Безопасность данных при работе в Глобальной сети сегодня не ограничивается только защитой пользователя от вирусов или мошенников. Фактически, любое действие — просмотр и загрузка контента, оставление комментария, переход на веб-страницу и т. д. — может использоваться в коммерческих целях или злоумышленниками. Как избежать этого и обеспечить достойный уровень анонимности в Интернете? CHIP предлагает несколько вариантов решения проблемы.

Способы идентификации

Основным методом «вычисления» личности пользователя в Сети является определение его IP-адреса, который позволяет вычислить географическое расположение человека и даже узнать точно, кто это такой. Этим способом активно пользуются как правоохранительные органы через СОРМ (обязательная к установке по требованию ФСБ система технических средств для обеспечения функций оперативно-розыскных мероприятий, которая по закону о связи есть у любого телеком-оператора, работающего на территории России),так и другие заинтересованные стороны через аналогичные поисково-аналитические системы сбора информации. На вычисление пользователя по IP может уйти совсем немного времени. Конкретный адрес находится в пуле выданных определенному оператору адресов, и правоохранительным органам достаточно сделать соответствующий запрос на раскрытие персональных данных абонента связи. Если IP динамически назначаемый, потребуется чуть больше времени. В этом случае провайдер раскроет подсеть, включающую определенный ограниченный список адресов, перебор которых позволит с нескольких попыток вычислить необходимого человека.

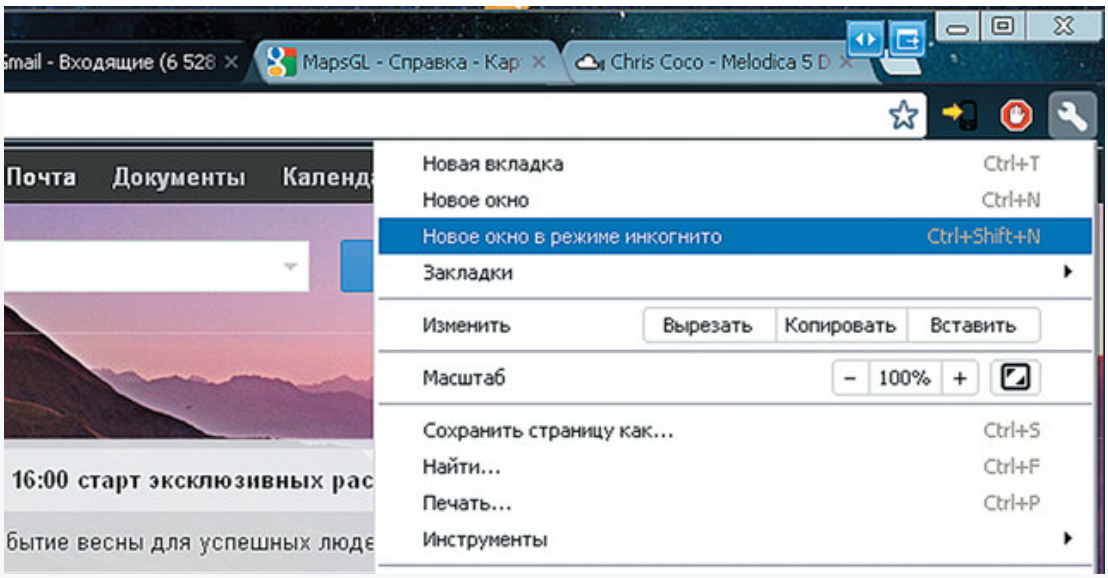
Понять, где он находится, еще проще: все IP связаны с MAC-адресами оборудования, на котором работает пользователь, — ноутбуков, компьютеров, планшетов и смартфонов. Те, в свою очередь, получают доступ в Сеть от телеком-оборудования, которое установлено в конкретном месте на карте (распределительные маршрутизаторы, вышки базовых станций, Wi-Fi-роутеры и т. д.). Именно поэтому сбор IP-адресов без ведома пользователей не раз приводил к громким скандалам, связанным с приватностью. Так, экипажи картографов Google умудрялись захватывать данные домашних беспроводных сетей и создавали таким образом интерактивную карту местонахождения пользователей, а компания Apple следила за владельцами iOS-устройств, собирая геолокационные сведения даже при отключенном GPS по базовым станциям операторов связи. Сейчас же информация о действиях в Сети активно собирается правообладателями, которые отслеживают загрузку и обмен медиаконтентом в Интернете, правоохранительными органами и многими рекламномаркетинговыми службами, которые составляют на интернет-пользователей «досье», чтобы потом навязчиво предлагать им товары и услуги.

Помимо IP-адреса в идентификации личности помогают и cookies — служебные файлы, в которых хранится информация о сеансах работы пользователя с веб-ресурсом (ОС, браузер, разрешение экрана, региональные настройки, часовой пояс и т. д.), а также логины и пароли, которые тоже могут вывести на след человека. Многие веб-сайты ставят в систему специальные следящие cookies, которые мониторят активность посетителей не только на этом ресурсе, но и на других. Не последнюю роль играют и социальные сети, накапливающие растущий с каждым мгновением массив информации о почти каждом человеке, который когда-либо был в них зарегистрирован. Если вы не выходите из своего аккаунта в соцсети, когда работаете в Интернете, то велик шанс, что в сервисе остается история просмотра сайтов, а если вы еще и активно «лайкаете» материалы на разных онлайн-ресурсах, то эти данные сохраняются в социальных сетях даже после удаления анкеты (если вы, конечно,вообще сможете ее удалить).

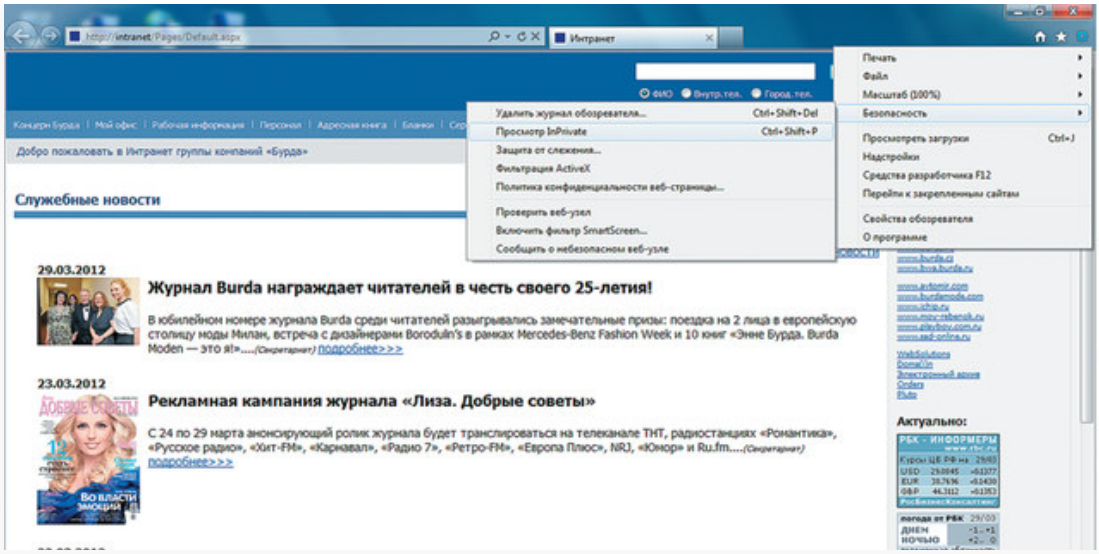
Способ первый: приватные режимы браузеров

В последние два года ведущие разработчики интернет-обозревателей (Mozilla Firefox, Internet Explorer, Google Chrome, Opera) начали оснащать свои продукты специальной функцией работы инкогнито. Этот режим предполагает запуск пользовательской

сессии, в течение которой в истории поиска и в журнале посещений не появляется ссылок на посещенные сайты. Также браузер самостоятельно удалит все cookies, временные файлы и введенные в регистрационных формах данные после завершения сессии (закрытия всех окон и вкладок в режиме инкогнито) — останутся только созданные закладки и загруженные файлы. Этот режим также отключает расширения браузера, которые используют личные данные пользователя. Если потребуется, их придется активировать по отдельности вручную в соответствующих разделах настроек.



Google Chrome: комбинация клавиш «Ctrl+Shift+N» или пункт меню «Новое окно в режиме инкогнито»

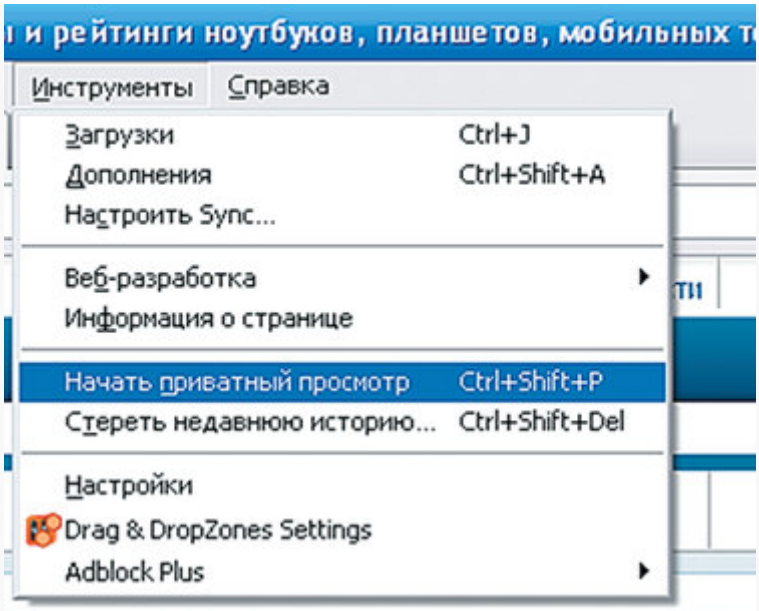


Internet Explorer: «Ctrl+Shift+P» или пункт «Просмотр InPrivate» в меню «Настройки | Безопасность»

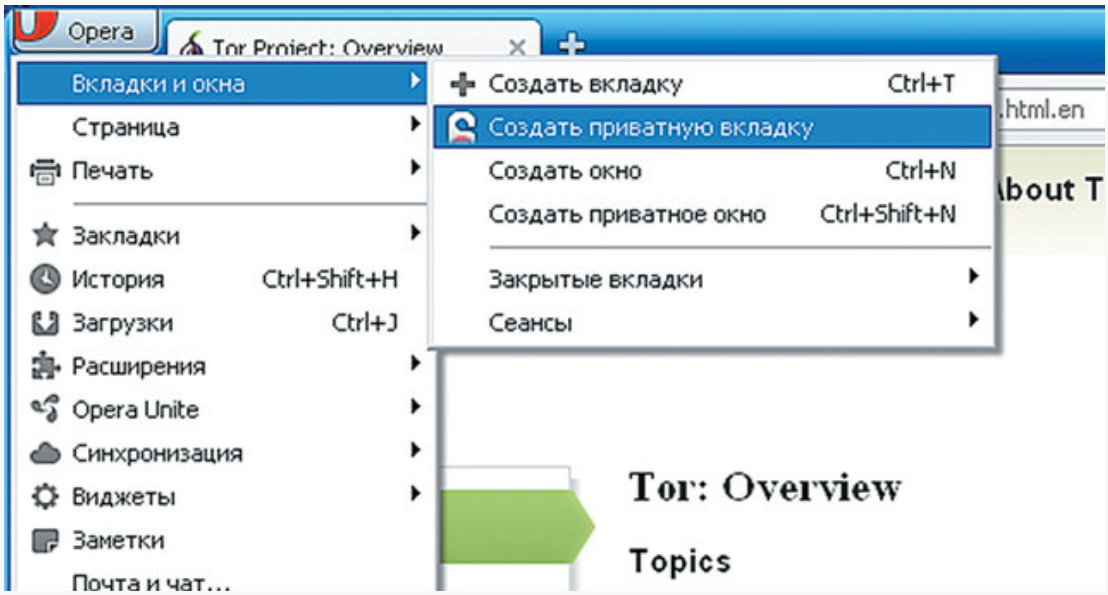
На мобильных устройствах режим приватности реализован только в вышедшей недавно публичной бета-версии Google Chrome для Android. Порты остальных браузеров не имеют такой функции.

На волне разбирательств с рекламными службами, отслеживающими активность пользователей в Сети по cookies, чтобы затем навязчиво предлагать им товары и услуги, в современных браузерах реализован и другой механизм приватности,

связанный с запретом наблюдения за пользовательской активностью по заголовкам веб-страниц. Технология Do not track сейчас применяется в Mozilla Firefox, Google Chrome, Internet Explorer и Safari. В некоторых версиях этих браузеров она включена изначально, а в других случаях ее надо активировать самостоятельно.



Mozilla Firefox: «Ctrl+Shift+P» или команда «Начать приватный просмотр»в меню «Инструменты». При работе в этом режиме браузер восстановит открытые до запуска приватного просмотра вкладки по окончании «маскировки»



Opera: пункт меню «Opera | Вкладки и окна | Создать приватную вкладку». Также можно кликнуть правой кнопкой мыши по пустому месту в заголовке окна и выбрать «Создать приватную вкладку»

Анонимайзеры и прокси

Еще один действенный метод обеспечения приватности в Сети — применение средств анонимизации и работа с интернет-сервисами через прокси-серверы. Это требует определенной настройки компьютера и чаще всего приводит к замедлению скорости

обмена данными, отключает определенные функции (например, не будут работать Flash-анимация и ActiveX-содержимое) и ограничивает активность пользователя (в браузере нельзя будет открывать файлы для просмотра и загружать их через встроенный менеджер закачек) из-за необходимости соблюдения приватности. Кроме того, вполне вероятно, что работа под прокси будет недолгой: адреса этих серверов активно блокируются для предотвращения массовых рассылок спама, DDoS-атак, несанкционированных проникновений и т. д.

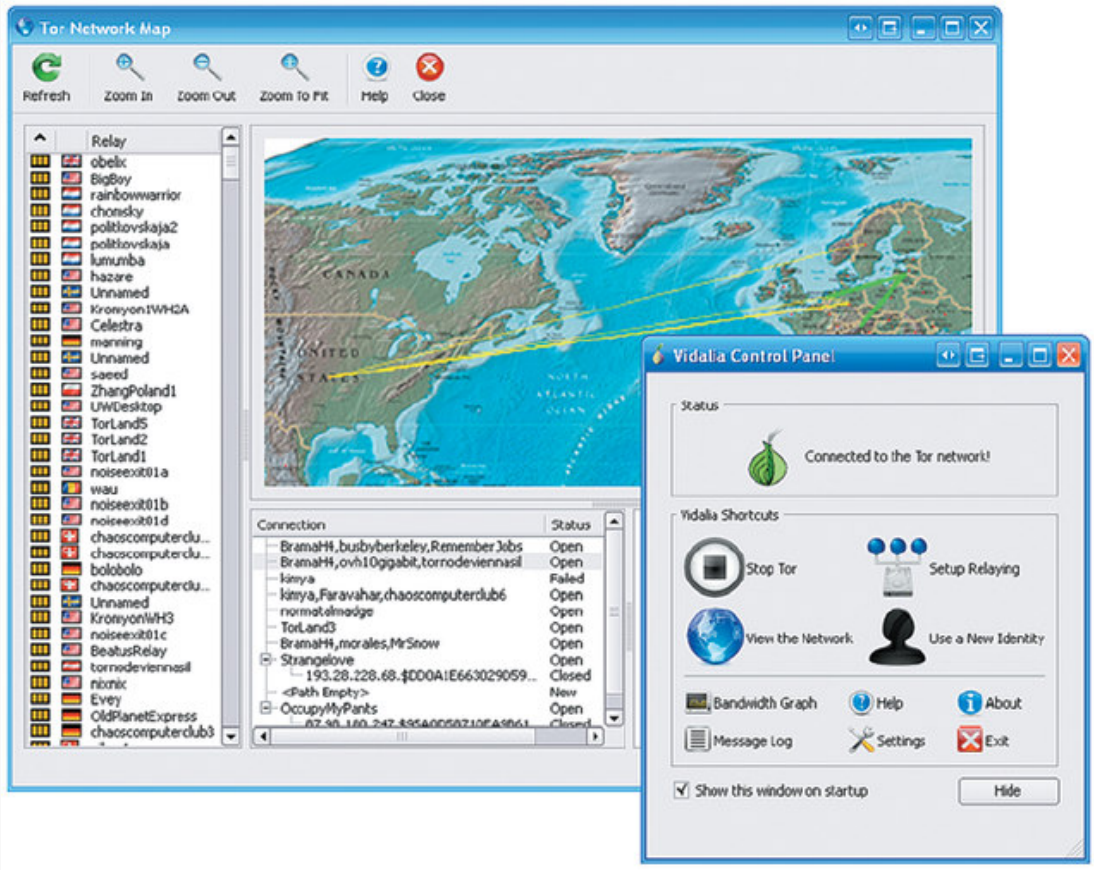
«Анонимизироваться» можно и путем подмены IP-адреса — такие программы были особо популярны несколько лет назад, однако сейчас они менее востребованы по перечисленным выше причинам. В своем описании их создатели заявляют о «скрытии IP» — под этим понимается смена и переадресация на один из списков прокси, который менее «засвечен» в Глобальной сети, чем все остальные. Более надежный способ — использование специальных клиентов, предлагающих организовать распределенный P2P-обмен трафиком, в котором не будет возможности «найти концы». Такие решения сегодня более актуальны, поскольку в них используется не некий список серверов, а другие IP-адреса конкретных пользователей Интернета, которые, естественно, очень быстро сменяют друг друга, передавая разбитую на фрагменты информацию. Обвинить их всех в нелегальной деятельности будет крайне затруднительно (но возможно, поскольку прецеденты вычисления пользователей BitTorrent, задействующих анонимайзеры, имели место). К таким программам относятся Tor, I2P и JAP.

Существуют способы перехвата и анализа трафика в публичных сетях. Зная, с какими адресами в Интернете вы устанавливаете соединение, можно как минимум узнать ваши предпочтения и поведение. Лучшее средство от «подглядывания» за вашим трафиком — Tor, децентрализованная сеть прокси-серверов. В составе программы есть анонимайзер TCP/IP-трафика и прокси-фильтр содержимого веб-страниц, который дополнительно обеспечивает анонимность. Весь трафик шифруется, и его невозможно перехватить на стороне провайдера, поскольку маршруты пересылки пакетов делятся на цепочки переходов между узлами сети, которые постоянно изменяются (каждые десять минут). В настоящее время Tor функционирует за счет порядка 2500 распределенных серверовнодов, к которым производится попеременное «многослойное» подключение с шифрованием. По умолчанию каждый пакет данных внутри сети проходит через три территориально удаленных нода, выбираемых случайным образом, будучи зашифрован тремя ключами безопасности. На каждом ноде соответствующая защита снимается для того, чтобы программа знала, в каком направлении далее отправляется фрагмент данных — это похоже на то, как чистят луковицу или капусту.

Кратко: Что надо знать про TOR?

Tor помогает предотвратить отслеживания маршрута передаваемых данных.
Программное обеспечение строит цепочки шифрованных соединений.
Подготовка

Для настройки Tor на компьютере лучше скачать готовые сборки анонимайзера вместе с прокси-сервером и браузером Aurora (форк-версия Firefox) с сайта проекта torproject.org. После установки приложения (лучше всего на флеш-накопитель) запустится клиент для прокси-сервера и браузер, в котором уже будут активированы все параметры для анонимизации.



Пользователи Tor запускают прокси-сервер на своем компьютере и становятся одним из узлов сети

Принцип работы

Tor-клиент пользователя получает список узлов от сервера доступа к ресурсам сети. Затем выбирается случайный путь до конечного сервера (схема 1). При подключении позже другого сайта цепочка узлов будет изменена (схема 2).

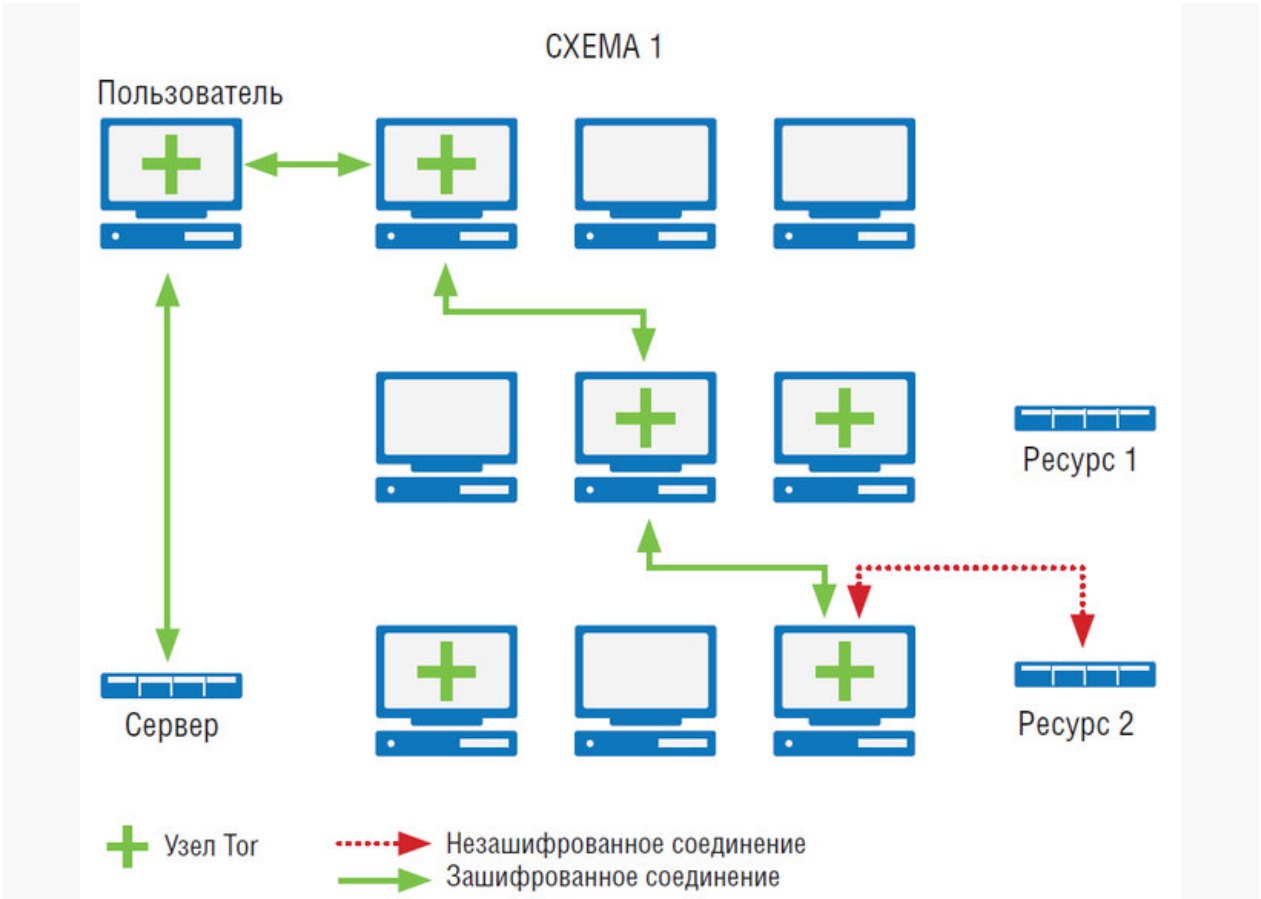


СХЕМА 1
Пользователь
Ресурс 1
Сервер
Ресурс 2
Узел Tor
Незашифрованное соединение
Зашифрованное соединение

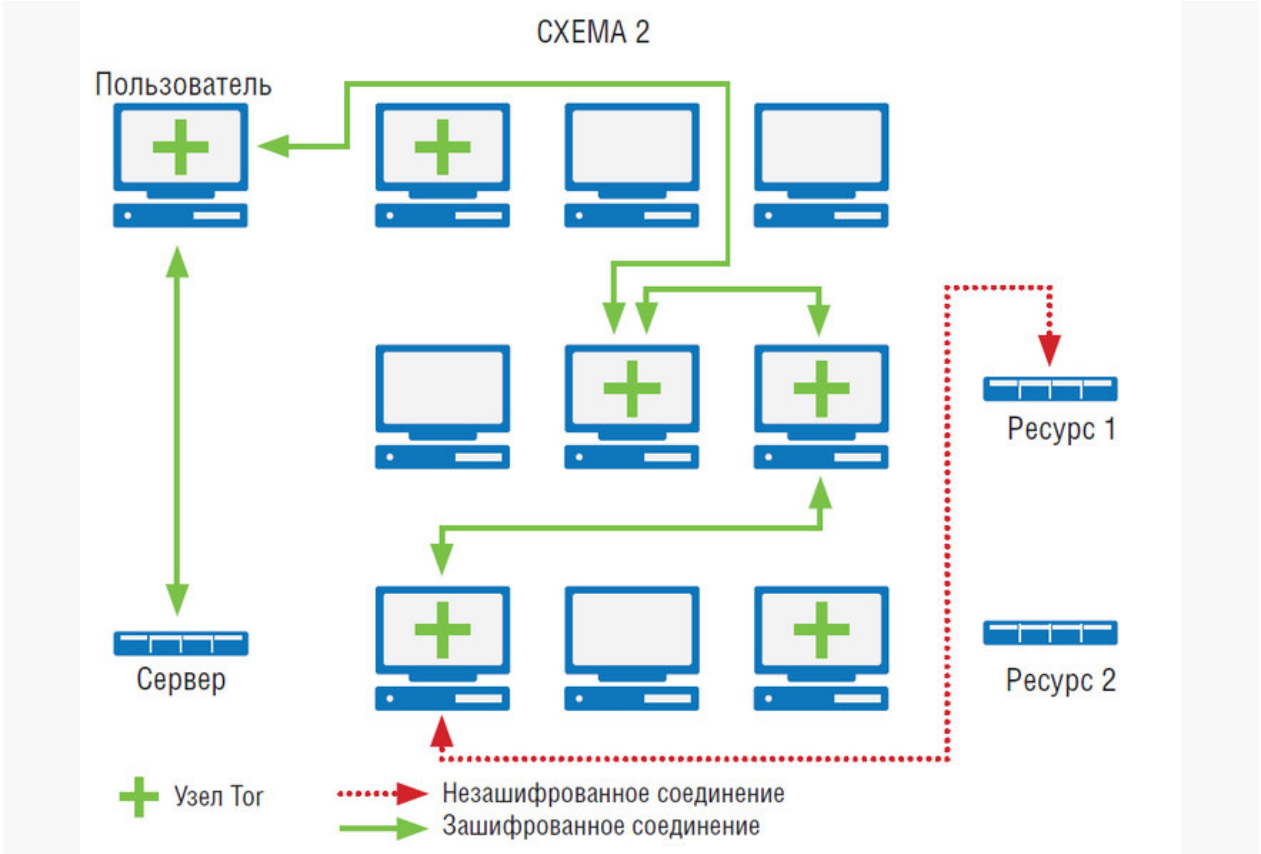


СХЕМА 2
Пользователь
Ресурс 1
Сервер
Ресурс 2
Узел Tor
Незашифрованное соединение
Зашифрованное соединение

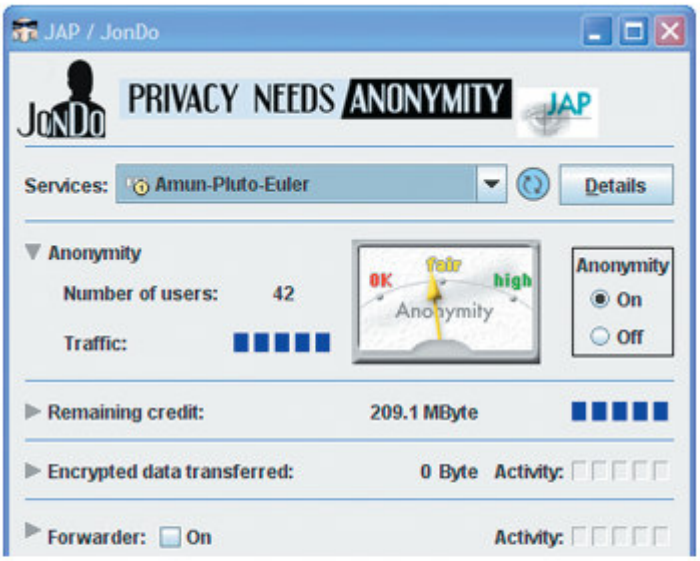
Дополнительно

Другие сервисы

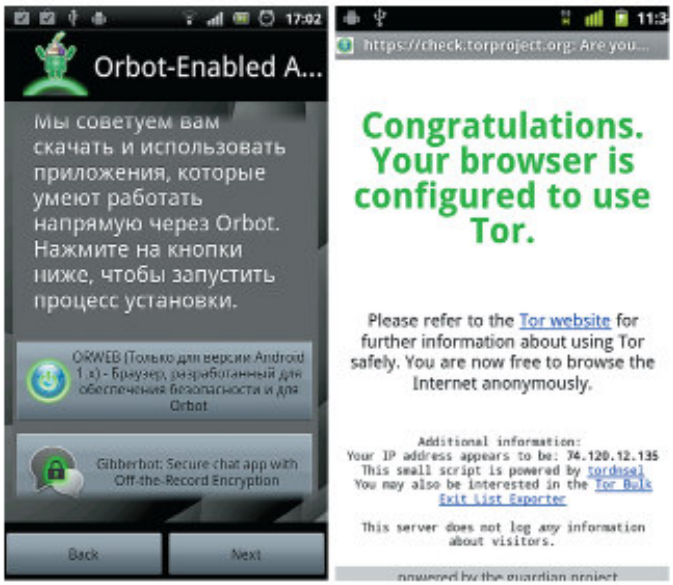
JAP (anon.inf.tu-dresden.de) скрывает вашу личность, пропуская трафик через цепочку микс-серверов до тех пор, пока ваш адрес не становится невозможно отследить. В пиринговой сети Netsukuku (netsukuku.freaknet.org) вместо привычной для IP-сетей DNS создана собственная ANDNA, которая делает каждый узел маршрутизатором трафика.

Мобильная анонимность

Для мобильных устройств на базе Андроид создано приложение, использующее технологию и код проекта Tor, — Orbot. Это консоль Tor для подключения программ и сервисов для устройств с root-доступом. Прочие же аппараты могут работать с Tor через браузер Orweb. Также прокси-сеть поддерживает мессенджер Gibberbot.



JAP анонимизирует только HTTP-трафик. В отличие от Tor, здесь пользователь не может менять цепочку прокси-серверов на произвольную



Клиент сети Tor для Андроид носит название Orbot. Если на смартфоне нет прав root, с Tor могут работать только специальный браузер Orweb и мессенджер Gibberbot

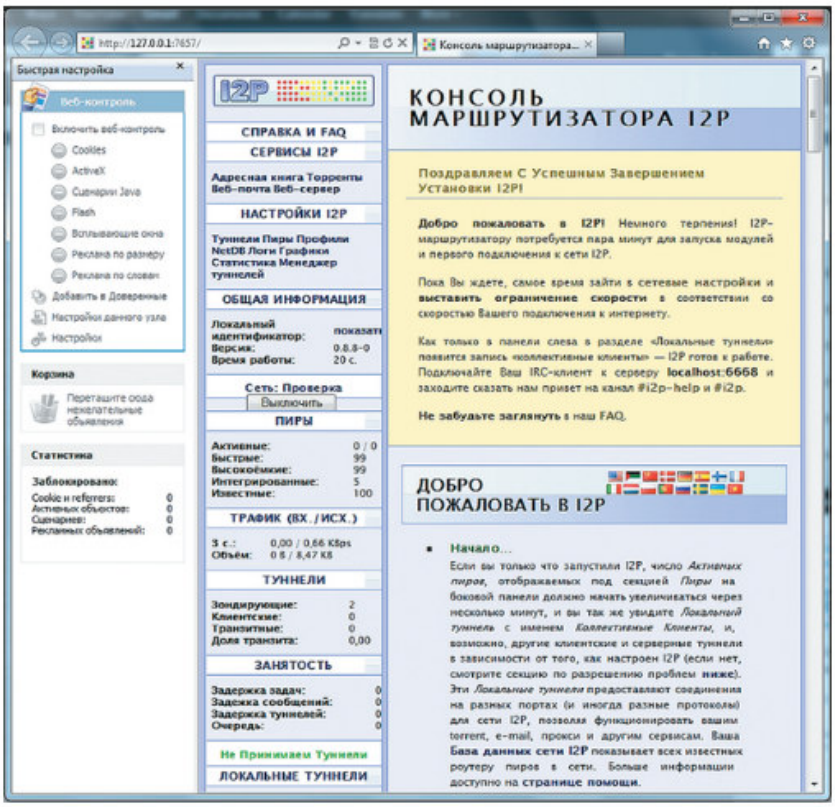
Следы в Сети

О среднестатистическом пользователе в Сети сегодня известно «по ту сторону экрана» даже больше, чем он может себе представить. На сайте youhavedownloaded.com можно увидеть, какие IP-адреса копировали торрент-файлы и файлы с файлообменных хостингов (используются сведения из DHT, где хранятся метки компьютеров, участвующих в раздаче, и временные лимиты). Впрочем, эта информация не всегда приводит к конечному пользователю, так как зачастую IP-адрес указывает на целую локальную сеть. На сайте можно посмотреть статистику и по собственному адресу.

Параллельный Интернет

I2P — это проект создания шифрованной сети, аналогичной по смыслу пиринговым, но не зависящей от IP-адресов и DNS-адресации (сайты имеют URL вида sitename.i2p). Она децентрализована, как и обычный торрент-трекер (сходство усиливается за счет системы распределения имен по DHT), при этом не требует подключения или аренды какого-либо серверного оборудования, а сам трафик, как и в Tor, является транзитным и делится между всеми посетителями. Формально все пользователи ПО-ретранслятора, которое расшифровывает и зашифровывает входящий и исходящий трафик в I2P, могут использовать свои компьютеры в роли веб-сервера и открыть анонимный сайт в I2P за пару минут (есть мини-веб-сервер с поддержкой CGI-скриптов и Perl). По большому счету, сеть напоминает реализацию шуток программистов о скачивании программ с localhost — действительно, все данные замыкаются на конкретной рабочей станции, которая выходит в I2P, но которую при этом невозможно вычислить извне. После установки кроссплатформенного клиентского ПО посещать сайты в I2P можно через обычный веб-браузер. Для этого необходимо задать в нем адрес прокси 127.0.0.1:4444. Также попасть на эти сайты можно через некоторое количество публичных прокси. Наиболее известный и стабильно работающий из них — awxcnx.de

(tinyurl.com/8x9okb2).



Локальный прокси-сервер анонимизации I2P можно установить на домашнем компьютере. Сервер управляется через веб-интерфейс

Что можно найти в 2P?

В I2P-сети размещаются преимущественно торрент-трекеры, а также сайты с базами персональных данных. К последним относится, например, сервис Rusleaks, публикующий информацию о различных интернет-скандалах. Конечно же, в данной сети присутствуют и ресурсы с «серым» и нелегальным контентом, среди которых всевозможные электронные библиотеки, контент-порталы и т. п. Узнать список сайтов I2P можно по адресам ugha.i2p/EepsiteIndex и perv.i2p.