Вы любите смотреть таргетированную рекламу? Вы не против того, что фейсбук сам отметит вас на фотографии друзей (а ее увидят посторонние люди)? Вам нравится видеть релевантные запросы в поисковике? Вы не против того, чтобы ваши предпочтения использовали для рекламы товаров вашим друзьям? Вам все равно, что гугл хранит всю историю вашего поиска, и вы не боитесь, что это может кто-то увидеть через 10 лет («скачать Аватар бесплатно без смс» или «как избежать проверки налоговой»)? Вы не против того, что ваши фото и комментарии увидит потенциальный работодатель или весь интернет, если вы вдруг случайно станете кому-то интересны?

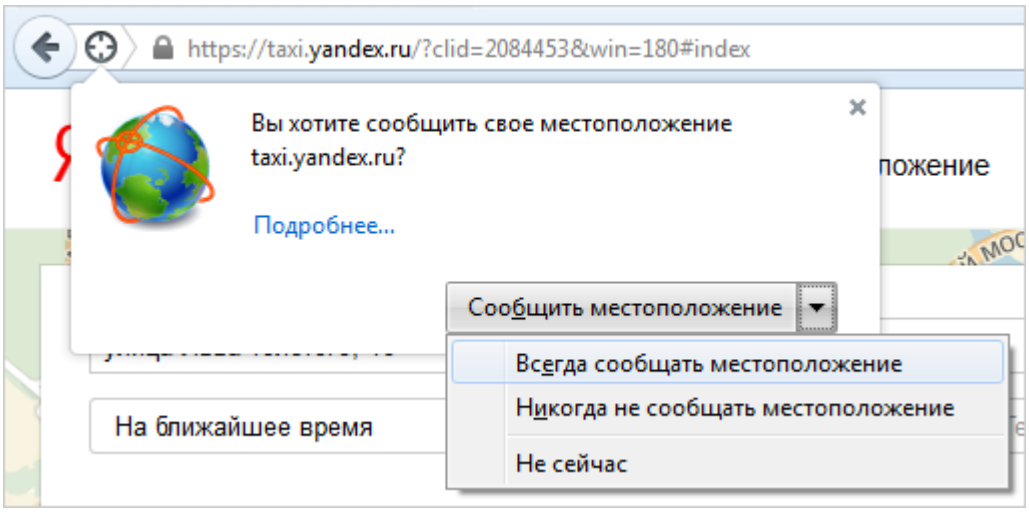
Если же вы решили озаботиться своей приватностью, иметь минимум данных для компромата и построения психологического и поведенческого профиля, когда вы или ваши родители совершите какой-нибудь факап и обратите на себя внимание общественности (или когда вы добьетесь успехов и кто-то из недоброжелателей будет специально искать эти данные) — добро пожаловать под кат с пошаговой инструкцией для основных программ и сетей. Нашей целью будет обеспечение максимальной приватности при сохранении максимального удобства серфинга. Понятно, что если вы хотите обеспечить себе максимальную конфиденциальность, то лучше не пользоваться социальными сетями, пользоваться различными анонимизаторами и т. д., но на это не все согласны пойти.

Шаг 1: Настройки геолокации в Mozilla Firefox

Геолокация — это определение местоположения (геопозиции) устройства пользователя.

Сайты и приложения запрашивают доступ к геопозиции, чтобы точнее отвечать на поисковые запросы и предоставлять актуальную информацию с учетом местонахождения пользователя.

Разрешить или запретить отслеживать местоположение. Когда сайт запрашивает информацию о том, где вы находитесь, в верхней части страницы появляется предупреждение:



Определите параметры геолокации:

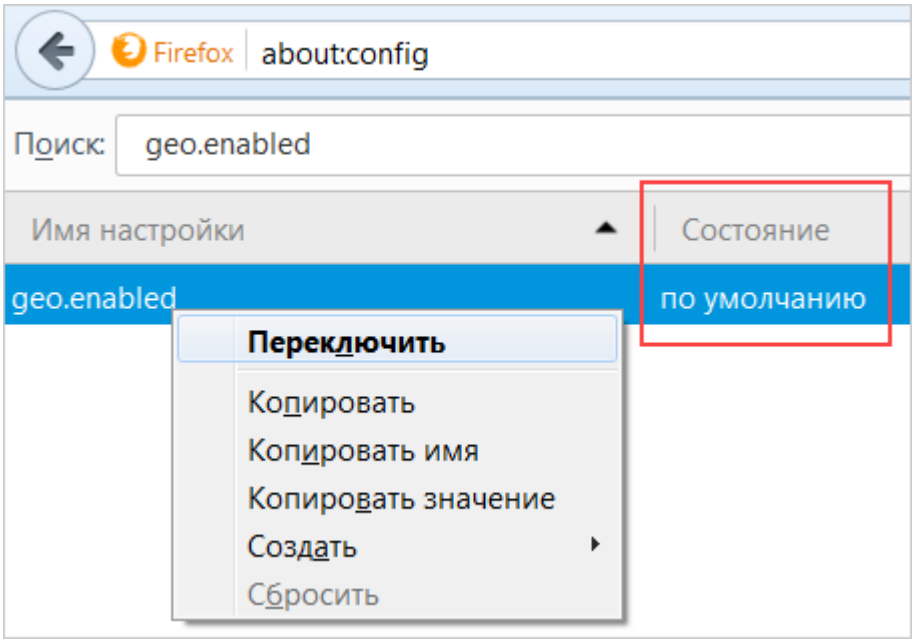
- Разрешить сайту отслеживать ваше местоположение — выберите пункт Всегда сообщать местоположение.
- Разрешить сайту отслеживать ваше местоположение до перезагрузки браузера — нажмите кнопку Сообщить местоположение.
- Запретить сайту отслеживать ваше местоположение до перезагрузки браузера — нажмите значок ×.
- Блокировать от сайта запросы на определение вашего местоположения — выберите пункт Никогда не сообщать местоположение.

- Отложить решение — выберите пункт Не сейчас.

Установить общие настройки геолокации. Чтобы установить общие настройки геолокации для всех сайтов и программ:

1. В адресной строке браузера введите команду about:config.
2. В открывшемся окне нажмите кнопку Я обещаю, что буду осторожен!
3. В строке Поиск введите geo.enabled.
4. Чтобы включить определение местоположения для всех сайтов, правой кнопкой мыши выделите строки с состоянием установлено пользователем и выберите пункт Переключить.

   Чтобы отключить определение местоположения для всех сайтов, правой кнопкой мыши выделите строки с состоянием по умолчанию и выберите пункт Переключить.

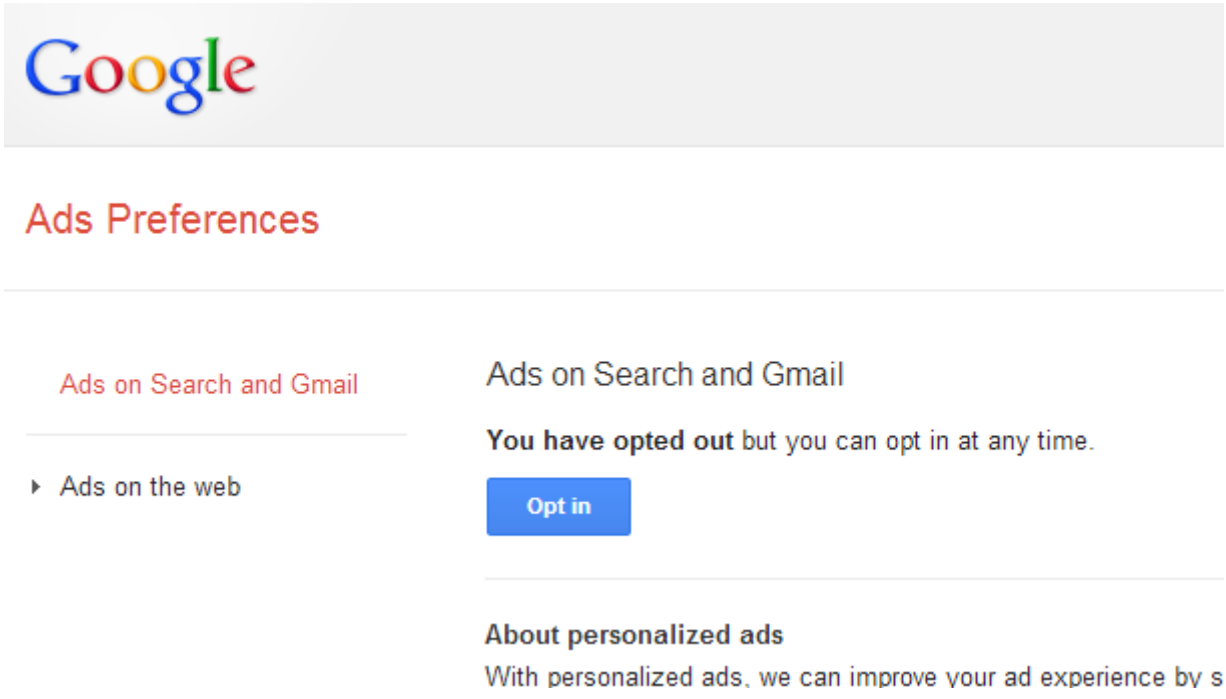


Изменить настройки:

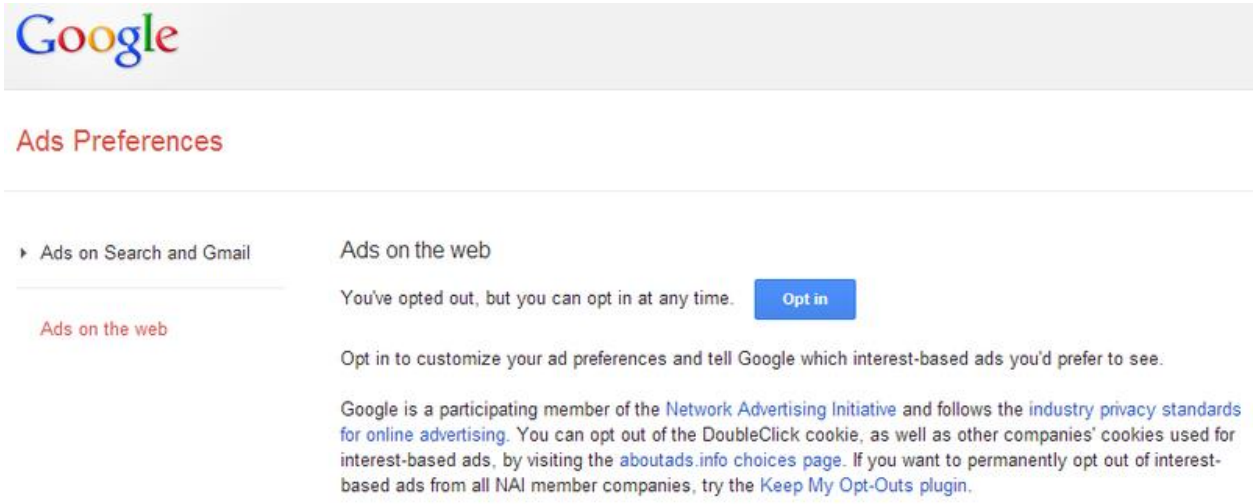
1. Перейдите на сайт.
2. Если меню браузера не отображается, нажмите клавишу Alt.
3. Выберите пункт Инструменты → Информация о странице.
4. На вкладке Разрешения выберите настройки параметра Знать ваше местоположение.

Шаг 2: Настройки учетки Google

В первую очередь минимизируем отслеживание в рекламных целях. Для этого зайдем на сайт www.google.com/ads/preferences и приводим ее к следующему внешнему виду путем нажимания на кнопки opt out и прочие отказы:



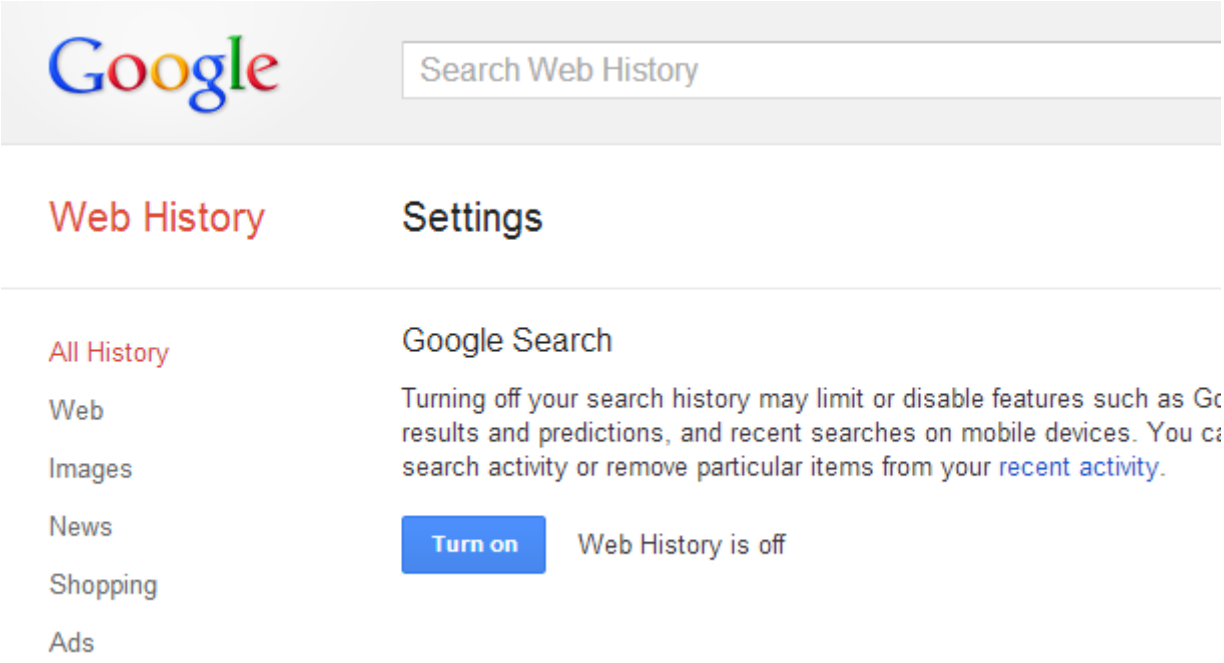
Аналогично должно быть в разделе Ads on the web (реклама на веб-страницах):



Если внешний вид отличается, ищите в этих разделах кнопки различных отказов от участия. Заодно во время отключения вы, возможно, узнаете о себе много нового (например, к каким категориям вы были присвоены во время вашего предыдущего серфинга).

Google search history

Аналогично тому, как браузер запоминает, на каких страницах вы были, «Гугл» по умолчанию запоминает все, что вы когда-либо искали. Смело идем отключать это поведение в www.history.google.com/history/settings превращая ее к следующему виду:



После чего удалите всю накопленную на вас информацию по поисковым запросам в www.history.google.com/history

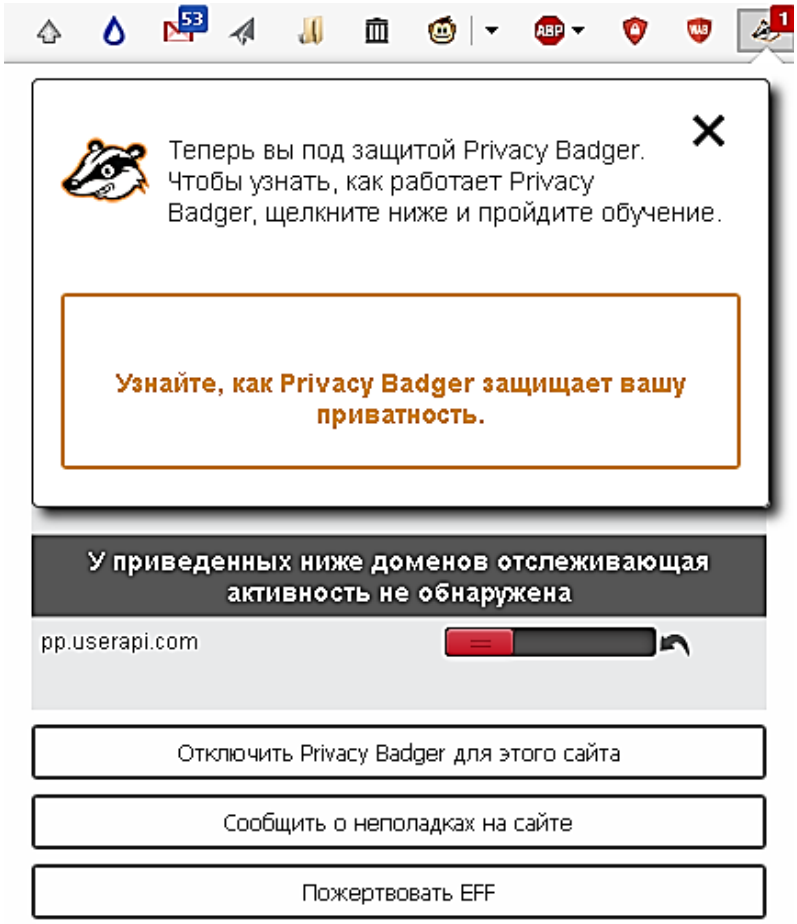
Прочие сервисы гугла

Зайдите на www.google.com/dashboard и посмотрите список всех сервисов, которыми вы когда-либо пользовались. Методично зайдите в каждый и пройдитесь по настройкам/контенту. Удалите ненужное, заблокируйте фотографии в «Пикассе», максимально деперсонилизируйте и ограничьте Google Plus. Думаю, не нужно говорить, что ваш профиль должен быть исключен из результатов веб-поиска, максимум фотографий удален, остальные альбомы заблокированы для не друзей, видимость постов ограничена (а, в идеале, удаляться через месяц после написания). Вся почта и старее года удаляться (поверьте, вы не будете ее перечитывать, в отличие от других людей, которым она вдруг станет очень интересна, когда вы, например, будете баллотироваться на какую-нибудь политическую или высокую должность).

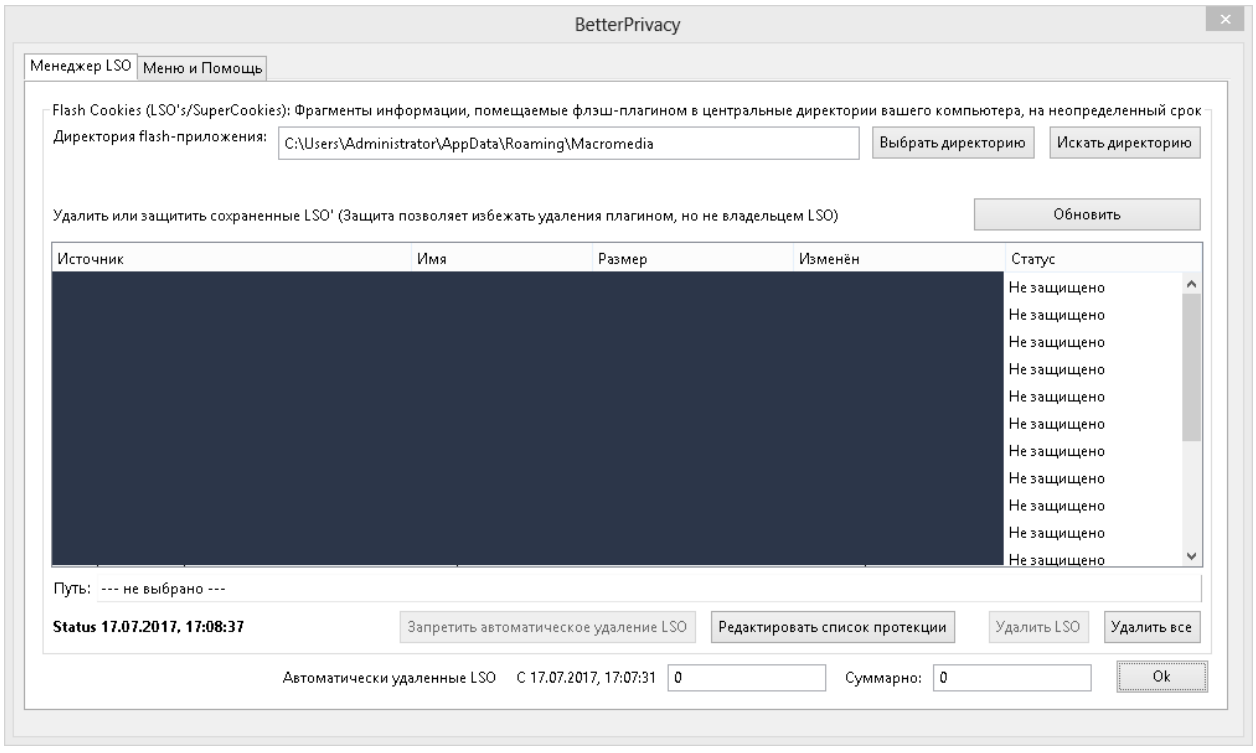
Шаг 3: Дополнения Firefox по защите приватности

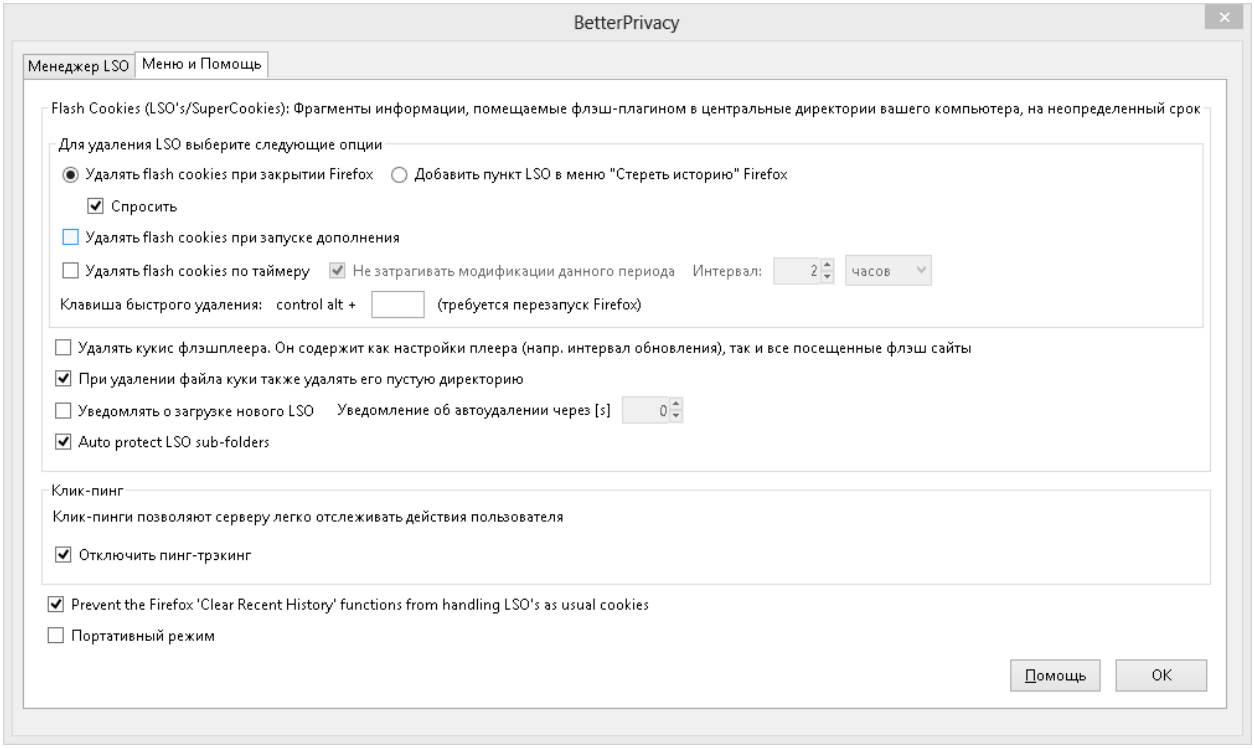
Помимо базовых настроек Firefox и некоторых поисковых сервисов существуют и другие средства, защищающие приватность в сети. Здесь приводится перечень дополнений Firefox, реализующих этот функционал в браузере.

Privacy Badger. Одно из таких самых простых дополнений Firefox. При загрузке любого сайта при активизации ярлыка с барсуком данное дополнение выводит сетевых «жучков», каждый из которых можно заблокировать, сдвинув справа налево его ползунок.

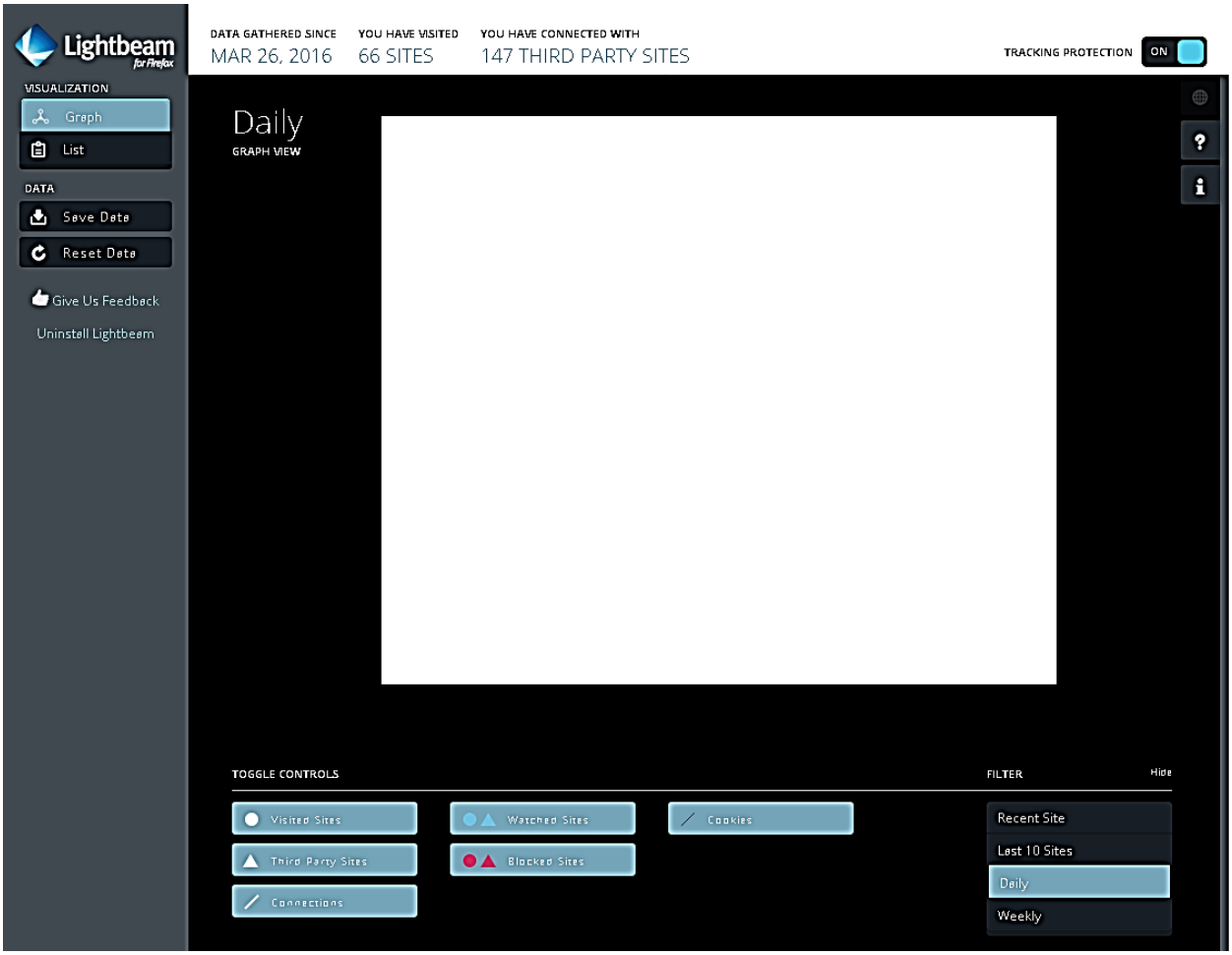


BetterPrivacy. Здесь ведется управление cookies (небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя), который удаляются после сеанса работы с браузером. Из-за этого придется перезаходить в свои учетные записи заново, но в связи с запоминанием паролей в браузере и соответствующим автозаполнением форм это становится не так критично.





Lightbeam. Данное дополнение не только блокирует слежение с веб-сайтов, но и выводит граф посещаемых вами сайтов (область его вывода отмечена белым прямоугольником на снимке окна дополнения).



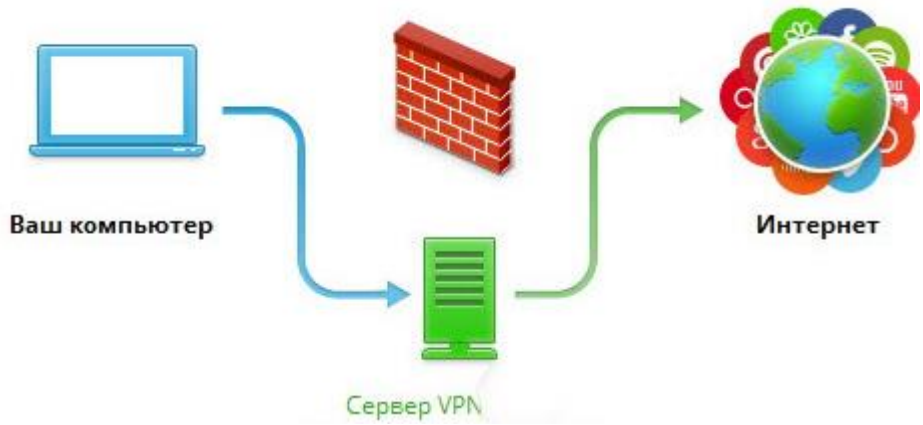
Зачем нужна на сайте Госуслуги полная регистрация? Для того, чтобы упростить получение многих документов и массы полезной информации без длительных походов в соответствующие государственные учреждения, без очередей.

Например, это может быть получение загранпаспорта с электронным чипом (на 10 лет) или без чипа (на 5 лет), замена паспорта гражданина РФ, замена водительского удостоверения в связи с истечением срока его действия, регистрация транспортных средств, запись на прием к врачу, в детский сад, в школу, а также вопросы, связанные с пенсией, с налогами и т.д.

Шаг 4: Программный VPN

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

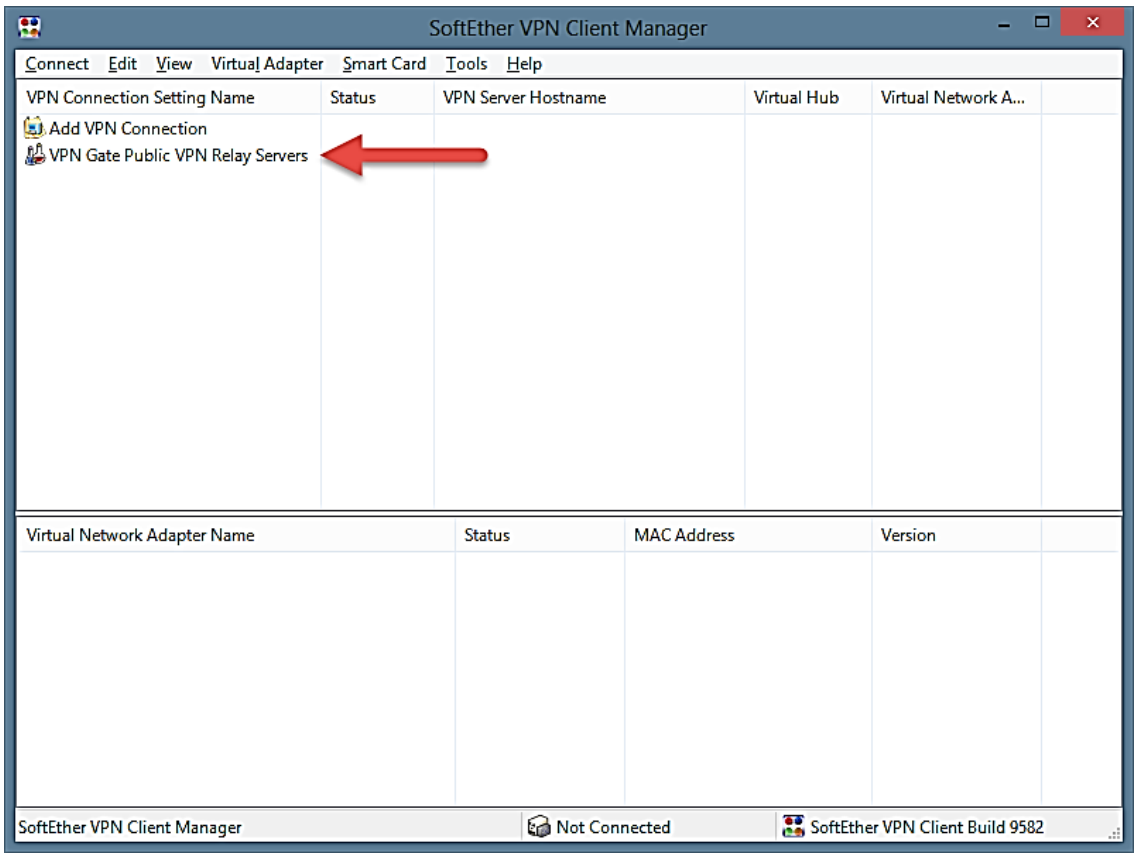
Он позволяет сделать анонимным Интернет-соединение с любым сайтом.



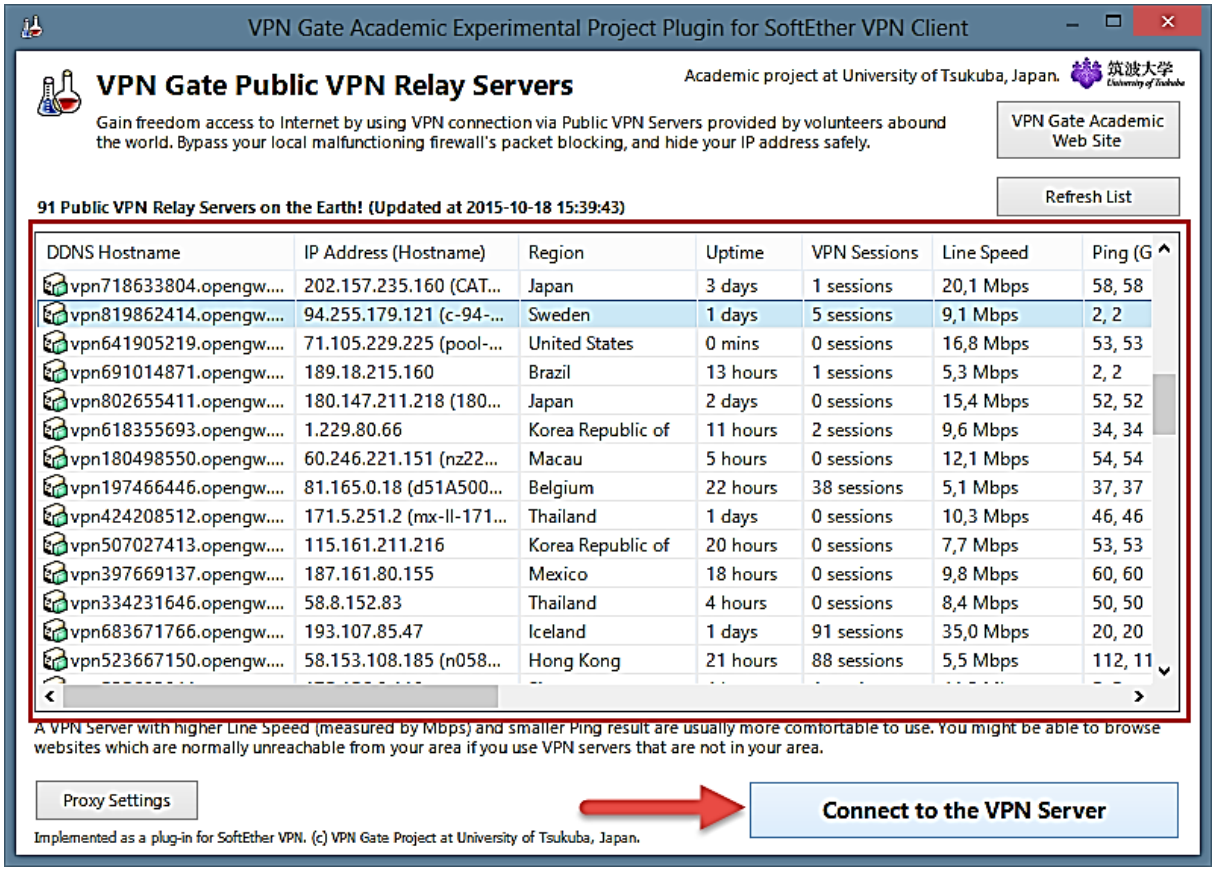
Из программного обеспечения, отвечающего за VPN-соединения, есть наиболее простая - SoftEther VPN Gate TinyURL.

Данный проект был запущен аспирантами университета города Цукуба в качестве эксперимента по изучению VPN сетей. И добровольцы по всему миру предоставили им свои vpn-сервера для работы. В данный момент проект открыт для всех желающих и, скачав их клиент или конфигурацию openvpn сервера, можно с легкостью подключиться и пользоваться интернетом с наибольшей защитой конфиденциальности.

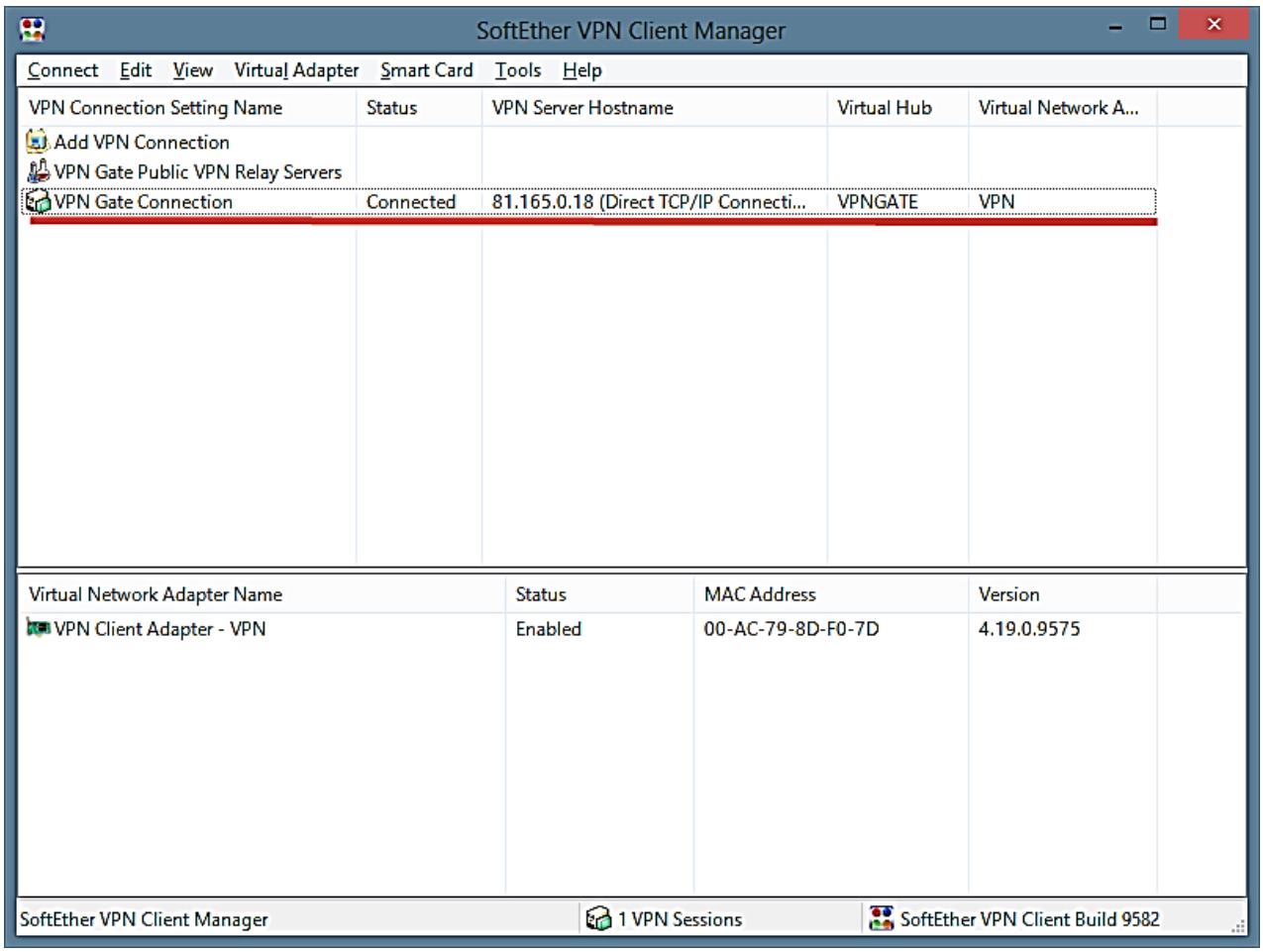
Скачиваем по ссылке http://download.vpngate.jp/common/cd.aspx/vpngate-client-2015.10.18-build-9582.133811.zip и устанавливаем её (Далее Далее Далее), распаковав перед этим архив с ПО. Запустите программу и в открывшемся окне выберите пункт **VPN Gate Public VPN Relay Servers**.



В открывшемся окне выберите нужный вам сервер (не рекомендуется брать азиатские сервера, там очень большие задержки), и нажмите **Connect to the VPN Server**



При успешном соединении в окне программы должна появиться еще одна запись:



Если соединение не удалось, попробуйте выбрать другой сервер

Кроме этого, существует Tor Browser, использующий так называемую луковую маршрутизацию – технологию анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторяется. Таким образом, промежуточные узлы не знают источник, пункт назначения и содержание сообщения.

Tor Browser использует тот же движок, что и Firefox, и поэтому дополнения обычного браузера вполне подходят под него

В качестве самостоятельного задания предлагается скачать и установить Tor Browser (https://www.torproject.org/dist/torbrowser/5.0.3/torbrowser-install-5.0.3_en-US.exe) и установить туда некоторые дополнения Firefox, упомянутые в разделе «Настройка фильтров содержимого интернета ».