Критика заблуждения о контроле Tor спецслужбами

Арс Либрев

Сеть Tor, это реализация технологии луковой маршрутизации. Она представляет собой систему серверов, распределенных по всему миру. При подключении к ней, трафик шифруется и последовательно перенаправляется через цепочку из нескольких узлов, благодаря чему становится невозможно без специальных методов определить, кто какие ресурсы посещает. Также Tor формирует собственную закрытую сеть сервисов. Вокруг технологии Tor сложилось много мифов. Суть одного из них в том, что Tor якобы контролируется американскими спецслужбами. То есть, этот миф говорит, что существует заговор спецагентов и разработчиков Tor с целью слежки за пользователями сети, позиционируемой как анонимная. К сожалению, некоторые люди и впрямь предпочитают верить своим домыслам, даже если у этих домыслов нет никаких оснований. В качестве же доказательств ими принимаются любые сведения, которые способны хотя бы косвенно указать на их правоту. Любые же доказательства отсутствия заговора трактуются как часть самого заговора. В такой картине, доказательства, которые могли бы подтвердить наличие заговора исчезают, которые показывают его отсутствие подделываются, свидетели запуганы, эксперты куплены.

Нет доказательств? Потому что их уничтожили. Есть доказательства обратного? Потому что их сфабриковали.

Спорить с такой позицией в принципе невозможно. Поэтому вряд ли имеет смысл пытаться переубедить самих конспирологов. Однако, есть люди, которые осознают несерьезность их методологической позиции (если такую позицию вообще можно назвать методологической), но кому не хватает осведомленности, чтобы вынести окончательный вывод о подконтрольности или не подконтрольности сети Tor.

Единственным фактом, который может хоть как-то указывать на правоту гипотезы о контроле Tor американским правительством, является то, что данный проект изначально разрабатывался военными США и до сих пор финансируется их правительством.[1] Конспирологи считают, что никаких других причин, кроме возможности следить за пользователями, финансировать данный проект у правительства США нет.

Tor действительно изначально создавался для безопасной коммуникации американских агентов. Но как отметила одна из разработчиков Tor Руна

Сендвик, если бы он продолжал развиваться так, как разрабатывался изначально — секретно и только для пользования спецслужбами — он не смог бы выполнять свою функцию. Ведь для любого было бы очевидно, что если кто-то пользуется сетью Tor — он американский агент. Когда же проект открылся и обрел массового пользователя, агенты стали растворяться среди других пользователей. Именно поэтому проект Tor выгоден правительству США и выгоден именно как свободный проект.[2]

Есть огромное количество разработок, которые, выйдя из военных ведомств, стали доступны простым обывателям — тренчи, тампоны с прокладками, консервы, сублимированные продукты, в том числе, сублимированный кофе.[3] Кстати, в Интернете можно найти соглашение между правительством Московской области и одним из производителей сублимированного кофе.[4] Это так, на заметку конспирологам — соглашение между правительством и производителем товара, использующего технологию, разработанную в военных целях. Конспирологам стоит задуматься, может когда они попивают кофеек, правительство их в рот чипирует?

Многие знают бывшего американского агента Эдварда Сноудена, опубликовавшего множество документов о массовой слежке, осуществляемой АНБ. И среди этих документов есть и те, которые раскрывают попытки АНБ разработать эффективные методы по деанонимизации пользователей Tor.[5] Среди этих методов были, например попытки заражения компьютеров, вредоносными cookie-файлами через рекламные сервисы Google,[6] эксплуатация уязвимостей браузера Firefox, на котором основан Tor Browser, и многое другое, на что были потрачены миллионы долларов.[7] Как следует из этих документов, несмотря на некоторые успехи, добиться полного контроля над сетью Tor АНБ не удалось.

Вопрос к конспирологам — если Tor и так находится под контролем спецслужб, зачем было что-то разрабатывать? Конечно, обладатели фольгированных головных уборов заявят, что Сноуден засланец, а все документы подделаны. Поскольку кивать им на принцип фальсифицируемости (утверждение можно всерьез рассматривать только если оно потенциально проверяемо), бритву Оккама (из всех объяснений, при прочих равных условиях, следует предпочитать наиболее простое), чайник Рассела (бремя доказательства лежит на утверждающем существование чего-либо, а не на критике, поскольку доказать отсутствие чего-либо, в принципе, невозможно) и техасского стрелка (поиск и демонстрация только тех фактов, которые укладываются в определенную концепцию, и игнорирование тех, которые ей противоречат) бесполезно, зададим конспирологам встречный вопрос. Проект Tor существует уже без малого двадцать лет, почему за столь долгий срок не произошло ни

одной действительной утечки о контроле за ним? Ведь в этот заговор, получается, должно быть вовлечено огромное количество людей — сотрудники спецслужб, чиновники, сами участники проекта Tor, держатели узлов, в конце концов. Это тысячи людей. И что за столь огромный срок существования заговора ни разу не произошло утечки? Да заговоры куда меньших масштабов без сливов не обходятся.

На это конспирологи, конечно, скажут, что спецслужбы настолько всемогущие, что способны замести вообще все следы заговора. Ну кроме факта финансирования сети Tor американским правительством. И вот тут неизбежно возникает вопрос — если они способны предотвратить все утечки и замести все следы, почему они не замели единственную ниточку, ведущую от проекта Tor к ним? Что мешало осуществлять финансирование тайно? Ведь когда правительству США действительно нужно замести следы своего участия в чем-то, они вполне успешно это делают. Именно так ими финансировались исследования по слежке за чат-комнатами,[8] эксперименты над детьми в Дании,[9] кампании по приходу к власти провашингтонских режимов в странах «третьего мира».[10] Именно так финансировались «эскадроны смерти» в странах Латинской Америки.[11] Почему же для скрытия единственного следа, ведущего от них к Tor, они не прибегли к этим проверенным годами неолиберального угнетения методам?

Всего озвученного вменяемому человеку уже достаточно для того чтобы понять несостоятельность мифа о подкотрольности сети Tor. Но давайте не будем на этом останавливаться и разберемся со случаями деанона участников сети Tor. Может быть эти случаи предоставят какие-нибудь доказательства, указывающие на возможность существования заговора?

Долгое время самой крупной площадкой по торговле нелегальными товарами в скрытом сегменте сети Tor оставался сайт Silk Road 2.0. Он был закрыт в 2014 году, в ходе крупной операции спецслужб США и Европола, после установления местонахождения его серверов.[12] Как им удалось это сделать? По информации из ФБР, для этого в среду операторов этого сайта были внедрены агенты, которые и слили данные.[13] Если у спецслужб уже был контроль над Tor, зачем им понадобилось кого-то внедрять? Этот вопрос отправляйте конспирологам до востребования.

За год до описанного случая в Ирландии, по запросу властей США, был арестован владелец одного из скрытых сервисов Tor.[14] После этого, на сайты данного хостинга, взятого под контроль ФБР, был внедрен вредоносный java-скрипт,[15] эксплуатирующий уязвимость браузера Firefox.[16] ФБР сделало это для деанонимизации как можно большего числа пользователей данных ресурсов. Эта информация в дальнейшем была официально подтверждена ФБР.[17] И снова

тот же вопрос — зачем американским спецслужбам внедрять какой-то скрипт для деанона, если сеть Tor и так им подконтрольна?

О том как был закрыт Silk Road 2.0 уже было сказано. Но при этом не упоминалось, что вместе с ним было закрыто еще более четырехсот скрытых сервисов Tor.[18] И если в отношении Silk Road 2.0 мы имеем данные о том, как это было осуществлено, то в отношении всех остальных сервисов у нас нет каких-либо точных сведений, о том, как был проведен их деанон. В этом отношении официальных заявлений спецслужбы не давали. У нас нет данных как эти сервисы были накрыты. Конспирологи, конечно, поспешат объявить это подтверждением того, что сеть Tor и так им подконтрольна, и именно поэтому они и сумели все их раскрыть. Но давайте постараемся разобраться, может быть есть какие-то другие объяснения?

Первое возможное объяснение. Поскольку Silk Road 2.0 был захвачен благодаря внедренным агентам, вполне возможно, что и другие серверы были скомпрометированы этим же путем.[19]

Вторым возможным объяснением является эксплуатация спецагентами распространенных веб-багов, таких как SQL-инъекции и удаленное включение файлов. Эксплуатация веб-уязвимостей практика вообще весьма распространенная. Вполне возможно, что и многие из закрытых сервисов были не слишком тщательно спроектированы и имели большую поверхность атак.[20]

Третьим возможным объяснением является деанонимизация через раскрутку цепочки транзакций биткоин.[21] В сети есть исследование данного метода, из которого следует, что это вполне возможно.[22] Поскольку как минимум часть закрытых сервисов использовала биткоин, возможность деанонимизации именно этим путем нельзя исключать.

Четвертым возможным объяснением является атака глобального пассивного наблюдения. Это весьма сложная и затратная атака, однако для крупных структур ни неподъемная, по крайней мере, для разовых акций.[23] У этой гипотезы, кстати, есть подтверждение. Есть свидетельства некоторых владельцев узлов Tor, сообщавших в Tor Project, что их узлы были захвачены правительственными агентами.[24] На возможность именно такого развития событий также указывает тот факт, что в течении нескольких лет, предшествовавших этой крупной операции по закрытию сервисов, появлялись различные сведения о попытках тех или иных структур исследовать возможность этой атаки. В ходе таких исследований, осуществлялись настоящие атаки этого рода.[25] У сети Tor есть некоторые средства защиты от этого, но они не являются абсолютными.

Пятым возможным объяснением является эксплуатация неизвестной уязвимости Tor.[26] В любом программном обеспечении есть свои уязвимости, и

ни один проект не застрахован от того, что какую-то уязвимость злоумышленники найдут раньше разработчиков. В Tor много раз находили уязвимости и исправляли их. Выше упоминалось о ныне уже закрытой уязвимости браузера Firefox. В свете этого стоит вспомнить об исследовании, проведенном сотрудниками университета Карнеги-Меллон, в ходе которого удалось обнаружить ранее неизвестную уязвимость и деанонимизировать некоторые скрытые серверы. Узнав о результатах этого исследования, ФБР через суд обязало сотрудников университета выдать им данные деанонимизированных, вместе со сведениями об уязвимости, а также запретило им выступать на хакерской конференции, где они собирались об этой уязвимости рассказать.[27] Появлялись даже заявления о том, что ФБР само заказало данное исследование, передав университету миллион долларов.[28]

Шестым возможным объяснением является атака на сторожевые узлы. Сначала проводится атака guard discovery, в ходе которой выясняется сторожевой узел конкретной скрытой службы (сторожевой узел единственный, который знает настоящий ip скрытого узла) затем этот узел тем или иным образом компрометируется — удаленно взламывается или захватывается физически (тут снова вспомним о свидетельствах некоторых держателей узлов, которые брались под контроль спецагентами). После этого уже возможно запустить атаку подтверждения трафика для идентификации скрытого сервиса.[29]

Таким образом, возможных вариантов того, как были накрыты скрытые сервисы много и некоторые из них имеют фактические подтверждения. Конспирологи, конечно, поспешат заявить, что это лишь предположения. Но ведь и подконтрольность Tor спецслужбам это тоже лишь предположение. Причем те предположения, которые были изложены выше, хотя бы вписываются в ту версию, которая подтверждается хоть какими-то фактами — документами АНБ, заявлениями ФБР, свидетельствами держателей узлов, самим кодом Tor, находящимся под свободной лицензией, в конце концов. А чем подтверждается версия о подконтрольности Tor? Если вы до сих пор считаете, что факта финансирования Tor американским правительством достаточно для того, чтобы посчитать эту гипотезу верной, то перечитайте эту статью.

Рассуждения сторонников концепции контроля Tor американскими спецслужбами не более обоснованы, чем построения плоскоземельщиков, борцунов с жидомассонами или рептилойдоведов.[30]

Критичность восприятия крайне важна, не стоит ставить домыслы выше фактов. Также важно беречь свою информацию. Tor в этом поможет.

1 История проекта Tor изложена на официальном сайте https://www.torproject.org/ru/about/history/. Государственные структуры США указаны на официальном сайте в разделе «Спонсоры» https://www.torproject.org/ru/about/sponsors/. *Brian Fung* «The feds pay for 60 percent of Tor's development. Can users trust it?» https://www.washingtonpost.com/news/the-switch/wp/2013/09/06/the-feds-pays-for-60-percent-of-tors-development-can-users-trust-it/?arc404=true. *Антон Осипов* «Кто платит за браузер Tor, позволяющий обойти блокировку сайтов» https://www.vedomosti.ru/technology/articles/2019/04/03/798234-tor-ne-dolzhen-zaviset-ot-pravitelstva

2 *Алина Гайнуллина* «Это не секрет, это просто не ваше дело. Руна Сендвик, одна из разработчиков анонимной сети Tor, рассказала о темной стороне интернета» https://lenta.ru/articles/2014/06/27/tor/

3 Статья о военных разработках, вошедших в обиход «Топ-25: Самые распространенные вещи, которые были изобретены военными» https://bugaga.ru/interesting/1146747851-top-25-samye-rasprostranennye-veschi.html. Команда Техноконтроль «Топ-10 военных разработок в повседневной жизни» http://technocontrol.info/tehno-fun/top-10-voennix-razrabotok--v-povsednevnoy-zhizni

4 Соглашение между правительством и одним из производителей кофе https://mosreg.ru/dokumenty/normotvorchestvo/perechen-dogovorov-i-soglasheniy-mo/2018-god/06-06-2018-14-05-45-soglashenie-ot-24-05-2018-158-mezhdu-pravitelstvom

5 Документы АНБ о попытках контролировать Tor http://cryptome.org/2013/10/nsa-tor.pdf. Статья о публикациях документов АНБ, посвященных Tor *Barton Gellman*, *Craig Timberg*, *Steven Rich* «Secret NSA documents show campaign against Tor encrypted network» https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html. Еще одна статья об этом «Опубликованы материалы о методах АНБ по получению контроля за пользователями Tor» https://www.opennet.ru/opennews/art.shtml?num=38087

6 *Антон Благовещенский* «АНБ отследить анонимов в сети Tor при помощи рекламных объявлений AdSense» https://rg.ru/2013/10/07/nsa-tor-google-site.html

7 О различных способах деанонимизации, которые пыталось применять АНБ сказано в статье «TOR (the onion router)–NSA Pricetag for Anonymity?» http://therearenosunglasses.wordpress.com/2014/07/05/tor-the-onion-router-nsa-

pricetag-for-anonymity/. *Анатолий Ализар* «Опубликованы документы АНБ о попытках взять под контроль сеть Tor» http://xakep.ru/61372/

8 Об этом рассказывается в статье «Спецслужбы намерены установить слежку за чат-румами» https://www.securitylab.ru/news/214659.php

9 *Jakob Stein* «Danske bornehjemsborn brugt i hemmelig undersogelse stottet af CIA» https://www.dr.dk/nyheder/indland/danske-boernehjemsboern-brugt-i-hemmelig-undersoegelse-stoettet-af-cia. Об этом также рассказывается в статье «ЦРУ проводило секретные исследования на детях-сиротах с шизофренией в Дании» http://alternatio.org/events/all/item/98070-tsru-provodilo-sekretnye-issledovaniya-na-detyah-sirotah-s-shizofreniey-iz-danii. *Виктория Кондратьева* «ЦРУ обвинили в проведении экспериментов над детьми с шизофренией» https://lenta.ru/news/2021/12/29/experiments/

10 О финансировании спецслужбами акций по подрыву власти в Чили можно прочитать в статье *Сеймур Херш* «Тайная война ЦРУ против Чили», пер. с англ. редакции «За рубежом» http://saint-juste.narod.ru/CIA_vs_Chile.html

11 Общую информацию об «эскадронах смерти» можно узнать из статьи *Хавьер Хиральдо* «Эскадроны смерти в Колумбии, их прошлое и настоящее», пер. с исп. и комментарии Виктора Камилинчука, под ред. Бориса Гилеева, Александра Тарасова и Дмитрия Штрауса http://saint-juste.narod.ru/paramilitares1.html. А также из статьи *Нэнси Мастронарди* «Феномен эскадронов смерти», пер. с исп. Дмитрия Штрауса, под ред. Александра Тарасова, комментарии Александра Тарасова https://scepsis.net/library/id_2713.html. Об «эскадронах смерти» в Ираке упоминается в статье *Александр Тарасов* «Гуманизм» https://scepsis.net/library/id_2080.html, со ссылкой на Newsweek. 8.01.2005. И там же говорится об «эскадронах смерти» в Латинской Америке, со ссылками на *Булычев И.М.* Заговор против народов Центральной Америки. М., 1984; *McCuen G.E.* Political Murder in Central America. Death Squads and U.S. Politics. Hudson (WI), 1984; *Benítes Manaut R., Lozano L., Bermúdez Torres L.* EE. UU. contra Nicaragua. La guerra de baja intensidad en Centroamérica. Madrid, 1987; El Salvador Death Squads. A Governmental Strategy. Sidney, 1988; Harvest of Violence. The Maya Indians and the Guatemala Crisis. Norman (OK) – Oklahoma City, 1992; Death Squads in Global Perspective: Murder with Deniability. L., 2003; *Wilkinson D.* Silence on the Mountain. Stories of Terror, Betrayal, and Forgetting in Guatemala. Durhan (NC), 2004; *McCoy A.W.* A Question of Torture: CIA Interrogation, from the Cold War to the War on Terror. N.Y., 2006.

12 *Анатолий Ализар* «Глобальная облава: 414 доменов Tor конфисковано» http://xakep.ru/operation-onymous/

13 *James Cook* «FBI Arrests Former SpaceX Employee, Alleging He Ran The Deep Web Drug Marketplace Silk Road 2.0» http://www.businessinsider.com.au/fbi-silk-road-seized-arrests-2014-11/. *Kashmir Hill* «How Did The FBI Break Tor?» https://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/

14 *Евгений Золотов* «С Тором шутки плохи: как поймали Эрика Маркеса и почему не слышно критиков РПЦ» https://www.computerra.ru/183474/anti-tor/

15 *Aodhan O Faolain, Ray Managh* «FBI bids to extradite largest child-porn dealer on planet» https://archive.is/20130804132945/www.independent.ie/irish-news/courts/fbi-bids-to-extradite-largest-childporn-dealer-on-planet-29469402.html

16 Отчет Mozilla об этой уязвимости «Investigating Security Vulnerability Report» https://blog.mozilla.org/security/2013/08/04/investigating-security-vulnerability-report/. Статья об этом «Уведомление о критической уязвимости в Tor Browser» https://www.pgpru.com/novosti/2013/uvedomlenieokriticheskojjujazvimostivtorbrowser. Еще одна статья «Hidden Services, Current Events, and Freedom Hosting» https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting. Возможность деанонимизации с помощью этой уязвимости описана в статье *Dan Auerbach* «Tor Browser Attacked, Users Should Update Software Immediately» https://www.eff.org/deeplinks/2013/08/tor-browser-attacked-users-should-update-software-immediately. *Владислав Мещеряков* «Арест детского порнографа уронил половину секретного интернета» http://www.cnews.ru/top/2013/08/05/arest_detskogo_pornografa_uronil_polovinu_sekretnogo_interneta_537958

17 *Kevin Poulsen* «FBI Admits It Controlled Tor Servers Behind Mass Malware Attack» https://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/

18 См. ссылку в сноске 12. Также есть статья *Benjamin Weiser, Doreen Carvajal* «International Raids Target Sites Selling Contraband on the Dark Web» https://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html

19 Сведения проекта Tor о возможных объяснениях крупной деанонимизации представлены в статье «Thoughts and Concerns about Operation Onymous» https://blog.torproject.org/thoughts-and-concerns-about-operation-onymous/

20 См. ссылку в сноске 19

21 См. ссылку в сноске 19

22 *Ivan Pustogarov* «Deanonymization techniques for Tor and Bitcoin» https://crypto.stanford.edu/seclab/sem-14-15/pustogarov.html. *Alex Biryukov, Dmitry Khovratovich, Ivan Pustogarov* «Deanonymisation of clients in Bitcoin P2P network» https://arxiv.org/abs/1405.7418

23 См. ссылку в сноске 19

24 Сведения о захвате узлов Tor правительственными агентами https://lists.torproject.org/pipermail/tor-dev/2014-November/007731.html

25 Об этом говорится в статье «Tor security advisory: "relay early" traffic confirmation attack» https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack/. *Ed Felten* «Why were CERT researchers attacking Tor?» https://freedom-to-tinker.com/2014/07/31/why-were-cert-researchers-attacking-tor/

26 См. ссылку в сноске 19

27 Обо всем этом говорится в статье «Американские исследователи взломали сеть Tor и передали результаты ФБР» https://lenta.ru/news/2016/02/25/torhacked/. *Владимир Тодоров* «Все хакеры делают это. Почему секс-скандал с разработчиком Tor угрожает всем любителям анонимности» https://lenta.ru/articles/2016/06/14/sexytor/

28 См. ссылки в сноске 27. Также об этом говорится в статье «ФБР заподозрили в выплате миллиона долларов за методику деанонимизации Tor» https://lenta.ru/news/2015/11/12/tor/

29 См. ссылку в сноске 19

30 Тем, кто прислушивается к конспирологам, имеет смысл посмотреть видео на youtube-канале Объективный взгляд «Критика конспирологии. 5 способов опровергнуть любой заговор» https://www.youtube.com/watch?v=sHItQmw9YUo. В нем показана принципиальная несостоятельность конспирологических построений. Также, чтобы понимать те проблемы человеческого мышления, которые и порождают ошибки, и для минимизации влияния которых и был выработан научный метод, имеет смысл ознакомится с роликам на все том же youtube-канале Объективный взгляд «Что заставляет нас ошибаться? Когнетивные искажения» https://www.youtube.com/watch?v=0HT4dyQkacQ, роликом на все том же youtube-канале Объективный взгляд «Логические ошибки» https://www.youtube.com/watch?v=waOfZhKF270, а также с роликом на youtube-канале Utopia Show «Ошибка техасского стрелка. Как узнать правду?» https://www.youtube.com/watch?v=1iYBzkGLQDM