Операционных систем для достижения анонимности и безопасности пруд пруди, но действительно стоящих, не так много. Предлагаю разобраться в вопросе выбора лучшей системы готовой решить любые задачи. Поехали!



**Tails OS** — дистрибутив Linux на основе Debian, создан для обеспечения приватности и анонимности. Является продолжением развития ОС Incognito. Все исходящие соединения заворачиваются в сеть Tor, а все неанонимные блокируются. Система предназначена для загрузки с \*LiveCD/LiveUSB и не оставляет следов на машине, на которой использовалась. Проект Tor является главным спонсором TAILS. Операционная система рекомендована к использованию «Фондом свободной прессы», а также использовалась Эдвардом Сноуденом для разоблачения «PRISM». (Раньше данный дистрибутив назывался Amnesia)(wiki).

Для того чтобы разобрать плюсы и минусы Tails, необходимо иметь строгое понятие для каких целей данная ОС и как она должна использоваться.

Tails — это операционная система с быстрым стартом, то есть после создания флешки с системой для доступа к сети интернет потребуется 1-2 минуты на хорошем железе, но ждать большого функционала от нее не стоит. Tails позволяет быстро подключиться к сети Tor, связаться со второй стороной по защищенному каналу, генерировать и сохранять пароли, очистить файлы от metadata, и если журналист — то написать статью и отправить в редакцию.

В основе Tails заложена задача, обеспечить анонимностью и безопасностью пользователя в сети, при этом максимально сохраняя удобство и простоту использования ОС, и как раз таки это у нее получается неплохо. Вся система работает в Live режиме и выгружается в оперативную память, Tails не выгружается на ssd или hdd, это сделано дабы после завершения сессии, нельзя было определить, чем пользователь занимался на компьютере, даже получив доступ к всему устройству.
Данная ОС категорически не рассматривается под установку на жесткий диск в качестве постоянной операционной системы. После выключения или перезагрузки системы все скачанные файлы, история браузера и т.д. — удаляются.

Можно создать Persistent зашифрованный раздел и хранить на нем пароли и файлы различного типа, но эти файлы должны быть с небольшой степенью конфиденциальности.

Для запуска Tails потребуется устройство с не менее 1GB RAM и допотопным процессором. (Оптимальные характеристики устройства для Tails: 8GB RAM и современный 2-х ядерный процессор)

Что касается установки сторонних программ — то это не конёк данной ОС.

Установка приложений в Tails не самое приятное занятие, часто возникают непредвиденные ошибки, даже если все сделано правильно и по инструкции, может быть такое, что после нескольких перезагрузок Ваш установленный софт просто исчезнет. В некоторых случаях, если нужна постоянная робота со сторонним софтом, лучший вариант — это создать сборку под свои нужды.

Задача Tails — не оставлять следов, по этому что-то больше чем доступ к сети Tor и простое хранение файлов, может стать проблемой. Лучше всего использовать Tails для быстрого доступа к сети и некоторым валютным операциям.

Хороший вариант применения Tails — доступ к удаленному web-ресурсу, работа с документами, связь по зашифрованному каналу, работа с криптовалютой.

К примеру, создание криптовалютного кошелька через Tails с сохранением всех данных кошелька в Persistent разделе неплох, в случае если кошелек с небольшой суммой (до 1000$) и часто задействуется. Собственно при необходимости быстро перекинуть валюту — достаточно всунуть флешку в любое устройство с интернетом и через 5 минут творить дела.

На Persistent разделе хранить данные криптовалютного кошелька с парой сотен тысяч долларов не стоит, документы с высшим приоритетом конфиденциальности тоже.

Говорить что Tails подходит как повседневная ОС под все задачи — не стоит.

Теперь плюсы и минусы!

Плюсы:

* быстрый доступ к сети (Tor, мессенджеры, онлайн крипто-кошельки)
* встроенный софт для очистки metadata
* встроенные мессенджеры
* генерирование/хранение паролей
* работает на слабом железе

Минусы:

* непростая установка системы (иногда необходимо 2 флешки)
* проблемная установка стороннего софта
* не подходит как постоянная система
* не подходит для хранения файлов с высшим приоритетом конфиденциальности
* не подходит для построения сильнейшем системы анонимности/безопасности

Tails хорошая система, но со своими минусами, она попросту заточена под конкретные задачи которые не всегда подойдут. Tails в большей мере решает вопрос анонимности, но не безопасности. Безусловно это анонимная и неплохая безопасная система, но есть дистрибутивы куда прогрессивней, Tails хорошо известна благодаря Сноудену и прорекламирована во многих кругах благодаря довольно быстрому освоению и своей простоте.



**Whonix** — дистрибутив Linux на основе Debian, ранее известный как TorBOX. Предназначен для обеспечения анонимности средствами VirtualBox и Tor. Его особенностью является то, что ни вредоносные программы, ни компрометация учётной записи суперпользователя не могут привести к утечкам IP-адреса и DNS. Всё программное обеспечение идущее в комплекте с системой предварительно настроено с учётом требований безопасности.

Система Whonix состоит из двух виртуальных машин, Whonix-Gateway и Whonix-Workstation, соединённых через изолированную сеть, где первая работает исключительно через Tor и выступает в качестве шлюза в сеть, и вторая, находится в полностью изолированной сети.
В данной реализации все сетевые соединения возможны только через Tor. Единственный доступ к сети для рабочей станции – это шлюз. Единственный путь трафика сети из шлюза и обратно – это сеть Tor. Весь трафик, всех приложений и процессов будет идти через Tor.

Приложения не могут получить доступ к интернету в обход Tor, они могут увидеть только локальный IP-адрес, для них имя пользователя будет просто «User», информация об устройстве будет без изменений. По временной зоне тоже отследить нельзя, часы настроены на UTC, а для синхронизации времени используются \*Timestamp HTTP-заголовков, отдаваемых случайно выбранным веб-серверам.

\*Timestamp — это последовательность символов или закодированной информации, показывающей, когда произошло определённое событие. Обычно показывает дату и время (иногда с точностью до долей секунд).

Главный компонент для построения анонимного/защищенного соединения – это шлюз, который можно использовать через любой дистрибутив в VirtualBox и получить почти такой же уровень защиты от отслеживания, но делать этого не стоит, безопасность будет не максимальной.

Хорошие плюсы системы — реализация разных связок Tor + VPN. Можно настроить систему так, что сначала весь трафик идет через VPN, после через Tor и снова через VPN. Разные связки дают хорошую анонимность/безопасность.

Whonix — это система с возможностью модификации и детальной настройкой, что иногда нельзя сделать в Tails. В данной ОС присутствует множество программ и настроек позволяющих построить систему анонимности/безопасности, убирать следы использования файлов, использовать мессенджеры, работать с разными типами файлов и т.д.

Whonix определенно хорошая система для анонимного/защищенного доступа к сети, но использовать ее на постоянно основе будет довольно проблематично. Так как Whonix построена на виртуализации — это влечет некоторые трудности.

К примеру трудности с работой внешних носителей. Если необходимо подключить флешку — то сначала она пройдет через основную ОС, к примеру Windows, после пройдет через VirtualBox и дойдет к Whonix системе, а это уже не безопасно.

Прийдется быть прикованным к устройству на котором установлена система Whonix, нельзя просто вставить флешку и получить доступ в любой момент, как в случае с Tails.

Плюсы:

* высокая степень анонимности/безопасности
* большое количество софта для работы
* возможность детальной настройки

Минусы:

* не портативна (привязанность к устройству)
* требует хорошее железо (процессор, видеокарта и оперативная память не ниже среднего)
* привязанность к VirtualBox, что означает большие риски в случае взлома ОС на которой установлен VirtualBox
* не оперативна, требует больше времени для доступа к сети по сравнению с другими ОС (необходимо запустить VirtualBox, Whonix-Gateway, Whonix-Workstation)

Whonix лучше всего использовать как запасную систему ибо она не портативна, а портативность это один из самых важных критериев. Также она привязана к VirtualBox, и так как это не Live-система, то обнаружить наличие Whonix будет довольно просто если не прибегать к методам криптографии.

Whonix должна использоваться только в крайних случаях. Акцент на ней сделан потому, что это гибкая система, она входит в ТОП самых безопасных систем хоть и со своими минусами, но обойти ее стороной будет крайне не верно.



**Linux Kodachi** — это операционная система, которая базируется на Debian, предоставляет надежную, контр криминалистическую анонимную/безопасную операционную систему, учитывающую все особенности и тонкости процесса анонимности и безопасности.

Задача Kodachi — обеспечение максимально анонимного и безопасного доступа к сети и защита самой системы. В Kodachi весь трафик принудительно проходит через VPN, затем через сеть Tor с DNS шифрованием. (VPN уже преднастроен и к тому же он бесплатный).

Kodachi позиционируется как anti-forensic-разработка, затрудняющая криминалистический анализ накопителей и оперативной памяти. Kodachi более продумана чем Tails.

В качестве среды рабочего стола для Kodachi была выбрана XFCE, дизайн системы сильно схож на MacOS. Необходимые параметры нагрузки на систему, состояния сетей и т.д. выводятся в режиме реального времени и отображаются прямо на рабочем столе, что в первую очередь позволяет мониторить используемые ресурсы системы и отслеживать работу сети Tor и VPN.

В Kodachi интегрирована поддержка DNScrypt — это протокол и одноименная утилита, шифрующая запросы к серверам \*OpenDNS методами эллиптической криптографии. Она устраняет целый ряд типичных проблем, вроде \*DNS Leak и оставления следов работы в сети на серверах провайдера.

**\*OpenDNS** — интернет-служба, предоставляющая общедоступные DNS-серверы. Имеет платный и бесплатный режим, может исправлять опечатки в набираемых адресах, фильтровать фишинговые сайты в случае набора неправильных запросов, может предлагать страницу с поиском и рекламой.

**\*DNS Leak** — это утечка IP ближайшего к системе DNS-сервера, которая может происходить при резолвинге. DNS-запросы могут идти в обход Proxy/VPN/TOR-подключения, то есть напрямую к DNS-серверу интернет-провайдера, что приведет к раскрытию реального местонахождения. Утечка DNS может происходить через браузер или дополнения в нем (Flash, Java, WebRTC, Silverlight).

Если потребуется крыть IP-адрес в Р2Р-сетях можно использовать «PeerGuardian», если необходимо поработать с подозрительными процессами, то их можно легко изолировать при помощи встроенной песочницы «Firejail». Приятной опцией в данной ОС  является возможность быстро изменять выходные узлы с опцией выбора конкретной страны используя «Multi Tor».

В общем говоря, Kodachi имеет приличное количество предустановленного софта для решения любых задач, например для шифрования информации (TrueCrypt, VeraCrypt), для передачи конфиденциальных сообщений (GnuPG, Enigmail, Seahorse, GNU Privacy Guard Assistant), для заметания следов (MAT, Nepomuk Cleaner, Nautilus-wipe, BleachBit).

К тому же в Kodachi есть собственный браузер основанный на Tor Browser, в который встроили наилучшее и вырезали проблемные модули.

В общем говоря, Kodachi идеальный инструмент почти для всего. Сразу из коробки Мы получаем огромное количество программ для безопасного/анонимного доступа к сети, связи по зашифрованным каналам через разные программы, софт для заметания следов, тотального шифрования всего потенциально шифруемого и т.д. (Это только малая часть преимуществ Kodachi)

Kodachi сильно сбалансированная система, это мощный инструмент для постройки системы анонимности и безопасности во всех пониманиях. Эту ОС лучше всего использовать в связке с зашифрованными носителями на которых будет храниться информация с высшим приоритетом конфиденциальности.

Именно Kodachi является лучшей системой на данный момент, она позволяет решать любые задачи.

Плюсы:

* быстрый старт (то есть быстрый доступ к сети как у Tails)
* большое количество предустановленных программ
* сильная система анонимности/безопасноти
* не сильно требовательна к железу

Как таковых минусов, в системе нет, но они могут проявиться в случае узконаправленных задач, но это причастно любой системе.

Есть еще неплохие ОС такие как Subgraph и Qubes.

Qubes OS использует интересный принцип запуска приложения, каждое из них запускается в отдельной виртуальной машине, разделенных на классы в зависимости от уровня важности для ОС. Браузер запускается в одной виртуалке, мессенджер – в другой машине, а для пользователя обе программы будто запущены на одном рабочем пространстве. Изолирование приложение означает, что если будет загружено вредоносное ПО на рабочий компьютер, то личные файлы не будут скомпрометированы. Но Qubes OS работает только после установки на внутренний накопитель, Live-режима у нее нет.

Ключевая идея Subgraph OS — запуск пользовательских приложений в изолированных песочницах. Для этого задействована подсистема «Oz», состоящая из демона(системного сервиса), получающего запросы на создание sandbox’ов, X-сервера Xpra и набора специальных утилит.

Subgraph OS слишком сырая система, поэтому для загрузки доступна только alpha-версия.
Subgraph и Qubes неплохие, но не на столько, что бы их ставить в лидеры. Subgraph OS слишком сырая, Qubes слишком заморочливая в плане настройки.

Итого, победителем становится Kodachi!

Отличная сбалансированная система с большим функционалом, всем необходимым софтом для решения любых задач, довольно гибка в настройке + из коробки преднастроен бесплатный VPN.