Андрей Солдатов

контрапункт

№1 / сентябрь 2015

Укрощение интернета

18 марта 2014 года Владимир Путин произнес “Крымскую речь”. После слов об общей исторической судьбе Крыма и России он перешел к внешней угрозе:

“Некоторые западные политики уже стращают нас не только санкциями, но и перспективой обострения внутренних проблем. Хотелось бы знать, что они имеют в виду: действия некоей пятой колонны — разного рода “национал-предателей” — или рассчитывают, что смогут ухудшить социально-экономическое положение России и тем самым спровоцировать недовольство людей? Рассматриваем подобные заявления как безответственные и явно агрессивные и будем соответствующим образом на это реагировать”[1].

Несколькими днями ранее три независимых онлайн-СМИ — grani.ru, ej.ru и kasparov.ru, а также блог Алексея Навального — были заблокированы по решению Роскомнадзора “за призывы к несанкционированным массовым мероприятиям”[2], а в российском интернете уже десять дней функционировал новый сайт predatel.net — список “национал-предателей”, в который авторы включили Алексея Навального, Бориса Немцова, Сергея Пархоменко, Сергея Алексашенко, Артемия Троицкого и других известных либералов. В этот момент российский подход к интернет-цензуре принял законченную форму: сочетание административных мер по блокированию нежелательной информации — и запугивание, поддерживаемое с самого верха.

Черные списки

С ноября 2012 года действуют новые правовые нормы, фактически устанавливающие цензуру в интернете — в частности, учрежден “Реестр запрещенной информации”. В настоящее время в стране есть четыре “черных списка” запрещенных сайтов. Первый состоит из ресурсов, запрещенных за экстремизм, во втором находятся сайты, обвиненные в пропаганде детской порнографии, суицида и наркотиков, в третий включают пиратские сайты. Четвертый список появился в феврале 2014 по инициативе депутата Андрея Лугового — для блокирования на основании требований прокуратуры (то есть без судебного решения) сайтов, содержащих призывы к несанкционированным протестам. Именно в четвертый список попали сайты ej.ru, kasparov.ru, grani.ru и блог Алексея Навального.

Элементы этой системы существовали и раньше: блокировка сайтов осуществлялась с 2007 года, однако это происходило по решению судов и несистемно, так что сайты, заблокированные в одном регионе, могли быть доступны в другом[3]. В ноябре 2012 года интернет-цензура приобрела системный характер: одно ведомство — Роскомнадзор — отвечает за блокирование сайтов из “черных списков” на всей территории страны, а постоянные рейды местных прокуратур и Роскомнадзора

постепенно привели к тому, что соответствующее оборудование по фильтрации "противоправного контента" было установлено везде — от школ и университетов до библиотек.

За образец была взята система, которую использует Росфинмониторинг для блокирования банковских счетов террористов. Росфинмониторинг сводит вместе данные, полученные от Генпрокуратуры, Минюста, Следственного комитета и МИД, и составляет перечень организаций, причастных к терроризму. Перечень выкладывают на специальном сайте, доступ к которому под паролем получают все банки. Счет клиента, попавшего в "черный список", блокируется.

Сейчас Роскомнадзор, ответственный за составление Реестра, вносит интернет-ресурсы в список запрещенных сайтов на основании судебных решений, данных, полученных от МВД, ФСКН, Федеральной службы по надзору в сфере защиты прав потребителей и прокуратуры, а иногда и по жалобам возмущенных граждан (например, активистов "кибердружин" Лиги безопасного интернета). Реестр, размещенный по адресу zapret-info.gov.ru, регулярно пополняется, а провайдеры и операторы связи обязаны регулярно знакомиться с его содержанием и блокировать доступ к сайту или странице, попавшим в "черный список". За халатное отношение к блокировке провайдер может лишиться лицензии.

Запугивание или технологии?

Опыт, накопленный за три года существования российской системы фильтрации, показывает, что она оказалась технологически малоэффективной — при желании пользователь может получить доступ к заблокированным сайтам, используя не только такие средства, как TOR, но и обычный переводчик Google translate (при отправке текста в переводчик доступ к источнику идет через сайт Google, и блокировка не срабатывает, так как рассчитана на доступ с территории Российской Федерации). Однако техническая слабость системы фильтрации никогда не смущала Роскомнадзор. Весной 2013 года Максим Ксензов, заместитель руководителя этого ведомства, выступил с первыми итогами внедрения интернет-фильтрации. Он признал, что "для квалифицированных пользователей в большинстве случаев остается возможным обход блокирования"[4], но тут же добавил, что это не так уж и важно, так как "пользовательская база, которая будет использовать защищенные туннели и/или специальное программное обеспечение для обхода блокирования, в настоящее время может считаться незначительной".

Действительно, число пользователей, стремящихся обойти цензуру, оказалось невелико. Это сразу почувствовали журналисты заблокированных сайтов — их аудитория уменьшилась почти в два раза. Кроме того, выяснилось, что, в отличие от тройки политических сайтов[5], владельцы других заблокированных ресурсов (число которых даже по официальным данным уже достигло нескольких тысяч) не готовы бороться за свои права. Об этом с видимым удовлетворением говорил в тот же день начальник Ксензова — руководитель Роскомнадзора Александр Жаров: "Среди тысяч владельцев этих ресурсов нашлись единицы тех, кто публично говорил о несогласии. И зафиксирован всего один случай обращения в суд"[6].

И добавил, что поддержку закону "О реестре запрещенной информации" выразили 82% российских граждан.

При этом, в отличие, например, от Китая, где для осуществления политической цензуры в интернете была создана многотысячная армия интернет-цензоров, Роскомнадзор остается сравнительно небольшим ведомством, в котором интернетом занимаются лишь несколько десятков человек. У Роскомнадзора есть "добровольные помощники", которые выискивают в интернете проявления неблагонадежности. Этой работой заняты две организации — Лига безопасного интернета и "МедиаГвардия" (проект "Молодой Гвардии" "Единой России"), однако деятельность этих активистов не слишком эффективна. Согласно годовому отчету Лиги безопасного интернета за 2014 год, у Лиги есть 20 тысяч "кибердружинников" в России, а также в СНГ, Восточной и Западной Европе (данную цифру

невозможно проверить с помощью независимых источников), однако в основном они ищут сайты, предлагающие интим-услуги и проч.[7]

Из двух организаций упор на политический сыск скорее есть у "МедиаГвардии". По ее собственному утверждению, "МедиаГвардия" располагает 3926 активистами, которым удалось за все время существования проекта закрыть 2475 сайтов — немного, если учесть, что проект был запущен еще в феврале 2013 года. Для сравнения: только у grani.ru Роскомнадзор к лету 2015 года заблокировал 500 зеркал, каждое из которых считается отдельным ресурсом. По данным Роскомсвободы (проекта Пиратской партии, выступающей за полную свободу в интернете), всего за время существования Реестра запрещенных сайтов в России было заблокировано 677 693 ресурсов (на момент написания статьи)[8].

Но несмотря на техническое несовершенство, главная задача государственной цензуры решается успешно: пространство свободного высказывания в интернете неуклонно сокращается.

Дело в том, что эффективнее формальных правовых актов, административного блокирования и "черных списков" оказываются неформальные методы: запугивание и прямые (но непрозрачные) переговоры с крупнейшими интернет-корпорациями.

Первыми на эту мысль Кремль навели сами интернет-гиганты: осенью 2012 года, испуганные тем, насколько технологически грубо в законе "О реестре запрещенной информации" прописана процедура блокирования сайтов, крупные интернет-компании для защиты своих интересов обратились не к общественности, не в суд, а туда, где в России принимаются все важнейшие решения — непосредственно к верховной власти.

Закон предполагал блокировать сайты по IP-адресу, а, учитывая, что на одном IP-адресе могут находиться десятки и сотни разных сайтов, это могло привести к блокированию интернет-сервисов целиком. Именно это произошло с YouTube, когда вспыхнул скандал вокруг фильма "Невинность мусульман", который многие посчитали оскорбительным для верующих. Роскомнадзор быстро отреагировал, и прокуратуры многих регионов потребовали от провайдеров заблокировать доступ к фильму. Три крупнейших оператора связи — МТС, "Вымпелком" и "Мегафон" — ограничили доступ к опальному видео. При этом "Вымпелком" заблокировал доступ к YouTube, где размещался ролик, целиком на территории Чечни, Дагестана, Карачаево-Черкесии, Северной Осетии и Ставропольского края. МТС и "Мегафон" проявили бóльшую гибкость и заблокировали доступ только к самому ролику. Возникший скандал и побудил руководителей крупнейших интернет-компаний обратиться в администрацию президента.

На первом же совещании заместитель руководителя Администрации Вячеслав Володин дал понять, что сама политика интернет-цензуры не обсуждается, и предложил вместо этого поговорить о технологии блокирования. Компании с этим подходом согласились. Таким образом — с поразительной легкостью — оказалась перейдена грань между свободным и цензурируемым интернетом, что значительно облегчило Кремлю дальнейшее наступление. В результате властям удалось переложить на бизнес не только затраты на разработку технологического решения, но и расходы на фильтрацию (оборудование по блокированию российские операторы должны покупать за свой счет).

В переговорах с властями позиция ведущих деятелей интернет-бизнеса — как российских компаний, так и представителей международных корпораций (Google и Twitter) — изначально была крайне слабой, поэтому не удивительно, что, начиная с осени 2012 года, в ходе встреч с государственными ведомствами, от рабочей группы в администрации президента до совещаний в Минсвязи и Роскомнадзоре, они постоянно отступали перед напором все новых законодательных инициатив, сокращающих свободу в Рунете — включая постоянное расширение поводов, по которым сайты могут оказаться заблокированы.

Поток всё новых и новых мер ужесточения контроля сам по себе создает в Рунете ощущение постоянной угрозы: существование в режиме "взбесившегося принтера" заставляет представителей интернет-бизнеса

вести себя осторожнее, заниматься самоцензурой и постоянно бегать на консультации в Кремль. Другое дело, что непонятно, как долго государство сможет выдерживать такой темп — набор возможных инициатив все-таки ограничен.

Роль Путина в “укрощении” Рунета

Преимущества и недостатки непрозрачного процесса переговоров власти и интернет-бизнеса стали очевидны 10 июня 2014 года, когда с лидерами этой сферы предпринимательства встретился Владимир Путин. Это была вторая встреча Путина с интернетчиками за 15 лет. В предыдущий раз он встречался с Рунетом в декабре 1999 года; за прошедшие годы интернет-бизнес вырос до серьезных масштабов и превратился в отрасль, в которой трудятся 1,3 миллиона айтишников. Рунет — это 8,5 процента ВВП, рынки, так или иначе вовлечённые в интернет-бизнес, — это свыше 5 триллионов рублей, а интернет-торговля — это уже 2,5 процента от всей торговли[9].

За этот период Россия вошла в число очень немногих стран, где местный интернет-бизнес способен удерживать лидирующие позиции, не уступая поле глобальным платформам, и не нуждается ни в каких формах государственного протекционизма.

Этот успех был достигнут в немалой степени благодаря выработке правил игры, главным среди которых было признание Кремлем роли общественных организаций Рунета. На упомянутой выше встрече в конце декабря 1999 года в Доме правительства они получили, с согласия Путина, право проводить предварительную экспертизу всех законопроектов, касающихся интернета. В 2000-е годы это правило соблюдалось, и интернетчики могли обсуждать идеи законотворцев на собственных площадках, включая РОЦИТ (Региональный общественный центр интернет-технологий), созданный в 1996 году для защиты прав пользователей Сети. То совещание Владимира Путина, тогда еще премьера, с интернетчиками было единственным разговором Путина с Рунетом в таком формате, и новую встречу ожидали с большим нетерпением.

Путин многие годы не проявлял интереса к интернету, но весной 2014 года он сделал несколько ключевых заявлений о глобальной сети — назвал интернет изобретением ЦРУ, атаковал Yandex[10]. Результатом стало падение курса акций самого Yandex’a, а заодно Mail.ru и Qiwi на NASDAQ. Эти заявления, прозвучавшие на фоне непрекращающегося потока репрессивных законодательных инициатив, вызвали панику в интернет-сообществе. В Москву стали приезжать американские портфельные инвесторы, встревоженные перспективами российского интернет-бизнеса.

После этого крупнейшие интернет-компании страны получили приглашение на встречу с президентом, на этот раз уже не в правительственном здании, а в одном из бизнес-центров Москвы.

До приезда Путина руководители компаний совещались на открытой сессии, обсуждая будущее российского интернета. Однако Аркадий Волож (Yandex), Дмитрий Гришин (Mail.Ru Group), Андрей Чеглаков (Ростелеком), Герман Клименко (Liveinternet), Николай Молибог (РБК), Сергей Фаге (Ostrovok.ru), Маэль Гаве (Ozon), Александр Мамут (Rambler & Co), Оскар Хартманн (KupiVIP.ru) и Борис Добродеев (ВКонтакте) избегали разговора о пагубных последствиях госрегулирования для Рунета в его нынешнем виде. “Блогерский” закон, который требует регистрации от блогеров с тремя тысячами и более последователей, был упомянут только единожды, новым лицом “ВКонтакте” г-ном Добродеевым-младшим, который нашел в этом повод для гордости за индустрию: в VK, сообщил он, имеется около 80 тыс. групп с более чем тремя тысячами последователей, что едва ли не больше, чем число интернет-сми в стране. Имя Владимира Путина и его жесткие высказывания в адрес интернета не были упомянуты никем из участников разговора.

В конце концов, когда Путин прибыл в бизнес-центр, стало ясно, что он согласился на эту встречу совсем не ради серьезного разговора с лидерами рынка. Встреча была организована Фондом развития интернет-инициатив, созданным Агентством стратегических инициатив (само Агентство было учреждено Путиным в бытность премьером с тем, чтобы

оно стало конкурентом Сколково в области инноваций), и фонд использовал признанных лидеров отрасли, включая Yandex и Mail.ru, чтобы на их фоне представить президенту собственные стартапы. Видимо, это и была главная тактическая задача встречи. Кстати, успешно выполненная: директор фонда Кирилл Варламов, бывший инженер "Уралмаша", выдвиженец "Общероссийского народного фронта" и доверенное лицо Путина на выборах 2012 года, сидел на встрече по правую руку от Путина, в то время как Аркадию Воложу из Yandex досталось кресло слева. Финансируемые государством симулякры оказались легитимизированы присутствием настоящих лидеров рынка.

Дмитрий Гришин был единственным, кто поднял вопрос о регулировании Рунета, но тон его выступления отчетливо отразил изменившиеся к лету 2014 года отношения между интернет-бизнесом и Кремлем:

"Мы не "отмороженные", мы на самом деле любим свою страну; мы хотим, чтобы здесь было комфортно жить и работать, и чтобы в интернете тоже было комфортно существовать. И мы понимаем, что интернет стал, в принципе, большим, он вырос и что это сейчас неотъемлемая часть всего общества. Поэтому в принципе регулирование, оно необходимо.

И, если посмотреть, очень часто идеи, заложенные в регулировании, они очень правильные. Но, к сожалению, иногда бывает, что реализация, в общем, пугает. И очень бы хотелось разработать, может быть, какой-то системный процесс, позволяющий нас не только слушать, но и услышать, и чтобы мы на деле увидели, что есть обратная связь, которую можно реализовывать. Это было бы очень и очень важно"[11].

Ведущие представители отрасли, даже получив возможность непосредственно обратиться к Путину, не решились выступить в свою защиту. Что бы ни говорилось в кулуарах, фонд Варламова оказался единственным бенефициаром непосредственного общения с президентом — Путин ясно дал понять, что для него лицом Рунета будут не самостоятельные игроки, создавшие современные конкурентоспособные компании, а созданные под покровительством государства проекты Фонда развития интернет-инициатив.

Год спустя, весной 2015 года, Путин снова принимал интернет-предпринимателей, на сей раз в президентской резиденции в Ново-Огарево. Зал был заполнен исключительно представителями стартапов, поддержанных Фондом развития интернет-инициатив Варламова[12]. На этой встрече было объявлено об учреждении новой платформы для диалога между Кремлем и интернет-бизнесом: ею стал Институт развития интернета, призванный заменить общественные структуры, которые были созданы настоящими лидерами интернет-бизнеса в 1990-е.

Те общественные организации, которые служили площадками для обсуждения законодательных инициатив в рамках договоренностей с Путиным, достигнутых в декабре 1999 года, к тому времени уже были поставлены под государственный контроль. В декабре 2014 года РОЦИТ, находившийся в последние годы в явном кризисе, был срочно реанимирован; председателем правления в нем стал глава комитета по информационной политике, информационным технологиям и связи Госдумы Леонид Левин — профессиональный пиарщик, не имевший непосредственного опыта работы в интернет-бизнесе.

В правление Института развития интернета вошли как Варламов, так и директор РОЦИТ Сергей Гребенников, а на сайте института прямо говорится, что идея его создания "поддержана Администрацией Президента РФ в лице В.В.Володина"[13].

Интересы спецслужб

Многие законодательные инициативы, выдвинутые под предлогом борьбы с незаконным контентом или защиты персональных данных российских граждан, часто определяются интересами спецслужб. Российская особенность интернет-цензуры в том, что она напрямую связана с электронной слежкой. Эта связь между интернет-цензурой и слежкой была заметна уже летом 2012 года, когда

обсуждался закон “О реестре запрещенной информации”.

Тогда интернет-компании поспешили в Кремль, чтобы обсудить, какие именно механизмы блокировки будет использовать государство, и выступили единым фронтом против блокировки по IP-адресу, поскольку, как говорилось выше, она ставила под удар целые сервисы из-за одного ролика или поста. Однако единственной альтернативой такого грубого метода является технология DPI (Deep Packet Inspection, или глубокого чтения пакетов), которая позволяет блокировать отдельную страницу на любом интернет-сервисе — от YouTube до социальной сети. Хотя DPI не упоминается в законодательстве о фильтрации, Министерство связи и массовых коммуникаций, а также представители крупнейших интернет-корпораций решили, что именно эта технология лучше всего подходит для фильтрации интернета.

По словам депутата Госдумы Ильи Пономарева[14], в конце августа под председательством министра связи Николая Никифорова прошла рабочая группа, в которой участвовали представители Google и ведущих участников интернет-рынка. На примере YouTube они обсуждали, как сделать механизм, который позволил бы заблокировать конкретный ролик, а не YouTube целиком. “Они договорились о механизме, который всех устроил”, — утверждал Пономарев, сторонник поправок и реестра, уточняя, что речь шла именно о DPI.

Большая часть технологий, анализирующих интернет-трафик, способна видеть только заголовки передаваемой через сеть информации, а также точку отправки данных и конечный пункт назначения. Технология DPI позволяет провайдеру заглянуть внутрь пакетов информации; она дает возможность не только вести мониторинг трафика, но и фильтровать его, “зажимая” определенный сервис или блокируя контент.

Как заметил в разговоре с автором Эрик Кинг, глава исследовательского направления в Privacy International, DPI позволяет государству влезть в интернет-трафик каждого, а также читать, копировать и даже модифицировать его письма и просмотренные страницы. “Мы знаем сейчас, — сказал Кинг, — что такие технологии использовались в Тунисе до революции”.

Уже в сентябре 2012 года стало ясно, что возможности DPI по идентификации можно без труда совместить с системой СОРМ, национальной системой прослушки.

СОРМ (Система оперативно-розыскных мероприятий) была разработана в недрах КГБ в конце 80-х и с тех пор постоянно обновлялась. В результате сегодня СОРМ-1 отвечает за прослушку телефонных линий, включая мобильную связь, СОРМ-2 перехватывает интернет-трафик, а СОРМ-3 должен обеспечивать сбор информации со всех видов связи, ее долгосрочное хранение и доступ ко всем данным об абонентах. Главная особенность системы — отсутствие какого бы то ни было контроля — осталась во всех версиях СОРМ. И это объясняется технологическим отличием российского стандарта СОРМ от европейского ETSI и американского CALEA.

В США и Европе правоохранительный орган получает в суде ордер на прослушку конкретного лица и пересылает его оператору, который снимает информацию и отправляет ее спецслужбе. В России офицер ФСБ тоже должен получить разрешение у судьи, но не обязан показывать его никому, кроме своего начальства. Операторы не имеют права знать, чьи переговоры или почту перехватывает спецслужба. Поэтому технически система устроена по-другому: в распоряжении ФСБ есть ПУ (пункты управления) СОРМ, которые соединены по защищенному кабелю с серверами оператора. Чтобы поставить кого-то на прослушку, сотруднику спецслужбы достаточно ввести команды на ПУ СОРМ, который находится в здании местного управления ФСБ. Эта система копируется по всей стране, и в каждом областном центре местное УФСБ соединяется кабелями со всеми региональными операторами. Система устроена таким образом, поскольку она была разработана в КГБ СССР, и в те времена, разумеется, никто не думал ни о каком контроле за прослушкой. После распада СССР добавилось требование получать судебный ордер, но технически систему менять не стали, и поэтому не предполагается показывать судебный ордер кому бы то ни было за пределами спецслужбы.

Осенью 2012 года в Москве на крупнейшей конференции по информационной безопасности InfoSecurity прошла дискуссия “СОРМ в условиях конвергенции”. В таких мероприятиях обычно принимают участие только профессионалы, и зал был заполнен начальниками отделов СОРМ операторов связи и представителями компаний-производителей спецтехники. Тема DPI сразу стала одной из главных в дискуссиях. Многие были уверены, что это единственный способ обеспечения функций СОРМ в новых “условиях конвергенции” — в эпоху облачных вычислений и многообразия телекоммуникационных сервисов. Идея совмещения СОРМ с находящимся в распоряжении операторов оборудованием DPI, казалось, никого не смутила, хотя профессионалы не могут не знать, что совмещение двух “ящиков” на тот момент было незаконно.

Окончательно две технологии, СОРМ и DPI, совместились в апреле 2015 года, когда в России стала действовать новая, обновленная система СОРМ в интернете. Эта новая версия СОРМ была внедрена по приказу Минсвязи №63, подписанному в апреле 2014 года, несмотря на протесты операторов[15]. Приказ требует установки оборудования, которое способно перехватывать информацию на таких сервисах, как: “электронный почтовый адрес сервисов Web-mail, в том числе mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com, aport.ru, rupochta.ru, hotbox.ru”[16].

Впервые российские спецслужбы получили возможность не только следить за определенными гражданами, но с помощью совмещенных функций СОРМ и DPI выявлять и идентифицировать в общем потоке данных тех, кто обсуждает в интернете определенные темы или заходит на определенные страницы на сайтах и в социальных сетях. Это делает российскую систему намного ближе к идее массовой слежки, чем еще год назад.

Впрочем, новые технологии слежки внедряются не только вместе с фильтрацией. Антиблогерский закон 2014 года, кроме регистрации блогеров, также требует от компаний, представляющих площадки для блогеров (в законе они названы “Организаторами распространения информации в сети «Интернет»”) *“хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети “Интернет” и информацию об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий, а также предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации…”*[17]

Это означает, что блогосервисы и социальные сети должны обеспечить российским спецслужбам круглосуточный доступ к метаданным своих пользователей. Пока спецслужбы получали новые полномочия, другие государственные ведомства в массовом порядке закупали системы мониторинга социальных сетей. Автором одного из самых громких проектов такого рода стала очередная окологосударственная структура, маскирующаяся под общественную: Фонд развития гражданского общества, возглавляемый экс-главой управления внутренней политики администрации президента Константином Костиным. Фонд намерен заняться исследованием новых медиа с помощью технологий американской компании Crimson Hexagon. Анонсируя этот проект в июле 2013 года, Костин заявил: “мы написали систему, которая будет анализировать происходящее в российских социальных медиа и не только политику”[18].

Хотя возможности контроля со стороны спецслужб за последние годы существенно расширились, российский подход к интернет-цензуре — по крайней мере, пока — обходится без массовых арестов блогеров или журналистов за опубликованные посты. Ситуация в России кажется гораздо мягче, чем, например, в Турции, где за профессиональную деятельность за решеткой сидят десятки журналистов. (Любопытно, что, несмотря на это, уровень свободы слова в Турции оценивается выше, чем в России[19]). Похоже, что российская система контроля интернета, чтобы быть эффективной, не нуждается в массовых репрессиях против блогеров и журналистов.

Следующий шаг

Есть три направления, от результативности которых сегодня зависит, по какому пути пойдет дальнейшее наступление на свободу в Рунете.

Первое — это давление на глобальные платформы, такие как Google, Facebook и Twitter, чтобы заставить их перенести серверы с персональными данными россиян на территорию России. Первые попытки подобного рода были предприняты незадолго до прилета Эдварда Сноудена в Москву, и, продвигая закон о переносе серверов, одобренный летом 2014 года, российские законодатели ссылались именно на разоблачения Сноудена[20]. Закон установил срок переноса серверов на сентябрь 2015 года. Эта история является очередным примером российского подхода по укрощению Рунета, в котором давление на компании и запугивание сочетаются с расширением технических и административных возможностей для спецслужб. Переговоры о переносе серверов идут за закрытыми дверями в Кремле; за последний год все крупнейшие глобальные сервисы неоднократно направляли своих представителей в Москву на переговоры. Судя по всему, давление оказывается эффективным. PayPal перенес свои сервера в Россию в феврале 2015 года[21]. В апреле на одном из совещаний в Минсвязи сотрудники Ростелекома доложили, что Google перенес сервера на их мощности[22]. А в июне переносить свои сервера в Россию стала корпорация Samsung[23]. Разумеется, все участники переговоров прекрасно понимают, что перенос серверов делает информацию на этих серверах доступными для российских спецслужб.

Второе направление — это борьба со средствами обхода интернет-цензуры, такими как виртуальные частные сети (VPN) и TOR. В России с осени 2013 года наблюдается взрывной рост пользователей TOR, и власти вполне отдают себе в этом отчет. Чиновники разного уровня, законодатели и активные лоялисты неоднократно заявляли о необходимости запрета подобных средств и, казалось бы, именно это может стать новым направлением для внесения дополнительных ограничений в законодательство и новым фронтом для наступления Роскомнадзора. Проблема, однако, заключается в том, что обычного законодательного запрета в этом случае будет мало. Требуется высокоэффективное технологическое решение. Кроме того, такой неотъемлемый элемент российского подхода к интернет-цензуре, как давление на компании, здесь не работает: офиса TOR в России нет, а шантажировать авторов TOR закрытием российского рынка невозможно, поскольку это некоммерческий продукт, специально созданный для работы в странах с репрессивными режимами. С другой стороны, давление на российских операторов и провайдеров, чтобы те за свой счет блокировали TOR, также не выглядит перспективным — такие технологии не доступны на рынке, и у провайдеров их просто нет.

Наконец, третье направление — это инфраструктурные изменения. Российский интернет, несмотря на 25-летнюю историю, все еще крайне централизован и географически уязвим. Россия связана с всемирной сетью на Западе через оптоволоконные кабели, в основном проложенные через Санкт-Петербург в Хельсинки и Стокгольм (лишь недавно добавилось направление на Франкфурт), и львиная доля этих кабелей принадлежит Ростелекому, национальному оператору, работающему под контролем государства. Кроме того, у России с ее огромной территорией относительно мало точек международного обмена интернет-трафиком (Internet exchange points) — всего около десятка (для сравнения, в США их 85). Крупнейшая и старейшая из них, MSK-9, находится в Москве, в помещении международной телефонной станции M9, которая, в свою очередь, также принадлежит Ростелекому.

Все это периодически заставляет российских чиновников задумываться о том, чтобы создать в России замкнутую инфраструктуру интернета, которую в “час икс” можно отключить от внешнего мира, сохранив работоспособность системы внутри страны. В сентябре 2014 года эта проблема обсуждалась на заседании Совета безопасности[24].

Весной 2015 года данная тема вновь актуализировалась — по сведениям газеты “Коммерсантъ”, Минкомсвязи готово предло-

жить правительству повысить устойчивость инфраструктуры Рунета путем создания отечественного реестра IP-адресов, а также системы мониторинга маршрутов трафика, необходимого для автономной работы сети[25].

Данное направление также предусматривает фактическую национализацию управления российским сегментом интернета: чиновники настойчиво говорят о возможной передаче функций управления российским доменом.ru от Координационного центра национального домена сети интернет (этот центр — неправительственная организация — был также создан в рамках договоренностей, достигнутых на встрече с Путиным в декабре 1999 года) какому-нибудь правительственному департаменту. Если это произойдет, управление важнейшими функциями Рунета окончательно перейдет к государству.

Однако даже если события будут развиваться по наихудшему сценарию, то есть глобальные сервисы перенесут свои серверы в Россию, почтовые службы и соцсети, такие как Gmail, Facebook и Twitter, станут прозрачными для российских спецслужб, их контент будет мгновенно блокироваться Роскомнадзором, а российские власти получат в свое распоряжение "рубильник", который позволит отключить Рунет от внешнего мира, это вряд ли поможет властям воспрепятствовать мобилизации недовольных через интернет, если в обществе — в условиях того или иного кризиса — возникнет такая потребность.

Российские спецслужбы, как и их предшественник КГБ, разрабатывали свой инструментарий по охране политического режима в расчете на борьбу с немногочисленными диссидентами и недовольными. Сегодня они могут блокировать контент, который создается активистами или журналистами, но не способны остановить поток информации, создаваемый тысячами пользователей — например, свидетелями какой-нибудь катастрофы. Как показали московские протесты 2011-2012 года, создание такого контента происходит лавинообразно и совершенно независимо от "козней Запада" и действий любых других иностранных государств.

Кроме того, Кремль постоянно совершает ошибку, пытаясь взаимодействовать с социальными сетями как с традиционными медиа. Примером является операция по смене собственника сети "ВКонтакте". Словно повторяя сценарий отъема компании "Медиа-Мост" у Владимира Гусинского в самом начале 2000-х, основатель "ВКонтакте" Павел Дуров был выдавлен сначала из руководства компании, а потом из страны, и заменен на Бориса Добродеева, сына руководителя ВГТРК. Кремль — ошибочно — посчитал, что если компания поставлена под контроль, то и сеть находится под контролем. Однако когда начался конфликт на Украине, информация о российских солдатах в зоне боев стала доступна именно благодаря "ВКонтакте", так как российские военнослужащие сообщали о том, где именно они несут службу, размещая свои фотографии в соцсети. В этом случае кто именно сидел в кресле руководителя компании — Дуров или Добродеев-младший — не имело значения: никто в компании не имел власти над контентом, генерируемым пользователями. Единственным доступным для Кремля решением в случае масштабного кризиса остается blackout, полное отключение Сети, что вряд ли всерьез рассматривается даже самыми радикально настроенными чиновниками Кремля.

***

В отличие от стран Центральной Азии и Китая, в России на протяжении первых двадцати лет своего существования интернет развивался как свободное пространство. Наступление на свободу в интернете началось лишь летом 2012 года, когда Рунет уже обладал своими ключевыми характеристиками: его инфраструктура построена на западных технологиях, функция фильтрации и блокировок не была заложена в него изначально. Кроме того, Рунет не рос внутри "великого файрволла", и армия государственных цензоров не следила за каждым шагом местных пользователей глобальной Сети.

Природа Рунета стала важнейшим вызовом для Кремля, когда летом 2012 года российские власти начали устанавливать контроль над этим информационным пространством.

Именно поэтому стратегия контроля, из-

бранная Кремлем, сильно отличается от тех методов, которые применяются, например, в Китае.

Ключевой элемент российского подхода — непрерывный поток репрессивных, крайне широко сформулированных инициатив, что заставляет компании-субъекты российского права спешить в Кремль и профильные ведомства за разъяснениями.

Технологии (как фильтрации, так и электронной слежки) играют в этой схеме подчиненную роль — их задача быть тем средством устрашения, которое призвано обеспечить лояльность как интернет-компаний, так и рядовых пользователей Рунета. Парадоксальным образом несовершенство механизмов фильтрации лишь усилило эффект от их внедрения: опасаясь полного блокирования своих сервисов, интернет-компании согласились на диалог с Кремлем и стали предлагать собственные технические решения, брать на себя затраты на их разработку и использование.

Запугивание является главным элементом этого подхода. Частично он оказался эффективным — как российские интернет-компании, так и глобальные интернет-корпорации удивительно легко перешли от работы в свободном интернете к существованию в цензурируемом пространстве, сосредоточившись на технических аспектах новой реальности. За те три года, что продолжается активное наступление на интернет-свободы, крупные компании лишь раз выступили с публичным протестом: в октябре 2013 года один из крупнейших телекоммуникационных операторов страны “Вымпелком” отправил в Минсвязи письмо с критикой проекта приказа, в котором устанавливались новые требования к системе легального перехвата интернет-трафика. В письме “Вымпелком” утверждал, что некоторые положения приказа противоречат Конституции, которая охраняет право граждан на тайну переписки, а также накладывает дополнительные расходы на операторов — требуя закупки дорогостоящего оборудования[26]. Еще несколько компаний поддержали протест “Вымпелкома”. Однако, несмотря на возмущение компаний, в апреле 2014 года приказ был подписан. Документ вступил в силу с апреля 2015-го, и именно он окончательно совместил функции двух технологий слежки — СОРМ и DPI[27].

Однако запугивание лучше всего работает, когда действует адресно, и Кремль добился куда больших успехов в укрощении руководства интернет-компаний, чем их пользователей. История с “украинскими” постами солдат в сети ВКонтакте показала, что там, где контент зависит от пользователей, действующих в условиях кризиса, российский подход оказался не эффективным.

Примечания

1 *Обращение Президента Российской Федерации. Выступление перед депутатами Государственной Думы, членами Совета Федерации, руководителями регионов России и представителями гражданского общества//* 2014. 18 марта. URL: http://kremlin.ru/events/president/transcripts/20603 (доступ 21.08.2015)

2 *Ограничен доступ к ряду интернет-ресурсов, распространявших призывы к несанкционированным массовым мероприятиям//* Роскомнадзор. 2014. 13 марта. URL: http://rkn.gov.ru/news/rsoc/news24447.htm?print=1 (доступ 21.08.2015)

3 В этот период блокировались сайты, на которых были опубликованы статьи и книги из списка текстов, запрещенных судами за экстремизм. См. ““*Экстремистские ресурсы” в Едином реестре запрещенных сайтов*” на сайте Центра СОВА. URL: http://www.sova-center.ru/misuse/docs/2014/08/d30056/ (доступ 21.08.2015)

4 *Материалы к выступлению заместителя руководителя Роскомнадзора Максима Ксензова на расширенном заседании коллегии Роскомнадзора 14 мая 2013 года в части, касающейся анализа существующих методов управления доступом к интернет-ресурсам и рекомендаций по их применению//* Роскомнадзор. 2013. 15 мая. URL: http://rkn.gov.ru/press/developments/speech/news19960.htm

5 *Попытки владельцев обжаловать решения о блокировке сайтов оказались безуспешны//* Ведомости. 2015. 10 марта. URl: http://www.vedomosti.ru/newspaper/articles/2015/03/10/blokirovka-bez-granits (доступ 21.08.2015)

6 *Выступление руководителя Роскомнадзора А.А. Жарова на расширенном заседании коллегии Роскомнадзора//* 2013. 14 мая. URL: http://rkn.gov.ru/press/developments/speech/news19962.htm (доступ 21.08.2015)

7 *Отчет Лиги безопасного интернета за 2014 год//* URL: http://www.ligainternet.ru/upload/docs/2014-LigaInternet.pdf (доступ 21.08.2015)

8 *Статистика блокировок//* Rublacklist.net. Роскомсвобода. URL: http://reestr.rublacklist.net/visual (доступ 21.08. 2015)

9 *Форум "Интернет-предпринимательство в России". Стенограмма//* Президент России. 2104. 10 июня. URL: http://kremlin.ru/events/president/transcripts/45886 (доступ 21.08.2015)

10 *Медиафорум независимых региональных и местных СМИ//* 2014. 24 апреля. URL: http://kremlin.ru/events/president/transcripts/20858 (доступ 21.08.2015)

11 Цит. по *Форум "Интернет-предпринимательство в России"*

12 Встреча с интернет-предпринимателями. Стенограмма// Президент России. 2015. 27 марта. URL: http://kremlin.ru/events/president/transcripts/49019 (доступ 21.08.2015)

13 Институт развития интернета (ИРИ). URL: http://xn — h1aax.xn — p1ai/about/(доступ 21.08.2015)

14 Личная беседа с автором статьи в 2012 году.

15 Приказ Минкомсвязи России *"Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий"//* Минкомсвязь России. 2014. 16 апреля. URL: http://www.minsvyaz.ru/ru/documents/4249/#tdocumentcontent (доступ 21.08.2015)

16 Там же

17 Федеральный закон Российской Федерации от 5 мая 2014 года N 97-ФЗ *"О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей"//* Российская газета. 2014. 6 мая. URL: http://www.rg.ru/2014/05/07/informtech-dok.html (доступ 21.08,2015)

18 Экс-глава Управления внутренней политики Кремля Константин Костин: Навальному опасно идти на выборы. Карьера Немцова закончилась на выборах мэра Сочи// Телеканал "Дождь". 2013. 1 июля. URL: http://tvrain.ru/teleshow/govorite_s_yuliey_taratutoy/eks_glava_upravlenija_vnutrennej_politiki_kremlja_konstantin_kostin_navalnomu_opasno_idti_na_vybory_karera_nemtsova_zakonchilas_na_vyborah_mera_sochi-346962/ (доступ 21.08.2015)

19 Так, например, Freedom House оценивает ситуацию со свободой прессы в Турции как "частично свободную", а в России как "несвободную". См. 2015. Freedom in the world// Freedom House. URL: https://freedomhouse.org/report-types/freedom-world#.Vda9hCztmkp (доступ 21.08.2015)

20 Хранить персональные данные россиян в России требует принятый в июле 2014 года закон №242-ФЗ *"О внесении изменений в отдельные законодательные акты РФ в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях"* (известен как "закон о персональных данных"). Он устанавливает срок переноса серверов с данными на сентябрь 2015 года.

21 *PayPal перенес серверы в Россию, чтобы хранить персональные данные//* ITReviewer.ru, 2015, 13 февраля. URL: http://itreviewer.ru/news/26703/paypal-perenes-servery-v-rossiyu-chtoby-hranit-personalnye-dannye/ (доступ 21.08.2015)

22 *Google начала переносить сервера в российские дата-центры//* РБК, 2015. 10 апреля. URL: http://top.rbc.ru/technology_and_media/10/04/2015/5522a9f69a794752a5f478fa (доступ 21.08.2015)

23 *Samsung переносит данные россиян на российские сервера//* Business info, 2015. 11 июня. URL: http://b-online.ru/infobusiness/3299-samsung-perenosit-dannye-rossiyan-na-rossiyskie-servera.html (доступ 21.08.2015)

24 *Совет безопасности обсудит отключение России от глобального интернета//* Ведомости. 2014. 19 сентября. URL: http://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet (доступ 21.08.2015)

25 *Рунет готовят к автономии//* Коммерсантъ. 2015. 27 марта. URL: http://www.kommersant.ru/doc/2694953 (доступ 21.08.2015)

26 *Федеральный сервер безопасности//* Коммерсант. 2014. 21 октября. URL: http://kommersant.ru/doc/2324684 (доступ 21.08.2015)

27 См. Приказ Минкомсвязи России *"Об утверждении Правил применения…"*