

Выпуск №2



Привет, анонимус. Перед твоими глазами уже второй выпуск «Вестника I2P», а значит, мы ещё живы и трудимся на благо тебя.

Сегодня все, кому не лень, пытаются поднять под себя инфосферу, запретить всё, что невыгодно или неудобно и установить жёсткий контроль над всем остальным. Правительства принимают один за другим выгодные для них законы: нельзя раздавать Wi-Fi, нельзя запускать гражданские дроны, нельзя открыто писать без лицензии, закроем любой сайт без суда, данные храни только в России, под каждым своим движением ставь подпись и вноси его в реестр. Коммерческие организации собирают данные о тебе, торгуют ими и раскрывают их властям, а тебе не оставляют выбора. В надёжных криптографических стандартах постоянно находят уязвимости.

Но даже в таких тяжёлых условиях твоя свобода в твоих руках. В этом номере мы расскажем о злободневных проблемах анонимности и информационной безопасности и поделимся с тобой способами их решения.

Мы представляем твоему вниманию сразу несколько новых рубрик, которые, вероятно, станут если не постоянными, то по крайней мере регулярными. Спасибо, что остаёшься с нами.

Сегодня в выпуске

- Новости мира I2P
- Анонимное поведение — как не выдать себя с головой
- Обзор способов общения внутри I2P — чем плохи традиционные методы, и какие подойдут на замену
- Шифрование при помощи PGP/GPG
- Невидимые миры: какие ещё есть сети кроме Интернета
- Юротдел — последние нововведения в законодательстве РФ, касающиеся информационной безопасности граждан

Новости невидимого мира^{NEWS}

Пока ты изучаешь содержимое «Вестника», а мы готовим следующий выпуск, Invisible Internet Project живёт своей жизнью, статус-кво постоянно меняется, многочисленные проекты развиваются, появляются новые, некоторые погибают. Здесь ты узнаешь о последних событиях и назревающих тенденциях, разберёшься где жизнь кипит, а где увядает. И в этот раз сводки о событиях в I2P откроет критически важная новость.

Abscond Bundle

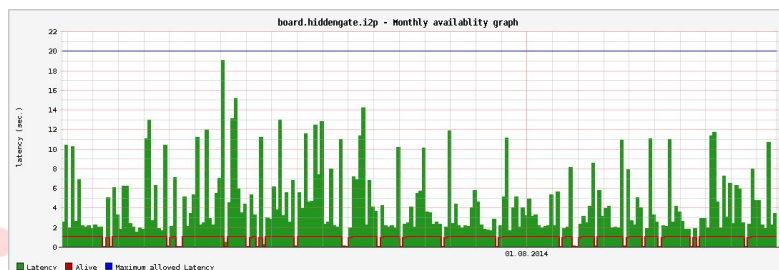
От создателя Anopcoin вышел [Abscond Bundle](#), настоящий портативный I2P-браузер. Он включает в себя собственно браузер на базе Firefox, маршрутизатор I2P, OpenJRE, плагины Orchid и I2P-Bote. Пока готова сборка только для Windows, а разработчик готовит buildscript'ы для Linux. При наличии уже установленного маршрутизатора I2P, он подключится к нему, однако лишнюю JRE всё равно запустит.

Отдельно стоит похвалить сам преднастроенный браузер, который по умолчанию скрывает даже больше данных о пользователе, чем TorBrowser (например, Unique ID браузера), а также общее высокое качество настройки и удобства. Тем не менее, его создатель предостерегает: сборка в процессе разработки, поэтому присутствуют баги и возможно наличие уязвимостей.

Reg.Rus.I2P

Совсем недавно появился весьма полезный сервис [reg.rus.i2p](#). Помимо регистрации доменных имён и подписки для адресной книги он предоставляет очень важную функцию: отслеживает доступность сайтов и качество их работы.

Со стороны пользователя не всегда можно проверить наверняка, лежит ли сайт или нет, ведь проблемы с соединением могут быть не только на стороне сервера. Данные собираются в наглядные графики за сутки, неделю, месяц и полгода. Высота столбцов показывает задержку отклика сайта в секундах от 1 до 20. При задержке больше 20 соединение сбрасывается и сайт отмечается как недоступный на данный момент.



По словам Alex'a, создателя ресурса, а также владельца Wiki [Rus.i2p](#), движок был написан всего за выходные и ориентирован на голый функционал. Остальные функции будут наращиваться позже, по мере сил, возможности, и при наличии свободного времени.

В сети I2P есть и были подобные сайты: это [identiguy.i2p](#) и ныне мертвый [who.i2p](#). Оба из них имели большой недостаток — малую выборку проверяемых сайтов и очень короткий период журналирования.

Bote

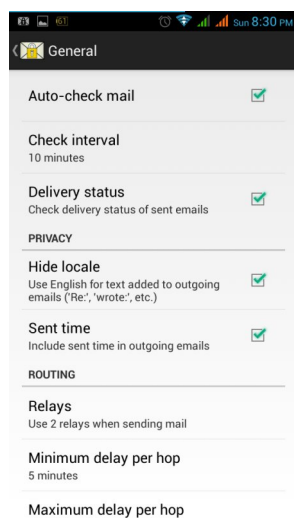
Плагин бессерверной шифрованной почты I2P-Bote был портирован на Android. Работа по его переделке велась целый год. Он рассчитан на максимальное удобство и простоту использования. Добавлена возможность импортировать свои личные ключи (то есть публичные адреса) с компьютера на портативное устройство, что позволяет проверять свою почту I2P-Bote где угодно.

Как и все портативные решения, связанные с I2P, работает либо на встроенном в «Bote» маршрутизаторе, либо на уже установленном. Отдельно работающий маршрутизатор I2P на Android работает вполне сносно, и для короткой проверки почты его хватает.

Подобные приложения на портативных устройствах — одно из самых перспективных направлений развития I2P, когда множество слоёв шифрования и peer-to-peer архитектура предоставляют надёжный транспортный слой для коммуникации пользователей.

Скачать можно здесь: <http://str4d.i2p/builds/Bote.apk>

Обсуждают тут: <http://zzz.i2p/topics/1638>



Плагин I2P для Vuze

Популярный бит-торрент клиент Vuze получил новый плагин под названием [azi2phelper](#). Этот плагин позволяет клиенту сидировать свои торренты в «обе стороны»: как во внешний Интернет, так и в I2P. Доступ осуществляется через встроенный в плагин «бортовой» маршрутизатор или через уже установленный. Сама сеть I2P также извлекает от плагина пользу в виде увеличения количества пиров на популярных торрентах (ТВ-сериалы, новые фильмы, музыка). Несмотря на малые скорости и большой объём, на зарубежных I2P-трекерах подобный контент популярен. Скорее всего, из соображений безопасности, анонимности или просто ради поддержки сети.

Azi2phelper также способствует улучшению кода DHT Снарка, так как разработчики поддерживают связь, а также помогает популяризации и росту сети в целом, что несомненно важно.

Формально плагин существует давно, но раньше он был на ранней стадии и разработка почти не велась. Теперь же работа возобновилась и создатель плагина просит пользователей Vuze тестировать его и искать баги.

Обсуждают тут: <http://zzz.i2p/topics/1613>

Капитан покинул корабль

Администратор сайта salt.i2p под псевдонимом efkt внезапно исчез. Произошло это примерно в середине мая, когда упал его сайт, и он внезапно перестал появляться на своём Irc2P-канале #salt. Сообщество и его приближённые выдвигали немало версий, от банальных (например, женитьбы) до конспирологических (пойман АНБ). Некоторые связывали исчезновение товарища со странными событиями около программы TrueCrypt, которые также пришлось на этот период.

Напомним, что salt.i2p являлся основным центром общения англоязычной крипто-тусовки, а канал #salt до сих пор является одним из трёх самых активных каналов в Irc2P, поэтому исчезновение его основателя и активнейшего участника вызвало сильное смятение у многих в анонимном сообществе в I2P.

Помимо самого ресурса были потеряны ценные технические материалы и мануалы об анонимности и I2P. Резервных копий, к сожалению, не осталось.

Мемпо

Недавно несколько пользователей I2P начали разработку desktop-дистрибутива Linux, ориентированного на повышение безопасности. Основные особенности: в основе Debian Wheezy, закалённое ядро и RBAC от grsecurity. Планируется встроенная поддержка различных инструментов шифрования. Для сети были выбраны Tor, OpenVPN, I2P и Freenet, для дискового шифрования LUKS, для шифрования корреспонденции GPG и OTR. Также планируется ввести собственный менеджер для облегчения создания виртуальных машин и изоляции.

На данный момент разработка находится на ранней стадии. Любой желающий может помочь проекту, направив критику и пожелания разработчикам. Они довольно открыты и рады помощи. Официальный сайт:

<https://wiki.debian.org/Mempo>



+



+





Анонимное поведение

Несмотря на то, что Интернет объединяет огромное пространство, личного пространства у человека становится всё меньше. Технология, которая призвана давать людям свободу слова и возможность открыто выражать свои мысли, с годами стала инструментом контроля и подавления. Из-за технологических особенностей Сети, за каждым пользователем тянется цифровой след из всей его активности. Тот, кто имеет возможности собирать эти данные, получает возможность использовать её против пользователей. Свобода слова не может существовать в условиях, когда за слова можно наказать любого. Даже сама по себе возможность быть наказанным воздвигает стену из цензуры и самоцензуры, делая невозможным публичное открытое обсуждение. Без этой открытости начинается стагнация, что начинают эксплуатировать обладающие ресурсами силы. Таким образом, к функции подавления и контроля добавляется функция пропаганды. Из-за своей открытой природы, цифровой след доступен третьим лицам, которые могут использовать её для вмешательства в личную жизнь. То, что должно оставаться секретом, может стать публичным достоянием. В такой ситуации единственный эффективный способ сохранить свою свободу слова и приватность — через анонимное поведение, то есть не давать никому и никогда возможности соединить след от деятельности в Сети со своей реальной личностью. Всегда будут некие силы, которые будут пытаться отнять свободу выражения различными способами. Для противостояния этим силам есть множество средств. Ниже мы приводим наиболее общие методы обеспечения анонимности и повышения информационной безопасности, разделённые на категории по степени важности. Методы каждой категории дополняют предыдущие.

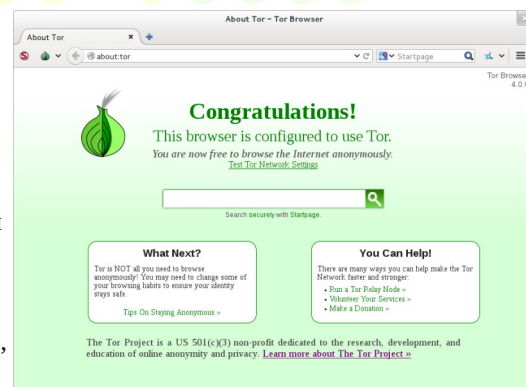
Critical

- **Не сообщать о себе лишней информации.** Есть набор атрибутов, зная которые, можно выделить конкретного пользователя из множества других. Это возраст, пол, образование, место проживания или часовой пояс, профессия, увлечения, данные о внешности и вообще любые индивидуальные характеристики человека. Подобные атрибуты позволяют стороннему наблюдателю эффективно отсеивать лишних пользователей по профилю, что постепенно ведёт к деанонимизации. Избежать этого можно, выработав у себя привычку быть осторожным при общении. Помимо этого, нужно научиться контролировать свои эмоции. В 2010 году Б. Мэннинг, в поиске моральной поддержки, сознался незнакомцу в приватном чате в том, что это он передал 250 тысяч военных документов в WikiLeaks. Незнакомец сдал его агентам ФБР, и теперь Мэннинг отбывает срок в 35 лет. Этого не произошло бы, держи он себя в руках.

- При использовании ресурсов, на которых нужно сохранить анонимность, обязательно **менять свой IP-адрес**. Он напрямую связан с именем в физическом мире (через контракт с провайдером, а при динамическом IP — через логи подключения). Запись о подключении какого-либо клиента к серверу может храниться на этом сервере практически вечно. Для смены IP удобно использовать Тор. Это анонимизирующая сеть, которая, грубо говоря, является цепочкой прокси и помогает легко сменить IP. Пользователи Windows могут установить портативный Tor Browser Bundle. Пользователи Linux могут установить его из большинства пакетных менеджеров. Смена IP касается не только сёрфинга сайтов, но и любых других Интернет-подключений к серверам — Jabber, мессенджеры и всё остальное. Тот же Тор может проксировать почти любой вид подключения, достаточно указать в настройках прокси хост 127.0.0.1 и порт 9050 или 9150. Некоторые сайты могут блокировать Тор из-за вредоносной активности. Через него также невозможно скачивать торренты, так как реальный IP будет «протекать». В таких случаях можно использовать VPN. Они бывают платные или бесплатные. Перечисленные средства смены IP-адреса следует применять для всего без исключений, или как минимум для работы, требующей анонимности.

- **Не использовать один ник дважды.** Если использовать тот же ник, что и на не анонимном ресурсе, сопоставить личности не составляет труда. Зная не анонимный ник, возможно достать реальный IP. Если не хватает фантазии каждый раз придумывать новые ники, можно использовать онлайн-генераторы, их много.

- **Не использовать при регистрации на различных ресурсах тот e-mail, который связан с реальным именем.** Даже если он нигде не отображается для других пользователей, он всё равно доступен для наблюдателя или как минимум администратору ресурса. Лучше всего использовать одноразовый e-mail



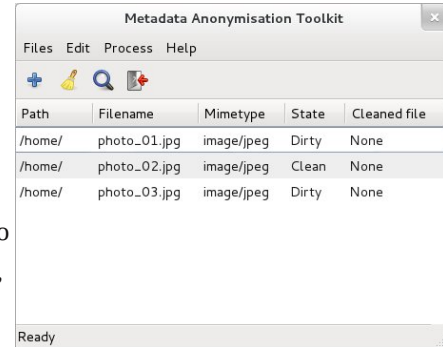


наподобие 10minutesmail. Он позволяет получить пароль или ссылку активации на одноразовый ящик и прямо через браузер. После регистрации всегда нужно менять пароль на более стойкий.

- Никогда **не использовать личный номер мобильного телефона** для подтверждения регистрации. Подобная двухфакторная аутентификация сводит на нет анонимность, так как номер часто связан с реальным именем и позволяет имеющим ресурсы ведомств узнать много всего, в том числе и местоположение. При желании для получения кодов регистрации можно использовать платные сервисы типа SMS REG или бесплатные браузерные. Но сначала лучше подумать, нужен ли подобный ресурс вообще.

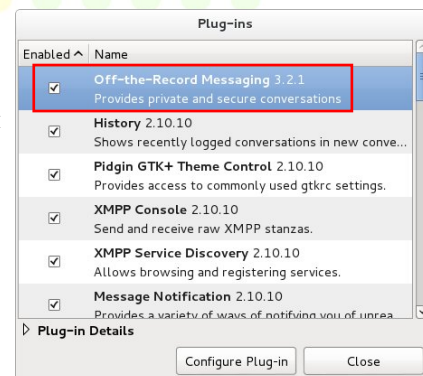
Advanced

- Обязательно **удалять метаданные при публикации любых файлов**. Метаданные могут содержать записи, на основе которых можно полностью деанонимизировать пользователя. Современные цифровые камеры могут вшивать в фотографию номер модели и производителя данной камеры. Некоторые смартфоны вшивают в фотографии GPS-координаты места съёмки. Чтобы избежать деанонимизации, нужно предварительно очищать любые публикуемые файлы. Для этого существуют специальные инструменты, например Metadata Anonymisation Tool для Linux и Exiftool для Windows, и множество похожих программ.



- Повысить безопасность веб-сёрфинга. Есть несколько расширений для популярных браузеров, позволяющих устранить некоторые уязвимости. Расширение **NoScript** блокирует различные скрипты сайтов, которые могут быть использованы для запуска вредоносного кода или вызова каких-нибудь программ, которые могут привести к деанонимизации. Некоторые сайты будут работать некорректно после установки NoScript, поэтому возможно придется вносить их в исключения. Второе расширение называется **HTTPS Everywhere**. Оно принуждает использовать защищённое соединение. Хотя в целом сертификаты TLS/SSL подвержены уязвимостям, это расширение позволяет повысить безопасность на тех сайтах, где соединение не имеет защиты вообще. Полезным может оказаться **RequestPolicy** — он защищает некоторые данные о пользователе, а также **AdBlock**, убирающий назойливую рекламу. В настройках самого браузера нужно **выключить геолокацию** (по понятным причинам), обязательно **отключить Flash**, который может деанонимизировать по той же схеме, что и скрипты.

- **Использовать OTR** для защиты приватности в личных чатах. Личные сообщения передаются в открытом виде, их может прочитать администратор сервера или вообще кто угодно, установив прослушку. Off-The-Record — это схема сквозного шифрования, которая автоматически создает одноразовые сессионные ключи и шифрует ими все сообщения (кроме самого первого). После завершения сессионные ключи уничтожаются и восстановить их, как и весь диалог в чате, злоумышленник не сможет. Ещё OTR имеет функции аутентификации — через обмен идентификаторами постоянных ключей через другое средство связи типа телефона, либо через общий секрет, о котором надо договориться заранее при личной встрече. Плагины OTR доступны для большинства мессенджеров, хорошо работают поверх XMPP, IRC и других протоколов. Для электронной почты **применять шифрование GPG**, которому посвящена отдельная статья в этом номере.

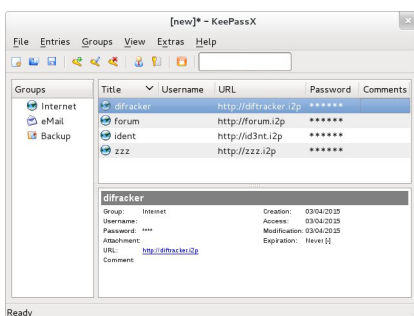


- **Использовать специальные средства для хранения паролей**. Хранить их в открытом виде в текстовом файле или на бумаге — плохая идея. Их могут украсть различными методами. Такие программы как KeePassX и Password Safe создают зашифрованную базу данных, запертую одним мастер-ключом, то есть достаточно придумать и запомнить один стойкий пароль. Хранилища паролей также имеют функцию генерации длинных паролей из случайных символов. Это удобно — они сразу записываются в базу данных, а из-за случайности и большой длины взломать их подбором сложно.



open source

- **Не использовать проприетарное программное обеспечение**. Из-за того, что невозможно просмотреть внутреннее содержимое программы, нельзя узнать все её функции и убедиться, что в ней нет встроенных чёрных ходов для спецслужб. Только закрытость системы позволяет встроить закладки, выполняющие любые функции по сбору данных о пользователе, который к тому же установил такую программу добровольно. Чтобы избежать утечек важной информации, нужно использовать только свободное ПО с открытым исходным кодом. Содержание открытых программ



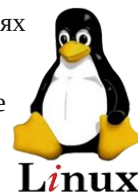


может просмотреть целиком любой желающий. Кроме проверки на закладки, свободное ПО имеет полностью открытый цикл разработки, который гораздо более эффективен за счёт цепи обратной связи — системы типа GitHub позволяют связаться с автором программы напрямую и оперативно решить любые обнаруженные уязвимости и баги. Прежде чем скачивать какую-либо программу, надо убедиться что она открытая и свободная. Это обычно указано на сайте программы. Если нет — надо найти открытый аналог. Использование открытых операционных систем (различные дистрибутивы Linux и системы BSD) также поможет повысить свою безопасность.

Paranoid



- Освоив **открытые ОС типа Linux**, продвинутые пользователи могут повысить безопасность своих систем ещё сильнее. Методы и инструменты повышения безопасности обычно зависят от конкретных задач. В некоторых случаях может пригодиться Whonix. Этот дистрибутив позволяет создавать изолированные виртуальные машины, трафик которых полностью проксирован через Tor. В самой виртуальной машине можно запустить любую другую ОС, даже Windows, и весь трафик виртуальной машины будет анонимизирован. Whonix идеально подходит для тех, кому нравится изолирование системы через виртуализацию, однако для него требуется достаточно мощное железо. Любители Gentoo могут повысить безопасность, используя ядро от GrSecurity, этот дистрибутив называется Hardened Gentoo. Такое ядро имеет большое количество патчей, которые устраняют низкоуровневые уязвимости, присущие обычному ядру Linux. Также существует SELinux, система контроля доступа на основе ролей. Изначально это средство было создано АНБ для защиты своих компьютеров. На сетевом уровне есть iptables, позволяющий создать эффективный firewall. Все упомянутые средства (и не упомянутые тоже) подходят только для действительно опытных пользователей, и их настройка требует внимания и осторожности.



- При установке различных программ, необходимо **сверять чек-суммы** скачанных файлов с теми, что размещены в источниках программы. Это поможет убедиться в их целостности. В случае, если файлы были испорчены при скачивании или преднамеренно изменены злоумышленником даже на один байт, чек-сумма будет полностью другая. Достигается это за счёт лавинообразного эффекта хэш-функций. Помимо чек-сумм, некоторые разработчики используют GPG-подписи файлов и сборок. Подписывает обычно релиз-менеджер своим ключом, выступая гарантом надёжности. Например, сборки Tor на протяжении многих лет подписывает Erinn Clarke. Проверка подписей скачиваемого ПО является хорошей практикой, так как помогает установить достоверность и целостность критически важных программ.



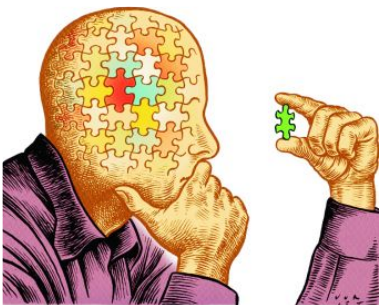
- Защитить компьютер от физического доступа помогут **инструменты для дискового шифрования**. Они расшифровывают раздел при запуске операционной системы и зашифровывают обратно при отключении. У пользователей Linux есть встроенный инструмент dm-crypt, имеющий все необходимые утилиты для дискового шифрования. Нужно только иметь в виду, что в Linux придётся шифровать не только root, но и swap, в противном случае некоторые данные будут не защищены. Также необходимо предварительно настроить DE на моментальное выключение машины, так как только выключение помогает надёжно запереть данные в экстренной ситуации. Полезной в некоторых случаях функцией может оказаться шифрование с убедительной отрицаемостью. Проще говоря, создание в зашифрованных разделах скрытого «двойного дна» с другими разделами без каких-либо меток, запертого другим паролем. Эффективно доказать существование такого «двойного дна» не сможет никакая экспертиза, возможно только предположить по размеру общего раздела. Для ретроградов и пользователей Windows есть TrueCrypt, прекративший своё существование в мае 2014 года при загадочных обстоятельствах. Единственный надёжный источник сборок и исходного кода — репозиторий с подписями: <http://cyberside.net/truecrypt/>. Последней надёжной версией является 7.1a. TrueCrypt также можно применять для дискового шифрования, создания скрытых разделов и зашифрованных томов. Использование этой программы достаточно простое и хорошо документированное. Для тех, кому нужно заменить устаревающий TrueCrypt, есть VeraCrypt: <https://veracrypt.codeplex.com/> Проект унаследовал части кода TrueCrypt, имеет режим совместимости с его томами и вообще активно развивается. Ещё один наследник TrueCrypt — это Ciphershed: <https://ciphershed.org/> Однако, он ещё в довольно ранней стадии разработки. Применяя дисковое шифрование, нужно знать, что существует несколько опасностей. Одна из них — это Cold boot attack, позволяющая запускать машину через короткий период после выключения. Вторая опасность — атаки типа Evil Maid, которые позволяют украсть пароль от зашифрованного раздела: <http://theinvisiblethings.blogspot.se/2009/10/evil-maid-goes-after-truecrypt.html>. Всё это нужно учитывать, оставляя компьютер без присмотра.



• По возможности, нужно **уменьшить площадь физической атаки**. При наличии встроенной карты WiFi, её следует удалить и использовать внешнюю, подключаемую через USB. Это позволит полностью и надёжно отключать компьютер от сети при необходимости, изолируя и уменьшая площадь атаки (физический способ изоляции компьютера от точек подключения Сети называется «Air gap»). Следует остерегаться встроенной Access Management System. Эта система предоставляет производителю удалённый полный доступ к машине. Изначально эта система используется для отслеживания при краже, однако её можно использовать для чего угодно. Не стоит покупать компьютеры с доставкой

по почте. У АНБ есть подразделение под названием Tailored Access Operations, работа которого заключается в перехвате почтовых посылок с компьютерами, установке аппаратных и программных закладок и дальнейшей отправке получателю. По мнению агентства, подобная схема считается одной из самых эффективных для внедрения в нужную систему.

• **Основа информационной безопасности — это знания.** Лучший способ повысить свою безопасность — изучать системы, криптографические алгоритмы и протоколы. Это долгий процесс, требующий терпения и времени. Наградой за труд станет возможность самому разбираться в уязвимостях и решать их.



У отдельно взятого пользователя не существует чётких границ между состоянием «аноним/не-аноним». Это состояние напрямую зависит от модели угроз, потому что разным злоумышленникам доступны разные ресурсы для атаки на этого пользователя. Для защиты от случайных факторов хватит и базовых средств, для сопротивления работе спецслужб потребуются лучшие техники. Не имея достаточно данных о своей модели угроз, выбор применяемых средств следует делать на основе компромисса. С одной стороны лежит привычное удобство, с другой стороны лежит огромный риск раскрытия чувствительных данных, генерируемых по умолчанию и независимо от пользователя. Также стоит иметь в виду, что 90% данных, добываемых разведкой, происходят из открытых источников, в основном из Сети. Другими словами, в цифровом веке пользователи по незнанию сами составляют на себя досье. Обладание личными данными даёт власть, поэтому владение ими всегда будет предоставлять интерес. Анонимность — это сложно, информационная безопасность — ещё сложнее. Каждый должен усвоить только одно: никто не защитит твои данные, никто не сохранит приватность, кроме тебя самого.

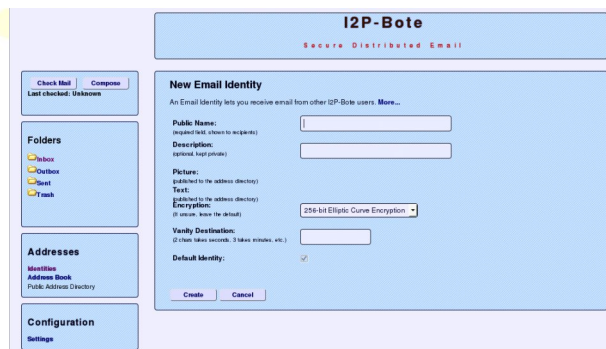
Способы общения внутри I2P



Многие пользователи привыкли для общения использовать большое количество популярных сервисов, которые все как один имеют ряд недостатков. Самые серьёзные — это слабая политика конфиденциальности, сотрудничество с органами и выдача любых пользовательских данных по первому запросу. Помимо этого, они подвержены перехвату данных, а некоторые специально встраивают ходы для спец. служб или закрывают глаза на существующие уязвимости. В такой ситуации целесообразно перенести хотя бы часть своих коммуникаций в I2P, используя одно из основных преимуществ этой сети — предоставление анонимного шифрованного транспортного слоя. Задавшись целью использовать это преимущество, мы рассмотрим популярные средства связи и их аналоги из I2P.

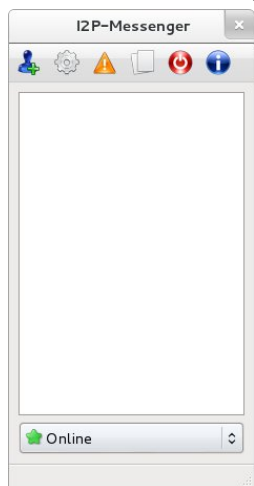
В качестве **ящика электронной почты** многие используют Gmail, Yahoo!, Hotmail или похожие сервисы. Преимущественно из-за их популярности и интеграции в другие службы и аккаунты. Есть несколько причин ограничить себя в их использовании. Например, упомянутые ранее программы сбора информации. С согласия Гугла то же Агентство Национальной Безопасности может собирать данные в широком диапазоне: содержание писем, время отправки, получатели, даже выборки с различным масштабом. Инструменты визуализации позволяют упорядочить этот большой объём данных в виде наглядных графов социальных связей и быстро найти искомые закономерности. Условия пользования фактически превращает любой сервис в доносчика, а требование указывать реальное имя и телефон при регистрации усложняет анонимизацию. В качестве замены можно использовать почту в I2P. Уже очень давно работает почтовый сервер, предлагающий почту с доменным именем **@mail.i2p**. Держит его некто postman. Как и с любой другой электронной почтой, нужно сначала зарегистрировать себе почтовый ящик. Сделать это можно по адресу: http://hq.postman.i2p/?page_id=16. Для работы с этим сервером в маршрутизаторе есть встроенный почтовый клиент, называется **Susimail**. Он имеет скромный веб-интерфейс с минимумом функций. Те, кого стандартный веб-интерфейс не прельщает, могут смело настроить любимый почтовый клиент для работы с этим сервером вручную. Настройка любого клиента тривиальна: указать в качестве почтового сервера 127.0.0.1 или localhost, указать порт POP3 7660 и порт SMTP 7659, а также имя ящика и пароль, аутентификация прямая. С регистрацией в I2P пользователь получает возможность принимать сообщения из внешнего интернета. Для этого надо заменить в своем адресе доменное имя @mail.i2p на @i2pmail.org. Однако оператор сервиса просит не использовать эту функцию слишком часто — это повышает нагрузки на сервер. Как и с любой почтой, можно дополнительно повысить приватность и безопасность, применяя GPG.

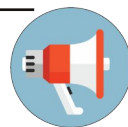
Если централизованной почты недостаточно, можно использовать **I2PBote**. Это плагин peer-to-peer почты для маршрутизатора. Полностью децентрализован, не имеет никаких критических узлов. Для распределения контента используется модель Kad. Плагин также добавляет свой собственный слой сквозного шифрования, что в сумме с криптографией I2P составляет три слоя шифрования между отправителем и получателем. Установка плагина простая: найти на сайте plugins.i2p ссылку для установки I2P-Bote, скопировать, открыть в маршрутизаторе «Настройки» -> «Клиенты», в самом низу вставить ссылку в форму и нажать «Установить». Плагин скачается и установится самостоятельно. После установки в основном меню появится пункт «Безопасная почта». По аналогии с GPG, для работы нужно создать свой ключ, только интересное отличие в том, что он же и будет является



адресом почты. Для основы ключа есть несколько алгоритмов на выбор, каждый из которых будет выдавать разную длину конечного адреса. В дополнительные функции входит ещё и задержка сообщения на промежуточных узлах, что делает timing-атаку невозможной.

Для более быстрого личного общения популярным средством является функция чата в **Skype**. Однако программа является проприетарной, поэтому провести адекватную проверку на лазейки невозможно. Сама компания отказалась выдавать спецификации своего криптографического протокола. Возможно, он слабый, чем могут воспользоваться различные ведомства, или на самодельных «секретных» алгоритмах, что ещё хуже. В качестве замены есть **I2P-Messenger**, простой кроссплатформенный мессенджер, написанный на C++ и с интерфейсом на Qt. Исходный код открыт. Скачать можно отсюда: <http://echelon.i2p/qti2pmessenger/>. Для его работы сначала нужно включить интерфейс SAM, открыв в маршрутизаторе «Настройки» -> «Клиенты» -> SAM, нажать кнопку «Запустить», поставить галочку «Запускать автоматически» и кнопку «Сохранить настройки». После





установки и запуска программа сгенерирует адрес автоматически. Адреса у этого мессенджера, как и у I2P-Bote, являются огромными нечитаемыми строками, ими и нужно обмениваться для использования. После добавления контакта могут быть задержки отображения статуса собеседника в несколько минут. Общего функционала мессенджера вполне хватает. Имеется чёрный список, можно менять статусы Online/Offline, ставить аватарки и даже передавать файлы.

Для группового общения вместо **Jabber-конференций** можно использовать **Irc2P**. Это несколько IRC-серверов, связанных в единую отказоустойчивую сеть. В маршрутизаторе I2P уже есть предустановленный туннель, направленный на все серверы в списке. Для подключения нужно выбрать IRC-клиент и указать в качестве сервера 127.0.0.1, порт 6668. После подключения можно делать всё то же самое, что и в обычном IRC — регистрировать ники, заходить на множество каналов, создавать свои каналы, писать личные сообщения и так далее. Общение на популярных каналах довольно оживлённое, однако на большинстве из них разговаривают на английском. Канал #i2p-dev используется разработчиками для обсуждения различных деталей проекта на постоянной основе и для тематических совещаний. Если при использовании соединение часто обрывается, можно увеличить количество туннелей. Для этого в консоли маршрутизатора открыть «Менеджер Туннелей» → Irc2P → «Резервное количество» и добавить 1 или 2 резервных, ниже нажать кнопку «Сохранить».

Помимо уже перечисленных программных средств периодически появляются различные **сервисы**, пригодные для общения. На момент написания имеются два стабильных **форума** — старейший в сети forum.i2p о самой сети и русскоязычный forum.rus.i2p со свободной тематикой. Есть **социальная сеть** visibility.i2p, рабочая и вполне способная заменить VK и всякие прочие фейсбуки. Довольно активным местом является **микроблоговая платформа** id3nt.i2p, представляющая из себя подобие твиттера.

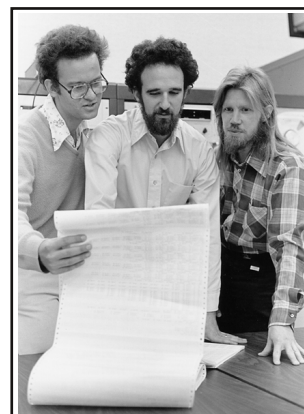
Основная проблема таких сервисов в том, что они очень часто пропадают после непродолжительной работы. Так пропали XMPP-серверы Salt и позже Jisko, pseudochan.i2p, who.i2p, anch.i2p. Причины могут быть разные — от нехватки ресурсов на хостинг до потери интереса при малой активности. Используя какой-либо публичный сервис в I2P, рекомендуется заранее обсудить с собеседником независимые от чужих серверов резервные средства связи на случай падения основного.

Заменяя привычные сервисы и средства связи на аналогичные в I2P, нужно понимать, что такая замена является компромиссом. Можно получить высокую степень анонимности и минимум два слоя шифрования, но платить за безопасность придётся удобством пользования. Как сказано выше, не все программы обладают привычными функциями или привлекательным внешним видом. Причина недоразвитости приложений в нехватке разработчиков или в отсутствии обратной связи с пользователями. К различным недостаткам самих средств добавляется специфика работы самой сети, что тоже может добавлять неудобства при использовании. Возможно, целесообразно будет сначала переводить наиболее важную часть коммуникаций в I2P, а затем пробовать перевести остальное по мере приобретения опыта.

Шифрование при помощи PGP/GPG

Защита своих данных от чужих глаз — вопрос жизни и смерти, а полагаться в этом вопросе на других означает доверять им свои данные. Защитить от любопытных носов свою переписку своими же силами поможет GnuPrivacyGuard. GPG — это инструмент асимметричного шифрования. Если проще, он создает такое сообщение, которое может прочитать только тот, кому ты его написал. Он незаменим при передаче любой важной текстовой информации. Это могут быть письма электронной почты, личные сообщения на форумах, или даже на публичных открытых сервисах. Помимо шифрования он также предоставляет несколько других функций для обеспечения безопасности.

Всегда самым очевидным способом защитить свои коммуникации было шифрование. Раньше для этого применялось симметричное шифрование, требовавшее передачи ключей по надёжному каналу. С развитием электронных коммуникаций, увеличением объёма данных и возможностей прослушки надёжная передача ключей стала трудной задачей. Поэтому в конце 1970-ых были разработаны асимметричные алгоритмы, позволяющие безопасно, открыто и автоматизировано обмениваться ключами. Схемы таких алгоритмов позволяют двум сторонам обменяться открытыми ключами, используемыми для обозначения получателя сообщения, и при зашифровке использовать открытый ключ получателя одновременно с секретным ключом отправителя. Расшифровать сообщение можно только секретным ключом получателя, и при этом будет видно, что шифрование выполнял именно владелец открытого ключа, то есть отправитель. В такой схеме секретные ключи, используемые для расшифровки, не нужно передавать, поэтому они остаются в безопасности, а отправитель сообщения выявляется при расшифровке, что исключает подмену информации. Но подобное изобретение было доступно только военным и спец. службам. В 1991 появился общедоступный инструмент асимметричного шифрования для личного использования — PGP, задавший стандарт, однако он был платным и являлся зарегистрированной товарной маркой. В 1999 был создан GPG — свободный, бесплатный, открытый и полностью совместимый со стандартом аналог PGP. Именно GPG стал самым популярным и зрелым инструментом асимметричного шифрования.

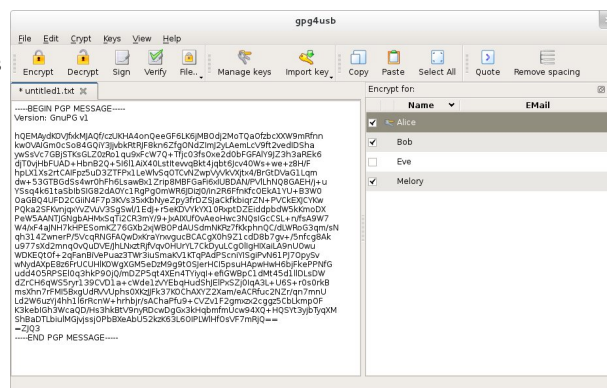


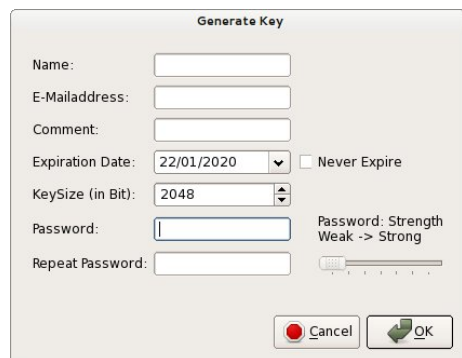
Авторы алгоритма шифрования с открытым ключом, слева направо: Меркль, Хеллман, Диффи

Важные термины

Прежде чем приступить к использованию GPG, нужно понять несколько главных особенностей этого инструмента. Первая и основная особенность — это понятие «ключи». Каждый пользователь создаёт себе свой личный ключ. Ключ пользователя состоит из двух частей — из публичной части («публичный ключ») и секретной части («секретный ключ»). Публичный ключ (далее просто «ключ») представляет собой своего рода визитную карточку, которую пользователь раздает всем своим контактам, желающим переписываться с шифрованием. Секретный ключ отвечает за процессы шифрования исходящих сообщений и расшифровки полученных. Его следует хранить в безопасном месте. Принято считать, что если кто-либо завладеет секретным ключом, то ключ можно считать скомпрометированным, а значит небезопасным. Этого следует избегать.

Вторая особенность — ключи, основанные на разных алгоритмах совместимы между собой. Неважно, использует ли пользователь RSA или ElGamal, для шифрования не нужно заботиться о таких деталях. Это достигается за счёт работы по упомянутому выше стандарту и через некоторые криптографические приёмы. Это одно из главных преимуществ GPG. Достаточно знать нужные команды, и программа сделает всё сама. В библиотеку входит большое количество асимметричных алгоритмов, симметричным шифров и односторонних хэш-функций. Разнообразие также является преимуществом, потому что позволяет создать одновременно и общие рекомендованные конфигурации, подходящие для большинства, и возможность тонкой настройки для более опытных пользователей.





Установка и создание ключей

Для начала работы нужно установить сам GPG. Пользователи Linux могут поставить его из любого пакетного менеджера, поискав там «gnupg», или собрать вручную. Пользователи Windows могут воспользоваться сильно устаревшим клиентом GPG4Win, который имеет несколько неприятных багов и больше функций, или портативным и более свежим клиентом GPG4USB, который имеет меньше функций, но намного проще и стабильнее.

Независимо от операционной системы и клиента, после установки нужно будет создать свой ключ, введя в терминале или кликнув в клиенте

соответствующую команду. Программа попросит определиться с алгоритмом шифрования. Обычно их два — это RSA и ElGamal (на самом деле три, если на Linux Вы отважились поставить экспериментальную ветку «modern» с криптографией на эллиптических кривых). Конкретных рекомендаций по алгоритмам нет, они разные и каждый выбирает себе схему по нраву. Затем необходимо определиться с размером ключа в битах. Здесь тоже нет короткого и однозначного ответа. У слишком длинных ключей есть и недостатки. Одно можно сказать с уверенностью: при выборе RSA и ElGamal не используйте ключи меньше 2048 бит, они крайне не безопасны. Далее программа попросит заполнить несколько форм: E-mail, Имя и комментарий. E-mail и Имя — это публичная информация, которую сможет увидеть каждый, с кем вы будете переписываться.

- В качестве почты можно указать другие виды связи, например ID какого-либо сервиса или мессенджера (Тех, Jabber, BitMessage и т. д.), разделив знаком «@» сам идентификатор/адрес и название сервиса. Чаще всего содержание именно этого поля используется для идентификации владельца ключа.
- Имя выбирать по своему усмотрению. Например, часто используемый ник или вообще «Anonymous».
- Поле комментария заполнять не обязательно. Можно ввести доп. адрес или свою должность. Комментарий будет виден другим пользователям.

После заполнения всех форм нужно ввести пароль. Его можно и пропустить, что не рекомендуется, так как это единственная мера безопасности, которая защитит секретную часть ключа в случае захвата файла с данным ключом злоумышленником. Также важно не забыть пароль, иначе работа с ключом будет более невозможна. При создании ключа нужно внимательно проверять корректность ввода всех полей — ошибки потом не исправить. Публичный ключ распространяется среди большого количества людей, поэтому среди пользователей не принято их часто менять — не у всех контактов может быть свежий ключ.

Сгенерировав свой GPG-ключ, можно начать его распространять. Для этого надо ввести команду отображения публичной части. Исторически сложилось так, что программа изначально применялась для шифрования почты и подписи публичных сообщений в почтовых рассылках, поэтому ключи отображаются по принципу формата PEM (англ. «Privacy-Enhanced Mail»). Формат представляет собой единый стандартный блок ключа, начинающийся заголовком ----BEGIN PGP PUBLIC KEY BLOCK----, за ним следует достаточно длинное тело самого ключа, закодированное цифрами и латинским алфавитом, и завершающий заголовок ----END PGP PUBLIC KEY BLOCK----. Весь блок с заголовками представляет собой ключ GPG, его и нужно распространять целиком. Помимо ручного распространения ключей, возможно использовать специализированные сервера. Пользователь загружает свой публичный ключ на сервер, и при необходимости любой может запросить его. Во многих программах в качестве сервера по умолчанию часто указывают сервер MIT.

Каждый GPG-ключ уникален. Запоминать и сравнивать такие большие блоки ключей вручную невозможно, поэтому для этого существуют отпечатки ключей. Каждый отпечаток ключа тоже уникален, формируется из публичной части, предоставляя короткую уникальную строку для идентификации. В строке отпечатка содержится 40 символов с разделением на 4 символа пробелами. Важно знать, что последние 8 или 16 символов являются еще и ID ключа. При использовании команд из терминала надо будет указывать ID для работы. Отпечатки удобны для быстрого сравнения двух ключей, или короткого указателя нужного ключа при нехватке места.

Шифрование сообщений и файлов

Шифрованные с помощью GPG сообщения состоят из похожих на публичный ключ блоков, только с заголовком ----BEGIN PGP MESSAGE----, а длина закодированной символами части зависит от длины сообщения. Подобные сообщения могут быть прочитаны только обладателем ключа, которому адресовано сообщение. Также можно зашифровать своё

послание для нескольких ключей, что очень удобно при общении небольшой группы людей. Шифровать можно и файлы, тогда результат шифрования будет записан в файл, а не кодирован текстовыми символами.

Подписи

Подпись сообщений является удобным средством открытого публичного подтверждения авторства, потому что, как и в случае с шифрованием, только истинный обладатель ключа может подписать свое послание таким ключом и подделать подобную подпись невозможно. Отличается от шифрованных сообщений тем, что текст остается открытым, заключённым с двух сторон соответствующим заголовком, а снизу добавляется небольшой блок самой подписи, также кодированный символами. При попытке изменить хотя бы один символ открытого текста, подпись станет не действительной. Проверка подписей также выполняется при помощи GPG.

Подписи тоже можно применять на файлах. Особенно часто эта функция применяется разработчиками ПО, связанного с безопасностью. Делается это для того, чтобы предотвратить подмену файлов злоумышленниками, которые могут встроить в программы вредоносный код. Подписываются обычно архивы или сборки, сама подпись сохраняется в отдельный файл с расширением .asc или .sig. Ключ публикуется в нескольких местах и/или загружается на сервер, где его очень трудно подменить. Сам процесс проверки называется «верификация подписи».

Web of Trust

Еще одна функция GPG, которую стоит упомянуть — это Web of Trust. Она используется для подтверждения принадлежности публичного ключа конкретному человеку. Для этого знакомые друг с другом пользователи GPG обмениваются ключами при личной встрече. Каждый из них сверяет отпечаток ключей и создает для каждого полученного ключа электронный сертификат, доказывающий достоверное соответствие между определенной персоной и публичным ключом. Создание сертификата называется «подписывание ключей». Сам сертификат потом загружается на сервер ключей, и любой может его запросить. Подразумевается, что чем больше пользователей подписали ключ, тем выше к владельцу доверие. Модель использования WoT предполагает, что пользователи всегда указывают в ключах свои реальные имена и все желающие установить сеть доверия могут физически встретиться для личного обмена ключами. Это делает подобную схему трудно выполнимой при анонимном общении. При псевдонимном общении для обмена можно использовать каналы связи или сервисы с аутентификацией, которая будет подтверждать достоверность. В любом случае, сети доверия при анонимном или псевдонимном общении не такие стойкие, частично из-за отсутствия «крепкого набора», формирующего основную группу доверенных пользователей, частично из-за человеческого фактора. Решение о целесообразности подобной сети доверия лежит целиком на группе пользователей, желающих ее построить.

Зачем вообще нужно всё это шифрование, если человек ничего не скрывает и не нарушает? Это один из самых часто задаваемых вопросов. На него есть несколько ответов. За последние годы возможность тотальной слежки за сетевой деятельностью миллионов пользователей стала уже вопросом не технической сложности, а ресурсов. Обладатели таких ресурсов — все спецслужбы мира и десятки крупных корпораций, с помощью таких программ как PRISM и X-Keyscore могут собирать и хранить годами все письма электронной почты, SMS-сообщения и историю звонков. Это нарушает конституционные права граждан на тайну переписки, однако влияние этих организаций такое сильное, что остановить неправомерный сбор информации невозможно. Использование GPG не снимет слежку с миллионов людей и не исправит магическим образом весь мир. Это всего лишь инструмент в руках человека. Инструмент, позволяющий сохранить письма и слова только для тех, кому они предназначены, и ни для кого больше. Это немного, но по крайней мере это возвращает право каждого человека на тайну переписки.

Если сбор данных и слежка кажутся слишком отдалёнными, можно рассмотреть шифрование с ещё более практичной стороны. Та же электронная почта в открытом виде проходит десятки промежуточных узлов. На каждом может быть сколько угодно уязвимостей и дыр безопасности, которые могут быть использованы кем угодно. В мире, где цифровые коммуникации играют ключевую роль, шифрование — это элементарное правило безопасности, предотвращающее огромное количество проблем. Глупо не воспользоваться возможностью повысить безопасность, учитывая что программа распространяется бесплатно, и освоить её можно достаточно быстро.

Подробнее ознакомиться с различными аспектами GPG можно на сайте PGPrU: <https://pgpru.com/>, а подробнее о командах можно почитать в официальном руководстве: <https://www.gnupg.org/gph/en/manual.html>.

Другие интернеты

Раз уж ты читаешь Вестник I2P, то наверняка сталкивался со словами Clearnet, Deepweb, Darknet, и так далее. Всё это — части многоэтажной внутренней структуры Интернета, сложившейся со временем. В неё определённым образом входит и I2P, а знание этих терминов позволяет если не лучше понять устройство Сети и связь её частей, то хотя бы не выставить себя деревенщиной в умном разговоре. Попробуем разобраться, что все эти слова означают, в чём разница, и что именно скрывается за этими обозначениями.

Определения

Clearnet — это часть ресурсов Интернета, которую большинство пользователей и называют собственно Интернетом, а именно всё, что можно найти с помощью поисковиков и переходов по ссылкам.

DeepWeb — доступная обычными способами, но не индексируемая поисковиками часть Интернета. Страницы, на которые нет ссылок, запрещённые к индексированию сайты, записи открытых баз данных, защищённые паролем разделы общедоступных сайтов, содержимое всевозможных архивов и так далее.

Darknet — сети, использующие для связи Интернет, но действующие по собственным протоколам и нестандартным портам. В народе зовутся «скрытосети». Для работы с ними следует что-то устанавливать и/или настраивать. Здесь числятся I2P, HiddenServices в TOR, P2P и F2F сети, децентрализованные сервисы типа Bitmessage и прочая экзотика.

Кроме этих, существуют и более глубокие слои, которыми мало кто интересуется, потому что достать оттуда что-либо довольно сложно, а найти там что-то стоящее ещё сложнее. Так, подключённые, но вообще не доступные узлы составляют Lost Net, а слежение за адресами, на которых ничего нет, позволяет обнаруживать по «фоновому шуму» крупные события вроде DDOS-атак.

С точки зрения анонимности и защиты персональной информации, из всего перечисленного наибольший интерес представляют даркнеты. Так что перечислим и сравним наиболее известные из них.



Сети

Сами даркнеты можно разбить на группы по выполняемым ими задачам. Это довольно условное деление с нечёткими границами, но применить его проще, чем отдельно описывать все особенности каждой сети.

В первую группу выделим сети, предназначенные для обмена информацией между пользователями. Сюда попадут файлообменники и мессенджеры.

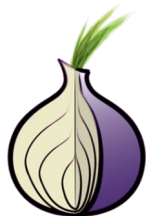
- **DC (Direct Connect)** Одна из первых пиринговых сетей для файлообмена, появившаяся в 2000-ом году на базе проприетарного клиента. Затем с помощью реверс-инженерии был создан свободный клиент DC++, ставший самым популярным. Сеть Direct Connect состоит из хабов — централизованных узлов, которые индексируют данные всей сети, и из клиентов, непосредственно хранящих эти данные. Поиск нужного контента осуществляется на хабах, которые при необходимости подключают запрашивающий клиент к другому клиенту, хранящему нужные найденные данные, после чего скачивание идёт напрямую.
- **eDonkey2000** Одна из первых файлообменных сетей, основанных на DHT. В отличие от BitTorrent, другого популярного DHT протокола, имеет полностью распределённый поиск, в то время как торренты полагаются на

поиск через внешнюю инфраструктуру — трекеры.

- **Tahoe-LAFS** Система распределённого хранения данных. Загружаемые в сеть данные шифруются, разделяются на небольшие блоки и загружаются на другие доверенные узлы с некоторой избыточностью. При скачивании загруженных данных процесс идёт в обратном порядке. Подобная система реализует принцип «Файловой системы с наименьшей ответственностью» (Least Authority File System), при котором нельзя наказывать за хранение одного пользователя, ведь файлы никогда не хранятся целиком на одном сервере. В этой системе шифрование гарантирует приватность и безопасность всех узлов, а избыточность блоков гарантирует надёжность хранения. Создатели специально исключили возможность загружать свои данные на узлы случайных пользователей сети, как это делает Freenet, поэтому предполагается, что пользователь вынужден искать надёжные узлы сам. Это могут быть собственные машины, платные сервера или узлы добровольцев.
- **Freenet** Анонимная сеть, организованная по принципу распределённого хранилища данных. Изначально создавалась как инструмент противодействия цензуре в Интернете. Файлы или сайты хранятся у множества случайных пользователей. В отличие от Tahoe-LAFS, скрывает все данные об источнике данных и их получателе. Хотя Freenet и является по сути хранилищем, его протокол может быть использован для создания распределённых форумов, почты, каналов и даже для чатов в реальном времени. На момент выхода в 2000 году именно Freenet повлиял на такие проекты как I2P, Tahoe-LAFS и GnuNet.
- **Bitmessage** Протокол и одноимённый клиент peer-to-peer почты со встроенным шифрованием. Адресами такой почты являются сами криптографические ключи пользователей. Распределение сообщений идёт через все узлы, но только владелец адреса-ключа может расшифровать предназначенные ему сообщения. Для защиты от спама была позаимствована модель Proof-of-Work из Биткойна: для отправки нового сообщения клиент выполняет ресурсоёмкую для процессора работу грубого перебора, что занимает некоторое время работы компьютера. Помимо личной почты, в BitMessage есть каналы, представляющие собой разновидность почтовой рассылки или чата. Отправлять сообщения можно как анонимно (от имени канала), так и со своего личного адреса. Как и с адресами Bitcoin, для поддержания анонимности приветствуется использование для каждой задачи отдельного адреса и частая смена адресов.

Во вторую группу запишем анонимайзеры — сети, предназначенные не для хранения и передачи контента, а для предоставления безопасного анонимного доступа к нему. Это, в первую очередь, TOR.

- **TOR (The Onion Routing)** представляет собой сеть для анонимного доступа к ресурсам Интернета, построенную по принципу луковичной маршрутизации (отсюда и название). В этой сети трафик от одного узла смешивается с трафиком других узлов, проходит несколько случайно выбранных промежуточных узлов и доходит до цели через последний узел, называемый выходным узлом. Смешивание и перенаправление трафика не позволяют выяснить истинный IP-адрес клиента; единственное, что увидит сервер — это адрес выходного узла.
- **JonDonym** Другая анонимизирующая сеть, где вместо луковичной маршрутизации применяются каскады перемешивания. Трафик от клиента проходит через один специализированный сервер, перемешивается с трафиком других пользователей, доходит до ещё одного сервера, где снова перемешивается, и так ещё несколько раз. Через сервера перемешивания проходит большой объём данных всех пользователей сети, что не позволяет профилировать отдельных пользователей, однако малое количество и отсутствие разнообразия каскадных серверов упрощает различные атаки на сеть. Ещё один недостаток каскадов перемешивания в том, что сервер является публичным и может быть отключён по предписанию суда той страны, в которой находится.



В последнюю группу соберём сети с HiddenServices — маленькие Интернеты со своими сайтами, доменами и сервисами как в Clearnet, но доступными только внутри этих даркнетов и только по их правилам. Это I2P, TOR и Freenet. Ниже будут описаны принципы и механизмы внутренней работы программ этих сетей.

- **Tor Hidden Services** Хотя сеть Tor создавалась как средство для анонимного доступа к ресурсам Интернета, внутренняя инфраструктура сети позволила разработчикам создать так называемые скрытые сервисы, местонахождение и IP-адрес которых никому не известен. Для начала скрытый сервис создаёт собственный ключ шифрования и распространяет его по сети. Затем он выбирает узлы встречи, подписывает их своим ключом и распространяет их адреса по сети. Теперь если какой-либо клиент хочет связаться с этим скрытым сервисом, для этого он ищет узлы встречи соответствующего сервиса и связывается с ними. Через эти узлы

встречи клиент передаёт скрытому сервису набор необходимых для связи данных: адреса своих собственных узлов встречи, уникальный токен для аутентификации и ключ для шифрования. Все эти данные зашифрованы и видны только самому скрытому сервису, чтобы узлы встречи не могли прослушивать. Получив контактные данные клиента, скрытый сервис связывается с ним через несколько промежуточных узлов, аутентифицируется, и связь идёт как в обычном соединении Tor. Адреса скрытых сервисов Tor содержат домен .onion.



- **I2P** Анонимная децентрализованная сеть, основанная на туннелях. Каждый сервис для связи генерирует публичный ключ шифрования, который также является уникальным адресом, и выстраивает туннель, выбирая несколько случайных промежуточных узлов. Затем сервис анонимно рекламирует последний узел туннеля как узел для связи. Клиент, желающий связаться с этим сервисом, ищет контактные данные в сетевой базе данных. Получив контактные данные, клиент указывает их последнему узлу в своём собственном туннеле. Установленное соединение идёт через сумму всех узлов в туннелях сервиса и клиента, и на каждом промежуточном узле соединение дополнительно шифруется. В отличие от Tor и Freenet, позволяет с некоторыми модификациями перенести многие привычные протоколы — BitTorrent, XMPP, IRC, почту и даже другие сети типа eDonkey2000 и Gnutella. Сеть поддерживает соединения TCP и UDP. Для повышения удобства распространения ключей, являющихся и адресами, в сети существует специальная инфраструктура для присваивания ключам-адресам читаемых адресов вида example.i2p, которая также позволяет автоматически добавлять свежезарегистрированные адреса.
- **Freenet** Как уже говорилось выше, Freenet основан на распределённом хранении. При первом запуске пользователь выбирает сколько дискового пространства он хочет выделить для сети. Это пространство становится частью распределённой системы. Программа также создаёт свой публичный ключ шифрования. На основе этого ключа выбираются соседние узлы по принципу «близости», то есть с похожими ключами. Близость позволяет другим узлам предугадать нахождение необходимого узла и запросить местоположение у соседей с похожим ключом. Передача данных на основе пакетных соединений или туннелирования невозможна, поэтому коммуникации основаны на передаче файлов, распространяющихся по распределённому хранилищу. Для размещения файла в системе, он сначала надёжно шифруется, и ему присваивается уникальный идентификатор, который распространяется по сети через таблицу маршрутизации. Узлы, у которых есть похожие идентификаторы, скачивают файл и добавляют его в своё хранилище. Эта «близость» опять поможет предугадать местонахождение файла по таблице маршрутизации. Владелец размещённого файла обладает его идентификатором, строкой описания и ключом. Они позволяют создать специальную ссылку для доступа к файлу — SSK, подписанную своим ключом. Эти ссылки должны распространяться другими средствами связи. Для доступа к файлу из SSK-ссылки, клиент запрашивает наличие уникального идентификатора в таблицах маршрутизации своих соседних узлов. Те запрашивают на основе «близости» таблицы своих соседей, пока не подберутся к месту нахождения файла. Затем он скачивается через посредников и расшифровывается. На основе передачи файлов в сети Freenet работает множество приложений: децентрализованная система форумов FMS, система распределённой почты и даже чат. Сайты внутри Freenet называются freesite.



Как видно из описания, принцип работы у всех сетей различается, и каждая сеть будет выполнять какие-то задачи лучше других. Tor создавался, грубо говоря, как прокси, и чрезвычайно эффективен для сокрытия IP-адреса клиента, поэтому скрытые сервисы являются скорее дополнением, чем главной задачей сети. На диапазоне применения сказывается и отсутствие многих функций. I2P создавалась как отдельная, изолированная сеть со своими сервисами и по возможностям предоставляет почти полноценный аналог обычного Интернета. Туннели в I2P предоставляют анонимность всем пользователям, так как из-за большого количества промежуточных узлов вычислить источник практически невозможно. Сквозное и промежуточное шифрование защищает от внешней и внутренней прослушки коммуникаций. Freenet создавался как безопасная сеть для обхода цензуры, однако из-за специфики хранилища создание веб-сервисов с динамичным содержанием невозможно, и сайты в Freenet всегда являются статическими страницами. Ещё один минус Freenet как хранилища в том, что непопулярные файлы в сети постепенно удаляются для освобождения места.

Юротдел



Начало текущего десятилетия ознаменовалось в России принятием ряда законов, несущих вред всему Интернету и ограничивающих твою, анон, свободу, и такие законы продолжают вводиться один за другим. Это случилось незаметно. Ты слышал об этом в новостях, но не придавал этому значения. Законопроекты продвигали под эгидой борьбы за авторские права, против терроризма, за права детей, и большинство согласилось. Лишь немногие поняли, что власти получили возможность моментально закрывать любой сайт без суда и следствия,

фильтровать содержимое Интернета и устранять неугодных без веских причин. Здесь и сейчас мы попробуем разобраться, что же случилось.

Ещё в 2012 году был создан «чёрный список» сайтов, страниц и IP адресов, доступ к которым провайдеры обязаны блокировать. Он пополняется ежедневно. По данным независимого проекта rublacklist.net, блокировке уже подверглось более 150 тысяч интернет-ресурсов, и более 95% были закрыты «за одно», просто потому что находились на том же IP, что и целевой сайт. Ты наверняка уже наткнулся на сайты, недоступные без видимых причин. Их число растёт, и целостность Интернета нарушается.

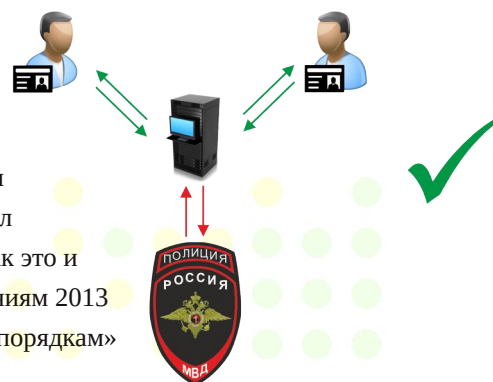
Новая запись в «чёрном списке» может появиться при получении жалобы или обнаружении информации, связанной со следующими вещами:

- детское порно;
- наркотики;
- суицид;
- «пиратское» кино;
- персональная информация;
- нелегальные митинги или беспорядки.

Думаешь, это к лучшему? А представь, что на твоём любимом сайте появился комментарий «Автор, вскрой вены!» или какой-нибудь тролль намеренно закинул картинку с голой малолеткой, и за это весь сайт бессрочно прикрыли. Именно так это и работает. И ведь не забыли про чисто политические мотивы: благодаря дополнениям 2013 года, любые резкие высказывания против власти могут назвать «призывом к беспорядкам» и заблокировать.

Дальше — хуже. Начиная с августа 2014 года, любая страница или сайт, на который заходит от 3000 человек в день, вносится в специальный реестр «блогов», а владелец считается блоггером. Он обязан публично раскрыть свою личность и контактные данные, выполнять в «блоге» премодерацию, и ему запрещено врать, любить порно (любое) и неприлично ругаться. Запрещённые вещи нельзя делать всем, кто что-либо размещает в этом «блоге», но ответственность за всех несёт блоггер.

Этот же закон обязует всех, кто участвует в передаче информации между пользователями, эту информацию сохранять, собирать данные о пользователях, хранить их внутри РФ и раскрывать по требованию. Любой сайт, который ты посещаешь, что-нибудь да узнаёт о тебе, это нормально, и к этому все привыкли. Но раньше большинство из них не сохраняли информацию и не старались намеренно её собирать, а теперь они обязаны. Только представь толщину твоего «личного дела», включающего всё что ты делал в Интернете за последние 6 месяцев (именно столько по закону должна храниться эта информация). Да ты сам о себе столько не знаешь, сколько записано там.



От редакции

На этом второй выпуск Вестника I2P заканчивается. Его подготовка заняла у нас гораздо больше времени, чем подготовка первого выпуска, более чем в два раза, но и содержание увеличилось соответственно. В будущем мы планируем попробовать публиковаться мелкими номерами, но чаще. Опыт других журналов, публикуемых в I2P, подсказывает, что регулярность подачи контента греет душу читателю больше, чем его количество, и не даёт интересу остыть.

А тем временем, у нас в редакции не хватает кадров. Помощь в работе над газетой нужна всегда, и это очевидно, но если об этом молчать, никто не откликнется. Поэтому мы обращаемся к тебе снова, Анон. Возможно, список вакантных позиций наведёт тебя или кого-то ещё на мысль, что всё это не так уж и сложно, и что пара часов личного времени на творческую работу — это даже интересно. Может, ты и не думал, что нам нужно?

- **Авторы** Главное в газете — тексты. Их пишут авторы. Чтобы выполнять работу автора, не нужно быть лауреатом литературных конкурсов. Это же газета, к тому же анонимная. Автору ставят задачу "написать о том-то", а дальше нужно просто изучить предложенный вопрос и связно изложить суть. На это способен любой полноценный человек. Если текст не будет отвечать стилистике или ещё какой-нибудь ерунде, его поправят редакторы.
- **Иллюстраторы** Газета без картинок — скучная газета. Их надо находить или рисовать, подбирать, редактировать, размещать...
- **Дизайнеры** Общий вид страниц и разделов определяют дизайнеры. Как тебе текущий дизайн? Мы перепробовали много разных вариантов, прежде чем пришли к этому. Если ты можешь лучше, милости просим.
- **Тайпсеттеры** Чтобы писать текст, нужен шрифт. Шрифт текста — как интонация в разговоре, поэтому подобрать шрифт — целая проблема. Нужно просмотреть тонны разных шрифтов, выбрать подходящие к дизайну или выражающие нужное настроение, убедиться в наличии нужных символов, найти где их можно скачать бесплатно и так далее. В приличных изданиях этим занимаются отдельные люди. И нам такой человек не помешает.
- **Редакторы** Авторы превращают эфемерную идею статьи в настоящий текст, но доводить его до готовности должны редакторы. Нужно проверять тексты на целый ворох типов ошибок, от простых орфографических до стилистических, фактологических и даже просто логических. Иногда текст может выражать не ту мысль или сообщать лишнее, иногда он не согласуется с иллюстрациями или соседними текстами, чаще сам с собой. Всё это исправляют редакторы. Если ты вскипаешь при виде ошибки и не можешь усидеть на месте от желания её исправить, добро пожаловать.
- **Пиарщики** Интересно, как ты узнал о Вестнике I2P? Знакомый дал ссылку? Случайно наткнулся? Никто не прочитает газету, если не рекламировать её. Для этого нужны коммуникабельные активные кадры.
- **Модераторы** В проекте HiddenGate есть Вики (где размещается наш редакционный отдел), форум и борда. Кто-то должен за ними присматривать и по мере необходимости решать возникающие вопросы.
- **Журналисты** Есть много интересных проектов, значимых людей, вокруг постоянно что-то происходит. Чтобы сообщать читателям новости, их нужно знать. Нам нужны люди, умеющие быть в курсе событий, чтобы ничто не проскользнуло мимо наших строк.
- **Технические специалисты** Анонимность, разумеется, не простой вопрос. Мы пишем о таких сложных вещах, как шифрование, сети, протоколы связи, криптовалюты, законы, и не всегда авторы и редакторы могут настолько хорошо разобраться в тематике, чтобы быть на 100% уверенными в правильности изложения материала. Поэтому на каждый вопрос нужен человек, способный расставить точки над i.

Чтобы связаться с нами, заходи на HiddenGate. И просто так тоже заходи. Размещённые там полезные статьи помогут разобраться в вопросах анонимности и сориентироваться в сети I2P, а на форуме и борде ты сможешь задать интересные вопросы и просто провести время за общением.

До следующего выпуска!