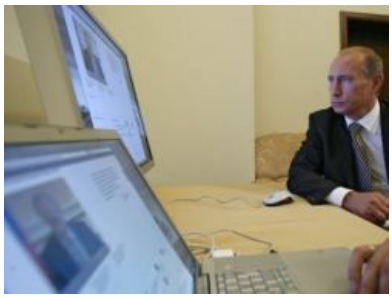
# Идентификация пользователей в интернете — Lurkmore

«Мы еще мало знаем о вас »

*— Эрик Шмидт, исполнительный директор Google*

**Идентификация пользователей в интернете** — множество методов узнать о пользователе *всё* из открытых и полуоткрытых источников в интернете.



Агент бдит.

## Вступление

«Если у тебя паранойя, это не значит, что за тобой никто не следит »

*— Курт Кобейн*

Попался, оппозиционер!

Пользуясь интернетом, человек оставляет о себе огромное количество информации. Возможно, в этом не было бы ничего плохого, если бы все были пророками и знали, как, кому и каким боком она потом выйдет. Но пока связь с астралом не налажена, неплохо было бы остановиться и оглядеться: а все ли я так делаю? У рядового пользователя интернета может сложиться обманчивое впечатление собственной анонимности во всемирной сети. Так вот, первое, что нужно уяснить — оно ложно! Если бы Оруэлл жил в наше время, он бы с ума сошел от паранойи. А причина одна — да-да, она самая. Печальнее всего, что пользователи сами убили малейший намек на анонимность в сети, и стоит ей хотя бы попытаться поднять голову, как люди тут же вгоняют анонимности новый осиновый кол в грудь.

## Общие сведения

«Учителя никогда не скажут вам, что невозможно жить, передвигаться, совершать какие-либо действия, не оставляя крошечных, ничтожных на первый взгляд, но неуничтожимых следов информации о личности каждого человека. Следов, которые можно извлечь, собрать, усилить… »

*— Уильям Гибсон, «Джонни Мнемоник»*

Следует разделить информацию о пользователе в сети на две неравные категории: то, что он оставляет сам, и то, что о нем без лишнего шума доносят программы. И стоит ли удивляться, что большую часть информации о себе пользователь выкладывает добровольно и безо всякого принуждения — а самое лучшее досье то, которое человек пишет о себе сам. Да-да, первая мысль про Контактик, Твиттер и Фейсбук была абсолютно верной. И если добавить к этому, что данные в них никуда не денутся из кэша поисковых систем и интернет-архивов, а все ваши сообщения, написанные сейчас, можно будет прочитать и через 5 лет, и через 40 лет, то становится страшно. Притом прочитать смогут не абстрактные сотрудники спецслужб, а все желающие. Мы живем в стеклянной клетке, которую сами и построили.

### Мобильные телефоны следят за Вами, сэр!

Кулхацкер в сериале про Мухтара
Всё что нужно — консоль Windows.

Как известно, Ричард Столлман не пользуется мобильным телефоном, чтобы всякие службы не могли отслеживать его перемещения на улице и вообще везде. В этом большой смысл, если вы Усама бен Ладен и много лет шифруетесь от ЦРУ, не имея телефона, или Джохар Дудаев, частоты вашего спутникового телефона известны ФСБ, и по звонку к вам прилетит самонаводящаяся ракета (пруфы ищите сами). Однако, для рядового гражданина с GSM-телефоном позиционирование — не самое страшное. Но обо всем по порядку, и начнем

с упомянутого позиционирования.

Политики конфиденциальности.

**Позиционирование**. Приблизительное определение местоположения включенного сотового телефона. Учитывая, что телефон не сам по себе левитирует, а лежит в кармане, то и местоположение пользующегося им человека известно. Используются две базовые методики: с помощью позиционирования относительно базовых станций и с помощью встроенного в телефон GPS (если он есть, а он есть в подавляющем числе смартфонов). Погрешность в случае первого метода в сетях GSM составляет около 100 метров (по расстоянию от вышки), а с учетом непредсказуемой городской застройки — то и более. Вообще говоря, возможность позиционирования в сетях GSM предусмотрена технологией разделения полосы пропускания по времени, и является побочным эффектом. Позиция телефона определяется как расстояние от базовой станции и направление секторной антенны, с которой он работает в данный момент. Что дает возможное положение абонента в виде урезанного сектора со стороной в сотню-другую метров. На этом принципе работает «ребенок под присмотром» от МТС, огорчая школьников, прогуливающих пары. Услуга от МТС, тащемто, должна исключать позиционирование человека, не давшего согласие, но если у тебя есть хороший знакомый в каком-нибудь опсосе, то он сможет навести на чувака, который держит у себя твой украденный и включенный мобильник.

Второй метод (GPS) дает точность от 5 до 50 метров, что уже довольно неплохо. Всегда можно проверить, насколько ваше размещение соответствует действительности, зайдя со смартфона на Google Maps (у автора чаще всего ошибка составляет метров 15). Более подробно об этом можно почитать тут.

**Прослушка** — следует определиться, чьей прослушки ты опасаешься. Если компетентных служб, то опасения вполне оправданы (СОРМ). По вполне достоверным данным ребята из ФСБ имеют договоренность с операторами мобильной связи и могут прослушать любой номер. А вот если вы опасаетесь кул-хацкеров с самопальными устройствами для перехвата и расшифровки на лету сигнала в GSM-сети, то тут можно успокоиться — на данный момент полноценного рабочего прототипа нет. Но работы ведутся, подробнее здесь.

Следует сказать, что в статье ниже речь идёт о телефонах на предустановленном Android, который отличается от открытого оригинала наличием предустановленного рекламного-шпионского софта. Часто на хорошие популярные модели есть возможность установить CyanogenMod или другую прошивку без встроенных шпионов, в том числе собранную самому. Правда китайские производители, бывает, не желают делиться исходным кодом, а выпросить закрытые бинарные драйвера у большинства, вообще всех, производителей сложно (за исключением Samsung, Google, Sony Ericsson и может ещё кого, у которых они в открытом доступе). Хотя некоторые производители выпускают и Android телефоны с «чистыми» прошивки вроде CyanogenMod, но это редкость и цена у них в примерно 4 раза выше.

До сих пор речь шла про обыкновенные телефоны. А сейчас следует перейти к самому интересному — Андроиду, Айфонам и прочим иже с ними. Вообще, мобильные телефоны радикально изменили правила игры — и Google с Apple это отлично понимают. Тот, кто будет контролировать рынок мобильных, будет контролировать будущее. Чем умнее телефон, чем больше в нем полезных и удобных функций, тем больше данных он отправляет о тебе фирме-производителю. И не только о тебе — задача умных телефонов индексировать и отправлять на сервера максимально возможное количество данных об окружающем мире. Вот только часть примеров.

**Skyhook** — это база данных на более чем 100 миллионов wi-fi точек по всему миру с их географическими координатами. С точностью до 20 метров, кстати. А пополняется она следующим образом — если вы желаете зайти с телефона по wi-fi на Google Maps, то ваш телефон проводит сканирование, узнает ssid и mac-адрес не только той точки, к которой вы подключаетесь, но и всех близлежащих и отправляет их Skyhook — партнеру Империи Добра. Зачем? Дело в том, что имея базу данных 70% wi-fi точек в США и Канаде, а так же точек во всех крупнейших городах мира, рекламодателям (Гуглу) удобнее вас отслеживать и давать адресную рекламу исходя из вашего местоположения. По крайней мере, пока — для этого.

**Гугл очки** — прекрасная, прорывная технология поиска по фотографии. Можно сфотографировать достопримечательность через телефон и тут же узнать всю информацию о ней из Гугла. А можно погуглить информацию о торговой марке, сфотографировав её логотип. Да ещё уйму чего можно сделать! Только надо понять, что если до этого у Гугла были только «уши», через которые он читал набиваемые тобой ему запросы, то сейчас появились и «глаза». А учитывая вездесущую привязку GPS, то Гугл знает где ты, на что смотришь и что хочешь об этом узнать. И, скорее всего, Гугл очки найдут применение не только в мобильных телефонах, да и сам функционал серьезно расширится и так удобно интегрируется с остальными сервисами Гугл, что не пользоваться им будет просто глупо. Ведь это же здорово — посмотреть на любой предмет и тут же узнать всю доступную информацию о нём, оглядеться на улице и увидеть имена людей, проходящих мимо, расценки в ближайшем кафе и прочее. Вот тут-то и начнётся самое веселое.

**Учетная запись Гугл** — синхронизация Android, которая, впрочем, настраивается пользователем, происходит весьма любопытным образом — все твои данные из телефона синхронизируются с аккаунтом Гугла и хранятся на сервере. Таким образом, Гугл знает твой календарь (в том числе — женский менструальный), твои контакты, твои звонки, список твоих дел, номер твоего мобильного… да всё, что ты делал с телефоном. Кстати, поговаривают, что телефоны на Андроиде делают регулярные скриншоты экрана и впоследствии отправляют на сервера Гугла — если есть владельцы Андроида с доступом к root, проверьте и отпишитесь сюда.

Но не надо думать, что Гугл — единственный, кто занимается подобными вещами. Он просто часто является законодателем моды на нарушение конфиденциальности пользователя, которую подхватывают другие. Тот же Apple делает всё то же самое, только порой взимает за это деньги (например за облачный сервис обмена данными между любыми mac-устройствами MobileMe). Ну и, конечно, что Гугл, что Эппл, благодаря возможности покупать приложения для телефона, знает номер твоей кредитной карточки.

Вообще, телефоны Android феноменальны, они полностью соответствуют ожиданиям от телефона. Если телефон от Apple — это расовый фашистский телефон (ня!), который разрешает вам делать только то, что позволил ~~Фюрер~~ Стив Джобс (если вы не сделаете джейлбрейк, конечно), то телефон Гугла, при наличии гуглоаккаунта, мягко говорит вам: «делайте что хотите, но только пожалуйста, рассказывайте мне обо всем-всем, ладно?». И этому вкрадчивому шепотку очень трудно отказать… Но только подумайте — а стоит ли делиться с транснациональной корпорацией, чья миссия «организовать мировую информацию и сделать ее общедоступной и полезной» большинством аспектов своей жизни. Да и Эппл стоило было бы знать поменьше о своих хомячках. Как этому всему противостоять? ~~Купить себе мобильный, который просто телефон, а не небольшой компьютер. Для остального лучше использовать ноутбук.~~ Не обязательно так уж переходить со смартфона на допотопный телефон, всему есть свой предел, даже вашей паранойе. А вообще, удаление всех Google сервисов и приложений с установкой сторонней прошивки меняет дело (криворуким таки рекомендуется мобильный телефон ввиду их криворукости, хотя в сети Интернет по поводу установки кастомных прошивок на конкретные модели смартфонов всё и так полностью разжёвано, даже для нуба). Юзерам iOS повезло меньше: они могут только поставить аналог root — jailbreak.

### Что же делать?

Если же пользоваться смартфоном или планшетом очень хочется, то выход есть: сразу же после покупки Android-девайса установить на него прошивку CyanogenMod, AOKP или, на худой конец, AOSP, снести к хуям все службы Google, включая Google Play (сами все сносятся при полном wipe папок data, system и cache, если сам юзер не захотел скачать себе GApps), а вместо него поставить F-Droid, который заботливо предупредит, через какие программы может произойти минимальная утечка информации. К слову, немалую долю F-Droid составляют программы специально для параноиков. Также крайне рекомендуется пользоваться файрволом, настроенным на использование белого списка. Установка MIUI не приведёт к полноценной защите от слежки, так как имеет проприетарные модули от китайцев.

Была еще Ubuntu Touch, которая кое-как пахала на некоторых ведроид-смартфонах, но проект благополучно сдох даже не родившись. Кроме того, есть устройства со вполне годной Sailfish OS, но софта под неё чуть более, чем нихуя.

## И браузеры тоже!

«Если ты куда-то что-то написал, то твой IP там наверняка есть. Отследить человека вполне реально, муторно, но если надо — реально. »

*— Зой*

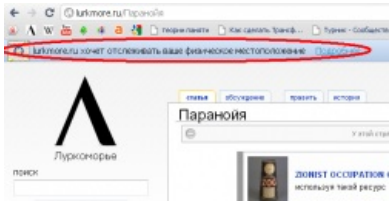
Когда-то давно для этой задачи были придуманы куки. Но, к сожалению, куки — лишь самое безобидное, с чем приходится сталкиваться пользователю, желающему сохранить анонимность в интернете.

**Дополнения в браузере** — с недавних пор рекламщики и агенты ZOG начали нагло скупать дополнения (расширения) к браузерам у их авторов и встраивать туда сбор статистики. Это не противоречит политике компаний-производителей браузеров, на странице дополнения честно появляется сообщение со списком собираемого. До этого все ограничивалось самовольной установкой Яндекс/Яху/Гугл/Bing.Бар'ами (от всех поисковиков и сервисов), которые пытались хоть как-то накрутить счётчик посещений своих сайтов и устанавливались вместе с «бесплатными» (здравствуй мышка, я твой сыр) программами. Но они так подзаебали пользователей, что теперь вылазит окошко, где самовольную установку таких дополнений надо подтвердить (по крайней мере в популярных браузерах). Надо сказать, что скупка пока не приняла массовый характер, чаще всего дополнение делают те, кто и будет собирать статистику.

Примером могут служить многочисленные клоны AdBlock Plus (название такое и никакое иначе, а источник adblockplus.org и никакой иной), которые используют его подписки, но при этом сами собирают статистику и продают её рекламщикам. Любые дополнения с открытым кодом абсолютно законно могут скопировать и продвигать под другим брендом с полным сбором всех посещённых вами адресов.

Что интересно, в магазине дополнений Chrome у некоторых из клонов даже имена полностью совпадали с оригиналом. С недавних пор, видимо, введён запрет на полное совпадение имён и теперь используются разные уловки вроде частичного совпадения написания названий или похожие иконки. Одно из первых сообщений о скупке

Самый известные случаи скупки: Wips.com s.r.o., BrowserProtect, ppclick



И Луркмор тоже.

**IP-адрес** (внешний ip, айпишник) — внешний ip-адрес есть у каждого компьютера в интернете, что, в целом, очевидно. И на первый взгляд идентификация с его помощью конкретного пользователя весьма затруднительна… Во-первых, существуют динамические айпишники, выдаваемые провайдером пользователю из некого диапазона адресов случайным образом при каждом новом подключении. А во-вторых, существуют сети, где множество компьютеров сидят на одном внешнем ip (да, и за прегрешения одного банят сразу всех). Предположим, что у вас все же статический белый ip и зашкаливающий градус паранойи. В таком случае, сразу ставьте Tor[1] или вливайтесь в ряды I2P[2]. Но сложности с идентификацией существуют только на первый взгляд. Если присмотреться внимательнее, то можно понять, что даже с помощью динамического айпишника можно определить страну и провайдера пользователя (и расколоть его — с уважением, куратор ZOG). Ну а это уже сужает круг поиска. Если вас это смущает, то для фальсификации в логах сервера своего ip без помощи Tor'а в Огнелисе существует дополнение, заставляющее поверить сервер, что ваш истинный внешний айпишник — всего лишь прокси, за которым скрывается «настоящий» ip (из произвольного диапазона, задаваемого в настройках).

**Cookies** (HTTP cookies) — пожалуй, самый известный общественности метод идентификации в интернете. Он работает следующим образом. Когда пользователь совершает свой первый http-запрос к сайту (перед названием сайта неспроста ставится `http://`), он получает от сайта куки — фрагменты данных, которые браузер сохраняет в виде файла (у осла, остальные используют более продвинутые методы хранения). Эти данные являются своего рода удостоверением личности пользователя на данном сайте и действуют до даты истечения. Как видно из названия, дата истечения указывает браузеру, когда удалить полученные куки. Как только срок хранения вышел — печеньки удаляются. Если дата не прописана — куки живут до конца сессии (например, закрытия браузера). Ну и, конечно, их можно удалить по запросу пользователя (то есть ручками). Самым интересным в плане печенек примером является, конечно же, Гугль. Империя Добра выдает куки сразу до 2020 года и искренне надеется с их помощью отслеживать запросы и переходы пользователя с сайта на сайт. Внимательный читатель в этом месте задастся вопросом — но как Гугл может следить за мной, когда я перехожу с одной страницы лурка на другую? Успокою — на лурке Гугль не отслеживает ваши метания с помощью печенек — тут у него другие методы, о которых будет упомянуто ниже. Но слежка вообще имеет место — с помощью так называемых сторонних кук. Идея в следующем — когда пользователь загружает страничку `www.example.ru`, помимо всего прочего, на ней присутствуют компоненты других сайтов — например `www.bigbrother.org`. Речь идет о картинках, баннерах и прочих элементах в духе java scripts. И вот эти-то компоненты вполне могут уговорить браузер принять куки с долгим сроком жизни от `www.bigbrother.org`. А если подобных баннеров Большого брата много на различных сайтах в интернете, то каждый сайт с ними будет узнавать ваш браузер. И всегда можно отследить, куда переходил пользователь, и что его интересует. Конечно, этим интересуются отнюдь не спецслужбы, а рекламщики (не будем вспоминать случаи, когда ФБР внедряла в компьютеры американцев свои куки). Надо же им знать на какую порнуху фапает пользователь и какой лубрикант он предпочитает — таков рекламный бизнес.

Как с этим бороться — грамотной политикой управления куками в браузере. Для Огнелиса рекомендуются это и это дополнения.

**LSO** (Local Shared Objects, flash cookies) — куки на основе flash. Основная опасность флеш кук в том, что устанавливаются они скрытно, удалить стандартными средствами браузера их невозможно и о них мало знает большинство пользователей. Бороться с ними можно в Огнелисе, установив дополнение BetterPrivacy. Не забудьте после установки порадоваться тому как насрано у вас в компьютере. Но защита будет неполной, если не запретить Adobe Flash Player сохранять LSO на жесткий диск. Для этого необходимо зайти на сайте Adobe на страницу диспетчера параметров. На вкладке «Глобальные параметры хранения» сократите до минимума разрешённый объём пространства на диске для хранения информации и запретите стороннему flash содержимому сохранять данные на компьютер. Кстати, с флеш куками связано интересное наблюдение. Если в настройках Skype запретить сохранять обычные http-куки, то он под шумок начинает сохранять LSO при каждом открытии браузера в надежде, что никто не узнает.

**Web bug** (web beacon, tracking bug, tracking pixel, pixel tag, 1×1 gif) — объект, внедряемый в веб-страницу или e-mail, невидимый для пользователя, но позволяющий определить, просмотрел или нет пользователь данную страницу/мыло. Первоначально веб баги представляли из себя пиксели 1x1, которые подгружались в страничку или почту со стороннего сайта (помните аналогию со сторонними куками?). Нынче же одними пикселами дело не ограничивается — под веб-багами подразумевается целый спектр разнообразных фич, позволяющих пеленговать пользователя (подробности в ссылках английской Википедии). В html-страницах веб-баги используются чаще всего для сбора статистики о посещаемости (в лурк их внедряет Google Analytics и LiveInternet). Гораздо интереснее дела обстоят в электронной почте — с помощью веб-багов можно не только определить какой айпишник открыл сообщение, но и кому

переслал его впоследствии).

**HTTP referer** — так называется в протоколе HTTP один из заголовков запроса клиента, позволяющий серверу определить, с какой страницы пользователь перешел на данный сайт. То есть, если был осуществлен переход с `www.hot-asian-boys.com` на `www.bigbrother.org`, то Большой брат смекнет о сексуальных предпочтениях пользователя. Данная проблема в Огнелисе решается с помощью RefControl. К сожалению, это далеко не всё. Бывают еще межсайтовые запросы — тут http-referer и web-bugs сильно перекликаются. Поясню на примере — допустим, пользователь просмотрел блог с вставленным видео с YouTube, потом глянул профили друзей на MySpace и в конце заказал книгу на Amazon. Внимание! Он ни разу не заходил на сайт Гугл, но Гугл уже знает, что за видео он смотрел и в каком блоге, какие друзья его интересовали и что за книги ему привезут. Помните, что Гугл смотрит за всеми. Всегда. Секрет в том, что на всех этих сайтах присутствуют разные компоненты Гугл: в блоге — ссылка на YouTube, принадлежащий Гугл, в MySpace — аналитика посещаемости Google Analytics, а на Amazon прописалась рекламная компания Гугл DoubleClick. И будь уверен — все переходы протоколируются и сопоставляются самыми передовыми статистическими алгоритмами, чтобы однозначно связать данные именно с тобой. Я имею ввиду фамилию, имя, отчество. Но не надо думать, что Гугл — это такое вселенское зло. Он живет от адресной рекламы и хочет знать твои интересы. И не только он — все поисковики этим грешат в меру возможностей. Просто Гугл делает это в планетарных масштабах, в отличии от того же Яндекса. Чтобы блокировать лишние запросы, существует дополнение RequestPolicy.

**Кэш браузера** — использовать кэш браузера можно различными способами. Самый простой — с помощью HTTP заголовка ETag. При обращении к странице сервер выдает ETag, который браузер использует для кэширования содержимого. При последующих запросах он отправляет этот ETag на сервер, который таким образом узнает, кто к нему пришёл. Самое приятное, что даже при перезагрузке страницы ETag не меняет значения и сервер будет тебя всё так же узнавать. Лечится с помощью NoScript.

Вообще, NoScript и AdBlock убирают массу дыр, с помощью которых ваш браузер становится единственным и неповторимым на просторах всемирной сети. С помощью NoScript вы можете управлять JavaScript, Java, Silverlight, Flash (которые стучат как дятлы по весне — тут подробнее). Без них невозможно гарантировать защиту пользователя от множества атак вроде XSS, CSRF и Clickjacking. Ну а AdBlock — это наше всё в борьбе с баннерами.

**TCP** — да, и протокол TCP тоже. Он с радостью предоставит информацию о твоей операционной системе. Дело в том, что в различных OS по-разному настроен TCP-стек. А роутер, как правило, не меняет пакет, а просто передаёт его дальше. Характеристики TCP-пакетов формируют свой фрагмент цифровой подписи. И для распознавания данных о твоей ОС проще всего применить утилиту p0f.

**Цифровой отпечаток браузера** — весьма любопытная технология, позволяющая идентифицировать браузер пользователя без всяких кук. Просто с помощью информации, передаваемой серверу — HTTP заголовков, наличия/отсутствия кук, java, javascript, flash, silverlight, по плагинам браузера и т. д. Это своего рода финальный босс, строящий уникальную цифровую подпись на основе вышеперечисленных элементов (и, вероятно, многих других), описанных в статье How Unique is Your Browser?. Притом приведённый тест ведёт всего лишь на Pantoptclick — открытый проект, созданный для защиты пользователей. И он использует небольшую часть приёмов, описанных в статье, а при этом — весьма эффективен. Реальный алгоритм может быть сложнее и гораздо (в десятки и сотни раз) эффективнее. Есть подозрение, что его-то как раз будут применять отнюдь не рекламщики, чтобы втюхать свой товар… На Pantoptclick реально довести уникальность своего браузера до 1 из 50000. Правда при этом следует учесть следующее — если вы замаскируете браузер так, что ничего невозможно будет о нем узнать, то среди прочих браузеров он будет выделяться как человек в космическом скафандре в центре густонаселенного мегаполиса. Можно попытаться замаскировать свою сборку во что-то довольно типичное с помощью User Agent Switcher, но тут главное не менять тип операционной системы. Помните — TCP докладывает о ней, и если он говорит, что у тебя Linux, а замаскированные User Agent Switcher HTTP заголовки убеждают, что Windows, то поздравляю — тебя нашли! Скорее всего, ты такой один в интернете.

**Поиск в Гугле и Яндексе** — если заглянуть в html-код страницы результатов поиска Гугла, то можно убедиться, что все найденные результаты являются не просто ссылками. Каждая ссылка результатов поиска содержит метод onmousedown, который заставляет браузер выполнить особые действия по щелчку на ссылке. В данном случае переход на нужную страницу происходит через редирект на адрес-посредник. То есть сначала браузер идёт на сервер Гугла, и только после захода туда происходит переход на нужную страницу. Переход осуществляется достаточно быстро, что незаметно на широком канале. А между тем, в Гугл попадает статистика с информацией, что ты искал и куда, в результате, пошёл. То же самое делает и Яндекс, и Яху, и многие другие поисковики. Противостоять этому можно, используя в браузере клиентские скрипты, которые приведут ссылки в правильный формат. Установи плагин к Фаерфоксу дополнение Greasemonkey и добавь в список скрипты зачистки ссылок для Гугла и Яндекса, либо аналогичного действия плагин от создателя AdBlock Plus. Полный список приложений на donttrack.us. Это единственный способ борьбы. Даже если настроить поиск Гугла, чтобы тот не сохранял историю поиска, это ни к чему не приведёт.

## Как от этого всего защититься?

Как видно, стучит буквально все[3]. Как от этого всего защититься простому не программисту? Никак, всё, что вы можете это уменьшить

риски и надеяться, что не попадетесь. Во-первых, надо понять, что любая защита не абсолютна и смириться с этим. Во-вторых, прислушаться к советам в данной статье. В-третьих, использовать Tor (о нём есть статья на лурке). В-четвертых — никогда, никогда не используйте панели от Гугла, Яндекса и прочих. Оно того не стоит — это гигантская дыра, в которую уходит всё, что только возможно, как об истории поиска, так и о компьютере в целом. Ведь ты хочешь, чтобы твоим компьютером пользовался только ты, а не маркетологи, не так ли? В-пятых, используйте Firefox (не Chrome!), для анонимности TorBrowser, но постарайся воздержаться от IE и Chrome. В-шестых — проверь свой браузер здесь. В-седьмых, вместо привычных гуглояндексов используй не отслеживающие пользователей поисковики вроде DuckDuckGo, Startpage или YaCy. А главное — помни, что те данные, которые собираются сейчас, не денутся никогда и никуда. Они навсегда останутся в кэше Гугла, Яндекса, Wayback Machine и рано или поздно будут обработаны (может и не на всегда, но на десятки лет могут). А можешь ли ты поручиться, что в будущем (кстати очень недалеком — почитайте о планах Гугла на 2020 год), математический аппарат не позволит составить досье на каждого пользователя интернета и установить за всеми мягкую, но неотступную слежку? Даже сейчас, пользуясь телефоном на базе Андроид с предустановленными рекламными программами (с сервисами Google, Яндекс и иже подобными, естественно, «чистые» сборки не содержат в себе такого говна), ты сливаешь своё местоположение и скорость движения (это мелочи, если вспомнить, что вся эта инфа доступна сотовому оператору всегда и без стороннего софта). Не считая абсолютно всей информации, которую ты ищешь с него в сети. А это только начало.

Безопасный режим: как зашифровать свои данные
Безопасный режим: как зашифровать свои данные | Приватность и свобода | Михаил Пожарский
Пожарский о слежке в интернетах

По возможности используй дистрибутивы Linux, для обычных пользователей удобны Ubuntu и OpenSUSE. Голая Убунта тоже порой стучит, так что оптимальный вариант для ламера — это производные от Ubuntu: Xubuntu или Kubuntu. Если используешь Windows никогда не ставь Сборки Windows, всегда настраивая вручную фаервол с запретами и отключай все авто-обновления. Старайся пользоваться Open Source программами даже под Windows. Никогда не ставьте сомнительные непопулярные скрипты и программы из сторонних репозиториев (для Linux) и сайтов (для Windows). В том числе не ставьте и взломанные, если на трекере их скачало несколько тысяч человек и антивирус молчит это не значит, что вируса там нет. Не ставьте программы с софт-порталов и файлообменников, всегда только с официального сайта.

Смартфон выбирайте только на Android, аппараты с другими открытыми прошивками сегодня редкость, но о них тоже не надо забывать. Следует выбирать тот, под который уже существуют сторонние прошивки с открытым кодом: CyanogenMod, Paranoid Android, чистый Android, MIUI и другие. Смотрите только на официальных сайтах прошивок, где наличие команды профессионалов и открытого когда гарантирует хоть что-то. Никогда не ставьте прошивки и программы на Android с сайтов 4pda, xda и подобных. Популярность тем и количество загрузок на них ничего не гарантирует. На сегодня под Android нету абсолютно надёжного магазина приложений. Можно посоветовать обратить внимание на два из них:

1. Самый большой и быстро обновляющийся (что очень важно для закрытия уязвимостей) это Google Play Market, приложения там проходят проверку на вредоносность, но при этом сервисы гугл и сам магазин шпионят.

2. Магазин бесплатных приложений с открытым исходным кодом F-Droid очень медленно развивается и обновление, например, Firefox там может опоздать на неделю (что уже большая дыра в системе); учитывая полную бесплатность сомнительна хорошая проверка приложений на вирусы. Критичные приложения, через которые можно пролезть в систему, такие как Firefox и другие программы для работы через интернет лучше обновлять с официальных сайтов вручную.

3. Официальные сайты разработчиков, выкладывающих свои сборки на определённые архитектуры (x86, ARM) ссылками на скачивание напрямую на сайте. Nuff said.

4. 4PDA. Nuff said too.

## Also

Есть такая организация ICANN, которая владеет центральными DNS серверами и распоряжается всем в интернете. Сервера ICANN получают информацию от всех внешних IP и это основа всего интернета. А кто вы думаете стоит за ICANN. Алсо, американские спецслужбы получают эту и любую информацию по первому свисту.

## См. также

- Неуловимый Джо — это ты, анонимус!
- Гнездо параноика
- Паранойя
- Закладки
- ZOG
- Tor
- I2P

## Ссылки

- Анонимности нет, смиритесь
  - Часть 1
  - Часть 2
- Выгуглен — рассказ писателя Кори Доктороу о том, к чему может привести постоянный и упорный сбор корпорацией Google данных о пользователях.
- Подключение картинок с внешних ресурсов
- Анонимности нет, смирись
- Подборка ресурсов для трушных анонов в сети TOR

## Примечания

1. ↑ Ставьте в любом случае, но используйте только для действительно **важных** сообщений. Не стоит засорять каналы Tor'а — кому-то в Азии он на самом деле может быть жизненно необходим.
2. ↑ И анонимность даже получше ТОРа будет и проекту посильная помощь
3. ↑ В лучших традициях Младшего брата Кори Доктороу.

ZOG

11 сентября 2012 год 25-й кадр AlexSword Backmasking Bitcoin F-19 Facebook Google SCP WikiLeaks X-files Zeitgeist ZOG А власти скрывают Англичанка гадит Андрей Скляров Антиглобализм Братание Вайомингский инцидент Вестник ЗОЖ Вражеские голоса Глобальное потепление ГМО Гнездо параноика Александр Гордон Городские легенды Госдеп Государственная тайна Двойники Путина Дело Дрейфуса Еврейские расовые жиды Жопоголизм Закладки Запрещённый ролик Зомби-апокалипсис Зона 51 Идентификация пользователей в интернете Инопланетяне Каббала Климов КОБ Кровавая гэбня Лунный заговор Люди в чёрном Масоны Метро-2 Мировой финансовый кризис Моссад НАТО Номерные радиостанции Общество потребления Оппозиция Паранойя Перепись населения Пиар План Даллеса Плоская Земля Резонатор Гельмгольца Саентология СДВ Система Стариков СУП США Теория заговора Терроризм Фальсификация истории ФБР Фоменко ФСБ Хазин Чёрные вертолёты Шулхан Арух Эльзагейт Юггот Юрий Петухов

Интернет

Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org SEO Skype Tor TOS Via WAP Ёбаное ВТ Админ Акадо Американские интернеты Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот Смайл Социальная сеть