Текст · 8 декабря 2021, 07:01
Александр Бородихин, Давид Френкель,

Банхаммер Тора. Как Россия решила победить даркнет

Да что такое этот ваш Tor?

Для широкой аудитории термины *Tor*, *Deep Web*, «даркнет» и «ноды» звучат экзотически — если неспециалист и слышал про такие вещи, то, как правило, из криминальных сводок или новостей *IT*-индустрии. Но за последнее десятилетие «глубокий интернет» стал заметным фактором общественной жизни: его не могут игнорировать ни люди, по тем или иным причинам избегающие контактов с государством, ни сами государства.

Через даркнет убивают, пробивают, сливают-, продают, вымогают и отмывают — это и попадает в новости. Меньшего внимания прессы удостаиваются люди, пользующихся даркнетом ежедневно: правозащитники, военные, журналисты, ученые — в общем, два с половиной миллиона человек, для которых безопасность передачи данных принципиальна.

Хотя основная цель *Tor* — сделать доступ к обычным сервисам в интернете анонимным, есть также набор сайтов и сервисов, которые вне *Tor* в принципе недоступны: когда говорят о даркнете, обычно имеют в виду так называемые *onion* или *hidden* ресурсы.

Ключевой угрозой анонимности пользователей считается возможность полностью расшифровать

трафик и прочитать, что пользователь пишет и кому. Сделать это удобнее всего «на выходе», то есть на пути между зашифрованной сетью и непосредственно сайтом; скрытые сервисы позволяют избежать такого сценария, поскольку трафик не расшифровывается полностью и не покидает сеть *Tor* вовсе, а местонахождение конечного сервиса скрыто от пользователей.

Многие скрытые сервисы декларируют своей целью защиту свободы слова и помогают людям из разных стран обходить блокировки (например, зеркало в *Tor* есть у соцсети *Facebook*). Но есть и сайты, использующие *Tor* для незаконной деятельности: торговли наркотиками, оружием и пиратства.

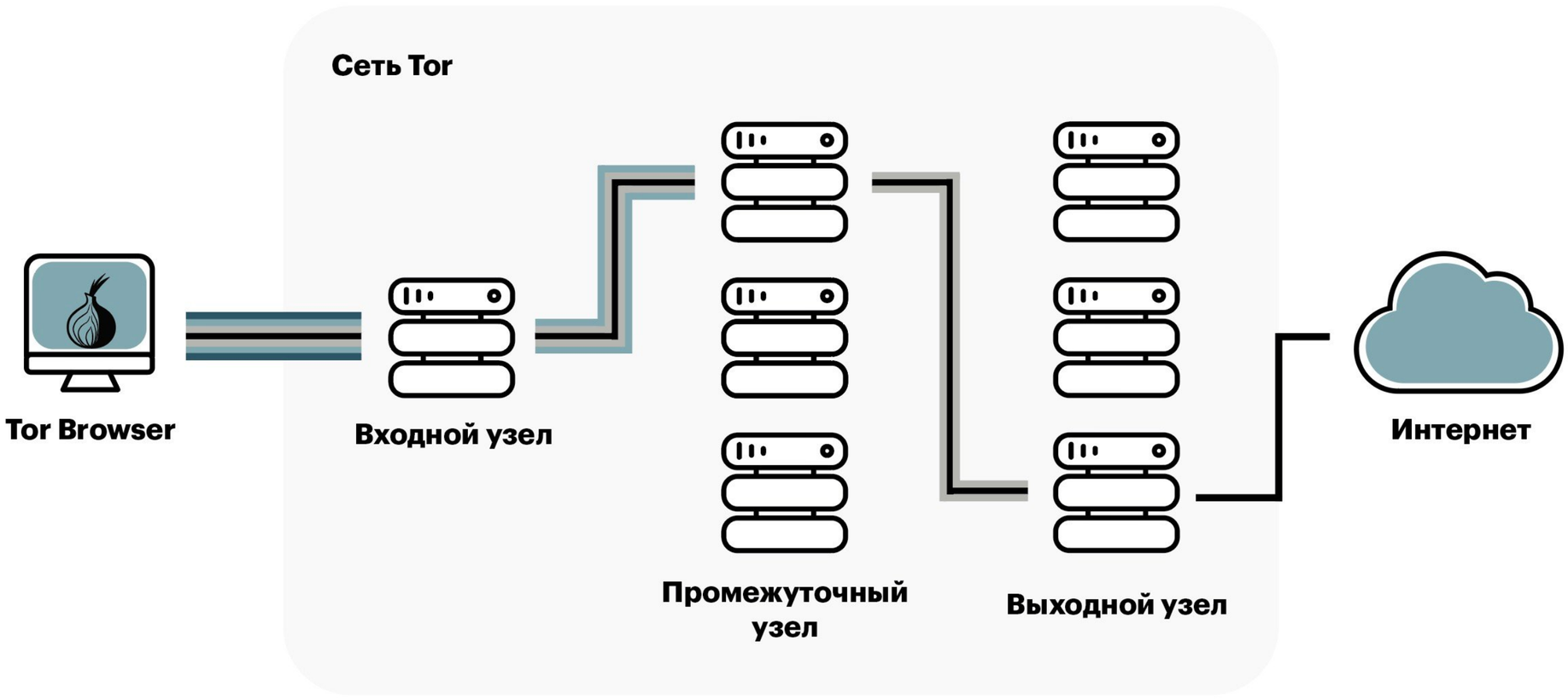
В США самым известным процессом против сервиса даркнета стало дело *Silk Road*. Созданный в 2011 году *Silk Road* стал первой заметной торговой площадкой, где за криптовалюту можно было купить наркотики, поддельные документы, краденые банковские карты или оружие. Закрыть сайт американская ФБР смогла лишь через два года: деанонимизировать и добиться пожизненного срока для создателя площадки Росса Ульбрихта помогли ошибка в коде сайта, внедренный агент и спецоперация в библиотеке, где чуть ли не важнее задержания самого подозреваемого был захват открытого ноутбука, залогиненного в системе *Silk Road*.

А в России в 2017 году стало резонансным уголовное дело преподавателя математики и программиста Дмитрия Богатова: его обвинили в призывах к массовым беспорядкам и терроризму

на небольшом форуме для сисадминов. Посты публиковал пользователь под псевдонимом «Айрат Баширов», и хотя Богатов объяснял, что не имеет к нему никакого отношения, его отправили под арест.

Выяснилось, что в квартире Богатова функционировал выходной узел сети *Tor,* то есть с его *IP*-адреса взаимодействовали с «открытым» интернетом другие пользователи. После нескольких месяцев в СИЗО и под домашним арестом на фоне международной кампании поддержки с Богатова сняли обвинения. Позже по этому же делу задержали Владислава Кулешова из Ставрополя, тот признал вину и отделался легким наказанием.

Претензии к владельцам выходных узлов у силовиков есть не только в России; известно об обысках и изъятии компьютеров у волонтеров *Tor* как минимум в Австрии и в США. Об опасности попасть под подозрение говорится на сайте проекта: «Если правоохранительные органы заинтересуются трафиком с вашего выходного узла, они могут изъять ваш компьютер. По этой причине лучше не запускать выходной узел у себя дома или с домашнего интернет-соединения».



Принцип работы сети Tor. Инфографика: Медиазона

Как это работает

Пользователи *Tor* выходят в интернет как и все, запуская приложение (браузер или мессенджер), но с ключевым отличием: в него встроена система «луковой маршрутизации» — так дословно расшифровывается название сети *Tor (The Onion Routing)*.

Если коротко, то маршрутизация — это поиск путей в сети, к примеру, между браузером и сайтом, который он пытается открыть. Данные в интернете редко попадают напрямую с сервера на устройство пользователя, обычно они проходят через множество узлов сети, а для навигации между ними существуют различные технологии по поиску кратчайшего маршрута.

Эти узлы — от оборудования провайдера до точек обмена трафиком в крупнейших городах мира — по своему принципу действия должны знать, от кого и куда идут данные. Если данные не зашифрованы, то узлы могут читать содержимое

трафика: владелец сайта видит, с какого *IP*-адреса подключается пользователь, это же знает и провайдер. Так силовикам удается вычислять автора какого-нибудь поста в соцсетях: они запрашивают у соцсети *IP*-адрес пользователя, а затем у провайдера — данные человека, который этим адресом пользовался в момент публикации.

Есть много способов скрыть от посторонних глаз содержимое интернет-трафика: если, скажем, открывать инкогнито-вкладки в браузере совсем бесполезно, то запускать *VPN* — уже имеет смысл. Правда, если покупать услуги у популярного сервиса, силовики могут затребовать у него сведения о пользователе. Те сервисы, которые не хранят данные о клиентах, можно заставить это делать или же заблокировать.

«Луковая маршрутизация» призвана еще сильнее усложнить деанонимизацию в сети. Переосмысляя принцип поиска маршрутов, *Tor* отказывается от поиска кратчайшего пути от сервера к пользователю и передает данные через несколько дополнительных случайно выбранных промежуточных узлов. Данные при этом неоднократно шифруются, оборачиваясь слоями, как луковица шелухой, а каждый промежуточный узел на маршруте расшифровывает по одному слою, разворачивая луковицу и узнавая дальнейший путь. Каждый узел знает только своих «соседей» — откуда данные пришли и куда их передать дальше.

> Есть еще «чесночная маршрутизация» *(Garlic Routing)* — для затруднения анализа трафика единичные сообщения-«зубчики» от разных пользователей объединяются в одну общую «головку», так что узлы сети не знают даже, какой из «зубчиков» чей. Такой метод используется в сетях еще одного протокола — I2P.

Узлами в сети *Tor* служат устройства волонтеров и активистских организаций. В сетях три типа узлов:

— входной *(guard)*, с которым соединяется пользователь;

— выходной *(exit)*, который знает, с каким сайтом надо соединиться;

— и промежуточный *(middle)*, который соединяет входной и выходной узлы, но ничего не знает ни про пользователя, ни сайт, который он пытается открыть.

Провайдер при этом не в состоянии прочитать передаваемые данные, потому что все отправляется в луковице из слоев шифрования.

При этом *Tor* не гарантирует полную анонимность: сеть ничего не может сделать с происходящим «на краях» — на стороне провайдера или на стороне конечного сайта. Пользователей все еще могут выдать отличительные характеристики их браузера[1] или особенности поведения в сети: в 2013 году студент Гарварда Элдо Ким прокололся, отправив через *Tor* сообщение о заложенной бомбе,

чтобы сорвать экзамены — но его компьютер был единственным в университете, который в момент отправки подключался к входным узлам *Tor*.

Открытость проекта, которой гордятся активисты, может стать и его слабой стороной: недоброжелатель может запустить сколько угодно собственных узлов, чтобы вычислять пользователей, если их данные будут проходить подконтрольные ему ноды-[2]. Еще в 2012 году в презентации *Tor Stinks*, опубликованной Эдвардом Сноуденом, американское АНБ[3] жаловалось, что агентству не хватает узлов в сети, чтобы отслеживать цепочки соединений. Позже регулярно появлялись слухи, что АНБ все же контролирует существенное число узлов в сети, но ни доказать, ни опровергнуть это пока не удалось.

Специалисты по кибербезопасности неоднократно находили большие группы узлов, принадлежащие таинственному владельцу *KAX17*. В октябре 2019 года сотни его узлов удалили из сети, но он смог восстановить сетку[4] на мощных дорогостоящих серверах по всему миру. Вероятность использовать *middle*-узел из этой группы для случайного пользователя достигала 35%.

Владелец узлов активно участвовал во внутренних дискуссиях на форумах *Tor,* но это не спасло его сетку: в конце ноября 2021 года, как раз перед началом блокировки *Tor* в России, их исключили из «луковой маршрутизации». Кому они принадлежали и использовались ли для деанонимизации пользователей, неизвестно.

Фото: The Christian Science Monitor / Ann Hermes / AP

2017. Незаметный удар

Если поискать саратовский поселок Дубки в *Google* и перейти по ссылке в *Maps,* сервис предложит три ключевых точки в населенном пункте: кафе «Мимино», магазин «Красное и белое» и Саратовский районный суд. Между ними — храм во имя царственных страстотерпцев[5], служащие автобусными остановками ангары, побеленные электрические столбы, пустыри и заборы.

Именно здесь, в центре Дубков, в 2017 году было вынесено решение мирового масштаба: Саратовский районный суд признал «запрещенной информацией» ссылку на скачивание анонимного браузера *Tor*-, по которому в 2021 году сайт проекта грозят заблокировать в России.

Суть заседания в декабре 2017 года можно передать одним предложением из решения судьи: «Как следует из материалов дела,

прокуратурой проведена проверка сайта *https* <данные изъяты> в сети "Интернет", в результате которого установлено, что на указанном сайте пользователи могут получить доступ к скачиванию программы браузера-анонимайзера для последующего посещения сайтов, на которых размещены материалы, включенные в Федеральный список экстремистских материалов, в частности к информации, размещенной на сайте <данные изъяты> на котором размещен информационной материал (признан экстремистским решением Ленинского районного суда <адрес> от ДД.ММ.ГГГГ)». Решение принимал судья Денис Симшин — этой осенью он решил сложить полномочия.

Название материала, вызвавшего интерес прокуратуры — как и адрес подлежащего блокировке сайта — из опубликованного текста решения суда вымараны. При этом в реестре Роскомнадзора упоминается решение Саратовского районного суда за 2017 год; также известно, что тогда суд в Дубках по просьбе прокуратуры предписывал блокировать сайты, торгующие поддельными водительскими удостоверениями, медицинскими справками, скручивателями счетчиков и предлагающие секс-услуги. Интерес к *Tor* у саратовских прокуроров тоже не уникален: в том же 2017 году суды блокировали различные анонимайзеры.

2021. Огонь по нодам

1 декабря 2021 года российские пользователи *Tor* начали жаловаться на невозможность подключиться к сети. За два дня блокировка стала массовой для

пользователей крупных российских провайдеров — в особенности мобильных операторов.

«Уважаемые пользователи, — обращается к клиентам крупнейший отечественный магазин по торговле нелегальными веществами. — С начала декабря пользователи РФ могут испытывать проблемы с входом в *Tor* из-за блокировки сети провайдерами интернета».

Сервис мониторинга блокировок *GlobalCheck* подтвердил, что ТСПУ[6] Роскомнадзора заблокировали доступ к существенной части[7] входных узлов сети *Tor*. Ведомство не блокировало работу всей сети, но мешало пользователям соединяться с публично доступными входными узлами.

Аналогичным образом много лет доступ к *Tor* блокируется в Китае. Для обхода такой блокировки существуют «мосты» *(bridges)* — узлы, которые сами не участвуют в работе *Tor*, но соединяют пользователя со входным узлом, который компьютер по какой-то причине не может найти. Адреса некоторых «мостов» можно получить в браузере *Tor* или на сайте *Tor Project*-.

Как сообщали пользователи форума *ntc.party*, «мосты» тоже попали под блокировки в России. Есть и более сложные методы: адреса менее публичных «мостов» можно запросить по специальной электронной почте; такие адреса остались доступны в России. «Мосты» используют разные методики, чтобы скрыть, что внутри них передается трафик *Tor*, обходя

таким образом системы анализа пользовательского трафика, в том числе ТСПУ Роскомнадзора.

> ТСПУ работают по принципу «глубокого анализа пакетов» *(Deep Packet Inspection, DPI)* — изучения характерных особенностей пользовательского трафика, позволяющих отличить один тип соединения от другого. К примеру, отличить шифрованный трафик *Tor* от обычного доступа в сеть. Так уже поступали власти Ирана и Казахстана, но на этот случай у *Tor* есть дополнительные средства для искусственного искажения потока данных так, чтобы вычленить трафик *Tor* было если не невозможно, то крайне ресурсозатратно.

6 декабря Роскомнадзор направил разработчикам *Tor* письмо с требованием удалить «запрещенную информацию», чтобы избежать блокировки сайта. Администраторы некоторое время пытались понять, о чем идет речь, а потом выступили с заявлением- , призвав пользователей из разных стран запускать больше «мостов», чтобы «помочь россиянам остаться в сети», а правозащитные организации — «оказывать давление на российские власти для отказа от цензурных мер».

Вечером 7 декабря Роскомнадзор добавил официальный сайт *Tor* в списки на блокировку провайдерами. Через четыре года после решения суда в Дубках главная страница *Tor Project* перестала открываться[8] из России.

Редактор: Дмитрий Трещанин

1. Так называемые цифровые отпечатки, fingerprints.

2. Узлы сети Tor.

3. Агентство национальной безопасности.

4. На пике в группу входило около 900 узлов, всего в Tor в 2021 году было около 6 тысяч узлов.

5. Императора Николая Романова и его семьи.

6. Технические средства противодействия угрозам — устройства для контроля за трафиком пользователей, которые Роскомнадзор устанавливает у интернет-провайдеров в рамках закона о «суверенном интернете».

7. Всего узлов около двух тысяч, точное число заблокированных неизвестно, но их было достаточно, чтобы пользователи заметили серьезные проблемы с подключением.

8. Без использования средств обхода блокировок.