Внимание: *В связи с массовым распространением ОС Android, начали появляться и вирусы под наиболее распространённые дистрибутивы Linux. Конечно, вирусов для Linux гораздо меньше, чем для Windows, однако угроза заражения вашего компьютера уже вполне реальна. Этим вирусам не требуются права суперпользователя, чтобы прописаться в системе им вполне достаточно обычных пользовательских прав. И обновления безопасности от них не спасут — ведь пользователь сам, не зная того, открывает заражённые файлы или заходит на сайты, заражённые вирусами.*

Для защиты от вирусов и противодействия вредоносному коду, начиная с версии 3.1.3, в ***FIDOSlax*** *добавлен аудит изменений файловой системы и установленных сетевых соединений,*

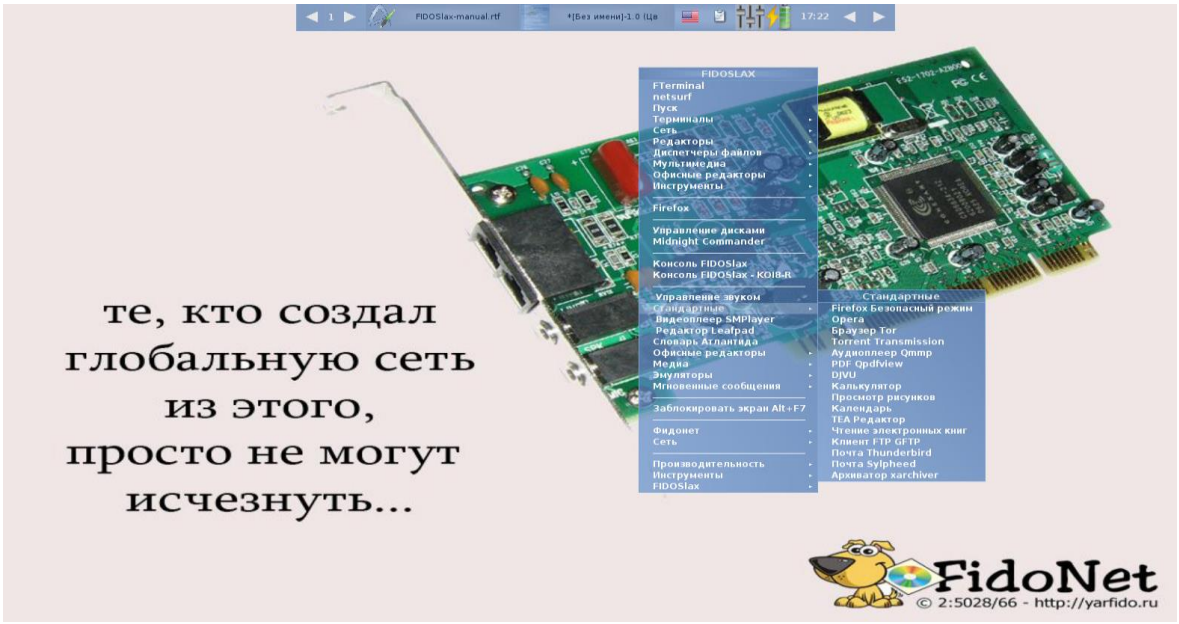
а также антивирус, работающий в режиме Real-Time monitoring.

Эта информация выводится в области оповещения пользователя — в верхнем левом углу экрана. Более подробно об угрозах безопасности для пользовательских дистрибутивов и противодействию вирусной угрозе в ***FIDOSlax Linux****, см. п. 12 документации.*

Документация FIDOSlax Linux

FIDOSlax Linux — быстрый дистрибутив Linux, который можно сразу же начать использовать на любом компьютере — без установки и настройки ПО — всё необходимые программы уже включены в образ DVD.

Вы можете уставить дистрибутив на накопителе USB-флеш, запустить его с раздела жёсткого диска — как вторую операционную систему, без удаления Windows или создания доп. разделов — дистрибутив отлично работает на уже имеющиеся разделах FAT32 или NTFS.



FIDOSlax Linux является **гибридным** дистрибутивом (т.е. занимает промежуточное положение между обычными дистрибутивами и дистрибутивами **Live**) и позволяет использовать **Linux** и приложения **Open Source** на компьютере. Сразу же после загрузки с **DVD/CD** можно начать работать в системе — с параллельно установленной на жёстком диске MS Windows.

Дистрибутив выпускается в трех вариантах:

1. **Стабильная версия** — iso-образ *fidoslax-desktop-edition-stable* с максимальным набором готового ПО, надежный и наиболее отлаженный. Основная графическая оболочка ***Fluxbox***. Эта версия рекомендуется для большинства компьютеров, выпущенных с 2000 г. по настоящее время. Содержит средства аудита файловой системы и сетевых соединений, а также встроенный антивирус — для защиты от вредоносного кода и вирусов;

2. **Текущая разрабатываемая версия** — iso-образ *fidoslax-desktop-edition-devel*, набор ПО меньший, а также менее стабильная и отлаженная, но с более новым ядром. Эта версия подойдёт для новых компьютеров, выпущенных с 2014 г., на которых более старое ядро стабильной версии не смогла распознать новых устройств. Основная графическая оболочка ***Fluxbox***. Со-

держит средства аудита файловой системы и сетевых соединений, а также встроенный антивирус — для защиты от вредоносного кода и вирусов;

3. **Ретро-версия** — iso-образ *fidoslax-retro-edition* — архивная и почти неподдерживаемая версия с меньшим набор ПО. Для любителей старины и архаики — основная графическая оболочка ***Tritity DE(KDE 3)***. Эта версия подойдёт для большинства компьютеров, выпущенных с 1998 по 2008 г.. Не содержит аудит файловой системы и сетевых соединений, также отсутствует встроенный антивирус.

Ранее **FIDOSlax Linux** был основан на дистрибутиве **Slax**, сейчас в качестве основы используется **Porteus(Портэус) Linux**, но есть и отличия — и усовершенствования, и дополнительные возможности.

Разница между **Slax** и **Porteus** небольшая: второй произошёл от первого, у них сейчас разная компрессия модулей — так называются пакеты, которые разворачиваются из архива прямо в оперативную память при запуске системы. За счёт этого дистрибутивы эти небольшие — и быстрые. Оба дистрибутива, и **Porteus**, и **Slax**, основаны на технологии **Linux Live Kit**. Активно используется ядерный модуль **aufs** (**AnotherUnionFS**) — вспомогательная файловая система, каскадно объединяющая и монтирующая каждый модуль **ПО** в корневую файловую систему Linux. Как и что работает на системном уровне можно почитать тут: ***http://www.linux-live.org***.

Отличия **FIDOSlax Linux** от **Slax** и **Porteus** в том, что первый работает чуть быстрее, а также включает готовый и оптимизированный набор программ для русских пользователей — офисных, мультимедийных, программ резервного копирования и восстановления данных.

Ниже тесты производительности для задач кодирования видео:
http://openbenchmarking.org/result/1609232-LO-FIDOSLAX688
http://openbenchmarking.org/result/1609239-LO-PORTEUS3108

Сравнение проводилось с использованием похожих DE — Fluxbox (FIDOSlax) и Openbox (Porteus), поэтому разница небольшая. Если сравнивать с другими версиями Porteus на том же ядре — выигрыш при использовании ***FIDOSlax*** достигать и 10% на том же железе.

Сейчас **FIDOSlax Linux** это не только дистрибутив, работающий на старом оборудовании с быстрыми приложениями под **GTK2**, но также полностью функциональный дистрибутив для десктопного применения с набором свежего и тяжёлого ПО — **LibreOffice**, **firefox** и т.д. Функционал системы легко расширяется при помощи дополнительных модулей с расширением ***.xzm**.

Что нового в стабильной версии 3.1.3

Изменения между версиями 3.1.2 и 3.1.3:

1 для отслеживания действий, произведённых вредоносным кодом, начиная с версии 3.1.3, в ***FIDOSlax*** ведётся аудит изменений файловой системы. История событий по изменению объектов файловой системы записывается в файл */var/log/files-mon*, более подробно см. п. 12 документации;

2 для отслеживания действий, произведённых вредоносным кодом, начиная с версии 3.1.3, в ***FIDOSlax*** ведётся аудит установленный сетевых соединений. История событий по установленным соединениям записывается в файл */var/log/program-mon*, более подробно см. п. 12 документации;

3 для защиты от вирусов и противодействия вредоносному коду, начиная с версии 3.1.3, в ***FIDOSlax*** добавлен антивирус ClamAV, работающий в режиме Real-time monitoring. Более подробно см. п. 12 документации;

4 Начиная с версии 3.1.3, в ***FIDOSlax*** ведётся отображение событий: по изменению файловых процессов; программ, установивших сетевые соединения; а также оповещений попыток заражения системы вирусами, — мониторинг отображается слева от панели задач, всегда в свободной области левого верхнего угла экрана;

5 обновлены некоторые модули – firefox и т.д., набор уже готового к использованию набора программ в каталоге *porteus/program* — более 1,3 Gb.

Более подробно о защите от вирусов и противодействии против вредоносного кода см. п. 12 документации.

Описание стабильной версии 3.1

1 Ядро версии **3.17.4**, в качестве основы использован **Porteus 3.1** — для расширения возможностей системы можно использовать модули этой версии **Porteus**;

2 Графическая оболочка **FLUXBOX**;

3 Новый установщик, использующий **Grub4DOS**, позволяет устанавливать **FIDOSlax Linux** на разделы FAT, NTFS, EXT2/EXT3/EXT4, интегрировать загрузку **FIDOSlax Linux** в меню различных загрузчиков Windows и Linux;

4 Большой набор уже готового к использованию набора программ — около 1 Gb уже готовых модулей, которые находятся в папке *porteus/program*;

5 Новая возможность, пока отсутствующая в **Slax** и **Porteus —** динамическая загрузка и выгрузка приложений, при помощи меню — одним щелчком мыши. Это позволяет более эффективно использовать **ОЗУ** и ресурсы процессора — пользователь решает сам какие программы будет использовать, — и только эти программы загружаются в память на лету;

6 Кроме клиента для социальной сети **FIDONet**, **FIDOSlax** содержит также встроенный сервер, позволяющий за 1 минуту поднять полностью функционирующий сервер(узел) **FIDONet**;

7 Кроме популярных фидошных артов, дистрибутив оформлен с использованием картин художников ренессанса;

8 И как обычно — три кодировки на выбор при помощи команды *lang* — **KOI8-R**, **CP1251** и **UTF-8**.

Содержание

12. Вирусная угроза для рабочих станций Linux. Противодействие вирусным атакам: аудит изменений файлов и установленных сетевых соединений, использование антивируса ClamAV для Real-time мониторинга

1. Установка FIDOSlax на USB-флеш накопитель

Скачайте iso-образ ***FIDOSlax*** с сайта *https://fidoslax.github.io/*; Раскройте образ *iso* на USB-флеш диск, извлеките из него папки *porteus* и *loader*. Для установки необходимо, чтобы эти два каталога были в корне накопителя — скопируйте их на USB-флеш диск.

Для Windows:

Перейдите на диск в каталог *loader*, правой кнопкой мыши щёлкните на файле ***INSTALL.bat*** и выберите в меню ***«Запустить от имени администратора»***.

Для Линукс:

Откройте терминал, перейдите на примонтированный раздел с ваше USB-флешкой в каталог *loader*, при помощи команд **su root** или **sudo -s** станьте **root**'ом. Запустите файл ***INSTALL.sh:***

 # sh ./INSTALL.sh

Появится окошко с инсталлятором, в нём два раза нажмите клавишу **Enter**.
Теперь ***FIDOSlax*** установлен на вашу флешку.

Для его запуска перезагрузите компьютер, при помощи клавиши **F12(**или аналогичной), в самом начале загрузки компьютера выберите первым загрузочным устройством вашу флешку. Появится меню **GRUB4DOS**, в нём выберите пункт «**FIDOSlax on USB/HDD**»

2. Установка FIDOSlax на жёсткий диск

По-умолчанию ***FIDOSlax*** поддерживает два способа установки на жёсткий диск — в качестве единственной ОС, а также совместно с Windows и другими дистрибутивами LInux:

2.1 Установка в качестве единственной операционной системе — на чистый жёсткий диск

Создайте раздел на жёстком диске и отформатируете его. В качестве файловой системы можно выбрать EXT3/EXT4, FAT32 или NTFS. Подключите этот раздел. Загрузитесь с iso образа и установите ***FIDOSlax*** при помощи команд, описанных в разделе **1. Установка FIDOSlax на USB-флеш накопитель.**

2.2 Установка жёсткий диск совместно с ОС Windows

Этот тип установки можно произвести только из Windows.

Скачайте iso-образ ***FIDOSlax*** с сайта *https://fidoslax.github.io/*; Раскройте образ *iso* на раздел диска, извлеките из него папки *porteus* и *loader*. Для установки необходимо, чтобы эти два каталога были в корне одного из разделов жёсткого диска — диска **C:** или **D:**.

Для Windows Vista и более старших версий:

Перейдите на диск в каталог *loader*, правой кнопкой мыши щёлкните на файле ***GRUB2WIN.bat*** и выберите в меню ***«Запустить от имени администратора»***.

Появится окошко с инсталлятором, в нём нажмите клавишу **Enter**. После этого появится окошко программы «**Grub2DOS Toolbox for Windows**». В меню **Tasks** этого окошка щёлкните мышкой и выберите «**Add Grub2DOS bootmgr toot menu (Vista/W2008 above)** », далее в появившемся списке «**Choose bootmgr file...**» выберите файл bootmgr, обычно **C:\bootmgr** и кликните мышкой на кнопку «**Do It!**»

Для Windows XP и Windows 2003 и младших версий:

Перейдите на диск в каталог *loader*, правой кнопкой мыши щёлкните на файле ***GRUB2XP-2003.bat*** и выберите в меню ***«Запустить от имени администратора»***.

Появится окошко с инсталлятором, в нём нажмите клавишу **Enter**.

Теперь ***FIDOSlax*** установлен на раздел как вторая операционная система. Для загрузки перезагрузите компьютер, затем в меню загрузчика Windows выберите пункт «**Grub4DOS**», появится меню **GRUB4DOS**, в нём выберите пункт «**FIDOSlax on USB/HDD**»

Примечание. Вы всегда можете отредактировать меню загрузчика **Grub4DOS.** В установленном виде это файл в корне раздела — menu.lst. В нём можно отредактировать пункты, добавить/убрать опции загрузки(cheatcodes — актуальные опции доступны в файле *loader/boot/docs/cheatcodes.txt*);

Также можно подредактировать шаблоны этого меню, они находятся в каталоге *loader/grubinst/menu.lst.*.template* — тогда установщик и загрузчик будет использовать нужные вам опции.

2.3 Установка жёсткий диск совместно с ОС Линукс

Этот тип установки можно произвести только из Линукс.

Скачайте iso-образ ***FIDOSlax*** с сайта *https://fidoslax.github.io/*; Раскройте образ *iso* на раздел диска, извлеките из него папки *porteus* и *loader*. Для установки необходимо, чтобы эти два каталога были в корне одного из разделов жёсткого диска.

Перейдите на диск в каталог *loader/grubinst/*, скопируйте файлы *grldr.mbr* и *grldr* в корень диска:

cp grldr.mbr grldr ../

Далее, в зависимости от типа вашего загрузчика, откройте один из шаблонов — *lilo.conf.tempate* или *grub.cfg.template*. Добавьте строки из шаблона в строки меню в конфигурационный файл вашего загрузчик и перегенерируйте меню стандартным для вашего дистрибутива образом.

Теперь ***FIDOSlax*** установлен на раздел как вторая операционная система. Для загрузки перезагрузите компьютер, затем в меню загрузчика выберите пункт «**FIDOSlax**» и загрузите его.

3. Логин и пароль по-умолчанию

Для входа в систему наберите *login*:

root

пароль:

toor

4. Запуск X Window и менеджера экрана FLUXBOX

После входа в систему наберите в консоли:

 # startx

5. Русификация

Для переключения раскладки языка **ЛАТ/РУС** используйте кнопку **правый ALT.**

Для изменения комбинации клавиш переключения, воспользуйтесь настройками Qxkb, щёлкнув на иконку с флагом страны в трее. Для сохранения изменений после перезагрузки, сохраните файл *~/.config/qxkb.cfg*, одним из способов, описанных в 6-ом разделе документации.

Пользователю доступны три кодировки **— CP1251, UTF-8, KOI8-R.**

Для смены кодировки наберите в консоли команду:

 # lang

и выберите нужную вам кодировку. После перезагрузки система будет запущена в нужной вам кодировке.

Смена кодировки при помощи команды **lang** возможна, если ***FIDOSlax*** запущен с USB/HDD.

При загрузке с DVD/CD команда **lang** не работает, но можно поменять кодировку, создав в корне раздела каталог *slax-data/autoload-32*. Затем скопируйте модуль с нужной кодировки из каталога *porteus/fidoslax* в *slax-data/autoload-32*. Переименуйте его расширение с *.1xzm на *.xzm и перегрузитесь.

6. Сохранение данных

По-умолчанию ***FIDOSlax*** стартует как обычный **LiveCD**, так что все изменённые данные после перегрузки все изменения пропадают — за исключением тех, которые вы делаете при помощи Волшебных папок(см. ниже).

Если вы установили ***FIDOSlax*** на флешку/раздел жёсткого диска вы можете сохранить изменения (конфигурационные файлы или каталоги с изменёнными фалами) при помощи команд **live2root**, **lived2dir** и **lived2dirs**. Для этого откройте терминал, переедите в каталог с изменёнными файлами, а затем выполните одну из следующих команд:

live2root *имя_файла*	Сохраняет один файл *имя_файла*
lived2dir	Сохраняет все файлы в текущем каталоге
lived2dirs	Сохраняет все файлы и подкаталоге в текущем каталоге

К примеру, Вы создали новые модули и хотите отредактировать меню программ **FLUXBOX**, чтобы появился новый пункт для запуска вашей программы.

Для этого открываете терминал и переходите в каталог с настойками **FLUXBOX:**

 # cd ~/.fluxbox

Меню находится в файле *usermenu*, открываете его с помощью редактора *leafpad*:

 # leafpad usermenu

И добавляет нужную вам строку для запуска новой программы.

К примеру, если вы поместили ваш *модуль.xzm* в каталог *porteus/program*, то тогда мы можете создать динамическое меню — которое загружает программу в память только тогда, когда вам это нужно. Для этого добавляете в нужном месте меню строку:

[exec] (Модуль) {модуль || mod-wrapper модуль}

Закрываете редактор. Чтобы изменения в меню после перезагрузки сохранились, теперь нужно выполнить команду:

 # live2root usermenu

При загрузке с DVD/CD команды **live2root, lived2dir и lived2dirs** не работают, но можно сохранить свои файлы, создав на разделе жёсткого диска или на флешке каталог *slax-data/специальный_подкаталог — Волшебную папку*, и после перезагрузки он будет подсоединён в нужном месте файловой системы.

Специальный каталог slax-data	Подключение данных
slax-data/slax-root	При загрузке, если на одном из дисков найден каталог slax-data/slax-root, то его содержимое будет подключено как подкаталоги для /root
slax-data/slax-etc	При загрузке, если на одном из разделов найдены файлы в slax-data/slax-etc, они будут подключены как файлы для подкаталога для /etc
slax-data/slax-rc.d	При загрузке, если на одном из разделов найдены файлы в slax-data/slax-rc.d, они будут подключе-

	ны как файлы для подкаталога для /etc
slax-data/slax-tmp	При загрузке, если на одном из разделов найден каталог в slax-data/slax-tmp, он будет подключен как /tmp
slax-data/slax-desktop	При загрузке, если на одном из разделов найден каталог в slax-data/slax-desktop, он будет подключен как /root/Desktop Далее вы сможете сохранять файлы на рабочий стол — и они после перезагрузки не пропадут, а появятся на рабочем столе.
slax-data/my-downloads	При загрузке, если на одном из разделов найден каталог в slax-data/my-downloads, он будет подключён как /root/Downloads Далее вы сможете сохранять файлы в этот каталог — и они после перезагрузки не пропадут, а будут находится в том же каталоге.
slax-data/my-documents	При загрузке, если на одном из разделов найден каталог в slax-data/my-downloads, он будет подключён как /root/my-documents. Далее вы сможете сохранять файлы в этот каталог — и они после перезагрузки не пропадут, а будут находится в том же каталоге.

В нашем примере с меню **FLUXBOX**, на разделе нужно создать каталог *slax-data* в нём подкаталог *slax-root*. Далее просто скопируйте целиком каталог *~/.fluxbox* в созданный вами *slax-data/slax-root*. После перезагрузки все изменённые файлы *~/.fluxbox/** будут подключены к */mnt/sdX1/slax-data/slax-root/.fluxbox* — и вы можете их редактировать в процессе работы *~/.fluxbox* — данные сохраняться после перезагрузки.

А если, к примеру, вы захотели чтобы после перезагрузки использовалась изменённую вами раскладку клавиатуры Qxkb, то в папке */mnt/sdX1/slax-data/slax-root/* создайте подкаталог *.config* и скопируйте туда файл ~/.config/qxkb.cfg

 # cp ~/.config/qxkb.cfg /mnt/sdX1/slax-data/slax-root/.config/

Кроме вышеперечисленных способов сохранения, можно использовать стандартные способы сохранения **Porteus Linux,** описанные в разделах **документация** и **FAQ.**

К примеру, вот тут описана реализация сохранения при помощи ***Волшебных папок***, заимствованная командой **Porteus Linux** из проекта **FIDOSlax Linux**.

7. Драйвера, использование модулей ПО

Вы можете скачать уже готовые официальные модули драйверов и ПО из проекта **Porteus Linux**, вот отсюда: **http://dl.porteus.org/i486/**

Также можно использовать уже готовые модули и драйвера, собранные другими участниками проекта, которые можно найти на форуме **Porteus**: **http://forum.porteus.org/**

Главное — модули должны быть той же версии, что и модули ***FIDOSlax***. Если, примеру, вы используете **FIDOSlax версии 3.1 32-bit**, то и модули вам нужны от **Porteus версии 3.1 32-bit**.

Вы можете создать модули и драйвера ПО самостоятельно. Это сделать проще всего, собрав их из исходников при помощи команды:

 # src2pkg тарбол

После того, как **src2pkg** создаст в */tmp* пакет с *тарбол*.txz* или *тарбол*.tgz,* создать модуль *xzm* можно при помощи команды:

 # txz2xzm тарбол.txz

или

 # tgz2xzm тарбол.tgz

Новый модуль **.xzm* появится в каталоге */tmp/*.

Также для создания новых модулей удобно использовать базу драйверов и ПО — **SlackBuilds.org** — *https://slackbuilds.org/* .

Принцип тот же — сперва собирается пакет *.tgz или *.txz, используя уже готовый набор правил **SlackBuilds.org** — как ими пользоваться, описано этой статье: *http://citkit.ru/articles/867/* .

Затем собранные пакеты при помощи команд *tgz2xzm* и *txz2xzm* преобразуются в модуль *xzm*.

Для того чтобы использовать новый модуль — поместите его в каталог в корень любого раздела жесткого диска или флешки:

porteus/base	В этом случае модуль будет использоваться постоянно при старте системы. Недостаток в том, что он занимает память и ресурсы- вне зависимости нужен ли он пользователю или нет.
porteus/program	В этом случае модуль будет использоваться только когда нужен. Недостаток в том, что пользователю нужно прописывать активацию и запуск модуля в меню **~./fluxbox/usermenu**.
slax-data/autoload-32	Используется, только если вы загрузились DVD/CD и у вас нет возможности поставить ***FIDOSlax*** на флешку и положить модуль в **porteus/base** или **porteus/program**.

8. Настройка сети

По-умолчанию ***FIDOSlax*** использует динамическое присвоение IP-адресов.

Для установки статического IP-адрес для сетевого интерфейса Ethernet, откройте терминал, щёлкнув мышкой правой кнопкой мыши на пустом месте экрана и выбрав **FIDOSlax Termilal**, затем перейдите каталог /etc/rc.d:

 # cd /etc/rc.d

Затем скопируйте */etc/rc.d/rc.nodhcp-eth.tpl* в /etc/rc.d/rc.nodhcp-eth0:

 # cp /etc/rc.d/rc.nodhcp-eth.tpl /etc/rc.d/rc.nodhcp-eth0

Откройте любым редактором (можно *leafpad*) файл */etc/rc.d/rc.nodhcp-eth0* и измените в нём следующие поля:

 # leafpad rc.nodhcp-eth0

И измените следующие строки:

STATIC="NO" — установите для этого параметра значение "**YES**";

NSERVER1="192.168.0.2" — в этом параметре задайте IP-адрес первичного DNS-сервера (обычно вашего провайдера);

IP="192.168.4.7" — в этом параметре отредактируйте IP-адрес для вашего компьютера;

NETMASK="255.255.254.0" — задайте маску подсети (обычно 255.255.255.0);

GATEWAY="192.168.0.2" — задайте шлюз по-умолчанию.

Сохраните изменения в файле, закройте редактор.

Затем запустите команду */etc/rc.d/rc.nodhcp-eth0*:

 # ./rc.nodhcp-eth0

Для сохранения введённых вами значений, запустите команду **live2root**:

 # live2root rc.nodhcp-eth0

Перезагрузите ***FIDOSlax*** — после перезагрузки IP адрес будет назначен сетевому интерфейсу *eth0*.

Если вы загрузились с DVD/CD, то можете создать папку */mnt/sdXn/slax-data/slax-rc.d, (к примеру, /mnt/sda1/slax-data/slax-rc.d/).* Если скопировать *rc.nodhcp-eth0* туда, то после перезагрузки ***FIDOSlax*** станет использовать файл этот файл. Более подробно разделе документации ***6. Сохранение данных.***

Если выполнить подобные действия на разных компьютерах, присваивая разные IP-адреса, то можно загружать ***FIDOSlax*** с одной и той же флешки с разными настройками сети, а также прочими настройками.

Настройка **Wi-Fi** осуществляется сборкой модуля драйвера и *firmware* для вашего оборудования, как это описано выше в разделе документации **7. Драйвера, использование модулей ПО.**

После помещения модулей драйверов в *porteus/base* и перезагрузки, вторым этапом идёт настройка профиля *wpa_supplicant*. Затем можно запустить ***wifi-radar*** из меню ***FIDOSlax>Wi-Fi***, после чего подключится к точке.

9. Резервное копирование

Для резервного копирования можно выбрать из меню клиент **burp**, также как и сервер резервного копирования **burp**, всё это включёно в ***FIDOSlax***. Это удобно, если вам нужно быстро сохранить сразу много рабочих станций по сети.

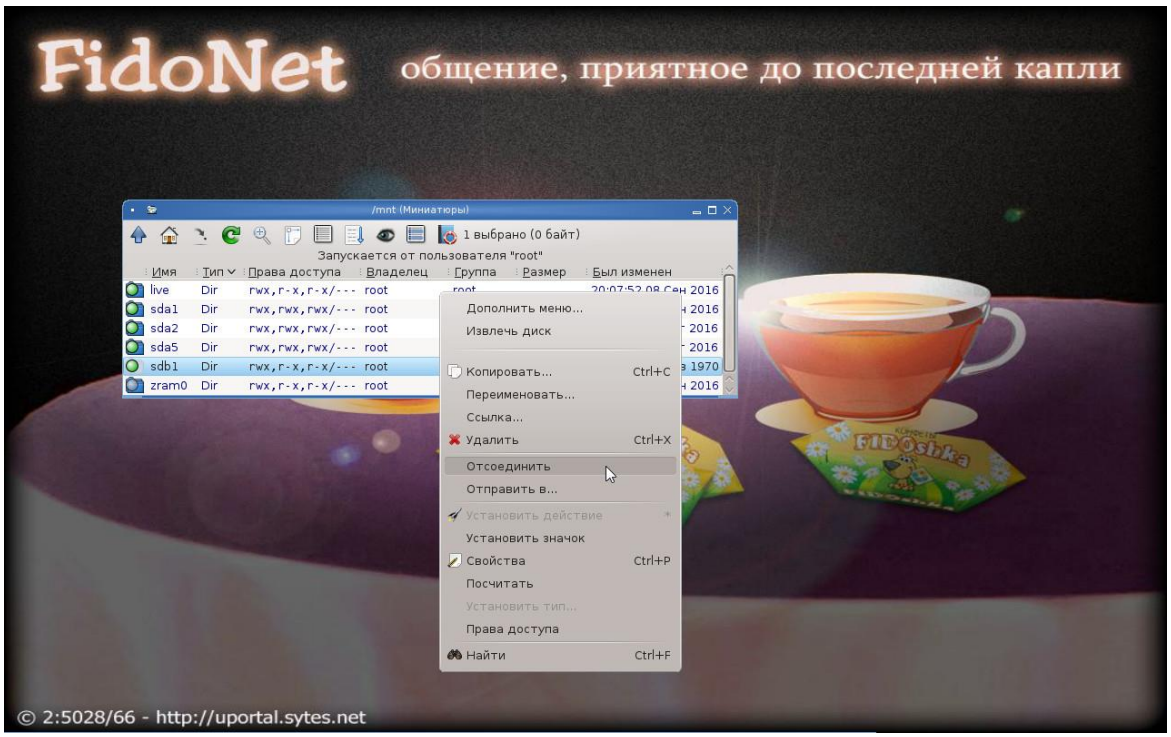
Для сохранения диска в образ, можно использовать *partclone.dd*, а также другие утилиты этого пакета.

Также можно выполнять резервное копирование при помощи *rsync/LuckyBackup.*

10. Монтирование дисков, создание образа ISO и шифрование

Используйте для подключения новых дисков, а также их безопасного отключения менеджер файлов **ROX-Filer**. Для этого запустите ROX-Filer, щёлкнув на правой кнопкой мыши на рабочем столе и выберете в центре меню рядом с пунктом «**Midnight Commander**» пункт «**Управление дисками**»(**Drive Manager**). Появится окно **ROX-Filer**. Подсоедините диск, вставьте флешку в USB разъём или CF-карточку в слот — и вы увидите, что в списке устройств новое неактивное (не подсвеченный зелёным) устройство. Для подсоединения диска просто щёлкните на нём левой кнопкой мыши, диск подключится и откроется.

Для безопасного отключения диска, закройте все программы, использующий этот диск, снова выберите пункт меню «**Управление дисками**»(**Drive Manager**), щёлкните правой кнопкой мыши на зелёном (активном) устройстве и выберите «**Отсоединить**»



Для создания образа ISO — скопируйте папки *loader* или *porteus* на чистый и пустой раздел диска/флешки, **добавьте/удалите** модули в *porteus/program*, затем откройте **терминал /командную строку cmd.exe** и перейдите в каталог loader.

Запустите **make_iso.bat** или **make_iso.sh**, передав этим скриптам имя файла и путь:

Для Windows:

C:\g:

G:\>cd loader

G:\loader>make_iso.bat d:/fdoslax.iso

Для Линукс:

#cd /mnt/sdb1/loader

 # sh ./make_iso.sh
Target ISO file name [Hit enter for]: /mnt/sdc1/fidoslax.iso

Использование флешки чревато тем, что вы можете потерять её — а с неё все ваши личные данные. Чтобы защитить вашу личную информацию, используете программу шифрования **ccrypt**, которая также включена в дистрибутив.

Для этого откройте терминал, перейдите в ту папку на флешки, в которой находятся ваши личные данные и введите команду:

 # ccryp -e *

Программа два раза спросит пароль, а потом зашифрует ваши данные.

Для расшифровывания введите:

 # ccrypt –d *

После ввода пароля, программа расшифрует вашу персональную информацию.

11. Фидонет

Кроме клиента для социальной сети **FIDONet**, дистрибутив содержит встроенный клиент социальной сети **FIDONet**, а также сервер — узел **FIDONet.**

Для чтения сообщений, настройки клиента или сервера, используйте соответствующее меню пункта **FIDONet**.

Для получения необходимой информации, вы можете использовать обучающие видео-ролики и презентации с пошаговыми инструкциями, доступные по этому адресу: *http://sf.net/projects/fidoip/files/media/*

Из меню **FIDONet** можно открыть книгу **Дмитрия Игнатова «Это ваше Фидо»,** которая включена в дистрибутив, также как и некоторые из его фидошных обоев для рабочего стола.

Также в дистрибутив включена ещё одна прекрасная разработка — текстовый редактор **TEA**, которую разрабатывает и поддерживает фидошник Пётр Семилетов. О возможностях этого редактора можно почитать тут: *http://semiletov.org/tea/#about* .

12. Вирусная угроза для рабочих станций Linux. Противодействие вирусным атакам: аудит изменений файлов и установленных сетевых соединений,

использование антивируса ClamAV для Real-time мониторинга

12.1 Вирусная угроза для рабочих станций Linux

Сетевая безопасность сервера отличается от безопасности рабочей станции. В первом случае обновлений ядра и бинарного кода сервисов, в которых уязвимость устранена, достаточно чтобы защитить систему. А во втором… Современным вирусам и вредоносным программам под Linux вполне достаточно обычных прав под которыми человек работает, если *пользователь* открывает заражённый документ (OpenOffice, MS Office, PDF) или заходит браузером на сайт, заражённый вирусом — даже если у вас установлена последняя версия браузера, заражение может производиться при помощи так называемых *уязвимостей нулевого дня*.

Но среди пользователей Linux по-прежнему распространено мнение, что «под Linux вирусы не работают». Сегодня это мнение полностью ошибочное, хотя раньше это действительно было так. С массовым внедрением мобильных и прочих устройств с ОС Android, стали появляться вирусы и под десктопные дистрибутивы Linux: *https://vms.drweb.com/search/?q=Android* .

Понятно, что программистам проще адаптировать зловредный код, чем самостоятельно писать оригинальный, поэтому счёт вирусов для десктопных дистрибутивов Линукс уже идёт не на десятки, а на сотни вирусов: *https://vms.drweb.com/search/?q=Linux* .

В этих результатах поиска вирусы исключительно под Линукс, а есть ещё и кроссплатформенные, а также вирусы-шифровальщики файлов под Linux, трояны и т.д., и искать их нужно в других категориях не по ключевому слову «Linux». Если *пользователь* сам запустил вредоносный код — открыв документ или заражённый сайт, — то от таких вирусов не спасёт последняя версия ядра или браузера. И таким вирусам для работы вполне достаточно обычных прав, под которыми человек работает. Вот пример такого вируса: https://vms.drweb.ru/virus/?i=8856496&lng=ru

И ему права суперпользвователя и не очень-то нужны. А вот ещё ссылка — на вирус, который каждые полминуты на заражённом компьютере делает слепок с экрана, и одновременно снимает звук с микрофона, чтобы отправить информацию в зашифрованном виде на удалённый сервер — тоже вирус под обычные пользовательские дистрибутивы Linux: https://vms.drweb.ru/virus/?i=7924647&lng=ru

И кто знает, сколько других подобных по Интернету уже бродит? Антивирусные компании отлавливают далеко не все — просто потому, что пользователи Linux тоже верят мифу, что под Linux вирусов нет, — соответственно, и беспокоиться не нужно. А оказывается, нужно. И нужен аудит изменений файловой системы, и аудит сетевых соединений, и антивирус.

12.2 Противодействие вирусным атакам: аудит изменений файлов и установленных сетевых соединений, использование антивируса ClamAV для Real-time мониторинга

Если вы используете ***FIDOSlax*** в качестве дистрибутива для восстановления данных (при помощи программ TestDisk, PhotoRec), сетевого копирования (клиент или сервер burp) и прочих сервисных задач, всё что написано о безопасности выше вам неактуально.

Но если вы используете ***FIDOSlax*** в качестве ОС для рабочей станции Linux в качестве десктопа, то имеет смысл ознакомится с нижеследующей информацией.

12.2.1 Аудит изменений файлов и установленных сетевых соединений

Для отслеживания действий, произведённых вредоносным кодом, начиная с версии 3.1.3, в ***FIDOSlax*** ведётся полный аудит изменений файловой системы. История событий по изменению объектов файловой системы записывается в файл */var/log/files-mon*.

Вот пример вывода этого файла:

tail –n3 /var/log/files-mon

11:13:49.828499 binkd(12904): CW /mnt/sda2/home/fido/outbound/139c033c.csy
11:13:49.833043 binkd(12904): CW /mnt/sda2/home/fido/binkd.log
11:13:49.835951 binkd(12904): CWO /mnt/sda2/home/fido/binkd.log

Формат файла:

время, приложение, название программы, номер процесса, тип действия (C — создание, W — запись, O — открытие, R — чтение) и полный путь к изменяемому/создаваемому файлу и его имя.

Для отслеживания действий, произведённых вредоносным кодом, начиная с версии 3.1.3, в ***FIDOSlax*** также ведётся журналирование установленных сетевых соединений. История событий записывается в файл */var/log/program-mon*. Слепок процессов и приложений, установивших соединение сохраняется раз в минуту — аудит соединений неполный, но этого вполне достаточно, чтобы отловить контрольное соединение вирусной программы.

К примеру, чтобы узнать с каким сервером связывался процесс binkd, изменявший объекты файловой системы в предыдущем выводе выполним поиск по номеру процесса (12904):

grep 12904 /var/log/program-mon

tcp 0 0 192.168.4.54:49624 192.168.0.1:3128 ESTABLISHED 12904/binkd: o 2:50

Формат файла — netstat.

При помощи анализа файлов */var/log/files-mon* и */var/log/program-mon* и сопоставлении времени и действий процессов и программ, вы сможете понять, что на вашем компьютере работает вредоносный код, даже если вирус не содержится в антивирусной базе данных.

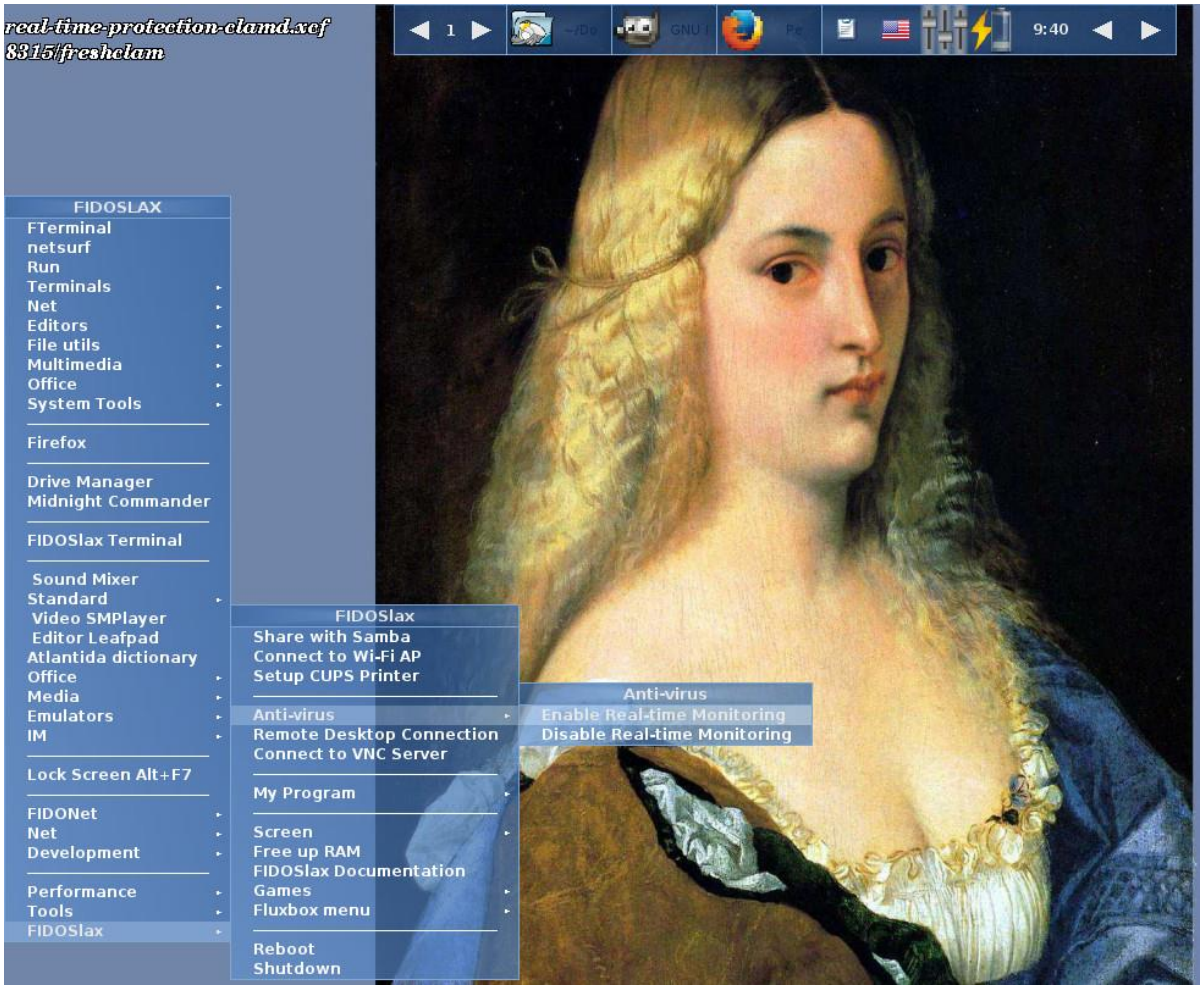
Также в последних версиях ***FIDOSlax*** (стабильной и разработческой) ведётся отображение этих событий. Информация выводится в области оповещения пользователя — в верхнем левом углу экрана. Раз в минуту этой в свободной области экрана выводится последний изменённый файл и последняя программа, установившее сетевое соединение.

На рисунке: последний изменённый объект файловой системы — файл ***Audit.xcf***, последняя программа, установившая сетевое соединение — ***firefox***, исходящий порт ***7634***.

Если в левом верхнем углу экрана появится имя файла, который вы не сохраняли/изменяли или имя программы, которую вы не запускали — то имеет смысл ознакомиться с файлами логов, чтобы понять вирус это или нет.

12.2.2 Использование антивируса ClamAV для Real-time мониторинга

Для защиты от вирусов и противодействия вредоносному коду, начиная с версии 3.1.3, в ***FIDOSlax*** добавлен антивирус ClamAV, работающий в режиме Real-time monitoring. Антивирус не активирован по-умолчанию, так как на старых ПК выпуска до 2008 года и ранее, после его включения, система может начать притормаживать. Однако если у вас хотя бы двуядерный процессор с ОЗУ более 1,5 GB, то можете смело включать Real-time monitoring — замедления системы вы не заметите. Для включения мониторинга реального времени, щелкните на рабочем столе правой клавишей мыши, и выберите меню ***FIDOSlax> Anti-virus>Enable Real-time monitoring***.

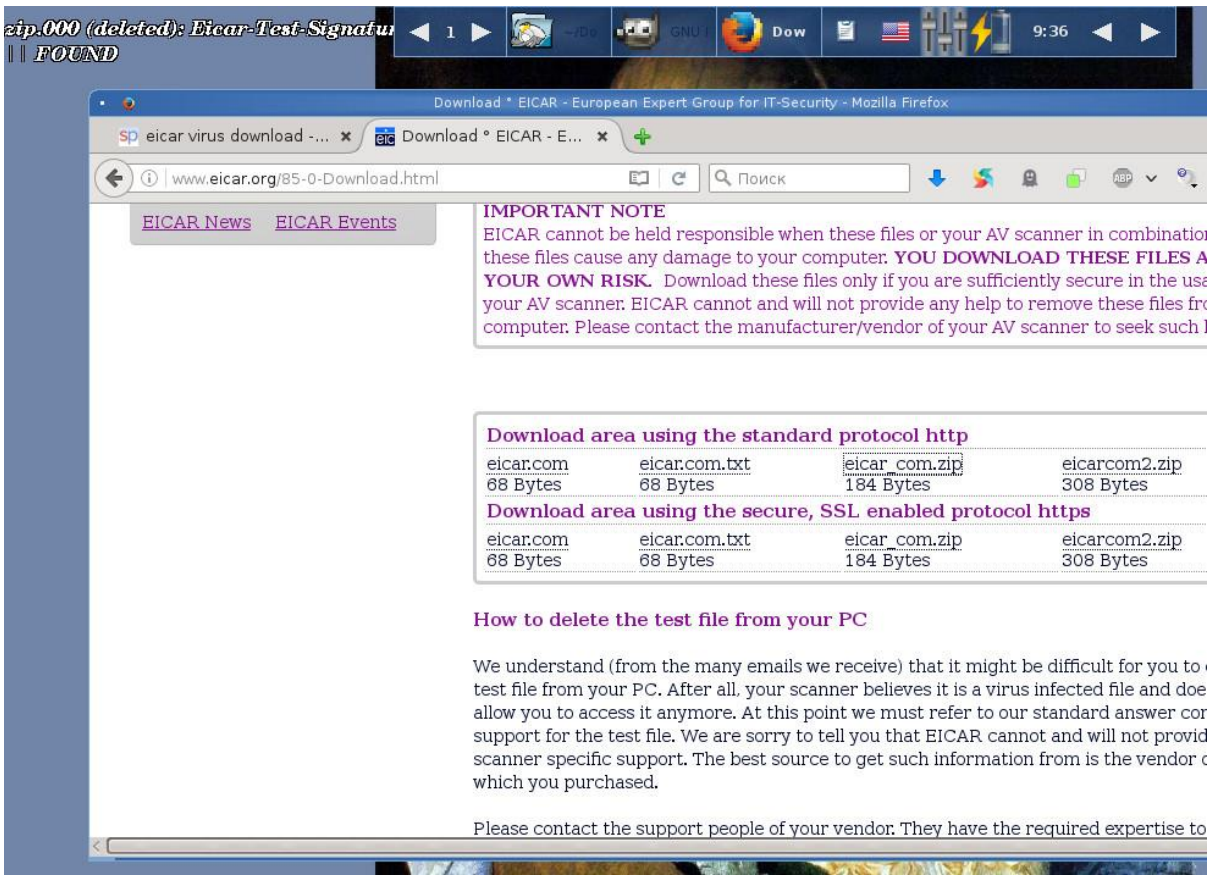


Вы можете проверить, что ClamAV загрузил последние обновления антивирусной базы данных — см. файл */var/log/clamav/freshclam.log,* а также что сервис clamd работает */var/log/clamav/clamd.log*.

После этого можете просматривать веб-сайты Интернет и открывать незнакомые файлы — в случае попытки заражения системы вы будете предупреждены.

На рисунке. Предупреждение о попытке заражения вашей рабочей станции появиться в левом верхнем углу, формат вывода: *имя файла, имя вируса, FOUND*.

Проверить работоспособность антивируса вы можете http://www.eicar.org/85-0-Download.html — на рисунке в левом верхнем углу экрана вы видите срабатывание предупреждения о попытке проникновения в систему тестового вируса EICAR.



К сожалению, ядро Linux даже в последней своей версии не может блокировать такого рода угрозы полностью. Поэтому, если вы увидели в левом верхнем углу экрана надпись «FOUND», сделайте сразу следующие действия:

1. Скопируйте файлы */var/log/files-mon* и */var/log/program-mon* куда-нибудь — по-умолчанию эти файлы находятся в оперативной памяти(live) системы и после перезагрузки удаляются;

2. Перегрузимте ***FIDOSlax*** — этим вы избавитесь от вируса. ***FIDOSlax*** — гибридный дистрибутив, промежуточным между обычным и live. Поэтому вирус просто не сможет прописаться в системе и не загрузится после перезагрузки;
3. Проанализируйте файлы */var/log/files-mon* и */var/log/program-mon*, и запустите *clamscan* для полного удаления файлов с вирусами.