Вячеслав Ансимов

Интернет — хороший, плохой, злой

Не навреди! …хоть сегодня

После многолетних разговоров и споров российское государство наконец решилось активно подлечить интернет — заняться информацией, доступной гражданам в глобальной сети. Законодательно определены виды запрещенного контента, механизмы его обнаружения и блокировки. Помимо извечной критики цензуры, обозначились и вполне конкретные технические и организационные проблемы реализации новых законов. Интернет-провайдеры всех уровней напряженно смотрят вверх, пытаясь угадать, каким боком и с какой силой все это упадет на них.

«Если не знаешь как, надо у кого-нибудь спросить»

Интернет — по мнению значительной части человечества, абсолютно независимая среда, в которой возможна полная свобода и, вообще, рай земной. Да, с точки зрения получения информации глобальная сеть оказалась куда доступнее книг, библиотек, журналов и газет. Однако с точки зрения размещения информации долгое время интернет был в основном полем для профессионалов. Чтобы что-то разместить, нужно было зарегистрировать домен, разобраться, как создают сайты, и, наконец, создать его со всей своей информацией. Это явно был не самый массовый путь.

Но вот появились всевозможные ЖЖ, фейсбуки, твиттеры, вконтакты и прочие wot-приложения и wot-сервисы (от waste of time — пустая трата времени). Вся эта блогосфера и социальные сети в корне изменили ситуацию. Каждый, не особо напрягаясь, может стать сам себе газетой, журналом и телевидением. Если будет писать интересно, то станет популярным без какой бы то ни было рекламы — обычной или контекстной. Последние пару-тройку лет социальные сети в России резко пошли на подъем и к 2012 году достигли критической массы, гравитация которой уже никак не могла выпасть из сферы внимания государственной власти. Вот, собственно, и ответ на вопрос: почему именно сейчас?

Желание, если уж не «навести порядок», то хотя бы как-то влиять на интернет и раньше периодически посещало государственных чиновников и разного рода народных избранников. За долгие годы единственным реальным достижением был СОРМ. Но это лишь извлечение данных о пользователях, законный «госшпионаж», а не попытка повлиять на контент. Проблема состояла в том, что чиновникам было совершенно не ясно, как действуют эти самые «интернеты». Например, один и тот же простой вопрос, как быть с «нехорошими» сайтами, которые хостятся за рубежом, каждый раз вызывал ступор. А есть еще масса нюансов, многие из которых, не побоимся сказать, отнюдь не тривиальны.

После мучительных размышлений и неудачных попыток чиновники наконец доросли до того, чтобы обратиться к специалистам. И специалисты, готовые сотрудничать, нашлись. Причем не какие-нибудь продажные коллаборационисты, а известные и уважаемые представители элиты рунета. Сколь ни кощунственной покажется эта мысль для «казацкой вольницы», но в сети, действительно, скопилось изрядное количество откровенного безобразия. Это вполне естественно для любой среды, когда порог вхождения в нее оказывается достаточно низким.

В 2011 году без какого-либо участия государства, как бы сама собой зародилась Лига безопасного интернета — некоммерческое партнерство, имеющее целью контролировать информацию в глобальной сети. Первыми «некоммерческими партнерами» были отцы-основатели — Константин Малофеев, миллиардер и крупнейший частный совладелец «Ростелекома» (10% акций), и четыре крупных провайдера. Сейчас членами организации являются: «Ростелеком», МТС, «ВымпелКом», «МегаФон», Mail.Ru Group, «Лаборатория Касперского» и другие товарищи. Предлагали и «Яндексу», но он отказался. Как видим, даже без «Яндекса» состав подобрался нешуточный и совсем не бедный. Не будем вдаваться в их истинные мотивы, но, возможно, это упреждающая реакция крупнейших участников рынка. «Если мафию уничтожить нельзя, то ее нужно возглавить». Попечительский совет лиги возглавляет Игорь Щеголев, который до мая 2012 года был министром связи и массовых коммуникаций, а сейчас — помощник Президента РФ. В совет входят представители ФСБ, МВД, Следственного комитета, Генеральной прокуратуры, Госдумы, Совета Федерации, Московского патриархата и ведущих операторов связи.

Специалистами лиги к декабрю 2011 года был разработан и представлен законопроект, определяющий механизмы обнаружения запрещенного («опасного») контента и способы его устранения или блокировки. В рекордные сроки законопроект был рассмотрен и одобрен в Госдуме и летом был принят Федеральный закон № 139-ФЗ от 28 июля 2012 года. Впервые в рос-

сийском законодательстве в отношении интернета был применен достаточно профессиональный подход. Были даны определения сайта, интернет-страницы, доменного имени, сетевого адреса, владельца сайта и хостинг-провайдера.

Но самым шумным достижением нового закона стал, конечно, введенный им «черный список сайтов», а точнее, механизм сбора информации о ресурсах, содержащих запрещенный контент. В самой идее привлечения всех пользователей сразу же обнаружились принципиальные дыры, а также просто ее физическая неспособность охватить сколь-нибудь заметную часть рунета. Но сначала остановимся на объекте всех этих грандиозных усилий — какой, собственно, контент запрещен?

Что у нас плохого

Факт существования и роста вредоносного контента ни у кого, похоже, сомнений не вызывает. Разногласия начинаются вокруг вопросов — следует ли с этим контентом активно бороться, и если следует, то как именно. Ну и, конечно же, вместе с общепринятыми представлениями сильно разнятся мнения о границах зловредности той или иной информации.

Этот материал предназначен в первую очередь для операторов, и мы хотели абстрагироваться от споров вокруг опасности или необходимости цензуры и от классификации запретов. Однако везде, где эти вопросы хоть каким-то боком вылезают, они стремятся занять все доступное пространство. Так что затронуть их все равно придется.

Информация, запрещенная к распространению в нашей стране, определена Уголовным и Административным кодексами, Конституцией, федеральными и местными законами и прочими нормативно-правовыми актами. Существуют также разнообразные ведомственные распоряжения, юридическая сила которых, однако, сомнительна.

Итак, что это за информация? Детская порнография, наркотики (изготовление, употребление, распространение), способы самоубийства, вредоносные программы, государственная и военная тайна, оскорбления, клевета, экстремизм, изготовление бомб, ядов и прочих опасных штуковин, пропаганда войны.

Все эти, безусловно, нехорошие вещи не приветствовались и раньше. Однако решение о принадлежности информации к указанным категориям должен был принимать только суд. Более того, суд может запретить распространять все что угодно, если оно нарушает какие-либо законы. Например, недобросовестную рекламу, материалы, нарушающие авторские права, и многое другое.

Но эту руку мы протянем не всем!..

Новый федеральный закон — это попытка обойтись в ряде случаев без судебного вмешательства. Для этих особых случаев очерчена граница — это, так сказать, абсолютное зло, вызывающее минимум сомнений и трактовок. Как всегда в подобных случаях на знамя поднимается забота о детях. Собственно, закон № 139-ФЗ — это «закон о законе», то есть он вносит поправки в другой закон, «О защите детей от информации, причиняющей вред их здоровью и развитию», а также в ряд других законов в части, касающейся «ограничения доступа к противоправной информации в сети интернет».

В категорию абсолютного зла попали: детская порнография, наркотики и суициды. На сайте лиги также упоминаются садизм, принуждение и членовредительство (видео). Идеологическую, национальную и религиозную вражду из «расстрельного списка» убрали.

Что и говорить, данные категории, действительно, неприятны. Их даже можно считать особо опасными. С точки зрения здравого смысла вопрос вызывает только детская порнография. Не в смысле сомнения в ее зловредности, а в смысле присутствия именно в законе о защите детей. Ограждать детей от детской порнографии додумались только у нас. Во всех странах детское порно запрещено само по себе, то есть для всех и прежде всего для взрослых, чтобы не распространять педофилию. Но вот запретить детям смотреть детское порно — это настоящая жесть.

Убить педофила — 2

В некоторых странах запрещена даже так называемая «искусственная» детская порнография — рисованная или синтезированная на компьютере. В самых развитых странах сайты, содержащие запрещенный порноконтент, обнаруживают, но не фильтруют бездумно, а выслеживают как создателей, так и посетителей, чтобы пресечь источник, а не лечить последствия. При этом эффективно работает международное сотрудничество. Так, полиция США регулярно передает коллегам в Британии списки IP-адресов и номеров кредитных карт посетителей сайтов с детским порно. Старый контент может включаться в блокирующие фильтры, чтобы легче было обнаружить свежий и выйти на изготовителей. Российское же решение пока больше похоже на паллиатив.

Подобный подход имеет место и по другим категориям. Например, в США и Израиле контент, связанный с экстремизмом и терроризмом, интересует прежде всего службы государственной безопасности, а не цензурные подразделения.

Как особо уязвимую категорию пользователей, детей, конечно, необходимо защищать особо. В том числе от многих вещей, в принципе не запрещенных. Например, не от детской порнографии, а от порнографии вообще. От экстремального насилия, жестокости, алкоголя, курения, разнообразной агрессивной пропаганды, в том числе религиозной или, например, вегетарианской и т.п. Упомянутый закон «О защите детей» как раз на это и направлен.

Взрослого человека нельзя ограничивать в праве наслаждаться порно, любоваться зверствами, морочить себе голову сатанизмом, сайентологией или иеговыми свидетельствами. Поэтому в законе «О защите» придумали предупреждающие таблички для детей: 18+, 16+, 12+, 6+. Предполагалось, что их должны у себя вывешивать и все веб-сайты на всех веб-страничках, где есть информация «с ограничениями по возрасту». Эту явную глупость июльский «закон об изменениях и поправках» изменил и поправил, то есть упразднил для всех, кроме «сетевых изданий».

Вместе с тем, еще одна поправка в Кодекс об административных правонарушениях гласит, что доступ в интернет в «местах, доступных для детей», должен быть ограничен. Как это понимать, неясно. Какие у нас места доступны для детей? Wi-fi зоны, интернет-кафе, домашние компьютеры, мобильники, PSP?.. Поправка устанавливает административную ответственность операторов связи или местных администраций за «неприменение мер защиты» детей от вредной информации. Меры могут быть как организационные, так и технические (фильтры).

Весь мир насилья мы разрушим

Между тем еще до принятия обсуждаемого закона уже существовала такая информация, запрет которой не требовал судебного решения. Точнее, он не требовал нового судебного решения, поскольку такое решение уже было. Речь идет о пополняемом федеральном списке материалов, которые различными судами были признаны экстремистскими. Судебные решения принимаются на основе статей Уголовного и Административного кодексов, а также специального «антиэкстремистского» закона. Сюда входят разжигание разно-

го рода ненависти, призывы к насилию, терроризм, пропаганда всевозможных «крайних» взглядов, опасных для общества и жизни граждан. Особенно примечательны рекурсивные определения, то есть содержащие само определяемое слово. Например: «экстремистскими считаются материалы, пропагандирующие экстремистские взгляды».

Слово «экстремизм» есть во всех языках, а явление — во всех странах. С экстремизмом борются везде, и часто довольно жестко. Даже в демократических странах существуют запреты на некоторые книги, чего уж говорить про Россию.

«Федеральный список экстремистских материалов» введен законом «О противодействии экстремистской деятельности» № 114-ФЗ от 25 июля 2002 года. В данном законе, так же как и в УК и АК, имеется свое определение экстремизма. Список составляется Министерством юстиции и сейчас содержит более полутора тысяч материалов — книг, статей, текстов, литературных произведений, газет, журналов, фильмов, произведений изобразительного искусства и даже музыкальных произведений.

Однако не будем дальше вдаваться в политические, моральные и культурные аспекты цензурных законов. Нас прежде всего интересует техническая реализация их исполнения.

Где у него кнопка?

В оффлайне соблюдение запретов проблем не вызывает. Отследить и арестовать тираж проще простого, виноватый — вот он, сидит в офисе. С интернетом все гораздо сложнее. Хостеров найти не всегда легко, иногда очень нелегко, а если и нашли, то далеко не до всех можно добраться. Но, по крайней мере, здесь хотя бы ясно, кого искать и что с ним делать. А вот как сподвигнуть на блокировку провайдеров доступа, то бишь операторов связи?

Попытки применять в интернете закон об экстремизме, за исключением единичных случаев, ни к чему не приводили. Технические механизмы появились в законодательной базе только сейчас. Новый июльский закон № 139-ФЗ нацелен на интернет и вводит соответствующие поправки в другие законы, кодексы и нормативные акты.

Кроме списка того, чего на сайтах быть не должно, сделали еще и список самих сайтов, на которых это все-таки есть. Как уже говорилось, дали определение сайтам, страницам, провайдерам и т.д. Определили, что хостеры должны по предписанию компетентного органа убрать указанный контент, а если хостеры недосягаемы, доступ к контенту должны заблокировать операторы связи (провайдеры).

Итак, с ноября Роскомнадзор ведет реестр запрещенных сайтов с указанием соответствующих IP и/или доменных имен, и/или URL-адресов. Пополняется список вручную — в основном за счет донесений бдительных граждан на сайт реестра Zapret-info.gov.ru. Донесения рассматривают уполномоченные эксперты и выносят решение. Если контент на сайте признают запрещенным, это решение доводится до хостинг-провайдера. В течение суток хостер должен информировать владельца сайта. Еще сутки даются владельцу, чтобы убрать нехороший контент. Если владелец не слушается, то на следующие сутки хостер сам должен заблокировать запрещенное содержание. Если же и хостер не слушается, то сайт заносится в реестр и все операторы связи обязаны заблокировать доступ к нему. Если после этого запрещенный контент владелец или хостер удаляют, то по их заявке сайт убирают из реестра в течение трех дней. Таков механизм — теперь технические подробности.

Все на борьбу со всеми!

Понятно, что эксперты Роскомнадзора, сколько бы их там ни сидело, замучаются просматривать «вручную» даже мизерную долю интернета, даже только русскоязычного. На помощь призваны все сознательные граждане — этакая распределенная система контроля, вроде поиска внеземных цивилизаций в проекте SETI. Со стороны интернет-общественности сразу появилась обширная критика, сопровождаемая практическими издевательствами над «очистным госсервисом».

В первую очередь нападкам подверглась чуждая отечественному менталитету идея «стукачества». Пользователи, у которых нет ничего святого, устроили профанацию этой светлой идеи. В первые же сутки работы реестра туда поступило порядка сотни жалоб на сайт президента РФ — Kremlin.ru. Граждане сообщали, что просмотр этого сайта вызывает у них мысли о суициде или желание употребить наркотики. Некоторым показалось, что они видели там детскую порнографию (видимо, уже после употребления). Двести пользователей предложили занести в черный список сам сайт реестра Zapret-info.gov.ru. Пять тысяч заявок оказались просто спамом, видимо, с целью парализовать работу реестра. К рассмотрению были приняты лишь две сотни, а предписания об удалении были сделаны в отношении всего шести сайтов. Результатом работы реестра за неделю оказался один заблокированный сайт.

Помимо простого спама с ложными доносами, реестр можно использовать в злых целях и более эффективно. Любой недоброжелатель может, например, сам поместить в комментариях неугодного ему сайта нехороший контент и после этого пожаловаться в реестр. Фразы о том, как здорово есть наркотики и прыгать с десятого этажа, можно поместить в гостевой книге, на форуме, в комментариях любого рода и в прочих интерактивных формах. Если имеется фото с детским порно (хотя бы склеенное в фотошопе), его можно разместить в профиле или, скажем, в фотоальбоме.

В то же время в плане производительности система все равно остается ничтожной, даже с привлечением всех пользователей. Как и следовало ожидать, это занятие привлекает далеко не всех.

Как можно заметить, в механизме работы реестра для каждого этапа прописаны сроки. Всего несколько этапов с шагом в сутки. Похоже, составители закона потеряли связь с реальностью. В отечественных административных структурах действуют свои релятивистские законы, и информация не может распространяться с такой скоростью.

В отличие от скорости распространения предписаний, в вопросе направления разработчики проявили больший реализм. Они признают, что многие предписания хостерам пойдут «на деревню дедушке», ибо для установления контактных данных используется база WHOIS, достоверность которой, мягко говоря, не очень. На сайте реестра имеется «Обращение Роскомнадзора к провайдерам хостинга по вопросам оперативного взаимодействия». Их призывают самих сообщать в Роскомнадзор свои контактные данные, а также списки обслуживаемых доменных имен с диапазоном IP-адресов. Оперативное взаимодействие с хостерами должно снизить вероятность «варварской» блокировки по IP-адресу, при которой могут пострадать невинные ресурсы.

За первый месяц работы реестра произошло несколько нашумевших случаев, когда жертвами IP-блокировки стали популярные ресурсы: библиотека «Либрусек», энциклопедия «Луркморье» и торрент-портал Rutracker.org. Указанные в базе WHOIS email-адреса оказались неактуальными. Установление контактов и выполнение предписаний происходило уже после введения блокировки.

Если для хостеров хотя бы теоретически ясно, кому писать и что делать,

то в случае с операторами связи все гораздо туманнее. Контакт с ними должен быть непрерывным, так как реестр обновляется ежечасно. Здесь Роскомнадзор возлагает инициативу на самих операторов. То есть они обязаны постоянно сверяться с реестром и, соответственно, производить блокирования-разблокирования. Соответствующие формы запросов на ручную и автоматическую выгрузку реестра имеются в разделе «Операторам связи».

Согласно закону, блокировки обязаны делать все (!) операторы связи. Тем не менее главные вопросы, которые волнуют операторов: кто же все-таки должен блокировать, как и где? Фильтры должны стоять на магистралях, в точках обмена трафиком или на последней миле? И, в конце концов, что означает «все» операторы связи? То есть, если где-то какой-то пользователь вдруг получил доступ к запрещенному сайту, то виноват его конечный интернет-провайдер? В свою очередь, в том, что этот конечный провайдер имеет доступ к запрещенному сайту, виноват магистральный провайдер и т.д. Виноваты все, то есть виноватых опять не найти.

В новом законе прописана ответственность операторов связи за допуск пользователей к запрещенному контенту. Точнее, прописано, что ответственность есть, но не определено, какая именно. По ссылкам на закон «О связи» ничего об ответственности нет. Восполнить пробел пытаются сейчас. Чиновники в Роскомнадзоре мечтают ввести штрафы для хостеров и операторов связи в 100 тысяч рублей. Соответствующие поправки в КоАП обсуждаются.

Потому и надежней
На все, что сложно,
Поставить клеймо «нельзя»

Ну и, собственно, метод блокировки — вопрос принципиальный во многих аспектах. Как уже отмечалось, Роскомнадзор сам признает простую блокировку по IP методом грубым и крайним. На одном IP-адресе могут располагаться несколько разных ресурсов, доступ к которым будет разом закрыт. Однако эту «крайнюю меру» чиновники считают допустимой «в случае технической невозможности ограничения доступа по доменному имени или указателю страницы сайта».

Если бы подобное «допущение» допустили бы где-нибудь на Западе, первый же судебный иск на пару-тройку миллионов со стороны пострадавшего сайта мгновенно бы вылечил законодателей и чиновников от всех допущений, упрощений и «технических невозможностей». Даже суточный простой в заблокированном виде, например, онлайнового магазина или сетевого сервиса вполне потянул бы на весьма убедительную сумму. Но мы, слава богу, живем не в такой зашуганной стране, наш суд всегда определит правильные приоритеты.

Что же это за «техническая невозможность» вынуждает наказывать не только тех, кто виноват, но и устраивать ковровые бомбардировки окрестностей? Блокировка по точному URL позволяет изымать только страницу с запрещенным контентом, но этот метод технически заметно сложнее IP-фильтрации, которую может организовать провайдер любого уровня. Кстати, для выхода из-под IP-блокировки владельцу ресурса достаточно сменить хостинг с сохранением доменного имени.

Разделяй и властвуй

Проблему решает технология фильтрации Deep Packet Inspection (DPI) способная в реальном времени разделять потоки данных по URL-адресам и протоколам передачи. С помощью DPI можно точно блокировать не только заданные страницы, но и определенные приложения, например торрент-клиенты, трафик FTP, электронной почты, Skype и прочее. Более того, всемогущая система позволяет идентифицировать и пользователей по их IP- и MAC-адресам. Например, можно отслеживать тех, кто пытается попасть на заданную страницу.

DPI может собирать исключительно полезную развед... простите, маркетинговую информацию, может не только блокировать, но и перераспределять нагрузку, приорететы, пропускную способность канала для различных видов трафика. Если грамотно использовать открывающиеся возможности оптимизации, можно добиться ощутимой экономии ресурсов, получить конкурентные преимущества, разработать наиболее востребованные тарифы и предложения. То есть, помимо точной фильтрации запрещенного контента, DPI может еще много для чего пригодиться и даже теоретически окупить себя.

Но у этой чудо-технологии есть один маленький недостаток: программно-аппаратные модули DPI — очень недешевые штуки. И прежде чем они себя окупят, их надо на что-то купить. К тому же DPI требуется квалифицированное подключение и обслуживание.

Основные разработчики — Cisco, Huawei, Allot и другие. Есть и отечественные разработки. Цена зависит от производительности, однако даже для мелкого провайдера с небольшим по нынешним меркам трафиком стоимость, скорее всего, будет недоступной. Или же у провайдера должен быть доступ к приличным кредитам и известная доля смелости. В настоящее время комплексы DPI активно осваивают крупнейшие операторы: «Ростелеком», «ВымпелКом», МТС, «МегаФон» и некоторые другие.

Что делать мелким операторам, которым DPI не по карману? Правильно — фильтровать по IP, дешево и сердито. На данный момент эффективность фильтрации по спискам реестра составляет по регионам 40–60%. То есть половину положенных сайтов заблокировать не удается.

Робокоп.RU

В заключение вернемся к вопросу пополнения реестра, так как от него зависит успех всей затеи. Пока очевидно, что ручной общественный режим совершенно неэффективен и вреден. Альтернативой может быть автоматическая система обнаружения запрещенного контента, которая будет шерстить интернет ботами и прочими пауками на манер поисковика. В принципе, это классическая задача искусственного интеллекта — распознавание вербальных и графических образов с заданной вероятностью ложных срабатываний. Порог срабатываний можно установить такой, чтобы с выходным потоком справлялся штат специалистов-операторов.

В России есть разработчики, которым такая система по плечу. Это компания «Ашманов и партнеры» — создатель ведущих отечественных антиспамерских систем и лингвистических продуктов. Более того, руководитель Игорь Ашманов известен как сочувствующий идеям Лиги безопасного интернета по части морально-нравственной защиты детей. Чиновники и депутаты уже объявили, что компания трудится над созданием системы обнаружения и выпустит ее в 2013 году. Однако сам Ашманов в прессе заявил, что никаких заказов пока не получал. Во всяком случае такова была ситуация в декабре 2012 — на момент написания статьи.

По заявлению руководителей Лиги безопасного интернета, в системе автоматического поиска запрещенной информации будет в том числе использована база запрещенного контента, которую собрала лига. В ней содержится только детской порнографии 4 террабайта! Где удалось набрать такие поражающие воображение объемы, трудно даже представить.

Ближайшее будущее должно прояснить ситуацию.