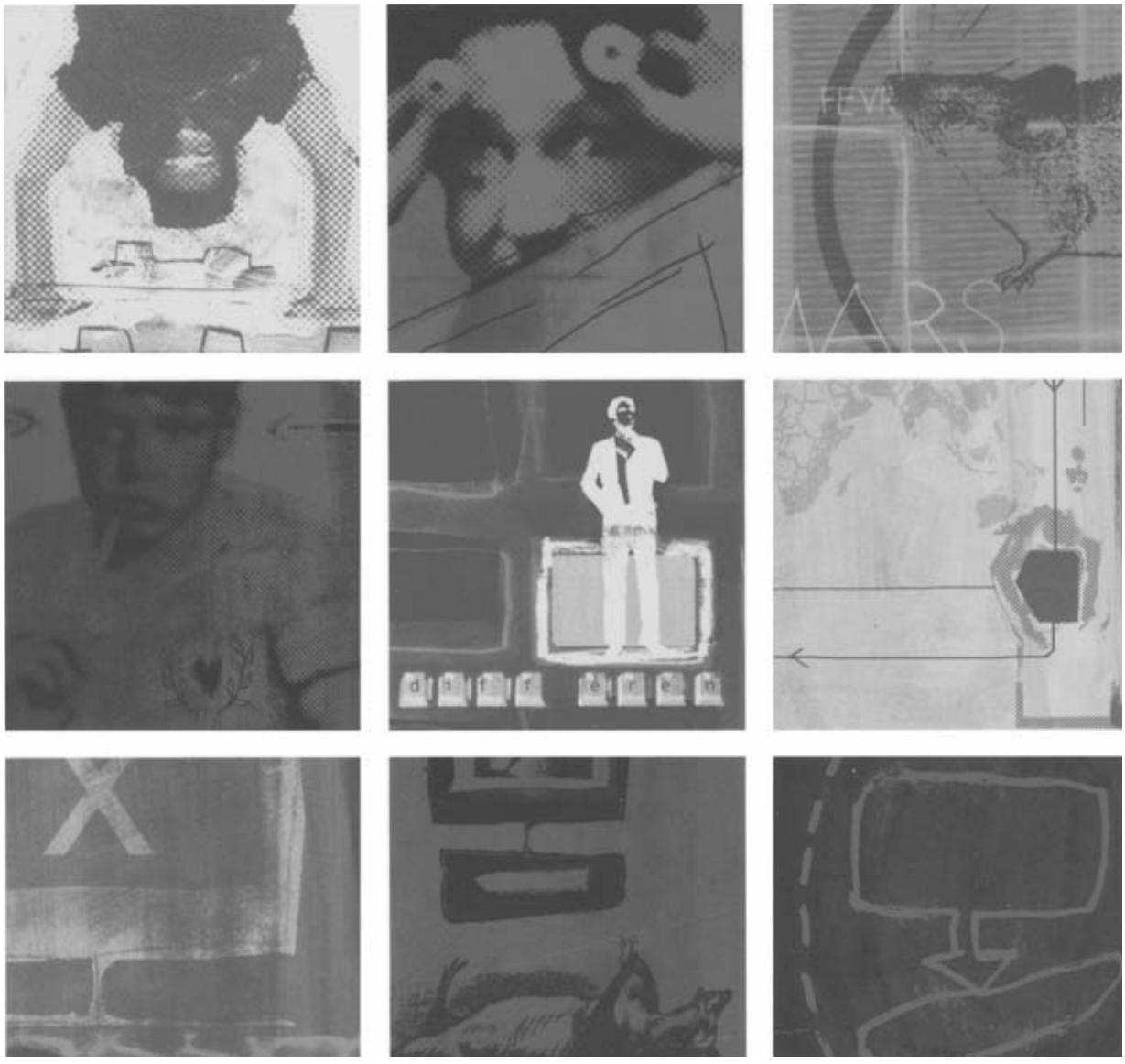
ПОСОБИЕ
ДЛЯ БЛОГГЕРОВ

РЕПОРТЕРЫ БЕЗ ГРАНИЦ



СЕНТЯБРЬ 2005

reporters
without borders
www.rsf.org

ПОСОБИЕ
ДЛЯ БЛОГГЕРОВ
РЕПОРТЕРЫ БЕЗ ГРАНИЦ

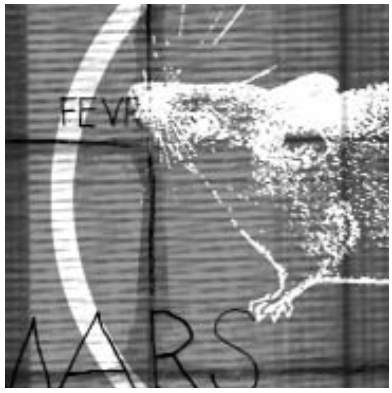
СЕНТЯБРЬ 2005

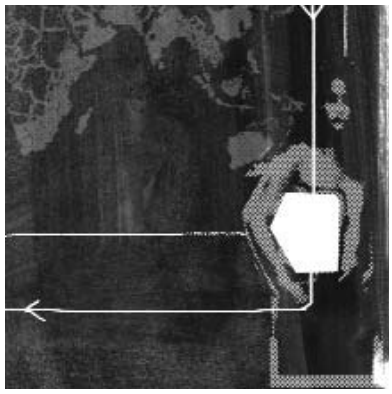
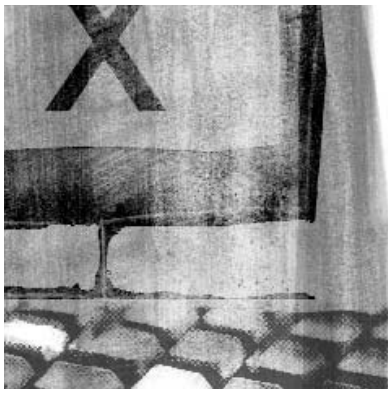
reporters
without borders

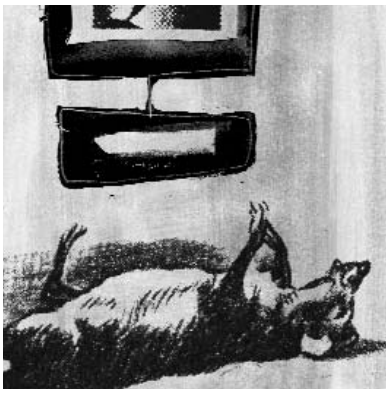
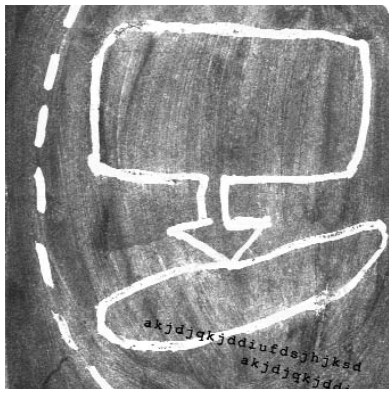
www.rsf.org

ПОСОБИЕ
ДЛЯ БЛОГГЕРОВ
СОДЕРЖАНИЕ

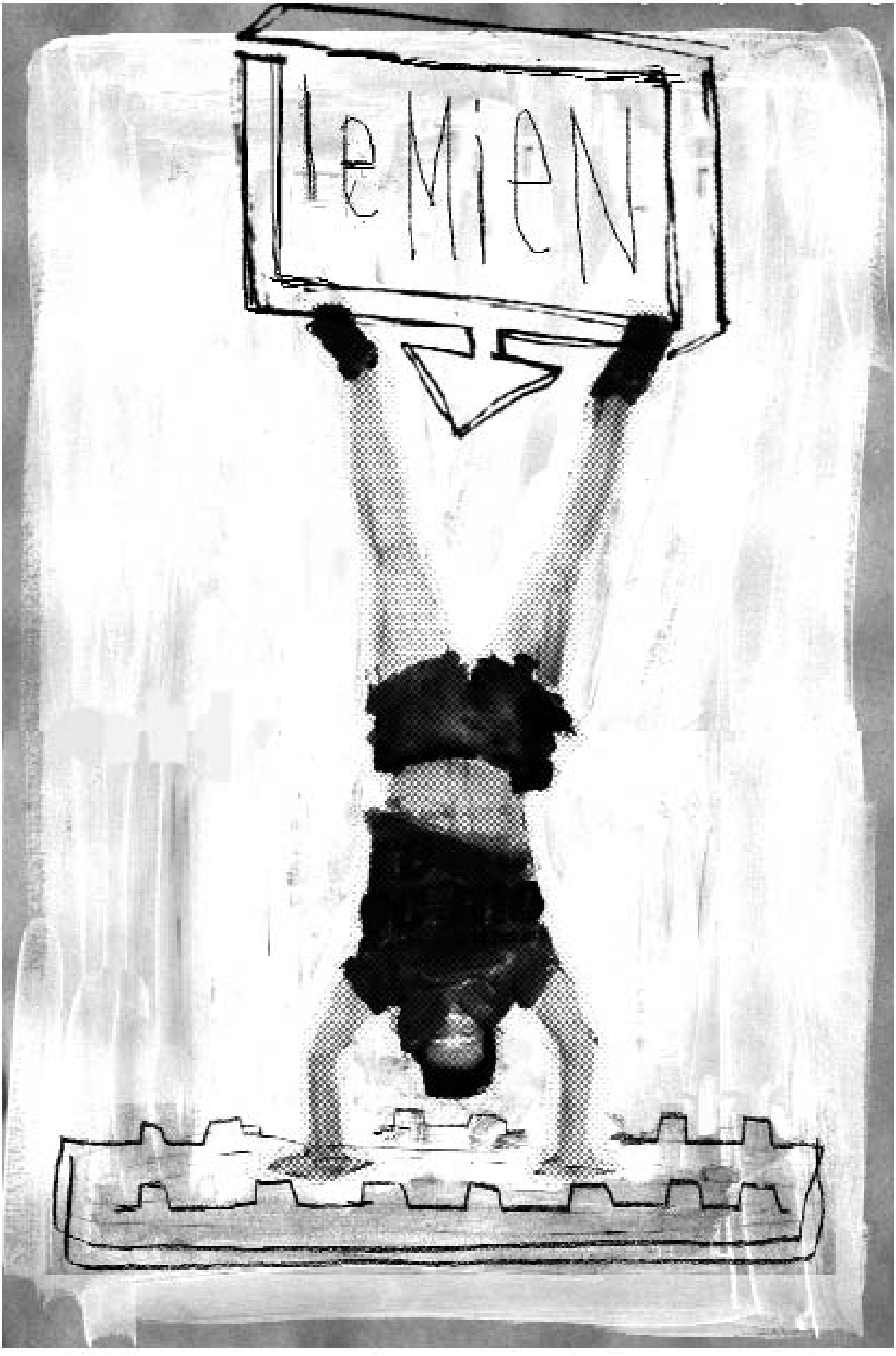




ISBN : 2-915536-36-8


LE MIEN

БЛОГГЕРЫ, НОВЫЕ ГЛАШАТАИ **СВОБОДЫ**

Жюльен Пэйн (Julien Pain)

Блоги восхищают людей. Или, напротив, беспокоят и мешают. Одни не доверяют им. Другие видят в блогах авангард новой информационной революции. Очевидно одно: они бросают вызов медиа в разных странах – от Соединенных Штатов до Китая и Ирана.

Еще рано выносить оценку блогам. Мы десятилетиями читаем газеты, смотрим телевидение и слушаем радио, мы научились быстро отличать новость от комментария, таблоид от серьезного журнала и развлекательную программу от документального фильма.

Однако по отношению к блогам у нас нет еще четких ориентиров. Эти «онлайновые дневники» различаются между собой еще больше, чем традиционные медиа, поэтому довольно трудно отличить новостной сайт от личного форума, сайт, посвященный серьезным исследованиям от сайта с набором бессмысленных фактов. Трудно отделить зерна от плевел.

Для того, чтобы заслужить доверие аудитории, некоторые блоггеры постепенно вырабатывают собственные этические нормы. Однако в интернете еще много ненадежной информации, а пользователи обмениваются оскорблениями. Блог дает возможность опубликовать материал всем, независимо от образования или технических навыков. Это означает, что скучных и плохих блогов будет столько же, сколько хороших и интересных.

Но блог – это мощный инструмент для обеспечения свободы слова, вызывающий восторг простых людей. Пассивные потребители информации стали энергичными практиками новой журналистики, которую американский пионер блоггинга Дэн Гиллмор назвал «народной журналистикой… создаваемой людьми для людей» (см. главу «Какой должна быть этика блоггера»).

Блоггеры часто становятся единственными настоящими журналистами в странах, где традиционные медиа находятся под давлением цензуры. Только они сообщают независимые новости, рискуя вызвать недовольство властей и быть арестованными. Многие блоггеры подвергались преследованиям и арестам. Один из авторов этой книги, Араш Сигарчи, был приговорен к 14 годам тюрьмы за то, что разместил онлайн тексты, критиковавшие иранский режим. Его история – свидетельство того, что многие блоггеры считают ведение блога обязанностью и необходимостью, а не хобби. Они ощущают себя глазами и ушами тысяч пользователей интернет.

Блоггеры должны соблюдать анонимность, размещая информацию, подвергающую их риску. Кибер-полиция настороже и хорошо умеет отслеживать «возмутителей спокойствия». Данное пособие рассказывает о том, как разместить материал, не раскрывая себя (глава «Как вести блог анонимно», написанная Этаном Цуккерманом). Конечно, хорошо обладать необходимыми техническими навыками, чтобы оставаться анонимным, но иногда могут помочь и немногочисленные простые приемы. Эти советы, конечно не для тех, кто использует интернет с целью совершения преступления (террористы, рэкетиры, педофилы). Пособие просто предлагает помощь блоггерам, оказавшимся в оппозиции, поскольку они стремились отстаивать свободу слова.

Тем не менее, основная проблема блоггера, даже при репрессивном режиме, - не безопасность. Проблема заключается в том, чтобы сделать блог популярным и найти свою аудиторию. Блог без аудитории не опасен для власти. Данное пособие предлагает технические решения для того, чтобы блог «подхватывали» основные поисковые системы (статья Оливье Андрие), а также ряд журналистских приемов («Как «прославить» блог?» Марка Глэйзера).

Некоторые блоггеры сталкиваются с проблемой фильтрации. Большинство авторитарных режимов в настоящее время обладают возможностями для цензуры интернет. На Кубе или во Вьетнаме сайты, критикующие режимы, рассказывающие о коррупции или о нарушении прав человека, недоступны. Так называемый «незаконный» или «подрывной» контент автоматически блокируется фильтрами. Но всем блоггерам нужен свободный доступ ко всем сайтам и ко всей блогосфере. В противном случае содержание блогов утрачивает смысл.

Вторая часть книги посвящена фильтрации («Как избежать цензуры: технические советы» Нарта Вильнева). Немного здравого смысла, настойчивость и, что самое главное, правильные инструменты, - и любой блоггер сможет обойти цензуру.

В пособии предлагаются технические советы для создания хорошего блога. Гораздо более сложная задача – создание успешного блога. Для того, чтобы стать заметным, необходимо быть оригинальным и предлагать новости или мнения, которые не освещаются основными медиа. В одних странах блоггеры озабочены, прежде всего, тем, чтобы не попасть в тюрьму. В других они стремятся заработать репутацию источника надежной информации. У блоггеров разные проблемы, но каждый из них находится на переднем фронте борьбы за свободу выражения.

Жюльен Пэйн - глава подразделения Свобода интернет, «Репортеры без границ».

ЧТО ТАКОЕ БЛОГ?

Pointblog.com

«БЛОГ» ИЛИ «ВЕБЛОГ» (BLOG, WEBLOG) – ПЕРСОНАЛЬНЫЙ ВЕБСАТ, КОТОРЫЙ :

- содержит, главным образом, заметки и новости (posts);
- регулярно обновляется;
- ведется в форме дневника (последние заметки размещаются вверху на странице), большинство материалов разделено по рубрикам;
- использует специальные интерактивные инструменты;
- обычно создается и поддерживается одним человеком, иногда анонимно.

ЗАМЕТКИ БЛОГА (BLOG POSTS):

- чаще всего текст (включающий внешние ссылки), иногда изображения, а также звуковые и видеофайлы (в последнее время используются все чаще);
- могут комментироваться посетителями;
- архивируются, доступ к ним сохраняется всегда.

ТАКИМ ОБРАЗОМ, БЛОГ ВО МНОГОМ ПОХОЖ НА ПЕРСОНАЛЬНУЮ ВЕБСТРАНИЦУ, ЗА ИСКЛЮЧЕНИЕМ ТОГО, ЧТО БЛОГ:

- легче создать и поддерживать, а потому он чаще обновляется;
- предполагает более открытый и личный стиль, более откровенные точки зрения;
- поощряет дискуссии с посетителями и другими блоггерами;
- устанавливает международные стандарты для блогов (текст организован в две-три колонки, сайт включает комментарии и RSS (really simple syndication) канал.

ЯЗЫК БЛОГГИНГА

Pointblog.com

БЛОГ (BLOG)
Сокр. от “веблог”. Сайт, содержащий письменные материалы, ссылки или фотографии, которые постоянно обновляются, обычно одним человеком.

ВЕСТИ БЛОГ (TO BLOG)
Поддерживать блог или размещать материал на одном из блогов.

БЛОГГЕР (BLOGGER)
Человек, который ведет блог.

БЛОГОСФЕРА (BLOGOSPHERE)
Все блоги, сообщество блоггеров.

СПИСОК ССЫЛОК (BLOGROLL)
Список внешних ссылок, размещаемых на блоге, часто это ссылки на другие блоги. Обычно размещается в колонке на базовой странице. Часто включает ссылки на сообщество блоггеров-друзей.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЛОГА (BLOGWARE)
Программное обеспечение, необходимое для ведения блога.

КОММЕНТАРИИ – СПАМ (COMMENT SPAM)
То же, что и почтовый спам. Роботы заполняют блог рекламой в форме комментариев. Это серьезная проблема, требующая использования специальных программ для того, чтобы закрыть доступ для некоторых пользователей или исключать определенные адреса в комментариях.

СИНДИКАЦИЯ КОНТЕНТА (CONTENT SYNDICATION)
Способы, благодаря которым автор или администратор сайта делают возможным рассылку материалов сайта или их части на другие ресурсы (сайты).

МОБЛОГ (MOBLOG)
Сокр. от «мобильный блог». Блог, который может обновляться удаленно, с использованием таких средств коммуникации, как телефон или цифровой помощник (наладонник).

ПОСТОЯННАЯ ССЫЛКА, ПЕРМАССЫЛКА, ПЕРМАЛИНК (PERMALINK)
Сокр. от «постоянная ссылка» (permanent link). Web-адрес каждого материала, размещенного на блоге. Удобная закладка, даже в тех случаях, когда материал заархивирован на блоге, с которого взят.

ФОТОБЛОГ (PHOTOBLOG)
Блог, содержащий, главным образом, фотографии в хронологическом порядке, постоянно обновляемый.

ПОДКАСТИНГ (PODCASTING)
Сокр. от iPod и broadcasting (вещание). Размещение аудио и видео материалов на блоге, а также RSS канал для цифровых плейеров.

ЗАМЕТКА (POST)
Обычно краткое сообщение, размещенное на блоге и сопровождаемое внешней ссылкой, которое посетители могут комментировать. Это может быть новость, фотография или просто ссылка.

RSS (REALLY SYMPLE SYNDICATION / ДЕЙСТВИТЕЛЬНО ПРОСТАЯ СИНДИКАЦИЯ)
Способ упорядочения последних сообщений, посланных на вебсайт. Особенно удобен для блогов, так как сообщает пользователям об обновлении блога. Также может «синдицировать» контент, давая возможность другим сайтам (просто и автоматически) воспроизводить контент сайта или его часть. Быстро распространяется, особенно часто используется у медийных сайтов.

RSS АГРЕГАТОР (RSS AGGREGATOR)
Программное обеспечение или онлайновая услуга, позволяющая блоггеру читать (to read) RSS канал (RSS feed), особенно последние сообщения на его любимых блогах. Агрегатор также называют «считывателем» (reader) или «считывателем канала» (feedreader).

RSS КАНАЛ (RSS FEED)
Файл, содержащий последние сообщения на блоге. Он считывается RSS агрегатором (RSS aggregator) и сразу же показывает обновление блога.

ОБРАТНАЯ ССЫЛКА (TRACKBACK)
Способ автоматической связи между сайтами, когда они обмениваются уведомлениями о том, что на блоге появилась информация, связанная с предыдущей заметкой (post).

WEB-ДНЕВНИК (WEB DIARY)
Блог.

ВИКИ (WIKI)
Гавайское «wikiwiki» - «быстро». Вебсайт, который может легко и быстро обновляться любым посетителем. Слово также стало означать инструменты, используемые для создания вики (вики движков). Блоги и вики имеют ряд сходных черт.

ВЫБОР **ИНСТРУМЕНТА**

Сирил Фьеве (Cyril Fievet), Марк Оливье Пейер (Marc-Olivier Peyer), pointblog.com

Блоги многим обязаны развитию программ, облегчающих процесс обновления вебсайтов.

Программные инструменты для ведения блога должны обеспечивать, прежде всего, удобный для пользователя интерфейс (доступный через веб - браузер), а также динамичное управление контентом, архивы и поиск.

Блог имеет два интернет адреса, которые остаются неизменными после установки блога:

- адрес для публичного доступа;
- адрес для администрирования, защищенный паролем, принадлежащим человеку, который запустил блог.

Блог можно установить посредством присоединения к блог-сообществу или на своем сервере.

БЛОГ-СООБЩЕСТВА

(См. главу «Как установить и запустить блог», The Civiblog system)
Установка блога на уже существующей платформе, как правило, занимает несколько минут. Вы выбираете имя пользователя и пароль, затем несколько нажатий на кнопку – и блог запущен (одни блог-сообщества предоставляют этот сервис бесплатно, другие – за деньги).
Такой способ подходит, если вы хотите создать блог «только для просмотра»: стоит немного (самое большее – несколько евро в месяц), обеспечивает простоту, скорость, а также определенные преимущества за счет трафика, генерируемого сообществом и за счет популярности сообщества в целом.
В числе неудобств можно назвать ограниченные возможности для создания интерфейса и более продвинутых характеристик, а также необходимость размещать рекламу. Одна из угроз при этом – риск прекращения функционирования сообщества (платформы).

САМОСТОЯТЕЛЬНОЕ ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ БЛОГОВ

Инструменты для блогов – это программное обеспечение, которое устанавливается на сервере, скрипты для автоматического запуска сайтов и базы данных для хранения размещенных материалов. После установки эти инструменты работают через стандартный web-браузер. При этом, для установки и запуска блога не требуется никаких специальных знаний, например, знания HTML. Однако инсталляция, выбор конфигурации и установление критериев доступа, создание базы данных, установка FTP-загрузки (FTP-loading) могут представлять некоторые трудности.

Это решение подходит для тех, кто уже знаком с блогами. Основное преимущество данного способа в том, что блог принадлежит исключительно вам, что позволяет без ограничений адаптировать и изменять его конфигурацию. Но для этого требуются определенные технические навыки. Кроме того, такой блог хуже защищен от комментариев – спама, сохранение контента вам тоже придется обеспечивать самостоятельно.

КАК ВЫБИРАТЬ БЛОГ-СООБЩЕСТВО?

Иногда переход из одного блог-сообщества в другое может представлять определенные сложности. Поэтому важно с самого начала сделать правильный выбор.

Для этого необходимо учитывать следующие моменты:

БЛОГИ В СООБЩЕСТВЕ

Некоторые сообщества объединяют пользователей одного возраста или людей с одинаковыми интересами. Просмотрите несколько дюжин блогов сообщества, чтобы выявить «типичную группу».

ВНЕШНИЙ ВИД БЛОГОВ

Сообщества (платформы) обычно предлагают некоторый набор цветов, шрифтов, интерфейсов страниц. Чтобы получить представление об этих возможностях, просмотрите несколько блогов. Многие бесплатные сообщества требуют от блоггеров размещения рекламы на всех страницах. Обратите внимание на адреса, которые могут выглядеть следующим образом: http://myblog.thecommunity.com, http://www.thecommunity.com/myblog или http://www.thecommunity.com/mynumber).

ВОЗМОЖНОСТИ

Просмотрите предлагаемые характеристики и выясните, сможете ли вы изменять дизайн блога, приглашать других авторов, размещать изображение или звуковые файлы, возможно ли обновление с использованием телефона. Изучите также возможности ограничения доступа (полного или частичного) для зарегистрированных пользователей.

СКРЫТЫЕ ЗАТРАТЫ

Некоторые сообщества предлагают бесплатные сервисы, однако при определенных объемах сохраняемых данных и за определенную пропускную способность может требоваться плата.

Это надо выяснить заранее.

МЕЖДУНАРОДНЫЕ ПЛАТФОРМЫ

Blogger - http://www.blogger.com

Бесплатный. Создан в 1999, куплен Google в 2003. Является крупнейшим сообществом, в которое входят около восьми миллионов блогов. Платформа проста в использовании, однако имеет ограниченные возможности.

LiveJournal - http://www.livejournal.com

Бесплатный или платный (около 2 долларов США в месяц). Одна из старейших платформ, шесть миллионов блогов, основные пользователи – молодежь.

MSN Spaces - http://www.msnspaces.com

Бесплатный. Платформа Microsoft, создан в конце 2004 года. Много возможностей (обмен фотографиями, Messenger link). Зарегистрироваться могут только те, кому исполнилось 13 лет.

ФРАНКОЯЗЫЧНЫЕ ПЛАТФОРМЫ

20six - http://www.20six.fr

Бесплатный или платный (3-7 евро в месяц). Много возможностей, имеет базовую и продвинутую версии.

Over-Blog - http://www.over-blog.com

Бесплатный. Хороший дизайн, прост в работе. Крупнейшая платформа Франции, очень популярна среди молодежи, хотя возможности ограничены.

Skyblog - http://www.skyblog.com

Бесплатный (с обязательной рекламой)

TypePad - http://www.typepad.com/sitefr

Платный (от 5 до 15 евро в месяц в зависимости от характеристик). Очень профессиональный, с широким выбором возможностей. Бесплатную версию можно приобрести через блог-сообщества Noos (http://www.noos-blog.fr) или Neuf Telecom (http://www.neufblog.com)

ViaBloga - http://viabloga.com

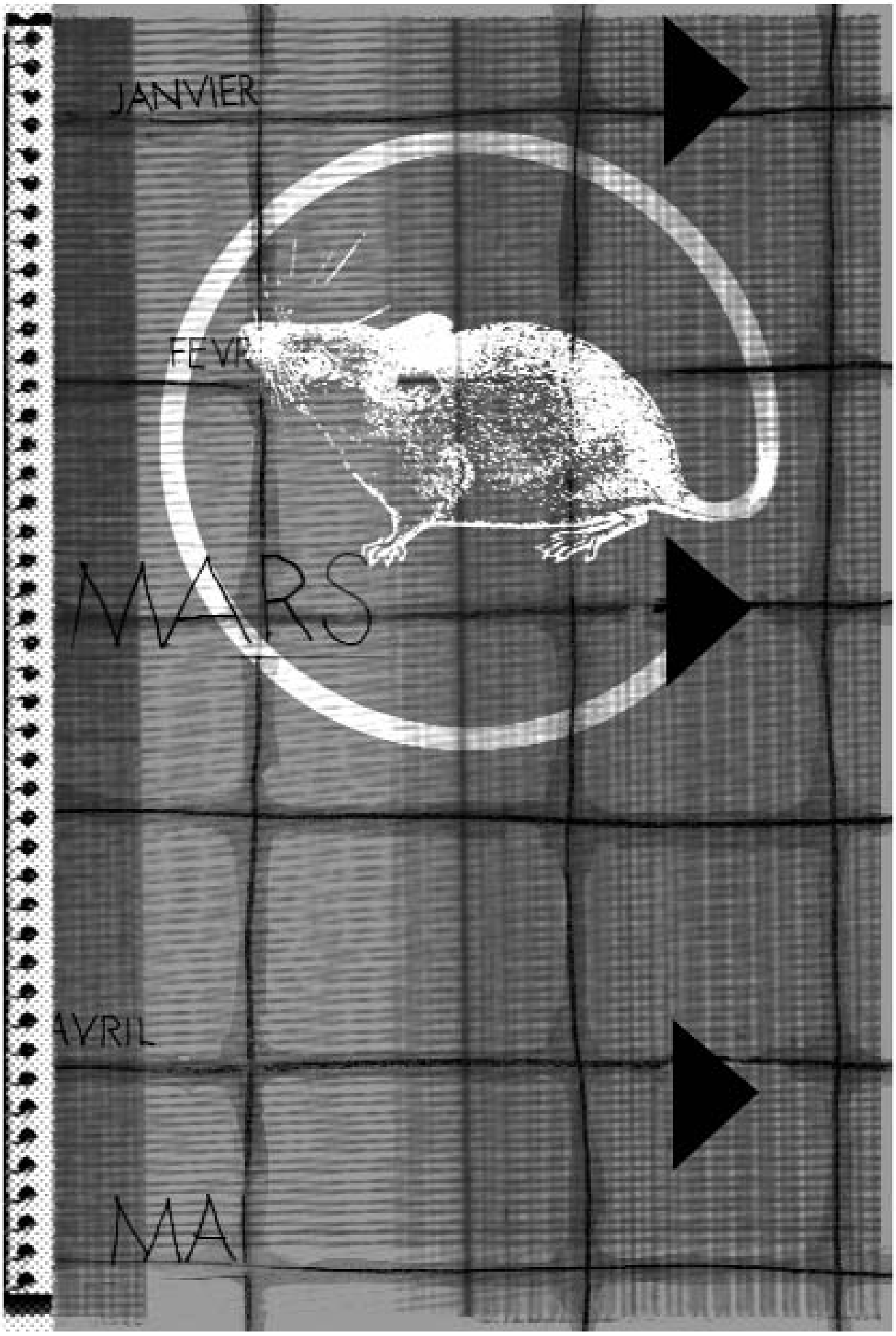
Бесплатный для некоммерческих ассоциаций, в остальных случаях – 5 евро в месяц. Оригинальный, динамичный, с интересными возможностями.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЛОГОВ

DotClear - http://www.dotclear.net
MovableType - http://www.movabletype.org
Wordpress - http://www.wordpress.org

Цель Pointblog.com – освещать сущность и развитие блоггинга как ключевого элемента современной интернет-революции. Сайт предназначен как для новичков, так и для опытных пользователей и состоит из блога и нескольких разделов. Блог принадлежит компании PointblogSARL, создателями и руководителями которой являются Кристоф Джинисти (Christophe Ginisty) и Сирил Фьеве (Cyril Fievet).

Мой блог


JANVIER
FEVR
MARS
AVRIL
MAI

КАК **УСТАНОВИТЬ И ЗАПУСТИТЬ** БЛОГ

Civiblog system (www.civiblog.org)

Блог гораздо легче поддерживать и обновлять, чем обычный веб-сайт. Блоговые платформы (или серверы) основаны на несколько специфических методах постинга, но в целом аналогичны тем, что используются для обычных сайтов. Цель этой статьи – помочь пользователям платформы Civiblog, представителям структур гражданского общества. Однако предлагаемые советы применимы и к другим подобным серверам. Civiblog использует платформу Blogware, предоставленную бесплатно компанией Tucowa.

Обратимся к тому, что сделало блоггинг таким популярным.

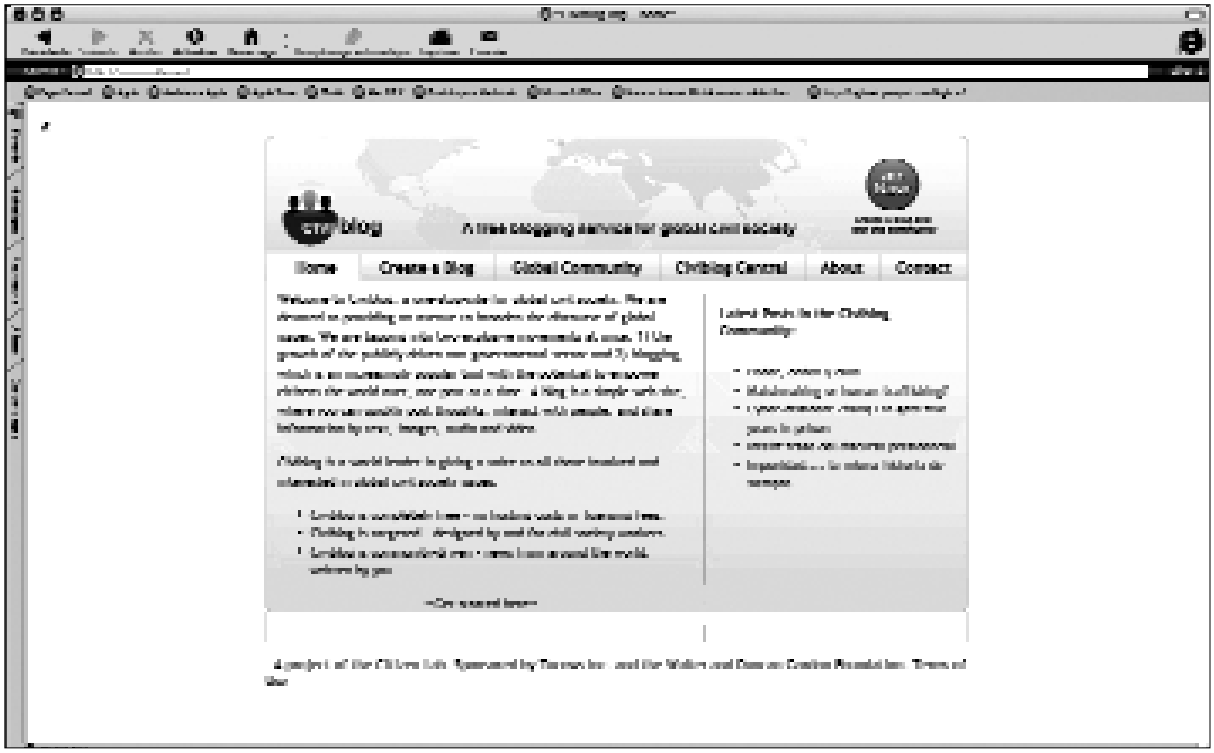
Технический ключ к блгосфере – это RSS (Really Simple Syndication) каналы. Базовым элементом RSS является XML (eXtensible Markup Language) файл, который блог генерирует автоматически, что позволяет другому сайту или блогу сделать на него ссылку. Когда вы «синдицируете» RSS канал, он размещает заголовки сообщений блога в вашем считывателе новостей (news reader) в почтовых программах Outlook или Thunderbird или прямо на сайте и блоге. При обновлении блога RSS канал также обновляется, благодаря чему информация быстро распространяется автоматически. Для того, чтобы своевременно обновлять материал, блоггеры должны овладеть этой технологией.

Другой технический инструмент блоггинга – это обратная ссылка (trackback), которая показывает происхождение материала, размещенного на блоге. Эта технология используется большинством платформ.

Когда сообщение размещается на блоге, к нему может добавляться обратная ссылка (trackback), которая автоматически уведомляет об обновлении и позволяет составить список всех сайтов, сообщения с которых или комментарии к которым размещены на данном сайте. С другой стороны, когда блог кто-то цитирует, движок оповещается об этом цитировании и рядом с сообщением появляются ссылки на посты других людей по этой же теме. Всегда интересно знать, что кто-то упомянул твой материал. Полезно также и то, что появляется возможность распространять материал и популяризировать свой блог.
Итак, при установке блога необходимо потратить некоторое время на знакомство с технологией.

ГЛАВНАЯ СТРАНИЦА CIVIBLOG

RSS канал отображен справа и автоматически обновляется, как только член сообщества посылает новую заметку.

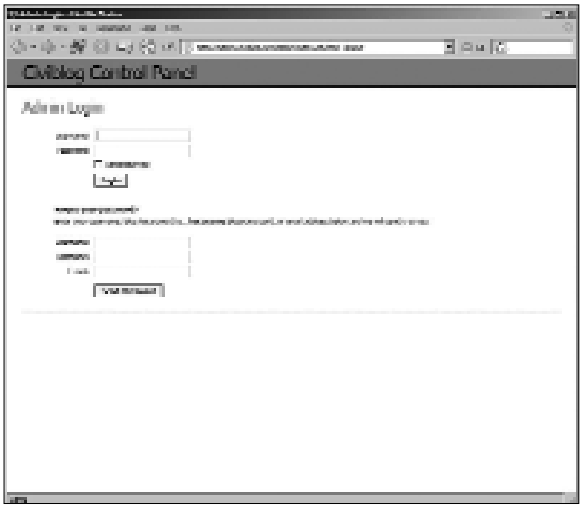


РЕГИСТРАЦИЯ

Для установки блога необходимо зарегистрироваться. На большинстве платформ это делается достаточно просто. Для регистрации на платформе Civiblog требуется минимальная информация. При этом проверяется, действительно ли блог устанавливается представителями структур гражданского общества, а не является просто семейным блогом или блогом для друзей. С момента регистрации до появления блога онлайн проходит примерно 24 часа. Коды доступа для запуска блога высылаются блоггеру по электронной почте.

ВХОД В СИСТЕМУ ДЛЯ АДМИНИСТРАТОРА

Блог имеет «внешний интерфейс» (front end, страница, на которую приходят посетители) и прикладную часть (back end программное обеспечение, выполняющее процессы обработки и другие задачи, невидимые посетителю; часть клиент-серверного приложения), где выполняется обновление и поддержание сайта. Доступ к прикладной части можно получить, имея имя пользователя и пароль, полученные при регистрации.

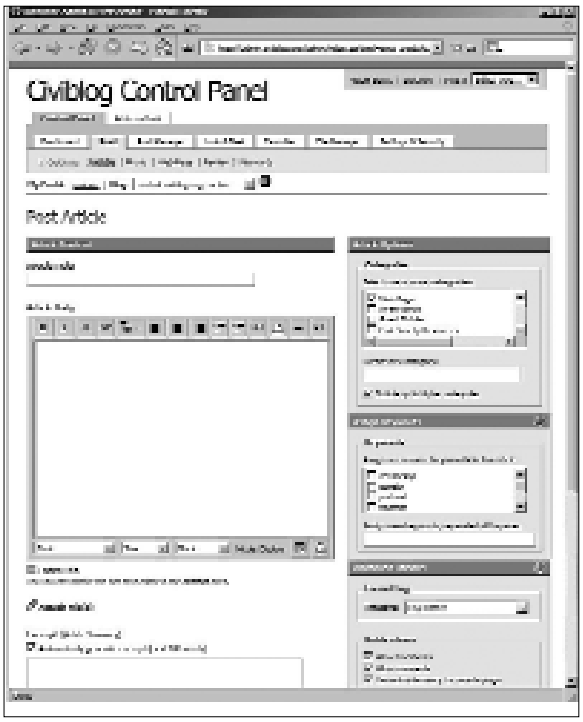


ЭЛЕКТРОННАЯ ИНРМАЦИОННАЯ ПАНЕЛЬ

Большинство блогов имеют «электронную информационную панель», которая позволяет видеть все, что происходит на блоге, включая последние заметки, комментарии и обратные ссылки. Отсюда можно получить доступ ко всем возможностям блога, изменять его вид, увеличивать пропускную способность, редактировать заметки, управлять доступом пользователей.

КАК РАЗМЕЩАТЬ СООБЩЕНИЯ

Одно из основных отличий блога от вебсайта – легкость обновления. Большинство платформ позволяют размещать сообщения в простом текстовом формате. Новые платформы, подобные Civiblog, позволяют изменять размер и цвет шрифта, вставлять ссылки и рисунки.

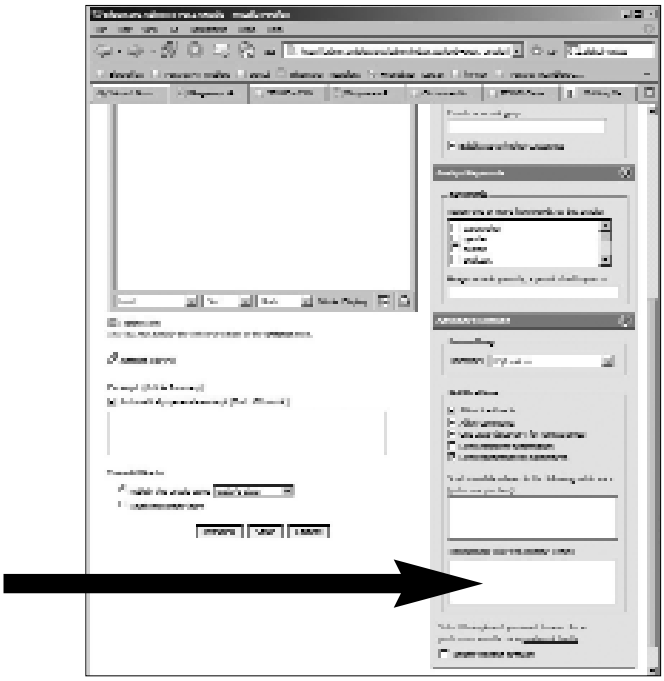


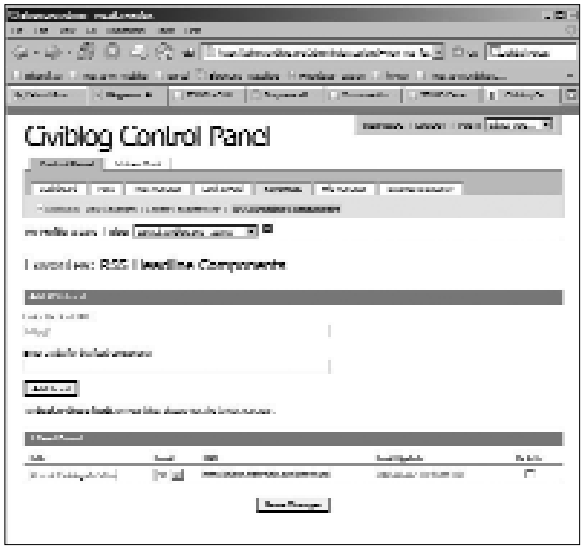
Для того, чтобы разместить заметку, необходимо:

1. Войти в систему.
2. Нажать на кнопку “post”.
3. Напечатать название и текст заметки.

4. Отформатировать текст.
5. Отнести заметку к одной из существующих рубрик или создать новую рубрику.

6. Кликнуть “save” в низу страницы. И это все. Став опытнее, вы сможете использовать такие инструменты, как обратные ссылки, пинги и ключевые слова.





ОБРАТНЫЕ ССЫЛКИ

Добавить обратную ссылку к заметке достаточно просто. Вы просто добавляете в окно “trackback URLs to notify”, находящееся справа, постоянный URL сайта, на который ссылаетесь. Обратная ссылка будет автоматически послана на сайт при сохранении заметки.

RSS СИНДИЦИРОВАНИЕ

Синдицирование RSS канала другого сайта или блога также не представляет сложностей:

1. Войдите в “back end” блога.
2. Нажмите кнопку “favourites”.
3. Затем - “RSS Headline Components”.
4. В соответсвии с инструкциями вставьте URL (оканчивающийся на .xml, .rdf или .py or .php) RSS канала, который вы хотите синдицировать.
5. Дайте каналу имя и кликните на “add feed”.
6. После создания канала вставьте его в блог.
7. Нажмите кнопку “look and feel”.
8. Затем – “layout”.
9. Затем – “RSS: your feed” (“your feed” – это имя , которое вы присвоили каналу в шаге 5) и тяните название канала в то место, где оно будет находиться на блоге.
10. Кликните “save” внизу страницы.

Дело сделано.

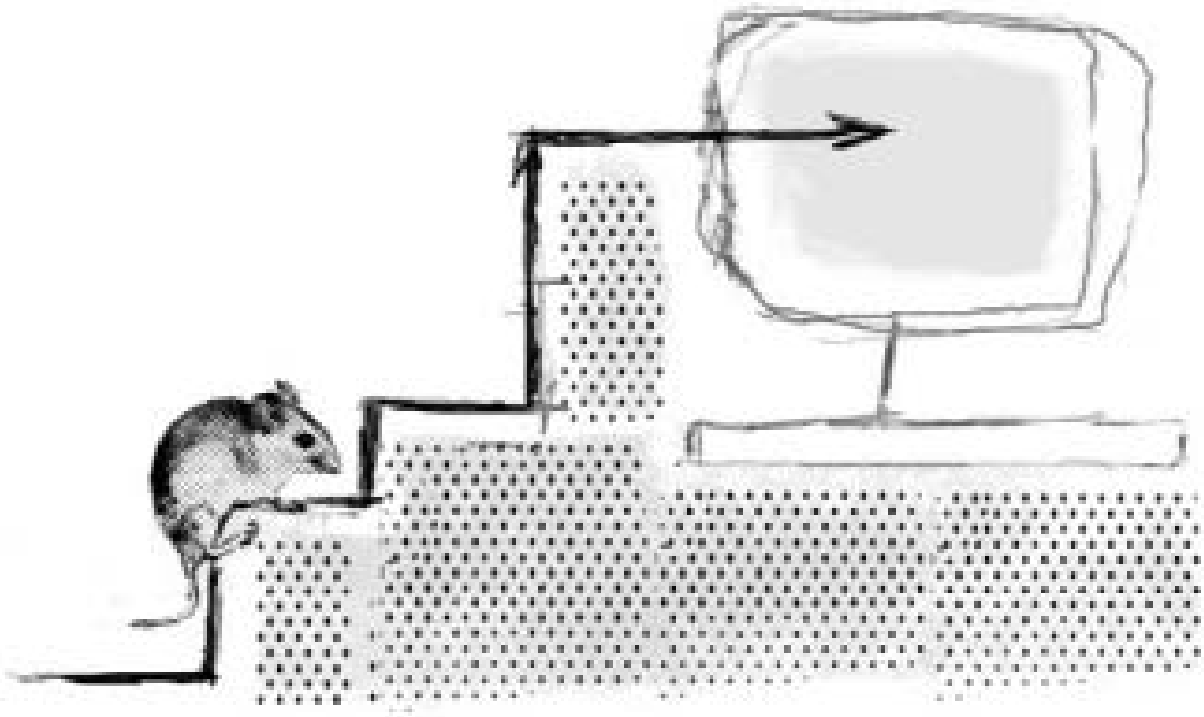
Адреса полезных сайтов:
Civiblog Central Resources Blog:
http://central.civiblog.org/blog/BloggingResources

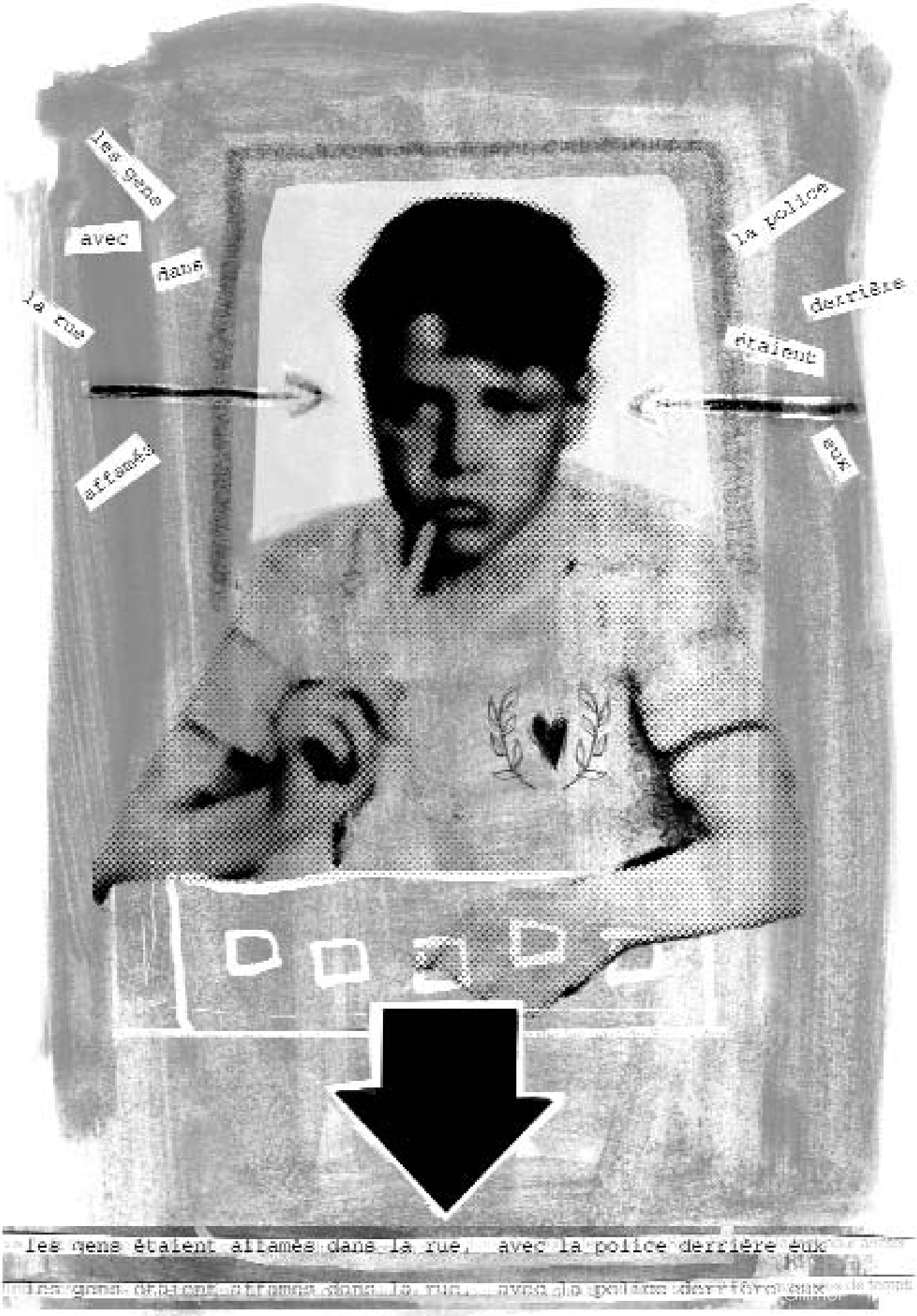
How to blog:
http://blogging.typepad.com/how_to_blog

The blogosphere:
http://blog.lib.umn.edu/blogosphere

The Weblog Workshop:
http://cyber.law.harvard.edu:8080/globalvoices/wiki/index.php/WeblogWorkshop

Blogging 101:
http://www.unc.edu/%7Ezuiker/blogging101/index.html





Полиция преследовала вышедших на улицу голодающих

КАКОЙ ДОЛЖНА БЫТЬ **ЭТИКА БЛОГГЕРА?**

Дэн Гиллмор (Dan Gillmor)

Не все блоггеры занимаются журналистикой. Большинство этого не делает. Но если уж они берутся за журналистику, они должны придерживаться определенных этических принципов.

Означает ли это, что они должны подписаться под каким-то моральным кодексом? Не обязательно.

Профессиональная журналистика переполнена этическими кодексами. Одни кодексы, стремясь зафиксировать все возможные нарушения, занимают больше страниц, чем Конституция США. Другие, краткие и лаконичные, делают акцент на желательном поведении. На вебсайте кибер-журналистики доступен адаптированный для блоггеров кодекс (http://www.cyberjournalist.net/news/000215.php), разработанный американским Союзом профессиональных журналистов. Это очень серьезный и интересный проект.

Все кодексы преследуют одну важнейшую цель: добиться доверия. Читатель (зритель, слушатель) не доверяющий репортажу, вряд ли обратит на него внимание. Исключение, конечно, составляет знакомство с неэтичным материалом в учебных целях: наблюдая неэтичное поведение других, можно избежать многих ошибок.

Для меня этика имеет отношение к одной очень простой вещи – к чести. Конечно, это слово многозначно. Но если мы не ведем себя достойно, вряд ли мы заслужим доверие людей.

В американской журналистике честь всегда ассоциируется со стандартами «объективности»: статья должна освещать различные точки зрения и все нюансы, чтобы читатель мог составить свое собственное мнение. Я считаю, что объективность – это важная, но недостижимая цель, потому что мы привносим свои предрассудки и убеждения во все, что делаем.
В современной журналистке, ориентированной не на лекцию, на на беседу, мораль определяется не столько кодексами, сколько ценностями и принципами, лежащими в основе честной журналистики.
Исходные основания хорошей журналистики: скрупулезность, точность, честность, открытость и независимость.

Между этими принципами не всегда можно провести разделительные линии. Их можно по-разному интерпретировать, каждое их этих слов перегружено подтекстами. Но я считаю, что они позволяют приблизиться к хорошей журналистике и что их легче осуществить в онлайновой журналистике. Рассмотрим их подробнее.

СКРУПУЛЕЗНОСТЬ

Когда я был репортером, а затем – колумнистом, я стремился узнать как можно больше. Ведь факты и мнения – основа репортажа. Мне больше всего нравилось, когда 95 процентов из того, что я узнавал, оставалось за пределами статьи. Я знаю, что лучшие репортеры всегда стремились сделать еще один телефонный звонок, проверить еще один источник. (Все интервью я завершал вопросом: «С кем еще, по вашему мнению, мне нужно побеседовать?»).

Сегодня тщательность – это нечто большее, чем опрос людей, адреса которых есть в наших записных книжках, реальных и виртуальных. Это, прежде всего, обращение к читателям. Так я и поступал, когда писал книгу о народной журналистике в 2004 году (то же начинают делать и другие авторы). Хотя многие факторы не способствуют этому, однако я уверен, что все больше журналистов будут использовать данный метод.

ТОЧНОСТЬ

Придерживайтесь фактов.

Рассказывайте не только о том, что вы знаете, но и том, чего вы не знаете. (Если читатель, слушатель, зритель знает то, чего не знаете вы, просто предложите ему/ей заполнить лакуны).

Точность означает немедленное исправление допущенных ошибок, что гораздо проще сделать онлайн. Тем самым мы можем смягчить ошибки или, по-крайней мере, уменьшить наносимый ими вред для новых читателей.

ЧЕСТНОСТЬ

Насколько просто говорить о точности, настолько же сложно говорить о честности. Часто честность – это позиция очевидца. Но и в этом случае можно опереться на ряд универсальных принципов.

Честность, среди прочего, означает умение прислушаться к различным точкам зрения и учесть их в своей работе. Это не означает, что нужно, как попугай, повторять все лживые высказывания для того, чтобы добиться того ложного баланса, который заставляет журналистов цитировать противоположные утверждения, притом, что факты с очевидностью доказывают правоту одной из сторон.

Честность предполагает также предоставление возможности высказаться людям, которые убеждены в том, что вы ошибаетесь, даже если вы с этим не согласны. Опять-таки, это гораздо легче сделать онлайн.

И, наконец, честность – это состояние души. Мы должны осознавать, что нами движет и всегда быть готовыми выслушать тех, кто с нами не согласен. Первое правило ведения беседы – умение слушать. От людей, которые со мной не соглашались, я узнал гораздо больше, чем от тех, кто придерживался того же мнения, что и я.

ПРОЗРАЧНОСТЬ

Открытость журналиста – это добавленная стоимость журналистики. Звучит просто, но осуществлять это нелегко.

Никто не станет спорить, что журналисты должны раскрывать такие вещи, как, например, конфликт финансовых интересов. Но до какой степени? Следует ли журналисту превратить свою жизнь в открытую книгу? Насколько открытым следует быть?

Личные предрассудки, даже неосознанные, влияют на работу журналиста. Я американец, воспитанный на убеждениях, которые множество людей в других странах (и даже в США) откровенно отрицают. Я должен понимать, что есть вещи, которые я принимаю как само собой разумеющиеся и которые необходимо подвергать периодической проверке в процессе работы.

Еще одну возможность раскрыться дают нам наши репортажи. Мы должны как можно больше ссылаться на источники, демонстрируя людям, что опираемся на реальные факты и данные. (Это, вероятно, имеет отношение к точности и скрупулезности, но и открытости без этого быть не может).

НЕЗАВИСИМОСТЬ

Честность в журналистике означает способность идти в своих репортажах до конца. Это невозможно, если средства массовой информации принадлежат нескольким крупным компаниям или находятся под пятой правительства.

Быть независимым онлайн проще. Можно начать блог. Но не следует думать, что блоггер сможет избежать давления капитала или правительства, если попытается зарабатывать блоггингом на жизнь.

Джефф Джарвис, выдающийся американский блоггер (buzzmachine.com) считает, что есть еще одна важная вещь. Блоггеры должны уважать этику беседы. Он говорит о том, что для меня чрезвычайно важно: беседа должна приводить к пониманию. Первое правило разговора – слушать. Этика требует умения слушать, потому что только слушая мы учимся.

Элизабет Фолл для O'Reilly Media

Дэн Гиллмор, основатель Grassroots Media Inc., компании, занимающейся развитием и популяризацией народной журналистики. Его первый сайт Bayosphere.com, в Сан-Франциско. Дэн Гиллмор – автор книги "We the Media : Grassroots Journalism by the People, for the People" (O'Reilly Media, 2004).

Его блог: http://bayosphere.com/blog/dangillmor

ЧТОБЫ БЛОГ ИНДЕКСИРОВАЛСЯ ПОИСКОВЫМИ МАШИНАМИ

Оливье Андрие (Olivier Andrieu)

Блоги – это вебсайты, поэтому они индексируются такими поисковыми системами, как Google, Yahoo ! Search или MSN Search. Чтобы стать успешным, блог должен отображаться на страницах поисковых систем по ключевым словам. Поэтому с самого начала сайт должен соответствовать классификационным критериям, которые используют поисковые системы.

Блоги имеют ряд встроенных характеристик, которые не только обеспечивают их индексацию поисковыми системами, но и положение в верхних строках. Например:

• Поскольку блоги – это личные дневники (по крайней мере сначала), на них размещено много текстовых заметок. Поисковые системы не индексируют сайты с большим количеством графики или флэш-анимации и минимальным текстовым сопровождением.

• Каждое «сообщение» обычно занимает отдельную страницу, доступную через «пермалссылку» (permalink) и посвящено отдельной теме. Поисковые системы индексируют такие страницы лучше, чем большие страницы с разными темами (например, архивы или главные страницы блогов).

• Название заметки обычно воспроизводится в заголовке страницы или в URL (адресе). Например, на блоге Radio Free Nepal (http://freenepal.blogspot.com) каждая заметка находится на отдельной странице. Например, http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html:

Название сообщения (State Vandalism in Nepal) встречается не только в URL страницы, но и в названии документа:

Название сообщения добавлено после названия блога, которое появляется на главной странице блога (freenepal.blogspot.com).

Наличие описательных ключевых слов в названии страницы (содержание тэга <TITLE> в языке HTML) и в URL документов являются ключевыми критериями для поисковых систем, поэтому очень важно давать правильные названия заметкам.

PREVIOUS POSTS

State Vandalism in Nepal

Peace Bond: Sign of Problems

Must-Read Stories: April 20

Municipal Election: For Covering Up the Death of Democracy

Articles of Interest: April 16

Attempts to Blur Borderlines

Articles of Interest: April 7

Press: Support King or Die

Vote for Radio Free Nepal!

• Текстовые ссылки создаются автоматически, прежде всего, ссылки на архивы (см. примеры страниц Radio Free Nepal).

Это очень важно для индексации страниц, поскольку текстовый контент ссылок (так называемое «якори» (anchors) является ключевым для определения релевантности поисковиками. В данном примере наличие слов “State Vandalism in Nepal” в первой ссылке или “Radio Free Nepal” – в девятой повышает релевантность страницы. Кроме того, релевантными будут считаться как страница с этими ссылками (наличие ссылок в тексте также важно для поисковых систем), так и страницы, на которые ссылки указывают.

КАК СДЕЛАТЬ БЛОГ БОЛЕЕ ЗАМЕТНЫМ

Блоги имеют ряд преимуществ, что обеспечивает их индексацию. Если поисковая система индексировала блог, у него гораздо больше шансов попасть на первые позиции, чем у стандартного вебсайта. Однако ситуацию можно исправить.

Мы предлагаем несколько советов, основанных на использовании ключевых слов блога.

1. Технологии

Если сайт еще не появился онлайн, отнеситесь внимательно к выбору технологии (Blogger, Dotclear, BlogSpirit, Joueb и др.). Выберите ту, которая обеспечивает максимальные возможности для индексирования:
• заголовок заметки должен полностью воспроизводиться в заголовке страницы (тэг <TITLE>) и в URL (что делается не всегда, так как в некоторых адресах перед заголовком размещаются дополнительные символы);
• возможность создания «пермассылок» (ссылки на страницы, содержащие одну заметку);
• избранная технология должна обеспечивать максимальные возможности для дизайна и персонализации сайта, в частности, графику, персональную таблицу стилей (style-sheets). Необходимо изучить как можно больше технических нюансов, чтобы максимально использовать возможности индексирования сайта.

Для того, чтобы разобраться в этом, просмотрите сайты, использующие избранную вами технологию. Это может многому научить.

2. Заголовки

Заголовки очень важны. Заголовок вашей заметки будет воспроизведен в заголовках страниц, в URL и в тексте ссылок, указывающих на них. Это три ключевых критерия для поисковых систем. Поэтому заголовок заметки должен включать самые важные термины. Избегайте заголовков вроде «Хорошо сказано!», «Добро пожаловать!» или «Здорово!». Заголовок должен предавать суть заметки и включать не более пяти слов. Подумайте о том, на какие слова вашей заметки должен отреагировать поисковик и вставьте их в заголовок. Это не просто, но эффективно.

3. Текст

Поисковые системы любят текст. Можно размещать сколько угодно фотографий, но они должны сопровождаться текстом. Постарайтесь, чтобы каждая заметка включала не менее 200 слов, тогда она будет хорошо индексироваться

поисковиками. Поисковики также не любят, если одна заметка посвящена нескольким темам. Золотое правило: одна тема - одна заметка.

4. Обращайте внимание на абзацы

Необходимо также обращать внимание на положение важных слов в тексте. Особенно серьезно необходимо отнестись к первому абзацу. Если, например, вы хотите, чтобы сообщение находилось по запросу «освобождение заложников», то данная фраза должна быть среди первых 50 слов заметки. То же касается и ключевых слов. Если страница начинается ключевыми словами, при прочих равных условиях, поисковики будут индексировать ее лучше, чем страницу с ключевыми словами в конце. Ключевые слова можно выделять жирным шрифтом, например. Такие сигналы также важны для поисковиков.

5. Избегайте дублирования контента

Все поисковые системы определяют дублирование контента. Если две страницы слишком похожи, индексироваться будет только одна. Вторая страница редко появляется в результатах поиска. Google, например, сообщает следующее: ((Чтобы показать Вам наиболее значимые результаты, мы опустили некоторые, очень похожие на уже показанные. Если Вы хотите, Вы можете повторить поиск, включив опущенные результаты.))

С блогами это происходит особенно часто, поскольку страницы с заметками выглядят очень похоже.

Например, если на каждой странице у вас одинаковое введение, разместите его либо в низу страницы, либо только на главной странице. Тогда ваши страницы не будут столь похожими.

6. Короткие заголовки

Самый удобный заголовок (контент тэга <TITLE>) для поисковой системы – это заголовок, состоящий из 5-10 слов и не включающий такие элементы, как артикли, союзы и предлоги. Заголовок страницы блога обычно состоит из двух частей:

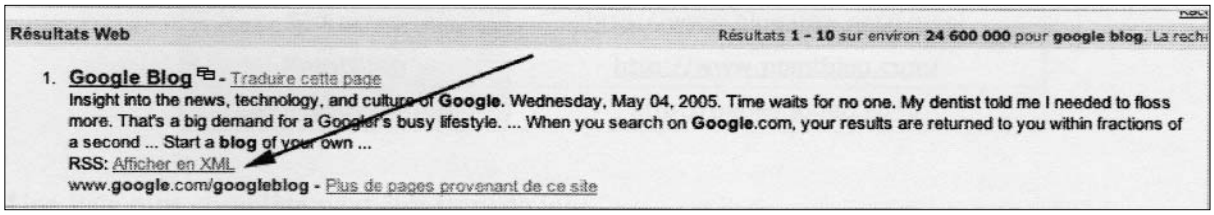
- Общий заголовок блога
- Повторение заголовка заметки.

Чтобы в общем заголовке было не больше 10 слов, необходимо использовать не более 5 слов, как в заголовке страницы, так и в заголовке заметки. Это сложно, однако, краткость и информативность – один из ключевых критериев для индексирования поисковыми системами.

Если возможно (не все технологии позволяют это), размещайте сначала заголовок заметки, а под ним – общий заголовок блога, а не наоборот.

7. Синдицирование

Большинство блоговых платформ позволяют создавать “XML поток” или «RSS канал», при помощи которых пользователи имеют доступ к вашим заметкам в удобном формате. Вы можете предоставить такие возможности на своем блоге (для установки требуется всего несколько минут). Вы не только привлечете больше посетителей. Это будет немедленно подхвачено, например, Yahoo!



Так что воспользуйтесь этой возможностью.

8. Обновление ссылок

Ссылки очень важны для поисковых систем, поскольку позволяют создать рейтинг популярности (в Google это называется PageRank). Ссылки на ваш блог создаются через:

- включение его в директории (см. ниже).
- поиски «братских сайтов», которые, не являясь вашими конкурентами, предоставляют материал на ту же тему.

Обмен ссылками между блогами должен происходить очень быстро (это часто делается в блог-сообществах, что является одним из преимуществ данных платформ). Дизайн блогов также удобен для ссылок, поскольку последние могут размещаться на полях.

ТЕМАТИЧЕСКИЕ ДИРЕКТОРИИ

Индексирование блога поисковыми системами (Google, MSN, Yahoo ! и Exalead) и общими директориями (Yahoo ! Directory и Open Directory) чрезвычайно важно. Тематические директории имеют значение, поскольку они:

- привлекают пользователей, интересующихся данной темой;
- позволяют увеличивать число ссылок на блог;
- способствуют знакомству с другим блоггерами, которые, возможно, захотят обмениваться ссылками.

Среди поисковых систем, которые могут индексировать блоги, можно назвать следующие:

Англоязычные	Blogwise :	http://www.blogwise.com/
	Daypop :	http://www.daypop.com/
	Feedster :	http://www.feedster.com/
	Technorati :	http://www.technorati.com/
	Waypath :	http://www.waypath.com/
	Blogarama :	http://www.blogarama.com/
	Syndic8 :	http://www.syndic8.com/
Франкоязычные	Blogonautes	http://www.blogonautes.com/
	Blogolist	http://www.blogolist.com/
	Weblogues	http://www.weblogues.com/
	Blogarea	http://www.blogarea.net/Links/
	Pointbloghttp	http://www.pointblog.com/
	Les Pages Joueb	http://pages.joueb.com/

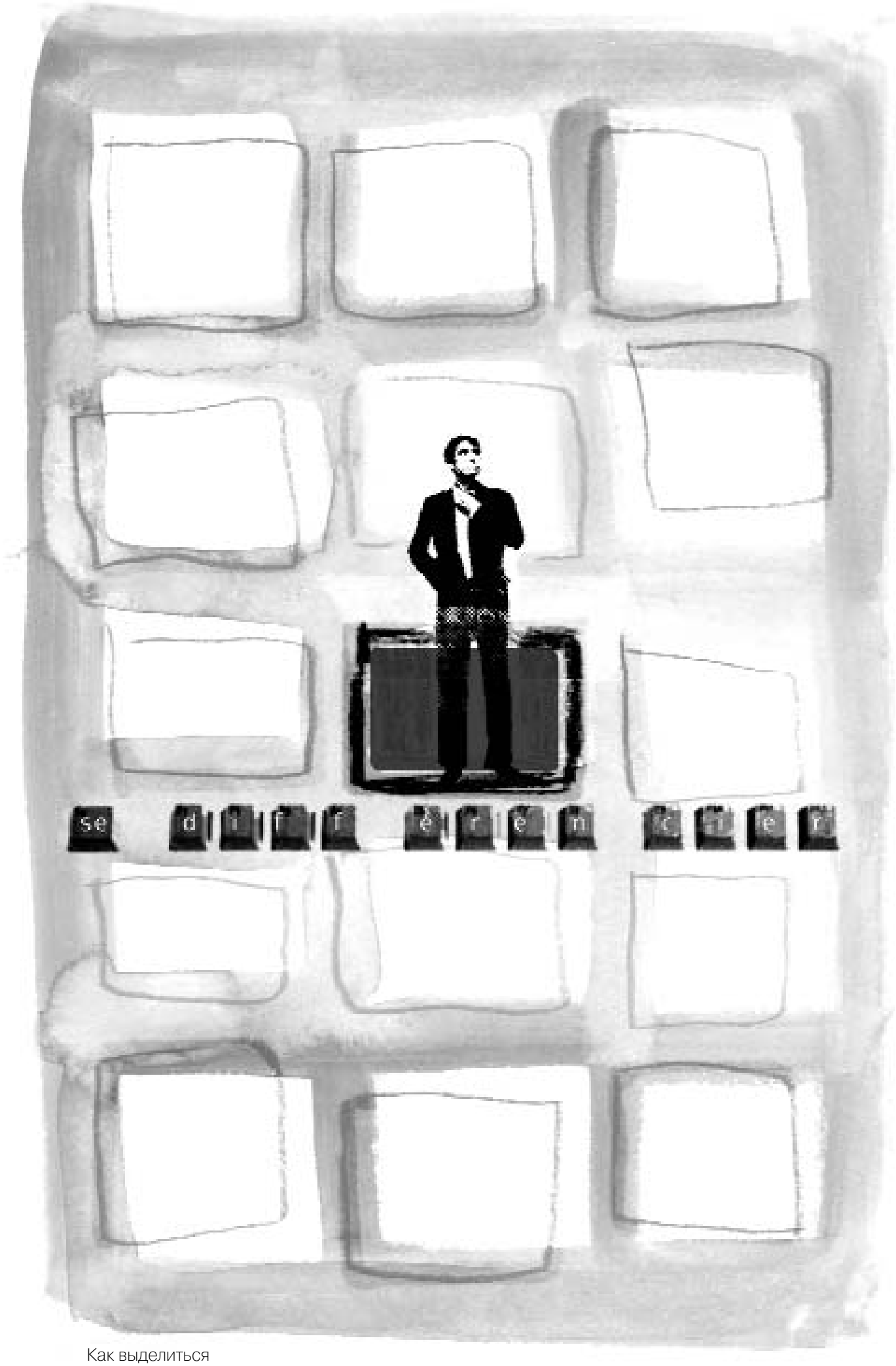
Большой список находится на:
http://search-engines.blogs.com/mon_weblog/2005/05/les_search-engines_de_.html

Можно просмотреть также директории:
http://www.canalblog.com/cf/browseBlogs.cfm
http://www.dotclear.net/users.html
http://www.blogspirit.com/fr/communautes_blogspirit.html

ЗАКЛЮЧЕНИЕ

Блог обладает всеми необходимыми элементами, чтобы хорошо индексироваться поисковыми системами. Следуя предложенным советам, вы сможете добиться хороших результатов и сделать свой блог «видимым». Итак, в добрый путь. И помните, что контент – это король.

Оливье Андрие – независимый интернет- консультант, специализист по методам индексации сайтов поисковыми системами, ведет блог www.abondance.com



Как выделиться

КАК “ПРОСЛАВИТЬ” БЛОГ

Марк Глейзер (Mark Glazer)

Что выделяет блог среди миллиардов заметок, размещенных на миллионах блогов во всем мире? Что отличает автора блога, на который посетители постоянно возвращаются и который получает признание медиа?

Это, прежде всего, обратная связь. Успеха добиваются блоггеры, которые поддерживают контакты со своими читателями, будь их 10 или 10 000, развлекая и просвещая их. Многие стремятся подчеркнуть различие между блоггерами и журналистами, писателями, специалистами по маркетингу. Однако все они преследуют общие цели: притащить за воротник людей и не отпускать их.

Некоторые авторы этой книги – Чанад Бахрейни из Бахрейна, Йан Шам - Шеклтон из Гонконга и Араш Сигарчи из Ирана - ведут блоги в странах, правительства которых очень внимательно следят за тем, что они пишут. Но их блоги читают во всем мире, стараясь узнать то, о чем пресса этих стран рассказывать боится. В странах, где нарушаются свобода слова, свобода совести, свобода прессы, онлайновые голоса блоггеров становятся важным источником информации о том, что происходит на улицах городов. Фотографии и сообщения, которые размещают блоггеры, нужны всем.

Но что же отличает эти и другие интересные блоги? Ниже предлагается описание основных характеристик, делающих блоги популярными.

УНИКАЛЬНОСТЬ

Лучшие блоггеры имеют оригинальный взгляд на вещи, знамениты своей уникальной идентичностью и рассказывают реальные истории. В основе веблогов лежит идея онлайнового журнала, личного дневника. Поэтому важно понимать, что ведение журнала отличается от академических статей, от безличного телеграфного стиля. Чанад Бахрейни – псевдоним блоггера

из Азии, живущего в Бахрейне. Находясь в одной из влиятельных арабских стран, блоггер имеет возможность по-особому освещать события, происходящие там. Йан Шам-Шеклтон - художник, автор перформансов, которая, переезжая из страны в страну, помогает организовывать акции протеста против блокирования китайских сайтов блога TypePad.

СВЕЖАЯ ИНФОРМАЦИЯ

Серьезная проблема заключается в том, что большинство блогов не успевают за событиями и предлагают устаревшую информацию. Поскольку большинство блоггеров не получают никакой платы за ведение блога, повседневная рутина не дает им возможности постоянно обновлять информацию. Многие начинают блог, размещают несколько заметок, а потом не могут найти время, чтобы обновить его. Чтобы добиться успеха, блоггеры должны регулярно писать заметки и освещать интересующие их темы, включая текущее состояние дел. Это не означает, что они должны размещать 12 заметок в день. Но если не обновлять блог в течение нескольких недель, посетители уйдут.

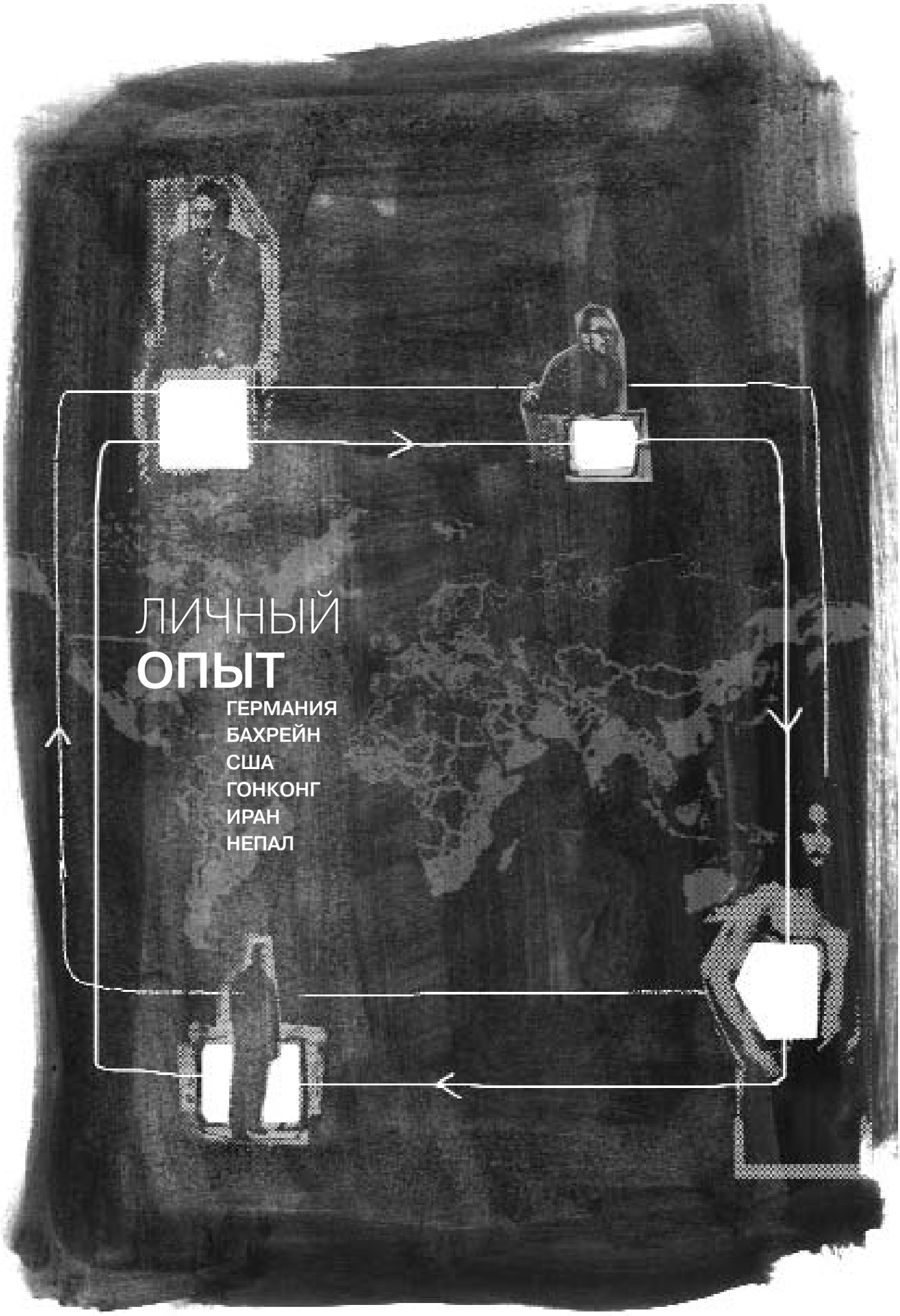
СВЯЗЬ С ЧИТАТЕЛЯМИ

Основной отличительной чертой блогов является интерактивность. Существует множество способов привлечь читателей, втянуть их в дискуссии и установить обратную связь с ними. Можно организовать онлайновый опрос, или дать свой электронный адрес, или просто обеспечить возможность комментировать заметки. У Джефа Уи (Jeff Ooi) возник конфликт с властями Малайзии из-за комментария одного из читателей его блога. Вместо того, чтобы убрать опцию, Уи решил модерировать комментарии, публикуя только аргументированные высказывания по теме. Он также начал вести блог под названием “The Ferryman” («Паромщик») на китайском языке, стремясь установить связи между китайской и малайзийской блогосферами.

ГОВОРИТЬ ПРАВДУ ВЛАСТЯМ

Хотя многие блоги можно комментировать, некоторые по-прежнему размещают старомодные «репортажи». Здесь трудно что-то посоветовать. Однако оригинальная тема или оригинальная точка зрения помогут вашему блогу выделиться. Чанад Бахрейни разместил фотографии и аудио файлы об акциях протеста в Бахрейне в 2004 году, когда один из гражданских активистов был заключен в тюрьму. В Иране блоггер Араш Сигарчи был арестован и приговорен к 14 годам тюрьмы за то, что критиковал власти по поводу ареста журналистов. Позже его освободили под залог, однако судебное разбирательство еще не закончено. Суть в том, что эти блоггеры, как и многие другие, имели мужество говорить властям правду и противостоять лжи, распространяемой правительством.

Марк Глэйзер – колумнист «Online Journalism Review» (http://www.ojr.org/), издания Школы коммуникаций Аннеберга Университета Южной Калифорнии, независимый писатель, живущий в Сан-Франциско. Его адрес: glaze@sprintmail.com



ЛИЧНЫЙ **ОПЫТ**

ГЕРМАНИЯ
БАХРЕЙН
США
ГОНКОНГ
ИРАН
НЕПАЛ

ГЕРМАНИЯ

“МЫ ЗАЩИЩАЕМ ПРАВА ЧЕЛОВЕКА И ГРАЖДАНСКИЕ ПРАВА”

Маркус Беккедаль (Marcus Beckedahl)
Netzpolitik.org

В конце 90-х, в возрасте 20 лет, я стал активным лоббистом идеи открытого и свободного информационного общества. Вместе с друзьями я создал НГО, целью которого была защита цифровых прав. Пять лет мы пропагандировали и защищали права человека и гражданские права в цифровой сфере. Мы организовывали конференции, участвовали в различных кампаниях, были членами сетей НГО. Например, мы руководили Координационной группой немецких организаций гражданского общества по подготовке к Всемирному саммиту по информационному обществу (WSIS).

В первые годы своей политической деятельности я использовал, главным образом, списки рассылки. Я разослал около 5,000 новостей и статей о сетевой политике. Однако эти рассылки читала небольшая статичная группа подписчиков. Блоги же открыты и прозрачны, обеспечивают гораздо больше возможностей для обмена знаниями и информирования о моей деятельности.

Свой первый блог я начал в 2002 году, на первом этапе подготовки WSIS. Я приехал на подготовительную встречу в Женеву со спальным мешком и ноутбуком. Мне нужен был инструмент, позволявший размещать информацию быстро, без использования HTML. Размещение новостей с использованием HTML занимало у меня слишком много времени. Я стал публиковать информацию и свои впечатления о том, как делается политика на уровне ООН, в блоге "Backpacking to world politics" («Турпоход в мировую политику»). Это был мой первый блог.

Свой последний блог Netzpolitik.org я начал весной 2004 года. Испытав ряд различных приложений, я остановился на Wordpress (бесплатная платформа и большое сообщество). Веблоги обеспечивают быстрый и удобный способ генерирования, размещения и редактирования контента. Самое важное для меня – интерфейс, который позволяет концентрироваться на самом существенном – на написании текста, а не на разметке документа в HTML-формате.

Мне нужен был простой интерфейс для сбора и компилирования информации, чтобы можно было «одним кликом» разместить на сайте написанный текст. Все это значительно упростило мою работу. Меня привлекает также технология “push-pull”. Большинство моих читателей подписаны на RSS канал и следят за моими статьями. Другие находят меня при помощи web-браузеров или поисковых систем.

Являясь членом ряда политических сообществ, я стремлюсь собирать и распространять на Netzpolitik.org новости о гражданских правах и правах человека, об открытом программном обеспечении, о свободном и открытом доступе к знаниям, информационном обществе для всех и о балансе законов об интеллектуальной собственности и цифровых прав. Свобода слова и свобода самовыражения зависят от законодательства о цифровых правах и интеллектуальной собственности. Однако немногие осознают важность этого. Вот почему я разъясняю ситуацию, помогая гражданам защищать свои права. Права гражданина находятся под угрозой во всем мире, в том числе и в Германии. Новые меры безопасности сопровождаются цензурой и слежкой. Граждане редко осознают, что это и есть потеря свободы.

Свободное программное обеспечение (например, операционная система Linux) имеет огромный потенциал для распространения и укрепления свободы слова и плюрализма в цифровую эпоху. Разумеется, я использую Linux. Я также пишу о новых разработках свободного программного обеспечения, о политических аспектах использования этого ПО и объясняю, почему даже новички могут использовать его. Я внимательно слежу за развитием онлайновой энциклопедии Wikipedia, а также за лицензированием creative commons (CC). Мой контент зашищен лицензией CC и я активно поощряю использование и копирование своих материалов для некоммерческих целей при условии ссылки на источник.

Еще одни важный вопрос – это эффективное использование сети интернет организациями гражданского общества. Я был руководителем проекта и консультантом по политической коммуникации в интернет. Специальные рубрики моего блога посвящены проведению электронных онлайновых компаний (eCampaigning) и электронной демократии (eDemocracy). Я анализирую возможности свободного ПО с точки зрения организации сотрудничества и активной работы, а также с точки зрения практической деятельности, в том числе - различные социальные аспекты коллективного генерирования и распространения знаний.

В netzpolitik.org я также собираю информацию и данные о конференциях, лекциях и встречах, посвященных информационному обществу, сообщаю как о ходе таких конференций, так и о своих впечатлениях. Каждый день я помещаю обзор новостей со множеством ссылок, комментирую разработку новых законов и деятельность НГО в этих областях. Мой блог постепенно становится узловой точкой немецкоязычного сообщества, откуда информация распространяется по другим источникам. Я также прошу моих друзей блоггеров писать о ключевых вопросах и быстрее распространять новости. Благодаря использованию RSS, я могу быстро компилировать обзор. За первые 10 месяцев мне удалось опубликовать более 800 статей, друзья помогли мне только немного.

К моему удивлению, блог ежедневно читают 2,500 человек. Мне много пишут, особенно молодые люди, которым я советую начать собственные блоги.

К счастью, Германия всегда защищала свободу слова. Никто не посадит меня в тюрьму за критику правительства. Я восхищаюсь мужеством людей, которые живут в условиях диктатуры и рискуют жизнью, обновляя блоги.

Маркус Беккедаль, 28 лет, исполнительный управляющий агентства "newthinking communications", занимающегося технологиями open source и стратегическими разработками, один из основателей и председатель немецкого НГО Netzwerk Neue Medien. Его блог - www.netzpolitik.org

БАХРЕЙН

“МЫ УНИЧТОЖИЛИ МОНОПОЛИЮ ПРАВИТЕЛЬСТВА”

Чанад Бахрейни (Chan'ad Bahraini)

Я начал блог по двум причинам: (1) интересно писать без каких бы то ни было формальных ограничений, сроков и требований, и (2) для того, чтобы стимулировать дискуссии по темам, которые редко обсуждаются в национальной прессе Бахрейна.

В настоящее время в Бахрейне государству принадлежат только телевидение и радио станции. Поэтому здесь не увидишь и не услышишь репортажей или обсуждений тем, которые даже отдаленно связаны с политической ситуацией в стране. Все газеты – частные, поэтому они несколько свободнее, чем вещание. Однако и в прессе ситуация не лучше, поскольку редакторы не отваживаются открыто критиковать некоторых влиятельных людей, членов правительства или королевскую семью (особенно короля и его дядю – премьер-министра).

Вместе с тем, интернет предоставляет возможности для свободного выражения мнений. Хотя правительство Бахрейна имеет опыт мониторинга и блокирования политических вебсайтов, ситуация несколько смягчилась в последние два года. Легкость, с которой можно создать вебсайт и писать анонимно (подобно мне), создает серьезные трудности для правительства, стремящегося с этим бороться.

Вот почему я чувствовал настоятельную необходимость организовать свободные и искренние дискуссии по всем темам (включая политику) – в ситуации, когда страна находится в состоянии перехода к демократии. И именно интернет стал площадкой, где я мог высказывать свое мнение, обсуждать различные точки зрения. Меня поддерживал и тот факт, что Махмуд (www.mahmood.tv), один из первых блоггеров Бахрейна, уже вел блог в течение года. При этом никаких конфликтов с правительством не возникало.

Главными целями моего блога были обсуждение и анализ событий в Бахрейне. Но из-за недостатка информации мне пришлось заниматься псевдожурналистикой. То есть, по возможности, я посещал все важные мероприятия, участвовал в акциях (особенно в демонстрациях протеста), а затем писал о них в блоге, размещал фотографии.

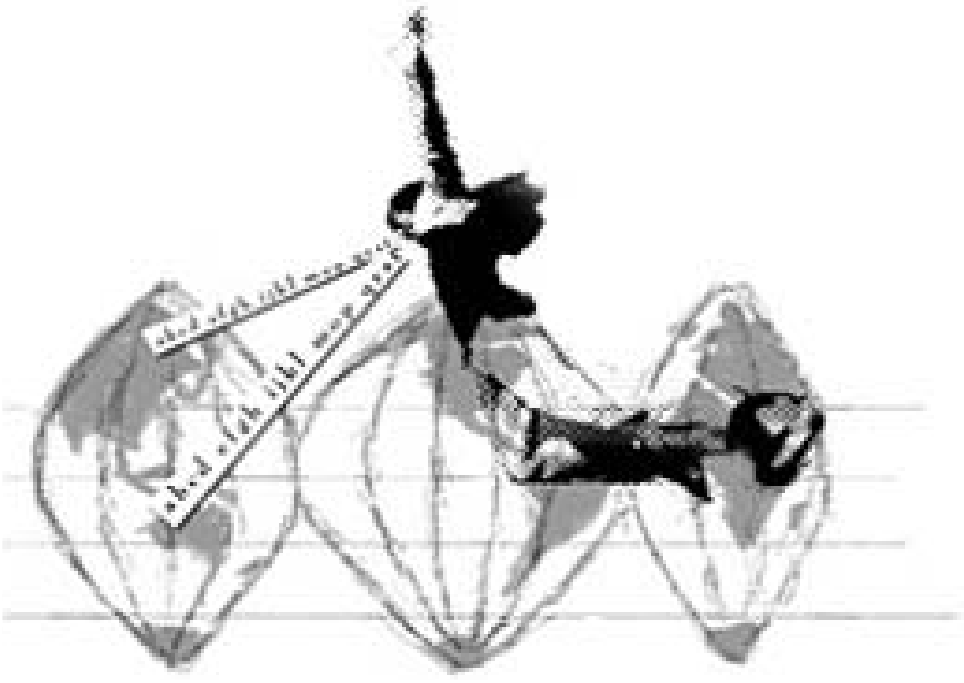
Теперь в Бахрейне уже несколько блоггеров, что очень хорошо. Создано пространство, где честно обсуждаются различные темы. Конечно, я получил много информации, которую вряд ли смог бы добыть сам, благодаря другим блогам Бахрейна. Наше сообщество существует не только онлайн. Раз в месяц мы встречаемся, чтобы поговорить на темы, обсуждаемые на наших блогах.

Вместе с тем, большинство онлайновых дискуссий в Бахрейне ведется на арабоязычных форумах, которые существуют гораздо дольше, чем блоги (e.g. bahrainonline.org). Блоггинг не стал еще широко распространенным явлением в Бахрейне, тем не менее наши блоги все в большей степени начинают выполнять функции «мостов» (этот термин использовал Хусейн Деракшан: http://hoder.com/weblog/archives/013982.shtml). Поскольку большинство блоггеров в Бахрейне пишут по-английски, мы можем контактировать и общаться (в обоих направлениях) с людьми во всем мире, они воспринимают нас как источник информации о том, что «на самом деле» происходит в Бахрейне.

Например, когда в феврале 2005 года были арестованы три модератора форума Bahrainonline.org, и мы написали об этом в блогах, новость распространилась во всем мире даже быстрее, чем в Бахрейне. «Репортеры без границ» опубликовали заявление об этом в день ареста. Я считаю, что привлечение внимания международной общественности сыграло существенную роль в том, что правительство, в конце концов, через пару недель освободило эту тройку. Боле того, наши блоги уничтожили монополию правительства на сообщение новостей о Бахрейне внешнему миру.

Ранее блоггеры в Бахрейне не сталкивались с преследованиями по поводу публикаций. Но ситуация стала меняться с начала 2005 года. Как уже отмечалось, в феврале были арестованы три модератора онлайнового форума за то, что на форуме появились посты, намеренно «провоцировавшие ненависть к правительству». Один из модераторов, Али Абдулеман, вел блог. В апреле правительство сообщило о том, что если владельцы вебсайтов не зарегистрируются в Министерстве информации, они будут преследоваться в соответствии с законодательством. Это означает, что правительство не понимает, в сущности, что такое интернет (и блоги) и не знает, как поступать в ситуациях, когда чувствует, что опасность грозит со стороны тех, кто пишет онлайн.

Выходец из юго-восточной Азии, Чанад Бахрейни живет в настоящее время в Бахрейне, где ведет блог chanad.weblogs.us. Он решил сохранить анонимность.



США

“ТЕПЕРЬ Я МОГУ ПИСАТЬ ТО, ЧТО Я ДУМАЮ”

Джей Роузен (Jay Rosen)
Press Think

Когда я начал интересоваться, как создать веблог, я получал разные ответы. Правда, все говорили: нужно писать короткие заметки. «Этого требует стиль»,- объясняли одни. «Это дает хороший результат», - говорили другие. Третьи доказывали, что именно этого ожидают занятые web-серферы. У них нет времени читать длинные и сложные аналитические статьи, втолковывали мне. Так говорили все.

Это вызвало у меня подозрение. Я не собирался писать длинные заметки в 2000 слов, но именно это произошло, когда я пытался выразить свои мысли в заметках так, чтобы они не повторяли то, что пишут другие и чтобы на них обратили внимание. (Я могу писать кратко, если хочу). Я решил не устанавливать никаких ограничений, самостоятельно определять, что работает, и как будет выглядеть PressThink.

Аргумент «у людей нет времени, чтобы…» казался мне неубедительным, я не верил этому. Этот совет ограничивал мою свободу писать то, что я думаю. А ведь основной причиной создания PressThink было стремление к освобождению: «Вау, теперь у меня есть собственный журнал. Теперь я могу писать то, что думаю». Меня интересовали пользователи, которым нужна глубина, сколько бы их ни было, океан к океану, заметка к заметке.

Моя позиция: это мой журнал, PressThink... Если он вам нравится, возвращайтесь. В абстрактном смысле, вероятно, мой блог является частью медиарынка, который соперничает в борьбе за аудиторию с игровыми шоу, футболом и многочисленными повторениями «Закона и порядка». Но это не так. PressThink, свободный гражданин добровольческой нации, не должен вести себя как участник рынка. Это мой длительный эксперимент в форме блоггинга.

Необходимо помнить, что веб предоставляет хорошие возможности для противоположных вещей. Для получения точной информации. Для блуждания «вокруг темы» в сети. Для беседы и взаимодействия. Веб открывает глубины, веб – это устройство для запоминания, «моментальная библиотека», фильтр. Использовать веблог для глубокого анализа, если большинству пользователей это не нужно – это тупик для веба, для этого подходят другие медиа. Но я не медиа. Странно то, что я стараюсь писать краткие вещи, но

получаются всегда длинные статьи. Некоторые читатели жалуются на это («слишком много слов тратится на ошибочное объяснение!» - типичная жалоба), но, в конце концов, это только веселит. Каждый хороший блог задает вебу вопрос: существует ли спрос на оригинальное... на меня? Но необходимо, чтобы блог некоторое время просуществовал, прежде, чем вы поймете, в чем же заключается ваша оригинальность.

Название PressThink («представления прессы») соответствует термину “group think” («групповые представления»), поскольку пресса и есть группа. Название также отражает тип мышления или доктрину журналистов, можно даже сказать, религию прессы. Именно эти темы интересуют меня. PressThink – это то, что я делаю, как критик и писатель.

Моя цель при этом – вычленить данный феномен из событий, которые освещает пресса. А затем исследовать его самому, или привлечь других к исследованию. Вот что означает название. Блог «о» представлениях прессы. Это также хитрая уловка для того, чтобы заставить журналистов больше думать. Я считаю, что некоторые блоггеры недооценивают значение названия блога. Я же не начинал блог, пока не нашел правильное название.

Я оставляю идеологическую критику прессы другим – людям и организациям, которые делают это увлеченно и хорошо. PressThink – это не сайт, следящий за правдивостью средств массовой информации, хотя я писал о таких проектах. PressThink не охотится за предрассудками, в обычном смысле слова, хотя я пишу об этой охоте. Я не поддерживаю Джорджа Буша, но я пишу об образе мышления его сторонников среди журналистов. Я писал в предисловии к своему веблогу: «Я стараюсь выявить, какие следствия в мире реальных событий имеет то, как и что мы пишем».

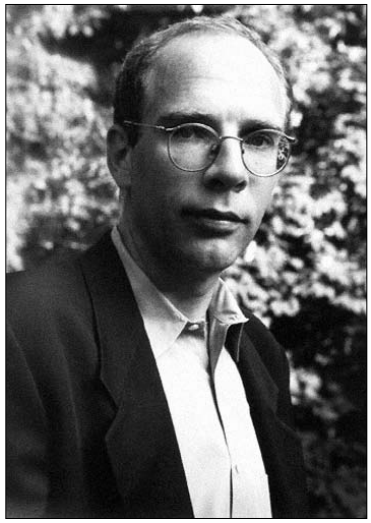
Меня как-то спросили, есть ли у меня свой метод ведения блога. Я читаю прессу, смотрю новости, прохожу по своему списку ссылок (blogroll), охотясь за чем-нибудь аппетитным, актуальным, интересным. Затем я собираю ссылки и начинаю писать. Чье-то письмо также может подать идею для интересной заметки. Я использую не определенный метод, а своего рода таблицу стилей, состоящую из моих собственных инструкций о том, как писать заметки для PressThink.

В типичной заметке PressThink, например, "Laying the Newspaper Gently Down to Die" ...http://journalism.nyu.edu/pubzone/weblogs/pressthink/2005/03/29/nwsp_dwn.html – пять основных элементов: заголовок, подзаголовок, эссе, дополнения (заметки, реакция, ссылки) и комментарии. Каждая часть требует особого стиля. Заголовок в сжатом виде сообщает о сути заметки и привлекает внимание. Подзаголовок содержит аргументы, предваряющие «рассказ». Само эссе – обычно 1,500 – 2,500 слов, с 20-30 ссылками, которые говорят сами за себя. Дополнения вводят заметку в контекст более широких дискуссий блогосферы, включая реакции на мой пост. Комментарии служат началом диалога.

Успешным я считаю такую заметку PressThink, где все части связаны друг с другом и представляют собой своего рода беседу. Заметка PressThink считается законченной только тогда, когда все дополнения, обратные ссылки и комментарии размещены, что занимает иногда более недели. Это один круг в ведении блога. Если все работает, пост через несколько оборотов возвращается на форум, который породил заметку – именно форум «думает». Конечно, я не знал о «таблице стилей» и логике постинга, пока не нашел их методом проб и ошибок. Вот почему только после определенного опыта ведения блога можно понять, что именно нужно делать.

Пока у меня не было PressThink, я вынужден был добиваться одобрения моих идей о журналистах и журналистике теми людьми, о которых я писал. Но теперь, когда у меня есть свой журнал, мне не нужно этого делать, а влиятельные журналисты и редакторы приходят на мой блог и читают, что я думаю. И это совсем другая ситуация. Я наконец-то обрел интеллектуальную свободу.

Джей Роузен живет в Нью Йорке, с 1986 года преподает журналистику в Университете Нью Йорка, где возглавлял кафедру в 1999 -2005 годах. Роузен - автор веблога PressThink, посвященного журналистике (www.pressthink.org), который он начал вести с 2003 года.



ГОНКОНГ

“Я СДЕРЖАЛА ОБЕЩАНИЕ, ДАННОЕ ПОГИБШИМ”

Йан Шам - Шеклтон (Yan Sham – Shackelton)

Сейчас 12.23, 4 июня. Сегодня – 16-я годовщина массового расстрела на площади Тянаньмынь в Пекине. В этот день, в 1989 году, вместе с другими участниками голодной забастовки, я сидела в туннеле рядом с гонконгским офисом информационного агентства Синьхуа. Это была забастовка в знак солидарности с китайскими студентами. Мы хотели демократии для них и для себя. Мы не хотели больше быть подданными британской колонии, но не хотели подчиняться коммунистической партии. Мы хотели быть свободными.

Через два – три часа я услышала по радио звуки первых выстрелов, крики и гудение движущихся танков. Мы посмотрели друг на друга и заплакали.

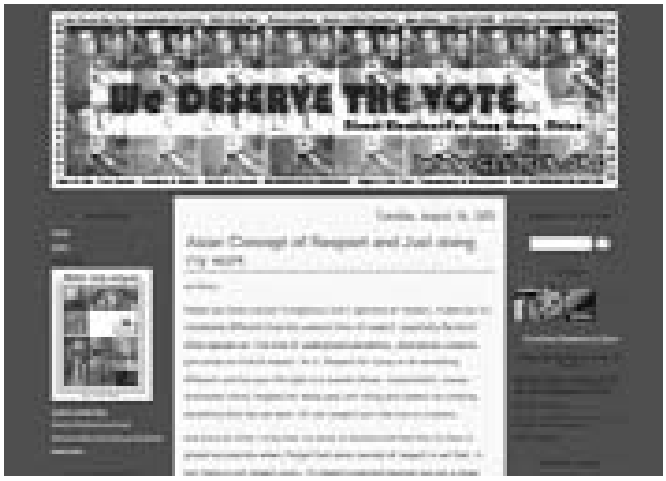
Сейчас мы все знаем, что Китай готовился использовать танки против борцов за демократию. Думаю, что именно в тот момент, когда я сидела, прислушиваясь к звукам подавления демократического движения 1989 года по радио, в туннеле, освещенном флуоресцентным светом, у меня появилась идея создать Glutter. Мне было 15 лет.

Если не в тот самый момент, то вскоре после него. Я дала обещание, которое могла дать только девушка, не имевшая жизненного опыта:

“Я никогда не забуду этого. Я обещаю запомнить это навсегда. Я проживу свою жизнь лучше ради всех нас, потому что я жива, а вы уже нет. Я не позволю этому повториться. Я буду напоминать миру о вас, о студентах на площади Тяньаньмын. Мои герои. Мои старшие братья и сестры.”

Я дала эти наивные обещания в спешке и от страха. Я не думала о том, как их выполнить и возможно ли это вообще. Я только чувствовала, что это звучало правильно, да и взрослые выкрикивали то же самое через громкоговорители.

Только сегодня я осознала, что все, что я пишу, все фотографии и художественные произведения – все это я делаю во имя демократии. Акции кибер-протеста, которые я организовывала, интервью, которые я давала, истории, которые я печатала – все делалось во имя свободы слова не только из-за



убеждений, но и потому, что это - один из способов успокоить подсознание. Блоггинг позволяет мне выполнить обещание, данное погибшим.

Я хочу, чтобы люди знали: я решила создать Glutter не потому, что следовала каким-то правилам, не из-за стремления подражать. Не потому, что хотела привлечь внимание и сделать себе имя. Мне больше нравятся ситуации, когда интерес к блогу спадает, а не периоды, когда он привлекает всеобщее внимание, потому что тогда я могу писать все, что хочу, могу рассказывать истории так, как я хочу, не испытывая давления извне.

Мой совет тем, кто собирается вести блог: слушайте только себя – и больше никого. Не читайте чужих блогов, не пытайтесь конкурировать или подражать им. Не сидите над списком «необходимо сделать», не пытайтесь реализовать все, что там написано. Я нарушила столько правил, потому что я о них не знала – и правильно.

Все что нужно для создания блога – начать его.

Все, что нужно для поддержания блога – просто записывать то, что вы хотите сказать.

Каждый из нас испытал когда-то момент политического пробуждения, это спусковой механизм, который помог нам увидеть несправедливость, которую необходимо устранить. В противном случае вы бы не стали активистами, вам не пришла бы в голову идея создать что-то. Пусть осознание этого руководит вами. Я думаю, вам есть, что рассказать о своих убеждениях, вы можете вдохновить других на борьбу за перемены. Вот и вся мудрость, которую я могу поведать сегодня.

Сейчас 2.33. Я слышу автоматные очереди. Тра-та-та-та. Каждый день в это время я слышу их. Мне было 15. Возможно, я была слишком молода для такого опыта. Но другие были слишком молоды, чтобы умирать.

По просьбе Йан Шам - Шеклтон, сообщаем, что она потратила шесть недель и написала шесть вариантов этой статьи, пытаясь рассказать все, что знает о блоггинге, пока не поняла: прелесть этого инструмента заключается в том, что можно быть самим собой. В своем блоге glutter.com она рассказывает об искусстве и о политике. Ее открытая демократическая позиция в Гонконге привела к тому, что блог подвергается цензуре в Китае.

ИРАН

“В БЛОГАХ МЫ МОЖЕМ ПИСАТЬ СВОБОДНО”

Араш Сигарчи (Arash Sigarchi)

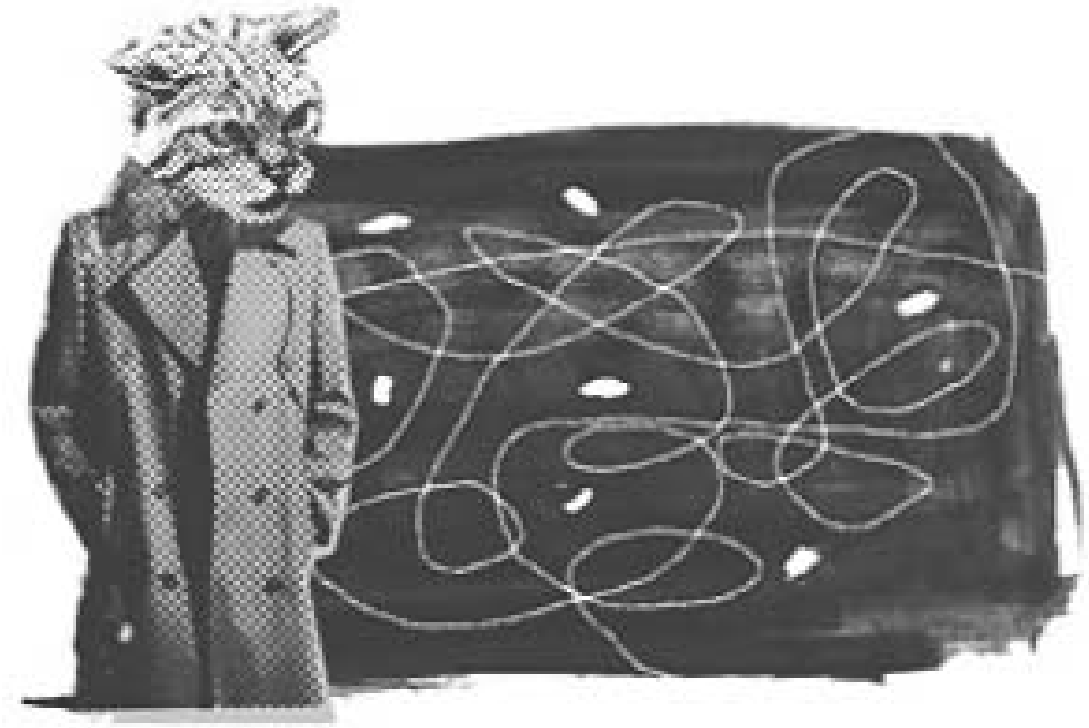
Сегодня мы понимаем значение высказывание Маршалла Маклюэна: «Мир – это глобальная деревня» лучше, чем он сам. Невидимые нити паутины интернет повсеместно пердают информацию о том, что происходит в Азии, южной и северной Америках, в Европе или на отдаленном острове у берегов Африки.

Годами журналистика сталкивалась с ограничениями, которые сейчас могут быть преодолены благодаря новым технологиям.

Я живу в стране, где из-за множества ограничений не могу выполнять свою работу. Это не только «организационные» факторы, которые влияют на работу средств массовой информации в мире, но и внешние факторы, например, законодательные ограничения, влияние правительства и отдельных лиц, односторонняя поддержка определенных источников новостей, группы давления и капитал в моей стране создают больше помех, чем в развитых странах. Поэтому я вынужден думать о независимости своей страны, о правдивых новостях и анализе. Одной из возможностей для преодоления барьеров стал блог.

В блогах мы можем писать свободно. Поскольку не требуется печатать новости или отправлять их в аудио-визуальные средства массовой информации, новости и точки зрения можно обнародовать гораздо быстрее. Блоги можно рассматривать как небольшие новостные и аналитические агентства, где автор является одновременно писателем и главным редактором.

Некоторые считают, что блоги должны уделять меньше внимания новостям. Люди любят рассказывать в блогах о своей повседневной жизни. У таких писателей-любителей мало читателей, часто это только друзья и родственники.



Но блоги известных журналистов и художников, политиков, экономистов, общественных деятелей и спортсменов, даже если они пишут только о событиях своей жизни, всегда пользуются популярностью, так как сообщают новости о знаменитостях. Поскольку этим людям есть что сказать, их блоги привлекают множество читателей.

Я считаю, что у каждого блога свои читатели, все зависит от интересов. Поэтому вряд ли можно устанавливать какие-то правила и ограничения для блогов.

Я избрал два метода. Первый – это неофициальное (разговорное) представление моего отношения к текущим проблемам и событиям. Второй – это написание новостей, анализ, интервью, репортажи или эссе. Так что у меня две группы читателей: те, кто хочет знать, что я делаю каждый день и те, кого интересует моя точка зрения, как журналиста, писателя и поэта.

Как онлайновое средство информации, блог дает пишущему возможность знакомиться со взглядами и критикой читателей и отвечать им, что позволяет автору развиваться. Тесные контакты с читателями дают блоггеру возможность делиться своими взглядами и писать то, что наиболее интересно читателям.
Как я уже говорил, в Иране, если вы хотите напечатать книгу, поэму, рассказ или даже журнал или газету, необходимо получить разрешение властей. Для многих журналистов и писателей это становится препятствием.

Если вы хотите напечатать рассказ, поэму или эссе в газете или журнале, работа должна подвергнуться цензуре. Очень многие иранские писатели

публикуются в блогах, что гораздо дешевле и не требует цензуры. Поэтому правительство, как в Китае и других странах, стремится ограничивать интернет доступ.

Интернет журналистика может содействовать свободе слова и плюрализму мнений. Будучи осужденным в Иране, я не теряю надежды и уверен, что в ближайшие годы руководителям моей страны придется уважать принципы как свободного доступа к информации, так и свободы слова.

Журналист и блоггер Араш Сигарчи родился в 1978 году, во время революции, свергнувшей шаха. Журналистикой занимается с 1993 года, с 15 лет. После победы на выборах 1997 года сторонника реформ Мохаммада Хатами, работал в изданиях, поддерживавших реформы. После того, как в апреле 2002 года его издание было закрыто, переселился в северный Иран, где редактировал 12-страничную ежедневную газету Gilan Emrouz (сейчас Gilan).

С 2001 года начал писать в коллективном блоге Gileh Mard ("Человек из Гилана"). В 2002 году создал персональный вебсайт Panjereh Eltehab ("Окно надежды") (www.sigarchi.com).

В начале 2005 года был на два месяца задержан Министерством информации и безопасности и приговорен к 14 годам тюрьмы. В настоящее время освобожден до окончания дела по рассмотрению апелляции.

НЕПАЛ

“МЫ РАССКАЗЫВАЕМ МИРУ О ТОМ, ЧТО ПРОИСХОДИТ”

Радио «Свободный Непал» (Radio Free Nepal)
http://freenepal.blogspot.com

1 февраля 2005 года. Вся полнота власти в стране захвачена королем Джанендрой, о чем он сообщил народу в телевизионной речи. После завершения передачи, я решил ознакомиться с международной реакцией на это событие, воспользовавшись модемом для интернет-доступа. Однако оказалось, что телефонная линия была блокирована. В попытке воспрепятствовать любой информации, критикующей его действия, король приказал военным блокировать не только интернет-провайдеров, но и телекоммуникационную связь вообще.

Люди по разному оценивали события, некоторые – позитивно. В редакции же моей газеты рисовали мрачное будущее: военнослужащие в студии в качестве цензоров. Тогда я решил вести дневник. Чтобы записывать события и то, что люди думают по поводу этих событий. Я использовал для этого компьютер.

Восьмого февраля телекоммуникационные услуги и интернет стали доступными. Я получил много электронных писем с просьбами объяснить, что случилось в Непале. И тогда я подумал, что мой дневник сможет объяснить ситуацию наилучшим образом. Мои друзья в Соединенных Штатах Америки предложили поместить дневник на блоге, с обратной датировкой. Поскольку я был новичком в этом деле, они запустили сайт и разместили заметки. Было решено, что я останусь анонимным и попрошу друзей также вести анонимные блоги, что обезопасит нас от возможных преследований и тюрьмы.

Свободный доступ к информации на RFN сделал сайт популярным в условиях жесткой цензуры в средствах массовой информации. Кроме того, Blogger.com рекомендовал посетить сайт. Мои друзья в США делали все возможное для популяризации, и через несколько недель сайт стал довольно известным.

RFN был создан для того, чтобы люди во всем мире могли понять, что думают непальцы о прямом правлении короля. В условиях жесткой цензуры средства массовой информации вынуждены писать то, что хочет король, а этого слишком мало, чтобы представлять голос народа. Несмотря на то, что RFN – это индивидуальное начинание, опирающееся на помощь очень

немногих, сайт лучше представляет голоса простых людей, поскольку свободен от цензуры и притеснений.

Первые заметки имели характер дневниковых записей. Позднее появились осмысление и анализ различных событий. В ситуации, когда король Непала, невзирая на выбор народа, установил прямое правление, RFN стал ресурсом, отражающим мысли простых людей.

Я добиваюсь установления демократии в стране, поскольку убежден, что только при демократии страна будет процветать, а моя карьера журналиста будет иметь смысл. Писать в условиях цензуры - то же, что пить кофе без сахара – невкусно. Мы, журналисты, знаем о многих событиях, сообщения о которых никогда не появятся в газетах. Например, обнародованные RFN сведения о том, что король приобретает собственность незаконным путем. Многие журналисты знали об этом, критиковали короля, смеялись над ним, но не могли об этом написать. RFN также ставит своей целью информировать мир о событиях в Непале. Если бы не было RFN, тысячи людей ничего не узнали бы о ситуации в стране. Я думаю очень важно, чтобы люди в мире думали о Непале и понимали, что здесь происходит.

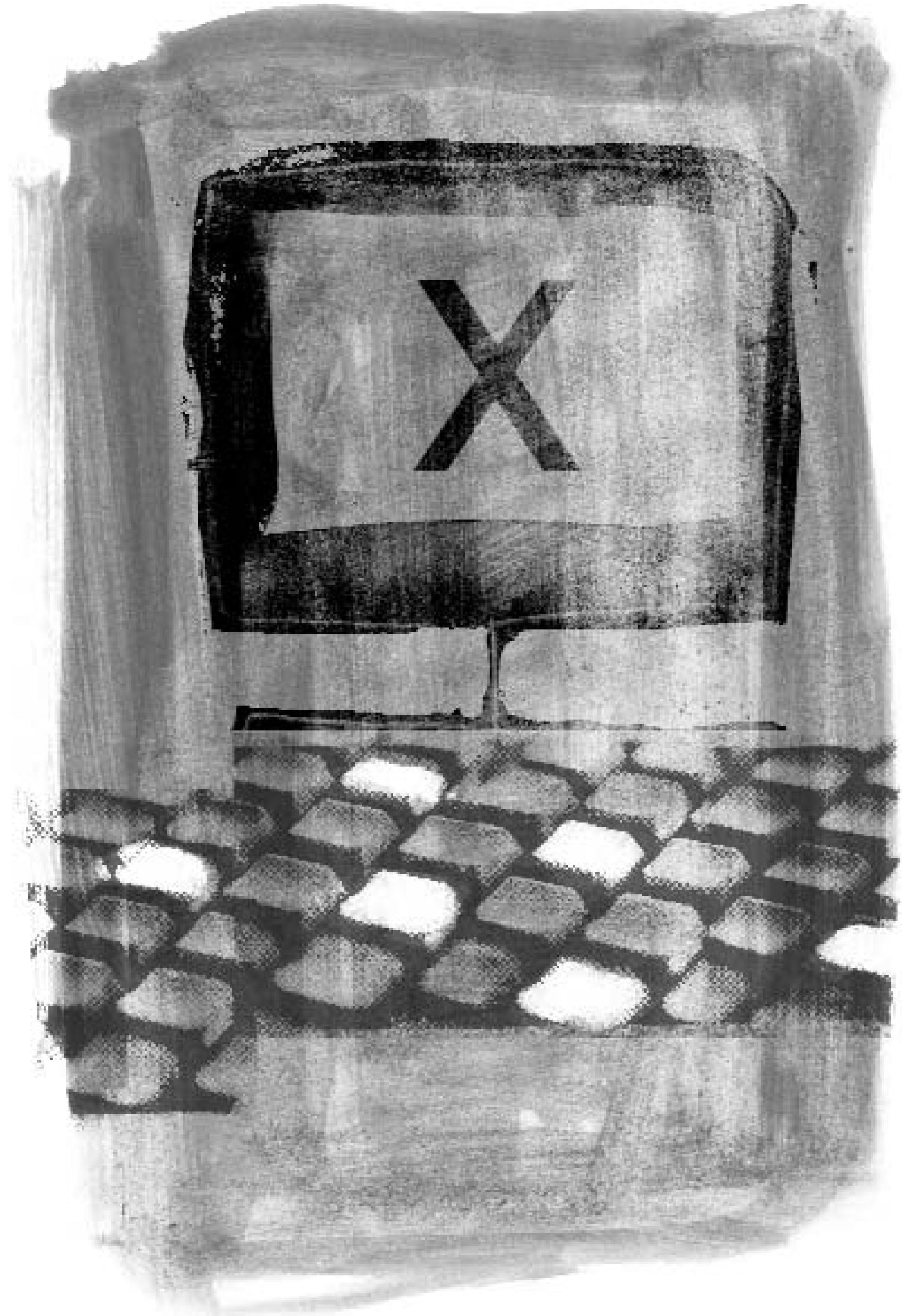
Информационно-коммуникационные технологии так много дали нашему обществу. Я пишу свободно, без страха, потому что уверен в блоггинге. Я пишу заметки, отправляю их другу в США по электронной почте, а он размещает их на блоге. Для того, чтобы раскрыть связь, необходимо потратить слишком много усилий. Когда в моей стране восстановится демократия, когда мы сможем снова свободно дышать, я буду гордиться тем, что внес свой вклад в это дело.

Меня часто спрашивали в электронных письмах о достоверности заметок. Я отвечал, что одно только имя не может быть гарантией достоверности. Я не хочу, чтобы мое имя стало известно, поскольку, пока в Непале не восстановилась демократия, ситуация может ухудшиться, и я могу попасть в тюрьму из-за блоггинга. Я не боюсь тюрьмы, но я хочу, чтобы RFN продолжало информировать мир о Непале. Я говорю им, что они узнают мое имя, когда правлению короля придет конец.

А пока спасибо всем за поддержку.

RFN БЛОГГЕР, НЕПАЛ
wewantdemocracy@gmail.com

Блог Радио «Свободный Непал» (RFN) бросает вызов захвату всей полноты власти королем Джанендрой и цензуре средств массовой информации. Имея целью восстановление демократии в стране, сайт RFN информирует мир о событиях, происходящих в Непале. Автор блога сохраняет анонимность, поскольку в противном случае ему может угрожать арест.


X

КАК ВЕСТИ БЛОГ **АНОНИМНО**

Этан Цукерман (Ethan Zuckerman)

Предлагаемое краткое техническое руководство по анонимному ведению блога предназначено для активных критиков властей в странах с далеко не прозрачным правительством. Оно - не для киберпанков, а для граждан развивающихся стран, которые стремятся обеспечить свою безопасность и неприкосновенность частной жизни.

В пособии «Как вести блог, не подвергаясь опасности», подготовленном Electronic Frontier Foundation (http://www.eff.org/Privacy/Anonymity/blog-anonymously.php), также можно найти ряд очень полезных советов.

СОДЕРЖАНИЕ

ЗНАКОМСТВО С САРОЙ

Сара работает бухгалтером в правительственном учреждении. Она узнает, что ее начальник, заместитель министра, присваивает государственные деньги. Она хочет, чтобы мир узнал о преступлении, но боится потерять работу. Если она сообщит о преступлении министру (в случае, если удастся добиться встречи), ее могут уволить. Она звонит репортеру местной газеты, но та отвечает, что для статьи нужно гораздо больше информации, а также документы, подтверждающие подозрения.

Поэтому Сара решает начать веблог, чтобы рассказать о махинациях в министерстве. Чтобы защитить себя, она должна быть уверена, что никто не узнает об авторе заметок в блоге. Поэтому она может вести блог только анонимно.

Существует два способ выяснить, кто ведет анонимный блог. Во-первых, это можно понять из заметок. Например, если она напишет «я являюсь помощником главного бухгалтера в аппарате заместителя министра угольной промышленности», читатель довольно легко может установить ее имя.

Второй способ – это возможность установить личность Сары на основании информации, сообщаемой web-браузерами и почтовыми программами. Каждый компьютер, подключенный к интернет, имеет IP адрес – серию из пяти цифр от 0-255, разделенных точками. Например, 213.24.124.38. Когда Сара использует web-броузер для размещения заметки, IP адрес включается в текст заметки.

Немного поработав, министерские компьютерщики смогут найти Сару по IP адресу. Сара может использовать домашний компьютер, связываясь с провайдером (ISP) с помощью модема. Но каждый провайдер фиксирует IP адрес и номер телефона пользователя. В одних странах министру потребуется специальное разрешение для получение этой информации, в других (прежде всего, в тех, где доступ в интернет предоставляется государственными компаниями), провайдеры спокойно предоставят эту информацию, и Сара может оказаться в скверной ситуации.

Однако существует ряд способов сохранить анонимность при использовании интернет. Чем в большей безопасности хочет оказаться человек, тем больше работы ему придется проделать. Сара, как и любой другой человек, который хочет вести анонимный блог, должна решить, до какой степени сильна ее паранойя, и сколько усилий она в состоянии потратить на то, чтобы ее не нашли. Как вы узнаете, некоторые стратегии требуют солидных технических знаний и большой работы.

ШАГ 1- ПСЕВДОНИМЫ

Самый простой способ обеспечит анонимность - использовать бесплатную интернет почту и бесплатную блоговую платформу за пределами страны. (Использовать платные сервисы не следует, поскольку по номеру счета или кредитной карты можно установить имя пользователя). Однако Сара может пользоваться псевдонимом. Тогда, найдя ее блог, министр обнаружит, что он принадлежит "A. N. Ymous", а электронный адрес автора блога - anonymous.whistleblower@hotmail.com.

Вот список некотрых провайдеров бесплатных почтовых услуг:

Hotmail
Yahoo
Hushmail - бесплатная почта
с хорошей криптографической защитой

Вот некоторые провайдеры бесплатного хостинга для блогов:

Blogsome - free WordPress blogs
Blogger
Seo Blog

Однако здесь существует одна проблема. Когда Сара подписывается на бесплатную услугу, вебсервер регистрирует ее IP адрес. В этом случае, ее можно найти, если она

пользуется компьютером дома или на работе и если компания, предоставляющая услуги почты и блоггинга, сообщит требуемую информацию. Не так-то просто заставить компании, предоставляющие данные услуги, предоставить такие сведения. Например, чтобы Hotmail сообщил IP адрес Сары, необходимо особое предписание или специальное решение судебных органов США. Но Сара не хочет рисковать в случае, если ее правительство сможет убедить компании сообщить ее IP адрес.

ШАГ 2 – ОБЩЕДОСТУПНЫЕ КОМПЬЮТЕРЫ

Для того, чтобы остаться неузнанной, Сара может использовать компьютеры, которые доступны многим людям. Зарегистрировать свою почту и блог она может при помощи компьютера в интернет-кафе, библиотеке или университетской компьютерной лаборатории. Если министр обнаруживает IP адрес отправителя заметок или комментариев, он видит что сообщения посланы из интернет-кафе, где за компьютером работали сотни людей.

У этой стратегии также есть слабые места. Если в кафе или лаборатории можно установить, кто пользовался компьютером в определенное время, Сару легко найдут. Она не должна отправлять сообщения поздно вечером, когда в лаборатории кроме нее никого нет, поскольку лаборант обязательно ее запомнит. Кроме того, ей все время нужно будет работать в разных интернет-кафе. Если министр обнаружит, что все сообщения были посланы из кафе "Joe's Beer and Bits" на Главной улице, он может приказать установить слежку и легко найти Сару.

ШАГ 3 – АНОНИМНЫЕ PROXY-СЕРВЕРЫ

Саре надоело ходить в интернет-кафе каждый раз, когда нужно отправить сообщение. С помощью соседа-компьютерщика она получила доступ к анонимному proxy-серверу с домашнего компьютера. Пользуясь почтой или платформой для блоггинга, она оставляет IP адрес прокси-сервера, а не адрес домашнего компьютера... теперь министру очень трудно найти ее.
Во-первых, она находит в Google список proxy-серверов по ключевым словам "proxy server". Она выбирает из списка publicproxyservers.com серверы с пометкой "high anonymity", она выписывает адрес proxy и порта.

Вот несколько надежных списков proxy-серверов:
• publicproxyservers.com - анонимные и не-анонимные proxy;
• Samair (http://www.samair.ru/proxy/) - только анонимные прокси, дает информацию о прокси-серверах, которые поддерживают SSL;
• rosinstrument proxy database (http://tools.rosinstrument.com/proxy/) - поиск по базе данных proxy-серверов.

Затем она переходит в раздел "preferences". В разделах «general", "network" или "security", она устанавливает необходимые опции для интернет - доступа через proxy-сервер. (В браузере Firefox эта опция - в разделах Preferences - General - Connection Settings). Она переходит к ручной настройке proxy, вводит IP адрес proxy-сервера, переносит

в поля HTTP proxy и SSL proxy и сохраняет параметры. Она перезагружает браузер и начинает работу в интернет.
Она замечает, что скорость несколько уменьшилась. Это из-за того, что каждая страница, которую она запрашивает, загружается обходным путем. Вместо прямого соединения с hotmail.com, она сначала связывается с proxy-сервером, который, в свою очередь, связывается с Hotmail. Пакет с Hotmail также идет сначала на proxy-сервер, а потом к Саре. Она также отмечает, что возникли задержки при доступе к вебсайтам, особенно к тем, которые требуют регистрации. Но зато ее IP адрес неизвестен провайдеру.

Можно провести с proxy-серверами следующий эксперимент. Зайдите на oreply.org, популярный римейлер (remailer). Вы увидите приветствие со своим IP адресом: "Hello pool-151-203-182-212.wma.east.verizon.net 151.203.182.212, pleased to meet you." А теперь посмотрите anonymizer.com, который позволяет видет некоторые вебстраницы через анонимный proxy. В правое верхнее окно страницы анонимайзера введите URL для http://www.noreply.org (или просто щелкните ссылку http://anon.free.anonymizer.com/; http://www.noreply.org). Вы увидите, что noreply.org теперь считает, что вы пришли с vortex.anonymizer.com (анонимайзер – хороший способ проверить proxy, не изменяя установок браузера, однако этот инструмент не работает с webmail или weblogging серверами).
Наконец, следуя инструкциям, настройте свой web-браузер на работу с анонимным proxy и зайдите на noreply.org, чтобы проверить, определяет ли он ваш IP. Увы, proxy также несовершенны. Если Сара живет в стране, где интернет фильтруется, многие пользователи будут работать с proxy-серверами, чтобы получить доступ к заблокированным сайтам. Правительство, в свою очередь, будет блокировать популярные proxy. Пользователи будут переходить на другие, правительство блокирует и их – и так по кругу. Все это будет отнимать достаточно много времени.

Сара столкнется с проблемами и в том случае, если она – одна из немногих, кто пользуется услугами proxy-серверов. Если заметки на ее блог пересылает один и тот же proxy-сервер, и если министр может потребовать регистрационные записи (logs) у любого провайдера, он может увидеть, что компьютер Сары – один из немногих, имеющих доступ к этому серверу. Он не сможет доказать, что Сара использовала proxy именно для разрешения заметок на блоге. Но он может придти к выводу, что поскольку блог анонимный, а Сара – одна из немногих в стране, кто пользуется доступом к proxy–серверам, значит, именно она отправляла заметки. Поэтому Саре лучше использовать популярные в стране proxy и часто менять их.

ШАГ 4 - РАСКРЫТЬ ИМЯ

Сара начинает думать о том, что владелец proxy-сервера, который она использует, пойдет на компромисс. Что если министр убедит оператора proxy сервера (силой закона или посредством взятки, фиксировать, кто из граждан его страны пользуется

услугами сервера и какие сайты эти люди посещают). Сара надеется, что администратор proxy -сервера защитит ее, но она даже не знает этого администратора. Кроме того, даже если администратор не интересуется подобными вещами, proxy-серверы могут оказаться открытыми.
У Сары есть друзья в Канаде (а в этой стране интернет не подвергается такой цензуре, как у нее на родине), которые могут помогать ей вести блог, сохраняя анонимность. Сара звонит другу и просит установить у себя систему обхода интернет-фильтров (circumventor) – один из десятков proxy-серверов, который пользователь может установить сам, что позволяет другим использовать его компьютер как proxy-сервер.

Джим, друг Сары, загружает circumventor (систему обхода), выложенную на сайте Peacefire.org (http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) и устанавливает его. Это не просто, так как сначала надо установить Perl, затем OpenSA и только после этого – саму систему (circumventor). Кроме того, его компьютер должен быть постоянно подключен к интернет, чтобы Саре не нужно было просить его подключиться каждый раз, когда она посылает заметки. Он устанавливает программное обеспечение, звонит Саре по мобильному телефону и сообщает URL , чтобы Сара могла иметь интернет-доступ через его прокси-серврер или для того, чтобы размещать заметки на блоге. Это особенно удобно, поскольку Сара может использовать proxy-сервер как дома, так и в интернет-кафе.

Хотя Джим очень помогает Саре, существует все же одна серьезная проблема. Джим работает с Windows , поэтому компьютер часто приходится перегружать. Каждый раз, когда это происходит, провайдер присваивает машине новый IP адрес. При этом Сара теряет доступ к серверу. Джим должен снова связаться с Сарой и сообщить новый адрес. Это неудобно и дорого. Сару также беспокоит то, что, если она использует один и тот же IP адрес достаточно длительное время, ее провайдер может под давлением правительства блокировать этот адрес.

ШАГ 5 - ЛУКОВИЧНАЯ МАРШРУТИЗАЦИЯ (ONION ROUTING) И TOR

Джим предлагает Саре поэкспериментировать с Tor. Это относительно новая система, обеспечивающая достаточно хорошую защиту анонимности в интернет. «Луковичная» маршрутизация (onion routing) развивает идею proxy-серверов – компьютеров, которые действуют от вашего имени. Каждый запрос, сделанный через этот маршрутизатор, проходит через ряд дополнительных компьютеров – от 2 до 20. Это практически исключает возможность определения, с какого компьютера был послан запрос.
Каждый шаг в цепочке зашифрован, что также усложняет для правительства процесс установления личности Сары. Более того, каждый компьютер в цепочке знает только ближайших соседей. Другим словами, маршрутизатор B знает, что запрос на вебстраницу пришел от маршрутизатора A и что необходимо передать этот запрос маршрутизатору C. Но сам запрос зашифрован – маршрутизатор B на самом деле не знает, какую страницу запрашивает Сара или какой маршрутизатор завершает цепочку.

Несмотря на сложность технологии, Сара приятно удивлена легкостью установки Tor (http://tor.eff.org/cvs/tor/doc/tor-doc-win32.html) и системы «луковичной маршрутизации» (onion routing). Она загружает программу установки, которая инсталлирует Tor, затем скачивает и устанавливает Privoxy, прокси, работающий с Tor. Кроме того, она получает дополнительные преимущества, так как со страниц, которые она запрашивает, автоматически убирается реклама.

После установки программного обеспечения и перезагрузки компьютера, Сара заходит на noreply.org и узнает, что она надежно защищена программой Tor - noreply.org считает, что запрос пришел из Гарвардского университета. Она делает вторую попытку, noreply показывает запрос из Германии. Так она узнает, что Tor меняет адрес для каждого запроса, что позволяет ей сохранять анонимность.
Однако это имеет некоторые неприятные последствия. При доступе к Google через Tor, переключается язык – английский, японский, датский, голландский – все в течении нескольких минут. Сара рада возможности изучать новые языки, но есть и другие неприятности. Саре нравится писать для Wikipedia, но она обнаруживает, что Wikipedia блокирует ее попытки редактировать статьи, используя Tor.

Tor также не лишен некоторых недостатков других proxy. Tor несколько уменьшает скорость, так что она использует его только в случае необходимости послать заметку на блог или просмотреть запрещенный сайт. Кроме того, она привязана к домашнему компьютеру.
Однако больше всего ее беспокоит то, что иногда Tor не работает. Очевидно, ее провайдер блокирует некоторые маршрутизаторы «луковицы»: когда Tor пытается связаться с блокированным маршрутизатором, после нескольких минут ожидания страница так и не открывается.

ШАГ 6 - MIXMASTER, INVISIBLOG И GPG

Однако существуют возможности решения нашей проблемы и без использования proxy-серверов, даже таких сложных, как Tor.
Из разговоров с местными компьютерщиками, она находит новое решение: Invisiblog (http://www.invisiblog.com/). Сайт поддерживается анонимно группой австралийцев, называющих себя vigilant.tv. Это сайт создан настоящими параноиками для параноиков. Это почта специального формата, которая посылается через римейлерную систему (remailer) MixMaster, имеющая криптографическую подпись.
Чтобы понять последнее предложение, Саре понадобилось немало времени. В конце концов, она установила GPG (http://www.gnupg.org/) – систему шифровки с открытым ключом (public-key encryption: http://en.wikipedia.org/wiki/Public-key_cryptography).
Кратко это можно описать следующим образом: система шифровки с открытым ключом позволяет посылать сообщения, которые может прочитать только адресат. При этом адресат не сообщает свой ключ, так что вы не можете читать письма его корреспондентов. Кроме того, данная система позволяет «подписывать» сообщения, так что их практически невозможно подделать. Таким образом, если посылать

сообщения на блог с такой подписью, блог сможет проверять, действительно ли данное сообщение отправлено Сарой (см. также главу «Как обеспечить тайну переписки?»).

Затем она устанавливает MixMaster, почтовую систему, созданную для того, чтобы скрывать происхождение электронного сообщения. MixMaster использует систему анонимных римейлеров – компьютерные программы, которые убирают всю информацию о происхождении электронного сообщения и отправляют его по назначению. Сообщение, прошедшее через 2-20 римейлеров, очень трудно трассировать, даже если один из римейлеров сохраняет информацию об отправителе. Для создания MixMaster необходимо менять исходники, что, конечно, не сделаешь без помощи компьютерщиков.
Она посылает первое MixMaster сообщение, содержащее открытый ключ, на Invisiblog. Invisiblog использует его, чтобы установить новый блог с замечательным названием "invisiblog.com/ac4589d7001ac238", включающее последние 16 байтов ее GPG-ключа. Последующие сообщения, подписанные отрытым ключом, она посылает на Invisiblog через MixMaster.

При этом скорость также замедляется. Поскольку мейлеры MixMaster перенаправляют сообщения, это может отнять от двух часов до двух дней. И она должна очень осторожно приходить на свой блог. Если она будет делать это часто и ее IP адрес будет часто протоколироваться блогом, можно будет догадаться, что именно она и является автором. Однако ее может успокоить тот факт, что владельцы Invisiblog не имеют ни малейшего представления о том, кто она такая.
Основная проблема Invisiblog заключается в том, что система чрезвычайно сложна для пользователей. Для многих довольно трудно установить GPG и понять все тонкости открытых и закрытых ключей. Даже системы криптографии, созданные для обычного пользователя, например, Ciphire, не так уж просты. В результате, очень немногие - даже среди тех, кому это действительно нужно – используют шифрование в электронной переписке.

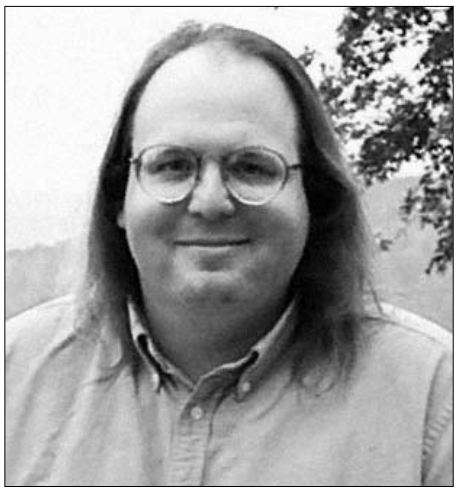
MixMaster – это технически сложная система. Пользователи Windows могут обратиться к ранним DOS-версиям программы, которые доступны на http://prdownloads.sourceforge.net/mixmaer/mix204b46.zip&download. Правда, когда я тестировал ее, она не стала работать... или моя почта все ходила взад-вперед между римейлерами. Все, кто хочет использовать более новые версии или установить программу на Linux или Mac, должны писать программы сами, а это умеют далеко не все опытные пользователи. Возможно Invisiblog станет более доступным, если будет принимать сообщения римейлеров доступных через веб, например riot.eu.org. Но пока вряд ли он сможет помочь тем, кто действительно в нем нуждается.

В странах с репрессивными режимами существуют и другие проблемы с шифрованием. Например, если компьютер Сары будет конфискован и ее ключ станет известен, это даст доказательство того, что Сара является автором подрывного

блога. А в странах, где шифрование не слишком популярно, уже сам факт отправления сообщения через MixMaster, где оно тщательно шифруется, может быть достаточным для того, чтобы ее деятельность привлекла пристальное внимание властей.

СТЕПЕНЬ АНОНИМНОСТИ

Подходит ли вам решение Сары – обучиться криптографии, программированию и использовать MixMaster? А может быть комбинации шагов 1-5 достаточно, чтобы вести блог анонимно? На эти вопросы нет единственно правильного ответа. При принятии решения всегда необходимо учитывать местные условия, уровень своей технической подготовленности и степень паранойи. Если вы считаете, что ведение блога рискованно и если вы сможете установить Tor, это очень хорошее решение.



И помните: не следует подписывать заметки блога своим настоящим именем!

Этан Цукерман, сотрудник Центра «Интернет и общество» Гарвардской юридической школы. Тема его исследований - отношения между гражданской журналистикой и традиционными медиа, главным образом, в развивающихся странах. Он основал и некоторое время возглавлял Geekcorps, некоммерческую организацию, проводившую тренинги в развивающихся странах. Этан Цукерман также один из основателей хостинговой компании Tripod.

КАК ИЗБЕЖАТЬ ЦЕНЗУРЫ: ТЕХНИЧЕСКИЕ СОВЕТЫ

Нарт Вилленёв (Nart Villeneuve)

СОДЕРЖАНИЕ

ФИЛЬТРАЦИЯ КОНТЕНТА

Технологии фильтрации позволяют контролировать доступ к интернет-контенту. Разработанные первоначально для индивидуальных нужд – чтобы родители могли ограничивать доступ детей к нежелательному контенту – технологии фильтрации в настоящее время широко используются различными организациями и государственными структурами. Контроль доступа к интернет-контенту становится приоритетом для целого ряда организаций и учреждений, в том числе для школ, библиотек и корпораций. Технологии фильтрации все шире используются на государственном уровне. Все население страны могут лишать доступа к определенным сайтам, при этом правительства практически не отчитываются в своих действиях.

Технологии фильтрации основываются на блокировании определенных сайтов, входящих в список запрещенных, и на контроле определенных ключевых слов, что позволяет осуществлять динамичное блокирование контента. Составляются списки доменных имен и URL, затем они систематизируются и сообщаются специальным прог-

раммам, которые блокируют определенные категории сайтов. Когда пользователи пытаются открыть страницу, программа фильтрации обращается к базе данных и блокирует доступ к страницам, включенным в список. Если блокируется поиск по определенным ключевым словам, программа проверяет каждую страницу (домен, URL и/или тело контента (body content) запрашиваемой страницы) и динамически блокирует доступ к web-странице, если обнаруживается какое-либо из запрещенных ключевых слов.

Системы фильтрации могут допускать две основных ошибки: избыточное и недостаточное блокирование. Они часто блокируют доступ к неправильно классифицированному контенту или, наоборот, не блокируют контент, доступ к которому запрещен. Однако главное – это покров тайны, окружающий создание списков сайтов, которые блокируются при помощи технологий фильтрации. Существуют, конечно, открытые списки (они касаются, в основном, порнографии), но списки коммерческих фильтров и списки фильтрации, осуществляемой государственными структурами, сохраняются в тайне. Списки категорий доменов и URL, входящих в коммерческие фильтры, являются интеллектуальной собственностью производителей и не сообщаются широкой публике. Хотя некоторые производители программного обеспечения для фильтрации открывают доступ к онлайновым программам контроля URL, списки блокируемых сайтов остаются секретными и недоступными для независимого наблюдения и анализа.

Очень часто правительства расширяют списки сайтов коммерческих технологий фильтрации. Эти списки часто включают сайты оппозиционных политических партий и газет, правозащитных организаций, международных агентств новостей, сайты, критикующие правительство. В большинстве стран фильтруется, прежде всего, контент на национальном языке, важной мишенью являются также сайты, где возможны дискуссии, в частности, блоги и интернет-форумы.

WEB-ТЕХНОЛОГИИ ОБХОДА ИНТЕРНЕТ-ФИЛЬТРОВ

В ответ на фильтрацию и мониторинг интернета государством, разрабатываются различные технологии, позволяющие пользователям обойти ограничения фильтрации. Существует ряд технологий, которые позволяют гражданам и общественным организациям защитить себя и обходить интернет-цензуру. Эти инструменты получили название «технологий обхода» (circumvention). Суть этих технологий заключается в том, что запрос из страны, где осуществляется фильтрация перенаправляется на машину -посредник, которую фильтр не может блокировать. Этот компьютер затем находит информацию по запросу и передает ее пользователю. Иногда такие технологии разрабатываются с учетом специфической ситуации в стране. Во многих случаях пользователи могут адаптировать для обхода (circumvention) технологии, которые изначально разрабатывались для других целей.

Одни технологии были разработаны частными компаниями, другие – группами хакеров и активистов. Программы могут представлять собой как простые скрипты, так и сложные сетевые протоколы. Принимая во внимание это разнообразие,

потенциальные пользователи должны научиться анализировать достоинства и недостатки определенных техник и технологий, чтобы выбрать способы обхода (circumvention), соответствующие их потребностям.

В реализации технологии обхода (circumvention) участвуют провайдер обхода (circumvention provider) и пользователь. Провайдер обхода устанавливает программу на ссвоем компьютере, находящемся вне зоны фильтрации и делает сервис доступным онлайн для пользователей в зоне контроля. Таким образом, успех технологии зависит от того, насколько она соответствует специфическим потребностям обеих сторон.

Цель данной статьи – проинформировать пользователей, решивших обратиться к технологиям обхода, о существующих возможностях и о критериях выбора подходящей технологии. При этом я учитывал потребности и возможности обоих сторон, пользователей и провайдеров технологий обхода, что необходимо для соблюдения баланса между требуемым уровнем безопасности и удобством технологии для конечного пользователя. Эффективный, безопасный и надежный обход зависит от выбора правильной технологии, нужной пользователю.

ЦЕНКА ПОТРЕБНОСТЕЙ И ВОЗМОЖНОСТЕЙ

Технологии обхода часто предназначены для различных типов пользователей с разными возможностями и опытом. То, что хорошо работает в одной ситуации, может быть не самым лучшим решением для другой. При выборе технологии обхода потенциальный провайдер должен задать себе следующие вопросы:

Сколько будет пользователей и какова пропускная способность каналов? (провайдера и пользователя).
Где находится пункт первичного интернет-доступа предполагаемых пользователей и цель использования?
Каков технический уровень? (провайдера и пользователя).
Доступны ли конечному пользователю надежные внешние контакты?
Какие меры наказания грозят провайдеру и пользователю за использование технологии обхода?
• Понимает ли конечный пользователь угрозы, связанные с использованием специфических технологий обхода?

КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ И ДОСТУПНАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ

Провайдер обхода должен оценить количество пользователей и соотнести это с возможной пропускной способностью канала. Конечный пользователь также должен принимать во внимание пропускную способность интернет-канала, поскольку использование обходных технологий замедлит скорость интернет-доступа.
Те, кто предполагает создать общественно доступный proxy-сервер, должны учитывать, что сервер могут использовать люди, не находящиеся там, где осуществляется фильтрация. Например, сервер может использоваться для загрузки фильмов, что может поглощать большой объем трафика. Поэтому вы, возможно, будете ограничивать либо

доступ к серверу, либо трафик. Различные технологии предоставляют различные возможности для разрешения подобных проблем.

ПЕРВИЧНЫЙ ПУНКТ ДОСТУПА И ИСПОЛЬЗОВАНИЕ

В зависимости от места доступа конечного пользователя, выбираются различные технологии обхода и услуги сервера. Например, пользователи, подключающиеся к интернет через общественно-доступные компьютеры и в интернет-кафе, скорее всего, не смогут устанавливать программное обеспечение, их доступ к онлайновым решениям также может быть ограничен. Некоторые будут стремиться использовать не только решения, основанные на технологии WWW (http), но и электронную почту (SMTP) и программы передачи файлов (FTP), поэтому им необходимо будет устанавливать новое программное обеспечение и изменять установки. Конечно, это требует определенных технических навыков.

УРОВЕНЬ ТЕХНИЧЕСКИХ ЗНАНИЙ

Чем выше уровень технических знаний (и меньше число пользователей), тем большее число решений становится доступным. Основными проблемами для простых пользователей являются инсталляция и запуск процесса, изменения конфигурации и другие действия, которые необходимо предпринять для реализации технологии обхода. Это касается как провайдера обхода, так и конечного пользователя. Некорректное использование технологий обхода подвергает пользователей неизбежному риску.

НАДЕЖНЫЕ КОНТАКТЫ

Большое значение для конечных пользователей имеет наличие людей, которым они доверяют, за пределами страны. Если у пользователя нет контактов, его возможности ограничены общедоступными системами. Но если пользователь может найти эти системы, то же могут сделать и те, кто осуществляет фильтрацию и блокирование. Имея надежные контакты, конечный пользователь может консультироваться с провайдером для того, чтобы выбрать решение, соответствующее его специфическим потребностям, сохраняя при этом конфиденциальность. Успешное и длительно использование технологий обхода в значительной степени зависит от надежных контактов с людьми, живущими там, где фильтрация не осуществляется.

ВОЗМОЖНЫЕ НАКАЗАНИЯ

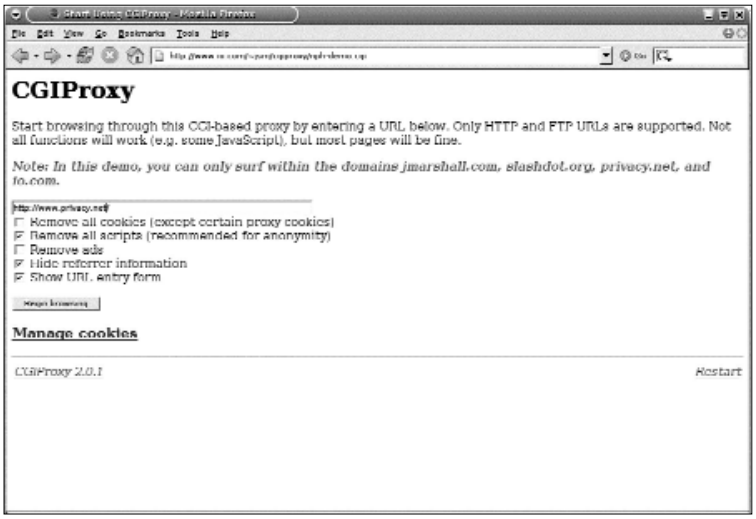
Чрезвычайно важно знать о наказаниях за использование технологий обхода. Выбор решения зависит от суровости наказания. Если законодательство достаточно мягкое и наказание не слишком сурово, пользователи могут выбрать эффективное решение, которое не требует чрезвычайной секретности. Но если законодательство сурово, необходимо выбирать технологии, которые обеспечивают максимальный уровень безопасности. Возможно даже придется придумывать легальное прикрытие для обходных технологий или другие меры предосторожности.

РИСКИ БЕЗОПАСНОСТИ

Очень часто пользователям предлагают обходные технологии, не предупреждая их о возможных рисках, которые могут быть минимизированы при использовании нужной технологии в нужном месте и при правильном поведении конечного пользователя.

WEB-ТЕХНОЛОГИИ ОБХОДА ИНЕТРНЕТ-ФИЛЬТРОВ

Web-технологии обхода – это специальные вебстраницы, содержащие форму, которая позволяет пользователю просто ввести URL, после чего онлайновая система обхода (web-based circumventor) осуществляет поиск страницы и показывает ее пользователю. Между пользователем и запрашиваемым сайтом не устанавливается связь, сервер передает запрос, что позволяет пользователю, оставаясь незамеченным, просматривать блокированные сайты. Онлайновые серверы также переписывают ссылки в запрашиваемой странице, так что пользователь может продолжать интернет-поиск. При использовании онлайновых систем обхода, конечному пользователю не нужно устанавливать никаких дополнительных программ. Все, что нужно сделать – это придти на соответствующий сайт, ввести URL сайта, который они хотят посетить и щелкнуть на кнопку (Внешний вид онлайновых систем обхода может быть разным, но их базовые функции одинаковы). Таким образом, не требуется никаких специальных технических знаний. Кроме того, эту технологию можно использовать независимо от типа доступа.



Proxy-серверы / изменение установок

Преимущества:

Онлайновые системы обхода просты в использовании и не требуют от конечного пользователя установки специальных программ.

Общедоступными онлайновыми услугами обхода могут пользоваться те, кто не имеет

надежных контактов там, где не осуществляется фильтрация.
Частные онлайновые системы обхода могут адаптироваться к специфическим нуждам пользователей, такие системы сложнее отследить органам, осуществляющим фильтрацию.

Недостатки:
Онлайновые системы обхода чаще всего ограничены web-трафиком (HTTP) и закрыты для шифрованного доступа (SSL). Так что web-сервисы (например, web-почта), которые требуют аутентификации, могут плохо функционировать. Общедоступные онлайновые услуги обхода обычно хорошо известны и могут быть заблокированы. Большинство таких серверов блокируется коммерческими фильтрующими программами.
Для того, чтобы пользоваться частными онлайновыми системами обхода, необходимо иметь связи с людьми в тех странах, где контент не фильтруется. В идеале, стороны должны иметь возможность общаться, не подвергаясь угрозе слежки.

ОБЩЕДОСТУПНЫЕ ОНЛАЙНОВЫЕ СИСТЕМЫ ОБХОДА

Существует как общедоступное программное обеспечение для обхода фильтров, так и общедоступные услуги. Большинство из них - бесплатные, хотя системы, предоставляющие дополнительные услуги (шифрованный доступ) могут требовать платную подписку. Вот несколько примеров:

http://www.anonymizer.com/	http://www.guardster.com/
http://www.unipeak.com/	http://www.webwarper.net/
http://www.anonymouse.ws/	http://www.proximal.com/
http://www.proxyweb.net/	http://www.the-cloak.com/

Поскольку эти адреса широко известны, они уже включены в большинство списков интернет - фильтров. Ясно, что если эти сайты блокированы, то пользоваться услугами невозможно. Кроме того, большинство общедоступных систем обхода не шифруют трафик между системой обхода и конечным пользователем. Любая информация, отправленная пользователем, может быть перехвачена оператором программы обхода.

Общедоступные системы обхода наиболее удобны для пользователей, которые подвергаются минимальному риску, не имеют личных контактов в странах, где не осуществляется интернет-фильтрация, обращаются к услугам от случая к случаю и не нуждаются в передаче важной информации.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Установка программного обеспечения для обхода фильтрации может требовать определенных технических знаний и ресурсов (сервер и пропускная

способность). Местонахождение частного сервера известно только тем, кто имеет к нему доступ, в то время как адреса общедоступных систем обхода и анонимных серверов известны как пользователям, так и тем, кто осуществляет фильтрацию (эти адреса также входят в списки блокировки всех коммерческих фильтров). Частную систему обхода гораздо сложнее найти и блокировать, чем общедоступную.

Частные системы обхода можно приспособить к специфическим нуждам конечного пользователя. Так, например, обычно изменяют номер порта на сервере и выполняют шифрование. Протокол защищенных сокетов (Secure Sockets Layer, SSL) - это протокол, гарантирующий безопасную передачу данных по сети. Этот протокол обычно используется сайтами для того, чтобы обеспечить защиту передаваемой информации, например номера кредитных карточек. Доступ к сайтам, защищенным SSL, обеспечивается посредством протокола HTTPS, вместо обычного HTTP.

Кроме того, SSL позволяет создать в корне сервера безвредную страницу и скрыть систему обхода при помощи случайного пароля и имени файла. Несмотря на то, что третья сторона может определить сервер, с которым связывается пользователь, она не сможет проследить путь запроса, поскольку часть запроса шифруется. Например, если пользователь запрашивает адрес https://example.com/sectretcircumventor/, третья сторона увидит только часть https://example.com/, и не узнает, что пользователь обращался к системе обхода. Если оператор размещает безвредную страницу на example.com, то система обхода вообще не будет обнаружен.

• CGIProxy: A CGI-скрипт, работает как HTTP или FTP proxy.
http://www.jmarshall.com/tools/cgiproxy
• Peacefire's Circumventor: автоматический инсталлятор программ, который облегчает установку и настройку CGIProxy для неопытных пользователей.
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
• pHproxy: экспериментальная, имеющая гибкие настройки онлайновая система обхода.
http://ice.citizenlab.org/projects/phproxy
• Psiphon: SSL- вебсервер с свтроенной онлайновой системой обхода (будет запущен в ближайшее время).
http://soon to be released

Частные онлайновые системы обхода, обеспечивающие шифрование, удобны для пользователей, которым необходимо постоянно обращаться к технологиям обхода и которые имеют надежные контакты в странах, где не осуществляется фильтрация интернет, с людьми, обладающими достаточными техническими навыками и ресурсами и способными поддерживать онлайновую систему обхода. Это наиболее гибкое решение для обычного интернет-трафика. Оно достаточно надежно и защищено от блокирования.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Системы обхода не всегда обеспечивают анонимность. Личность конечного пользователя скрыта от операторов посещаемых сайтов. Если же сеанс связи между пользователем и онлайновой системой обхода осуществляется в режиме простого текстового протокола (HTTP), на котором основано большинство бесплатных услуг, контент может быть легко перехвачен и проанализирован третьей стороной, в частности, провайдером услуг интернет (ISP). Поэтому даже при успешном обходе фильтрации, власти могут установить факт посещения пользователем онлайновой системы обхода. Более того, они могут определить контент, включая список сайтов, которые посещал пользователь онлайновой системы обхода.

Онлайновые системы обхода, которые работают в режиме простого текста (нешифрованного) часто используют замену знаков в URL, чтобы сбить с толку системы, предназначенные для фильтрации контента по ключевым словам в URL. Например, простая технология ROT-13 основана на том, что буквы заменяются одним из 13 символов, предшествующими им в алфавите: URL http://ice.citizenlab.org принимает вид uggc://vpr.pvgvmrayno.bet/ . Другими словами, текст URL кодируется таким образом, что ключевые слова, по которым осуществляется фильтрация, исчезают из URL. Тем не менее, контент сайта остается доступным для прослеживания даже в случае удачного обхода.

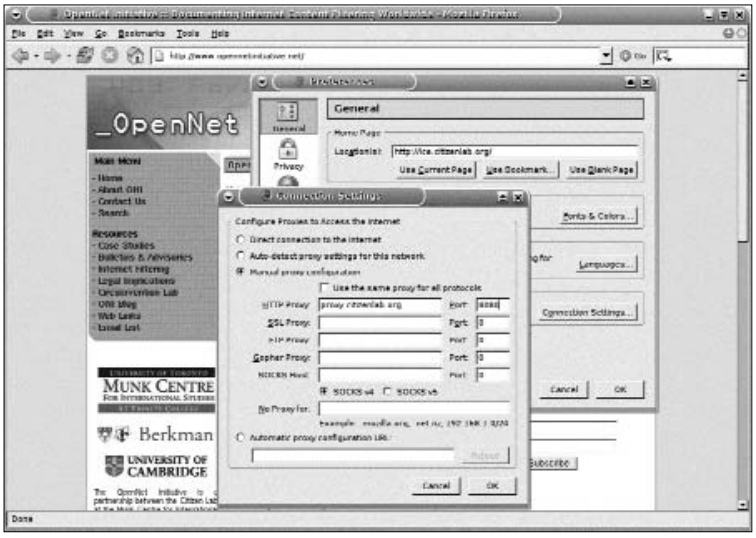
Существуют также риски, связанные с использованием скриптов и фрагментов данных о предыдущих обращениях пользователей (cookies). Многие онлайновые системы обхода удаляют такие фрагменты и скрипты. Однако при этом должны соблюдаться определенные предосторожности. С этим связан и риск использования паролей при входе в систему, основанную не передаче простого текста и использования системы для запроса информации с шифрованного сервера (encrypted server). В этой ситуации, системы обхода получают информацию от SSL-сервера посредством передачи шифрованных данных, но затем посылают контент пользователю в виде простого открытого текста. Таким образом, создается возможность для перехвата информации.
Некоторые из перечисленных выше проблем могут быть решены посредством использования шифрованной связи с онлайновыми агентами доступа (proxies). Доступ к некоторым онлайновым программам (proxies) возможен на основе SSL (HTTPS) протоколов, которые шифруют связь между конечным пользователем и онлайновой системой обхода. В этом случае третья сторона может видеть связь пользователя с онлайновой системой обхода, но не получит доступа к контенту. Если использование технологий обхода фильтрации опасно, пользователи обязательно должны удостовериться, что они используют SSL протокол.

Несмотря на то, что связь пользователя с онлайновой системой обхода

онлайновым может быть надежно защищена, любая информация проходящая через систему, может быть перехвачена его владельцем. Таким образом, необходимо предпринять меры для того, чтобы владелец системы обхода не раскрывал информацию. В зависмости от места расположения системы или сервера, у властей может появиться возможность доступа к регистрационным записям (log files).

Пользователи должны понимать, что и при использовании SSL-протоколов, существуют определенные опасности. Например, пользователи могут привлечь внимание властей из-за использования криптографии, что считается незаконным в некоторых странах. Кроме того, власти могут определить, какие сайты пользователь посещает при помощи обходного модуля, используя такие технологии как атаки HTTP fingeprinting и Man-in the Middle (MITM) attacks. Тем не менее, страницы с динамическим контентом и ситемами обхода, которые добавляют ложный текст или изображение к запрашиваемому контенту могут свести риск от подобных атак до минимума. Если у пользователей есть "отпечатки пальцев", или цифровая подпись SSL-сертификата, они могут вручную проверить аутентичность сертификата, избежав риска MITM атаки (1).

PROXY-СЕРВЕРЫ



Proxy -сервер - это сервер, расположенный между клиентом (web-браузером) и web-сервером. Proxy-сервер действует как буфер между клиентом и сервером и может поддерживать различные запросы, включая web-трафик (HTTP), протокол передачи файлов (FTP) и зашифрованный трафик (SSL). Proxy-серверы используются отдельными людьми, учреждениями и государствами для разных целей, в том числе для обеспечения безопасности, анонимности, кэширования и фильтрации. Для того, чтобы использовать proxy-сервер, конечный пользователь должен произвести настройку конфигурации своего web-браузера в соответствии с IP-адресом или именем хоста proxy-сервера, а также номером порта, который использует proxy-сервер. Несмотря на простоту решения, иногда бывает невозможно настроить браузер в пунктах общественного интернет-доступа - библиотеках или интернет-кафе, на работе.

1. Подробнее о возможных атках на модули обхода - в статье Беннетта Хейзелтона (Bennett Haselton) List of possible weaknesses in systems to circumvent Internet censorship (http://peacefire.org/circumventor/list-of-possible-weaknesses.html)." и в ответе Поля Барановски (Paul Baranowski) http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

Преимущества:
Существует большой выбор программных пакетов, которые попозволяют прозрачно использовать различные типы трафика, а не только web-трафик (HTTP), и которые можно настроить для работы на нестандартных портах. Существует множество общедоступных proxy-серверов.

Недостатки:
Многие proxy-серверы не настроены на шифрование по умолчанию, поэтому трафик между пользователем и сервером не защищен.
Пользователь должен получить разрешение изменить необходимые настройки браузера, и если провайдер услуг интернет требует, чтобы трафик шел через его proxy-сервер, общедоступными серверами нельзя будет воспользоваться.
Использование общедоступных proxy-серверов может быть незаконным, поэтому такие серверы могут быть не всегда доступными для пользователя.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ PROXY-СЕРВЕРОВ

Программное обеспечение для proxy-серверов может быть установлено надежными людьми в странах, где интернет-контент не фильтруется. Эти люди должны обладать некоторыми техническими знаниями. Программное обеспечение proxy-серверов должно устанавливаться там, где возможна большая пропускная способность интернет-канала. Кроме того, должны использоваться технологии криптографии. Это особенно удобно в ситуациях, когда небольшая организация нуждается в технологиях обхода фильтрации интернет. После того как пользователи настроили свой браузер для работы через proxy-сервер, они могут осуществлять поиск информации в интернет. Не являясь самыми незаметными технологиями обхода, proxy-серверы все же более надежны, чем онлайновые proxy-системы. Они более удобны для доступа к сайтам, которые требуют аутентификации и паролей, например, к web-почте.
Proxy-сервреры также легко адаптировать к специфическим потребностям конечного пользования с учетом применяемых механизмов фильтрации.

- Squid - бесплатное программное обеспечение для proxy -серверов, может быть защищено при помощи сервера Stunnel.
  http://www.squid-cache.org, http://www.stunnel.org
  http://ice.citizenlab.org/projects/aardvark
- Privoxy имеет дополнительные возможности фильтрации для защиты конфиденциальности. http://www.privoxy.org
- Secure Shell (SSH) встроенный socks proxy ($ ssh -D port secure.host.com)
  http://www.openssh.com
- HTTPport/HTTP хост позволяет обойти HTTP proxy, который блокирует интернет-доступ.

Частные proxy-серверы с опциями шифрования - лучшее решение для пользователей в офисах, когда необходим постоянный доступ к модулям обхода фильтрации. Такой сервер должен находиться за пределами страны, обеспечивать необходимую пропускную способность и поддерживаться надежными людьми, обладающими необходимыми техническими навыками.

ОБЩЕДОСТУПНЫЕ PROXY -СЕРВЕРЫ

Открытые proxy-серверы - это серверы, которые поддерживают контакты с удаленными компьютерами. Часто трудно определить создан ли такой сервер намеренно или просто неправильная конфигурация сервера позволяет осуществлять такую связь.

ПРЕДУПРЕЖДЕНИЕ: В соответствии с законодательством некоторых стран использование proxy-серверов может трактоваться как "несанкционированный доступ", а пользователи могут понести за это наказание. Мы рекомендуем не использовать открытые proxy-серверы.

Местонахождение открытых proxy-серверов

На многих вебсайтах можно увидеть списки открытых proxy -серверов, однако это не гарантирует, что перечисленные в них серверы функционируют. Нет также гарантий того, что эти списки точны, в особенности это касается уровня анонимности и географического расположения серверов. Помните, что вы пользуетесь этими серверами на свой страх и риск.

Список сайтов с открытыми proxy:

http://www.samair.ru/proxy/
http://www.antiproxy.com/
http://tools.rosinstrument.com/proxy/
http://www.multiproxy.org/
http://www.publicproxyservers.com/

Программное обеспечение: ProxyTools/LocalProxy

http://proxytools.sourceforge.net

Открытые proxy: нестандартные порты

Во многих странах, где осуществляется фильтрация интернет, блокируется доступ к стандартным портам proxy. "Порт" - это абстракция, используемая транспортным протоколом интернет для обозначения соединения. Различные интрнет-сервисы передают данные через определенные порты. Номера портов распределяются организацией Internet Assigned Numbers Authority (Центральный координатор по присвоению уникальных параметров протоколов интернет). Например, порт 80 зарезервирован для HTTP трафика. Когда браузер получает доступ к определенному сайту, вы на самом деле устанавливаете связь с портом 80. Proxy-серверы также имеют порты, приписанные им по умолчанию. Программы фильтрации могут блокировать доступ к этим портам. Поэтому для успешного обхода фильтрации необходим proxy, который настроен на работу через нестандартный порт.

http://www.web.freerk.com/proxylist.htm

PROXY-СЕРВЕРЫ: БЕЗОПАСНОСТЬ

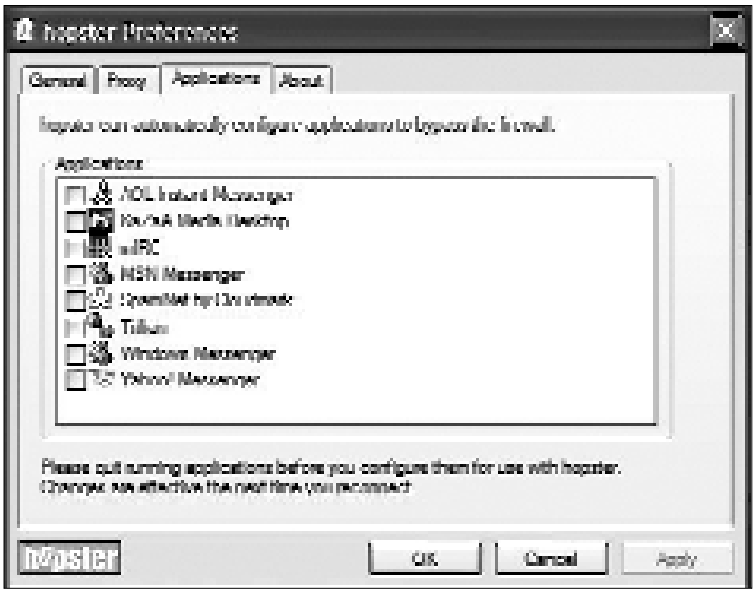
От конфигурации proxy-сервера зависит уровень анонимности соединения. Кроме того, что proxy-серверы не обеспечивают шифрование данных, они могут передавать информацию о конечном пользователе серверу, на который поступил запрос, что дает возможность установить IP -адрес компьютера, с которого поступил запрос. А поскольку связь между вами и proxy-сервером осуществляется в режиме открытого текста, контент легко перехватить. Информация же, проходящая через proxy-сервер, всегда может быть перехвачена его владельцем. Поэтому мы не рекомендуем использование общедоступных proxy-серверов. Открытые proxy-серверы часто используются из-за простоты доступа, однако они не обеспечивают необходимый уровень защиты, хотя и позволяют успешно обойти фильтрацию.

Как и онлайновые proxy, proxy-серверы не обеспечивают безопасность. Конечный пользователь может получать нежелательные скрипты и "cookies" . Кроме того, даже при использовании инструментов шифрования, proxy-серверы могут подвергнуться атакам MITM и HTTP fingertips. Необходимо также отметить, что при использовании некоторых браузеров возможна утечка информации при соединении с proxy-серверами, обеспечивающими не только web-трафик, но и другие типы трафика. При запросе какого-либо вебсайта, доменное имя переводится в IP-адрес. Некоторые браузеры выполняют эту операцию сами, т.е процесс не осуществляется через proxy. В этом случае запрос сайта с блокированным доменным именем выполняется серверами Системы доменных имен (Domain Name System, DNS) в стране, которая осуществляет фильтрацию (2).

2. Смотри сайт: http://tor.eff.org/cvs/tor/doc/CLIENTS

Мы не рекомендуем пользоваться открытыми общедоступными proxy-серверами. Такие серверы пригодны для периодического использования в странах, где это не влечет за собой серьезных последствий. Открытые proxy-серверы не следует использовать для передачи важной информации.

ТУННЕЛИРОВАНИЕ



Программное обеспечение для туннелирования

Туннелирование, или переадресация портов, позволяет инкапсулировать открытый, нешифрованный трафик при помощи протоколов шифрования. Пользователь, подвергаемый цензуре, должен загрузить клиентскую программу, которая создает тоннель к компьютеру, находящемуся вне пределов фильтрации. Пользователю доступны все обычные сервисы, однако он получает доступ к ним через шифрованный туннель, ведущий к безопасному компьютеру, который, в свою очередь, перенаправляет запросы и ответы на них. Существуют различные программы для туннелирования. Те, у кого есть связи с людьми в странах, не осуществляющих фильтрацию, могут использовать частные услуги. Те же, у кого таких контактов нет, могут подписаться на платные коммерческие услуги.

Бесплатные сервисы, как правило, используют рекламу. Рекламные запросы передаются открытым текстом (HTTP). Эти запросы могут быть перехвачены и третья сторона может узнать об использовании услуг переадресации. Кроме того, многие услуги туннелирования используют socks proxy, что может привести к утечке информации о запрашиваемых доменных именах.

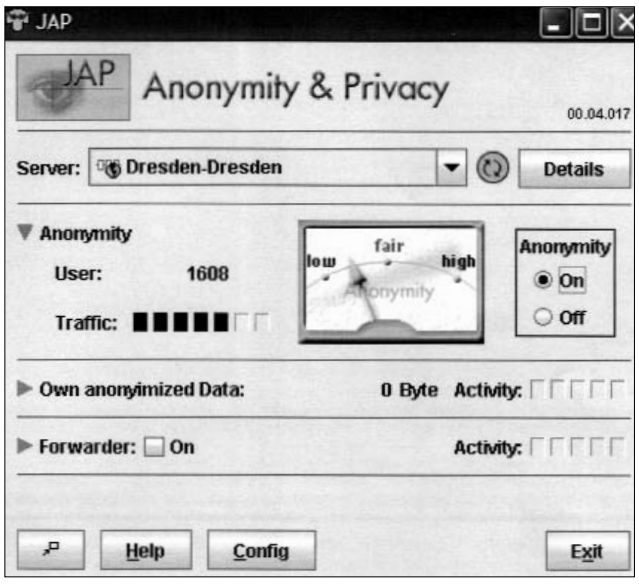
http://www.http-tunnel.com/
http://www.hopster.com/
http://www.htthost.com/

Преимущества:
Переадресация портов обеспечивает шифрованную передачу данных.
Приложения обычно могут использовать различные протоколы, а не только web-трафик.
Существуют коммерческие услуги, которыми можно пользоваться даже в странах, осуществляющих фильтрацию интернет.

Недостатки:
Коммерческие услуги переадресации портов могут быть известны, а потому также подвергаться фильтрации. Приложениями туннелирования невозможно пользоваться в пунктах общественного интернет-доступа (библиотеках, интернет-кафе и т.п.), где нельзя устанавливать свои программы. Использование таких приложений может требовать более глубоких технических знаний, чем другие методы обхода фильтрации.
Технологии переадресации портов наиболее удобны для пользователей, обладающих определенными техническими знаниями, которым нужны безопасные (но не анонимные) услуги обхода фильтрации, причем не только web-трафика. Услуги туннелирования, предоставляемые на коммерческой основе, могут быть отличным решением для пользователей, которые не имеют контактов в странах, где не осуществляется фильтрация.

АНОНИМНЫЕ КОММУНИКАЦИОННЫЕ СИСТЕМЫ

Технологии обхода и анонимные коммуникационные системы похожи и часто взаимодействуют, хотя предназначены для разных целей. Анонимные коммуникационные системы, прежде всего, обеспечивают конфиденциальность запрашивающего пользователя от провайдера контента. Кроме того, некоторые усовершенствованные системы используют разнообразные техники маршрутизации, чтобы обеспечить защиту от самой системы анонимных коммуникаций. Системы обхода интернет-фильтрации не всегда гарантируют анонимность пользователя. Они обеспечивают безопасные коммуникации для преодоления специфических запретов на отправку и получение сообщений. Для выполнения этой задачи требуются безопасные технологии связи, иногда некоторая "маскировка", но не обязательно анонимность.
Анонимные коммуникационные системы часто используют для обхода интернет-фильтров. Преимущество таких систем заключается в том, что имеется несколько сетей, войдя в одну из которых, можно обойти запреты на доступ к определенному контенту, сохраняя анонимность.



Использование анонимных коммуникационных систем для обхода фильтров требует установки соответствующего программного обеспечения. Те, кто имеет доступ в интернет через публичные терминалы, библиотеки или интернет-кафе, вероятнее всего, не смогут использовать такие системы. Кроме того, анонимные коммуникационные системы также могут замедлить скорость интернет-подключения.

Пользователи, стремящиеся обойти интернет-фильтрацию на национальном уровне или на уровне провайдера интернет-услуг, могут узнать, что власти принимают меры для блокировки анонимных коммуникационных систем. Если используемая система оперирует через статический порт, фильтрующие программы легко могут быть настроены на блокирование доступа к ней. Чем более известна анонимная коммуникационная система, тем больше риск того, что ее блокируют. Кроме того, для борьбы с системами, использующими одноранговые или общедоступные узлы, власти могут просто закрыть доступ к этим хостам. Власти могут также запустить собственный узел, чтобы проследить пользователей, пытающихся подключиться к нему.В некоторых странах, где установлены серьезные ограничения, трафик к известным системам прослеживается, и их использование таких систем может привлечь внимание к пользователю (3).

Преимущества:

Они обеспечивают как безопасность, так и анонимность.

Они могут обеспечивать безопасный доступ с использованием различных протоколов, не ограничиваясь web-трафиком.

Часто их поддерживают сообщества пользователей и разработчиков, которые могут обеспечить техническую помощь.

Недостатки:

Они не создаются исключительно для обхода, широко известны и могут подвергнуться фильтрации.

Их нельзя использовать в местах публичного доступа, где пользователи не могут устанавливать программное обеспечение, например, в интернет-кафе или в библиотеках.

• Tor - это сеть виртуальных туннелей, позволяющих повышать безопасность и более надежно обеспечивать конфиденциальность при использовании интернет. Tor также позволяет разработчикам программного обеспечения создавать новые инструменты коммуникаций со встроенными функциями безопасности. Tor обеспечивает основу для ряда приложений, позволяющих организациям и индивидуумам обмениваться информацией через общественные сети, не нарушая конфиденциальность. http://tor.eff.org

• JAP позволяет осуществлять интернет-поиск анонимно. Вместо подключения напрямую к web-серверу, пользователь осуществляет обход, используя шифрованное соединение через нескольких посредников, так называемых "mixes".
http://anon.inf.tu-dresden.de/index_en.html

• Freenet - бесплатное программное обеспечение, которое позволяет сообщать и получать информацию в интернет без боязни цензуры. оно полностью децентрализовано, так что и публикаторы, и потребители информации полностью анонимны.
http://freenet.sourceforge.net

3. Дополнительную информацию о системах обхода можно получить из статьи Беннетта Хейзелтона (Bennet Hazelton) "List of possible weaknesses in systems to circumvent Internet censorship"(http://peacefire.org/circumventor/list-of-possible-weaknesses.html) и ответ на нее Поля Барановски (Paul Baranowski): http://peacefire.org/circumventor/list-of-possible-weaknesses.html

Использование таких систем может потребовать довольно высокого уровня технической квалификации.
Анонимные коммуникации предназначены для технически грамотных пользователям, которым необходимы как технологии обхода фильтрации, так и анонимность при использовании различных протоколов, а не только web-трафика. Такие системы также невозможно использовать в общественных пунктах интернет-доступа.

ЗАКЛЮЧЕНИЕ

К выбору технологий обхода фильтров интернет необходимо отнестись со всей серьезностью, тщательно проанализировав специфические потребности, доступные ресурсы и требования безопасности конечного пользователя. Существует широкий спектр технологий, доступных пользователям, которые хотят избежать интернет-фильтрации. Однако, их успешное и стабильное использование зависит от ряда факторов, включая уровень технических умений пользователя, потенциальный риск безопасности и контакты за пределами страны. Правительства также могут принять ответные меры и блокировать сервисы и возможности обхода интернет-фильтрации.

Ключ к успешному и стабильному использованию систем обхода фильтрации - доверие и эффективность. Системы обхода должны учитывать конкретные обстоятельства и обеспечивать возможность адаптации для нужд конечного пользователя. Они должны быть безопасными, реконфигурируемыми и "замаскированными". Между провайдером услуг и конечным пользователем должны быть установлены отношения доверия. Необходимо также осознавать как специфику юридических и политических условий, в которых вынужден работать пользователь, так и ограничений технологий обхода.

Нарт Вилленёв - директор программы технических исследований Citizen Lab (Гражданская Лаборатория), центра междисциплинарных исследований Центре международных исследований (the Munk Centre for International Studies) Университета Торонто. В качестве разработчика программ и исследователя, сотрудничает с OpenNet Initiative (ONI), осуществляя мониторинг и документируя фильтрацию интернет в различных странах. Нарт Вилленёв также занимался сбором, анализом и разработкой технологий обхода интернет-фильтров. Кроме цензуры интернет, Нарт исследует такие феномены, как хактивизм, кибертерроризм и интернет-безопасность. Нарт Вилленёв недавно закончил обучение в рамках программы исследований мира и конфликта в Университете Торонто.

Нарт Вилленёв выражает особую благодарность Мишелю Левеск (Michelle Levesque), Дереку Бамбауэру (Derek Bambauer) и Беннетту Хэйзелтону (Bennett Haselton.

КАК ОБЕСПЕЧИТЬ **КОНФИДЕНЦИАЛЬНОСТЬ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ**

Людовик Пьера (Ludovic Pierrat)

В настоящее время большинство правительств имеют возможность просматривать электронную почту. "Киберполиция" в странах с репрессивными режимами использует эти возможности для ареста политических оппонентов, многие пользователи интернет попадают в тюрьмы за отправление или даже пересылку электронных сообщений. Один из политических диссидентов на Мальдивах был в 2002 году осужден на 15 лет тюрьмы за переписку с Amnesty International. Пользователь интернет из Сирии находится в тюрьме с февраля 2003 года за то, что переслал бюллетень, распространяемый по электронной почте. Я предлагаю несколько советов для обеспечения конфиденциальности электронной почты.

Использование адреса электронной почты, выданной интернет - провайдером (AOL, Wanadoo, Free или любой другой компанией) не гарантирует конфиденциальность. Владельцы сетей, через которые проходит ваша почта, могут с легкостью перехватить ее. Когда власти любой страны начинают следить за интернет - пользователями, провайдеры обычно предоставляют им возможность читать почту.

Адреса web-почты (Yahoo! или Hotmail) более надежны, поскольку не используют серверы местных провайдеров. В таком случае, чтобы отследить, необходимо читать или перехватывать письма в процессе передачи, что технически гораздо сложнее. К сожалению, это преимущество весьма относительно, поскольку полицейские специалисты или хакеры смогут просматривать вашу почту. Шифрование - это основной способ реального обеспечения конфиденциальности сообщений. Существуют два способа шифрования.

КЛАССИЧЕСКОЕ ШИФРОВАНИЕ

Энн и Майкл хотят обменяться секретными сообщениями, поэтому они договариваются о кодах шифровки и дешифровки и о ключах шифрования. Затем они обмениваются сообщениями, используя шифры. Проблема заключается в том, что тот, кто перехватит письма, в которых они обмениваются ключами, сможет читать их переписку. Коме того, этот человек сможет посылать поддельные сообщения Энн и Майклу. Поэтому Энн и Майкл должны обменяться ключами так, чтобы их никто не смог перехватить, при личной встрече, например.

АССИМЕТРИЧНОЕ ШИФРОВАНИЕ

Лучший способ решения проблемы - ассиметричное шифрование. Для этого нужны два ключа - один для шифрования, а другой - для расшифровки. Ключом для шифрования (открытый ключ) можно спокойно обменяться онлайн, поскольку он не может быть использован для дешифровки сообщений. Ключ для дешифровки (закрытый, или секретный) вы никому не сообщаете.

При ассиметричном шифровании Энн имеет два ключа (открытый, который она сообщает, и закрытый, который она держит в секрете). Энн посылает свой открытый ключ Майклу, который с его помощью шифрует свои письма Энн. Однако только Энн, при помощи своего закрытого клоча, может дешифровать письма Майкла. Майкл, в свою очередь, сообщает Энн свой открытый ключ. Конфиденциальность переписки обеспечена.

Но поскольку открытый ключ передается через интернет без всякой специальной защиты, необходимо проверить его достоверность. Каждый ключ имеет "отпечатки пальцев" (короткий набор символов), который можно легко уточнить по телефону.

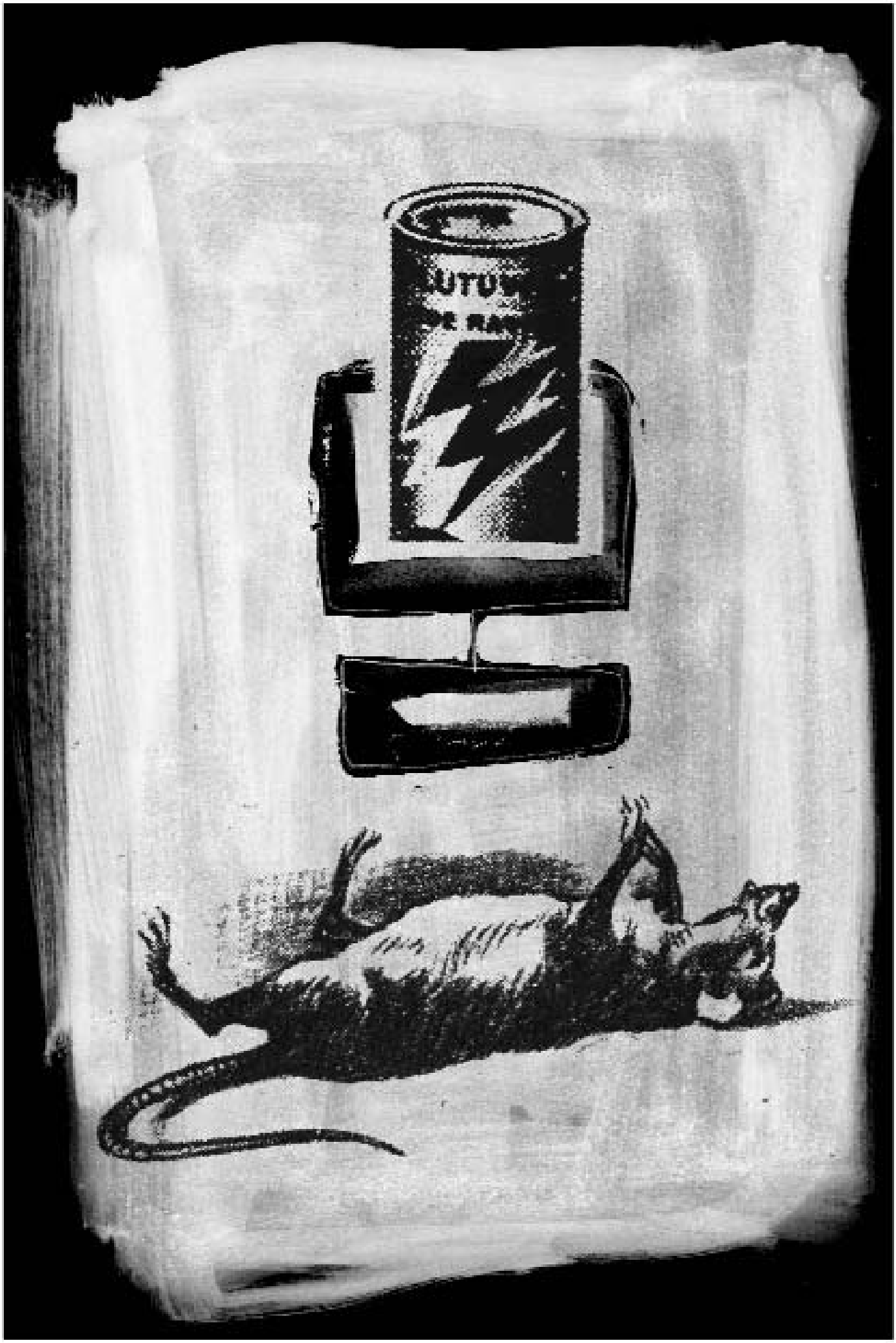
Непроверенный ключ может быть фальшивым, созданным для того, чтобы третьи лица могли следить за перепиской, что лишает шифрование всякого смысла. Надежность асинхронного шифрования полностью зависит от проверки достоверности открытого ключа и секретности закрытого.

OpenPGP (Open Pretty Good Privacy) - это стандартный способ ассиметричного шифрования. Наиболее популярное программное обеспечение для создания и использования двойных ключей и управления открытыми ключами корреспондентов - это GnuPG (GNU Privacy Guard), которую можно использовать в различных почтовых программах, например, Thunderbird или Outlook, ebmail или instant messaging.

Программы можно загрузить с сайтов:
GnuPG :http://www.gnupg.org/
Специальную версию для Windows:
http://www.stud.uni-hannover.de/~twoaday/winpt.html

Людовик Пьера. Инженер вычислительной техники, владелец компании Wa, занимающейся консультированием и производством в сфере информационных технологий.

akjdjqkjddiufdsjhjksd
akjdjqkjddiufdsjhjksd



ЧЕМПИОНАТ МИРА ПО ЦЕНЗУРЕ В ИНТЕРНЕТ

Жульен Пэйн (Jullien Pain)

Большинство авторитарных режимов стремятся контролировать то, что граждане читают и делают онлайн. Они достигают все больших успехов в блокировании «спорного» материала, особенно при помощи технологий, приобретенных у Соединенных Штатов. В этом отношении Китай давно опередил всех, став мировым лидером. Каждая страна из предлагаемого далеко не полного списка выработала свой стиль и тактику, но цель у них одна – диктовать правила игры.

КИТАЙ - ЧЕМПИОН МИРА

Китай стал одним из первых репрессивных режимов, осознавших, что, поскольку без интернет не обойтись, его надо контролировать. Это одна из многих стран, которым удается блокировать материалы, критикующие ражим, при увеличении числа пользователей интернет. В чем же главный секрет? Удачное сочетание инвестиций, технологии и дипломатии.

Пекин потратил десятки миллионов долларов на сложнейшее оборудование для фильтрации и контроля интернет. Система основана на постоянно обновляемом черном списке сайтов. Доступ к «подрывным» сайтам (а это очень широкое понятие, включающее порнографию, политическую критику, призывы к свободе Тибета и независимости Тайваня) – блокируются на уровне национальных магистральных сетей (основных узлов соединения). Но на этом цензура не останавливается, режим автоматически может блокировать доступ к сайтам, где индексируются «сомнительные» ключевые слова или комбинации слов, например «тяньаньмын» + «массовый расстрел».

Режим может также подвергать немедленной цензуре онлайновые дискуссии. Новейшее программное обеспечение и кибер-полиция – вот только два условия из множества, позволяющих правительству потрошить онлайновые форумы (активизировавшиеся в последнее время) и виртуально уничтожать политических диссидентов. Максимальный срок онлайновой жизни призыва к свободным выборам, например, - около получаса. Министерство промышленности и информации внимательно следит за блогами, договорившись о цензуре с китайским блоговыми платформами. Так что заметка о далай ламе автоматически появится со множеством пустых мест вместо «незаконных» слов.

Но откуда у Китая такое совершенное и эффективное оборудование для цензуры, если всего десять лет назад в стране не было ни одной крупной интернет-компании? Помогли крупные американские компании, во главе с Cisco. Для того чтобы получить часть огромного китайского рынка с более чем 100 миллионами пользователей интернет, эти компании закрыли глаза на то, для чего используются технологии. Скорее всего, некоторые из них напрямую сотрудничали с правительством, помогая установить фильтры и оборудование для контроля.

Китай поставил на колени крупнейшие мировые поисковые системы. Несколько лет назад Yahoo ! согласился убрать из китайской версии все материалы, которые режим считает оскорбительными. Google долгое время отказывался сделать это, но сейчас, похоже, движется в том же направлении.

Полиция и суды очень сурово обходятся с редакторами сайтов, которые не подчиняются правилам, установленным правящей Коммунистической партией. 75 кибер-диссидентов брошены в тюрьмы за то, что пытались размещать онлайн независимые новости. Некоторые из них осуждены более, чем на 10 лет заключения.

Поэтому, прежде чем создать блог в Китае, лучше познакомиться с правилами. Блоггеры, живущие в стране – лидере онлайновй цензуры, должны быть осторожными и изобретательными.

ВЬЕТНАМ: ОЧЕНЬ СИЛЬНАЯ КОМАНДА

Вьетнам честно следует китайскому примеру. Но, будучи более идеологически твердой, страна не обладает экономической и технологической мощью соседа. Во Вьетнаме есть кибер-полиция, которая фильтрует «подрывной» материал на веб-сайтах и шпионит в интернет-кафе. Но, как и в Китае, здесь физически уничтожают кибер-диссидентов и блоггеров. Трое уже сидят более трех лет в тюрьме за то, что отважились выступить онлайн в защиту демократии.

Президент Зине эль-Абидине бен Али

ТУНИС: ОБРАЗЦОВЫЕ ИГРОКИ

Президент Зин эль-Абидин Бен Али, семья которого является монопольным провайдером интернет-доступа в стране, создал очень эффективную систему цензуры онлайновой деятельности. Запрещен доступ к оппозиционным сайтам. Кроме того, пользователи не могут видеть многие новостные сайты, например, сайт ежедневной французской газеты Libйration. Режим также всячески старается убедить людей не пользоваться web-почтой, поскольку за этим почтовыми системами сложнее следить, чем за стандартными программами типа Outlook Express. Для того, чтобы получить доступ к почтовому

ящику на Yahoo!, в интернет-кафе в Тунисе приходится ждать до 20 минут, причем ожидание часто заканчивается получением сообщений “timed out” или “page not found”. Сайт Репортеров без границ также недоступен в стране.

Тем не менее, складывается впечатление, что международное сообщество полностью одобряет контроль интернет в Тунисе, поскольку одна из структур ООН, Международный телекоммуникационный союз (International Telecommunication Union /ITU), избрала Тунис местом проведения Международного саммита по информационному обществу, который состоялся в ноябре 2005 года. Мысль о том, что Тунис может служить образцом развития интернет, ужасает.

ИРАН: ПОЛИЦИЯ БЕЗНРАВСТВЕННОСТИ

Онлайновая цензура осуществляется не только коммунистическими режимами в Азии. В последние годы значительно улучшились системы фильтрации в Иране, и Министерство информации с гордостью сообщает, что блокирован доступ к сотням тысяч вебсайтов. Муллы, прежде всего, фильтруют контент, имеющий то или иное отношение к сексу, но они также нетерпимы к независимым новостным сайтам.
Режим использует самые жесткие методы цензуры, поставив рекорд в 2005 году, когда в течение 10 месяцев были арестованы и брошены в тюрьму 20 блоггеров. Трое из них оставались в заключении в 1 августа 2005 года.

КУБА: ЛЕГЕНДА

Кубинский режим известен умением прослушивать телефонные разговоры, но интернет здесь тоже хорошо умеют фильтровать. Китайская модель поощрения интернет-активности при усилении контроля слишком дорога, поэтому президент Фидель Кастро выбрал более простой путь – сделать интернет недоступным практически для всех кубинцев. Интернет на Кубе – это привилегия немногих, которые должны получать разрешение на доступ от правящей Коммунистической партии. Но даже если вы имеете доступ в интернет (часто незаконно), вы получаете значительно урезанную цензурой версию.


Фидель Кастро

Немногие знают, что Куба – одна из стран с мизерным количеством интернет пользователей и что интернет здесь подвергается такой же цензуре, что и

традиционные средства массовой информации. Почему люди не знают об этом? Может быть, потому, что они еще остаются под влиянием мифа о кубинской революции.


Король Абдаллах Бен Абдель Азиз аль-Сауд

САУДОВСКАЯ АРАВИЯ: РЕКОРДНЫЕ ОЧКИ

Саудовские власти открыто говорят о том, что они фильтруют интернет. Если вы пытетесь получить доступ к запрещенному сайту, вместо надписи “page not found”, вы видите сообщение о том, что этот сайт блокирован правительственными фильтрами. Официальное Управление интернет (Internet Service Unit (ISU) с гордостью расскажет о том, что блокировано 400,000 сайтов и покажет онлайновую форму, которую могут заполнить пользователи, считающие, что необходимо блокировать какой-либо еще сайт. В управлении утверждают, что фильтрация осуществляется с целью защитыь граждан от информации, оскорбляющей принципы ислама и социальные нормы. Интересно также отметить, что технологии фильтрации продала режиму американская компания Secure Computing.

УЗБЕКИСТАН: МАСТЕРА ДРИББЛИНГА

«В стране не существует цензуры интернет», - заявил в июне 2005 года узбекский министр информации. Заявление звучит очень странно, если вспомнить, что все сайты узбекской оппозиции недоступны, и онлайновым журналистам угрожают физической расправой.

Жюльен Пэйн возглавляет подразделение Свобода интернет,
в организации «Репортеры без границ»

РЕПОРТЕРЫ БЕЗ ГРАНИЦ / REPORTERS SANS FRONTIÈRES
GUIDE PRATIQUE DU BLOGGER ET DU CYBERDISSIDENT

Международный Секретариат
5, rue Geoffroy-Marie, 75009 Paris, France
Тел.: 33 1 4483-8484
Факс: 33 1 4523-1151

Website: **www.rsf.org**

Редактор: Сильви Девилетт
Контакты: Энн Мартинез-Сэз / communication@rsf.org

Дизайн и иллюстрации:
Nuit de Chine
ndc@nuitdechine.com

Перевод на русский: **e-belarus.ORG** © 2006
Контактный адрес: blogging@e-belarus.org

ISBN: 2-915536-35-X