Веб-серфинг в шапке-невидимке

Liberte Linux: ОС для настоящего анонимуса

В анонимной работе в интернете уже давно заинтересованы не только господа в черных шляпах: нередки случаи, когда обычных пользователей привлекали к ответственности всего лишь за нелестный комментарий или запись в блоге. Спрос рождает предложение, так что сегодня речь пойдет об инструменте достижения анонимности Liberte Linux.

Запили мне Liberte на флешку

Liberte Linux относится к семейству LiveUSB-дистрибутивов, то есть дистрибутивов, которые живут на флешках и прочих съемных носителях. Это весьма удобно в тех случаях, когда требуется быстро развернуть среду для (анонимной) работы на постороннем компьютере, будь то десктоп, ноутбук или нетбук без оптического привода. Среди ключевых особенностей дистрибутива, отличающих его от аналогичных решений, стоит отметить следующие:

- повышенная безопасность системы (так как в основе — Hardened Gentoo Linux);
- простота использования;
- нетребовательность к системным ресурсам;
- весь сетевой трафик идет через Tor;
- возможность общаться с другими анонимусами через скрытые сервисы Tor (опция доступна полностью в версии 2011.1);
- шифрование всей пользовательской информации.

Несмотря на то, что дистрибутив основан на Gentoo, компилировать ядро и софт не потребуется, а если приспичит собрать из исходников, то этот процесс максимально автоматизирован. Образ, который можно записать на флешку или SD-карту, уже содержит в себе все нужное для работы. В состав дистрибутива входит только легковесное ПО, основанное на GTK; минималистичный и быстрый менеджер окон Openbox; модульный X-сервер с TrueType шрифтами. Поддерживаются все unicode-локали и раскладки клавиатур, а также имеется поддержка виртуальной экранной клавиатуры. Все приложения собраны с использованием инструментария сборки проекта Hardened Gentoo, который включает такие патчи, как SSP (защита от переполнения стека и буфера) и ASLR (рандомизация распределения памяти). Весь необходимый для работы софт есть в наличии:

- Midori 0.2.8 — легковесный браузер, основанный на движке WebKit и тулките GTK;
- Claws Mail 3.7.6 — быстрый и легкий клиент электронной почты с графическим интерфейсом, полностью поддерживающий шифрование GnuPG;
- Sakura 2.3.8 — эмулятор терминала, основанный на VTE;
- Audacious 2.4.0 — аудиопроигрыватель с поддержкой всех распространенных форматов (mp3, ogg, flac, ape);
- GNOME Mplayer 0.9.9.2 — стандартный для окружения GNOME проигрыватель видеофайлов, фронтэнд для mplayer на GTK;
- PCManFM 0.9.7 — файловый менеджер с графическим интерфейсом (Midnight Commander также в твоем распоряжении);

Если тебя занесет в страны, выделенные черным — не забудь прихватить с собой флешку с Liberte Linux: в них интернет-цензура наиболее жесткая

• Evince 2.30.3 — просмотрщик документов pdf (с поддержкой DjVu);
• Abiword 2.8.6, Gnumeric 1.10.6 — офисные приложения с поддержкой форматов Microsoft Word и Excel.
Для установки дистрибутива нам потребуется архив с образом и установочными скриптами (можно скачать с официального сайта dee.su/liberte, либо взять на прилагаемом к журналу диске), а также флешка емкостью не менее 256 Мб. Дистрибутив нетребователен не только к свободному месту, но и к другим аппаратным частям. Заявляется, что он будет работать на компах с оперативной памятью 128 Мб и процессорами вплоть до Pentium Pro.

Рассмотрим установку из Linux:
1. Создаем точку монтирования для флешки: `mkdir /media/usbstick`.
2. Монтируем флешку: `mount /dev/sdb1 /media/usbstick`.
3. Распаковываем архив в корневую директорию флешки: `unzip liberte-2010.1.zip -d /media/usbstick`.
4. Копируем установочный скрипт на локальный диск: `cp /media/usbstick/liberte/setup.sh /tmp/setup.sh`.
5. Делаем его исполняемым: `chmod +x /tmp/setup.sh`.
6. Размонтируем флешку: `umount /dev/sdb1`.
7. Запускаем скрипт установки: `/tmp/setup.sh`

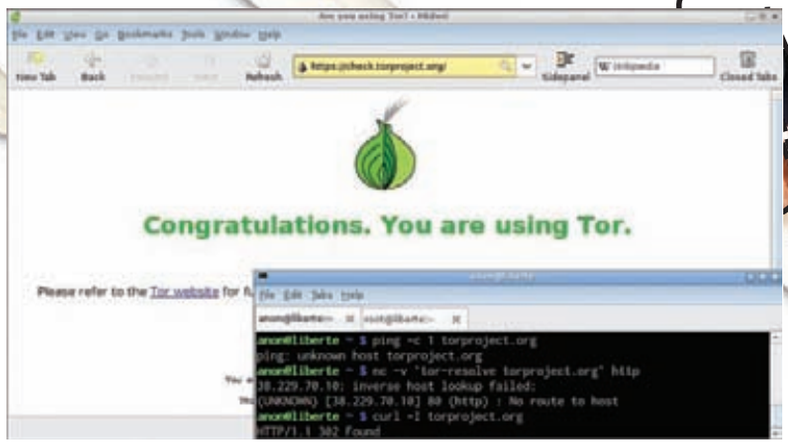
Также для установки понадобится утилита syslinux версии 4.02, которая в большинстве случаев устанавливается через штатный менеджер пакетов твоего дистрибутива. Я использую Arch Linux, где на момент написания статьи была доступна syslinux 4.03 — из-за этого пришлось немного отредактировать первые строчки в скрипте:

```
$ head -n5 setup.sh
#!/bin/sh -e
# Установленная версия syslinux
sysver=4.03
# Путь к mbr.bin (можно узнать командой «find / -name mbr.bin»)
sysmbr=/usr/lib/syslinux/mbr.bin
```

Установка из Windows более прозаична, нужно лишь распаковать содержимое архива на флешку и запустить скрипт setup.bat с правами администратора. Так как утилита syslinux идет внутри архива, то ничего дополнительно устанавливать не нужно.

It's easy to use!

Теперь, указав в BIOS'е приоритетную загрузку со съемных носителей, можно увидеть окно загрузчика Liberte, где требуется выбрать один из двух режимов загрузки — графический или консольный. Графический используется в большинстве случаев, а консольный полезен тем, что через него можно получить рутовый доступ, переключившись на второй виртуальный терминал (Alt+F2). Правда, следует учесть, что после двух минут бездействия рутовая консоль делает автологаут. Там же можно разблокировать учетную запись рута командой «usermod -U root» и изменить пароль по умолчанию с помощью утилиты passwd. Воспользовавшись sudo, мы ограничим свои действия всего лишь несколькими командами, поэтому запуск под рутом иногда может быть вполне оправдан.



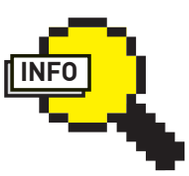
Строгие правила брандмауэра в действии

Liberte Linux не только дает возможность анонимного доступа к Сети, но и хранит все пользовательские данные в виртуальном зашифрованном разделе OTFE с применением стойкого алгоритма шифрования AES-256 в режиме XTS. Этот раздел в виде файла находится на флешке и имеет динамический размер, который можно изменять командой otfe-resize. Настройки параметров зашифрованного раздела могут гибко изменяться под нужды пользователя с помощью конфига, представленного ниже.

```
$ cat /etc/conf.d/liberte
# Параметры зашифрованного хранилища
OTFEFILE=/otfe/liberte.vol
OTFELABEL="Liberte OTFE"

# Размер хранилища, указывается как часть от общего свободного места на носителе (A/B)
OTFESIZE=1/4

# Используемые алгоритм и режим шифрования, размер ключа шифрования и алгоритм хеширования
OTFECIPHER=aes-xts-plain
OTFEKEYSIZE=256
OTFEHASH=sha256

# Имя раздела LVM
# (используется утилитой otfe-resize)
OTFEVOLUME=otfe
```

В случае обострения параноидальных симптомов можно зашифровывать отдельные файлы с помощью GnuPG или GPA, которые входят в состав дистрибутива.
Во время первой загрузки нас попросят указать пароль для зашифрованного виртуального раздела OTFE. При каждой последующей загрузке его нужно будет вспоминать и вводить, иначе система не загрузится.
Для доступа в сеть используется браузер Midori с уже

dvd
На диске, прилагаемом к журналу, лежит готовый образ Liberte Linux и установочные скрипты под Linux и Windows.



info
• В разделе Install на сайте проекта Liberte Linux можно найти ссылку на торрент с образом VirtualBox дистрибутива.

• Некоторые старые компьютеры поддерживают загрузку только с FAT(16) разделов USB-устройств.

Основное splash-лого дистрибутива как бы намекает

настроенным Tor. Примечательно, что весь разрешенный трафик идет через Tor, что исключает непредвиденные утечки информации (например, открытые запросы к DNS-серверу, несмотря на прокси, или запросы к DHCP-серверу, содержащие реальное имя хоста), а остальной трафик просто блокируется брандмауэром. В этом можно убедиться, набрав «iptables -L» под рутом. Пакетный фильтр по умолчанию настроен на блокирование всех входящих и исходящих пакетов за исключением трафика DHCP, DNS, NTP и Tor, причем передаваемые по DHCP параметры максимально урезаны, а передача имени хоста, ARP и IPv4LL (IPv4 Link-Local Addresses) — блокируется.
Для обеспечения приватности в Wi-Fi сетях MAC-адрес беспроводного интерфейса генерируется случайным образом с помощью утилиты mac-randomize. Так как для регистрации на некоторых точках доступа необходим прямой вход браузером, в Liberte предусмотрена возможность отдельного запуска браузера от обособленного пользователя, который имеет доступ только к DNS и портам типовых сервисов web-регистрации. Стоит отметить интересный момент при работе с дистрибутивом: если внезапно наступил шухер, то можно просто выдернуть флешку из порта (и съесть), а компьютер через несколько секунд выключится сам.

Сборка из исходников

Liberte можно легко собрать из исходников. Для этого подойдет любой Linux дистрибутив, необязательно быть пользователем Gentoo. Во время сборки оказалось, что у меня не установлен пакет rsync, поэтому пришлось доустановить его и заново запустить процесс. Для успешной сборки также необходим пакет SquashFS Tools 4.1. Вся процедура занимает несколько часов на более-менее современном процессоре и требует около 4 Гб свободного места на харде.

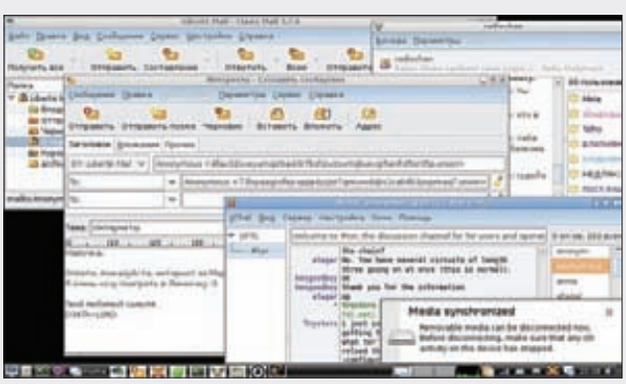
Privatix Live-System

Разработка суровых немецких анонимусов. Эта система основана на Debian и может быть установлена как на CD-, так и на USB-устройства. Причем установка на USB происходит только из загруженного LiveCD. В дистрибутиве присутствует удобная графическая утилита для шифрования съемных носителей — UsbCryptFormat, а также утилита для простого резервного копирования зашифрованных данных CryptBackup в несколько кликов. Серфинг веба здесь происходит через Firefox и Torbutton. Система весьма требовательна к свободному месту — для установки требуется как минимум 3 Гб.

Liberte Linux

Простые американцы чтут Вторую поправку к Конституции, согласно которой самый обычный гражданин может противостоять нагло попирающему его права государству, зажав купленную в кредит автоматическую винтовку M-16 в одной руке и гамбургер в другой. В мире сетей и двоичных кодов неравная расстановка сил в этой милой и наивной фантазии внезапно меняется — даже если вездесущему оку электронной разведки противостоит простой анонимус в тапочках, сжимающий флешку с современными средствами шифрования в одной ладошке и журнал «Хакер» в другой. Именно поэтому Liberte Linux ставит своей целью дать юзерам возможность скрыто и безопасно общаться между собой в любое время и в любом месте, где есть компьютер с выходом в Сеть. Данная функциональность, являющаяся основной для дистрибутива, реализована в версии 2011.1, которая, видимо, выйдет к моменту публикации статьи.
На скриншоте видно, что обмен сообщениями в новой версии происходит через привычный интерфейс программы для отправки почты — в данном случае, Claws-Mail. Для анонимусов, предпочитающих удобство общения потаканию паранойе, в релиз включены также IRC-клиент XChat и IM-клиент Pidgin — с настройками, ориентированными на приватность общения. Также включены простые средства создания mp4-видеороликов и аудиоклипов в формате Speex с помощью веб-камеры и микрофона.
Конечно, с визуальной точки зрения Liberte уступает более наворочен-ным дистрибутивам, в которых можно включать такие свистелки, как Compiz. Но главный упор при разработке Liberte делается на качество и надежность работы, а также нетребовательность дистрибутива к железу. Анонимус, знай: о тебе заботятся, для тебя делают самое лучшее, бесплатно и без СМС.

Maxim Kammerer <mk@dee.su>, автор дистрибутива.

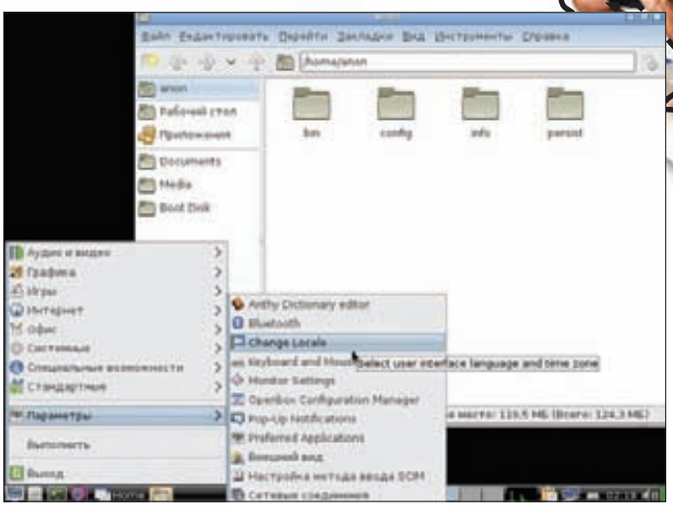


Liberte Linux 2011.1

DemocraKey LiveCD

Дистрибутив был разработан в ответ на ужесточение цензуры в интернете правительствами Китая и США. Весьма интересный проект, который нацелен не столько на анонимность, сколько на сохранность персональных и финансовых данных. Автор этого проекта даже предлагает приобрести уже готовую флешку с этим дистрибутивом и радоваться жизни, а также намекает на то, чтобы все заинтересованные быстрее покупали его изделие, пока оно еще легально на территории США. Кроме всего прочего, в состав дистрибутива входит антивирусный сканер, который может помочь излечить инфицированную винду, расположенную по соседству. Среди стандартного арсенала анонимуса: анонимный веб-серфинг через Tor, шифрование почты и трафика клиента мгновенных сообщений (Pigdin + OTR).

Поздравляем! Твой браузер уже сконфигурирован



Локаль дистрибутива легко поддается изменению (по умолчанию — английская)

Процесс сборки выглядит следующим образом:
1. Скачиваем исходники (рекомендуется скачивать из svn, тогда вероятность возникновения проблем при сборке меньше):

```
svn co https://liberte.svn.sourceforge.net/svnroot/liberte/trunk/liberte liberte
```

2. Запускаем сборку в папке /tmp/livecd:

```
liberte-2010.1-src/build /tmp/livecd
```

Если по какой-то причине невозможно скачать исходники из svn, то их можно взять с сервера sourceforge.net:

```
$ wget https://downloads.sourceforge.net/project/liberte/2010.1/liberte-2010.1-src.tar.bz2
$ tar xjf liberte-2010.1-src.tar.bz2
$ mv liberte-201X.Y-src liberte
```

В скрипте build поддерживается параметр fresh, который используется для новой сборки дистрибутива.
На основе исходников Liberte Linux можно собрать собственный LiveUSB-дистрибутив. Список пакетов находится в файле src/var/lib/portage/world — приверженцы более «человечных» окружений рабочего стола (или, наоборот, более суровых тайловых менеджеров окон) могут установить их туда, а также изменить набор интересующего софта. Потребуется просто добавить в конфиг строчку с нужным названием. Точное название приложений можно подсмотреть в дереве портежей по адресу gentoo-portage.com/browse. Все пользовательские настройки находятся в /home/anon/ и, чтобы лишний раз не мучиться с их допиливанием, можно просто скопировать нужные конфигурационные файлы из своей домашней директории (если, конечно, ты являешься счастливым пользователем линукса). Системные настройки, как и полагается, находятся в /etc.

The (Amnesic) Incognito Live System

Этот проект стал преемником дистрибутива Incognito LiveCD после того, как автор объявил об окончании разработки. Но, в отличие от Incognito LiveCD, этот дистрибутив может быть записан как на CD-диск, так и на флешку. Создатели гарантируют, что, во-первых, все соединения с Сетью принудительно происходят через Tor, а во-вторых, при работе не остается никаких следов на локальных носителях.
В качестве окружения рабочего стола используется GNOME, а в комплекте идет несметное количество GTK-программ (Firefox, OpenOffice, Pigdin с плагином для безопасной передачи сообщений OTR и так далее) — всего около 2 Гб софта! Благодаря тому, что система распространяется в том числе и как образ iso, ее легко можно запустить на виртуальной машине типа VirtualBox.

Есть куда стремиться

Tor позволяет клиентам и серверам предоставлять скрытые сервисы. То есть можно запустить веб-сервер, SSH-сервер и так далее, не раскрывая свой IP-адрес пользователям. И, поскольку при этом не используется никакой публичный адрес, можно запустить скрытый сервис, находясь за файерволом. По задумке автора, в процессе первой загрузки на основе слепка сертификата и сервисного ключа сети Tor будет генерироваться уникальный e-mail пользователя, который в последующем можно будет использовать для связи с другими пользователями дистрибутива Liberte через скрытые сервисы Tor. В текущем релизе (2010.1 на момент написания статьи) данная возможность пока не доведена до кондиции, хотя она заявлена как ключевая. В Liberte Linux пока нет поддержки набирающей популярность сети I2P (также известной под названием «Проект Невидимый Интернет») — анонимной, самоорганизующейся распределенной сети, которая использует модифицированный DHT Kademlia, но отличается тем, что хранит в себе хешированные адреса узлов сети, зашифрованные AES IP-адреса, а также публичные ключи шифрования, причем соединения по Network database тоже зашифрованы. Автор дистрибутива открыт для новых идей. Если у тебя есть предложения по развитию проекта, то их можно отсылать на адрес mk@dee.su.

Заключение

Тенденция к ужесточению интернет-цензуры в ближайшие годы будет сохраняться, поэтому готовым к этому надо быть уже сейчас. Несмотря на мое неприятие политики MS в целом, с одним высказыванием Билла Гейтса все же хочется согласиться: свобода слова в Сети рано или поздно победит...

warning

Не стоит забывать, что анонимность, как и все в нашем мире, не бывает абсолютной. Поэтому ответственность за совершенные действия рано или поздно может придти!

links

- dee.su/liberte — сайт проекта Liberte Linux;
- amnesia.boum.org — сайт проекта T(A)ILS;
- mandalka.name/privatix — сайт проекта Privatix LiveSystem;
- sourceforge.net/projects/democrakey — страничка проекта DemokraKey;
- i2p2.de/intro_ru.html — сайт проекта «Невидимый Интернет»;