

Opera



<https://www.opera.com/>

ОГЛАВЛЕНИЕ

Общие сведения.....	4
Архив предыдущих версий. FTP.....	4
Список команд (ключей) запуска.....	4
Внутренние (internal) страницы браузера.....	4
Настройка.....	5
Включение дополнительных (скрытых) настроек.....	5
Общая настройка опций.....	5
Настройка параметров в opera://flags.....	6
Параметры запуска.....	6
Защищённый поиск в сети.....	7
Синхронизация профиля в tmpfs (RAM) с помощью Profile Sync Daemon для Linux.....	7
Интеграция базы данных KeePassX с помощью расширения.....	8
Управление образом Docker с использованием Simple Docker UI.....	9
Установка и настройка Adobe Flash Player.....	10
Расширения.....	12
Общие сведения.....	12
Как установить стороннее расширение?.....	12
Популярные расширения.....	12
Скрипты.....	26
Общие сведения.....	26
Популярные скрипты.....	26
Стили.....	29
Популярные стили.....	29
Вопросы и ответы.....	30
Назначение браузера браузером по умолчанию. Как открывать ссылки из внешних приложений, имея portable версию браузера? Добавление браузера в «Программы по умолчанию» для Windows 7.....	30
Удаление из программ по умолчанию и реестра.....	31
Как настроить браузер для работы с проху при использовании ssh-туннеля?.....	31
Как скачать и сохранить Chrome расширение из магазина?.....	31

Запуск браузер с разными профилями (неполная версия)	32
Баги.....	33
Исчезновение паролей при входе в ОС под учётной записью администратора с последующим возвращением к обычному пользователю.....	33

Общие сведения

Архив предыдущих версий. FTP

[FTP](#)

Список команд (ключей) запуска

<http://peter.sh/experiments/chromium-command-line-switches/>

Внутренние (internal) страницы браузера

opera://net-internals
opera://appcache-internals
opera://indexeddb-internals
opera://chrome:inspect
opera://media-internals
opera://net-internals
opera://profiler
opera://serviceworker-internals
opera://sync-internals
opera://tracing
opera://webrtc-internals
opera://view-http-cache
opera://gpu
opera://flags

Расширение **About://Internal Pages** для быстрого доступа: [\[Opera Store\]](#) [\[GitHub\]](#) [\[Home Page\]](#)

Настройка

Включение дополнительных (скрытых) настроек

Перейти в настройки (Меню > Настройки или сочетание клавиш Alt+P) и нажать поочерёдно клавиши: Вверх, Вверх, Вниз, Вниз, Влево, Вправо, Влево, Вправо, В, А (английские)

Общая настройка опций

Выполняется по желанию!

Открыть Настройки (Меню > Настройки или сочетание клавиш Alt+P).

Вкладка **Безопасность**:

- Дополнять поисковые запросы и адреса с помощью сервиса подсказок в адресной строке — *отключить*
- Предсказывать сетевые действия для ускорения загрузки страниц — *отключить*
- Помогите усовершенствовать Орега, отправляя информацию об использовании функций браузера — *отключить*
- Включить защиту от вредоносных сайтов — *включить*
- Автоматически отправлять отчеты об аварийном завершении в Opera — *отключить*
- Отправлять сайтам заголовок «Не отслеживать» — *включить*
- Загружать изображения для рекомендованных источников в «Новостях» на основании истории посещений — *отключить*
- Разрешить партнерским поисковым системам проверять, установлены ли они по умолчанию — *отключить*
- Включить автозаполнение форм на страницах — *отключить*
- Предлагать сохранение вводимых паролей — *отключить*, если используется программа для управления паролем.
- Отключить непроксируемый UDP — *включить*
- Блокировать сторонние файлы cookie и данные сайтов — *включить*
- Не разрешать никаким сайтам обрабатывать протоколы — *включить*

Вкладка **Сайты**:

- Не разрешать никаким сайтам создавать ключи в формах (рекомендовано) — *включить*
- Flash: *По запросу*

- Запретить сайтам отслеживать мое физическое местонахождение — *включить*
- Запретить сайтам показывать системные уведомления — *включить*
- Разрешать идентификацию для защищенного содержимого — *отключить*
- Запретить сайтам доступ к микрофону — *включить*
- Запретить сайтам доступ к камере — *включить*
- Запретить всем сайтам использовать системные эксклюзивные сообщения для доступа к аудиоустройствам MIDI — *включить*

Вкладка **Браузер**:

- Загружать фоновые вкладки с задержкой — *включить*
- Использовать прокси для локальных серверов — *отключить*
- Запрашивать папку сохранения перед загрузкой файла — *включить*
- Показывать панель закладок — *включить*

Настройка параметров в opera://flags

Открыть параметры браузера выполнив в адресной строке команду `opera://flags`

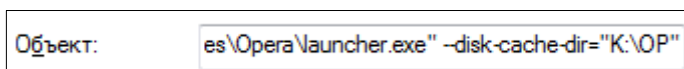
Отключение сообщения о переходе в полноэкранный режим: найти параметр `Simplified fullscreen / mouse lock UI` и включить его.

Подсказка: быстрый доступ из адресной строки `opera://flags/#simplified-fullscreen-ui`

Параметры запуска

1. Создать ярлык для `Opera.exe`
2. Открыть свойства ярлыка.
3. Добавить в поле «Объект» необходимые параметры (список ниже), и не забыть поставить пробел перед добавлением команды.

Пример:



Отключение WebRTC на Android:

`--disable-webrtc`

Отключение кэша:

`--disk-cache-size=1 --media-cache-size=1`

Перенос кеша:

--disk-cache-dir="К:\ОР"

где К:\ОР путь к папке для перенаправления хранения кэша.

Перенос профиля:

--user-data-dir="L:\ТТ"

где L:\ТТ путь к папке для перенаправления хранения профиля.

Защищённый поиск в сети

<https://encrypted.google.com/>

<https://encrypted.google.com/search?q=%s>

<https://duckduckgo.com/> | <http://3g2upl4pq6kufc4m.onion/>

Синхронизация профиля в tmpfs (RAM) с помощью Profile Sync Daemon для Linux

Source (источник), скачать: <https://github.com/grayky2/profile-sync-daemon>

Wiki Eng: <https://wiki.archlinux.org/index.php/Profile-sync-daemon>

Wiki Rus: [https://wiki.archlinux.org/index.php/Profile-sync-daemon_\(Русский\)](https://wiki.archlinux.org/index.php/Profile-sync-daemon_(Русский))

Обсуждение: <https://bbs.archlinux.org/viewtopic.php?pid=1026974>

profile-sync-daemon — псевдо-демон, автоматически переносит профиль, кэш и другие данные браузера в tmpfs (RAM), соответственно операций ввода/вывода браузера перенаправляются в оперативную память, таким образом, уменьшается износ жесткого диска, затем синхронизируется с HDD/SSD используя символические ссылки и rsync.

Демон автоматически производит резервные копии на случай возникновения сбоев.

При загрузке системы профиль копируется в оперативку, при выключении обратно на диск.

Важно. При возникновении внезапной перезагрузки, некоторые данные могут быть утеряны.

Проверка работоспособности. Для того, чтобы увидеть, что Profile Sync Daemon работает и профиль браузера используется в TMPFS, можно перейти в каталог /run/shm (в Debian /dev/shm) и посмотреть находится ли профиль там. Или проверить директорию профиля командой ~/.mozilla/firefox чтобы увидеть, является ли папка профиля символической ссылкой на папку /run/shm

Интеграция базы данных KeePassX с помощью расширения

Описание

Автозаполнение данных в форме ввода на веб-сайтах используя файл паролей хранилища KeePassX.

Установка

Установить расширение **СКР** [\[Chrome Store\]](#)

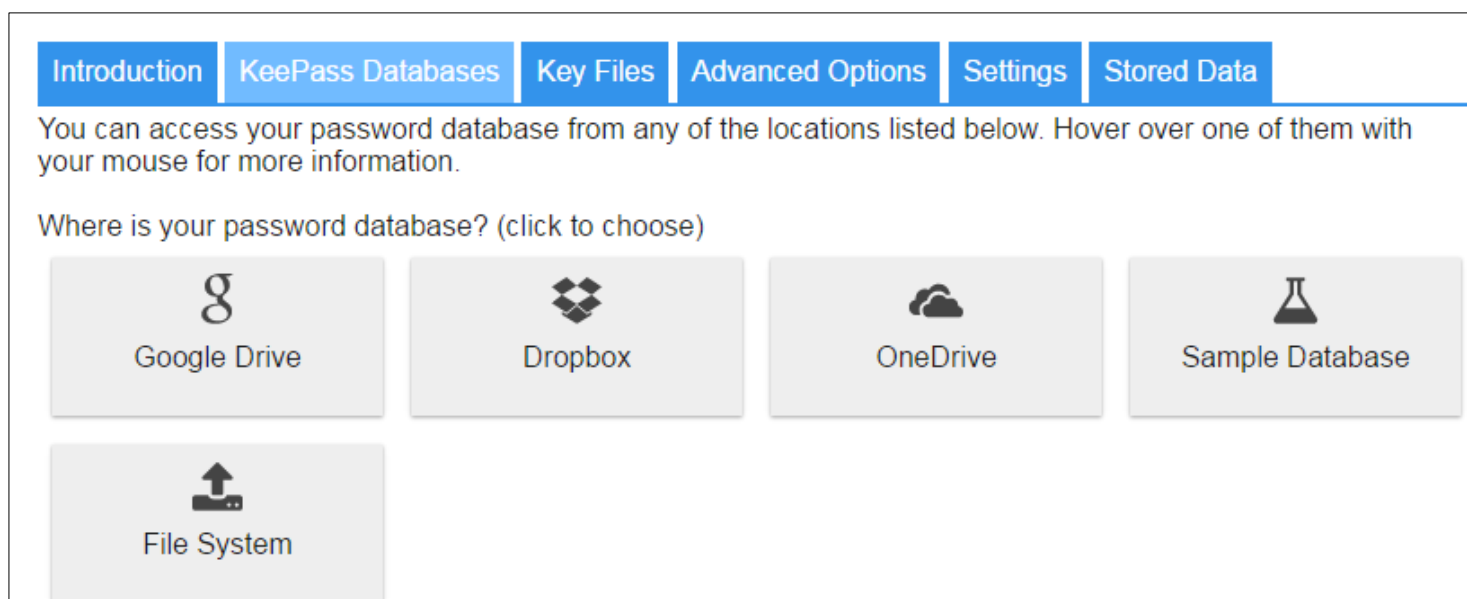
Основные характеристики:

- Нет необходимости в специальных разрешениях (Права доступа и риски <https://github.com/perfectapi/CKP/wiki/CKP-Extension-Permissions-and-Risks>)
- Работает с KeePass v1 (.kdb) и v2 (.kdbx) файлами баз данных, с любой комбинацией ключевого файла и мастер-пароля
- Автоматический ввод пароля на веб-сайте (Если разрешение не предоставлено, можно скопировать вручную)
- Пароли шифруются в памяти
- Простое переключение между несколькими файлами баз данных
- Автоматическая разблокировка ключей только для баз данных
- Обеспечивает интеграцию с базой данных паролей KeePassX в режиме только для чтения.

Использование

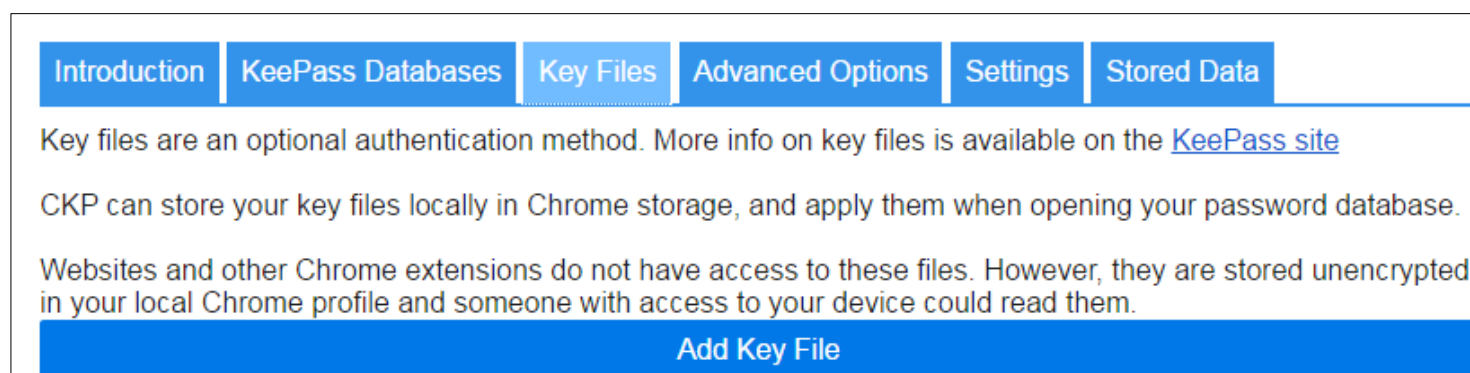
Открыть настройки расширения (альтернативный вариант: нажать на значёк расширения в адресной строке, далее открыть Settings, чтобы посмотреть параметры расширения.)

Перейти на вкладку KeePass Databases, указать (подключить) файл базы данных который содержит пароли:

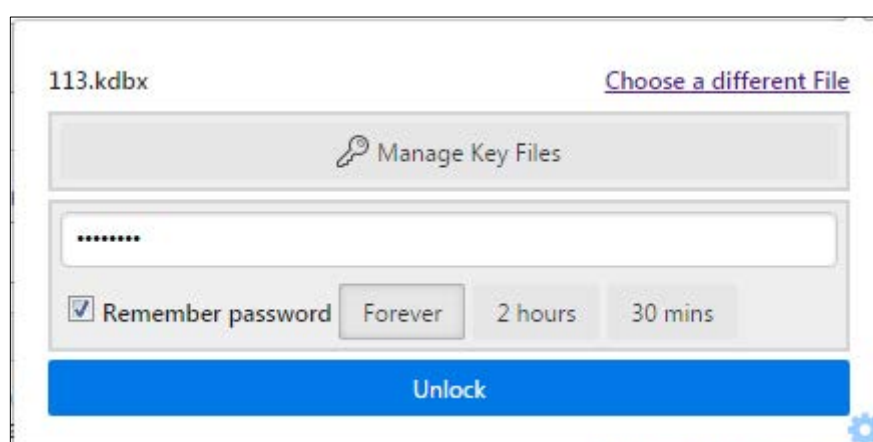


Примечание: Выбрав файл внутри File System, его необходимо будет выбрать повторно при обновлении базы данных.

Если был создан Файл-ключ в KeePassX, его необходимо добавить:



Перейти на сайт где требуется ввести данные и нажать на значок расширения в адресной строке. Далее выбрать файл с базой данных KeePassX и ввести мастер пароль, чтобы разблокировать базу данных. При необходимости выбрать Key-file:



Дополнительно

Офф. Сайт: <http://perfectapi.github.io/CKP>

GitHub: <https://github.com/perfectapi/CKP>

Wiki: <https://github.com/perfectapi/CKP/wiki>

С предложениями улучшения и любыми вопросами: <https://github.com/perfectapi/CKP/issues>

Управление образом Docker с использованием Simple Docker UI

<https://www.maketecheasier.com/manage-docker-images-chrome/>

Установка и настройка Adobe Flash Player

[Adobe Flash Player](#) предназначен для просмотра видео в Интернете.

[Настройка параметров](#) включает в себя: настройку хранения информации посещённых веб-сайтов, доступа к микрофону/камере сайтом, пиринговой полосы пропускания каналы, сохранения Flash-содержимого.

Запрет хранения Flash LSOs

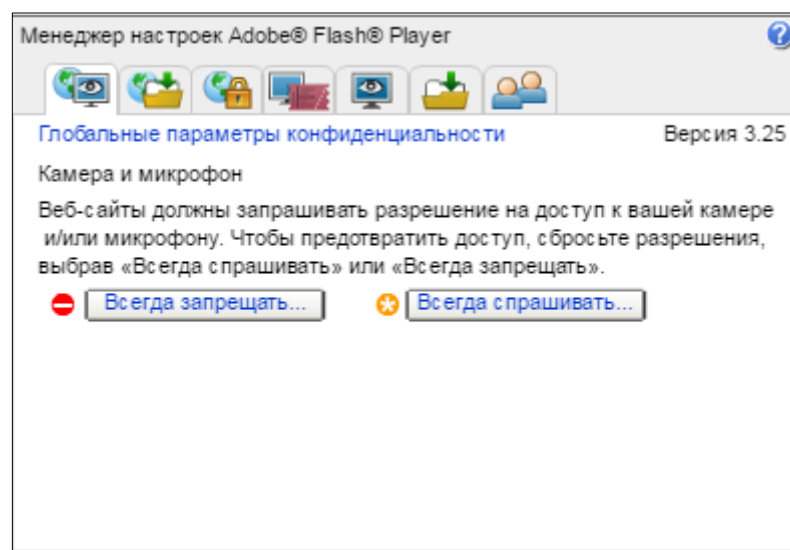
Wiki: https://en.wikipedia.org/wiki/Local_shared_object

Описание на русском: <https://habrahabr.ru/post/111176/>

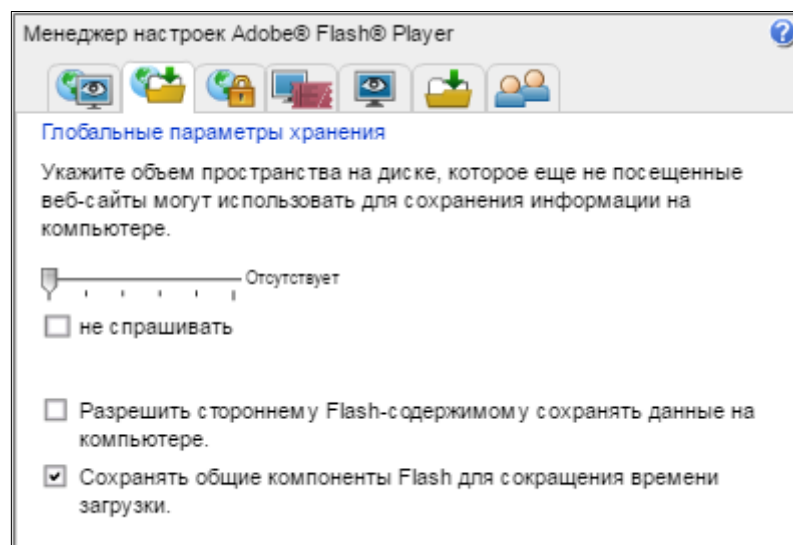
Flash LSOs (сохраняются локально) похожи на обычные куки (cookies) и включены по умолчанию. Для их отключения перейти по адресу:

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html

Выбрать вкладку **Глобальные параметры конфиденциальности** (первая слева) и нажать на кнопку «Всегда запрещать...»:

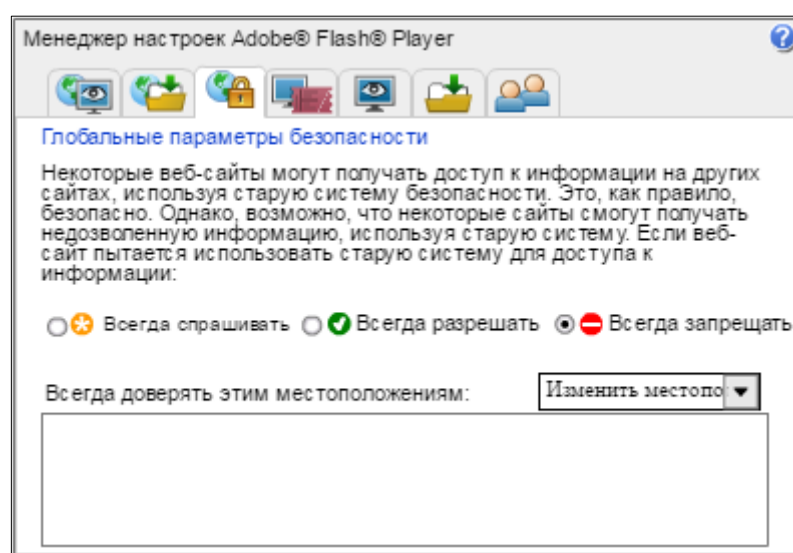


Выбрать вкладку **Глобальные параметры хранения** (2 слева) и отрегулировать объём дискового пространства как показано ниже:



А также снять флажок рядом с «Разрешить стороннему Flash-содержимому сохранять данные на компьютере».

Выбрать вкладку **Глобальные параметры безопасности** (3 слева) и установить опцию «Всегда запрещать»:



В завершений добавить в файл hosts адрес stats.adobe.com для запрета отслеживания адобом посещений сайтов.

Расширения

Общие сведения

Официальный сайт аддонов: <https://addons.opera.com/>

Дополнительные можно найти на <https://github.com/> и <https://chrome.google.com/webstore/category/extensions>

Как установить стороннее расширение?

1. Открыть Меню → Расширения → Управление расширениями
2. Нажать кнопку Режим разработчика.
3. Выбрать нужный вариант (Загрузить распакованное расширение... или Упаковать расширение...) нажав соответствующую кнопку.

Популярные расширения



About:Internal Pages

[\[Opera Store\]](#) [\[GitHub\]](#) [\[Home Page\]](#)

Расширение для быстрого доступа к внутренним страницам, таким как about:plugins about:bookmark и др.



AdNauseam

[\[Opera Store\]](#) [\[Chrome Market\]](#) [\[GitHub\]](#) [\[Wiki\]](#) [\[FAQ\]](#) [\[Home Page\]](#)

Защищает от слежения рекламных сетей.

Онлайновая реклама становится более агрессивной и тоже используется для скрытого профилирования сетевой активности. Ее блокирование решает проблему лишь частично и может демаскировать пользователя еще сильнее. Поэтому принцип генератора «белого шума» используемый в данном расширении защищает пользователя от отслеживания баннерными сетями и средствами персонализации рекламных показов.

AdNauseam скрывает настоящие переходы по ссылкам в потоке автоматических кликов. Он просто кликает в фоне на все подряд, мешая причислить пользователя к определенной целевой аудитории. Работая совместно с uBlock, AdNauseam забивает базы данных рекламных сетей ложной статистикой. Профилирование пользователей становится бесполезным, а саму рекламу они обычно не видят вовсе — за редким и настраиваемым исключением.

После установки плагин AdNauseam нужно запустить вручную. Он работает скрыто, но позволяет просматривать логи и статистику своей работы. Фоновые клики по рекламным ссылкам открываются в «песочнице» — неотображаемой вкладке браузера. Несмотря на «песочницу», фоновое кликание по всем ссылкам подряд в AdNauseam повышает риск нарваться на drive-by-угрозы через фишинговые ссылки. Кроме того, авторы расширения наверняка смогут извлечь прибыль из потока фиктивных кликов, если их плагин обойдет средства противодействия накрутке.



Browsec VPN

[\[Opera Store\]](#) [\[Chrome Market\]](#) [\[Home page\]](#)

Расширение выполняет функций VPN.

Особенность расширения в том, что можно выбрать страну проксирующего сервера.

Шифрование трафика: Да

Анонимность: Да

Проксирование всего трафика: Да

Выборочное проксирование: Нет



Extension source viewer

[\[Opera Store\]](#) [\[GitHub\]](#) [\[Chrome Market\]](#)



СКР

[\[Chrome Store\]](#) [\[Home Page\]](#) [\[GitHub\]](#) [\[Wiki\]](#)



Cupcake

[\[Chrome Market\]](#) [\[GitHub\]](#)



Download Chrome Extension

[\[Opera Store\]](#)

Позволяет устанавливать расширения из Google Chrome Web Store.



Don't track me Google

[\[Google Market\]](#) [\[GitHub\]](#)



Fast Film

[\[Chrome Store\]](#) [\[GitHub\]](#)

Добавляет на сайтах kinopoisk и imdb иконки популярных торрент-сайтов, нажатие по которым позволяет быстро перейти к поиску фильма или сериала.



Flashcontrol

[\[Chrome Store\]](#)

Блокирование флеш-контента на веб страницах. Доступен белый список.



Fox Web Security

[\[Chrome Store\]](#)



friGate

[\[Home page, download link\]](#)

Расширение выполняет функций VPN.

Расширение использует собственный список заблокированных сайтов. Также, вы можете составлять списки с собственными сайтами, которые вы хотите проксировать. Для пользователя это удобно тем, что можно сохранять свой реальный IP, там где это требуется и использовать прокси, там где он необходим (для обхода блокировок сайтов) или там где нужно скрыть свой реальный IP. Расширение умеет определять, заблокирован ли у вас конкретный сайт, или нет, и включаться только в том случае, если он заблокирован, однако доступна опция «проксировать всегда». Можно использовать свой собственный прокси, а не прокси сервиса. Заявлен режим «AntiDPI» для обхода провайдерского DPI.

Доступ на сайты, не входящих в список расширения, происходит, минуя прокси, +если сайт доступен напрямую, то прокси тоже не включается;

Прокси https — трафик шифруется, а еще сжимается с помощью гугловского PageSpeed. Правда это все происходит с трафиком который идет через прокси, естественно.

Примечание. Firefox-версия умеет проксировать все сайты, в отличие от Chrome-версии.

Шифрование трафика: Нет
Анонимность: Да
Проксирование всего трафика: Нет
Выборочное проксирование: Да



h264ify

[\[Chrome Store\]](#) [\[GitHub\]](#)

Заставляет воспроизводить видео на Youtube в H.264 вместо VP8/VP9.
Требуется включить GPU acceleration. Для этого выполнить в адресной строке команду opera://flags далее найти параметр Override software rendering list и включить его.



Imagus

[\[Home page + download link\]](#) [\[Forum\]](#) [\[Форум, дополнительные возможности\]](#)

Увеличивает миниатюры изображений при наведении мыши на ссылки.



Jidesha

[\[GitHub\]](#)

Desktop Sharing in Jitsi Meet



LanguageTool

[\[Chrome Store\]](#) [\[GitHub\]](#) [\[Home Page\]](#)

Проверка грамматики, пунктуации, орфографии



LessPass

[\[Home Page\]](#) [\[Chrome Market\]](#)

<https://github.com/lesspass/lesspass>

<https://github.com/lesspass/webextension>

<https://github.com/lesspass/native>

Хранение уникальных паролей для всех сайтов и приложений — целое искусство. Самый распространённый вариант — записать все пароли в один файл, который защищён мастер-паролем. По такому принципу работает большинство парольных менеджеров.

У этого способа много преимуществ, но есть два главных недостатка: 1) трудно синхронизировать пароли между устройствами; 2) нужно всегда иметь в распоряжении сам файл с паролями. То есть потерял файл с паролями — и до свидания.

Новый парольный менеджер LessPass с открытым исходным кодом лишён этих недостатков, потому что работает на [чистой детерминированной функции](#).

Концепция

Концепция LessPass заключается в том, что регенерация одноразовых паролей происходит на лету при помощи чистой функции, которая выдаёт детерминированные значения каждый раз при расчёте каждого уникального пароля.

На вход функции подаются четыре аргумента:

мастер-пароль

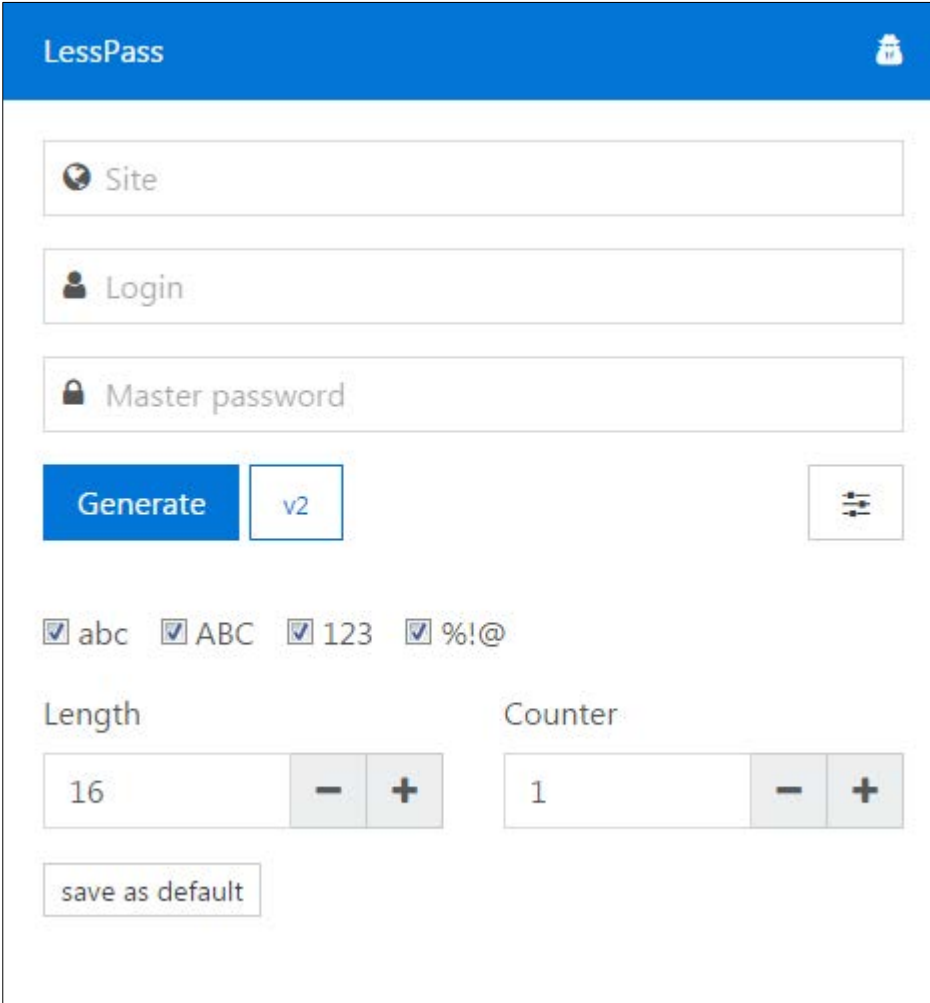
логин на сайте

адрес сайта

опции генерации пароля

В любой момент на любом компьютере вы можете повторно запустить функцию — и вычислить свой уникальный пароль для конкретного сайта.

Как это выглядит:



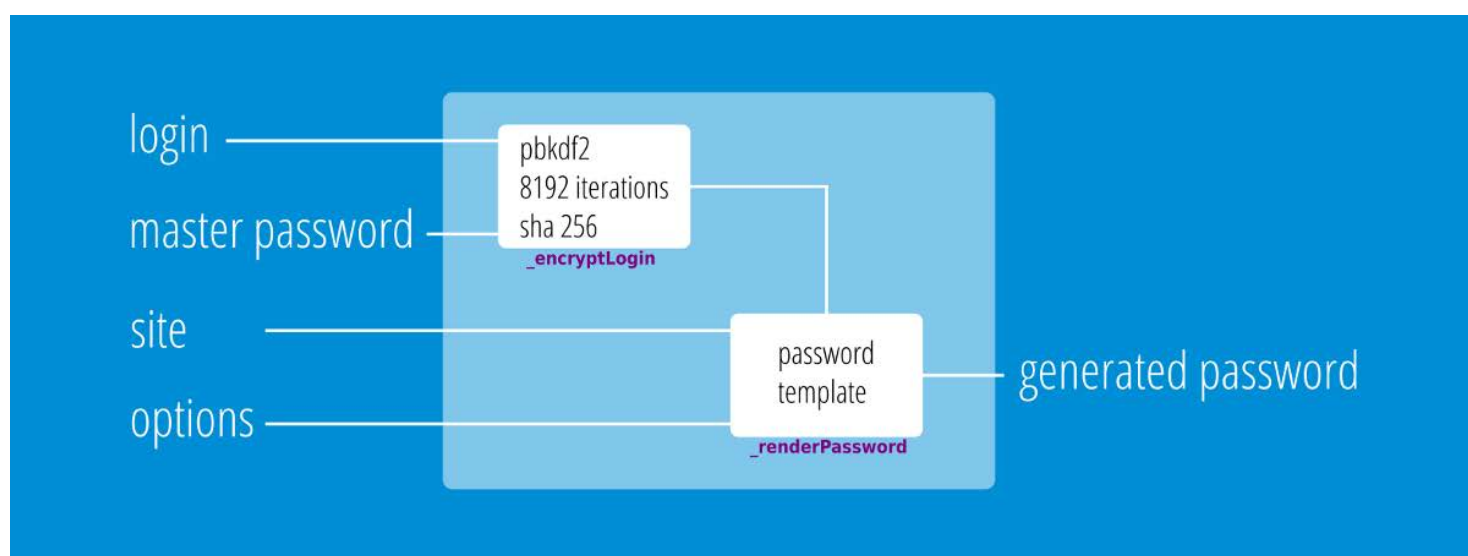
The screenshot shows the LessPass web interface. At the top is a blue header with the 'LessPass' logo and a shield icon. Below the header are three input fields: 'Site' (with a globe icon), 'Login' (with a person icon), and 'Master password' (with a lock icon). Below these fields is a blue 'Generate' button, a 'v2' button, and a settings icon (three horizontal lines). Under the buttons are four checked checkboxes: 'abc', 'ABC', '123', and '%!@'. Below the checkboxes are two sections: 'Length' and 'Counter'. The 'Length' section has a text input with '16' and two buttons, '-' and '+'. The 'Counter' section has a text input with '1' and two buttons, '-' and '+'. At the bottom is a 'save as default' button.

Из такой концепции сразу понятно главное достоинство подобного подхода — у вас вообще нет файла с паролями, как в других парольных менеджерах. Чего нет — то невозможно потерять. Теперь вместо извлечения уникального пароля из зашифрованного хранилища мы каждый раз заново генерируем этот пароль. Благодаря детерминированности функции и неизменности входных параметров всегда генерируются одни и те же уникальные пароли для всех сайтов.

Какая безопасность нужна для детерминированной функции? В первую очередь — чтобы по результату её работы нельзя было определить все её аргументы, тем более что некоторые аргументы уже известны злоумышленнику, как и сама функция.

Проще говоря, если злоумышленник знает два или три из четырёх аргументов, а также результат функции, он не должен узнать четвёртый аргумент — мастер-пароль.

Для защиты мастер-пароля от брутфорса вычисление уникальных паролей LessPass прогоняет 8192 итерации функции [PBKDF2](#) с хэш-функцией SHA-256.



Сгенерированный первой функцией хэш обрабатывается для соответствия шаблону, установленному третьим и четвёртым параметрами (набор используемых символов, длина пароля).

Теперь, чтобы «вспомнить» уникальный пароль для конкретного сайта — просто запускаем программу LessPass. Это крошечная программа состоит всего из [109 строчек](#).

Генерация паролей работает в виде скрипта на [сайте LessPass](#), или на клиентском компьютере. Выпущены соответствующие расширения [для Chrome](#) и [для Firefox](#). Скрипт генератора можно запустить и в локальном облаке. Например, с помощью локального облака [Cozy](#).

Таким образом, при использовании такого парольного менеджера невозможно потерять файл с паролями, потому что такого файла его не существует. Никаких проблем ввести уникальный пароль с любого устройства. Нужно только заново сгенерировать его.

Недостатки LessPass очевидны и вытекают из его достоинств. Самое главное, что при компрометации мастер-пароля все десятки или сотни производных уникальных паролей для всех сайтов сразу можно считать потерянными.

Второй недостаток — вы не можете нормально и удобно поменять пароль для конкретного сайта. Для этого придётся изменить один из параметров генерации паролей (Counter). Впоследствии придётся помнить, какой конкретно параметр использовался для каждого сайта. Где единица, где двойка, где тройка, и так далее. Кроме того, нужно помнить уникальные требования каждого сайта к паролям. Например, какие-то банковские приложения могут ограничить пароль только цифрами и длиной в шесть цифр. Для решения этой проблемы в LessPass реализованы профили для сайтов. В профиле хранится вся информация, необходимая для генерации пароля, кроме мастер-пароля.

Третий недостаток — для брутфорса пароля злоумышленнику не требуется физический доступ к компьютеру пользователя. Ему не нужен ваш файл с зашифрованными паролями. Чисто теоретически, это упрощает его действия. Пользователь вообще не заметит, что на него идёт атака.

Ситуация ухудшается тем, что в данной конкретной реализации LessPass использует всего 8192 итерации PBKDF2-SHA256. По [мнению специалистов](#), этого крайне недостаточно для надёжной защиты от брутфорса на GPU. Ещё несколько лет назад рекомендовалось минимум 100 000 итераций, а вычислительная мощность брутфоса примерно удваивается каждый год. Так что будем считать, что нынешняя реализация LessPass — просто демонстрационная версия, доказательство работоспособности концепции.

LessPass — не единственный детерминированный менеджер паролей, работающий на чистой функции. Есть и другие аналогичные программы, в том числе [Master Password App](#) и [Forgiva](#). У всех этих программ те же недостатки, о которых упоминалось выше. К тому же, в них нельзя импортировать свои старые пароли, так что при миграции на такую программу придётся заново генерировать все пароли.



Mailvelope

[\[Chrome Store\]](#) [\[GitHub\]](#)

OpenPGP шифрование почты веб-почты.



Multipass

[\[Opera Store\]](#) [\[Chrome Market\]](#) [\[GitHub\]](#) [\[Home Page\]](#)



nzbget-chrome

[\[Chrome Market\]](#) [\[GitHub\]](#)

interact with nzbget



Octotree

[\[Opera Store\]](#) [\[GitHub\]](#)

В левой части окна браузера будет создана панель с древовидной структурой репозитория для быстрого перехода по его содержимому.



Padlock

[\[Chrome Market\]](#) [\[GitHub\]](#) <https://padlock.io/>

OpenSource Password Manager

Proxy Switcher & Manager

[\[Opera Store\]](#) [\[Chrome Market\]](#) [\[Home Page\]](#) [\[GitHub\]](#)



pass-browser-chrome

[\[Home Page\]](#) [\[GitHub\]](#) [\[Chrome Store\]](#)



PDF Viewer

[\[Chrome Store\]](#)

Альтернативный просмотр PDF в браузере.



Proxy for Chrome

[\[Chrome Market\]](#)

Бесплатные прокси сервера.



Random User-Agent

[\[GitHub\]](#) [\[Chrome Store\]](#)



Reddit Enhancement Suite

[\[GitHub\]](#) [\[Home Page\]](#)



Remote Torrent Adder

[\[Chrome Store\]](#) [\[GitHub\]](#) [\[Wiki\]](#)

Позволяет автоматически добавлять торрент файлы в клиент, без необходимости это делать вручную.

RSS Detector

<https://addons.opera.com/ru/extensions/details/rss-detector/?display=en>



ScriptSafe

[\[Home Page\]](#) [\[Chrome Store\]](#) [\[GitHub\]](#)

Расширение блокирует скрипты, iFrame по умолчанию, использует чёрный список для блокирования нежелательного контента, и многое другое.



Smart HTTPS

[\[Home Page\]](#)

Расширение будет пытаться использовать HTTPS для каждой ссылки.



Smart RSS

[\[Opera Store\]](#) [\[GitHub\]](#)



StreamON

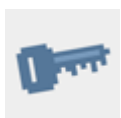
[\[GitHub\]](#)



Stylish

[\[Opera Store\]](#) [\[GitHub\]](#) [\[Wiki\]](#)

Управление пользовательскими стилями.



SuperGenPass

<https://chriszarate.github.io/supergenpass/>

<https://github.com/chriszarate/supergenpass>

FAQ <https://github.com/chriszarate/supergenpass/wiki/FAQ>



Tampermonkey

[\[Opera Store\]](#) [\[GitHub\]](#) [\[Home page\]](#)

Управление пользовательскими скриптами (userscript.js).



TrackMeNot

[\[Chrome Store\]](#) [\[GitHub\]](#) [\[Home page\]](#)

Препятствует отслеживанию генерируя фиктивные поисковые запросы, растворяя в них реальные и затрудняя сбор информации о пользовательских предпочтениях. Опция burst-mode лучше имитирует поведение человека, поскольку без нее запросы отсылаются через регулярные интервалы. Она также помогает избежать бана со стороны Google (поисковик перенаправляет на страницу для ввода капчи, если подозревает, что запросы с твоего IP-адреса отправляет бот). Если редирект происходит даже с burst-mode, просто измени интервал отправки ложных запросов на более длительный (скажем, десять в час).

Сам факт использования расширения для обфускации легко определяется сайтами и рекламными сетями. По умолчанию поисковые запросы в TrackMeNot выполняются только на английском языке. Теоретически можно указать в настройках русскоязычные RSS как источник ключевых слов, но на практике это приводит к сообщениям об ошибке плагина или отсеvu только английских терминов.



TransOver

https://github.com/artemave/translate_onhover



Translator

[\[Opera Store\]](#)

Автоматически переводит на выбранный язык выделенный текст. Также можно вставить свой текст и перевести его.



Twitch Live

[\[Chrome Store\]](#) [\[GitHub\]](#)

Уведомления о запуске трансляций на Twitch.tv



Type Sample

[\[Chrome Store\]](#) [\[Home page\]](#)

Bookmarklet позволяющий определить какой шрифт использует веб-сайт. Для его установки нужно перетащить кнопку на одну из панелей браузера.



uBlock Origin

[\[Opera Store\]](#) [\[GitHub\]](#) [\[Wiki\]](#)

Блокирует рекламу и сбор статистики в интернете на веб-страницах, плюс можно вручную выбирать элементы, которые необходимо скрыть. Поддержка белых списков сайтов, где реклама не будет блокироваться.

В связи с тем, что подписки по умолчанию блокируют некоторые сайты используемые многими пользователями далее идет описание правильной настройки uBlock Origin.

Настройка подписок: В настройках дополнения отключить подписки:

1) uBlock filters – Badware risks, 2) Peter Lowe's Ad server list, 3) Malware Domain List, 4) Malware domains.

Включить подписки:

1) Anti-Adblock Killer | Reek, 2) Basic tracking list by Disconnect, 3) RU: RU AdList.

Остальные подписки по умолчанию.

Кастомные правила:

Блокирование юзера по нику на форуме ru-board:

`forum.ru-board.com##a.tpc[href$="A1exander1"] ~ .post`

Примечание. Для того чтобы в расширении заработала подписка **Anti-Adblock Killer** необходимо установить одноимённый скрипт <http://reek.github.io/anti-adblock-killer/> а потом активировать фильтр в настройках расширения.

Дополнение:

[RU AdList CSS Fixes](#) — стили оформления для корректной блокировки рекламы на отдельных сайтах, не реализуемые средствами блокировщика.

[RU AdList JS Fixes](#) —

[Prebake Cookie removal](#) [\[GitHub\]](#) — список фильтров для блокирования навязчивых cookies. Для активаций фильтра перейти в настройки → Сторонние фильтры → Пользовательские и выбрать фильтр.

[Форум поддержки RU AdList](#)

[Известные проблемы](#)

<https://easylist.to/>

На самом деле, существуют всего 2 подписки - EasyList (и региональные дополнения, в данном случае RU Adlist) и Adguard. И если синтаксис подписки Adguard полностью поддерживает только одноимённый блокиер, то RU Adlist используют BCE остальные - Adblock, Adblock Plus, uBlock, uBO и пр.



uMatrix

[\[Opera Store\]](#) [\[GitHub\]](#) [\[Wiki\]](#) [\[Wiki+\]](#)

Резалка кросс-доменных запросов. Блокирует запросы в зависимости от типа контента. Также умеет блокировать XHR (отдельно от обычных запросов), скрипты, куки, рефереры, плагины, медиа (HTML5 аудио и видео) и вебсокеты (только на Firefox). Присутствует частичная поддержка фильтров Adblock+ и возможность блокировки фоновых запросов браузера (behind-the-scene HTTP requests).

Алгоритм блокирования кук несколько отличается от того, что у Cookie Monster и Cookie Controller - первые два не дают сайтам устанавливать куки, а uMatrix дает ставить, но не дает читать, убирая из всех HTTP-запросов заголовков Cookie (но при этом через document.cookie установленные куки все еще видны), а через некоторое время - подчищает. Также в отличие от CM/CC, uMatrix не умеет запрещать писать в DOM Storage, а может только периодически его очищать.

Элементы интерфейса и основные принципы работы:

A B C D E F									
uMatrix 0.9.3.4									
github.com	all	cookie	css	image	plugin	script	XHR	frame	other
1st-party									
github.com	7								
api.github.com							1		
assets-cdn.github.com		5			3				
avatars1.githubusercontent.com			1						
cloud.githubusercontent.com			1						
githubapp.com									
collector.githubapp.com			1						
google-analytics.com									
www.google-analytics.com			1						

- A** — Выпадающее меню с выбором области действия фильтров: глобально/для домена/для сайта. Остальные кнопки будут влиять на выбранную область.
- B** — Включение/выключение фильтров.
- C** — Подмена useragent, referrer.
- D** — Сохранение временных пользовательских настроек
- E** — Сброс временных (не сохранённых) настроек.
- F** — Перегрузка страницы с новыми настройками.

Расширение может работать в одном из двух режимов:

- 1) блокировать всё, пропускать выборочно (белые списки) - режим по умолчанию.
- 2) пропускать всё, блокировать выборочно (чёрные списки). В этом режиме автоматически блокируются только известные рекламные сайты и трекеры.

Режим устанавливается кликом по полю с надписью «all»:



После выбора области действия фильтров и режима работы, кликом по названиям в верхнем поле можно глобально разрешить или запретить загрузку конкретных элементов. Например, пропускать все картинки и css, но блокировать плагины и скрипты. После чего, с помощью матрицы, можно менять правила запросов для конкретного сайта или домена. Такие настройки будут временными, чтобы их сохранить, нужно нажать на иконку с замком (D).

В отношении cookie расширение работает по принципу «впускать всех, а выпускать по списку». Т.е. все cookie, даже заблокированные, попадают на компьютер, но сайт может прочитать только те, что разрешены. В общих настройках можно включить автоматическое удаление заблокированных cookie, а также задать время, через которое будут удаляться session cookies.

Behind-the-scene HTTP requests. Это фоновые HTTP запросы, которые совершают другие расширения и сам браузер. Данная функция станет доступна, если нажать на иконку HTTP Switchboard в тулбаре браузера, находясь на странице настройки расширения.



uTorrent Link Sender

[\[Chrome Store\]](#) [\[GitHub\]](#)

Добавляет в контекстное меню пункт для отправки ссылок начинающихся с magnet:? или заканчивающихся .torrent в uTorrent Web UI.



Violent monkey

[\[Opera Store\]](#) [\[GitHub\]](#)

Управление пользовательскими скриптами (userscript.js).



WebRTC Leak Prevent

[\[Chrome Market\]](#)

Убирает утечку dns и ip через webrtc, но могут быть проблемы с видеосвязью.



WhatFont

[\[Chrome Store\]](#) [\[Home page\]](#) [\[GitHub\]](#)

Определение используемого шрифта на веб-странице.



YouTube Notifications

<https://github.com/Wassup789/YouTube-Notifications>



Доступ к Рутрекеру

[\[Opera Store\]](#)

[\[Chrome Market\]](#)

<https://dostup-rutracker.org/>

Как проверить, что все работает?

Устанавливаем плагин, идем на rutracker.org.

Открываем панель разработчика (F12 windows, cmd+alt+i Mac).

Заходим во вкладку "Console" или "Консоль".

На всякий случай еще раз обновляем страницу.

Если увидели "[rutracker-проху] success" - все в порядке.



Обход блокировок Рунета

<https://chrome.google.com/webstore/detail/обход-блокировок-рунета/npgcnondjocldhldegnakemclmfkngch>

<https://github.com/anticensorship-russia/chromium-extension>

Скрипты

Общие сведения

Для установки и управления скриптами нужно установить расширение **Violent monkey** [[Opera Store](#)] [[GitHub](#)] или **Tampermonkey** [[Opera Store](#)] [[GitHub](#)] [[Home page](#)]

Большинство популярных скриптов можно найти на <https://openuserjs.org/> и <https://greasyfork.org/>

Популярные скрипты

[Adobe Download Enabler](#) [[GitHub](#)] — включает прямое скачивание файлов Adobe Creative Cloud.

[AdsBypasser](#) — [[OpenUserJS](#)] [[GitHub](#)]

[Amazon URL Cleaner](#) — показывает сокращённый url для товара

[Anti-Adblock Killer Reek](#) — [[Home Page](#)] [[GitHub](#)] [[OpenUserJS](#)] разрешает AdBlock, uBlock и др. блокировщики рекламы где они запрещены.

[AutoSaveDiv](#) — локально сохраняет содержимое поля textarea в котором был набран текст, тем самым позволяя восстановить набранный текст, например после случайного закрытия вкладки или падения (crash) браузера.

[BT MetaSearch](#) — поиск торрент-раздачи между несколькими трекерами одновременно.

[Clean links](#) — clean up links. Remove targets, embedded redirects, and window.open() style links.

[Download YouTube Videos as MP4](#) — [[GitHub](#)] [[Opera Store](#)] скачивание видео с YouTube.

[FuckFuckAdblock](#) — блокирует скрипт FuckAdblock.js определяющий использование блокировщиков рекламы.

[General URL Cleaner](#) —

[Google Hit Hider by Domain](#) — (фильтр поиска/блокирование сайтов) [[Greasyfork](#)] [[Openuserjs](#)] Скрипт позволяет скрыть сайты из результатов поиска Google, которые вас не интересуют. Он также работает и с DuckDuckGo, Startpage.com, Bing и Yahoo.

http://www.jeffersonscher.com/gm/Google-Hit-Hider-by-Domain_About_v160.pdf

[Google Translate](#) —

[Habrahabr Enhancement Suite](#) —

[imgur https](#) — при переходе на одноимённый сайт «подменяет» http на https.

[Linkification](#) —

[Linkify plus](#) — [\[GitHub\]](#) turn plain text URLs into links. Supports http, https, ftp, email addresses.

[Linkify Plus Plus](#) — [\[GitHub\]](#) преобразовывает текстовую ссылку в кликабельную.

[LinkDragSelectionForChrome](#) — позволяет выделить ссылку с любого места как текст.

[NZB-RSS direct link](#) — add convenient links to the NZB.

[nzbget enter submit](#) — enhance the NZBGet interface's in page forms so that pressing enter will submit them.

[No Dereferers](#) [\[GitHub\]](#) — удаляет dereferers из ссылки.

[Protect textarea](#) — protect from closing or navigating away from a web page with changed textareas.

[Reddit comment expander](#) — expand all comments. Useful when your default expand threshold is high, for popular subs, but less popular subs mean you need to expand all of the (very few) comments to see them.

[Reddit no link tracking](#) — remove outbound link tracking on Reddit.

[Window open butler](#) — prevent window.open() calls, but also provide a UI to recover the blocked window in the (rare) case that it's actually desired.

[Rutracker Re-Downloader](#) — добавляет раздачу в список отслеживания, проверяет обновления для отдельных или нескольких торрентов из списка. После проверки для тех раздач, которыеновились, в списке обновляется ссылка на скачивание торрент-файла.

[Rutracker Personal Ban List](#) — скрывает сообщения пользователя при добавлений его никнейма в чёрный список.

[Secure share on Imgur](#) —

[Select like Opera](#) — позволяет выделить ссылку с любого места.

[Text to Link](#) — преобразовывает текстовую ссылку в кликабельную.

Альтернатива: <https://greasyfork.org/en/scripts/19801-text-to-link> и

<https://greasyfork.org/en/scripts/22837-text-to-link-mod>

[Textarea BackUp](#) — сохраняет набранный текст внутри textareas and contentEditables, тем самым позволяя восстановить его, например в случае падения браузера или случайного выключения компьютера. Истекает через 30м (значение по умолчанию).

Альтернатива: <https://greasyfork.org/en/scripts/19509-textarea-backup-with-expiry-fix>

[Type Sample](#) — bookmarklet позволяющий определить какой шрифт используется на веб-странице. Для его установки нужно перетащить кнопку на одну из панелей браузера.

[WhatFont](#) — bookmarklet для определения используемого веб-шрифта на сайте.

[Youtube +](#) — [[OpenUserJS](#)] скрипт предоставляет разные возможности надстройки для одноимённого сайта, такие как: проигрывание видео во всплывающем окне; включение 60fps; навигация внутри видео по фреймам; создание и сохранение скриншота с любого места на видео и многое другое.

[Youtube + Vimeo popup](#) — отображение видео во всплывающем окне.

Стили

Популярные стили

Современный Rutor

<https://userstyles.org/styles/118305/rutor>

Habrahabr night mode

https://github.com/WaveCutz/habrahabr.ru_night-mode

<https://userstyles.org/styles/101604/new-habr-night-mode>

Форум Overclockers.ru

Доработка форума Overclockers.ru, главного сайта и Персональных страниц

<https://greasyfork.org/ru/scripts/1866-Форум-overclockers-ru>

Вопросы и ответы

Назначение браузера браузером по умолчанию. Как открывать ссылки из внешних приложений, имея portable версию браузера? Добавление браузера в «Программы по умолчанию» для Windows 7

Выполнить reg-сценарий, предварительно заменив путь к лаунчеру в строке ApplicationIcon и в разделе [HKEY_LOCAL_MACHINE\Software\Classes\OperaURL\shell\open\command], следующего содержания:

```
Windows Registry Editor Version 5.00
```

```
; Infamous capabilities:
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Opera\Capabilities]
```

```
"ApplicationDescription"="Opera - for me"
```

```
"ApplicationIcon"="C:\\Opera\\launcher.exe,0"
```

```
"ApplicationName"="Opera"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Opera\Capabilities\FileAssociations]
```

```
".htm"="OperaURL"
```

```
".html"="OperaURL"
```

```
".shtml"="OperaURL"
```

```
".xht"="OperaURL"
```

```
".xhtml"="OperaURL"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Opera\Capabilities\URLAssociations]
```

```
"ftp"="OperaURL"
```

```
"http"="OperaURL"
```

```
"https"="OperaURL"
```

```
; Register to Default Programs
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]
```

```
"Opera"="Software\\Opera\\Capabilities"
```

```
; OperaURL HANDLER:
```

```
[HKEY_LOCAL_MACHINE\Software\Classes\OperaURL]
```

```
@="Opera Document"
```

```
"FriendlyTypeName"="Opera Document"
```

```
[HKEY_LOCAL_MACHINE\Software\Classes\OperaURL\shell]
```

```
[HKEY_LOCAL_MACHINE\Software\Classes\OperaURL\shell\open]
```

```
[HKEY_LOCAL_MACHINE\Software\Classes\OperaURL\shell\open\command]  
@="\"C:\\Opera\\launcher.exe\" -- \"%1\""
```

Далее необходимо задать программу по умолчанию в настройках ОС.

Удаление из программ по умолчанию и реестра

Выполнить reg-сценарий следующего содержания:

```
Windows Registry Editor Version 5.00
```

```
[-HKEY_LOCAL_MACHINE\SOFTWARE\Classes\OperaURL]  
[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]  
"Opera"=-
```

Как настроить браузер для работы с проху при использовании ssh-туннеля?

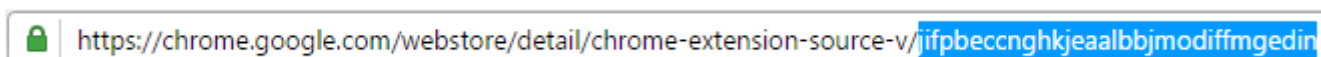
Windows

1. Запустить SSH-туннель
2. Открыть меню браузера → Настройки (Alt+P) → Браузер → Сеть → Изменить настройки прокси-сервера
3. В открывшемся окне нажать кнопку Настройки сети, отметить Использовать прокси-сервер для локальных подключений (не применяется для коммутируемых или VPN-подключений) и нажать кнопку Дополнительно. В 4 строке (Socks) ввести localhost и порт 8080 → ОК → Готово.

Как скачать и сохранить Chrome расширение из магазина?

Способ №1. Использование специального URL

Если расширение не установлено, открыть его страницу установки и скопировать идентификатор расширения. Как правило, extension ID является последней частью URL:



The image shows a browser address bar with a URL: <https://chrome.google.com/webstore/detail/chrome-extension-source-v/jifpbccnghkjaalbbjmodiffmgedin>. The extension ID 'jifpbccnghkjaalbbjmodiffmgedin' is highlighted in blue.

Получив таким образом extension ID, выполнить в другом браузере, например Firefox, IE или Edge, заменив "<EXTENSION_ID>" на скопированный идентификатор расширения, следующий URL:

https://clients2.google.com/service/update2/crx?response=redirect&prodversion=49.0&x=id%3D<Extension_ID>%26installsource%3Dondemand%26uc

Важно. Если попытаться открыть URL в браузере, он не позволит загрузить расширение.

Способ №2. Расширение

Скачать и установить расширение **Chrome extension source viewer** [\[Chrome Market\]](#)

Запуск браузер с разными профилями (неполная версия)

Windows

1. Создать дубликат ярлыка браузера.
2. Открыть свойства ярлыка.
3. Добавить аргумент командной строки в поле «Объект»: `--profile-directory="profile name"`
4. Повторить эти действия для всех профилей, которые необходимо создать, или уже созданы.

Linux

1. В Linux, можно создать специальный **.desktop* файл, чтобы запустить браузер с другим профилем.
2. Открыть папку файлового менеджера: `/usr/share/applications`
3. Найти файл с именем **.desktop*
4. Скопировать этот файл в папку: `/home/your user name/.local/share/applications`
5. Если такой папки нет, то создать её.
6. Переименовать `~/.local/share/applications/*.desktop` файл, чтобы указать, что он будет относиться к пользовательскому профилю.
7. Change the Name section to something like Google Chrome (My Profile):
8. Change all the Exec sections in the file to make them look like this:
9. `/usr/bin/google-chrome-stable --profile-directory="my other profile" %U`
10. So, you need to add the `--profile-directory` parameter to command line.
11. Повторить эти действия для всех профилей, которые необходимо создать, или уже созданы.
12. Пользовательские профили будут видны в меню приложений.

Баги

Исчезновение паролей при входе в ОС под учётной записью администратора с последующим возвращением к обычному пользователю

Пароли слетают если запустить Opera в USB варианте при работе под учётной записью администратора.

Для установленной обычной версией по идее тоже должны.