склонны считать, что именно навязывание гражданам Советского Союза (в первую очередь – правящим элитам и интеллигенции) «западных ценностей» и установок на реформы и привело к распаду огромной страны и смене государственного курса.

«К чему это вступление? – спросит нас читатель. – И какое отношение межгосударственные противостояния имеют к теме книги?» Прямое. Холодная война продемонстрировала несостоятельность стратегии руководства СССР в информационной войне против Запада и отсутствие резервов для ведения затяжного конфликта, что и привело к разрушительным последствиям. Уже не является секретом, что стратегическая оборонная инициатива (СОИ), о программе которой в марте 1983 года объявил президент США Рональд Рейган, во многом была блефом, информационным вбросом, рассчитанным на ответную реакцию руководства СССР. И эта реакция не заставила себя ждать – Советский Союз был втянут в очередной виток гонки вооружений, что окончательно доконало и без того разрушающуюся экономику страны.

Ввязываясь в затяжной конфликт, к которому относится длительная информационная война вообще и в Интернете в частности, вам стоит четко дать себе ответ на два как минимум вопроса: верна ли ваша стратегия действий и хватит ли вам сил на всю дистанцию?

В обществе масштабные информационные войны чаще всего ведутся в политике и бизнесе. Но в основном затяжной характер конфликты приобретают именно в бизнесе, чему есть вполне логичные объяснения.

Российские политики еще не привыкли руководствоваться хрестоматийным правилом своих западных коллег, которые считают, что новая предвыборная кампания начинается на следующий день после победы на выборах. В нашей стране до сих пор в почете короткие кампании, когда кандидаты на выборные должности вспоминают о необходимости начала избирательной гонки лишь за несколько месяцев до дня выборов. Возможно, эта особенность отечественной политики связана с еще не до конца сформированными политическими традициями, а возможно, это наше родное «авось успеем».

Так что, захоти мы изобразить информационные войны в политической сфере в гра-

фическом виде, то скорее получится не прямая линия, а синусоида, где верхним точкам графика будет соответствовать колоссальная концентрация ресурсов и напряженные боевые действия, спадающие до нулевой отметки по окончании избирательной кампании.

Еще одна особенность информационной войны в политике – ее достаточно низкая эмоциональная составляющая, потому что проводят ее, как правило, профессионалы.

Но в бизнесе конечного срока, к которому надо успеть победить, обычно нет (если только речь не идет о срыве контракта или переговорах с высокопоставленным лицом, к визиту которого нужно дискредитировать предпринимателя). А ресурсы, выделяемые для информационной войны владельцами бизнеса, как правило, меньше, чем в политике. Бизнесмен, даже когда он обращается к услугам профессионалов по информационным противостояниям, чаще всего сам старается принимать участие в боевых действиях, чем крайне осложняет и без того нелегкую задачу PR- и кризисных специалистов. Действия заказчика почти всегда выбиваются из стратегического плана и ставят под угрозу его успешное воплощение. А уверенность его в том, что он как плательщик име-

ет полное право вмешиваться в ход войны, во многих случаях делает его практически непредсказуемым и тем более неуправляемым. Информационная война в бизнесе, в отличие от политики, часто перерастает в межличностный конфликт, развивающийся даже тогда, когда его продолжение абсолютно нецелесообразно и ничего, кроме вреда, обеим сторонам принести не может. Если у вас нет стратегии ведения войны в такой ситуации и ресурсного обеспечения на затяжные позиционные бои, то лучше вообще в конфликт не ввязывайтесь. Длительные боевые действия, в том числе в информационной войне, без стратегии вестись не могут – в противном случае это будет беспорядочными вылазками, войной на истощение. На ваше истощение.

Но если конфликт стал затяжным, и при этом стратегия ведения войны у вас разработана, вы должны распределить ресурсы так, чтобы они обеспечивали непрерывное добавление новых материалов в Интернет. При этом можно выделить два основных метода работы.

1. Прием «Поплавок». На определенном этапе информационной войны наступает момент, когда первоначальные попытки

сбить ваши ресурсы DOS-атаками доказали свою бесперспективность и остались в прошлом, интернет-ресурсы, продвигающие вашу точку зрения, находятся достаточно высоко в выдаче поисковых машин, но при этом выше них или выше части из них расположены ресурсы противника. В этот момент мы рекомендуем сосредоточиться на продвижении вверх не любых ваших сайтов или блогов, а тех, которые уже находятся достаточно высоко. Ведь они уже прошли отбор у поисковых машин и чем-то им «понравились», раз поднялись высоко в выдаче. Для того чтобы продвинуть их еще выше, надо давать на них новые гиперссылки, лучше постоянные. В текстах на страницах ваших интернет-ресурсов ключевые слова должны становиться якорными словами гиперссылки на один из ресурсов-поплавок. После текста (или сбоку от него, если текст очень большой) желательно также ставить гиперссылки, которые в качестве якорных слов содержали бы не только ключевые слова, по которым проводится продвижение сайта, но и другие (причем разные в разных гиперссылках). В больших текстах, по мнению ряда специалистов, нежелательно ставить ссылки после текста, а лучше поставить

их сбоку в верхней части страницы, поскольку пауки имеют ограничения по размеру индексируемого текста и могут просто не дойти до конца страницы.

Например, в тексте словосочетание **Секретов Секрет Секретович** может стать гиперссылкой, ведущей на сайт № 1, а на сайты № 2, 3 и 4 будут вести после текста или сбоку от него ссылки **Секретов Секрет Секретович** и «Конек-Горбунок», почему **Секретов Секрет Секретович** любит куличи, ну, **Секретов Секрет Секретович**, «вы, блин даете»!

2. Мероприятие «Полярная ночь». Если информационная война перерастает в затяжной позиционный конфликт, то важно создать количественный перевес над противником. Тем более что в Интернете это количественное изменение обязательно приведет к качественному росту.

Для достижения этой цели можно использовать методику, примененную на практике под условным названием «Полярная ночь». В рамках реализации этого плана в Интернете на ресурсах Web 2.0 следует регулярно (лучше – ежедневно) размещать определенное количество сообщений, изобличающих противника и/или поддерживающих ваш собственный имидж. Количество этих сооб-

щений зависит от масштабов информационной войны и от того, какими финансовыми и кадровыми ресурсами вы располагаете. Если ваши сообщения представляют интерес для широкой публики, то, возможно, подобное мероприятие будет проводиться спонтанно, по инициативе ваших сторонников, и усилий от вас не потребует.

Ресурсы Web 2.0 предпочтительны, потому что их RSS-потоки попадают в раздел «поиск по блогам» Гугла или «Блоги Яндекса» в Яндексе, и это позволит дополнительно проинформировать большое количество людей.

Постоянно увеличивайте количество площадок, с которых идет ваша контратака. Проще всего с этой целью увеличивать количество блогов. Старайтесь использовать блоги с разных площадок, поскольку к ним по-разному относятся различные поисковики. Так, например, на момент написания книги блоги Живого Журнала были «любимы» Гуглом, тогда как блоги Liveinternet.ru им игнорировались. Яндекс периодически диаметрально менял свое отношение к блогам в Живом Журнале, зато с блогов на Liveinternet.ru публиковал длинные списки со страниц, где группируются теги. А ведь помимо этих двух основных блогowych пло-

щадок есть и другие. Используйте их все. Ищите зарубежные площадки. Ищите площадки на региональных порталах. Невозможно заранее предсказать, как к какой площадке относятся те или иные поисковые машины. Так, при наблюдении за одним корпоративным конфликтом в Интернете вдруг выяснилось, что неизвестная ранее нам блогерская площадка в Украине настолько «любима» Гуглом, что размещенный на ней кем-то из участников конфликта блог через сутки оказался на первой его странице.

Со временем давление вала информации, размещенной вами в Интернете, будет нарастать. А по мере «взросления» ваших блогов их авторитет будет повышаться, что даст вам дополнительные очки в борьбе против черных пиарщиков.

«Зачистка» Интернета по окончании информационной войны. Возможна ситуация, когда будет принято решение свернуть мероприятия по отражению информационного нападения в Интернете. Причины при этом могут быть самыми разными, но, с технической точки зрения, дальнейшие мероприятия от них не зависят. Важно, что появляется необходимость убрать из Интернета материалы, участвовавшие в информационной вой-

не.

Это не всегда надо делать необратимо. Значительно чаще имеет смысл «оставить бронепоезд на запасном пути», чтобы при необходимости возобновить мероприятия в любой момент.

Что можно предпринять для этого? Проще всего с блогами: их можно просто поставить «под замок». Для этого в настройках блога для всех его страниц указывается режим просмотра «только для друзей» или «лично-е». В первом случае запись будет видна только тем, кто внесен вами в список друзей, а во втором – только вам. В обоих случаях поисковые машины не увидят ваши сообщения и со временем они исчезнут из Интернета (правда, на это может уйти от одной недели до года). Если активно обращаться к администрации поисковиков с просьбой снять информацию на том основании, что на страницах Интернета ее нет, процесс снятия информации можно сократить до нескольких дней. При аргументированном обращении администрация поисковых машин идет на встречу пользователям (но речь идет только о страницах, на которых больше нет текста, содержащегося в КЭШе поисковых машин).

На сайтах можно просто поменять содержимое страницы на другое, сменить адрес страницы, не давая на нее гиперссылок, убрать страницу с сайта полностью или закрыть сайты целиком.

Сервисы закладок, фотохостинги и страницы на других социальных сетях также можно «поставить под замок».

Сложнее обстоят дела с ресурсами, которые открыты не вами и вам неподконтрольны, либо если забыты пароль и адрес электронной почты, указанные при открытии (на практике подобное явление встречается довольно часто – когда в азарте войны экстренно открываются площадки, коды доступа к которым потом никто не может вспомнить). В таком случае иногда нельзя сделать вообще ничего. Людей, перепечатавших ваши тексты, еще можно попросить убрать их (хотя не факт, что они пойдут вам навстречу), а вот площадки, к которым утерян доступ, могут остаться в Интернете навсегда.

Единственным действенным средством борьбы против оставшихся интернет-ресурсов является сдвигание их в глубины Интернета ресурсами противника, несущими читателю позитивную информацию о нем. Од-

нако вашему противнику это удастся только при вашем молчаливом согласии. Достаточно вам принять меры к подъему этих раскрученных и заточенных под войну против конкретного врага страниц, как все его усилия окажутся напрасны. Поэтому даже самый упертый противник, получивший в Интернете отпор, понимает, что «повторный курс лечения» может быть прописан ему в любой момент.

Функциональный план действий по отражению негативной информационной атаки в Интернете

Приведенный ниже функциональный план действий по отражению негативной информационной атаки в Интернете – это, разумеется, не более чем пример. Для разработки этого плана авторы представили ситуацию появления в Интернете черного PR, направленного на деловую репутацию бизнесмена, работающего в сфере строительства. Для более четкой детализации действий можно добавить в план графу «сроки», хотя для информационной войны в сетевом пространстве это непринципиально – здесь нет четких временных границ, связанных, к примеру, с графиком выхода традиционных СМИ.

Функциональный план представлен в табл. 2.

№	ДЕЙСТВИЕ	Примечания
1. Анализ атаки		
1.1	Выявление направления атаки	В данном разделе плана попытайтесь дать себе ответы на вопросы: «На что направлено нападение?», «Какую цель преследует агрессор?», «Кто может быть лицом или заказчиком?», «Как может развиваться ситуация?» Чем яснее вы сможете представить себе проблему, тем вернее будут ваши дальнейшие шаги
1.2	Определение возможной цели	
1.3	Определение возможного источника	
1.4	Прогнозирование развития нападения	
2. Постановка целей		
2.1	Доведение моей точки зрения до аудитории	Четко и ясно определите цели, которые вы хотите достигнуть в этой информационной войне. Не ставьте себе цели вроде «довести противника до полной нищеты и несуществования». Едва ли вы сможете их достичь, да и обратная реакция загнанного в угол оппонента может вас весьма неприятно удивить. Достаточно будет отразить нападения, сохранить свою репутацию и отбить желание говорить агрессию. Выводить ресурсы на позицию можно бесшумно — например, публикуя нейтральные по содержанию тексты, содержащие ключевые слова. В таком случае в момент начала контратаки просто меняется текст. Ресурсы уже раскрычены, поэтому удар получается ошеломляющим. Недостаток этого способа в том, что некоторое время — обычно от недели до месяца — стороннему наблюдателю будет казаться, что вы не предпринимаете никаких ответных мер. Можно выводить ресурсы «шумно», сразу публикуя с них материалы о противнике. Этот способ позволяет немедленно продемонстрировать, что вы начали противоздействие, но некоторое время противнику (в особенности плохо представляющему себе возможности
2.2	Дискредитация источника порочащей информации	
2.3	«Размывание» негативной информации	
2.4	Понижение рейтинга «моих» ресурсов в поисковых системах и количества этих ресурсов. Планирование архитектуры «сетевой группировки». Принятие решения о шумном или бесшумном выводе своих ресурсов на позиции перед ударом	
2.5	Снижение рейтинга ресурсов противника в поисковых системах (как правило, достигается незаконными действиями, поэтому будет рассмотрено в этой книге)	

Продолжение табл. 2.

		и механизмы работы Интернета) будет казаться, что вы слабы и угрозы не представляете. Выбор предпочтительного способа поиска контента зависит от конкретной ситуации
3. Целевая аудитория		
3.1	Деловые партнеры	Определите целевую аудиторию, на которую будет рассчитано ваше основное воздействие. Не забывайте, что Интернет – это максимально открытая информационная площадка, где любой желающий легко получит доступ к вашим материалам и ресурсам. Подача материала должна быть максимально интересной для целевых аудиторий, но тем не менее достаточно понятной для большинства интернет-пользователей
3.2	Референтная группа	
3.3	Интернет-СМИ	
3.4	Традиционные СМИ	
3.5	Индустриальные аналитики	

Заключение

Когда мы начинали писать эту книгу, в большинстве источников преобладала точка зрения, что черному PR в Интернете противостоять невозможно. Наш опыт показал, что это не так. Противостоять черному PR в Интернете можно и нужно. Главное правильно оценить степень опасности, рассчитать свои ресурсы и как можно скорее проконсультироваться с профессионалами. Даже если затем вы станете противодействовать агрессии сами, вам все равно необходимо грамотно выстроить стратегию и определить наиболее уязвимые точки – ваши и противника. Мы считаем, что противодействие черному PR в Интернете должно осуществляться как органичная часть репутационного менеджмента предприятия или персоны, и в этом случае успех будет наиболее полным.

В целом же можно сказать, что Интернет в начале XXI века устроен таким образом, что сторона, которая выступит в роли агрессора, проиграет с большей вероятностью, чем та, что станет обороняться, потому что победить в информационной войне в Интер-

нете можно лишь в том случае, если вы способны дискредитировать противника полностью и на самых жизненно важных для него направлениях. В противном случае очень скоро получится лишь выравнивание уровня негативной информации против обеих сторон. Это вряд ли может устроить агрессора, но обычно вполне устраивает того, на кого напали. Ведь если вначале обороняющаяся сторона была «в негативе», а агрессор – нет, то затем они оказываются запачканы оба. Но вряд ли такая ситуация порадует нападавшую сторону.

Таким образом, если на вас напали в Интернете, не надо поддаваться панике. Дать противнику эффективный отпор можно. А при грамотном и профессиональном подходе к организации обороны можно даже получить при этом дополнительные дивиденды.

Примечания

1

Мы вообще-то довольно саркастично относимся к попыткам окраски PR в любой цвет. С нашей точки зрения, технология не может быть «черной» или «белой». С таким же успехом можно говорить о ядерной физике как о «черной физике», а о микробиологии как о «черной биологии» лишь потому, что первая дала миру атомную бомбу а вторая – бактериологическое оружие.

2

От *schelmen* (нем.) – объявлять подлецом.

3

www.bd.fom.ru/report/map/int0701

4

По данным компании comScore Networks (США), проводящей подсчет пользователей КузинЮщук А. В.: Противодействие черному PR в Интернете / 4

сети Интернет, www.comscore.com/

5

Региональное информационное агентство
«Дейта ru», www.deita.ru/

6

Сервис Яндекса «Пульс Блогосферы».
www.blogs.yandex.ru/pulse/

7

www.ru.wikipedia.org/

8

www.steganos.com/us/products/home-office/internet-anonym-vpn/overview/

9

www.tor.eff.org/overview.html.ru

10

Голикова Л. Любовь к искусству со взглядом на будущее, www.ko.ru/document.asp?d_no=1106&cp_no=31&cp_type=ct_no.14.12.1999.

11

www.ru.wikipedia.org

12

www.community.com/darom/

www.livejournal.com

13

www.community.livejournal.com/fmob

14

www.blogging.ru/obzor-sajtov-socialnyx-novostej/

15

www.cnews.ru/news/line/index.-shtml?2005/09/20/187391

16

www.dolboeb.livejournal.com/781076.html

17

www.dolboeb.livejournal.com/781076.-html?thread=20507156

18

Guestbook (*англ.*) – гестбук, гостевая книга.

19

Спам (spam) (англ.) – электронные почтовые сообщения, присылаемые вам от неизвестных людей или организаций, которым вы не давали на это разрешения.

20

DoS-атака, от *DenialofService* – «отказ в обслуживании» и DDoS-атака, от *DistributedDenialofService* – «распределенный отказ обслуживания» (англ.) – разновидности хакерских атак на компьютерные системы. Их целью является создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен. Википедия. www.ru.wikipedia.org

21

www.humour.tom.ru/anekdot/anekdot7.-html

22

Вальтер Николаи. Военная пропаганда в Первой мировой войне. www.ru-ci.ru/Valter_Nikolai_Voennaya_Propaganda.html

23

Ольшевский А. С, Ольшевская А. С. Негативные PR-технологии. – М.: Инфра-М, 2004.

24

Лири Т. Семь языков бога. – М.: Пересвет: Янус, 2001.

25

К сожалению, описание методов и инструментов, которые с довольно высокой точностью могут доказать причастность того или иного человека к информационной атаке, выходят за рамки этой книги и потому рассматриваться не будут.

26

КузинЮщук А. В.: Противодействие черному PR в Интернете / 4

27

Справка по изучению практики рассмотрения федеральными судами Республики Хакасия за 2004–2006 года дел о защите чести и достоинства, частной жизни граждан/Верховный Суд Республики Хакасия. Отдел обеспечения судопроизводства по гражданским делам. Абакан. 22 декабря 2006 г. www.supcourt.khakasnet.ru/obzor/chest2004-2006.-html

28

Post (*англ.*) – почта. В контексте употребления в Сети – написанные и отосланные сообщения для какой-нибудь телеконференции.

29

Салтыков-Щедрин М. Е. Собр. соч.: В 20 т. Т. 16. – М., 1974. С. 270.

30

Гоголь Н. В. Театральный разъезд. Сочинения Гоголя, 1842. С. 587.

31

Spin-doctor – на современном американском политическом жаргоне политтехнолог, эксперт по связям с общественностью, специалист по контактам с прессой, препарирующий информацию в духе, выгодном предоставляемой им политической структуре, и обеспечивающий ее подачу в СМИ под нужным углом зрения.

32

В то время – председателя совета директоров КрАЗ.

33

www.kogot7.freesevers.com/

34

www.comromat.ru

35

www.flb.ru

36

Контент – информационное наполнение сайта.

37

Индекс цитирования – показатель авторитетности и популярности веб-сайта, измеряющийся частотой его цитирования.

38

Поскольку это явление носит уже не единственный характер, а каждый отдельный факт появления сайтов-клонов вызывает широкий общественный резонанс, мы, не претендуя на авторство, считаем возможным использовать термин «клонер» в отношении создателей подобных интернет-ресурсов.

39

Мишень, объект, цель – люди или организации, против которых направлены усилия черных пиарщиков.

40

Message (*англ.*) – содержание коммуникативного сообщения, основная идея, концепция сообщения.

41

«Почтовый клиент» – программа, предназначенная для чтения, приема, отправки и других операций с письмами.

42

Калмыков А. А., Калмыкова Л. А Интернет-журналистика. – М.: Юнити, 2005. С. 115.

43

Wikipedia, www.en.wikipedia.org/wiki/Blog

44

Википедия. Статья RSS www.ru.wikipedia.org/wiki/RSS

45

www.yushchuk.livejournal.com/tag/

46

Белов А. Подкастинг у всех на ушах, [www.-internetua.com/in/2436](http://www.internetua.com/in/2436)

47

Рамблер Vision. Описание проекта, [www.-help.rambler.ru/article.html?s=183&id=153](http://www.help.rambler.ru/article.html?s=183&id=153)

48

Живой Журнал. Поддержка. Вопросы и ответы, [www.livejournal.-com/support/faqbrowse.bml?faqid=268](http://www.livejournal.com/support/faqbrowse.bml?faqid=268)

49

Зачем он это сделал, мы не знаем. Но известно, что после этого поступка господин Секретов стал широко рекламировать себя и свое творение, особо подчеркивая, что именно он является автором.

50

Ашманов И., Иванов А Продвижение сайта в поисковых системах, – М.: Вильямс, 2007.

51

Евдокимов Н. В. Основы контентной оптимизации – М.: Вильямс, 2007.

52

www.wiki.liveinternet.ru/ServisDnevnikovLiveInternet/Soobshhestvo?v=197v

53

Подольн Р. Слухи о смерти форумов сильно преувеличены. www.habrahabr.ru/blog/i-am_clever/10313.html

54

КузинЮщук А. В.: Противодействие черному PR в Интернете / 4

Подольн Р. Слухи о смерти форумов сильно преувеличены. www.habrahabr.ru/blog/i-am_clever/10313.html

55

10 Minute Mail. www.10minutemail.com/10MinuteMail/index.html

56

www.anekdot.ru/

57

www.ontext.info

58

Ющук Е. Интернет-разведка. Руководство к действию. – М.: Вершина, 2007.

59

Парсинг – в данном случае процесс автоматического сбора определенных данных с сайта с помощью специально настроенных программ.

60

Правила использования материалов газеты «Ведомости». www.vedomosti.ru/about/rules.shtml

61

Блог Алекса Экслера. exler.livejournal.com/325982.html

62

Яндекс. Лента lenta.yandex.ru/

63

Сайт программы Check&Get. www.activeurls.com/ru/news.htm

64

Подробную статью о «полевых испытаниях» «Аваланча» можно прочитать по адресу: www.ci-razvedka.ru/Avalanche.html

65

www.web.archive.org

66

www.be1.ru/services/stat/

67

www.softkey.ru

68

69

Есть и другое мнение, согласно которому термин «информационная война» впервые появился в статье Сергея Митрофанова «Информационные войны эпохи заката гласности» (/Коммерсантъ. 1991. 4 февраля).

70

1996 г.

71

1998 г.