**Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Всероссийский государственный университет юстиции»**
(РПА Минюста РФ)

Юридический факультет

Кафедра информационного права, информатики и математики

Творческая работа
«Анонимность в интернете»

Выполнил студент
1 курса 13 группы
очной формы обучения
Поляков Дмитрий

Научный руководитель
Крылов Г.О.

Москва 2016

Оглавление

Предисловие

Когда заходит речь о сетевой безопасности, большое внимание следует уделить всему, что касается анонимности в интернет. В сознании среднестатистического пользователя интернета бытует следующее мнение: «для чего мне озадачиваться вопросами анонимности? Я ведь не совершаю никаких противоправных поступков, пусть об этом беспокоятся хакеры…» однако, давайте задумаемся, насколько комфортно вы бы себя чувствовали, если бы любой прохожий на улице знал где вы проживаете. Кто-то из них наверняка начал бы следить за вами и, несомненно, постарался бы проникнуть к вам домой. Думаю, что такое положение дел уж точно никому не должно понравиться. Так почему проблеме анонимности в интернет придают так мало значения? Ответ прост - это пользовательская неграмотность и как с любой неграмотностью с ней нужно бороться.

https://yandex.ru/images/search?text=%D0%B0%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%BD%D0%BE%D1%81%D1%82%D1%8C%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5&img_url=http%3A%2F%2Fwww.sostav.ru%2Farticles%2Frus%2F2012%2F18.09%2Fnews%2Fimages%2Fx5s0payf.jpg&pos=12&rpt=simage

Анонимность - сокрытие реальной идентичности, “паспортных данных”. Явление, широко распространенное в интернете.

28 Мая 2015 года совет по правам человека ООН предоставил отчет заседания, посвященного анонимности и шифрованию в интернете, в котором сделан вывод, что возможность анонимного использования интернета и шифрование личных данных коммуникации необходимы и должны расцениваться как часть прав человека.

23-я статья Конституции РФ:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. **Ограничение этого права допускается только на основании судебного решения.**

Согласно **п. 4 ст. 6 федерального закона № 149-ФЗ** *вы можете предпринимать меры по защите информации* и защищать свои права в случае незаконного получения информации – ведь попытка узнать, какие сайты вы посещаете, это и есть незаконное получение информации, поскольку разрешения на получение такой информации, скорее всего, у злоумышленника нет

Требование не использовать средства анонимизации и шифрования трафика может быть расценено как нарушение **п. 8 ст. 9 федерального закона № 149-ФЗ**:

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

На основании перечисленных правовых актов использование средств анонимизации и шифрования трафика не является незаконным в рф

Анонимность в интернете

https://yandex.ru/images/search?text=%D1%81%D0%BB%D0%B5%D0%B6%D0%BA%D0%B0%20%D0%B2%20%D1%81%D0%B5%D1%82%D0%B8&img_url=http%3A%2F%2Fstatic8.depositphotos.com%2F1005669%2F1005%2Fi%2F950%2Fdepositphotos_10052412-Lens-scanning.jpg&pos=7&rpt=simage

Каждый час тысячи пользователей ищут и находят самую разнообразную информацию. Однако, пользуясь Интернетом в своих личных целях, все они оставляют определенные данные о себе. Эти данные можно использовать для полного или частичного определения личности.

Обычно выход в сеть не обходится без получения, а затем предоставления **IP-адреса**. Это, фактически, номер, по которому Вы определяетесь, как пользователь интернета, и любое действие в сети привязано к этому номеру.

Кроме того, распространена слежка через поисковые системы.

К чему может привести открытость в сети?

Имея на «руках» IP-адрес, можно деанонимизировать его – получить информацию о владельце данного IP.

С какой целью собирают такие данные?

1.Самая распространенная на сегодня цель – сбор пользовательской статистики. Сбор осуществляют специальные программы, через которые в дальнейшем определяется местоположение пользователя и некоторые другие данные;

2. Менее распространенная цель – сбор информации о противоправных действиях. Правоохранительные органы, в частности, имеют право запрашивать персональные данные у провайдеров Интернета;

3. Простая цель – интерес со стороны частых лиц. Это так называемое профилирование – когда активность интернет-данных (в нашем случае это IP) логически соотносят к определенному псевдониму (например, адресу электронной почты или никнейму в социальной сети).

4. Мошенническая цель – внезапно можно обнаружить, что кто-то украл деньги с Вашей банковской карты или электронного счета. И единственное, что изначально знал злоумышленник – это IP-адрес.

Что может узнать по IP простой пользователь?

Сегодня достаточно просто узнать информацию о владельце IP. Это, без преувеличения, каждому под силу, стоит лишь воспользоваться онлайн-сервисом, который предоставляет whois-данные.

С помощью таких сайтов можно получить имя человека, которому выдан данный IP, его e-mail, а в некоторых случаях даже телефон и физический адрес. Чуть сложнее, но вполне возможно, «подсмотреть», какие порты открыты на устройстве с этим IP (если владелец адреса находится online). Делается это специальными сканерами портов, которые могут показать и другую информацию о компьютере и о пользователе.

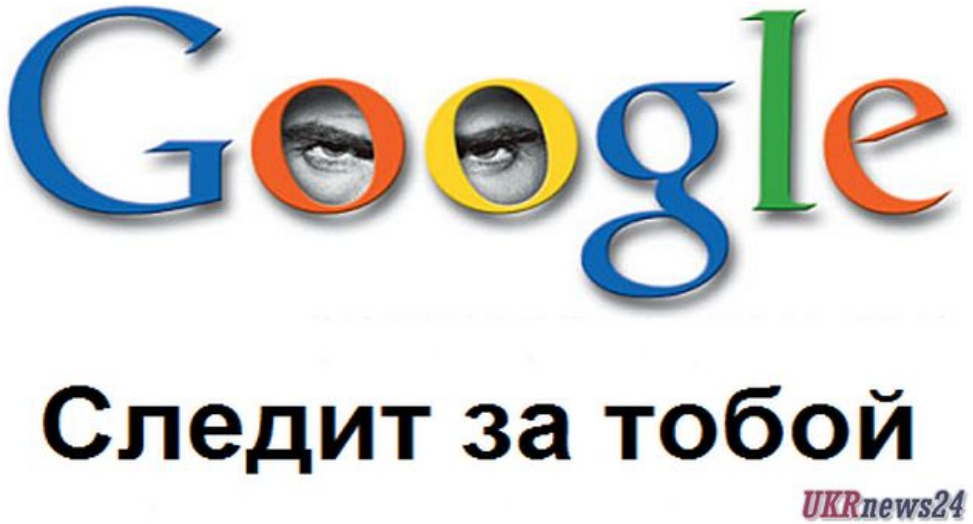
Анонимный поиск в интернете

Браузер — ваше окно в интернет. Многие данные утекают и собираются именно через него. Сайты, которые вы посещаете, могут делиться информацией между собой посредством оставления у вас различных **куки-файлов** (это лежит в основе таргетированной рекламы, когда вам показывают автомобили, если вы любите ходить, например, на автомобильные сайты)

Практически любой поисковик собирает о вас информацию: что вы ищете, в какое время, с какого компьютера, в каком браузере и так далее

Можно с точностью сказать, что в гугл хранятся более-менее подробные профили 1,5-2 млрд человек:

- пол;
- возраст;
- родной язык;
- место жительства;
- имя и фамилия;
- дата рождения;
- интересы, хобби;
- история работы;
- где и как вы проводите свободное время;
- родственные, семейные связи и так далее…



https://yandex.ru/images/search?text=%D0%B3%D1%83%D0%B3%D0%BB%20%D1%81%D0%BB%D0%B5%D0%B4%D0%B8%D1%82&img_url=http%3A%2F%2Fpimg.mycdn.me%2FgetImage%3FdisableStub%3Dtrue%26type%3DVIDEO_S_720%2

Cookies

https://yandex.ru/images/search?text=%D0%BA%D1%83%D0%BA%D0%B8&img_url=http%3A%2F%2Fhappymylife.ru%2FphotoDB.ashx%3Ftype_img%3Dnews%26w%3D848%26h%3D276%26items%3D31491f05-1d34-48ab-bc5c-ef5aacf84ac5&pos=16&rpt=simage

Куки-файлы — это файлы текстового формата. Поначалу они выполняли только полезные функции и предназначались для сохранения рабочей информации о пользователях интеренет-ресурса. Например, посещал ли пользователь ранее данный ресурс. Но, чтобы не перегружать этой информацией сервера компании, куки сохраняются на жестком диске ПК самого пользователя. Позже куки стали использоваться для фиксации всей информации, т.е для шпионажа.

Анонимные сети

Анонимные сети — компьютерные сети, созданные для достижения анонимности в Интернете и работающие поверх глобальной сети.

Оверлейная сеть (*Overlay Network*) — общий случай логической сети, создаваемой поверх другой сети. Узлы оверлейной сети могут быть связаны либо физическим соединением, либо логическим, для которого в основной сети существуют один или несколько соответствующих маршрутов из физических соединений. Примерами оверлеев являются сети **VPN** и **одноранговые сети**, которые работают на основе интернета и представляют собой «надстройки» над классическими **сетевыми протоколами**, предоставляя широкие возможности, изначально не предусмотренные разработчиками основных протоколов.

Сетевой протокол — набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Маршрутизация (*Routing*) — процесс определения маршрута следования информации в сетях связи.

Уровни стека TCP/IP

Распределение протоколов по уровням модели TCP/IP

1	**Прикладной** (Application layer)	напр., **HTTP**, RTSP, FTP, DNS
2	**Транспортный**(Transport layer)	напр., **TCP**, UDP, SCTP, DCCP *(RIP, протоколы маршрутизации, подобные OSPF, что работают поверх IP, являются частью сетевого уровня)*
3	**Сетевой**(Internet layer)	Для TCP/IP это **IP** *(вспомогательные протоколы, вроде ICMP и IGMP, работают поверх IP, но тоже относятся к сетевому уровню; протокол ARP является самостоятельным вспомогательным протоколом, работающим поверх канального уровня)*
4	**Канальный**(Link layer)	Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM и MPLS, физическая среда и принципы кодирования информации, T1, E1

Прокси-сервера

https://yandex.ru/images/search?text=%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8%20%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%B0&img_url=http%3A%2F%2Fimages.techpuffs.com%2F2012%2F02%2Fworking-module-of-a-proxy-server.jpg&pos=10&rpt=simage

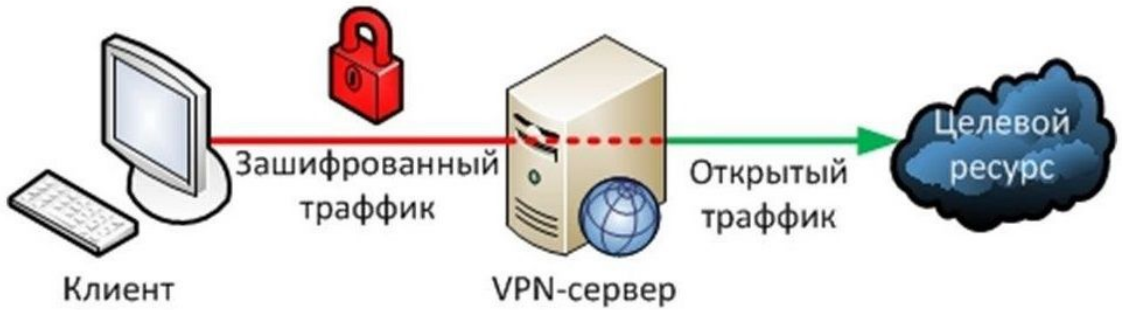
Когда вы набираете в строке браузера какой-нибудь адрес, то сначала
запрос отправляется на сервер DNS, который преобразует строку символов в набор из 32 нулей и единиц–IP адрес, использующийся для маршрутизации.

Зная этот адрес, злоумышленник может выведать персональные данные пользователя. Как себя защитить?

Для начала можно попробовать спрятаться с помощью прокси-сервера,
который является как бы посредником между компьютером пользователя и серверами Сети. Главный «предатель» — это IP адрес. **Прокси-сервер** отправляет запросы на веб-сервера как бы от себя. И он сам получает всю ответную информацию.

Подавляющее большинство прокси-серверов в своих запросах передают в специальном поле IP-адрес конечного пользователя.
Канал передачи данных от пользователя к прокси-серверу не зашифрован.

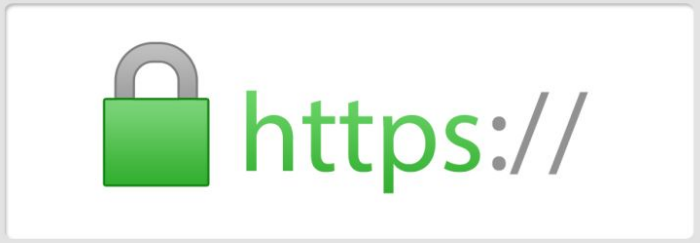
VPN



https://yandex.ru/images/search?text=vpn&img_url=http%3A%2F%2Fwww.anti-malware.ru%2Ffiles%2Fadm%2F01_32.png&pos=26&rpt=simage

В отличие от прокси-серверов, VPN (виртуальные частные сети) создают зашифрованные туннели между сервером и вашим компьютером. Вы должны иметь в виду, что правительство или ваш провайдер имеет необходимые средства для определения сервера VPN, к которому вы подключены, но не более того. Ваш IP адрес и действия остаются скрытыми шифрованием.

Как уже было сказано, серверы VPN имеют возможность отслеживать вашу активность в Интернете. Хороший VPN-сервис стремится избегать регистрации деталей. Само собой разумеется, что компрометирование деятельности пользователя в первую очередь вредит самой сети VPN.



https://yandex.ru/images/search?text=https&img_url=http%3A%2F%2

HTTPS (*hypertext transfer protocol secure*) — расширение протокола **HTTP**, для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов **SSL** или **TLS**.

Протокол был разработан компанией Netscape communications для браузера Netscape navigator в 1994 году. **HTTPS** широко используется в мире и поддерживается всеми популярными браузерами

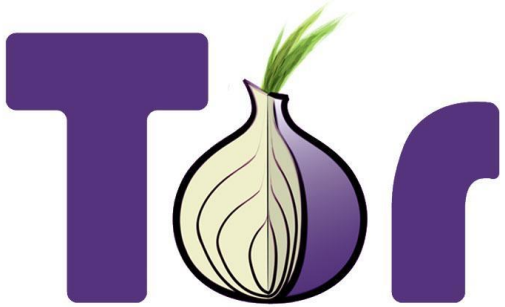
HTTPS не является отдельным протоколом. Это обычный **HTTP**, работающий через шифрованные транспортные механизмы **SSL** и **TLS**. Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от **снифферских** атак и атак типа **man-in-the-middle**, при условии, что будут использоваться шифрующие средства и *сертификат сервера проверен и ему доверяют*.

На 28 июня, 2016, **10,2 % сайтов** из списка «Alexa top 1,000,000» используют протокол **HTTPS** по умолчанию.

Схема работы HTTPS

https://yandex.ru/images/search?text=%D1%81%D1%85%D0%B5%D0%BC%D0%B0%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B%20https&img_url=https%3A%2F%2Fsambuca.ru%2Fwp-content%2Fuploads%2F2016%2F07%2Fkak-rabotaet-ssl.jpg&pos=4&rpt=simage

TOR browser.



https://yandex.ru/images/search?text=%D1%82%D0%BE%D1%80%20%D0%B1%D1%80%D0%B0%D1%83%D0%B7%D0%B5%D1%80&img_url=https%3A%2F%2Fotvet.imgsmail.ru%2Fdownload%2F81146252_39a6e8dbc5a2e2ab429ec38ead7e3bf5_800.jpg&pos=2&rpt=simage

Tor (*The Onion Router)*[*— свободное и открытое программное обеспечение для реализации второго поколения так называемой* ***луковой маршрутизации****. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде****.***

С помощью **Tor** пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол **TCP**. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов — узлов. Технология **Tor** также обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом. С помощью этой сети можно обеспечить анонимное использование **Bitcoin**.

Схема работы TOR

В основе лежит распределенная система узлов — так называемых **нод**, между
которыми в зашифрованном виде передаются данные.

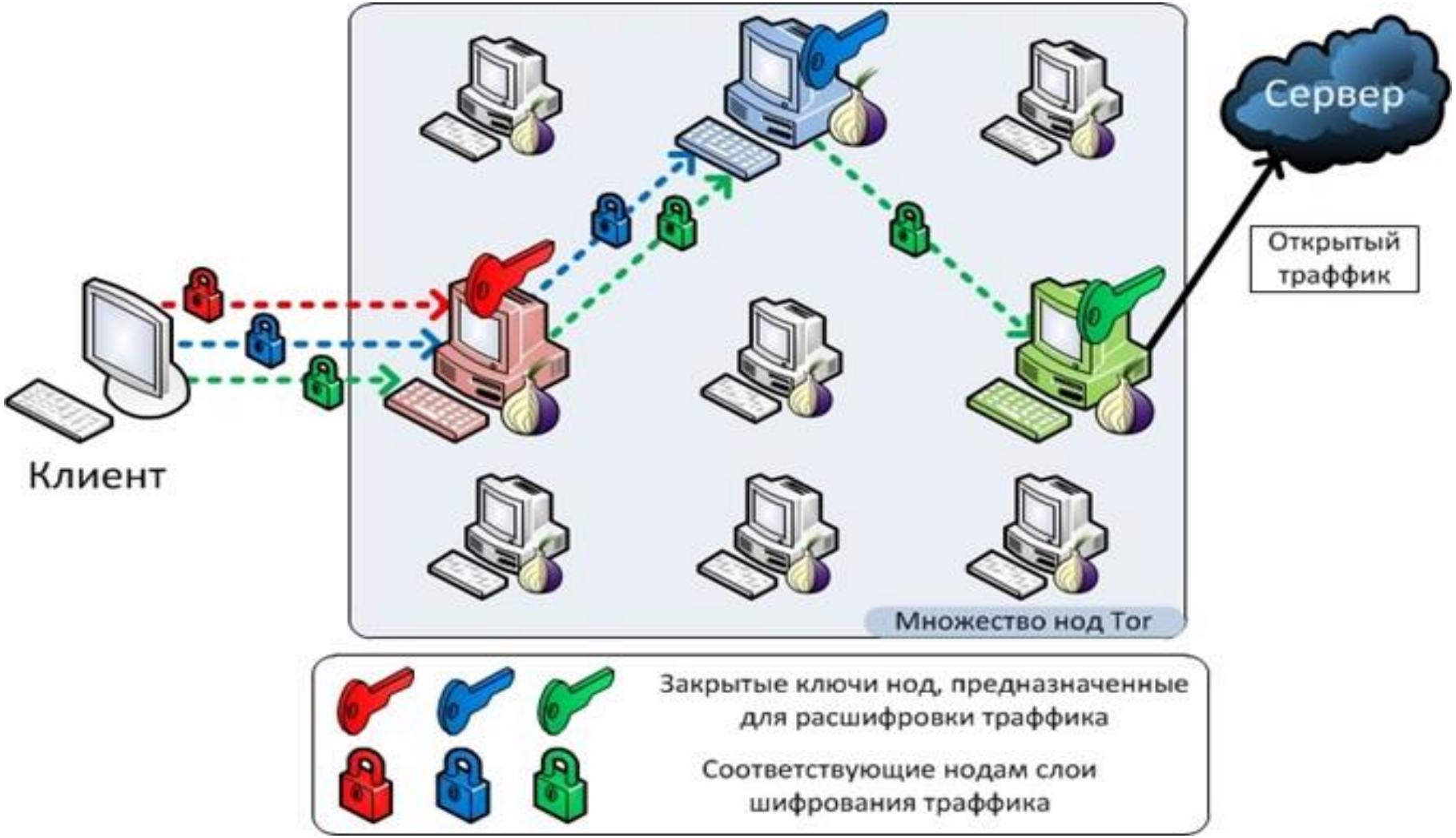
Для соединения обычно используется три сервера, которые образуют временную цепочку. Каждый сервер выбирается случайным образом, при этом он знает только то, от какого звена получил данные и кому они предназначаются.

Мало этого — цепочки постоянно меняются. Даже в случае перехвата данных на одном из серверов отследить полный маршрут пакетов (в том числе и их отправителя) не представляется возможным.

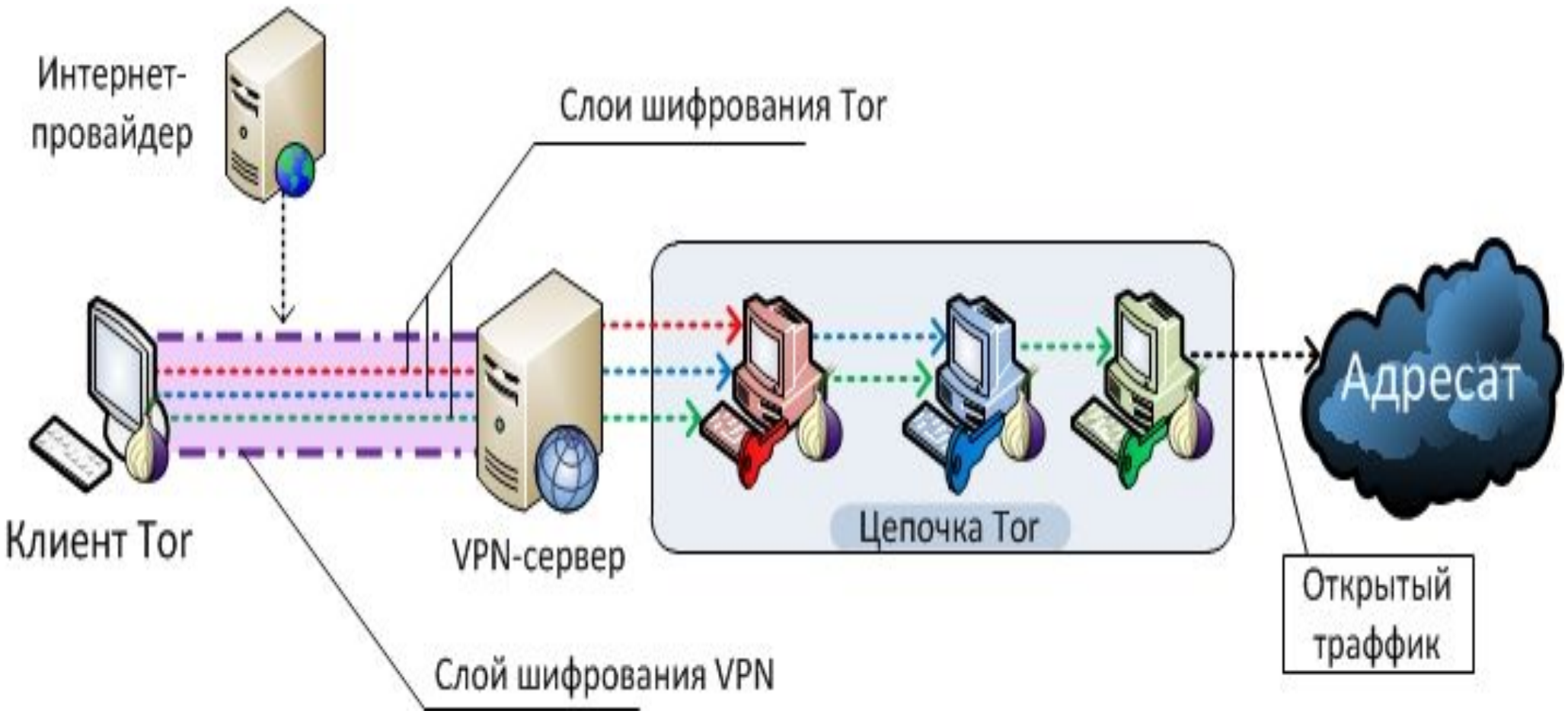
Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьей ноды, потом для второй и, в конце концов, для первой.

Когда первая нода получает пакет, она расшифровывает «верхний» слой шифра и узнает, куда отправить пакет дальше. Второй и третий сервер

Схема работы тор браузера

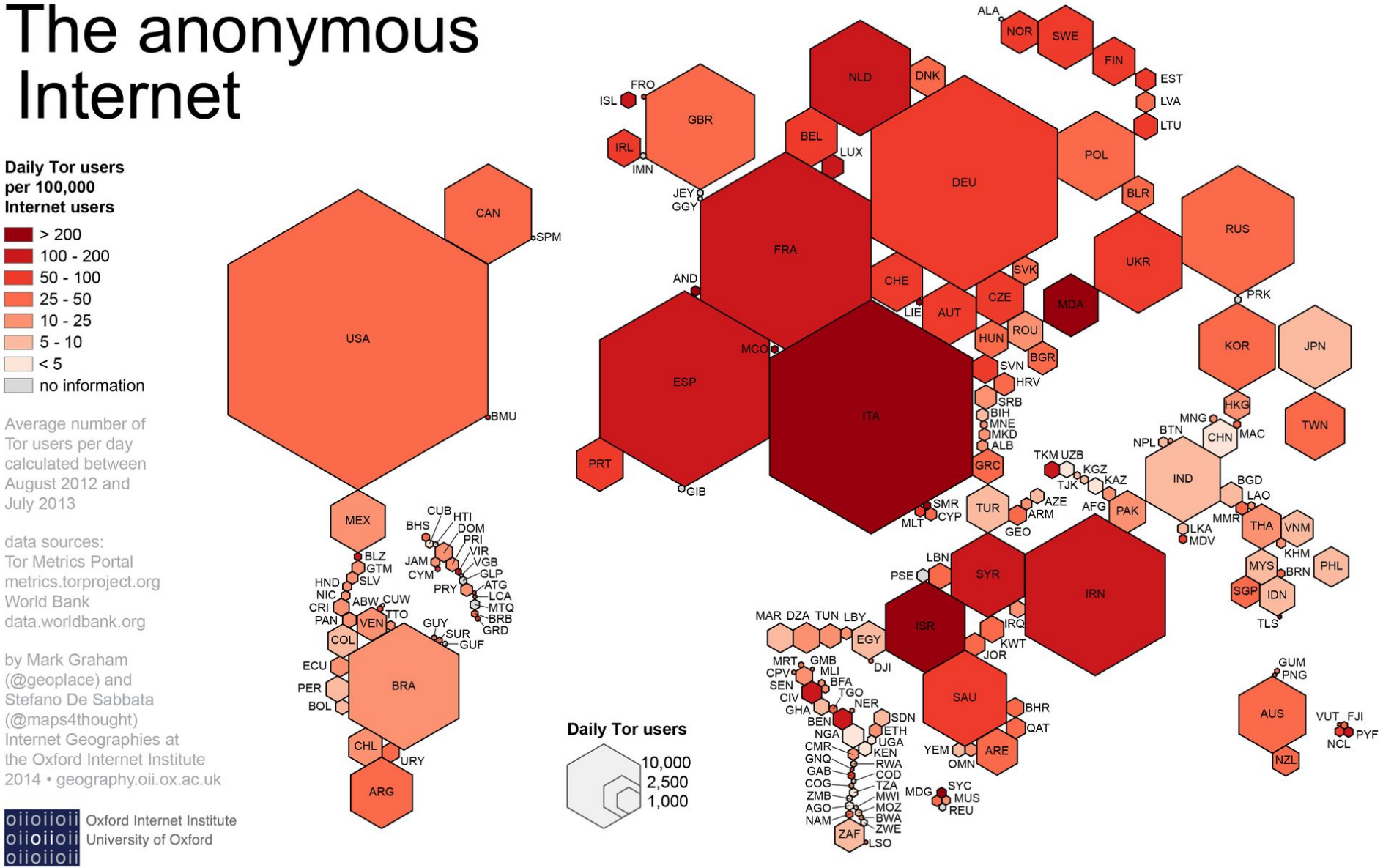


https://yandex.ru/images/search?text=%D1%81%D1%85%D0%B5%D0%BC%D0%B0%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B%20%D1%82%D0%BE%D1%80%20%D0%B1%D1%80%D0%B0%D1%83%D0%B7%D0%B5%D1%80%D0%B0&img_url=https%3A%2F%2Fcryptoworld.su%2Fwp-content%2Fuploads%2F2016%2F01%2Fm4Jq1s7.jpg&pos=5&rpt=simage

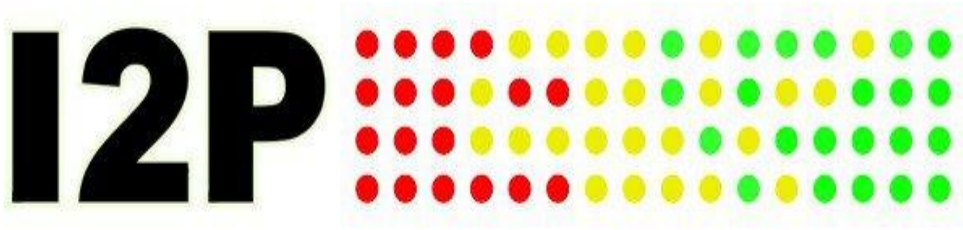


https://yandex.ru/images/search?text=%D1%81%D1%85%D0%B5%D0%BC%D0%B0%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B%20%D1%82%D0%BE%D1%80%20%D0%B1%D1%80%D0%B0%D1%83%D0%B7%D0%B5%D1%80%D0%B0&img_url=https%3A%2F%2Fcryptoworld.su%2Fwp-

The anonymous Internet



https://ru.wikipedia.org/wiki/Tor#/media/File:Geographies_of_Tor.png



https://yandex.ru/images/search?text=i2p&img_url=http%3A%2F%2Fblf81.com%2Fdata%2F56c979a8281f7.jpg&pos=4&rpt=simage

I2P (***invisible internet project, IIP, I^2P)*** — проект, начатый с целью создания анонимной компьютерной сети, работающей поверх сети интернет.

Сеть **I2P** является оверлейной (то есть, работающей поверх другой сети — сети интернет), устойчивой (отключение узла не повлияет на функционирование сети), анонимной (невозможно или трудно определить IP-адрес узла). При передаче данных между узлами сети применяется шифрование.

Внутри сети **I2P** можно разместить любой сервис (или службу) (форум, блог, файлообменник, электронную почту, систему для мгновенного обмена сообщениями (чат), систему для совместного использования файлов и т. д.) с сохранением анонимности сервера.

Как работает I2P

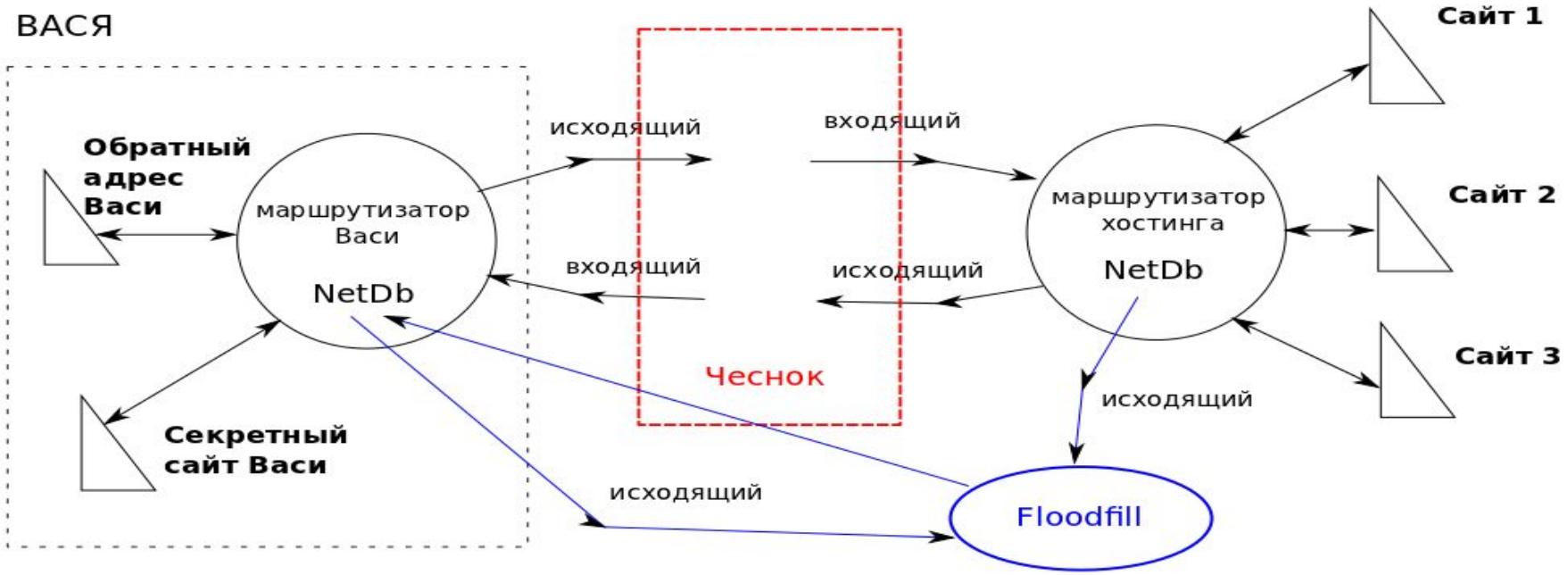
Сеть **I2P** состоит из узлов двух видов: маршрутизаторы, имеющие помимо **I2P**-адресов обычные **IP**-адреса и видимые в обычном интернете, и узлы, находящиеся позади маршрутизаторов и собственных IP-адресов не имеющие, — они и образуют тот самый «невидимый интернет».

Floodfill-маршрутизаторы служат своего рода «досками объявлений», куда узлы публикуют информацию о себе и куда приходят запросы клиентов. Во избежание подделки данные подписываются ключом, входящим в адрес.

Весь трафик в сети шифруется от отправителя до получателя. В сумме при пересылке сообщения используется четыре уровня шифрования (сквозное, **чесночное**, туннельное, а также шифрование транспортного уровня)

Каждое сетевое приложение на компьютере строит для себя отдельные шифрованные, анонимные туннели

Схема работы I2P



https://xakep.ru/2014/09/04/i2p-secrets/

https://yandex.ru/images/search?text=%D0%B1%D0%B8%D1%82%20%D1%82%D0%BE%D1%80%D1%80%D0%B5%D0%BD%D1%82&img_url=http%3A%2F%2Fwww.filecluster.com%2Fnews%2Fwp-content%2Fuploads%2F2013%2F12%2Fbittorent.png&pos=1&rpt=simage

ANts P2P — файлообменная сеть, анонимизирующая весь поток данных, используя систему маршрутизации, в которой, в отличие от **BitTorrent**, участники обмениваются трафиком не напрямую, а через несколько узлов.

Каждому участнику известен только IP-адрес его непосредственного соседа. Таким образом, отправитель не знает, куда идет его файл, а получатель не знает, откуда он пришёл.

Для большей безопасности данные между отдельными отправителями и получателями шифруются по симметричному алгоритму .

Существуют также системы, анонимизирующие систему **BitTorrent**, такие как **Anomos, Torrentprivacy, Tribler и т.д.**

Заключение

— При использовании стандартного браузера отключать все сторонние плагины;

— Отключать в браузере использование Cookies, ведение истории и кэширование;

— В режиме анонимности не заходить на деанонимизирующие Вас сайты (например, в социальные сети или публичные сервисы);

— Не использовать непроверенные приложения;

— В серфинге через открытые точки Интернета не использовать личные данные, а также данные Ваших денежных средств;

— Регулярно менять цепочки (TOR) или узлы (VPN и прокси-серверы).

В заключение, хотелось бы сказать, что технические средства – это лишь малая составляющая анонимности в Интернете. Однако, перечисленных в данной работе методов анонимности вполне достаточно, чтобы значительно усложнить задачу потенциальным недоброжелателям.

Библиографический список

1. https://habrahabr.ru/post/173461/
2. https://xakep.ru/2015/11/12
3. https://whoer.net/blog/anonimnost-v-internete/
4. https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8
5. http://antsp2p.sourceforge.net/
6. http://www.rusblock.com/2012/10/i2p.html
7. https://ru.vpnmentor.com/blog/%D0%BF%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D0%B8%D0%BB%D0%B8-vpn-%D0%B2-%D1%87%D0%B5%D0%BC-%D1%80%D0%B0%D0%B7%D0%BD%D0%B8%D1%86%D0%B0/
8. http://www.comss.ru/page.php?id=2468
9. http://www.spy-soft.net/tribler-tor-anonimnost-v-seti-bittorrent/
10. http://www.pearsonhighered.com/educator/academic/product/0,,0321497708,00%2ben-USS_01DBC.html