Петр САРУХАНОВ — «Новая»

Не прощайтесь с блокировками

Радость по поводу новых технологий борьбы с цензурой в интернете преждевременна

Забавно наблюдать, как в мейнстримную прессу, особенно заряженную политикой, залетают «сенсации» из мира IT и наполняют читателей надеждами. Надежды эти, увы, по большей части ложные, поэтому так обидно прочитать сначала, что «все блокировки Роскомнадзора превратятся в тыкву», а потом, после изучения вопроса, узнать, что блажен, кто верует.

Свежий сюжет, который предлагаю читателю к совместному разбору, завязан на публикации в блоге весьма прогрессивного фонда Mozilla, в которой рассказывается о намерении в скором времени включить *по умолчанию* в браузере Firefox опции DNS-over-HTTPS (DoH).

Публикация эта выдержана даже не в осторожном, а в испуганном духе: «Мы планируем подключить DoH в Соединенных Штатах в конце сентября. Сначала мы подключим небольшое число пользователей и будем наблюдать за развитием событий, прежде чем задействовать эту опцию для широкой аудитории. Если все пройдет без осложнений, мы сообщим дополнительно о полной готовности (*включить DoH по умолчанию в браузере. — С. Г.*)».

И вот в ответ на эту опаску-оглядку по просторам прогрессивного отечества вирусно разливается публикация под названием «ПРОЩАЙ ДИ-ПИ-АЙ» (ноги, как я понял, растут из телеграм-канала Михаила Климарева «ЗаТелеком»). Из текста мы узнаем, что теперь «все блокировки РКН превратятся в тыкву. Для обходов блокировок не понадобится ничего, кроме браузера Firefox. Блокировки по DNS не будут работать от слова совсем, ибо все запросы там будут зашифрованы. А блокировки по IP перестанут работать, ибо теперь можно будет тупо изменить IP заблокированного адреса, а РКН об этом не узнает... Великий и ужасный DPI здесь тоже не поможет. Ибо ну вот идет https трафик до рандомных хостов... и чо вы с ним сделаете?»

Мы и в самом деле с этим «ничо» не сделаем, потому что ситуация сильно сложнее. Начнем с технологии. DNS-over-HTTPS означает простую вещь. Когда вы хотите посетить сайт, вы набираете в адресной строке браузера его название, например, novayagazeta.ru. Интернет человеческого языка не понимает, поэтому ваш запрос сначала отправляется на специальные серверы доменных имен (DNS-серверы), которые переводят названия сайтов в соответствующие им цифровые IP-адреса. Например, IP-адрес «Новой газеты» — 198.100.146.115. Именно этот цифровой адрес DNS-сервер передает дальше в Сеть, после чего страница сайта воспроизводится в вашем браузере.

По умолчанию ваш запрос с названием сайта, который вы набираете в адресной строке браузера, отправляется в Сеть в незашифрованном виде, поэтому посредник может его прочитать и тем самым узнать, какой сайт вы собираетесь посетить. Протокол DNS-over-HTTPS позволяет передавать пользовательские запросы к серверу DNS не в открытом виде, а через зашифрованный протокол HTTPS.

Надо сказать, что Mozilla (а также Google) тестируют DNS-over-HTTPS уже больше года — с июня 2018 года. Начиная с версии 62 (а сегодня доступна уже версия 68) любой пользователь браузера Firefox может включить DoH *самостоятельно* в настройках, поэтому резонно предположить, что воодушевивший соотечественников меморандум имеет отношение не столько к самой технологии, сколько к ее применению в браузере *по умолчанию*. При этом речь идет только о гражданах США и Великобритании, поскольку именно в этих странах инициатива Mozilla вызвала яростную критику и противодействие со стороны влиятельных общественных организаций — Фонда надзора за интернетом и Ассоциации провайдеров интернета. Последние даже наградили Mozilla издевательской премией в номинации «Интернет-преступник года».

Что же так возмущает англосаксонскую общественность в протоколе DNS-over-HTTPS? Коллизия в том, что на пользовательских запросах к серверам DNS строятся американские и британские системы родительского контроля и слежения за нарушением авторских прав.

Отрок отправляется на какой-нибудь порноресурс, а специальные программы вроде OpenDNS, SafeDNS, Quostodio, Net Nanny или Symantec Norton Family Premier перехватывают его запрос и делают пальчиком: «Ай-ай-ай, такой-сякой шалунишка! Рано тебе заглядывать в эту сторону!»

Аналогично стращают и борцы из Американской ассоциации звукозаписывающих компаний (RIAA): набрал в адресной строке браузера что-нибудь вроде thepiratebay.org, а тебе, голубчику, вместо торрента с любимой песней прилетает ответка с напоминанием о многомиллионном штрафе за скачивание и распространение контрафакта.

Теперь самое интересное. Я понимаю эйфорию, которая заставила коллегу Климарева писать о «тыкве» блокировок РКН. Автор, кажется, решил, что отечественные провайдеры блокируют по требованию государства нежелательные сайты так же, как в Америке — через запросы DNS. Поэтому и понадеялось, что протокол DNS-over-HTTPS приблизит вожделенный момент с «ПРОЩАЙ ДИ-ПИ-АЙ».

Тут нас, однако, поджидает первая — малая — неприятность (малая, потому что будет еще и вторая — уже большая). По DNS в РФ блокировку осуществляют только 10–15 процентов провайдеров. А остальные 85–90% используют блокировку на совсем другом уровне — протоколе указания имени сервера, т.н. Server Name Indication (SNI).

Термин тоже звучит страшно, но объясняется просто. В момент установки соединения по зашифрованному протоколу HTTPS происходит обмен сертификатами между сервером и компьютером пользователя (то, что называется handshaking, рукопожатием). При этом обмене, предшествующем шифрованию последующего трафика, имя запрашиваемого пользователем сайта передается в открытом, а не зашифрованном виде. Тут-то его и перехватывают родные провайдеры, сопоставляют запрос с запретным списком РКН и, в случае совпадения, выдают пользователю вместо нужного сайта заглушку про постановление советского правительства.

Теперь вы понимаете, что DoH ровным счетом ничего не изменит в сложившейся ситуации и никакого «ПРОЩАЙ ДИ-ПИ-АЙ» не случится.

Можно, конечно, потрафить тщетным надеждам и сказать, что с осени 2018 года интенсивно ведется подготовка к внедрению нового протокола — Encrypted SNI (ESNI), который шифрует в «рукопожатии» имя запрашиваемого сайта с помощью публичного ключа сайта, получаемого из системы имен DNS. И если в новые версии браузеров включат обе опции — и DoH, и ESNI, тогда можно будет с натяжкой уже говорить о технических сложностях блокировки сайтов, которые не нравятся Большому брату.

Не хочется быть гонцом плохих вестей, но и утаивать помянутую выше большую неприятность не имею права. Вы не задумывались, почему в США, ЕС и других «свободных» странах не заморачиваются с изощренными технологиями противодействия нежелательным вылазкам нетизанов, вроде скачивания на торрент-трекерах новинок кинопроката и посещения сайтов, разжигающих расовую неприязнь и гендерную нетерпимость? Почему структуры-церберы «глушат» запросы нерадивых пользователей преимущественно по DNS, а не по SNI, как то делают более продвинутые российские и китайские борцы за чистоту идей?

В июле я уже рассказывал читателям («Коды и котики») об удивительном изобретении «наших американских партнеров» — *универсальном коде*, который массово прививается населению и делает избыточным любые непопулярные запретительные меры. Население нагружено на уровне *общественного порицания* такими жесткими конструкциями самоконтроля, что без всякого внешнего принуждения добровольно сторонится любых действий, которые государство полагает нежелательными.

Ментальность русского народа веками формировалась глобальным нигилизмом и органическим недоверием к власти, поэтому универсальный код американского образца не действует по определению. Зато замечательно работает мотивация *самосохранения*, которая в последние 100 лет окончательно прописалась в генотипе и служит теперь мощным фактором выживания на национальном уровне.

Подавляющему большинству жителей РФ не нужны ни DoH, ни ESNI, ни сайты из списка РКН. Наш человек со спокойным сердцем готов принять (и принимает) любой запрет в интернете, вплоть до полной самоизоляции национального сегмента.

И это и не хорошо, и не плохо. Это — форма национального самосохранения и результат работы исторической памяти, основанной на опыте взаимоотношений с родной властью.

Дальше — больше. Абсолютно все, кто в РФ интересуются «черным списком» РКН, стряхнули технические препоны, как назойливую муху. О том, как пользоваться VPN, знают даже ученики начальных классов. Кому нужно, те пользуются. Таких меньшинство. Большинству это не нужно. Поэтому никакого «ПРОЩАЙ ДИ-ПИ-АЙ» в обозримом будущем не наступит — что с DoH, что с ESNI, что с VPN, что с Великим русским файрволлом, что с чертом лысым и картавым. Когда говорит психология масс, IT-технологии молчат.

> «Наш человек со спокойным сердцем готов принять любой запрет в интернете»

Сергей ГОЛУБИЦКИЙ —
специально для «Новой»