Текст · 22 сентября 2020, 08:25
Александр Бородихин, Давид Френкель,

Россия запрещает запрещать запрещать. Что значат новые поправки в законодательство об интернете

В понедельник министерство связи представило законопроект, в котором предложило наказывать за использование «в Российской Федерации» новейших технологий, затрудняющих блокировку сайтов и защищающих данные пользователей. Очередная инициатива по ограничению свобод в интернете уже вызвала недоумение у технических специалистов. «Медиазона» рассказывает, что за технологии показались опасными российскому государству на этот раз.

Что случилось

4 декабря 2019 года президент Владимир Путин находился в Сочи, где провел переговоры с сербским президентом Александром Вучичем и совещание с руководством Минобороны. На официальном сайте Кремля об этом не сообщалось, но в этот день состоялось также оперативное совещание Совета безопасности о «противодействии распространению противоправной информации в сети "Интернет"». Единственное упоминание об этом мероприятии в открытых источниках содержится в пояснительной записке к законопроекту, подготовленному Минсвязи во исполнение решений Совбеза. Это законопроект

о запрете на «использование на территории Российской Федерации протоколов шифрования, позволяющих скрыть имя (идентификатор) Интернет-страницы или сайта в сети "Интернет"».

В тексте самого законопроекта эта формулировка не уточняется, но в пояснительной записке говорится, что «все большее распространение получают протоколы с применением криптографических алгоритмов и методов шифрования *TLS 1.3, ESNI, DoH (DNS* поверх *HTTPS), DoT (DNS* поверх *TLS)*».

Использование этих алгоритмов, признают в министерстве, «способно снизить эффективность использования существующих систем фильтрации» и помешать российским властям блокировать нежелательный контент. За нарушение запрета сайты, внедряющие новые технологии шифрования, в случае принятия поправок также можно будет немедленно заблокировать.

«Принятие законопроекта, направленного на запрет массового использования в Российской Федерации протоколов шифрования окажет положительное воздействие на выявление ресурсов в сети "Интернет", содержащих информацию, распространение которой в Российской Федерации ограничено или запрещено», — пишут авторы законопроекта.

Что все это значит

«Протокол шифрования, позволяющий скрыть имя (идентификатор) Интернет-страницы или сайта в сети "Интернет" — это абстрактный

или конкретный протокол, включающий набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационные процессы», — такое определение закрепляет предложенная министерством редакция закона «Об информации». Далее кратко описаны протоколы и технологии, которые ведомство собирается поставить вне закона.

HTTPS[1] — протокол безопасной передачи данных, который сегодня поддерживается всеми популярными браузерами; в отличие от обычного *HTTP*, здесь трафик шифруется. При обращении к сайту по протоколу *HTTPS* устройство пользователя и сервер «общаются» при помощи общего секретного ключа, который генерируется для каждого сеанса после проверки браузером цифрового сертификата сайта.

TLS[2] — при установке *HTTPS*-соединения между браузером и сервером по этому протоколу первым делом осуществляется «рукопожатие». В списке сообщений, которыми браузер обменивается с сервером, первым идет *ClientHello* («приветствие клиента») — описание поддерживаемых программой пользователя методов и версий шифрования. Последнее десятилетие интернет работал на алгоритме *TLS* версии 1.2, сейчас мир переходит на 1.3. Новая версия позволяет шифровать пользовательский запрос уже на уровне *ClientHello,* чтобы провайдер или злоумышленник не мог понять, к какому сайту обращается пользователь, а следовательно, не мог предотвратить передачу данных или внедрить в нее свои данные.

ESNI[3] — расширение к протоколу *TLS 1.3,* которое шифрует информацию о том, к какому домену направляется запрос, уже во время первоначального «рукопожатия», на уровне запроса *ClientHello.* Технологию разработали сравнительно недавно, в 2018 году, инженеры *Mozilla, Cloudflare* и *Apple*. В самом простом виде она позволяет скрыть от посторонних глаз название сайта, к которому обращается пользователь. Поскольку технология *HTTPS* предусматривает размещение на одном *IP*-адресе нескольких сайтов, блокировка конкретных ресурсов существенно затрудняется: если закрыть доступ к сайту по его *URL* (-ссылке) или *IP*-адресу технически невозможно, нужно более глубоко анализировать «технический» трафик пользовательского устройства, но и там — шифрованная информация. По данным «Технического центра Интернет», в российской

доменной зоне до 200 тысяч сайтов используют правильно настроенный *ESNI*.

DNS[4] **через HTTPS (DoH), DNS через TLS (DoT)** и аналогичные технологии преследуют одну цель — не допустить перенаправление браузера клиента с желаемого сайта на некий сторонний (такие попытки могут осуществлять как злоумышленники, так и провайдеры по предписанию госструктур). Шифруя *DNS*-запросы, пользователь затрудняет мониторинг трафика — например, развернутыми в России и других странах системами «глубокого анализа пакетов» *(DPI)*. Разработку этих технологий ведут крупнейшие *IT*-компании: *DNS* через *HTTPS* поддерживают браузеры *Firefox, Chrome, Edge* и *Opera*, поддержку получили новые версии операционных систем *MacOS* и *iOS*.

В целом, если протокол *HTTPS* шифрует весь пользовательский трафик кроме информации о домене, к которому обращается пользователь, то остальные упомянутые выше технологии позволяют разными способами зашифровать и эту техническую информацию, сделав соединение еще более защищенным от посторонних глаз.

> «В России сервера *DNS over TLS* и *DNS over HTTPS* "подняты" у "Яндекса", — сообщил "Медузе" специалист по алгоритмам шифрования Дмитрий Белявский. — Согласно этому законопроекту, все те сайты, которые используют их, в России будут вне закона и должны будут быть заблокированы. А так как по одиночке их заблокировать невозможно как раз по причине

использования этих технологий, то блокировать будут целыми подсетями хостинг-провайдеров, то есть опять Роскомнадзор будет блокировать целые диапазоны IP-адресов *Amazon Web Services, Digital Ocean, Cloudflare,* как это было, когда ведомство пыталось заблокировать *Telegram* в России несколько лет назад».

В феврале 2020 года Роскомнадзор разблокировал два миллиона *IP*-адресов, которые заблокировал ранее в попытках прекратить работу *Telegram;* весной 2018-го массовые блокировки затронули работу многих сайтов. Сам мессенджер летом внезапно разблокировали.

«Это малозначащий набор слов. Выводить отсюда, что хотели запретить весь *HTTPS* — нелепо, — прокомментировал публикацию законопроекта *IT*-специалист Филипп Кулин в своем телеграм-канале. — <...> Отсюда можно вывести только то, что кто-то[5]

не утруждал себя посещать уроки русского языка и литературы в школе. Если вообще в школу ходил».

Сотрудничавший с «Фондом борьбы с коррупцией» программист Владислав Здольников связал инициативу Минсвязи с успехом «Умного голосования». Он отмечает, что развернутые сейчас системы *DPI* считают весь *ESNI*-трафик подозрительным и блокируют.

Аналогичный подход используют власти Китая: с конца июля обновление к «великому китайскому файерволу» начало блокировать *HTTPS*-соединения, использующие протокол *TLS 1.3* с расширением *ESNI* (его предыдущая, нешифрованная версия *SNI,*

позволяющая цензорам увидеть запрашиваемый домен, работает).

Что же теперь будет

В записке к законопроекту Минсвязи есть отсылка к официальному реестру компьютерных программ, где «содержатся сведения о протоколах с применением криптографических алгоритмов и методов шифрования возможных к использованию в соответствии с законодательством Российской Федерации» (пунктуация оригинала сохранена).

Отечественные альтернативы зарубежным протоколам шифрования в документе не упоминаются, однако известно, что в прошлом году были зарегистрированы два разработанных под руководством ФСБ криптоалгоритма: «Магма» и «Кузнечик»[6].

К их надежности у зарубежных исследователей появились вопросы: хотя разработчики говорили об отсутствии скрытых структур[7] в ключевом элементе криптоалгоритма *SBox*, похожие «неслучайные» структуры нашлись; разработчики тогда объяснили это совпадениями и упрекнули коллег в «спекулятивном характере» претензий.

Переводить чиновников на российскую криптографию «при электронном взаимодействии между собой, с гражданами и организациями» президент Путин поручил еще в 2016 году.
Во время разработки «закона о суверенном интернете» планировалось вписать туда требование

о защите всего российского трафика отечественным шифрованием, но реализацию этой идеи решили отложить.

Теперь в ближайших планах — запуск государственного удостоверяющего центра для выдачи отечественным сайтам внутренних *TLS*-сертификатов с криптографией по ГОСТу, однако действовать они смогут только при условии включения соответствующего кода в популярные операционные системы и браузеры.

Редактор: Дмитрий Ткачев

---

1. Hypertext Transfer Protocol Secure, безопасный протокол передачи гипертекста.
2. Transport Layer Security, протокол защиты на транспортном уровне.
3. Encrypted Server Name Indication, шифрованная индикация имени сервера.
4. Domain Name System, система доменных имен.
5. Автор законопроекта.
6. Описанные в ГОСТ 34.12-2018 блочные шифры с размером блока в 64 бита и 128 бит соответственно. Для обоих разработаны рекомендации для использования с протоколом TLS 1.3.
7. В численном массиве шифра не должно быть численных последовательностей, подчиненных некой воспроизводимой логике.