Автор: Владимир Санин © Colta.ru ИНТЕРНЕТ И ИТ, МИР 2647 27.08.2012, 00:43 350

# Так ли страшны «черные списки»?

Проект ФЗ РФ № 89417-6 способен создать пользователям только временные неприятности, но опасаться масштабной цензуры в сети нет оснований.

Несмотря на летнее затишье, полным ходом идут консультации интернет-компаний с представителями закона — то есть Российской ассоциации электронных коммуникаций (РАЭК) с Минкомсвязью. Все участники процесса и заинтересованные лица понимают, что известный законопроект о «черных списках» не имеет ровным счетом никакого отношения ни к защите детей, ни к порнографии, ни к другим видам незаконного контента, а является инструментом политической цензуры. Не понимают этого, правда, 73% граждан России по версии ВЦИОМа, но это ничего, это им скоро объяснят — в ближайшем РОВД, а особенно невезучим — в СИЗО.

Пока же отрасль пытается как-то минимизировать свои потери. Закон предусматривает три ступени блокировки: по адресу страницы (например, http://blahblahblah.livejournal.com), по домену (livejournal.com) и по IP-адресу. Интересы провайдеров и контентных компаний тут некоторым образом расходятся — так что приходится искать компромисс. Блокировка по домену категорически не устраивает, например, Livejournal Inc. — поскольку из-за одного дневника будет заблокирован весь ЖЖ. Именно это и произошло, когда правительству Казахстана разонравился в свое время дневник Рахата Алиева. Блокировка по адресу страницы — инструмент гораздо более прицельный, но дорогой: МТС, например, придется потратить на систему фильтрации 50 миллионов долларов. Понятно, что провайдеров с такими деньгами у нас можно пересчитать по пальцам одной руки. В результате с рынка уйдут мелкие компании, что в итоге уменьшит конкуренцию, ухудшит качество услуг и — ну да, сделает интернет в России более контролируемым. Сейчас вроде бы достигнут какой-то промежуточный компромисс, смысл которого не совсем, правда, ясен.

Давайте попробуем разобраться с тем, будет ли этот закон работать и как. Что они могут нам сделать?

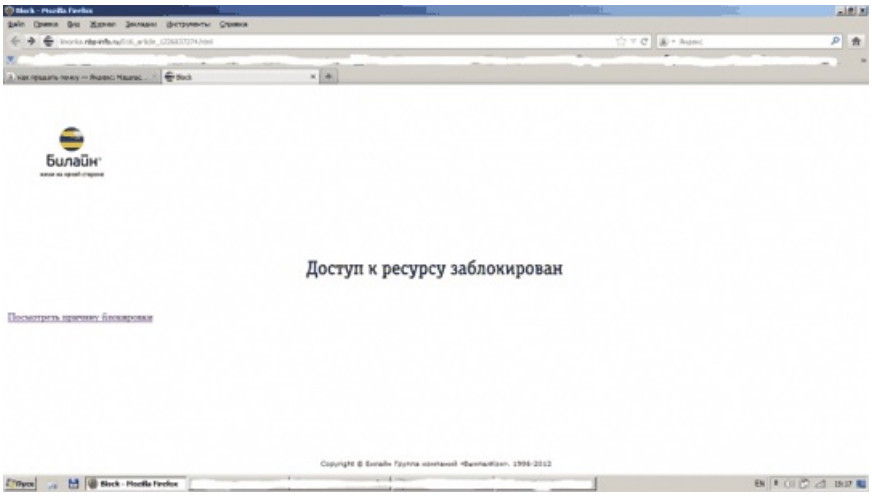
Во-первых, разделегировать доменное имя. Как это работает, мы видели в момент превращения torrents.ru в rutracker.org. Сайты просто будут уходить из зоны .ru. Это очень жаль, но ничего страшного не произойдет.

Во-вторых, возможна блокировка по IP-адресу — проще всего, дешевле всего, вреднее всего и бессмысленнее всего. Времена, когда одному сайту соответствовал один IP-адрес, давно прошли, и даже эпоха shared hosting заканчивается. Пока это самый распространенный вариант: на одном сервере, имеющем один IP-адрес, расположено множество сайтов. Стоит Роскомнадзору (или кто будет вести эти самые «черные списки») попытаться прикрыть один из них — и вы перестаете видеть все остальные сайты с того же сервера. В общем, именно поэтому контентные компании настаивают на дорогой блокировке по URL. Что произойдет, если все-таки попытки ограничения доступа по IP будут предприниматься в сколько-нибудь товарных масштабах?

Ответ: ничего.

То есть какие-то интернет-магазины и сервисы потеряют деньги за то время, пока их сайт будет недоступен, а в остальном — ничего. Владельцы сайтов перейдут на облачные сервисы — Amazon, Google или даже Microsoft. На них у сайта нет постоянного IP-адреса, а есть много — и они все время меняются. Роскомнадзор может попробовать эти изменения отслеживать в реальном времени, но это поможет только отчасти, сайт на таком хостинге все равно будет виден, хотя и с некоторыми перебоями. То есть так можно заткнуть stand-alone-страничку на собственном домене у небольшого провайдера — но сколько вам таких известно?

Теперь перейдем к блокировке по домену. При этом обычно происходит подмена DNS-записей на DNS-серверах операторов связи. Вообще система DNS преобразует доменное имя (например, blahblahblah.com) в его IP-адрес (например, 194.158.0.0) и наоборот. Запрос этот можно на уровне провайдера перехватить и дать неверный, то есть требуемый Роскомнадзором, ответ. В результате вы видите что-нибудь вот такое:




Что делать? Не пользоваться DNS-серверами провайдера, а пользоваться публичными, находящимися за пределами России, скажем, Google Public DNS. Перейти на них не просто, а очень просто, вот инструкция для Windows XP, например.

Ну и, наконец, блокировка по URL. Два базовых решения, которые следует пробовать сначала, — анонимайзеры и VPN.

Под анонимайзерами я здесь имею в виду либо анонимные прокси-серверы, либо сервисы типа Tor. Последний в смысле обхода цензуры — это, конечно, несколько overkill, из пушки по воробьям. Самая сильная сторона Tor — обеспечение анонимности, которой мы здесь не касаемся. Пользоваться им в последнее время стало уже даже не просто, а очень просто — как обычным браузером Firefox, — но скорость чрезвычайно низка. Кроме того, в принципе, Tor можно попытаться заблокировать на государственном уровне, как китайские товарищи, но получается не очень.

Анонимные прокси-серверы хорошо подходят, если вам нужно просто почитать что-нибудь, и хуже — если нужно пользоваться сервисами, многие из которых отказываются работать с такими пользователями. Никакой реальной анонимности они при этом не обеспечивают, это просто так называется. Настраивается эта штука легко, списков прокси тоже бесконечно много, вот, например, один из них.

Наконец, VPN, технология, очень просто говоря, шифрующая всю информацию, которой вы обмениваетесь с тем или иным сайтом, — это наиболее универсальный ответ на интернет-цензуру, который обойдется вам в 15—20 долларов в месяц. Можно и бесплатно, но за деньги как-то надежнее. Пользоваться русскими сервисами типа Hideme.ru в текущей ситуации нет смысла (особенно если вы озабочены анонимностью), но наличия карточки любого российского банка достаточно для того, чтобы подключиться к сервисам западным.

В общем, ответ на вопрос о том, стоит ли бояться нового закона, устроен примерно вот как. В основном — нет, не стоит, работать он не будет. Есть два способа отрезать доступ к сайту в России — перекрыть интернет целиком (это очень легко) или физически воздействовать на владельца (хотя в случае Ingushetia.ru и это не помогло). Оба весьма действенны, но мы сегодня не о политике как таковой, а об интернете. При всем том, разумеется, стоит принять определенные меры безопасности для обеспечения своей анонимности — сделать так, чтобы не был виден ваш реальный IP. О том, как это сделать, поговорим как-нибудь в следующий раз.

Автор: Владимир Санин © Colta.ru ИНТЕРНЕТ И ИТ, МИР 2647 27.08.2012, 00:43 350
URL: https://babr24.com/?ADE=108077 Bytes: 6368 / 6304 Версия для печати

Автор текста: **Владимир Санин**.

**НАПИСАТЬ ГЛАВРЕДУ:**

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

**ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:**

эл.почта: bratska.net.net@gmail.com

**КОНТАКТЫ**

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

**ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:**

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

**СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:**

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта