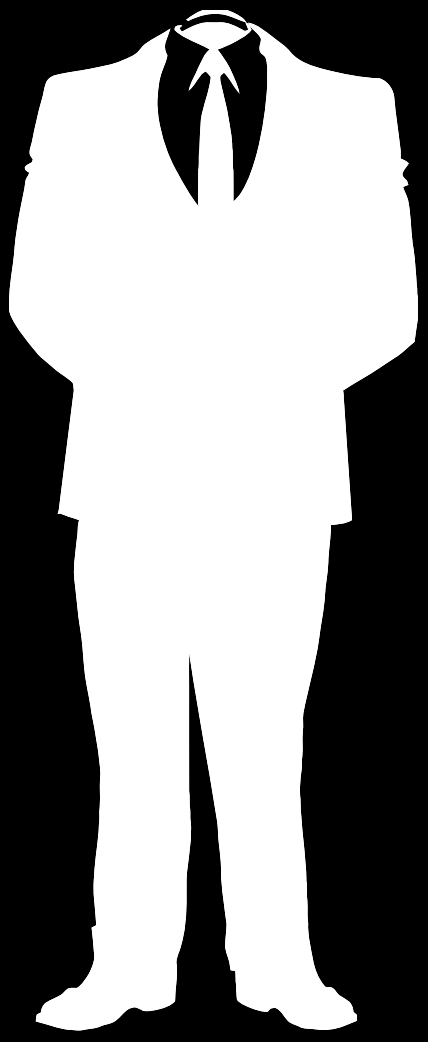
Настольная книга анонима

Зачем нужна анонимность и как её достичь?



Оглавление

Глава 1

Введение

1.1. Причины появления книги

В последнее время правительства многих стран стремятся уничтожить анонимность, оправдываясь «безопасностью граждан». Однако данное стремление направлено не на увеличение безопасности, оно направлено только на усиление контроля. Чиновникам нужна уверенность в том, что на следующий день они не потеряют своего кресла, что вы проголосуете за них на следующих выборах, что вы не узнаете об их лжи, что вы не выйдете на улицы, недовольные их произволом, что они продолжат также воровать деньги из бюджета и брать взятки. Они ищут способ контроля. Государства, называющие себя демократическими, становятся авторитарными. Но правительства, вмешивающиеся в личную жизнь, не являются единственной причиной жажды анонимности. За вами может также следить ваш работодатель, хозяин хот-спота в любимой кафешке, администрация вашего учебного заведения. Маркетологи следят за вами, чтобы показать вам более таргетированную рекламу. Организации, борющиеся с пиратством, следят за вами, чтобы отсудить у вас деньги за две скачанные композиции уже умершего певца. И если вас все это не устраивает, то данная книга для вас.

1.2. Связь с автором

Вы можете сообщить об ошибках или связаться со мной по иным причинам с помощью электронной почты anonhandbook@tormail.org или отправив свои изменения в репозиторий https://gitorious.org/anonymous-handbook. Также доступен сайт http://anonhandbook.org, его зеркало в I2P http://anonhandbook.i2p и в Tor — http://oxgzwiiypou6udlp.onion.

Глава 2

Необходимость анонимности в современном мире

2.1. Преследования

2.1.1. Обычные люди

Попадание данных о платежах «РосПилу» в руки активистам движения «Наши»

РосПил — некоммерческий проект «Фонда борьбы с коррупцией», занимающийся мониторингом государственных закупок с целью установления фактов коррупции. Финансируется за счет добровольных пожертвований.
Движение «Наши» — прокремлевское молодежное движение.
В апреле и мае 2011 года от имени некоторых новостных изданий неизвестными лицами были совершены звонки людям, которые отправляли пожертвования проекту «РосПил»[12]. Переводы осуществлялись на кошелек в системе Яндекс.Деньги. Представители Яндекса отметили, что данные по сотне человек, переводивших деньги на счет РосПила они действительно предоставляли ФСБ РФ[13]. Позже было выяснено, что звонки осуществляла комиссар движения «Наши» Юлия Дихтяр[14]. В ФСБ отказались комментировать то, как данные, предоставленные им, получили третьи лица[14].

Дело Витольда Филиппова

Витольд Филиппов поставил «лайк» под кадром из фильма «Американская история Икс», не запрещенного ни в одной стране. Прокуратура усмотрела в этом случай распространения нацистской символики[15]. 24 августа 2012 года он был приговорен к штрафу в 1000 рублей по статье 20.3 КоАП РФ («Пропаганда и публичное демонстрирование нацистской атрибутики или символики») без права обжалования[16].

2.1.2. Журналисты

По уровню свободы прессы, согласно отчету Freedom House 2012 года, Россия находится на 172 месте из 197 стран[17], а по данным «Репортеров без границ» — на 142 из 179[18]. С 1993 по 2009 год в России было убито 176 журналистов[19], а с 1998 года было совершено 871 нападение на журналистов и редакции[20].

Избиение Михаила Бекетова

Михаил Бекетов — журналист, обладатель премии Press Freedom Award[21], премии правительства РФ в области печатных СМИ[22], учредитель и главный редактор газеты «Химкинская правда», в которой публиковались статьи с критикой в адрес химкинской администрации. 24 мая 2007 года была

сожжена его машина[23], а 13 ноября 2008 года он был избит неизвестными[24], после чего долгое время находился в больнице и получил инвалидность 1-й группы[25]. Дело до сих пор не раскрыто.

Нападения на Олега Кашина

Олег Кашин — российский полический журналист, неоднократно подвергавшийся нападениям. Наибольший резонанс получило нападение на него 6 ноября 2010 года. Двое неизвестных поджидали его около его дома, в котором он снимал квартиру. Место своего проживания он держал в тайне. Один из нападавших держал Кашина, второй начал наносить удары железным прутом, который он прятал в букете[26]. Избиение продолжалось полторы минуты, за это время было нанесено 56 ударов[27]. Журналиста доставили в больницу, где были диагностированы переломы нижних конечностей, лицевого скелета и черепно-мозговая травма[28]. Несмотря на широкий общественный резонанс и поручение президента России Дмитрия Медведева о взятии дела под особый контроль[29], оно до сих пор не раскрыто.

Убийство Анны Политковской

Анна Политковская — российская журналистка и правозащитница. Была застрелена около лифта своего дома 7 октября 2006 года[30]. 19 февраля 2009 года суд присяжных оправдал подозреваемых Ибрагима и Джабраила Махмудовых, Сергея Хаджикурбанова и Павла Рягузова[31], однако вскоре Верховный суд РФ отменил этот оправдательный приговор и отправил дело на новое рассмотрение[32, 33]. В августе 2008 года был задержан Дмитрий Павлюченков[34]. В марте 2012 года он заявил, что слежку за Политковской заказал Лом-Али Гайтукаев, получивший от Ахмеда Закаева заказ, который якобы был удобен Березовскому[35]. Следствие по делу все еще продолжается.

Убийство Магомеда Евлоева

Магомед Евлоев — журналист, правозащитник, создатель сайта Ингушетия.Ru. Был убит выстрелом в голову 31 августа 2008 года. По официальной версии, Евлоев пытался отобрать автомат у сотрудника, сидевшего рядом с ним, после чего милиционер, находившийся рядом с водителем, выхватил пистолет и нацелил его на Евлоева. Выстрел, по утверждениям милиционеров, произошел случайно[36]. По данным редакции портала Ингушетия.Ru, Евлоев прилетел в одном самолете с президентом республики Ингушетия Муратом Зязиковым. После того, как президент уехал, Евлоева окружили сотрудники охраны министра внутренних дел Ингушетии, силой посадили его в машину и увезли. По дороге они выстрелили ему в голову и выбросили из машины[37].

Убийство Пола Хлебникова

Пол Хлебников — публицист, журналист, главный редактор русскоязычной редакции журнала Forbes. 9 июля 2004 года был застрелен около офиса российского отделения Forbes в Москве[38]. Дело так и не было раскрыто.

2.1.3. Блогеры

С 2008 по 2012 год правозащитной организацией «Агора» было зафиксировано 72 попытки введения регулирования Интернета, 16 нападений на блогеров, 160 уголовных преследований, 56 гражданско-правовых санкций, 386 фактов административного давления, 848 случаев ограничения доступа, 124 случая цензуры[39, 40, 41]. По уровню свободы слова в Интернете в 2012 году Россия занимала 30 место из 47[42].

Дело Саввы Терентьева

Савва Терентьев — блогер из Сыктывкара, фигурант первого уголовного дела в России, возбужденного за комментарий в блоге. Комментарий был оставлен 15 февраля 2007 года к записи, повествующей об изъятии жестких дисков компьютеров, принадлежащих редакции газеты «Искра» сотрудниками отдела «К»[43]. Текст комментария, оставленного блогером[44]:

> ненавижу ментов сцуконах. не согласен с тезисом ”у милиционеров остался менталитет репрессивной дубинки в руках властьимущих”, во-первых, у ментов, во-вторых, не остался. он просто-напросто неискореним. мусор - и в африке мусор. кто идет в менты - быдло, гопота - самые тупые, необразованные представители жив(отн)ого мира. было бы хорошо, если б в центре каждого города россии, на главной площади (в сыктывкаре - прям в центре стефановской, где елка стоит- чтоб всем видно было) стояла печь, как в освенциме, где церемониально, ежедневно, а лучше дважды в сутки (в полдень и полночь например) - сжигали бы по неверному менту, народ, чтоб сжигал, это был бы первый шаг к очищению общества от ментовско-гопотской грязи

7 июля 2008 года Терентьев получил год условно[45]. 12 июля 2011 года он получил политическое убежище в Эстонии[46].

Дело Ирека Муртазина

Ирек Муртазин — журналист, блогер, автор книги «Минтимер Шаймиев: последний президент Татарстана» и политический активист. 12 сентября 2008 года он разместил в своем блоге информацию о том, что президент Республики Татарстан, Минтимер Шаймиев, скончался. Текст размещенного поста выглядел так[47]:

> Пришла страшная весть...
> ...на 72-ом году жизни, во время отдыха в Турции (в Кемере) скоропостижно скончался Минтимер Шарипович Шаймиев. Честно говоря – не верится. Точнее, не хочется верить. Потому что, если это правда, то начнется такая свара, такая нешуточная борьба за то, чтобы занять освободившееся кресло, что чубы у холопов будут трещать и вдоль и поперек. И именно из-за подобных перспектив, ближайшее окружение Минтимера Шариповича попытается скрыть эту информацию. Чтобы успеть перегруппироваться (вплоть до скоропостижной эвакуации из страны). Именно поэтому официальная информация, думаю, будет не раньше чем через неделю

Муртазин был не первым человеком, разместившим информацию о смерти президента. Например, за два часа до его поста, появился пост в сообществе kazan с вопросом об истинности слухов о смерти Шаймиева[48]. Пресс-служба Шаймиева быстро опровергла слухи о смерти президента[49]. 10 декабря 2008 на блогера было заведено уголовное дело по обвинению в клевете и нарушении неприкосновенности частной жизни[50]. 29 декабря 2009 года на него напали неизвестные и избили[51]. Сам Муртазин считает нападение на него политическим[52]. 26 ноября 2009 года Ирека Муртазина признали виновным в клевете и возбуждение социальной ненависти либо вражды к определенной социальной группе (представителям власти[53]) с угрозой применения насилия (в его блоге, книге и газетах) и назначили наказание в виде 1 года и 9 месяцев лишения свободы с отбыванием наказания в колонии-поселении[54]. 31 января 2011 года было удовлетворено заявление об условно-досрочном освобождении Муртазина[55].

Дело Дмитрия Шипилова

Дмитрий Шипилов — блогер, разместивший в своем блоге сатирический диалог между губернатором Кемеровской области Аманом Тулеевым и его женой[56]. Суд приговорил Дмитрия Шипилова к 11 месяцам исправительных работ с удержанием 10% в пользу государства по статье 319 УК РФ (Оскорбление представителя власти)[57].

Глава 3

Общие правила анонимности

3.1. Нераскрытие информации

Даже если информация кажется вам незначимой и вы считаете, что по ней будет сложно установить вашу личность, не раскрывайте ее. Информация об одном лишь поле позволяет сократить число вариантов примерно в два раза. Комбинируя известную информацию, легко можно определить конкретного человека. Не распространяйтесь ни о своем роде занятий, ни о музыкальных вкусах, ни тем более о месте жительства и возрасте, если хотите остаться анонимным. Избегайте лишних вопросов.

3.2. Ложная информация

Для того, чтобы воспрепятствовать процессу установления вашей реальной личности вы можете специально давать ложную информацию. Например, вы можете сказать, что вы из Саратова, живя в Ростове-на-Дону. Поскольку тот, кто хочет установить вашу личность, не знает, где правда, а где ложь, то ваша ложь сильно усложняет ему задачу. Придумайте виртуального персонажа с выдуманными данными, от имени которого вы будете выступать.

3.3. Лингвистический анализ

Каждый человек имеет собственный идиолект — совокупность речевых особенностей, свойственных только ему. Поэтому даже если вы не указываете в тексте личной информации, остается возможным установление вашей личности. Допущенные в тексте ошибки, сленг, редкоиспользуемые слова и многая другая информация может помочь в установлении личности автора с помощью лингвистического анализа. При составлении текстов, авторство которых вы хотите сохранить в секрете, используйте стиль, отличный от стиля, которым вы пользуетесь в реальной жизни.

Глава 4

Анонимность в Интернете

! Не стоит забывать, что следующие методы необходимо использовать, по возможности, совместно друг с другом и с методами, перечисленными в предыдущей главе.

4.1. Прокси

! Не забывайте, что хозяева прокси-серверов и анонимайзеров видят трафик нешифрованным.

! Некоторые прокси-сервера передают заголовок X-Forwarded-For с реальным IP-адресом клиента.

Прокси-сервер — сервер, который позволяет пропускать через себя пользовательский трафик.
Для использования прокси просто задайте его адрес в настройках браузера и других приложений, трафик которых вы хотите пропускать через прокси.

4.1.1. Списки открытых прокси

1. http://xroxy.com
2. https://hidemyass.com/proxy-list
3. http://freeproxy.ch
4. http://proxylists.net
5. http://nntime.com

4.2. Веб-прокси

Веб-прокси) — веб-страница, которая позволяет пользователю получить контент с заданного адреса через себя.
Для использования веб-прокси, перейдите на его страницу и введите адрес сайта, который вы хотете посетить.

4.2.1. Некоторые веб-прокси

1. https://hidemyass.com
2. http://anonymouse.org

3. http://hide.pl
4. http://hideme.ru
5. http://guardster.com/free/

4.3. VPN

! Не забывайте, что хозяин VPN-сервиса видит трафик нешифрованным.

VPN — технология, позволяющая создавать сети поверх существующего Интернет-подключения. Из-за высокой скорости работы, простоты настройки и шифрования трафика от клиента до VPN-провайдера часто используется как средство сокрытия реального IP-адреса при доступе в Интернет. VPN-провайдеры обычно предоставляют свои услуги на платной основе.

4.3.1. Некоторые VPN-провайдеры

1. https://ipredator.se
2. https://kebrum.com
3. https://relakks.com
4. https://vpntunnel.se
5. http://ivacy.com

4.4. SSH-туннели

SSH — протокол, созданный для безопасной передачи данных. Часто используется для удаленного управления другими компьютерами, но может использоваться и для создания туннелей.
SSH-туннель — туннель, созданный с помощью SSH-соединения и используемый для передачи данных. Существуют организации, предоставляющие SSH-туннелирование на платной основе.

4.4.1. Использование

```
ssh –D localhost:port login@address
```

port — порт, трафик на который будет пропускаться через SSH-туннель.
login — ваш логин на удаленном сервере.
address — адрес удаленного сервера.
После этого установите в приложениях, трафик которых вы хотите туннелировать, например, в браузере, адрес SOCKS-прокси localhost с портом, который вы указали в предыдущем шаге.

4.4.2. Некоторые провайдеры SSH-туннелей

1. https://tunnelr.com
2. http://torvpn.com
3. http://vpnsecure.me
4. http://guardster.com
5. http://anonyproz.com

4.5. Настройка браузера

! Браузер передает огромное количество информации. По отдельности эта информация не представляет никакого интереса, но собранная вместе она может позволить практически со 100% вероятностью установить вашу личность.

4.5.1. Настройка браузера Firefox

Для изменения настроек можно использовать специальную страницу *about:config* или добавлять их напрямую в файл настроек *prefs.js*, находящийся в папке профиля. Некоторые полезные настройки доступны через стандартное меню настроек

Предпочитаемые языки

В меню «Настройки» → «Содержимое» → «Языки» удалите из списка все языки, кроме английского. Порядок должен быть en-us, затем en. Несмотря на то, что многие сайты будут теперь использовать по умолчанию английский язык, это повысит вашу анонимность, так ваш браузер станет менее уникальным.

Шрифты

По умолчанию Firefox передает список установленных шрифтов. Это может повысить уникальность вашего браузера, что отрицательно скажется на анонимности. Для отключения этого в *about:config* нужно поменять значение *browser.display.use_document_fonts* на 0.

Local storage

По умолчанию в Firefox включен Local storage и браузеру присвоен уникальный ID. Также страницы могут записывать в него свою информацию. Отключить Local storage можно изменением в *about:config* значения *dom.storage.enabled* на *false*.

Кеш

Для того, чтобы скрыть факт повторного посещения страницы, необходимо отключить кеш. Измените в *about:config* значения *browser.cache.disk.enable* и *browser.cache.memory.enable* на *false*.

DNS-запросы через SOCKS5 прокси

По умолчанию Firefox делает DNS-запросы в обход SOCKS5-прокси (например, при использовании Tor), что может помочь установить провайдеру, какие сайты вы посещали. Измените значение *network.proxy.socks_remote_dns* на *true*.

Передача информации о посещенных сайтах

Установите значение *browser.safebrowsing.enabled* в *false* и *browser.safebrowsing.malware.enabled* в *false* для тключения передачи информации о посещаемых веб-сайтах (система для борьбы с фишингом).

Подмена User Agent

Заменить значение User Agent можно и без расширений. Для этого существует параметр *general.useragent.over* установите его значение, например, в *«Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.7) Gecko/200091221 Firefox/3.5.7»*. Если выставить наиболее распространённое значение, то это поможет снизить уникальность пользователя.

Запрет Cookie для сторонних сайтов

Установите значение *network.cookie.cookieBehavior* в 1 для запрета Cookies для сторонних сайтов.

Запрет на передачу заголовка HTTP referer

Установите значение item *network.http.sendRefererHeader* в 0 для отключения передачи заголовка HTTP referer для обычного соединения, и значение *network.http.sendSecureXSiteReferrer* в 0 для отключения передачи для зашифрованного соединения.

Отключение Java

Для отключения Java установите значение *security.enable_java* в *false*.

4.5.2. Дополнения

HTTPS Everywhere

HTTPS Everywhere — дополнение для браузеров Firefox и Chrome/Chromium, переадресующее на HTTPS версию сайта, если она доступна. Это позволяет защититься от перехвата передаваемых данных, но не позволяет скрыть сам факт посещения вебсайта. Скачать дополнение можно тут https://eff.org/https-everywhere.

BetterPrivacy

BetterPrivacy — дополнение для браузера Firefox, позволяющее удалять флеш-куки (Local Shared Objects). Это небольшие куски данных, которые Adobe Flash может сохранять на компьютерах. Ссылка: https://addons.mozilla.org/firefox/addon/betterprivacy/.

Ghostery

Ghostery — дополнение для браузеров Firefox, Safari, Chrome/Chromium, Opera и Internet Explorer, позволяющее блокировать скрипты, невидимые изображения и прочие методы, используемые многими компаниями для слежки за пользователями. Работает и с LSO, может заменить BetterPrivacy. Сайт: https://www.ghostery.com.

TrackerBlock

TrackerBlock — дополнение, аналогичное по функциональности Ghostery, доступное для браузеров Firefox, Chrome/Chromium и Internet Explorer. Сайт: http://privacychoice.org/trackerblock.

Beef Taco

Beef Taco — дополнение для браузера Firefox, позволяющее блокировать куки ресурсов, шпионящих за пользователями. Сайт: http://jmhobbs.github.com/beef-taco/.

User Agent Switcher

User Agent Switcher — дополнение для браузера Firefox, позволяющее менять заголовок User-Agent, передаваемый браузером. Сайт: http://chrispederick.com/work/user-agent-switcher/. Вы можете скачать дополнительный список User-Agent здесь http://techpatterns.com/forums/about304.html и импортировать его в дополнение.

Smart Referer

Smart Referer — дополнение для браузера Firefox, которое позволяет отправлять адрес предыдущей страницы только если она находится на этом же домене. Скачать: https://addons.mozilla.org/firefox/addon/smart-referer/.

TrackMeNot

TrackMeNot — дополнение для браузеров Firefox и Chrome/Chromium, делающее переодические поисковые запросы к популярным поисковым системам с целью обезличить логи. Сами запросы являются случайными словами из заданной RSS-ленты. Сайт: https://cs.nyu.edu/trackmenot/.

NoScript

NoScript — дополнение для браузера Firefox, позволяющее блокировать JavaScript, Flash, Java и другие элементы на недоверенных сайтах. Сайт: http://noscript.net.

RequestPolicy

RequestPolicy — дополнение для браузера Firefox, позволяющее защититься от подделки межсайтовых запросов. Сайт: https://requestpolicy.com.

Cookie Monster

Cookie Monster — дополнение для Firefox, позволяющее управлять разрешениями на использование Cookies, например, разрешать их использование только доверенным сайтам. Скачать: https://addons.mozilla.org/firefox/addon/cookie-monster/.

ipFlood

ipFlood — дополнение для Firefox, симулирующее использование прокси путем добавления случайных IP-адресов в заголовки X-Forwarded-For, Client-IP и Via. Скачать: https://addons.mozilla.org/firefox/addon/ipflood/.

IPFuck

IPFuck — дополнение для Firefox, аналогичное ipFlood. Сайт: http://ipfuck.paulds.fr/.

4.5.3. Плагины

Сам факт наличия каких-либо редкоиспользуемых плагинов увеличивает уникальность вашего браузера. Также некоторые плагины, например Java, передают ваш настоящий IP адрес, даже если вы за прокси.

4.6. Анонимные оверлейные сети

Никогда не используйте анонимные сети с настройками, которые позволяют использовать Интернет в одном браузере в обход самой сети. В этом случае будет достаточно вставить любое изображение из внешнего Интернета, чтобы получить ваш реальный IP-адрес.

Оверлейные сети — это такие сети, которые работают поверх другой уже работающей сети.

4.6.1. Tor

Tor — анонимная оверлейная сеть, использующая принцип луковой маршрутизации, исходные коды которой распространяются на условиях лицензии BSD[58].
Луковая маршрутизация — технология анонимного обмена информацией, использующая многократное шифрование и пересылку через цепочки узлов. Каждый луковый маршрутизатор в цепочке удаляет слой шифрования и пересылает сообщение дальше, согласно полученным инструкциям, где все повторится. И так до тех пор, пока сообщение не достигнет адресата. Такое название технология получила из-за сходства данного процесса с очисткой луковицы.

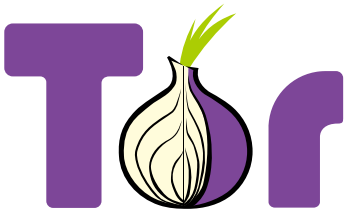


Рис. 4.1: Логотип Tor

Установка

Для установки посетите https://torproject.org или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

Самым простым способом использования Tor является установка Tor Browser Bundle. Просто скачайте его с https://torproject.org/projects/torbrowser.html, распакуйте и запустите.
Вы также можете установить Tor и задать в настройках приложений, которые вы хотите через него использовать, адрес socks5-прокси 127.0.0.1:9050.
Для использования приложений через Tor, не имеющих настроек прокси, скачайте torsocks — https://code.google.com/p/torsocks.

Недостатки

Не забывайте, что при использовании обычного Интернета через Tor, последняя нода в цепочке (exit-нода) видит трафик нешифрованным.

1. Медленная скорость работы.
2. Число нод ограничено (не через каждого пользователя Tor проходит трафик), из-за этого IP-адреса exit-нод блокируются на некоторых ресурсах, а в странах с жесткой интернет-цензурой, например, в Китае, блокируются адреса всех нод. Для обхода этой блокировки существуют бриджи — https://bridges.torproject.org.
3. Адреса скрытых сервисов сложно запомнить.

4.6.2. I2P

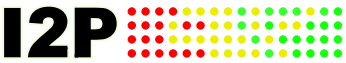


Рис. 4.2: Логотип I2P

I2P — анонимная оверлейная сеть, использующая принцип чесночной маршрутизации, исходные коды которой распространяются на условиях нескольких свободных лицензий[59]. В отличие от Tor, который в первую очередь направлен на доступ к сайтам обычного интернета (хотя в нем и существуют скрытые сервисы, аналогичные ипсайтам в I2P, а в I2P можно получить доступ к внешнему Интернету, используя аутпрокси), основной целью I2P является доступ именно к скрытым ресурсам — ипсайтам. Ипсайт от обычного вебсайта отличает только его нахождение в сети I2P.
Чесночная маршрутизация — вариант луковой, отличающийся тем, что несколько «луковиц» пересылаются совместно, что усложняет установку авторства сообщений.

Установка

Для установки посетите http://i2p2.de или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

После установки настройте свой браузер на использование HTTP-прокси 127.0.0.1:4444 и посетите страницу http://127.0.0.1:7657. Перед вами консоль маршрутизатора I2P — место, из которого можно управлять всеми настройками I2P.
Для начала перейдите в меню «Настройки I2P» (http://127.0.0.1:7657/config) и установите ограничения скорости в соответствии со скоростью вашего интернета. Затем добавьте следующие подписки susidns (http://127.0.0.1:7657/susidns/subscriptions).

```
http://www.i2p2.i2p/hosts.txt
http://i2host.i2p/cgi-bin/i2hostetag
http://stats.i2p/cgi-bin/newhosts.txt
http://tino.i2p/hosts.txt
http://dream.i2p/hosts.txt
http://biw5iauxm7cjkakqygod3tq4w6ic4zzz5mtd4c7xdvvz54fyhnwa.b32.i2p/uncensored_hosts.txt
http://trevorreznik.i2p/hosts.txt
http://cipherspace.i2p/addressbook.txt
http://hosts.i2p/hosts.cgi?filter=all
http://bl.i2p/hosts2.txt
http://rus.i2p/hosts.txt
http://inr.i2p/export/alive-hosts.txt
http://joajgazyztfssty4w2on5oaqksz6tqoxbduy553y34mf4byv6gpq.b32.i2p/export/alive-hosts.txt
http://qckbnfmbwiueuq2p234wiklgzs6zoc5bbuuubvkr3gb7ziwlsjoa.b32.i2p/list.txt
http://3i2rcjcis3fmy2ylj356qko2eaj5dx5pxlsqc6wqyeirod5uzwzq.b32.i2p/hosts.txt
```

Нажмите «сохранить» и «перезагрузить». В I2P отсутствуют корневые DNS-сервера, копия адресной книги хранится на каждом роутере. Данные подписки позволят вам обновлять информацию об адресах ресурсов в своей адресной книге.
Остальные настройки можно оставить по умолчанию. Подождите некоторое время для полноценной интеграции с сетью. После интеграции вы сможете полноценно пользоваться сетью. Попробуйте, например, посетить такие ресурсы, как http://forum.i2p (главный форум, есть рускоязычный раздел), http://rus.i2p (русская I2P-вики), http://pastethis.i2p (pastebin-подобный ресурс). Роутер желательно не выключать, так как при его перезапуске потребуется повторная интеграция с сетью.

Недостатки

! Не используйте аутпрокси для передачи конфиденциальных данных, владелец аутпрокси видит трафик нешифрованным.

1. Низкая скорость доступа.
2. Для синхронизации с сетью нужно время.

4.6.3. Freenet

Freenet — анонимная оверлейная сеть, использующая принципы P2P и F2F и распространяющаяся на условиях GNU GPL v2[60]. В отличие от Tor и I2P, позволяющих размещать любые ресурсы внутри сети, Freenet по сути представляет собой хранилище статичных данных.
P2P (Peer-to-peer) — компьютерная сеть, в которой все участники равны и выполняют одновременно роль как клиента, так и сервера.
F2F (Friend-to-Friend) — разновидность P2P-сети, в которой все соединения разрешаются только с доверенными узлами.

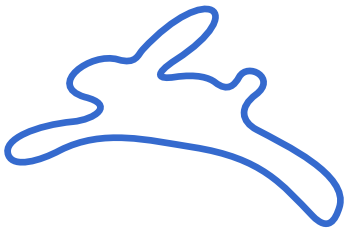


Рис. 4.3: Логотип Freenet

Установка

Для установки посетите https://freenetproject.org или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

Запустите Freenet и откройте в браузере страницу http://127.0.0.1:8888.

Недостатки

1. Низкая скорость доступа.
2. Требуется наличие некоторого количества свободного места на жестком диске.
3. Все сайты представляют собой статичные страницы.

4.6.4. GNUnet

Установка

Для установки посетите https://gnunet.org/ или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Рис. 4.4: Логотип GNUnet

Использование

Недостатки

1. Низкая скорость доступа.

4.6.5. JonDo

JonDo (**JonDonym**, также **Java Anon Proxy** или **JAP**) — программное обеспечение, представляющее доступ к цепочке прокси-серверов.

Установка

Для установки посетите https://anonymous-proxy-servers.net или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

JonDo напоминает Tor, но в отличии от Tor, где каждый доброволец может поднять как промежуточный сервер, так и exit-ноду, JonDo опирается на помощь отдельных организаций. Однако, Tor может использоваться в цепочке JonDo, для этого достаточно добавить адрес socks5-прокси Tor в настройки.
Бесплатная версия позволяет проксировать только HTTP и HTTPS трафик, в платной версии доступны все протоколы, а также нелимитирована скорость.
Для использования запустите JonDo и настройте браузер на использование прокси-сервера 127.0.0.1:4001.

Недостатки

1. В бесплатной версии можно проксировать только HTTP и HTTPS.
2. В бесплатной версии скорость ограничена до 30–50 кБит/с.
3. В бесплатной версии размер передаваемого файла ограничен 2 МБ.
4. Число нод очень сильно ограничено.

4.7. Анонимный файлообмен

4.7.1. I2Phex

I2Phex — форк Phex, клиента сети Gnutella, созданный для работы в I2P. Сайты: http://phex.svn.sourceforge.net/viewvc/phex/phex/branches/i2phex/, http://echelon.i2p/i2phex/, http://forum.i2p/viewforum.php?f=25.

4.7.2. iMule

iMule — форк aMule, клиента сети Kad, созданный для работы в I2P. Сайты: http://imule.i2p, http://echelon.i2p/imule/.

4.7.3. I2PSnark

I2PSnark — торрент-клиент в сети I2P, входящий в стандартную поставку I2P-маршрутизатора. Имеет веб-интерфейс, доступный по адресу http://127.0.0.1:7657/i2psnark/.

4.7.4. Robert

Robert — сторонний торрент-клиент в сети I2P. Сайт: http://echelon.i2p/robert/.

4.7.5. MUTE

MUTE — анонимная файлообменная сеть, основанная на муравьиной маршрутизации и одноименный клиент. Сайт: http://mute-net.sourceforge.net/.
Calypso — альтернативный клиент сети MUTE. Сайт: http://calypso.sourceforge.net/.

4.7.6. Retroshare

RetroShare — F2F и P2P анонимная сеть, позволяющая обмениваться файлами, мгновенными сообщениями, сообщениями BBS и безсерверной почтой. Сайт: http://retroshare.sourceforge.net/.

4.8. Анонимные платежи

4.8.1. Анонимные пластиковые карточки

Анонимные пластиковые карточки — карточки, которые зарегистрированны на какого-то другого человека. Обычно являются предоплаченными и их пополнение невозможно. Продаются на различных интернет-форумах и интернет-аукционах.

4.8.2. Bitcoin

Bitcoin — открытая электронная анонимная P2P криптовалюта с ограниченной эмиссией. В отличие от прочих валют, у Bitcoin отсутствует владелец и эмиссионый центр, эмиссия выполняется каждым участником сети. Данные о всех транзакциях хранятся в блоках, помещенных в распределенную базу данных.

Рис. 4.5: Логотип Bitcoin

Эмиссия — выпуск в обращение денежных средств.
Bitcoin в экономическом плане напонимает золото, но в отличии от золота его проще передавать, проще хранить, проще проверить подлинность и легко дробить на более мелкие суммы.

Установка

Для установки посетите http://bitcoin.org или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

! Кошельки в Bitcoin анонимны, но все транзакции открыты и каждый может их просмотреть через сервисы, подобные http://blockexplorer.com. Проводите деньги через биржи.

! Если вы потеряете свой кошелек (wallet.dat) или у вас его украдут, то вы не сможете вернуть деньги. Храните кошелек в безопасности, пользуйтесь функцией шифрования, делайте бекапы после каждой транзакции.

При первом запуске Bitcoin автоматически создает кошелек. Адрес его можно увидеть на вкладке «Получение монет». Там же вы можете создавать новые адреса, количество их не ограничено.

Недостатки

1. Немгновенные транзакции (транзакции на самом деле мгновенные, но в целях избежания мошенничества многие продавцы ждут генерации некоторого количества блоков, обычно 6).
2. Адреса кошельков сложно запомнить.
3. Так как у системы нет владельца, то ни заблокировать кошелек, попавший в руки мошенникам, ни вернуть вам деньги никто не сможет.

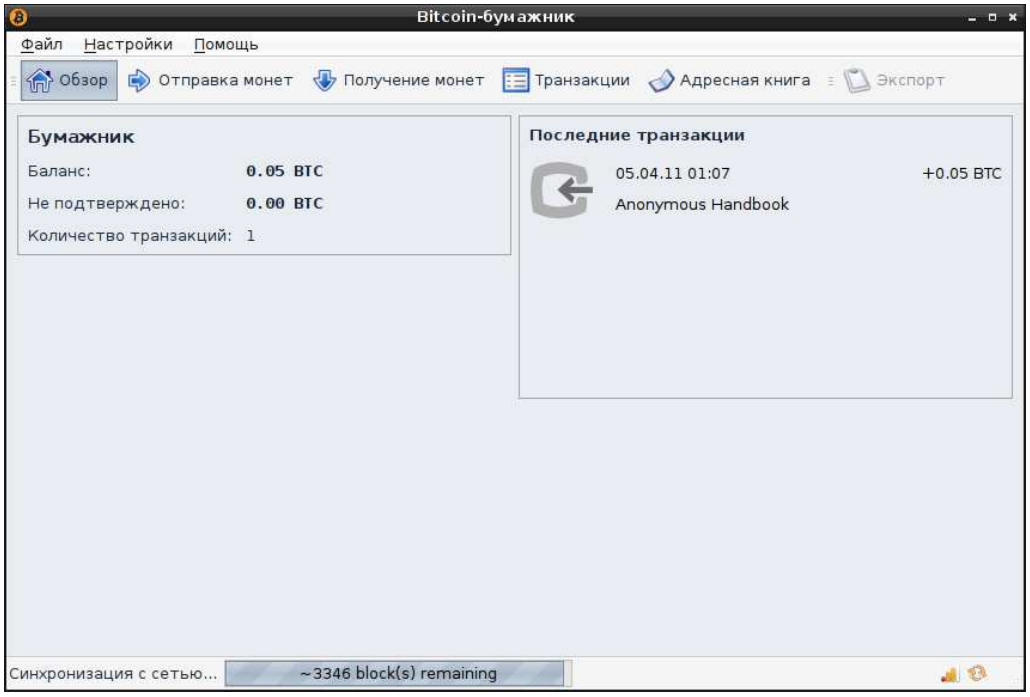


Рис. 4.6: Интерфейс Bitcoin

4.8.3. Liberty Reserve

Liberty Reserve — оффшорная платежная система, головной офис которой расположен в Сан-Хосе, Коста-Рика. Позволяет иметь кошельки в долларах США, евро и граммах золота. Транзакции являются неотменяемыми, данные, указываемые при регистрации, никем не проверяются. Комиссия составляет 1 % от суммы транзакции, но не меньше 1 цента и не больше 3 долларов, снимается с получателя платежа.

Регистрация

Зайдите на сайт https://www.libertyreserve.com/ и кликните на «Create Account». Заполните форму. Не указывайте реальных данных. «First Name» — имя, «Last Name» — фамилия, «Account Name» — логин, «E-mail» — электронная почта, «Re-enter e-mail» — повторить электронную почту, «Security Question» — секретный вопрос, «Answer» — ответ, «Personal welcome message» — сообщение приветствия, «Account Functions» — включить или не включать API, для большинства пользователей можно оставить «User (API disabled)» (не включать). Введите каптчу и кликайте «Agree» (принять).
На следующей странице для вас будет сгенерирован «Password» (пароль), «Login PIN» (PIN-код) и «Master Key» (мастер-ключ), также будут показан секретный вопрос и ответ на него, которые вы выбрали в предыдущей форме. Сохраните эти данные в безопасном месте. На почту вам должно придти письмо, в котором содержится ваш «Liberty Reserve account number» (персональный номер учетной записи). Его тоже необходимо сохранить в безопасном месте.
После этого вам нужно войти в свой аккаунт. Кликните на «Login» (вход) на сайте Liberty Reserve и введите свой «Account Number» из почты, пароль и каптчу. Нажмите «Next» (далее).
Будет показано сообщение приветствия (personal welcome message). Если оно совпадает с тем, которое вы вводили в момент регистрации, то значит вы находитесь на настоящем сайте Liberty Reserve, а не на фишинговой странице. Поставьте галочку на «I confirm that my custom welcome message is correct» (Я подтверждаю, что мое сообщение приветствия верно) и кликните «Continue» (продолжить).
Кликните на «Login PIN» и введите свой пин-код, выданый вам системой. Ввести его нужно с появившейся экранной клавиатуры. Нажмите «Login».
Заполните форму, опять выдуманными данными. «Address» — адрес, «City» — город, «Country» — страна, «State/Region» — штат/регион, «Zip/Postal Code» — почтовый индекс, «Date of Birth» — да-

та рождения в формате мм/дд/гггг, «Phone» — телефон, «Account will be used for» — аккаунт будет использован для, «Your Occupation» — род занятий. Нажмите на «Submit».
Вы зарегистрированы. Можете начинать пользоваться системой.

Недостатки

1. Так как у системы есть владелец, то ваш аккаут теоретически может быть заблокирован, а ваши данные предоставлены кому-либо.

4.9. IM-сервисы

4.9.1. I2P-Messenger

I2P-Messenger — программа мгновенного обмена сообщениями, работающая в сети I2P. Сайт: http://echelon.i2p/qti2pmessenger.

4.9.2. TorChat

TorChat — программа мгновенного обмена сообщениями, работающая поверх Tor. Сайт: https://github.com/prof7bit/TorChat.

4.9.3. JTorChat

JTorChat — версия TorChat, переписанная на Java. Сайт: https://github.com/jtorchat/jtorchat

4.9.4. Cryptocat

Cryptocat — доступный через браузер чат-сервис с прозрачным шифрованием на Javascript. Сайт: https://crypto.cat.

4.10. Ремейлеры

Ремейлеры — сервера, занимающиеся пересылкой сообщений электронной почты по указанному адресу.
Ремейлеры бывают псевдонимными (иногда их называют Type 0 или nym) и анонимными. Анонимные делятся на три типа:

1. Ремейлеры шифропанков
2. Mixmaster
3. Mixminion

4.10.1. Ремейлеры шифропанков

Ремейлеры шифропанков (Type I) — ремейлеры, удаляющие из получаемых писем всю информацию, которая может быть использована для идентификации, и пересылающие их на указанный адрес. Зачастую письма можно посылать зашифрованными с помощью GPG. Возможно использование цепочек из нескольких ремейлеров.

4.10.2. Mixmaster

Mixmaster (Type II) — ремейлеры, требующие установки специальной программы для отправки сообщений. Более безопасны, чем Type I, так как, например, пакеты с сообщениями всегда фиксированного размера, что не позволяет отслеживать письма по размеру. Сайт: http://mixmaster.sourceforge.net.

4.10.3. Mixminion

Mixminion (Type III) — ремейлеры, также требующие установки специальной программы, но еще более безопасные, так как используют луковичную маршрутизацию и имеют еще несколько улучшений. Сайт: http://mixminion.net.

4.11. Прием почты

! Хозяева всех перечисленных сервисов (кроме I2P-Bote) могут читать вашу почту. Шифруйте отправляемые письма.

4.11.1. I2P-Mail

I2P-Mail — обычный почтовый сервис, находящийся в сети I2P. Позволяет получить почту в домене mail.i2p и i2pmail.org. Пользоваться можно как внутри I2P, так и во внешнем интернете. Адрес: http://hq.postman.i2p.

4.11.2. I2P-Bote

I2P-Bote — несовместимая с обычной почтой безсерверная анонимная почта, реализованая в виде плагина для I2P. Сайт: http://i2pbote.i2p, http://i2pbote.net.

4.11.3. TorMail

TorMail — обычный почтовый сервис, работающий как скрытый сервис Tor. Позволяет получить почту в доменах tormail.org и tormail.net. Адрес: http://jhiwjjlqpyawmpjx.onion.

4.11.4. Privacybox

Privacybox — сервис анонимных контактых форм, работающий в I2P, Tor и обычном интернете. Адреса: https://privacybox.de, http://privacybox.i2p, http://c4wcxidkfhvmzhw6.onion.

4.11.5. TorPM

TorPM — сервис обмена сообщениями, работающий через веб-сайт. Позволяет обмениваться простыми текстовыми сообщениями, напоминающими обычную электронную почту. Адрес: http://4eiruntyxxbgf
onion/pm.

4.12. Шифрование данных

4.12.1. Truecrypt

Truecrypt — кроссплатформенное приложение для шифрования данных на лету. Позволяет шифровать как запоминающие устройства, так и создавать контейнеры для хранения шифрованных данных. Имеет возможность создания скрытых томов — к одному контейнеру можно получить доступ с помощью двух ключей, один из которых вы можете назвать, если к вам будет применено насилие, не раскрыв при этом содержимого секретного тома.

Установка

Для установки посетите http://truecrypt.org или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

Недостатки

4.12.2. dm-crypt

dm-crypt — подсистема прозрачного шифрования в Linux и DragonFly BSD. Позволяет шифровать на лету блочные устройства. В Windows доступ к шифрованным dm-crypt данным можно получить с помощью FreeOTFE (http://freeotfe.org).

Установка

Хоть dm-crypt и является частью ядра и его использование возможно без установки дополнительных утилит, все же для удобства лучше установить пакеты cryptsetup (https://code.google.com/p/cryptsetup) и cryptmount (http://cryptmount.sourceforge.net).

Использование

dm-crypt можно использовать для полного шифрования диска вместе с операционной системой. Многие дистрибутивы (например, Debian) имеют такую опцию в инсталляторе. Вам необходимо будет только создать небольшой незашифрованный раздел, на котором будет храниться загрузчик, и примонтировать его в /boot.
dm-crypt также можно использовать и для создания криптоконтейнеров:

```
# Создание пустого файла crypt.luks размером в 100 мегабайт
dd if=/dev/zero of=crypt.luks bs=1M count=100
# Подключение файла к зацикленной файловой системе
losetup /dev/loop0 crypt.luks
# Заполнение первых двух мегабайт случайными данными
dd if=/dev/urandom of=/dev/loop5 bs=1M count=2
# Создание криптоконтейнера
cryptsetup luksFormat -c aes-cbc-essiv:sha256 -s 256 -y /dev/loop0
# Открытие криптоконтейнера
cryptsetup luksOpen /dev/loop0 crypt
# Создание файловой системы
mkfs.ext4 /dev/mapper/crypt
# Закрытие криптоконтейнера
cryptsetup luksClose crypt
# Закрытие зацикленного устройства
```

```
losetup –d /dev/loop0
```

Монтировать криптоконтейнер можно с помощью pam-mount:

```
mount.crypt crypt.luks /mnt –o loop
```

Недостатки

4.12.3. eCryptfs

Использование

Недостатки

4.12.4. GPG

Установка

Для установки посетите http://gnupg.org или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

Для генерации ключей используйте следующую команду:

```
gpg ––gen–key
```

Просмотреть список доступных ключей:

```
gpg ––list–keys
```

Экспортировать открытый ключ:

```
gpg ––armor ––output pubkey.gpg ––export "ключ"
```

! Храните закрытый ключ в безопасности!

Экспортировать закрытый ключ:

```
gpg ––armor ––output key.gpg ––export–secret–keys "ключ"
```

Импортировать ключ:

```
gpg ––import "файл"
```

Зашифровать файл с помощью открытого ключа:

```
gpg ––encrypt ––recipient "ключ" –o "зашифрованныйфайл" "файл"
```

Расшифровать файл:

```
gpg ––output "файл" ––decrypt "зашифрованныйфайл"
```

Недостатки

4.13. Шифрование в IM

4.13.1. Off-the-Record Messaging (OTR)

! OTR не подходит для шифрования офлайн-собщений, так как подтвержденный вам ключ используется только для передачи других ключей, генерируемых каждую сессию. Ключи, используемые для шифрования сообщений, удаляются после завершения сессии. Сделано это было для того, чтобы нельзя было доказать авторство сообщений после завершения диалога.

OTR — криптографический протокол, предоставляющий шифрование в системах мгновенного обмена сообщениями. Встроенную поддержку имеют клиенты Adium, climm, MCabber, CenterIM, Phoenix Viewer, Vacuum IM, Jitsi, BitlBee, Spark, с помощью плагина OTR доступен в Pidgin[61], Kopete[62], Miranda IM[63], Psi+[64], Trillian[65], irssi[66], Gajim[67]. Также существует OTR localhost AIM Proxy, позволяющая использовать OTR в любом клиенте, но на данный момент поддерживаются только протоколы AIM/ICQ. Сайт: http://cypherpunks.ca/otr/, плагины для вашего клиента предоставляются сторонними разработчиками.

4.13.2. GPG и Jabber

XEP-0027 — расширение протокола XMPP (Jabber), позволяющее использовать GPG (OpenPGP) для шифрования сообщений[68]. Поддерживается клиентами Centericq, Gajim, Kopete, Psi и Miranda IM (с помощью плагина).

4.13.3. ZRTP

ZRTP — протокол шифрования передаваемого голоса в сетях VoIP. Поддерживается клиентами Twinkle, SFLphone, Jitsi, Linphone.

4.14. Шифрование почты

4.14.1. GPG

GPG позволяет шифровать любые данные, в том числе и почтовые сообщения. Подробнее работа GPG рассматривается в разделе «Шифрование данных».

Enigmail

Enigmail — дополнение для почтового клиента Thunderbird и набора приложений SeaMonkey, предоставляющее удобный интерфейс для работы с GPG в почтовых сообщениях. Сайт: http://enigmail.net.

4.14.2. S/MIME

S/MIME (**Secure/Multipurpose Internet Mail Extensions**) — стандарт подписи и шифрования электронной почты.

Получение бесплатного сертификата

Бесплатно сертификат можно получить у следующих центров сертификации:

1. https://cert.startcom.org
2. https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate
3. https://www.cacert.org/index.php?id=1 (корневой сертификат присутствует не везде)

Создание самоподписанного сертификата

Для этого нам понадобится OpenSSL (https://openssl.org).

```
openssl genrsa -des3 -out server.key 1024
openssl req -new -key server.key -out server.csr
openssl x509 -req -days 365 -in server.csr -signkey server.key -out
   server.crt
```

Использование

Для использования импортируйте ключ в ваш почтовый клиент. Сохраните ключи в безопасности.

4.15. Стеганография

! Использование стеганографии само по себе не делает недоступной передаваемую информацию, зная метод (что случается при использовании общедоступной программы) или подвергнув изображение стеганализу можно прочитать скрытую таким образом информацию. Используйте стеганографию совместно со сторонними или встроенными криптографическими утилитами.

Стеганография — способ тайной передачи информации путем сохранения в тайне самого факта передачи информации. Чаще всего используется совместно с криптографическими методами.
Компьютерная стеганография соответственно занимается, как можно догадаться, внедрением скрытой информации в различного рода файлы (изображения, звук, видео). Компьютерная стеганография делится на два вида: та, что скрывает данные в непосредственно в информации-контейнере (об этом, применимо к изображения, как раз далее) и та, что использует различные поля в форматах файлов-контейнеров (например, в *.jpg есть поля для комментариев).
Внедрение скрытого сообщения в изображение непосредственно связано со свойством избыточности в последних. В изображениях присутствует информация (шум), непосредственно не влияющая на восприятие человеком картинки. На замене части такого шума в изображении на внедряемое сообщение и основаны стеганографические алгоритмы.
Изображения, полученные сканированием (фотографированием) реальных объектов действительно содержат подобный шум (неоднородность освещения, тепловой шум в схемах и т.д.), однако в чисто цифровых (созданных на компьютере) изображениях его нет, поэтому для использования их в качестве контейнеров необходима предварительная обработка — наложение (псевдо-)случайно сгенерированного шума на изображение.

4.15.1. steghide

steghide — программное обеспечение, позволяющее скрывать данные в JPG, BMP, WAW и AU файлах. Поддерживается также шифрование алгоритмами CAST-128, ГОСТ 28147-89, Rijndael-128, Twofish, ARCFOUR, CAST-256, LOKI97, Rijndael-192, SAFER+, WAKE, DES, Rijndael-256, Serpent, XTEA, Blowfish, ENIGMA, RC2 или Triple DES. По умолчанию используется Rijndael-128.

Установка

Для установки посетите http://steghide.sourceforge.net/ или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

Вставка данных в изображение:

(a) (b) (c)

Рис. 4.7: Использование steghide: (a) исходное изображение; (b) в изображении закодирована фраза «Feci quod potui, faciant meliora potentes» с паролем «cogitoergosum»; (c) разница между изображениями.

```
steghide embed -cf "coverfile.jpg" -ef "embedfile.txt" -sf
    "stegofile.jpg" -p "password"
```

coverfile.jpg — файл, в который вставляются данные.
embedfile.txt — файл, который вставляется в изображение.
stegofile.jpg — файл со вставленным изображением.
password — пароль.

Извлечение данных:

```
steghide extract -sf "stegofile.jpg" -p "password" -xf
    "extractfile.txt"
```

stegofile.jpg — файл со вставленным изображением.
password — пароль.
extractfile.txt — файл, в который нужно записать извлеченные данные.

Недостатки

4.15.2. OpenStego

Установка

Для установки посетите http://openstego.sourceforge.net/ или установите пакет с помощью пакетного менеджера вашего дистрибутива.

Использование

Недостатки

4.15.3. StegoShare

StegoShare специально приспособлен для того, чтобы прятать несколько файлов в нескольких изображениях и расшаривать их в P2P-сетях.

Установка

Для установки посетите http://stegoshare.sourceforge.net или установите пакет с помощью пакетного менеджера вашего дистрибутива.

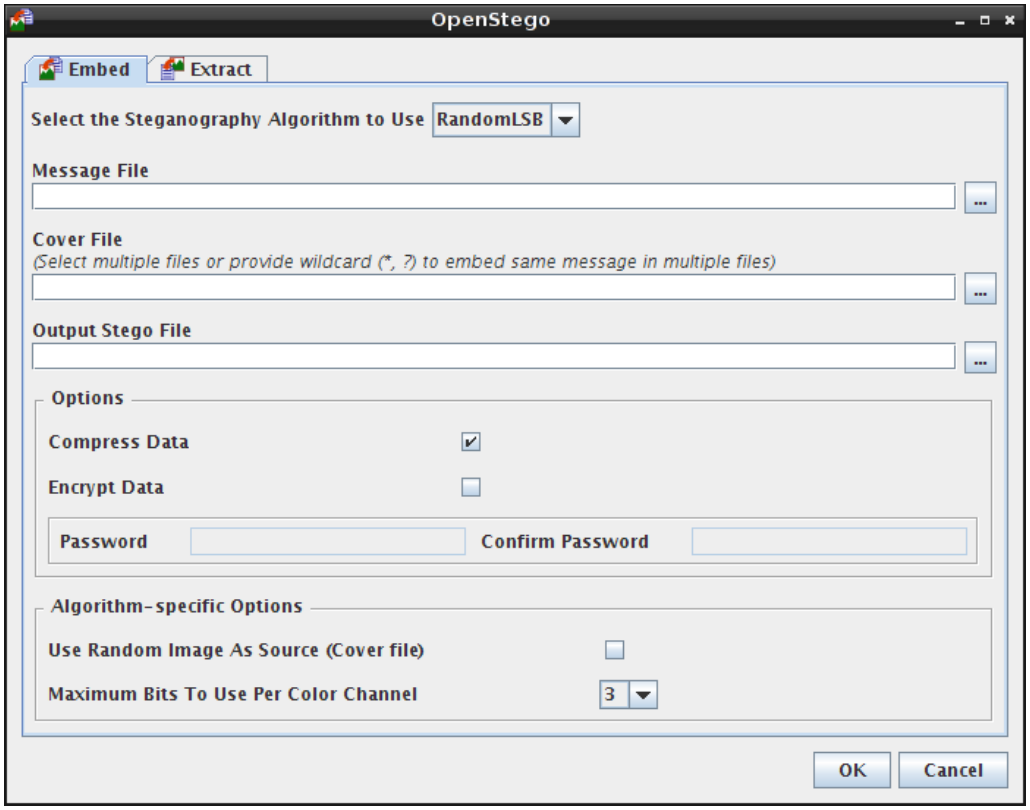


Рис. 4.8: Интерфейс OpenStego

(a) (b) (c)

Рис. 4.9: Использование OpenStego: (a) исходное изображение; (b) в изображении закодирована фраза «Feci quod potui, faciant meliora potentes» без пароля; (c) разница между изображениями.

Использование

Недостатки

4.16. Альтернативные DNS

4.16.1. Namecoin

Namecoin — распределенная система доменных имен, основанная на Bitcoin, хранящая в блоках информацию о доменах. Она сохранила многие плюсы Bitcoin, например, никто не может заблокировать ни один домен. В настоящее время возможно получение доменов в зоне .bit, однако воспользоваться ими смогут только те, кто предварительно настроил свой компьютер.

Установка

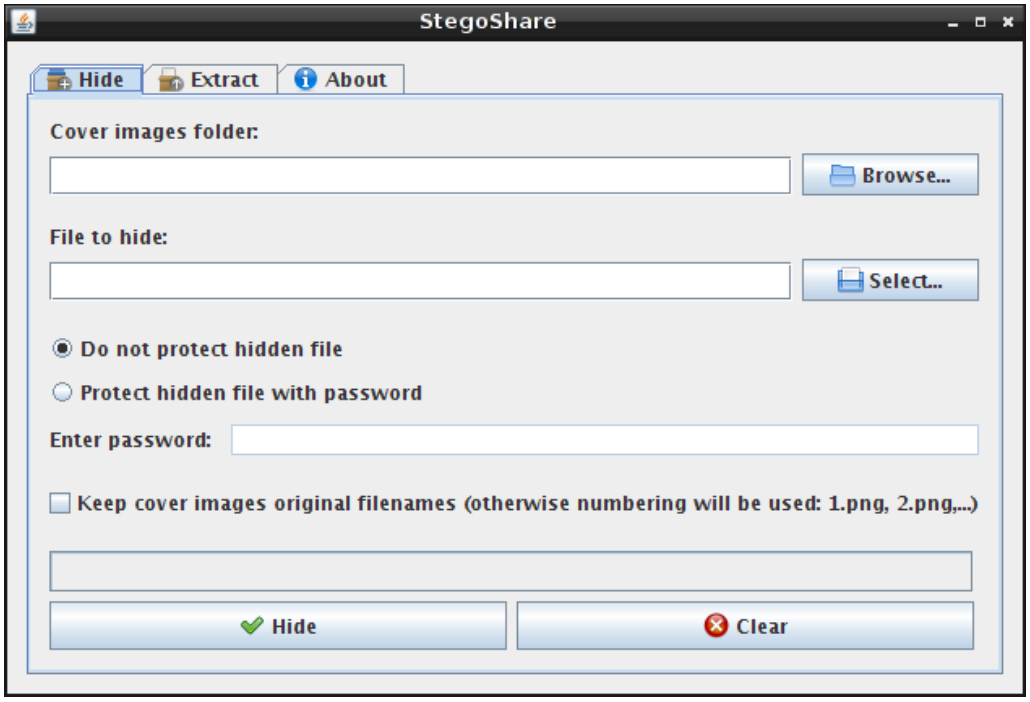


Рис. 4.10: Интерфейс StegoShare

(a) (b) (c)

Рис. 4.11: Использование StegoShare: (a) исходное изображение; (b) в изображении закодирована фраза «Feci quod potui, faciant meliora potentes» без пароля; (c) разница между изображениями.

! Стоит заменить, что все методы, не подразумевающие установку собственного резолвера, не безопасны. При использовании прокси-серверов владелец может перехватывать все данные, а при использовании открытых DNS-серверов владелец может установить сам факт посещения конкретного сайта.

Существует несколько способов использовать Namecoin.

1. Использовать открытый прокси, адреса которых перечислены здесь https://dot-bit.org/How_To_Browse_Bit_Domains#List_of_App_proxies.

2. Использовать альтернативный DNS-сервер с поддержкой Namecoin, адреса открытых серверов перечислены здесь https://dot-bit.org/How_To_Browse_Bit_Domains#List_of_DNS_servers.

3. Использовать DNS-суффикс https://dot-bit.org/How_To_Browse_Bit_Domains#List_of_DNS_suffixes.

4. Использовать веб-прокси https://dot-bit.org/How_To_Browse_Bit_Domains#List_of_Web_proxies.

5. Использовать BIND с NamecoinToBind.
   Подробнее https://github.com/khalahan/NamecoinToBind.

6. Использовать ncproxy совместно с Tor (наилучший вариант): https://dot-bit.org/forum/viewtopic.php?p=1448#p1448.

7. Использовать NmcSocks (тоже возможно использование вместе с Tor): https://github.com/itsnotlupus/nmcsocks.

Недостатки

4.16.2. Собственный кеширующий DNS сервер

! Запросы на получение записей доменных адресов, не находящихся в кеше, все равно будут отправляться на другие DNS-сервера, владельцы которых могут установить факт посещения вами определенных ресурсов. Локальный DNS-сервер лишь минимизирует количество таких запросов.

pdnsd

pdnsd — простой кеширующий DNS сервер, созданный для использования локально.
Конфигурация pdnsd находится в файле */etc/pdnsd.conf*.
Адреса используемых DNS-серверов находятся в секции *server*, параметр *ip*, где они перечисляются через запятую. Размер кеша задается в секции *global*, параметр *perm_cache*. Остальные параметры можно оставить по умолчанию.
Теперь осталось только установить использование DNS-сервера по адресу 127.0.0.1.

4.17. Хранение паролей

! Не используйте один и тот же пароль на нескольких ресурсах и не используйте простых паролей. Не храните пароли в открытом виде, пользуйтесь менеджерами паролей, которые используют криптографические методы для предотвращения кражи ваших паролей.

4.17.1. KeePassX

KeePassX (не путать с KeePass) — кроссплатформенный менеджер паролей, распространяющийся на условиях GNU GPL v2, форк KeePass. Сайт: https://keepassx.org.

4.17.2. KeePass

KeePass — кроссплатформенный (через Mono) менеджер паролей. Сайт: http://keepass.info.

4.17.3. KWallet

KWallet — кроссплатфоменный менеджер паролей, разрабатывающийся в рамках проекта KDE. Сайт: http://utils.kde.org/projects/kwalletmanager/.

4.17.4. Revelation

Revelation — менеджер паролей для GNU/Linux и *BSD. Сайт: http://revelation.olasagasti.info.

4.18. Безопасное удаление файлов

! Простое удаление файлов оставляет возможность для восстановления, так как файлы на самом деле никуда не исчезают, а просто помечаются как удаленные и на этот сектор диска становится возможна запись.

4.18.1. shred

shred — утилита из пакета GNU coreutils, позволяющая переписывать указанные файлы несколько раз, что делает практически невозможным их восстановление. Сайт GNU coreutils: http://www.gnu.org/software/coreutils.

Использование

```
shred -u "файл"
```

shreg

shreg — графический интерфейс для shred. Сайт: https://github.com/arxell/shreg.

4.18.2. wipe

wipe — аналогичная утилита для UNIX-подобных систем, работающая по тому же принципу. Сайт: http://lambda-diode.com/software/wipe/.

Использование

```
wipe "файл"
```

4.19. Метаданные

! В метаданных может храниться огромное количество информации о создателе файла.

4.19.1. mat

mat — утилита, позволяющая удалять метаданные из файлов png, jpg, Open Document Format (.odt, .odx, .ods, ...), MS Office OpenXML (.docx, .pptx, .xlsx, ...), pdf, tar, zip, mp3, mp2, mp1, mpa, ogg, flac, torrent. Сайт: https://mat.boum.org.

Использование

```
mat "файл"
```

4.19.2. ExifTool

ExifTool — библиотека и утилита для работы с метаданными, поддерживающая огромное количество форматов. Сайт: http://owl.phy.queensu.ca/~phil/exiftool.

Использование

Очистить файл от всех метаданных:

```
exiftool -overwrite_original -all= "файл"
```

4.19.3. ImageMagick

ImageMagick — комплекс утилит для работы с изображениям. Сайт: http://imagemagick.org

Использование

Очистить файл от всех метаданных:

```
convert -strip "файл" "чистыйфайл"
```

4.20. Смена MAC-адреса

MAC-адрес — уникальный идентификатор оборудования в сети. Устанавливается производителем оборудования, однако приоритет указанного в операционной системе MAC-адреса выше, так что будет использоваться он.

4.20.1. macchanger

macchanger — утилита для смены MAC-адреса в Linux. Позволяет выбирать как полностью случайный MAC-адрес, так и адрес из пространства конкретного производителя оборудования или конкретного типа устройства. Сайт: http://www.alobbs.com/macchanger.

Использование

Установка случайного MAC-адреса для устройства eth0:

```
macchanger -r eth0
```

Восстановление заводского MAC-адреса для устройства eth0:

```
macchanger -p eth0
```

Глава 5

Анонимность в реальной жизни

5.1. Желтые точки

При печати материалов (например, листовок) не стоит забывать, что многие принтеры кодируют микроточками информацию о времени печати и о серийном номере принтера[69]. Данная информация может быть использована для установления личности авторов отпечатков. Список принтеров, размещающих и не размещающих желтые точки смотрите в отчете Electronic Frontier Foundation[70].

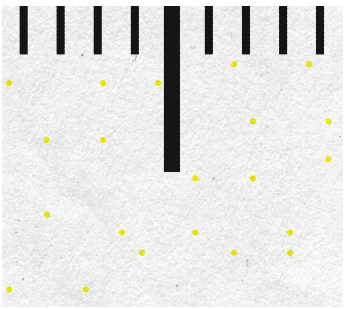


Рис. 5.1: Желтые точки. Изображение: Parhamr

5.2. Мобильные телефоны

Использовать мобильные телефоны, в общем случае, не безопасно. Вышки сотовой связи имеют ограниченный радиус действия, а операторы связи знают, где находится каждая вышка и к какой вышке подключен в данным момент каждый абонент. Все SIM-карты на территории РФ должны оформляться на конкретного человека, личность которого подтверждается и заносится в специальную базу (однако, можно купить так называемую «анонимную SIM-карту», такие SIM-карты продаются на различных форумах и аукционах). Также каждый мобильный телефон имеет уникальный номер — IMEI, по которому можно определить владельца даже после смены SIM-карты (смена IMEI возможна, но не для всех моделей телефонов). Вся эта информация согласно законодательству РФ должна храниться в течении трех лет и предоставляться через систему СОРМ-3 органам федеральной безопасностих[71].

1. Используйте анонимную SIM-карту.

2. Не используйте мобильный телефон в местах, которые можно однозначно связать с вами (работа, дом, образовательное учреждение и т.д.).

Глава 6

Законы, ограничивающие свободу слова и анонимность

6.1. Постановление Правительства РФ от 16 апреля 2012 г. № 313

Постановление Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» запрещает практически любую деятельность, связанную с криптографией, за исключением деятельности с использованием:

1. шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну;

2. шифровальных (криптографических) средств, а также товаров, содержащих шифровальные (криптографические) средства, реализующих либо симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит, либо ассиметричный криптографический алгоритм, основанный либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит, либо на методе вычисления дискретных логарифмов в иной группе размера, не превышающего 112 бит;

3. товаров, содержащих шифровальные (криптографические) средства, имеющих либо функцию аутентификации, включающей в себя все аспекты контроля доступа, где нет шифрования файлов или текстов, за исключением шифрования, которое непосредственно связано с защитой паролей, персональных идентификационных номеров или подобных данных для защиты от несанкционированного доступа, либо имеющих электронную подпись;

4. шифровальных (криптографических) средств, являющихся компонентами программных операционных систем, криптографические возможности которых не могут быть изменены пользователями, которые разработаны для установки пользователем самостоятельно без дальнейшей существенной поддержки поставщиком и техническая документация (описание алгоритмов криптографических преобразований, протоколы взаимодействия, описание интерфейсов и т.д.) на которые является доступной;

5. персональных смарт-карт (интеллектуальных карт), криптографические возможности которых ограничены использованием в оборудовании или системах, указанных в подпунктах »e» - »i» настоящего пункта, или персональных смарт-карт (интеллектуальных карт) для широкого общедоступного применения, криптографические возможности которых недоступны пользователю и которые в результате специальной разработки имеют ограниченные возможности защиты хранящейся на них персональной информации;

6. приемной аппаратуры для радиовещания, коммерческого телевидения или аналогичной коммерческой аппаратуры для вещания на ограниченную аудиторию без шифрования цифрового сигнала, кроме случаев использования шифрования исключительно для управления видео- или аудиоканалами и отправки счетов или возврата информации, связанной с программой, провайдерам вещания;

7. оборудования, криптографические возможности которого недоступны пользователю, специально разработанного и ограниченного для осуществления следующих функций:

   (a) исполнение программного обеспечения в защищенном от копирования виде;

   (b) обеспечение доступа к защищенному от копирования содержимому, хранящемуся только на доступном для чтения носителе информации, либо доступа к информации, хранящейся в зашифрованной форме на носителях, когда эти носители информации предлагаются на продажу населению в идентичных наборах;

   (c) контроль копирования аудио- и видеоинформации, защищенной авторскими правами;

8. шифровального (криптографического) оборудования, специально разработанного и ограниченного применением для банковских или финансовых операций в составе терминалов единичной продажи (банкоматов), POS-терминалов и терминалов оплаты различного вида услуг, криптографические возможности которых не могут быть изменены пользователями;

9. портативных или мобильных радиоэлектронных средств гражданского назначения (например, для использования в коммерческих гражданских системах сотовой радиосвязи), которые не способны к сквозному шифрованию (то есть от абонента к абоненту);

10. беспроводного оборудования, осуществляющего шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя (за исключением оборудования, используемого на критически важных объектах);

11. шифровальных (криптографических) средств, используемых для защиты технологических каналов информационно-телекоммуникационных систем и сетей связи, не относящихся к критически важным объектам;

12. товаров, у которых криптографическая функция гарантированно заблокирована производителем.

Полный текст постановления и приложения к нему можно прочитать здесь: http://government.ru/gov/results/18742/.

6.2. Указ Президента РФ от 3 апреля 1995 № 334

Указ запрещает деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации без лицензий, а также ввоз шифровальных средств иностранного производства без лицензии Министерства внешних экономических связей Российской Федерации[72].

6.3. Федеральный закон Российской Федерации от 28 июля 2012 г. № 139-ФЗ

Федеральный закон Российской Федерации от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации», также известный как **Законопроект № 89417-6** — закон, установивший цензуру в российском сегменте сети Интернет. Согласно закону, в России создается «Единый реестр доменных имен и (или) универсальных указателей страниц сайтов в сети Интернет и сетевых адресов сайтов в сети Интернет, содержащих информацию, запрещенную к распространению на территории Российской Федерации федеральными законами», в который вносятся доменные имена или ссылки на страницы. В течении суток о внесении в список должен быть проинформирован владелец сайта, если владелец не удалит информацию, из-за которой страница попала в реестр, то хостинг-провайдер обязан заблокировать сайт, тоже в течении суток. Если и он это не делает, то доступ к сайту обязаны ограничить операторы связи.
Против данного закона высказались: Совет по правам человека при президенте РФ[73], Русская Википедия[74] Яндекс[75], Google[76], LiveJournal[77], Вконтакте[78].
Законопроект был принят Государственной Думой Российской Федерации 11 июля 2012 года во втором и третьем чтении[79].
28 июля законопроект был подписан президентом РФ Владимиром Путиным, а 30 июля 2012 года был опубликован и вступил в силу[80, 81].
Согласно Постановлению Правительства Российской Федерации от 26 октября 2012 года № 1101, организацией, составляющей список запрещенных сайтов, стал Роскомнадзор[82].
1 ноября 2012 года на сайте http://zapret-info.gov.ru появилась форма для проверки наличия сайта в черном списке, а также форма для жалобы на контент в сети. Полностью список не публикуется.
Полный текст федерального закона: http://rg.ru/2012/07/30/zakon-dok.html.

6.4. СОРМ

Система технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ) — комплекс технических средства, направленных на обеспечение возможности проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и сетях персонального радиовызова общего пользования.
Поставщики услуг связи обязаны устанавливать СОРМ за свои деньги.
Следует различать СОРМ-1, созданный для прослушивания телефонных разговоров, СОРМ-2, созданный для протоколизации Интернет-соединений[83] и СОРМ-3 — комплекс, предназначенный для сбора, хранения и обработки информации об абонентах и оказанных им услугам связи, а также для предоставления оперативного доступа к этим данным[84]. В нормативно-правовых актах встречается только термин «СОРМ», термины «СОРМ-2» и «СОРМ-3» являются условными[85].

6.4.1. СОРМ-1

Система технических средств по обеспечению оперативно-розыскных мероприятий на сетях подвижной радиотелефонной связи (СОРМ СПРС) — система прослушивания телефонных разговоров и установления местоположения абонентов. СОРМ СПРС должна обеспечивать[86]:

1. контроль исходящих и входящих вызовов контролируемых подвижных абонентов в СПРС;
2. контроль исходящих вызовов (местных, внутризоновых, междугородных и международных) от всех абонентов СПРС к определенным абонентам (анализ по номеру В);
3. предоставление данных о местоположении контролируемых подвижных абонентов (ПА), подвижных станций (ПС) при их перемещении по СПРС;

4. сохранение контроля за установленным соединением при процедурах передачи управления вызовом (handover) как между базовыми станциями (БС) в пределах одного центра коммутации подвижной связи (ЦКП), так и разных ЦКП;

5. контроль вызовов при предоставлении ПА дополнительных услуг связи, в частности, изменяющих направление вызова (Call Forwarding). При предоставлении ПА такой услуги в процессе установления соединения должны контролироваться номера, на которые вызов перенаправляется (возможно неоднократное перенаправление вызова до установления разговорного состояния);

6. контроль за соединениями, обеспечивающими передачу телефонной и нетелефонной информации (передача данных, факсимильная связь, короткие сообщения);

7. при предоставлении контролируемому ПА дополнительной услуги, обеспечивающей возможность ПА одновременного разговора с несколькими абонентами, например «конференцсвязь», должны контролироваться номера всех абонентов;

8. возможность получения по запросу с пункта управления (ПУ) информации о ПА по его идентификатору или присвоенному номеру телефонной сети общего пользования (ТфОП), цифровой сети с интеграцией служб (ЦСИС), а именно предоставляемые данному ПА услуги связи.

6.4.2. СОРМ-2

СОРМ-2 — комплекс технических средств, направленных на осущественние оперативно-розыскных мероприятий путем логгирования и перехвата Интернет-трафика.
Сеть передачи данных обеспечивает техническую возможность передачи на пункт управления ОРМ следующей информации, относящейся к контролируемым соединениям и (или) сообщениям электросвязи, в процессе установления соединений и (или) передачи сообщений электросвязи[87]:

1. о выделенных абоненту (пользователю) сетевых адресах (IP-адресах) до реализации функции преобразования (трансляции) сетевых адресов и до начала передачи первого информационного пакета, а также информации о завершении контролируемого соединения;

2. передаваемой в контролируемом соединении и (или) сообщении электросвязи, включая информацию, связанную с обеспечением процесса оказания услуг связи в том виде и последовательности, в которых такая информация поступала с пользовательского (оконечного) оборудования или из присоединенной сети связи;

3. о местоположении пользовательского (оконечного) оборудования, используемого для передачи (приема) информации контролируемого соединения и (или) сообщения электросвязи, за исключением сетей передачи данных, в которых не предусмотрена технологическая возможность определения местоположения пользовательского (оконечного) оборудования.

6.4.3. СОРМ-3

СОРМ-3 — комплекс технических средств, предназначенный для сбора, хранения и обработки информации об абонентах и оказанных им услугам связи, а также для предоставления оперативного доступа к этим данным.
Оператор связи обязан своевременно обновлять информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи.
Базы данных должны содержать следующую информацию об абонентах оператора связи:

1. фамилия, имя, отчество, место жительства и реквизиты основного документа, удостоверяющего личность, представленные при личном предъявлении абонентом указанного документа, — для абонента-гражданина;

2. наименование (фирменное наименование) юридического лица, его место нахождения, а также список лиц, использующих оконечное оборудование юридического лица, заверенный уполномоченным представителем юридического лица, в котором указаны их фамилии, имена, отчества, места жительства и реквизиты основного документа, удостоверяющего личность, — для абонента-юридического лица;

3. сведения баз данных о расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонентов.

Указанная информация должна храниться оператором связи в течение 3 лет и предоставляться органам федеральной службы безопасности, а в случае отсутствия у органов федеральной службы безопасности необходимых оперативно-технических возможностей для проведения оперативно-разыскных мероприятий, связанных с использованием технических средств, указанные мероприятия осуществляют органы внутренних дел, являющиеся уполномоченными органами, в том числе в интересах других уполномоченных органов, путем осуществления круглосуточного удаленного доступа к базам данных[71].

Глава 7

Законы, гарантирующие свободу слова и анонимность

7.1. Статья 23 Конституции РФ

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

7.2. Статья 24 Конституции РФ

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

7.3. Статья 29 Конституции РФ

1. Каждому гарантируется свобода мысли и слова.

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.

3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

7.4. Статья 19 Всеобщей декларации прав человека

Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

Глава 8

Почему софт должен быть открытым?

8.1. Безопасность через неясность и принцип Керкгоффса

Безопасность через неясность (Security through obscurity) — уничижительное название принципа построения криптографических систем, согласно которому для обеспечения безопасности в тайне держатся особенности проектирования или реализации.
Принцип Керкгоффса — принцип построения криптографических систем, сформулированный Огюстом Керкгоффсом в 1883 году, заключающийся в том, что в тайне должен держаться только определенный набор параметров алгоритма (ключ), а сам алгоритм должен быть открытым.

8.2. Что такое Open Source

Open Source — программное обеспечение с открытым исходным кодом. Понятие Open Source не идентично понятию «свободное ПО» (хотя часто ПО принадлежит одновременно обоим категориям) — под свободным ПО подразумевают ПО, на которое действуют права на свободное использование, изучение, распространение и изменение, тогда как в случае с Open Source акцент делается на доступность исходных кодов.

8.3. Почему проприетарное ПО бывает опасно

8.3.1. Обновление Windows с отключенной службой Windows Update

24 августа 2007 года на компьютерах с отлюченной системой Windows Update (с отключенными автоматическими обновлениями) без ведома пользователя обновились некоторые файлы[88]. Теоретически это означает то, что Microsoft в любое время может исполнить любой код на любой Windows-машине (имеет бэкдур), даже если на них отключена служба автоматического обновления.

8.3.2. Carrier IQ

Carrier IQ — компания, разрабатывающий софт, устанавливающийся производителем на многие мобильные устройства. Carrier IQ записывает данные с GPS-навигатора, состояние звонков, нажатия клавиш, интернет-трафик и многое другое, после чего в некоторых случаях отправляет эту информацию производителю устройства или на собственные сервера[89][90].

8.3.3. Возможность получить IP адрес любого пользователя Skype

После декомпиляции и деобфускации исходного кода Skype стало возможным узнать IP-адрес любого пользователя, зная только его ник. Инструкция о том, как это сделать, размещена здесь: http:

//pastebin.com/LrW4NE2p. IP-адрес можно узнать даже в течении трех дней после того, как пользователь вышел из сети. Это — типичный пример излишней надежды на прицип «безопасность через неясность», который привел к серьезным проблемам.

8.3.4. Отправка данных о запускаемых приложениях в Windows 8

SmartScreen — новая технология, появившаяся в Windows 8 и включенная по умолчанию[91]. SmartScreen работает так: когда вы скачиваете приложение из Интернета, то в Microsoft передается хеш файла, имя файла и сертификат (если присутствует)[92]. При этом для передачи используется SSLv2, который не безопасен и злоумышленник может получить доступ к передаваемым данным[93].

Дальнейшее чтение

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. — URL: http://bitcoin.org/bitcoin.pdf.

[2] Dingledine R., Mathewson N., Syverson P. Tor: The second-generation onion router. — URL: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

[3] Репортеры без границ. Handbook for bloggers and cyber-dissidents. — URL: http://en.rsf.org/IMG/pdf/guide_gb_md-2.pdf.

[4] Free Software Foundation, Inc. Using the GNU Privacy Guard. — URL: http://www.gnupg.org/documentation/manuals/gnupg/.

[5] Руководство по Ubuntu для новичков. — URL: http://help.ubuntu.ru/manual/pdf.

[6] Руководство по установке Debian GNU/Linux. — URL: http://www.debian.org/releases/stable/i386/index.html.ru.

[7] Стив Рамбам. Анонимности нет, смиритесь (часть 1) // Hackers On Planet Earth. — 2008. — URL: https://www.universalsubtitles.org/ru/videos/YSEgofMg2wgv/ru/80608/.

[8] Филипп Циммерманн. Введение в криптографию. — PGP Corporation, 2004. — URL: https://pgpru.com/biblioteka/osnovy/vvedenievkripto.

[9] Eckersley P. How unique is your web browser? // Proceedings of the 10th international conference on Privacy enhancing technologies. — PETS'10. — Berlin, Heidelberg : Springer-Verlag, 2010. — P. 1–18. — URL: https://panopticlick.eff.org/browser-uniqueness.pdf.

[10] Solove D. J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy // San Diego Law Review. — 2007. — Vol. 44. — URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.

[11] Е. И. Галяшина. Основы судебного речеведения. — СТЭНСИ, 2003. — ISBN: 5813701133. — URL: http://rusexpert.ru/books/rech/rech.pdf.

Литература

[12] Анастасия Каримова. Транзакция устрашения // Коммерсантъ. — 2011. — май. — URL: http://www.kommersant.ru/doc-y/1624936.

[13] Коммерсантъ FM. Алексей Навальный выведет ”Наших” на чистую воду. — URL: http://www.kommersant.ru/doc-y/1634036.

[14] Русская служба BBC. Навальный: инцидент с ”РосПилом” - давление на интернет. — URL: http://www.bbc.co.uk/russian/russia/2011/05/110503_navalny_incident_comments.shtml.

[15] NEWSru.com. В Татарстане замглавы ячейки первой легальной партии националистов решили привлечь за ”лайк” в соцсети. — URL: http://newsru.ru/russia/02aug2012/like.html.

[16] Росбалт. В Татарстане блогер ”без права обжалования” оштрафован за кадр из американского фильма. — URL: http://www.rosbalt.ru/federal/2012/08/24/1026082.html.

[17] Karlekar K. D., Dunham J. Freedom of the press 2012 // Freedom House. — 2012. — URL: http://www.freedomhouse.org/sites/default/files/BookletforWebsite.pdf.

[18] Reporters without borders. World press freedom index 2011-2012. — 2012. — URL: http://en.rsf.org/IMG/CLASSEMENT_2012/C_GENERAL_ANG.pdf.

[19] Фонд защиты гласности, Центр экстремальной журналистики, Международная федерация журналистов. Журналисты погибшие в России - Убийство. — http://journalists-in-russia.org/jir/rjournalists/index/incident:Убийство. — 2009.

[20] Фонд защиты гласности. Нападения на журналистов и редакции. — 2012. — URL: http://www.gdf.ru/attacks_on_journalists/.

[21] Суд избавил журналиста от клеветы / Александр Черных, Александр Воронов, Ангелина Давыдова, Иван Тяжлов // Коммерсантъ. — 2010. — декабрь. — URL: http://www.kommersant.ru/doc/1556258.

[22] РИА Новости. Главред ”Химкинской правды” Бекетов получил премию правительства РФ. — 2011. — октябрь. — URL: http://www.ria.ru/media/20111031/476834949.html.

[23] NEWSru.com. В Химках сожгли машину главреда газеты, потребовавшего отставки властей. — 2007. — май. — URL: http://newsru.com/russia/24may2007/beketov.html.

[24] Лента.ру. В Химках избили главного редактора местной газеты. — 2008. — ноябрь. — URL: http://lenta.ru/news/2008/11/13/beketov/.

[25] Forbes. Путин пообещал ускорить расследование дела об избиении журналиста Бекетова. — 2012. — январь. — URL: http://www.forbes.ru/news/78356-putin-poobeshchal-uskorit-rassledovanie-dela-ob-izbienii-zhurnalista-beketova.

[26] Арматура как средство цензуры / Андрей Козенко, Владислав Трифонов, Мария Семендяева, Михаил Кирцер // Коммерсантъ. — 2010. — ноябрь. — URL: http://www.kommersant.ru/Doc/1534956.

[27] Елена Милашина. «Скоро год. Вы никого не поймали. Что мне делать?» // Новая газета. — 2011. — ноябрь. — URL: http://www.novayagazeta.ru/inquests/49335.html.

[28] Эхо Москвы. Избитый в Москве журналист Кашин пришел в сознание. — 2010. — ноябрь. — URL: http://www.echo.msk.ru/news/725257-echo.html.

[29] Дмитрий Медведев поручил Генпрокуратуре и МВД взять на особый контроль расследование нападения на Олега Кашина. — 2010. — ноябрь. — URL: http://kremlin.ru/news/9441.

[30] Газета.RU. Политковскую убили за два часа до сенсации. — 2006. — октябрь. — URL: http://www.gazeta.ru/2006/10/07/oa_219132.shtml.

[31] Лента.ру. Суд оправдал обвиняемых в убийстве Политковской. — 2009. — февраль. — URL: http://lenta.ru/news/2009/02/20/court/.

[32] Лента.ру. Верховный суд РФ отменил оправдательный приговор по делу Политковской. — 2009. — июнь. — URL: http://lenta.ru/news/2009/06/25/polit/.

[33] Лента.ру. Дело об убийстве Политковской отправили на доследование. — 2009. — сентябрь. — URL: http://lenta.ru/news/2009/09/03/prok/.

[34] РИА Новости. Павлюченков задержан по подозрению в организации убийства Политковской. — 2011. — август. — URL: http://ria.ru/inquest/20110823/422540826.html.

[35] Наталья Козлова. Заказчики поименно // Российская газета. — 2012. — март. — URL: http://www.rg.ru/2012/02/29/delo-site.html.

[36] Сергей Машкин, Муса Мурадов. Магомед Евлоев организовал посмертный митинг // Коммерсантъ. — 2008. — сентябрь. — URL: http://kommersant.ru/doc/1019413.

[37] Лента.ру. В Назрани скончался раненый владелец сайта ”Ингушетия.ру”. — 2008. — август. — URL: http://lenta.ru/news/2008/08/31/evloev1/.

[38] Лента.ру. В Москве убит главный редактор российского издания журнала Forbes. — 2004. — июль. — URL: http://lenta.ru/most/2004/07/09/killed/.

[39] Дамир Гайнутдинов, Павел Чиков. Несвобода Интернета (2008-2011) // Ассоциация АГОРА. — 2011. — URL: http://www.openinform.ru/fs/j_photos/openinform_313.pdf.

[40] Дамир Гайнутдинов, Павел Чиков. Несвобода Интернета (2011) // Ассоциация АГОРА. — 2012. — URL: http://openinform.ru/fs/j_photos/openinform_353.pdf.

[41] Дамир Гайнутдинов, Павел Чиков. Россия как глобальная угроза свободному Интернету // Ассоциация АГОРА. — 2013. — http://eliberator.ru/files/АГОРА. Несвобода Интернета 2012.pdf.

[42] Kelly S., Cook S., Truong M. Freedom of the net 2012 // Freedom House. — 2012. — URL: http://www.freedomhouse.org/sites/default/files/resources/FOTN2012-FullReport.pdf.

[43] Лента.ру. Прокуратура заподозрила пользователя ЖЖ в оскорблении милиции. — 2007. — апрель. — URL: http://lenta.ru/news/2007/04/12/livejournal/.

[44] NEWSru.com. Дело сыктывкарского блоггера Терентьева, обвиняемого в разжигании социальной розни, передано в суд. — 2008. — март. — URL: http://www.newsru.com/russia/12mar2008/terentiev.html.

[45] Газета.Ru. Блогер Терентьев получил год условно. — 2008. — июль. — URL: http://www.gazeta.ru/news/lastnews/2008/07/07/n_1240265.shtml.

[46] Русская служба BBC. Эстония предоставила убежище блогеру из России. — 2011. — июль. — URL: http://www.bbc.co.uk/russian/international/2011/07/110713_terentyev_estonia_asylum.shtml.

[47] Ирек Муртазин. Пришла страшная весть... — 2008. — сентябрь. — URL: http://irek-murtazin.livejournal.com/218516.html.

[48] hotlips2005. Шаймиев умер? — 2008. — сентябрь. — URL: http://kazan.livejournal.com/2919161.html.

[49] Газета.Ru. Пресс-служба Шаймиева опровергла сообщения о его смерти. — 2008. — сентябрь. — URL: http://www.gazeta.ru/news/lenta/2008/09/12/n_1269689.shtml.

[50] Клуб регионов. Ирек Муртазин: «Написать на меня заявление Шаймиева убедили люди из его окружения». — 2008. — декабрь. — URL: http://club-rf.ru/news/tatarstan/irek_murtazin_napisat_na_menya_zayavlenie_shaymieva_ubedili_lyudi_iz_ego_okruzheniya/.

[51] Комсомольская правда. Бывшего пресс-секретаря президента Татарстана избили бейсбольными битами рядом с домом. — 2009. — январь. — URL: http://kazan.kp.ru/daily/24224.01/425229/.

[52] Каспаров.ru. Методом кнута. — 2009. — декабрь. — URL: http://www.kasparov.ru/material.php?id=4959E1DF8D9CA.

[53] ИА REGNUM. Шаймиев в суде признал власть отдельной социальной группой. — 2009. — август. — URL: http://www.regnum.ru/news/1194892.html.

[54] Комсомольская правда. Экс-пресс-секретарю президента Татарстана Муртазину дали реальный срок. — 2009. — ноябрь. — URL: http://www.kp.ru/online/news//577494/.

[55] Интерфакс. Бывший пресс-секретарь Шаймиева, блогер Муртазин освобожден по УДО. — 2011. — январь. — URL: http://www.interfax.ru/news.asp?id=175463.

[56] Дмитрий Шипилов. Говорит и показывает. — 2011. — ноябрь. — URL: http://shipilov.livejournal.com/82673.html.

[57] Грани.ру. Блогер получил 11 месяцев за оскорбление Тулеева. — 2012. — апрель. — URL: http://grani.ru/Internet/m.196855.html.

[58] The Tor Project, Inc. Лицензия Tor. — URL: https://gitweb.torproject.org/tor.git?a=blob_plain;hb=HEAD;f=LICENSE.

[59] I2P Project. I2P software licenses. — URL: http://www.i2p2.de/licenses.html.

[60] Freenet Project. LICENSE. — URL: https://github.com/freenet/fred-staging/blob/master/LICENSE.

[61] Cypherpunks.ca. Off-the-Record Messaging. — URL: http://www.cypherpunks.ca/otr/.

[62] dreadhead. Kopete OTR plugin. — URL: http://kde-apps.org/content/show.php?content=55002.

[63] Miranda IM. OTR. — URL: http://addons.miranda-im.org/details.php?action=viewfile&id=2644.

[64] Engel T. Jabber Off-the-Record Messaging. — URL: http://public.tfh-berlin.de/~s30935/.

[65] Twanfox. Trillian Off-the-Record. — URL: http://trillianotr.kittyfox.net/.

[66] irssi-otr: Off-the-Record Messaging (OTR) for the irssi Internet Relay Chat (IRC) client. — URL: http://irssi-otr.tuxfamily.org/.

[67] How to get OTR encryption for gajim. — URL: http://gajim-otr.pentabarf.de/.

[68] Muldowney T. — XEP-0027: Current Jabber OpenPGP Usage. — XMPP Standards Foundation, 1.3 edition, 2006. — URL: http://xmpp.org/extensions/xep-0027.html.

[69] Electronic Frontier Foundation. DocuColor tracking dot decoding guide. — URL: http://w2.eff.org/Privacy/printers/docucolor/.

[70] Electronic Frontier Foundation. List of printers which do or do not display tracking dots. — URL: https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots.

[71] Михаил Фрадков. Постановление Правительства Российской Федерации от 27 августа 2005 г. N 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» // Российская Газета. — 2005. — URL: http://www.rg.ru/2005/09/02/pravila-dok.html.

[72] Министерство связи и массовых коммуникаций РФ. Указ от 3 апреля 1995 г. N 334 «О мерах по соблюдению законности в области разработки, производстава, реализации и эксплауатации шифровальных средств, а также предоставления услуг в области шифрования информации». — 1995. — URL: http://www.libertarium.ru/ukaz_334.

[73] Лента.ру. Совет по правам человека предупредил Рунет о цензуре. — URL: http://lenta.ru/news/2012/07/03/nochinaplease/.

[74] Викимедиа РУ. Забастовка Википедии на русском языке. — URL: http://wikimedia.ru/blog/2012/07/10/zabastovka-vikipedii-na-russkom-yazyke/.

[75] Елена Колмановская. О законопроекте № 89417-6. — URL: http://clubs.ya.ru/company/replies.xml?item_no=48073.

[76] Алла Забровская. Новый закон угрожает свободному Интернету. — URL: http://googlerussiablog.blogspot.com/2012/07/blog-post.html.

[77] Живой Журнал за свободу информации . — URL: http://livejournal.livejournal.com/19317.html.

[78] Константин Ходаковский. Яндекс и Вконтакте поддержали Википедию, выступив против законопроекта № 89417-6 // 3DNews. — 2012. — июль. — URL: http://www.3dnews.ru/software-news/632136.

[79] Вечернее пленарное заседание Госдумы 11 июля. — URL: http://www.duma.gov.ru/news/273/180195/.

[80] Владимир Путин. Федеральный закон Российской Федерации от 28 июля 2012 г. N139-ФЗ // Российская Газета. — 2012. — июль. — URL: http://rg.ru/2012/07/30/zakon-dok.html.

[81] Лента.ру. Закон о реестре запрещенных сайтов вступит в силу 30 июля. — URL: http://www.lenta.ru/news/2012/07/29/blacklist/.

[82] Дмитрий Медведев. Постановление Правительства Российской Федерации от 26 октября 2012 г. N 1101 г. Москва // Российская газета. — 2012. — URL: http://www.rg.ru/2012/10/29/reestr-dok.html.

[83] Алексей Боярский. Зарплата Большого брата // Коммерсантъ Деньги. — 2011. — URL: http://www.kommersant.ru/doc/1800370.

[84] ИС СОРМ «Январь». — URL: http://www.mfisoft.ru/products/sorm/sorm3/yanvar.

[85] Антонов Игорь. СОРМ на службе государства. — URL: http://www.vr-online.ru/content/sorm-na-sluzhbe-gosudarstva-1163.

[86] Госкомсвязь России. О технических требованиях к системе технических средств для обеспечения функций оперативно-розыскных мероприятий на сетях электросвязи Российской Федерации. — 1999. — URL: http://docs.cntd.ru/document/58859907.

[87] Министерство связи и массовых коммуникаций РФ. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 27.05.2010 N 73 «Об утверждении Требований к сетям электросвязи для проведения оперативно - разыскных мероприятий. Часть II. Требования к сетям передачи данных». — 2010. — URL: http://minsvyaz.ru/ru/doc/?id_4=206.

[88] Dunn S. Microsoft updates Windows without users' consent // Windows Secrets. — 2007. — URL: http://windowssecrets.com/top-story/microsoft-updates-windows-without-users-consent/.

[89] Eckhart T. CarrierIQ // Android Security Test. — 2011. — URL: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/.

[90] Eckhart T. CarrierIQ Part 2 // Android Security Test. — 2011. — URL: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/carrieriq-part2/.

[91] Colvin R. SmartScreen® Application Reputation – Building Reputation. — 2011. — URL: https://blogs.msdn.com/b/ie/archive/2011/03/22/smartscreen-174-application-reputation-building-reputation.aspx.

[92] Thoughts on the Windows SmartScreen scare. — 2012. — URL: http://www.withinwindows.com/2012/08/24/thoughts-on-the-windows-smartscreen-scare/.

[93] Kobeissi N. Windows 8 Tells Microsoft About Everything You Install, Not Very Securely. — 2012. — URL: http://log.nadim.cc/?p=78.

Настольная книга анонима. Зачем нужна анонимность и как ее достичь?

Работа анонимного исследователя

http://anonhandbook.org
http://anonhandbook.i2p
http://oxgzwiiypou6udlp.onion
https://gitorious.org/anonymous-handbook

https://diasp.org/u/anonhandbook
https://twitter.com/AHandbook
http://id3nt.i2p/u/anonhandbook

anonhandbook@tormail.org
https://privacybox.de/anonhandbook.msg

Bitcoin: 1643YL8nKMTuqE5fUPBB1pgrS9sdzchmT3

----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFAIOv0BCACxw3hOXf55/trVGb3x3LFv+4AlbRO8MswriVFF0SpSudZL35Tr
NrNzY30MWVerwvFUo0otT5MGtAva0AGuZngBOElSS+3a9eC8oaAyhcgOmT28lKuZ
4GItB8mcFsjWR3ARhNYg+N/wQXfhjP7xMwNJEhQjoOU+Fy0bGFYjlkX1fsiwjB3y
q/xPkj3iqoeBBPKKbmL6YTNiHzVyF+BmQMvhZzIYh9ll9uP83RgBFe+IaUdugRTr
nYpo3w0fbmhuOIYnybng1X7bEPiJ3xoJKgHYWQmpLGg8TVuivq5zdn4rta9MOlYL
SPw/udkrB5fqBP0H8Jpn+tGA54NAA2uFnaG5ABEBAAG0LUFub255bW91cyBIYW5k
Ym9vayA8YW5vbmhhbmRib29rQHRvcm1haWwubmV0PokBOAQTAQIAIgUCUAg6/QIb
AwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQzcYbHTogZo/IIgf/VeSL1Y4H
HYWMEuHhC1Cq4BO/+slwJA0wBPIjwL7n3lzhqwoEXwts/HAKMntaKXNS3y32YIf5
f4HMA6eJbYs8XcH9sxDuIW7s7Dugg7ifF1MIXlUR2SzkYWSNwR9a141tqGuhxxQv
b95pYoxTeLwuDufNIHD+OPZyxggIHaw+Sxm9LVnVzfGPZxC9ZSLNIVtotcHlREy/
Bk0/FTeaDhZc1OUOa17NQteQUGX8IzyOzVLt9w4RFaLau5y6Z2ETjWp4ZY6wGbrC
fClvu8cx9uZuFpWJmpFladJwVLRWntPQovCvu4TmOZvCX0s6NQ9ncYMD8+CopP+N
owh0bq2amivzorkBDQRQCDr9AQgAq1Gmlzzk321bQUuKa/sD+GzvQ4wuOJY2aFxH
RMMZknhTZUWzdQUT29dTCOW+jiOyGYFDBHhlepRucjuv8wdI0pJy3IzezL4EcAdx
OqmH+NG5zYyzRzsTcMiFY0Dmzui1UN+aEKU5p+GkzqFW249okJUHfkWI4TFfjb0b
MJbI2Ga09/mpz9P32VdZjsw0Kp8HtyqJEnBSFCp06MP4BfugGsMlP066bCu/zdwb
/AnHx9u2SJ03TBjgv05+NxNpHKy0DxBv2ER4ltLWA2opdMiI5uG5TPJrWOvAuuvE
GGqktW5kDvJEmXmxlFhOyznm91IXkNgxsP8smKtrVFfueQcs0QARAQABiQEfBBgB
AgAJBQJQCDr9AhsMAAoJEM3GGx06IGaP+ZUH/Aul5wub0j45HFK9ePEbmxxrtNaH
iBRRJEjo+HtDObiN5ORrNGstzQ+yq58dDIkN+RAxPQEMutLCEjutOxvmEKljnXmo
15oYFORnbC3+ABQZb/Pa6epd/KXbVCZdEr5Z1+ex81Ma1OUZeC2ae1DpJmrECtlB
4GVXU/u9yA/ZKVtv+j4a+HUUsSDj3vmYiiiaXybpxfuVl456GEe4qKYGGcYtBxh1
9iUdjrO/VjvJBswDCT1DTApx/rG+WArP6Bc/yEHGb8KnIFzaVEeH4ovmBXHGkOah
+5zwu/G/GOQVBcASHtgiA4Vxn9jOkWQMEV4wKoAJwzFPMdxmcRohRklyc0Y=
=pphE
-----END PGP PUBLIC KEY BLOCK-----