

Топ-15 лучших дистрибутивов Linux, ориентированных на безопасность



Топ-15 лучших дистрибутивов Linux, ориентированных на безопасность

Быть анонимным в Интернете — это не то же самое, что безопасное использование Интернета, однако, оба этих свойства предполагают сохранение конфиденциальности себя и своих данных вдали от посторонних глаз организаций, которые в противном случае могут воспользоваться уязвимостями системы, чтобы нанести ущерб целевым сторонам.

Существует также риск слежки со стороны **NSA** (Агентство национальной безопасности) и ряда других организаций высшего уровня, и поэтому хорошо, что разработчики взяли на себя задачу создавать специализированные дистрибутивы, содержащие множество инструментов, позволяющих пользователям работать в режиме онлайн и одновременно сохранять конфиденциальность.

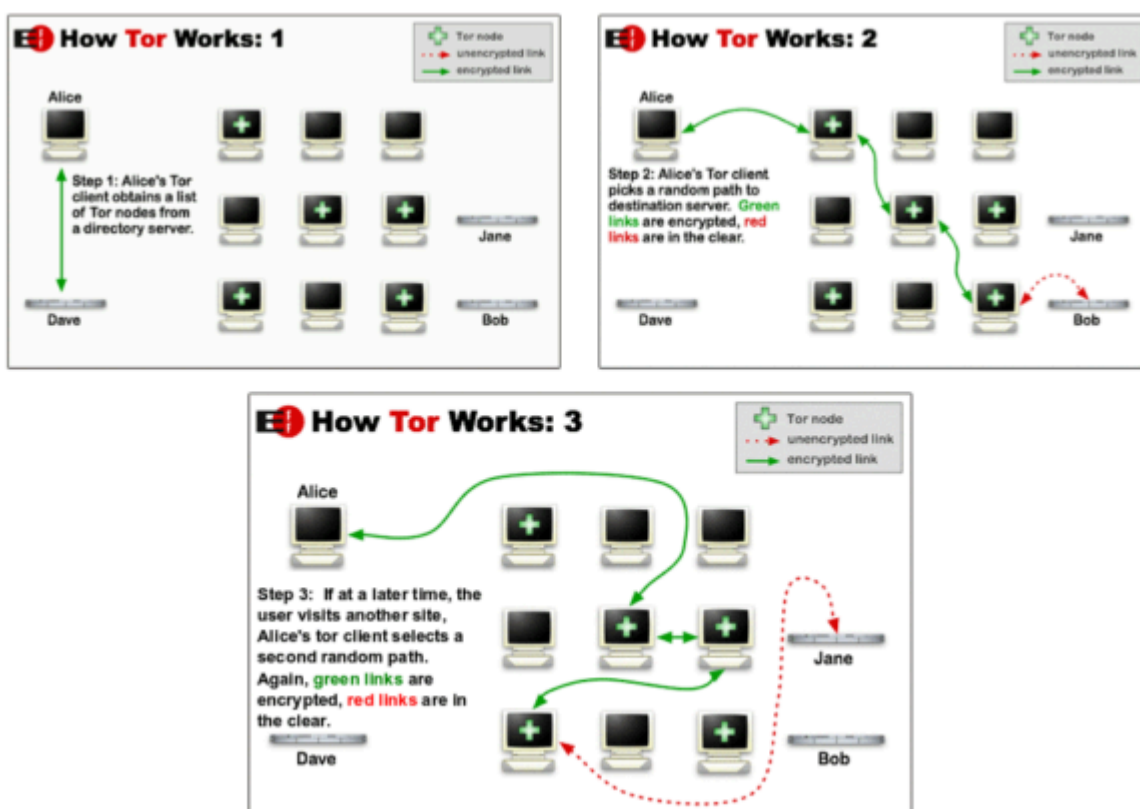
Поскольку эти дистрибутивы Linux, ориентированные на конфиденциальность, нацелены на нишу в сообществе Linux, многие из них достаточно надежны, чтобы их можно было использовать для вычислений общего назначения, и многие другие можно настроить для поддержки требований практически любой конкретной пользовательской базы.

Общим фактором почти во всех дистрибутивах Linux, ориентированных на конфиденциальность, являются их связь с Tor. Многие из них поставляются со встроенной сетевой службой Tor для обеспечения анонимности, что, в свою очередь, предоставляет пользователям среду, в которой они могут безопасно жить без отслеживания данных. Это и есть основное отличие от большинства провайдеров VPN, которые по-прежнему будут регистрировать ваш реальный IP-адрес, в то же

время имея возможность видеть любые данные, которые вы можете передавать на выходе из серверов VPN.

Тем не менее, VPN по-прежнему имеет огромное количество преимуществ по сравнению с данными дистрибутивами, что делает его несколько лучше в некоторых моментах (в зависимости от вашего случая использования). Например, когда вы учитываете общий доступ к файлам P2P и общую скорость Интернета, VPN выигрывает здесь (подробнее об этом позже).

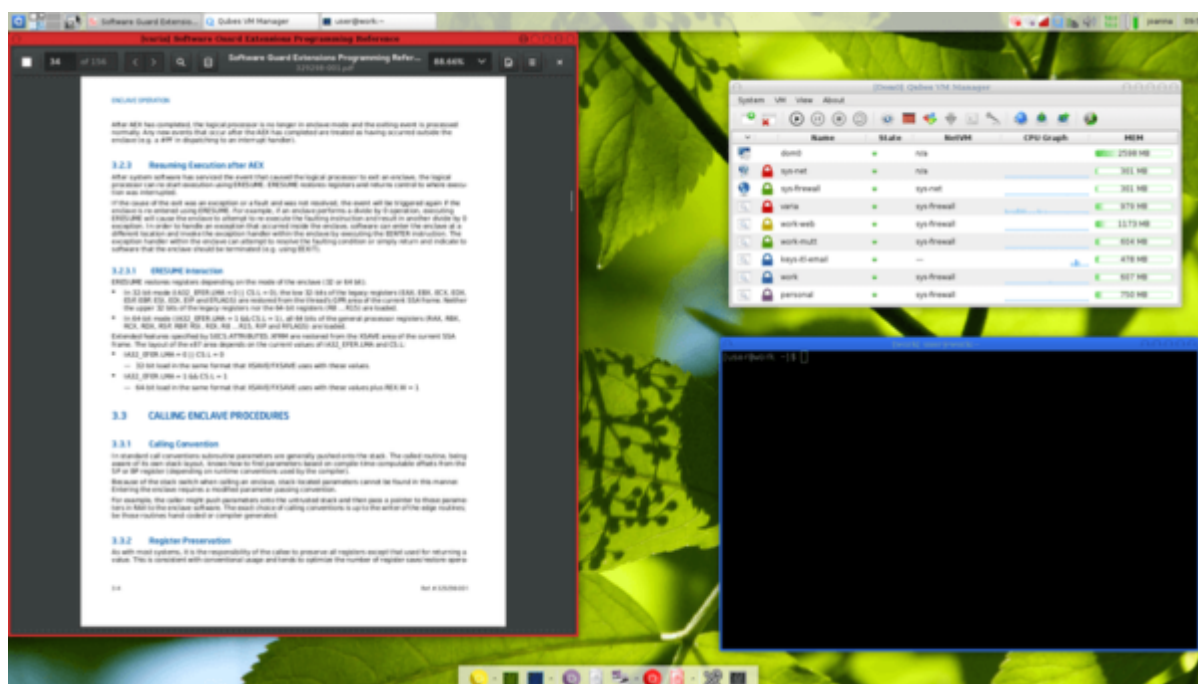
Сеть Тор защищает весь сетевой трафик, проходящий через нее, путем отсылки данных от нескольких случайных узлов, чтобы снизить вероятность отслеживания трафика. Напомним, что во время этого процесса каждый фрагмент данных повторно шифруется несколько раз, поскольку он проходит через случайно выбранные узлы, прежде чем, наконец, достигнет своего пункта назначения, как показано на изображениях ниже.



Теперь, когда у вас есть общее представление о том, как Тор работает на благо своих пользователей, вот наш список 15 лучших дистрибутивов Linux, ориентированных на безопасность.

1. Qubes OS

Qubes OS — это ориентированный на безопасность дистрибутив на основе Fedora, который обеспечивает безопасность путем реализации безопасности путем разделения на части. Это происходит путем запуска каждого экземпляра запущенных программ в изолированной виртуальной среде и последующего удаления всех его данных при закрытии программы.



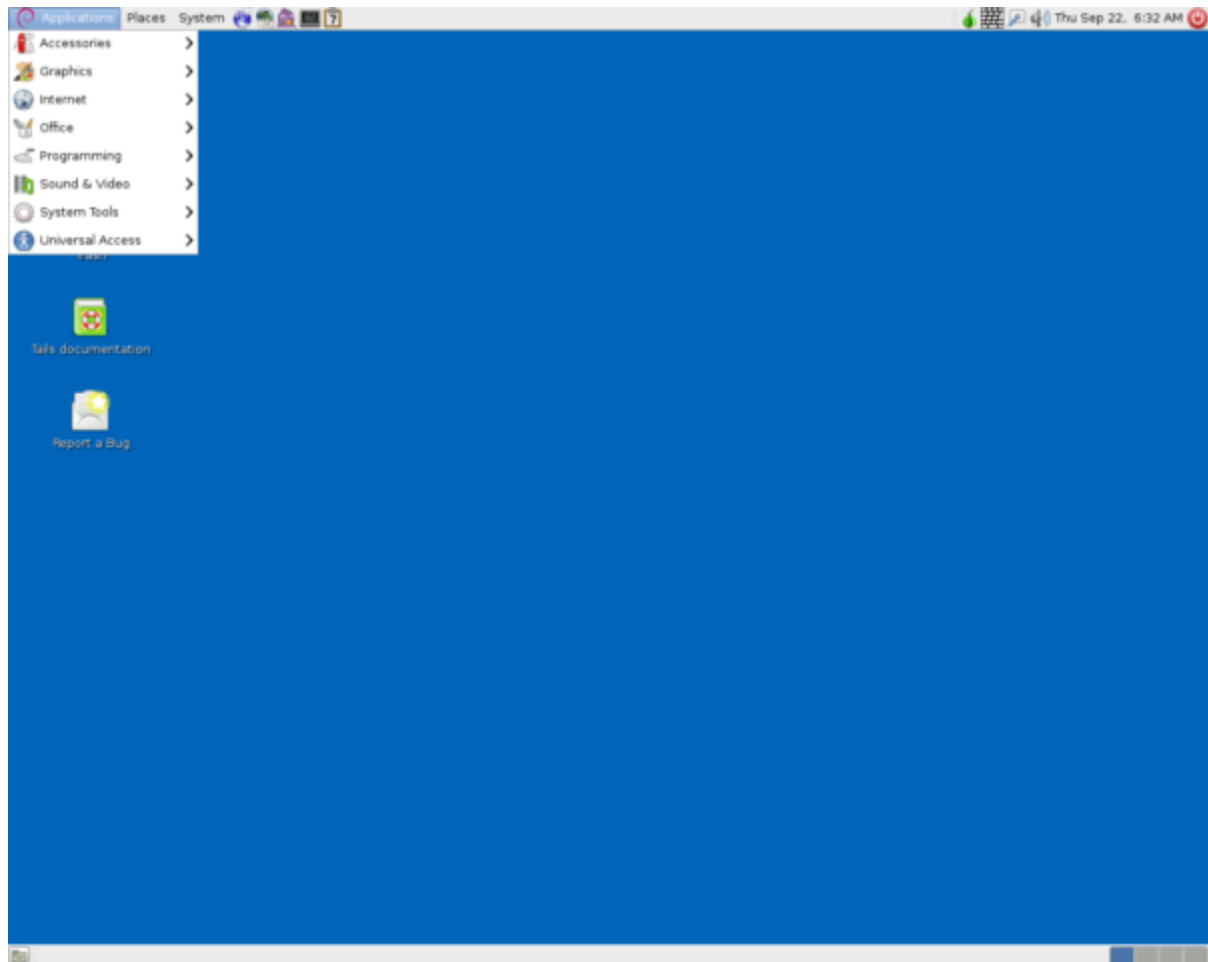
OS Qubes использует диспетчер пакетов RPM и может работать с любой рабочей средой по вашему выбору, не требуя больших ресурсов компьютера. Цитируемый Эдвардом Сноуденом как «лучшая операционная система, доступная на сегодняшний день», это, безусловно, хороший выбор, если вы хотите убедиться, что ваши личные данные принадлежат вам самим, будь то онлайн или офлайн.

[Скачать Qubes OS](#)

2. TAILS: The Amnesiac Incognito Live System

Tails — это ориентированный на безопасность дистрибутив Debian, разработанный для защиты личности пользователей в Интернете и обеспечения их анонимности. Его название означает «Amnesiac Incognito Live System» и построено так, чтобы

форсировать весь входящий и исходящий трафик через сеть Tor, блокируя все отслеживаемые соединения.



Он использует **Gnome** в качестве среды рабочего стола по умолчанию и, будучи Live DVD/USB, может быть удобно запущен с DVD/USB носителя, тогда он сохраняет все свои данные в оперативной памяти. Он поставляется с инструментами с открытым исходным кодом, которые специально предназначены для особых целей конфиденциальности, таких как подмена MAC-адреса и маскировка окон.

[Скачать ОС Tails](#)

,

3. BlackArch Linux

BlackArch Linux — это легкий дистрибутив на основе Arch Linux, предназначенный для тестировщиков, экспертов по безопасности и исследователей безопасности. Он предлагает пользователям все функции, которые может предложить Arch Linux, в сочетании с кучей инструментов кибербезопасности, насчитывающих 2000+, которые можно установить как по отдельности, так и в группах.



По сравнению с другими дистрибутивами в этом списке, BlackArch Linux — относительно новый проект, но он может выделиться как надежная ОС в сообществе экспертов по безопасности. Он поставляется с возможностью выбора пользователем любой из этих сред рабочего стола: **Awesome**, **Blackbox**, **Fluxbox** или **spectrwm**, и, как и ожидалось, он доступен в виде Live образа DVD и может быть запущен с помощью DVD/USB.

[Скачать BlackArch Linux](#)

4. Кали Линукс

Kali Linux (ранее BackTrack) — это бесплатный расширенный дистрибутив Linux для тестирования, разработанный для экспертов по безопасности, этического взлома, оценки сетевой безопасности и цифровой криминалистики.



Он сконструирован для бесперебойной работы как на 32-, так и на 64-битных архитектурах, и сразу же поставляется с набором инструментов для тестирования на проникновение, которые заботятся о безопасности.

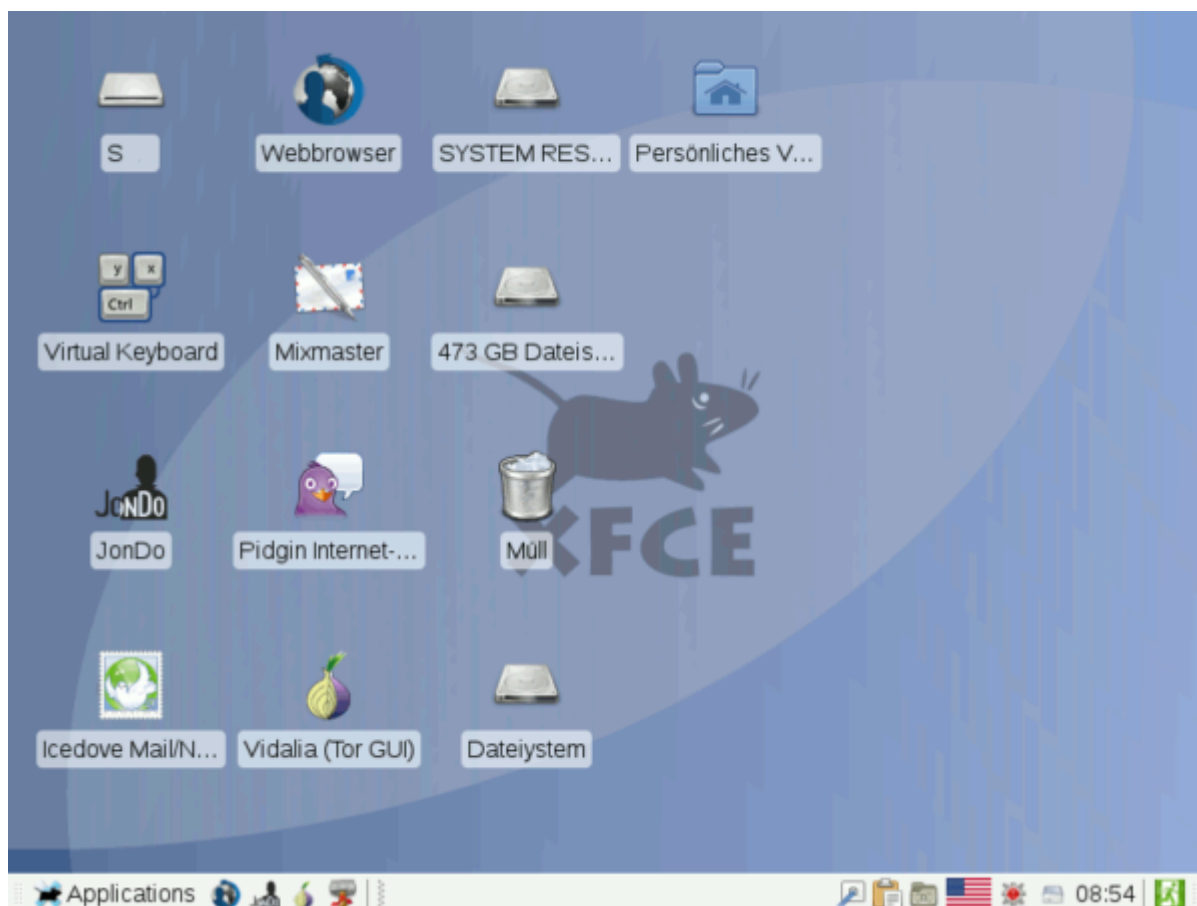
О Kali Linux можно сказать гораздо больше (как и в случае с любой другой операционной системой в этом списке), но я оставлю для вас более глубокие исследования.

[Скачать Kali Linux](#)

5. JonDo/Tor-Secure-Live-DVD

JonDo Live-DVD — это более или менее коммерческое решение для анонимности, которое работает аналогично Tor, учитывая тот факт, что дистрибутив также направляет свои пакеты через указанные «смешанные серверы» — JonDonym — (узлы в случае Tor), позволяющие пересылать пакеты зашифрованными каждый раз.

Это жизнеспособная альтернатива TAILS, особенно если вы ищете что-то с менее ограниченным пользовательским интерфейсом (хотя это еще живая система) и опытом, близким к среднему.



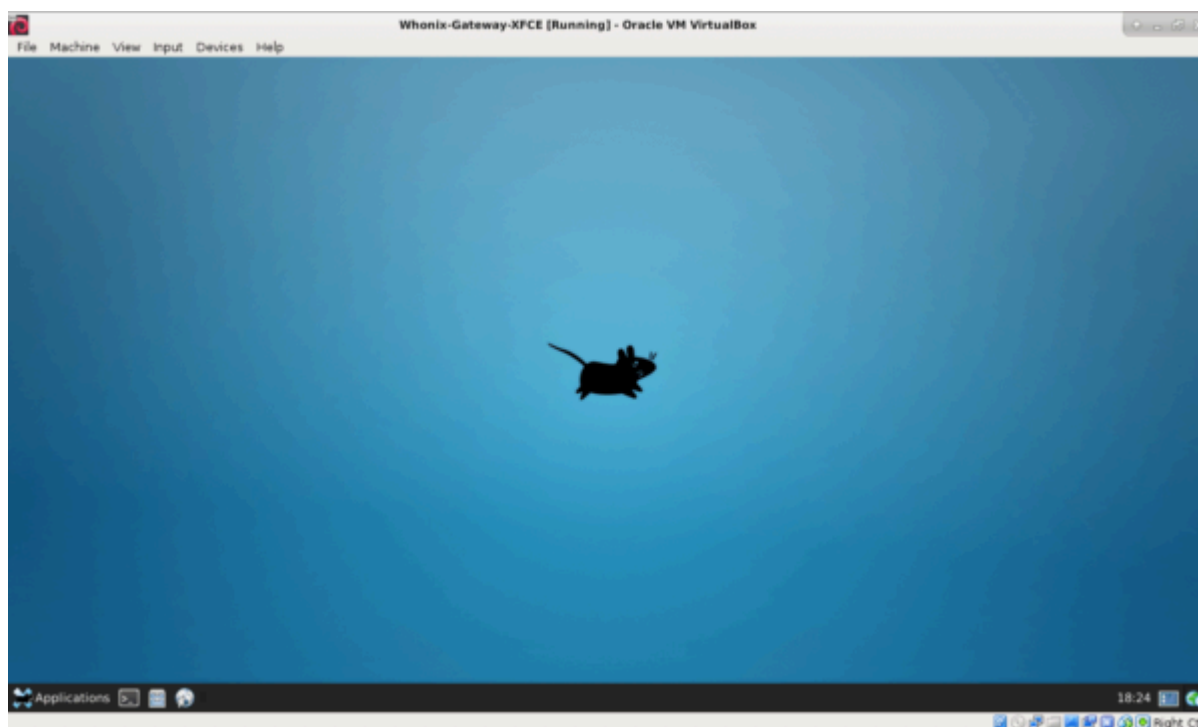
Дистрибутив основан на Debian, а также включает в себя набор инструментов для обеспечения конфиденциальности и других часто используемых приложений.

Однако JonDo Live-DVD — это сервис премиум-класса (для коммерческого использования), который объясняет, почему он ориентирован на коммерческое пространство. Как и Tails, он не поддерживает какой-либо собственный способ сохранения файлов и требует дополнительных усилий, чтобы предложить пользователям более высокую скорость вычислений.

[Скачать JonDo/Tor-Secure-Live-DVD](#)

6. Whonix

Если вы ищете что-то немного другое, **Whonix** использует совершенно иной подход, нежели упомянутый выше дистрибутивы, поскольку он не является Live системой, а вместо этого работает в виртуальной машине — в частности, в **Virtualbox** — где он изолирован от вашей основной ОС, чтобы минимизировать риск утечки DNS или проникновения вредоносных программ (с привилегиями root).



Whonix состоит из двух частей: первая — это «**Whonix Gateway**», который действует как шлюз Tor, а другая — «**Whonix Workstation**» — изолированная сеть, которая маршрутизирует все свои соединения через Tor-шлюз.

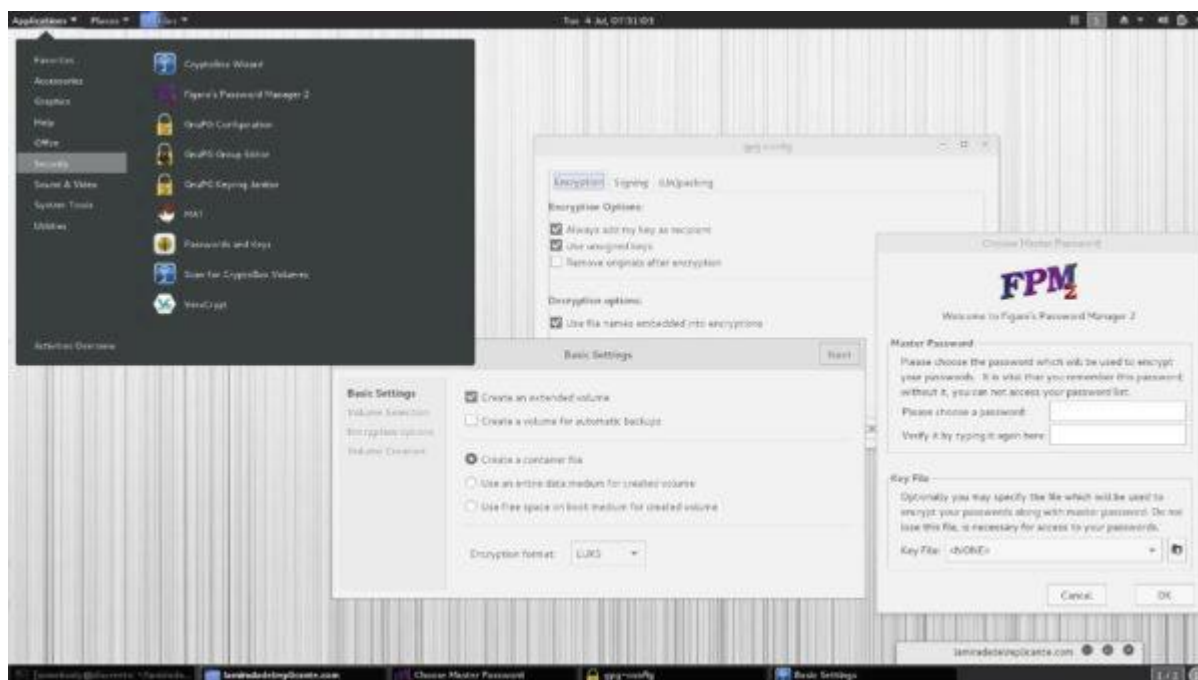
Этот дистрибутив на основе Debian использует две виртуальные машины, что делает его относительно ресурсоемким, поэтому время от времени вы будете испытывать задержки, если ваше оборудование медленное.

[Скачать Whonix](#)

,

7. Discreet Linux

Discreet Linux, ранее UPR или Ubuntu Privacy Remix, представляет собой дистрибутив Linux на основе Debian, разработанный для обеспечения защиты пользователей от троянского наблюдения за счет полной изоляции его рабочей среды от персональных. Он распространяется в виде live CD, который нельзя установить на жесткий диск, и сеть намеренно отключена во время его работы.



Discreet Linux является одним из уникальных дистрибутивов в этом списке и, очевидно, не предназначен для повседневных вычислительных задач, таких как обработка текстов и игр. Его исходный код редко обновляется, учитывая небольшую потребность в обновлениях/исправлениях, но он поставляется с рабочей средой **Gnome** для легкой навигации.

[Скачать Discreet Linux](#)

8. IprediaOS

IprediaOS — это дистрибутив Linux на базе Fedora, созданный для анонимного просмотра веб-страниц, электронной почты и обмена файлами, предлагая пользователям стабильность, скорость и вычислительную мощность. Будучи операционной системой, заботящейся о безопасности, IprediaOS разработана с минималистской философией, позволяющей поставлять только жизненно важные приложения, а также автоматически и прозрачно шифровать и анонимизировать весь проходящий через нее трафик, используя анонимную сеть I2P.



Функции, которые предоставляет **IprediaOS**, включают I2P Router, Anonymous IRC-клиент, Anonymous BitTorrent-клиент, анонимный просмотр Интернета, поиск анонимных eepSites (i2p-сайтов), анонимный почтовый клиент и LXDE.

[Скачать IprediaOS](#)

9. Parrot Security OS

Parrot Security OS — еще один дистрибутив на основе Debian, предназначенный для тестирования, этического взлома и обеспечения анонимности в Интернете. Он содержит надежную и портативную лабораторию для экспертов в области цифровой криминалистики, которая включает в себя не только программное обеспечение для обратного проектирования, криптографии и конфиденциальности, но также для разработки программного обеспечения и анонимного серфинга в Интернете.

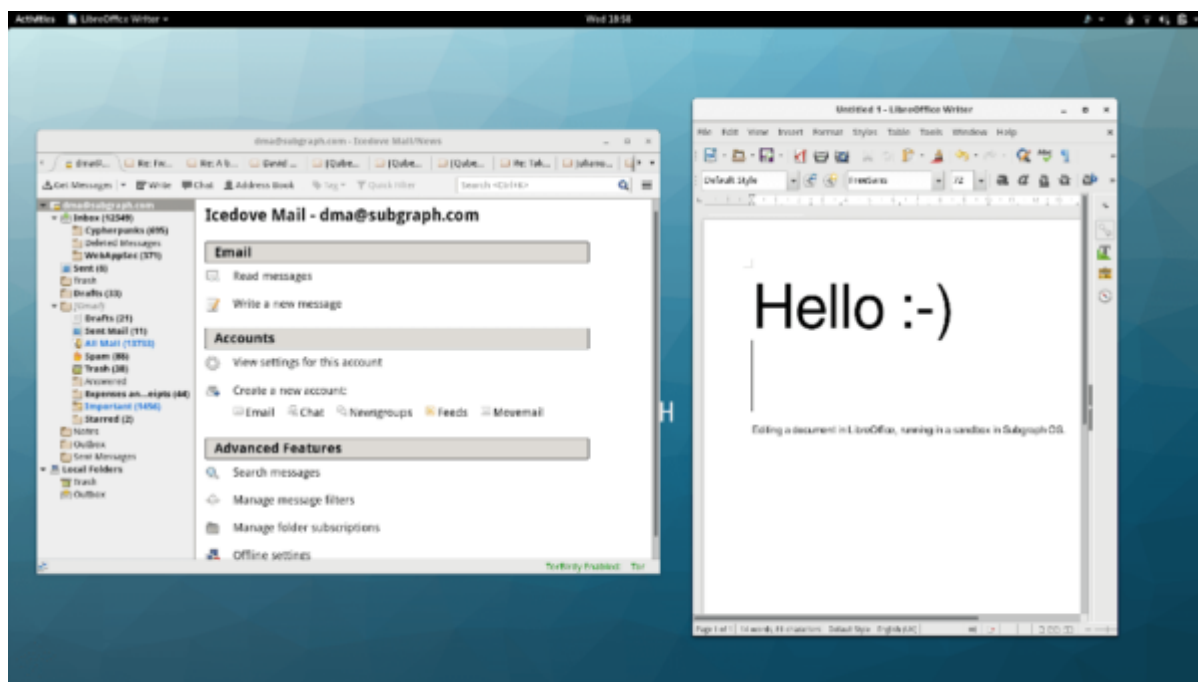


Он распространяется в виде скользящей версии, которая поставляется только с основными приложениями, такими как Tor Browser, OnionShare, Parrot Terminal и MATE, в качестве среды рабочего стола по умолчанию.

[Скачать ОС Parrot Security](#)

10. Subgraph OS

Subgraph OS — это легкий дистрибутив на основе Debian, разработанный, чтобы быть невосприимчивым к наблюдению и помехам со стороны злоумышленников в любой сети, независимо от уровня их сложности. Он создан для использования усиленного ядра Linux в сочетании с брандмауэром приложений, чтобы блокировать доступ определенных программ к сети, и он заставляет весь интернет-трафик проходить через сеть Tor.

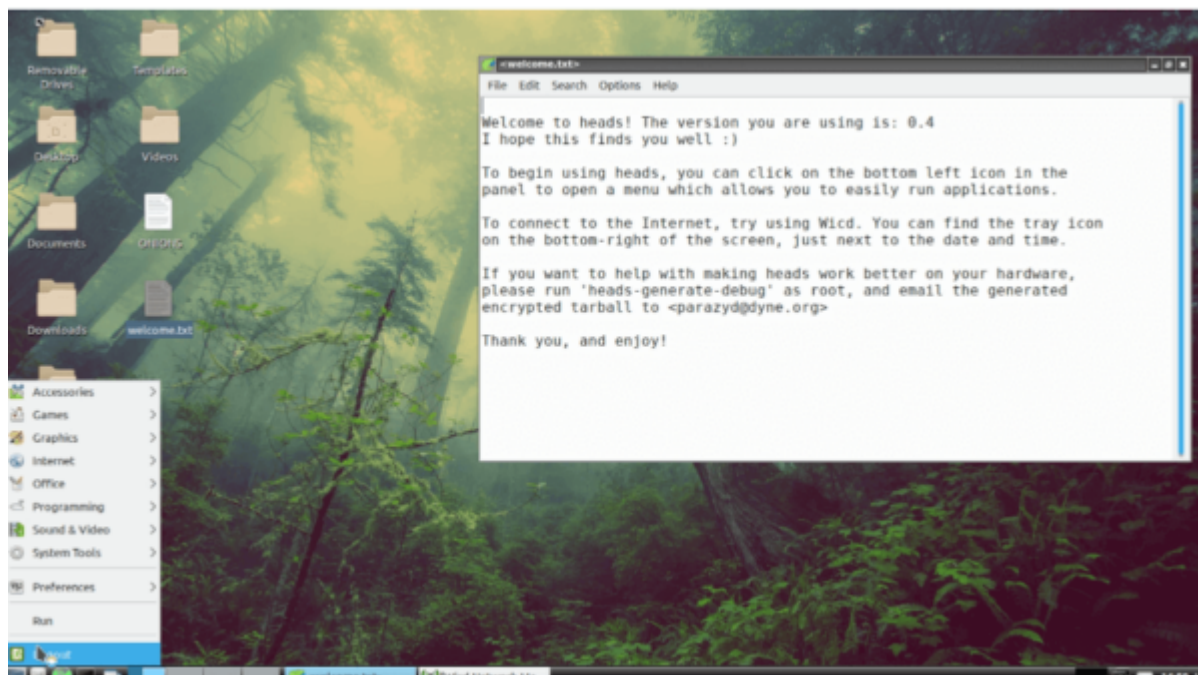


Предназначенная как защищенная от атак вычислительная платформа, цель Subgraph OS состоит в том, чтобы предоставить простую в использовании ОС со специальными инструментами конфиденциальности без ущерба для удобства использования.

[Скачать Subgraph OS](#)

11. Heads OS

Heads — это бесплатный дистрибутив Linux с открытым исходным кодом, созданный с целью соблюдения конфиденциальности и свободы пользователей и обеспечения их безопасности и анонимности в Интернете.

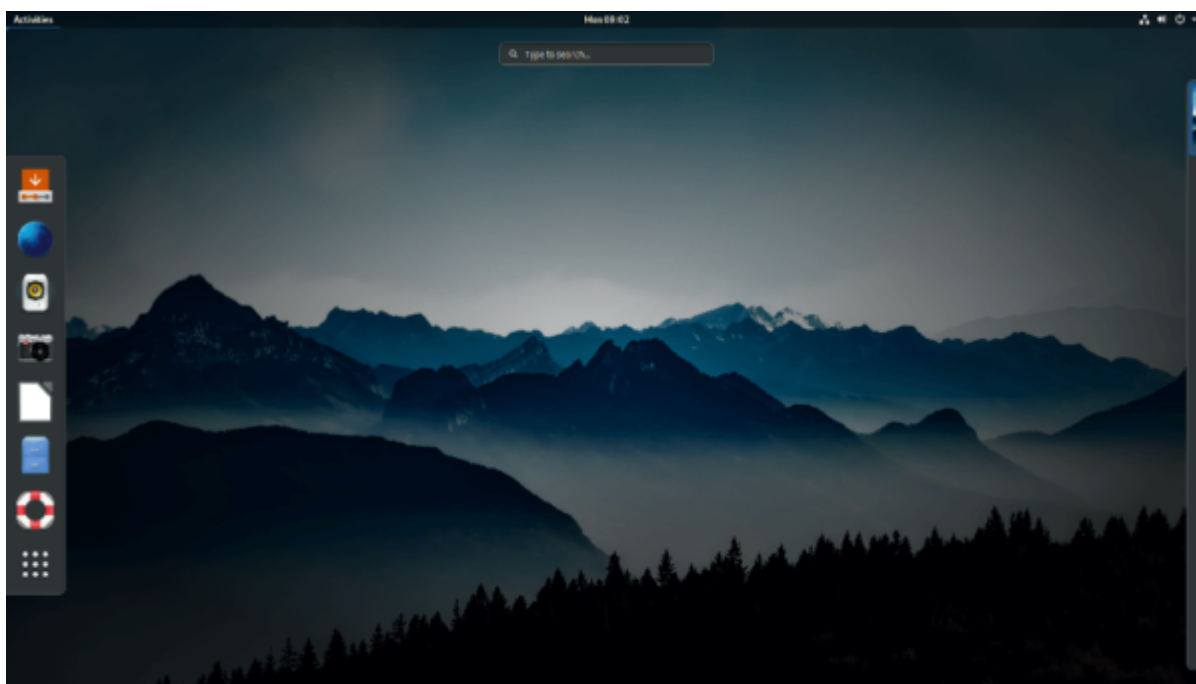


Он был разработан, чтобы стать ответом на некоторые «сомнительные» решения Tails, такие как использование системного и несвободного программного обеспечения. То есть все приложения в Heads являются бесплатными и с открытым исходным кодом, и он не использует **systemd** в качестве системы инициализации.

[Скачать Heads OS](#)

12. Alpine Linux

Alpine Linux — это легкий ориентированный на безопасность дистрибутив Linux с открытым исходным кодом, разработанный для обеспечения эффективности ресурсов, безопасности и простоты на основе BusyBox и musl libc.



Он предназначен для того, чтобы предоставить пользователям полный контроль над их вычислительной системой с полной настраиваемостью, привлекательной анимацией и минимальным объемом данных. Он поставляется с **GNOME** в качестве среды рабочего стола по умолчанию.

[Скачать PureOS](#)

14. Linux Kodachi

Linux Kodachi — это легкий дистрибутив Linux, разработанный для работы с флешкой или DVD. Сразу же, он фильтрует весь сетевой трафик через виртуальную прокси-сеть и сеть Tor, чтобы скрыть местоположение своего пользователя, и делает все возможное, чтобы удалить любые следы своей деятельности, когда он будет использоваться.

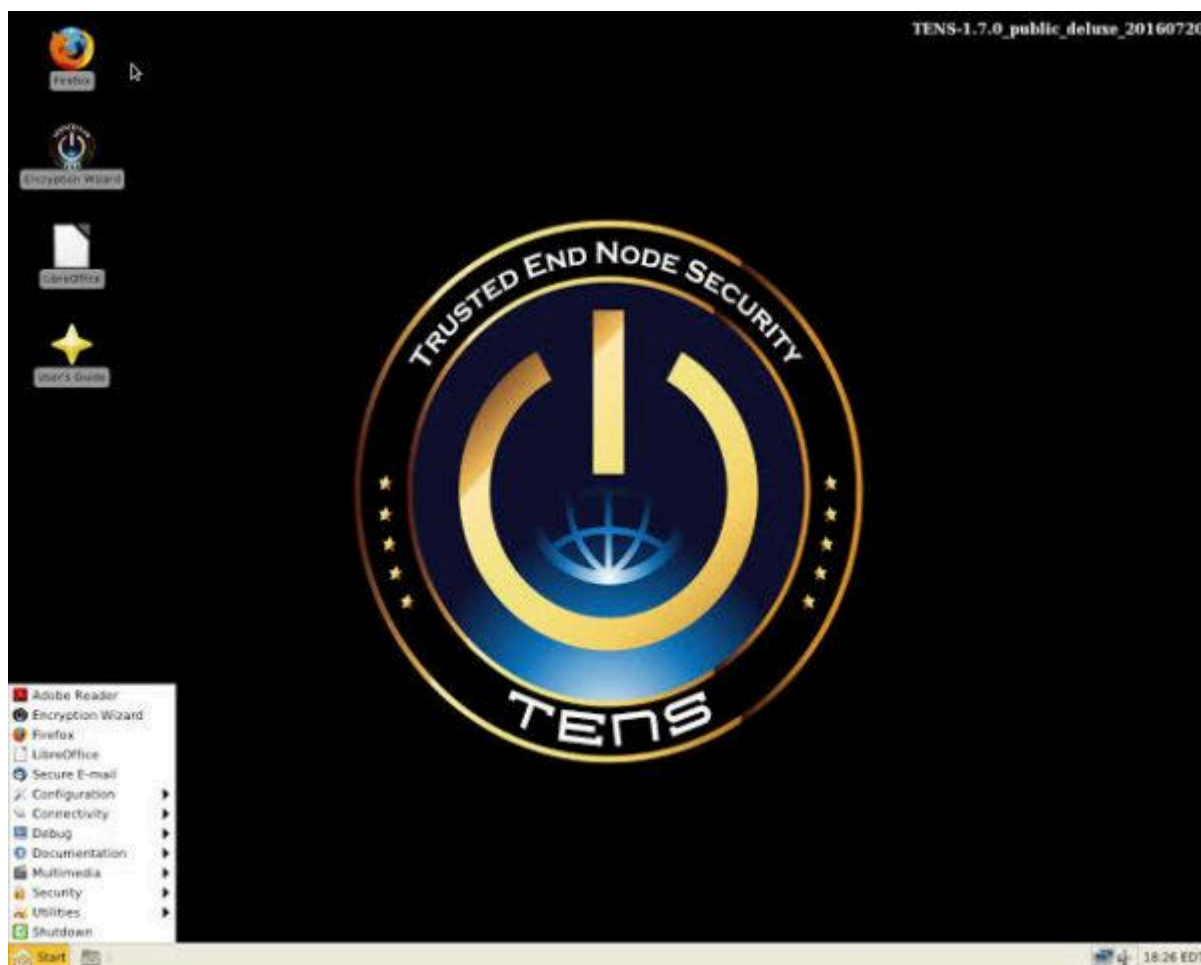


Linux Kodachi основан на **Xubuntu 18.04**, поставляется с настольной средой XFCE и несколькими встроенными технологиями, которые позволяют пользователям оставаться анонимными в сети, а также защищают свои данные от попадания в нежелательные руки.

[Скачать Linux Kodachi](#)

15. TENS

TENS (ранее Lightweight Portable Security или LPS) расшифровывается как **Trusted End Node Security**, и это программа, которая загружает базовую ОС Linux с портативного устройства хранения без монтирования каких-либо данных на локальный диск.



TENS не требует никаких привилегий администратора для запуска, никакого контакта с локальным жестким диском, ни установки, среди некоторых других расширенных функций безопасности. Да, и забавный факт, TENS управляется и выпускается Информационным управлением ВВС США.

[Скачать TENS OS](#)

Вывод

Я не знаю, сколько дистрибутивов в нашем списке вы использовали ранее, но выбор любого из них для тест-драйва — это первый шаг к гарантированию вашей безопасности в Интернете, и ваш выбор зависит от ваших личных предпочтений.

Спасибо за уделенное время на прочтение статьи!