Вестник I2P

Привет, анонимус. Газета, которую ты сейчас читаешь, посвящена анонимной, распределённой сети I2P (**Invisible Internet Project**), а также средствам противодействия интернет-цензуре. Если ты уже давно знаком со скрытосетями, активно пользуешься TrueCrypt, знаешь чем TOR отличается от I2P, можешь легко и непринуждённо объяснить преимущества и недостатки RSA, то эта газета — не для тебя. Наша цель — рассказать тем, кто не знает. Мы хотим помочь обычному юзеру преодолеть барьеры, созданные людьми, одержимыми жаждой наживы и моралистами. Открыть для тебя Интернет, в котором не действуют правила, навязанные транснациональными корпорациями, медиамагнатами и правительствами.

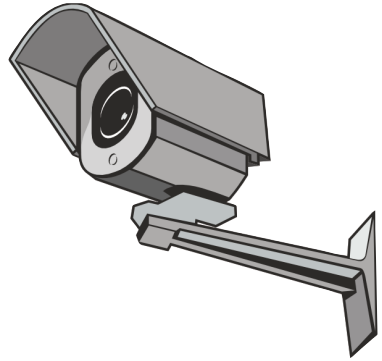
Сегодня в выпуске

Вместо предисловия

Раз уж ты нашёл эту газету, то, видимо, уже неоднократно задумывался о том, как скрыть или зашифровать передаваемую тобой информацию, о том как защитить свою персональную информацию. Использование I2P позволяет отчасти решить эти проблемы с помощью способов, доступных даже обывателю. Конечно, некоторые вещи нужно знать и понимать. Определённый порог вхождения есть. Но этот порог помимо нас уже сумело преодолеть множество людей, далёких от компьютерной тематики. **Это не сложно.** Когда разберёшься что к чему, это станет настолько же привычной вещью, как использование социальных сетей или поисковых систем.

Что же нужно будет сделать? Скачать и установить сам маршрутизатор I2P и программы, с которыми придётся работать (к примеру браузер, который не будет за тобой следить), затем всё настроить. Но это — только первый шаг. Потом придётся скорректировать своё поведение, чтобы не делать глупостей и не выдавать себя на блюдечке. Нужно привыкнуть не подписываться реальным именем и теми никнеймами, которые ты использовал до этого, научиться использовать действительно

сложные пароли и хранить их в тайне, научиться отличать псевдоанонимность от анонимности и действовать соответственно, понимать что безопасно, а что — нет. На первый взгляд это кажется нелёгкой задачей, но ты ведь понимаешь как надо вести себя в Интернете, чтобы не нацеплять вирусов и не вестись на разных мошенников? Здесь всё примерно так же.



Ну а теперь твой главный вопрос: **зачем?** Ты не нарушаешь законов, не хочешь революции, тебе нечего скрывать. А так ли всё радужно, как ты сейчас думаешь? Совсем недавно торренты были привычной вещью. Качали все. Теперь торренты закрывают. Качать фильмы незаконно. Качать бесплатно книги и читать их on-line тоже незаконно — ты нарушаешь авторские и смежные права. Скоро тебя заставят платить за всё подряд, подсовывая при этом второсортный товар, набитый под завязку рекламой. Наверняка ты и сам уже это видел. Когда удастся протолкнуть в странах первого мира законы, работающие на правообладателей и медиамагнатов, будет поздно задумываться об анонимности, бесплатном доступе и свободной информации. Это касается не только России и стран СНГ. Это общемировая практика, так происходит повсюду. Конечно, в «просвещённых странах» не принимают законы о чёрных списках. Там неугодные сайты быстро закрывают суды. Наши законы об авторском праве — это адаптация их законов.

И разве тебя не беспокоит, что кто-то там, наверху, хочет знать о каждом твоём слове и каждом клике? В большинстве случаев, он уже знает. Поисковые системы собирают историю запросов и анализируют твои интересы (за исключением, пожалуй, **DuckDuckGo.com**), браузер сохраняет и передаёт историю поиска, лицензионные соглашения отнимают у тебя права на твою информацию, всё что ты делаешь записывается и может быть использовано против тебя.

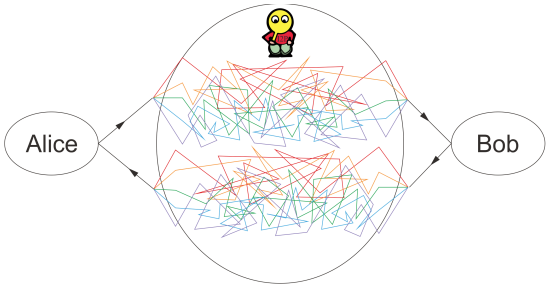
В общем-то, решать тебе. Наше дело — предложить. Ситуации, когда данные «случайно» утекли с компьютера или из социальной сети отнюдь не редки. Ситуации, когда нам приходится получать нежелательную информацию (спам, письма счастья, непристойные предложения), стали настолько часты, что с ними не сталкивался наверное только человек, который не пользуется Интернетом. Да, наша информационная безопасность это труд, но этот труд не напрасен. Всё в наших собственных руках.

Что такое I2P?

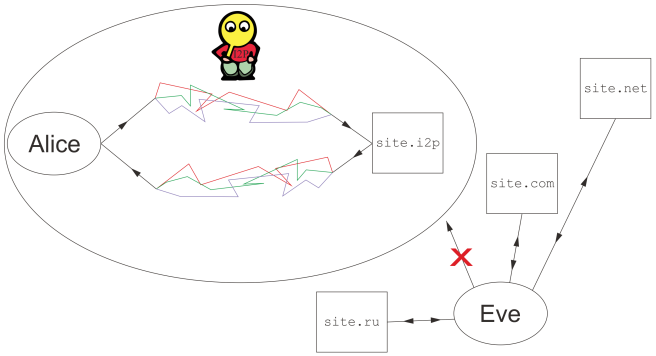
Если говорить предельно коротко и по существу, то Invisible Internet Project — это другой Интернет внутри уже известного тебе. Но технически правильно будет сказать, что это распределённая пиринговая сеть, построенная таким образом, что

при работе в ней персональные данные не раскрываются, а вся передаваемая информация зашифрована.

Ну и как это выглядит? Ты посылаешь запрос, и он идёт от тебя не прямо к цели, а шифруется, делится на части, и эти части идут сложными меняющимися путями внутри I2P.



И куда идёт этот запрос? К чему-то ещё в сети I2P. Это может быть другой пользователь (например, при переписке), а может быть сервер, на котором расположен **eep-site** — ресурс, доступный только внутри сети. Иными словами, эта сеть — целый Интернет, к которому нельзя получить доступ извне. Со своими сайтами, поисковиками, почтой, мессенджерами, торрентами и даже соцсетями.



Но, в отличие от всем известного Интернета, сеть I2P:

- Распределена — в ней нет критических узлов, поэтому её нельзя «выключить», пока к ней подключен хотя бы один компьютер
- Автономна — её работа не зависит от каких-либо «внешних» факторов вроде серверов, дата-центров, финансирования или работы команды специалистов
- Анонимна — в отправляемую тобой информацию по умолчанию не включается ничего, что как-то идентифицировало бы тебя и позволяло отличить от всех остальных
- Использует обычное интернет-соединение, поэтому доступ к I2P есть везде, где есть Интернет
- Масштабируема — не испытывает трудностей при росте числа пользователей, даже наоборот — сеть работает быстрее и эффективнее, когда в ней больше узлов
- Нецензурируема — поскольку участники анонимны, сервисы и сайты свободны, а все узлы — равноправны, искусственное ограничение доступа (вроде блокировок сайтов) в принципе невозможно

Мы предлагаем тебе использовать I2P в повседневной жизни так же, как ты используешь Интернет. Общайся, не беспокоясь о прослушке, ищи информацию, не давая составлять на себя досье, качай и раздавай всё что пожелаешь, не боясь что контент заблокируют, говори что думаешь, не боясь цензуры.

Право на свободный обмен информацией

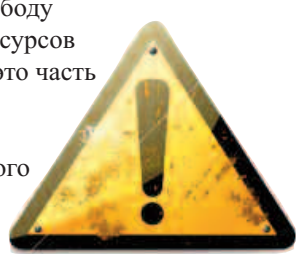
Право на свободный обмен информацией и отсутствие цензуры прописаны в Конституции нашей страны. Эту Конституцию принимали мы сами в ходе референдума. Всё, что записано в ней, является в Российской Федерации основополагающим законом. Все остальные законы, в том числе ограничивающие это право, являются второстепенными и должны быть отредактированы в соответствии с конституцией. Мы не станем разводить политический диспут, агитировать «за» или «против», бороться с политиками или законами. В России это совершенно бесполезно. Проект I2P предлагает взять назад отобранное право, право конституционное.

Использование средств криптографии пока законно, и в России не существует ответственности за попытку скрыть от третьих лиц сам факт передачи информации или её содержание. У нас защищены законом персональные данные, право на тайну переписки, свобода слова. Если в открытом интернет-пространстве на наши свободы может покуситься любой, обладающий для этого достаточными знаниями и средствами, то в I2P этой проблемы нет. Не существует метода однозначно установить личность, скрывающуюся за тем или иным псевдонимом. Веб-сервер, обрабатывающий твою информацию, получает её от точно такого же маршрутизатора, как и у тебя. Он не может увидеть IP-адрес твоего компьютера. Именно из-за этого сеть стала прибежищем тех, кому есть что скрывать. Конечно, сетью пользуются и люди, нарушающие закон: наркоманы и наркоторговцы, педофилы, революционеры и сепаратисты. Но они точно так же пользуются Интернетом, и там их гораздо больше.

Многие из тех, кто слышал об I2P, знают о ней как о сети с незаконным содержимым. Спешим опровергнуть. Сеть — всего лишь инструмент, как топор, например. Топором можно рубить дрова, изготовить сруб для бани, а можно отрубать головы. Независимо от того как используется топор, он не становится хорошим или плохим, легальным или нелегальным. Также и сеть не становится лучше или хуже из-за людей, которые её используют. Никто и никогда не снимает ответственность за сказанное и сделанное с самих пользователей. Наша свобода заканчивается там, где начинается свобода других людей. Прежде чем открыть

первый eep-сайт в своём браузере, повтори эту фразу. Подумай об этом и тогда, когда захочешь что-то написать или опубликовать. Да, по ту сторону Интернета нет цензуры, нет собаки с полицией, никто не сможет тебя вычислить и сдать властям. Но, нарушая свободы других людей, ты помогаешь тем, кто хочет свободу отнять.

Мы ни в коей мере не являемся сторонниками педофилии, порнографии, незаконного оборота оружия и наркотиков. Мы выступаем за свободу распространения информации. Часть содержимого некоторых ресурсов может вызвать шок или протест у некоторых пользователей. Но это часть свободы, неизбежное её последствие. Не бросайся осуждать и угрожать, требовать чего-либо. Просто закрой этот сайт. На страницах нашей газеты нет и никогда не будет рекламы подобного рода проектов. Все ссылки на момент публикации тщательно проверяются.



Как туда попасть?

Теперь о главном: как подключиться. Для работы маршрутизатора должна быть установлена java (**http://www.java.com/ru/download/**). Далее нужно скачать саму программу-маршрутизатор. Сделать это можно с официального сайта проекта: **http://i2p2.de/** или с **http://geti2p.net/**

Установка маршрутизатора под Windows очень проста: запусти инсталлятор и следуй инструкциям, на соответствующем этапе обязательно поставь галочку «установить как сервис». Инструкции по установке в других системах есть на сайте. В результате установки, кроме всего прочего, у тебя появится ярлык, с помощью которого можно запустить маршрутизатор. Сразу ты ничего не увидишь, у него нет окон. Пока твой браузер не настроен как надо, попасть внутрь сети не удастся. Но, прежде чем настраивать, надо подумать об анонимности и безопасности. Использовать один браузер для просмотра веб-страниц в Интернете и в I2P — не самая лучшая идея. Для работы в скрытосети лучше завести отдельный браузер. Многие опытные пользователи рекомендуют установить Firefox Portable (**http://portableapps.com/apps/internet/firefox_portable**) и в нём производить необходимые настройки. Надеюсь, ты прислушаешься к этой рекомендации. Настраиваем Firefox на работу через прокси вот так:

> FIREFOX → Настройки → Дополнительно → Сеть. Нажимаем на кнопку «Настроить». Отмечаем пункт «ручная настройка прокси», в поле адреса вводим 127.0.0.1, порт 4444. Подтверждаем кнопкой “OK”. Готово. Теперь твой браузер будет принимать и получать информацию через встроенный в маршрутизатор прокси-сервер.

Теперь браузер будет обращаться ко всем сайтам не напрямую, а через I2P. Но мы рекомендуем не останавливаться на этом, а озаботиться настройками содержимого. Известны случаи использования java-скриптов и flash-приложений для сбора информации и нанесения вреда анонимности пользователя. Поэтому на всякий случай лучше отключить скрипты и установить блокирующий плагин вроде flashblock.

Как настроишь браузер, набери в адресной строке **http://127.0.0.1:7657/**, откроется консоль маршрутизатора. Основное меню выглядит как на картинке справа. Если оно не такое, а совсем короткое — щёлкни на самом верхнем заголовке, и оно развернётся. Здесь самое главное — статус сети. Если написано «Сеть: OK» или «Сеть: Заблокирован извне», то всё работает. «Заблокирован извне» означает, что твой провайдер пытается блокировать использование I2P, но маршрутизатор знает как с этим бороться и особой разницы ты не заметишь. Это также может быть вызвано блокировкой твоим собственным брандмауэром, тогда ты можешь это исправить, покопавшись в его настройках. Если статус иной, нажми на него и увидишь что это значит и как это поправить.

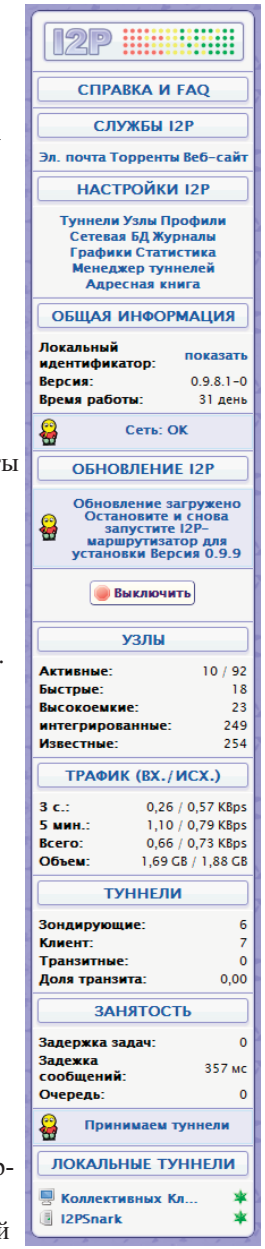
Если всё в порядке, можно посетить любой ресурс, который имеется в твоей адресной книге. Но пока в ней не так много адресов. Самый удобный способ их добавить — через подписки: Консоль маршрутизатора → Адресная книга → Подписки. Там находится список адресов, приведи его к следующему виду:

```
http://bl.i2p/hosts2.txt
http://cipherspace.i2p/addressbook.txt
http://dream.i2p/hosts.txt
http://hosts.i2p/
http://i2host.i2p/cgi-bin/i2hostetag
http://inr.i2p/export/alive-hosts.txt
http://stats.i2p/cgi-bin/newhosts.txt
http://tino.i2p/hosts.txt
http://trevorreznik.i2p/hosts.txt
http://www.i2p2.i2p/hosts.txt
```

Не забудь нажать «Сохранить» под списком.

Даже если сайта, на который ты хочешь попасть, нет в адресной книге, ты без труда сможешь туда добраться через специальные jump-сервисы. Это такие большие адресные книги, которые по запросу с именем сайта, отсутствующего в адресной книге, выдают его полный адрес и опционально пополняют им твою книгу. Ссылки на jump-сервисы отображаются при неудачной попытке перехода на eep-site.

Вот и всё. Возможно, понадобится подождать 10-15 минут, чтобы маршрутизатор успел интегрироваться в сеть и настроить туннели. Больше время



работы и число компьютеров в сети — выше скорость.

Помимо широкого разнообразия сайтов, имеются в наличии торрент-трекеры, блогосоциальные сети, имиджборды и форумы. Полный простор для обмена информацией любого рода. И при этом **отсутствует цензура**. Конечно, I2P — не самый лучший помощник для доступа к запрещённым сайтам, закрытым Роскомнадзором. Эти сайты располагаются в привычном для нас Интернете. I2P — это отдельная сеть со своими ресурсами, она не создавалась как анонимайзер и не предназначена для обхода блокировок. Хотя прокси-сервера во внешнюю сеть имеются в наличии, и ими можно воспользоваться в случае крайней нужды. Но для этой цели гораздо удобнее использовать TOR. В I2P нет традиции защиты авторского права, содержимое большинства ресурсов можно использовать свободно, не ссылаясь и не выплачивая вознаграждений, а также изменять и приспосабливать под собственные нужды.

На работу через I2P можно настроить любую программу, поддерживающую прокси, можно использовать любой браузер, почтовый клиент, xmpp-клиент и т.д. Конечно, в I2P не будет некоторых удобных фишек типа поиска из адресной строки и кнопок социальных сетей, но зато не будет и многих проблем. Например, на момент выхода этого номера в сети почти нет спама и рекламы. Не только навязчивой рекламы в виде всплывающих окон или пищащих и визжащих java-скриптов, но и даже статических баннеров (рекламных полей на сайтах), за очень редким исключением. Почтовый ящик не атакуют тысячи предложений получить сегодня, недорого и без предоплаты новый холодильник и гороскоп в подарок. Вспомни каким был Интернет в начале 2000-х. Тут всё примерно так же.

Я в сети, куда идти?

В I2P мы подготовили для тебя стартовую площадку: **hiddengate.i2p**. Там ты найдёшь более подробные инструкции по настройке, описание решений распространённых проблем, рекомендации по поддержанию анонимности, обзоры ресурсов сети и всевозможные обсуждения. Кроме того, мы подготовили для тебя небольшой список полезных ресурсов, с которых можно начать обзор содержимого сети:

- lenta.i2p — агрегатор новостей, публикуемых самими пользователями
- zerofiles.i2p; flz.i2p — файловые хостинги
- tracker2.postman.i2p; runode.i2p — торрент-трекеры
- rus.i2p — официальная русскоязычная энциклопедия
- progromore.i2p — проект о программировании
- e-reading.i2p — библиотека. С книгами.
- forum.i2p; forum.rus.i2p — форумы про I2P
- hiddengate.i2p — наш проект по внедрению **тебя** в I2P. Читай там всё.
- epsilon.i2p, aperi.i2p, direct.i2p — поисковики
- cat.i2ch.i2p — тематический каталог сайтов I2P

Да, имеются даже поисковики. Они не так хороши как те, к которым ты привык, но всё же работают. Мы не приводим ссылки на социальные сети, потому что считаем, что их использование вредит анонимности, однако они существуют, и желающие без особого труда смогут их найти.

Если вдруг тебе уже хочется разместить внутри I2P собственный сайт, в этом нет большой проблемы, правда, с бесплатным хостингом дела обстоят не очень хорошо, поэтому почти наверняка придётся заплатить. Однако, ты можешь совершенно бесплатно хостить что угодно на своём собственном железе с помощью встроенных в маршрутизатор средств, и даже за доменное имя платить не придётся.

Часто задаваемые вопросы

Кто автор этой программы и кто придумал эту сеть? Можно ли им доверять?

Авторы самого маршрутизатора анонимны, их реальных имён никто не знает. Проект разрабатывается коллективно, принять участие может каждый по мере возможностей. Программа распространяется под свободной лицензией. Её можно абсолютно легально установить и использовать в большинстве стран, где не запрещена криптография. При этом ты не нарушишь ничьих авторских прав. Исходный код программы открыт, так что если ты сомневаешься в безопасности, скачай исходники и проверь самостоятельно. Используемые в настоящий момент алгоритмы шифрования являются одними из самых надёжных. Тем более, сеть конструировалась с расчётом на то, что любой узел или вся цепочка могут оказаться скомпрометированы. Даже если вся цепочка маршрутизаторов принадлежит тем, кто следит за тобой, они не смогу расшифровать информацию, которую ты передаёшь, если у них нет секретного ключа или миллиона лет на его подбор.

Ололо, я нашёл список всех IP-адресов, вы не анонимны!

Отлично, а теперь попробуй связать хоть один адрес с той информацией, которую он передаёт. Если у тебя получится, то ты — гений.

Мой маршрутизатор не знает сайт, на который я хочу попасть!

Да, так часто бывает. Так как службы DNS нет, маршрутизатор обращается к адресной книге, спрашивая адрес ресурса. Если сайта нет в книге, то он не откроется. На странице будет предложено несколько jump-сервисов, которые могут подсказать тебе адрес. Нажми на любую из предложенных ссылок, после чего тебя перенаправят на страницу с адресом и предложат его сохранить. Сохрани адрес, после чего тебя перенаправят на сайт, который ты хотел открыть.

Надо ли мне как-то скрывать факт использования I2P?

Сеть I2P проектировалась не с расчётом на то, что сам факт пользования ею пользователем не будет известен, а на то, что связать передаваему информацию с конкретным человеком вообще невозможно. Само использование I2P не предполагает предосудительных действий, а что именно ты в ней делаешь выяснить нельзя.

Почему такая низкая скорость?

Скорость зависит от того, насколько твой маршрутизатор интегрирован в сеть, сколько знает других маршрутизаторов и со сколькими обменивается данными. Чем больше клиентских туннелей открыто, тем выше скорость обмена данными. Для того, чтобы скорость стала выше, нужно просто подождать. Открыть первые сайты ты сможешь уже через 15 минут, а через сутки скорость скорее всего тебя приятно удивит. Не останавливай маршрутизатор без особой необходимости. Если у тебя безлимитный Интернет и нет проблем с электричеством, просто не выключай компьютер. Этим ты поможешь не только себе, но и другим участникам сети. Когда хорошенько освоишься, стоит почитать документацию и покопаться в настройках, оптимизировав всё под своё соединение.

Не открывается тот или иной ресурс

Да, так бывает. Возможно, сеть перегружена, или твой маршрутизатор плохо интегрирован в сети. Возможно, ресурс умер. Некоторые сайты работают не круглые сутки, особенно если они расположены на домашних компьютерах. У владельца могут быть проблемы с интернет-соединением. Отнесись к этому философски. Сеть развивается. В том числе благодаря тебе.

Сайт %имя.i2p% в открытую публикует запрещённые материалы, сколько можно терпеть?!

Что ты, что ты! Не нужно терпеть. Закрой вкладку браузера, удали его из адресной книги, никогда туда больше не заходи. Свобода — это право выбора, просто не выбирай такое.

Накидайте мне контента, запилите биржу, социалочку, контактик

Анонимус — не твоя личная армия. Ты никому ничего не должен, и тебе никто ничего не должен. Если чего-то не хватает, то запили сам. Можешь предложить идею, вдруг её кто-нибудь реализует.

Как платить анонимно?

Существует множество криптовалют типа Bitcoin, Litecoin и их форков, которые принимаются большинством торговых площадок. Если ты хочешь пожертвовать или продать, установи необходимый софт, почитай на ресурсах I2P про то, как использовать их действительно анонимно, и пользуйся.

Ты тоже можешь помочь проекту

Мы не всесильны и не всемогущи, нам требуется твоя помощь. В финансах никто из редакторов не нуждается, поэтому материальные пожертвования пока не принимаются. Но ты можешь написать статью или прислать чужую статью, которая могла бы оказаться полезной. Мы рассмотрим её и, вероятно, разместим в одном из выпусков или отредактируем. Информация и работа по её обработке — самое ценное, что нужно на сегодняшний день. Если умеешь хорошо писать, смыслишь в веб-дизайне или умеешь ещё что-то полезное, мы будем тебе рады. Также можно распространить эту газету на форумах или в социальных сетях. Её даже можно напечатать и раздать знакомым. Можно разместить ссылку или сам файл в своём блоге. Можно скопировать тексты, переписать их или раскритиковать в пух и прах. Но мы против продажи. Ты получил эту информацию бесплатно, поэтому не стоит пытаться заработать на ней. Все имеют право знать. По всем вопросам ты можешь написать на **vestnikglavred@mail.i2p** (работает только внутри I2P, туда нельзя послать письмо с @mail.ru, @ya.ru или @gmail.com) и **vestnikglavred@i2pmail.org** (работает для внешних адресов).

В следующем выпуске

- Как правильно себя вести для сохранения анонимности
- Электронная почта. Регистрация, использование, шифрование.
- i2p-bote — почта без сервера. Что и как?
- Техническая сторона: сравнение I2P и TOR
- PGP - ассиметричное шифрование. Работаем с почтой и файлами.

И многое другое.

Заинтересовался?
Торопишься?
Отсканируй код
и прочитай потом!