Dr.WEB®
LiveCD

Защити созданное

Руководство пользователя

Dr.Web® LiveCD
Версия 6.0.0
Руководство пользователя
17.01.2011

Dr.Web, Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com
Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение

Dr.Web® LiveCD — это программный продукт, основанный на стандартном антивирусном сканере **Dr.Web**. Он позволяет восстановить систему в тех случаях, когда вследствие вирусной активности не представляется возможным произвести загрузку компьютера с жесткого диска обычным способом. С помощью диска скорой антивирусной помощи вы можете не только очистить свой компьютер от инфицированных и подозрительных файлов, но и попытаться вылечить зараженные объекты.

Dr.Web LiveCD поставляется в виде загрузочного диска с переносной операционной системой на базе Linux и встроенным программным обеспечением, предназначенным для проверки и лечения компьютера, работы с файловой системой, просмотра и редактирования текстовых файлов, просмотра веб-страниц и ведения электронной переписки.

Таким образом, **Dr.Web LiveCD** обеспечивает доступ к ресурсам компьютера как в случае невозможности загрузить его с жесткого диска, так и в нормальных ситуациях, обеспечивая удобный настраиваемый интерфейс (подробнее об этом варианте использования продукта см. Создание загрузочного флеш-накопителя для **Dr.Web LiveCD**).

Dr.Web LiveCD загружается в одном из двух режимов:

- в обычном режиме с графическим интерфейсом;
- в текстовом режиме (advanced mode) с интерфейсом командной строки (консольный сканер).

Обычный режим является предпочтительным в силу большей наглядности и функциональности. Именно работе в графической оболочке посвящена основная часть руководства. Тектовый режим предназначен для более опытных пользователей, хорошо знакомых с Unix-подобными операционными системами, и используется при невозможности запуска режима с графическим интерфейсом. Работа с консольной оболочкой описана в последнем разделе

руководства.

1.1. Антивирусная защита Dr.Web

Dr.Web® LiveCD - это антивирусное решение для восстановления системы, приведенной в нерабочее состояние в результате действий вирусов или какого-либо вредоносного ПО. Чтобы защитить систему от возникновения подобных ситуаций, необходима постоянная надежная защита с использованием передовых антивирусных технологий.

Передовые технологии компании **«Доктор Веб»** позволяют организовать надежную антивирусную защиту как в рамках крупных корпоративных сетей, так и на домашнем компьютере или в домашнем офисе. Решения **Dr.Web** отличаются исключительной нетребовательностью к ресурсам компьютера, компактностью, быстротой работы и надежностью в обнаружении всех видов вредоносных программ.

Среди продуктов компании **«Доктор Веб»** для постоянной защиты от вирусов, вредоносного ПО и спама присутствуют такие решения, как:

- защита корпоративных сетей (**Dr.Web Enterprise Security Suite**)
- защита рабочих станций (**Dr.Web Security Space 6.0**, **Dr.Web для Windows 6.0**, **Dr.Web для Linux**, **Консольные сканеры Dr.Web**);
- защита файловых серверов (**Dr.Web для Windows**, **Dr.Web для UNIX**, **Dr.Web для Novell NetWare**);
- защита почты (**Dr.Web для MS Exchange**, **Dr.Web для IBM Lotus Domino**, **Dr.Web для UNIX**, **Dr.Web для MIMEsweeper**);
- защита SMTP-шлюзов (**Dr.Web Mail Gateway**);
- защита интернет-шлюзов (**Dr.Web для Unix**);
- защита мобильных устройств (**Dr.Web для Windows Mobile**)
- интернет-услуга для провайдеров (**Dr.Web AV-Desk**).

Дополнительную информацию о продуктах компании можно получить на официальном сайте **Dr.Web**.

1.2. Системные требования

Для запуска антивирусного решения **Dr.Web LiveCD** минимальными необходимыми требованиями являются:

- процессор i386;
- 256 МБ оперативной памяти (512 МБ если нет возможности использовать виртуальную память на жестком диске);
- CD-ROM, DVD-ROM или флеш-накопитель с объемом памяти не менее 200 МБ.

1.3. Запуск Dr.Web LiveCD

Убедитесь, что ваш компьютер загружается в первую очередь с CD-привода, в котором находится диск **Dr.Web LiveCD**, либо с другого носителя, на котором записан **Dr.Web LiveCD**. При загрузке на экран выводится меню, в котором пользователю предоставляется возможность выбора режима запуска.

С помощью стрелок на клавиатуре выберите один из следующих вариантов загрузки и нажмите ENTER:

- чтобы запустить версию **Dr.Web LiveCD** с графическим интерфейсом, выберите обычный режим загрузки **Dr. Web-LiveCD (Default)**;
- чтобы запустить **Dr.Web LiveCD** в текстовом режиме (консольный сканер), выберите режим **DrWeb-LiveCD (Advanced)**;
- выберите **Start Local HDD**, если вы желаете загрузить компьютер с жесткого диска и не запускать **Dr.Web LiveCD** (отменить запуск **Dr.Web LiveCD**, произвести загрузку системы 0 раздела 0 диска (hd0,0));

- для проверки памяти (например, если машина работает крайне нестабильно, в случайный момент времени перегружается) выберите вариант **Testing Memory**.

Нажав на клавишу TAB, вы сможете отредактировать каждый из способов загрузки вручную.

2. Графическая оболочка Dr.Web LiveCD

Программный продукт **Dr.Web® LiveCD** содержит графическую оболочку с оконным интерфейсом, аналогичную GUI ОС Linux (рис 1).

На рабочем столе с заставкой в виде фирменного знака **Dr.Web** по умолчанию располагаются значки приложений, входящих в состав **Dr.Web LiveCD**.

На панели задач (горизонтальная панель в нижней части экрана) размещаются:

- кнопка открытия системного меню  ;
- значки быстрого запуска встроенных приложений;
- значки для переключения между рабочими столами;
- значки открытых в данный момент приложений;
- системные часы (в правом углу).

В состав **Dr.Web LiveCD** входят следующие основные приложения:

- **Антивирус Dr.Web для Linux**;
- браузер **Firefox**;
- почтовый клиент **Sylpheed**;
- файловый менеджер **Midnight Commander**;
- терминал для работы с командной строкой непосредственно из-под графической оболочки;

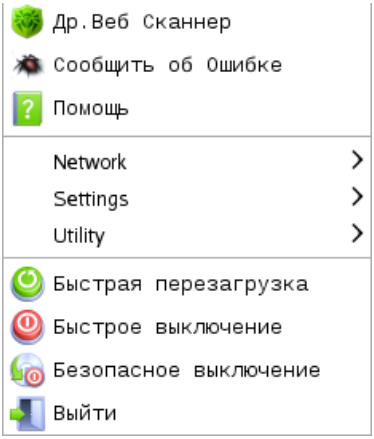
- текстовый редактор **Leafpad**.

Рисунок 1. Графическая оболочка.

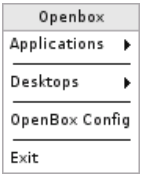
Запуск основных компонентов можно осуществить одним из следующих способов:

- при помощи двойного нажатия левой кнопкой мыши по значку соответствующего компонента на рабочем столе (по умолчанию на рабочий стол вынесены основные компоненты оболочки);
- при помощи одиночного нажатия левой кнопкой мыши по значку соответствующего компонента в панели задач (кроме файлового менеджера и **Сканера Dr.Web для Linux**);
- выбрав требуемый компонент в системном меню оболочки.

Системное меню открывается при нажатии на кнопку на панели задач.



Контекстное меню **Openbox** рабочего стола открывается нажатием правой кнопки мыши.



2.1. Антивирус Dr.Web

При загрузке **Dr.Web LiveCD** в графическом режиме автоматически будет запущен **Центр Управления Dr.Web для Linux** (рис. 2).

С помощью **Центра Управления** вы можете:

- проверить вашу систему с помощью **Сканера Dr.Web**;
- обезвредить обнаруженные угрозы или поместить подозрительные файлы в Карантин;
- настроить параметры сканирования и автоматической обработки обнаруженных угроз;

- обновить вирусные базы;
- просмотреть полный отчет о сканировании вашей системы.

Монитор **SpIDer Guard**, уведомления и одновременное использование несколькими пользователям не поддерживаются.

Чтобы узнать все подробности об использовании **Антивируса Dr.Web для Linux**, обратитесь к справке программы.

Для обеспечения максимальной эффективности сканирования **Антивирус** обновляет вирусные базы автоматически. Обратите внимание, что для обновления вирусных баз требуется доступ в Интернет. Подробности настройки сетевого подключения приведены в разделе Конфигурация сети.

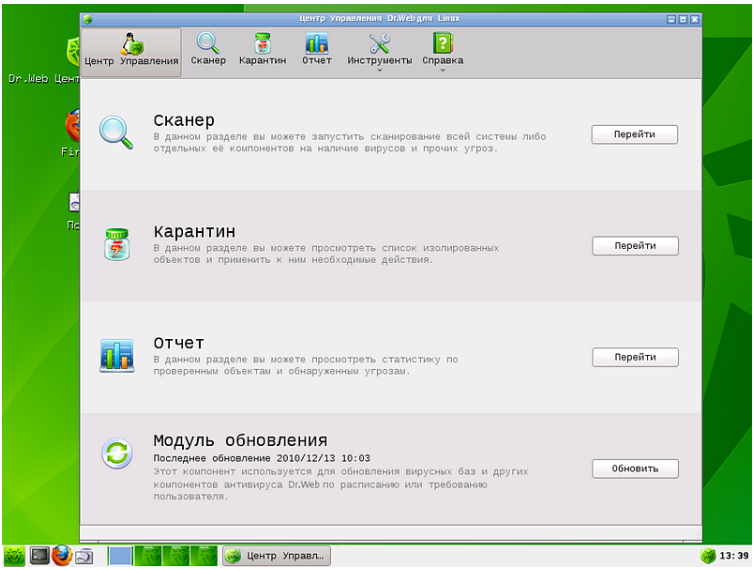


Рисунок 2. Центр управления Dr.Web для Linux.

2.2. Настройки

Настройки программы **Dr.Web LiveCD** доступны через пункт **Settings** системного меню и включают следующие опции:

- Внешний Вид - настройка параметров графической оболочки;
- Графические настройки - настройка X Window System;
- Конфигурация Меню - настройка панели задач графической оболочки;
- Конфигурация Сети - настройка сетевых взаимодействий;

Чтобы задать настройки, выберите соответствующий пункт меню. Откроется окно настроек.

2.2.1. Внешний вид

Эти настройки позволят вам указать параметры графической оболочки Openbox: цветовые темы, рабочий стол и т.п. (рис. 3)

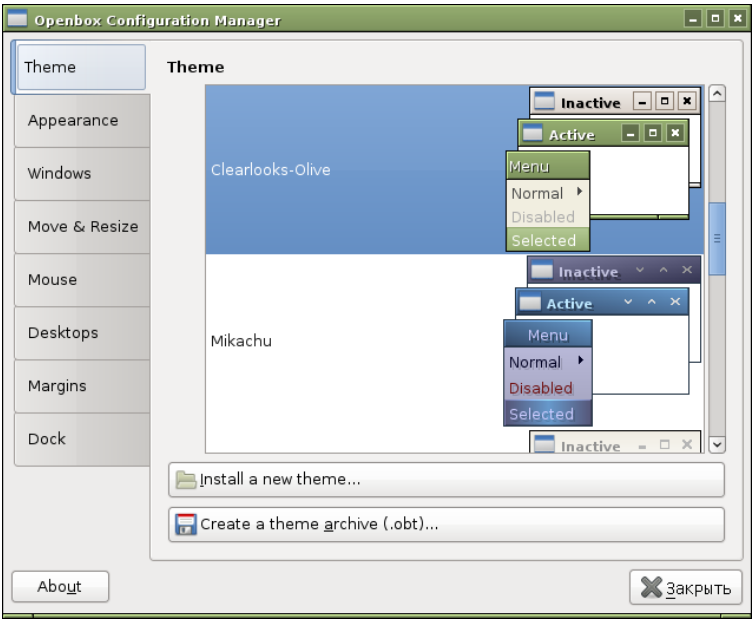


Рисунок 3. Окно настроек графической оболочки.

2.2.2. Графические настройки

Эти настройки позволят вам указать параметры системы X Window (разрешение экрана, тип видеодрайвера, тип мыши, клавиши переключения раскладки клавиатуры) (рис. 4).

Рисунок 4. Окно настроек X Window System.

2.2.3. Конфигурация меню

Эти настройки позволят вам выбрать положение, размер и специальный эффекты отображения панели задач (вкладка **General**, рис. 5), а также задать настройки модулей установленных расширений для графической оболочки (вкладка **Plugins**).

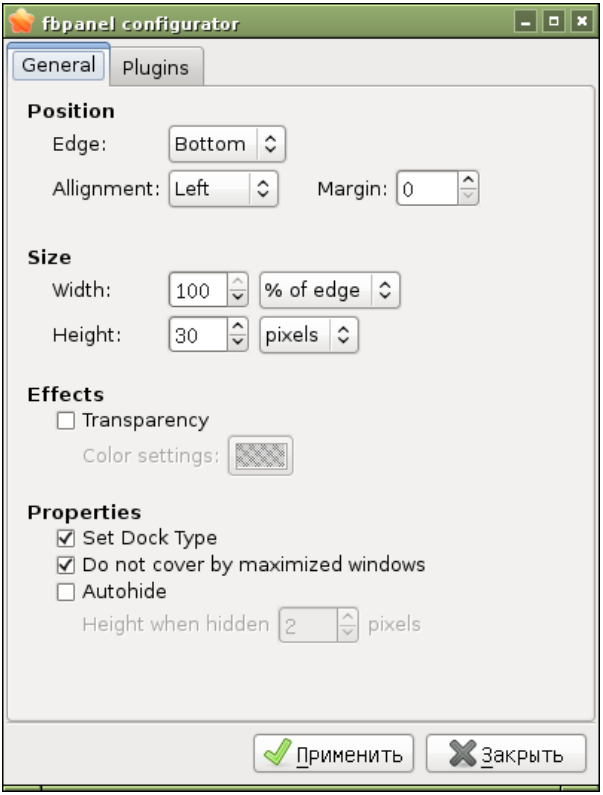


Рисунок 5. Окно настроек панели задач.

Настройка	Комментарий
Position	Задайте следующие параметры: • положение панели на экране (**Edge**) - слева (**Left**), справа (**Right**), вверху (**Top**), внизу (**Bottom**); • выравнивание элементов панели (**Allignment**) - по левому краю (**Left**), по правому краю (**Right**), по центру (**Center**) • отступ от края рабочего стола (**Margin**) в пикселях.
Size	Задайте размер панели: • ширину (**Width**) в процентах от ширины рабочего стола (% of edge), пикселях (**pixel**) или (**dynamic**); • высоту (**Height**) в пикселях (**pixel**).
Effects	Задайте эффекты отображения панели: • прозрачность (**Transparency**) и соответствующие цветовые настройки (**Color settings**).
Properties	Задайте прочие настройки: • использование док панели (**Set Dock Type**); • положение поверх всех окон (**Do not cover by maximized windows**); • автоматическое сокрытие панели (**Autohide**) и размер в скрытом состоянии в пикселях.

2.2.4. Конфигурация сети

Эти настройки позволят вам задать параметры подключения к сети вручную, или получить их через DHCP (рис. 6).

Рисунок 6. Окно настроек сети.

2.3. Встроенные приложения

В данном разделе описываются приложения, входящие в состав **Dr.Web LiveCD**. Доступ к ним осуществляется с помощью пунктов **Network** и **Utility** системного меню.

Пункт системного меню **Utility** открывает выпадающий список:

- Create Live USB - создать загрузочный флеш-накопитель;
- **Leafpad** - открыть встроенный текстовый редактор (блокнот);
- Midnight Commander - открыть файловый менеджер;
- **Terminal** - открыть терминал командной строки.

Пункт системного меню **Network** открывает выпадающий список:

- Firefox - открыть встроенный браузер;
- Sylpheed - открыть встроенный почтовый клиент.

2.3.1. Браузер

Несмотря на невозможность загрузить компьютер с жесткого диска, интернет-браузер Mozilla Firefox, включенный в состав **Dr.Web LiveCD**, позволит вам просматривать веб-сайты и сохранять просмотренные страницы (рис. 7). Сохраненные страницы можно будет просмотреть после полного восстановления и загрузки ОС.

Для доступа к веб-страницам посредством встроенного браузера потребуется наличие выхода в Интернет через локальную сеть (Local Area Network connection).

По умолчанию в окне браузера загружается официальный сайт компании **«Доктор Веб»**.

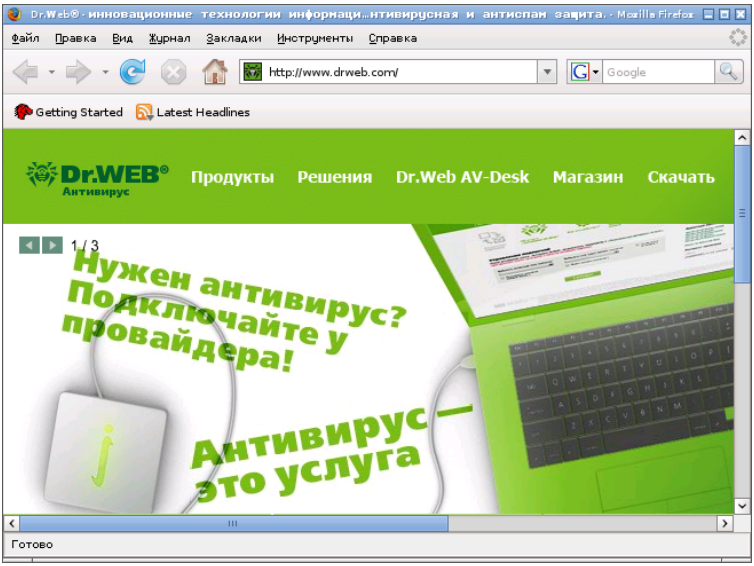


Рисунок 7. Встроенный браузер.

2.3.2. Почтовый клиент

При помощи встроенного почтового клиента **Sylpheed** (рис. 8) вы сможете вести полноценную переписку по электронной почте.

Для работы с данным почтовым клиентом изначально настроена учетная запись на сервере `mail.drweb.com`, через которую вы можете отправлять сообщения. Можно создать дополнительные учетные записи для ведения переписки.

Для создания новой учетной записи выберите меню **Настройка -> Создать новую учетную запись**. Введите всю необходимую для отправки почты информацию: адрес электронной почты отправителя, параметры для отправки (протокол SMTP) и получения (протокол POP3) почты, а также сопроводительную информацию.

Для обращения к нескольким учетным записям можно создать отдельные почтовые ящики. Для этого выберите меню **Файл** -> **Почтовый ящик** -> **Добавить почтовый ящик**. В свойствах почтового ящика необходимо указать, какая учетная запись будет использоваться: в контекстном меню ящика выбрать **Свойства** -> вкладка **Написать** -> выпадающий список **Учетная запись** -> указать требуемую запись.

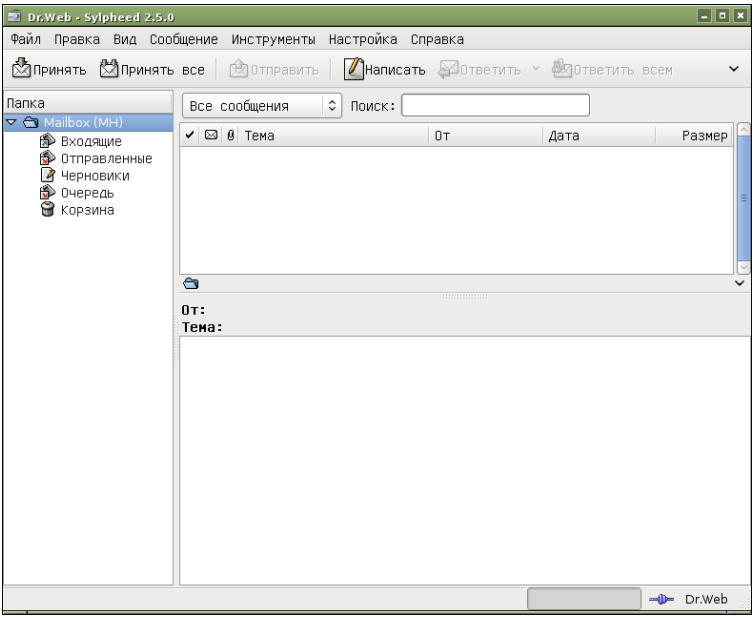


Рисунок 8. Почтовый клиент.

Sylpheed обеспечивает безопасное соединение с почтовым сервером, поддерживая шифрование соединения через протоколы SSL и TLS.

В случае невозможности загрузить ОС с жесткого диска и, соответственно, использования привычных программ, этот почтовый клиент в составе **Dr.Web LiveCD** позволит вам получать и отправлять письма через вашу электронную почту до полного устранения проблемы.

2.3.3. Файловый менеджер

Встроенный файловый менеджер **Midnight Commander** (рис. 9) аналогичен файловому менеджеру Norton Commander. Используя полноэкранный режим изображения, **Midnight Commander** предоставляет операционной системе интуитивный пользовательский интерфейс и является полезным инструментом для работы с файлами как для опытных пользователей, так и для начинающих.

Домашняя страница проекта: http://www.ibiblio.org/mc/.

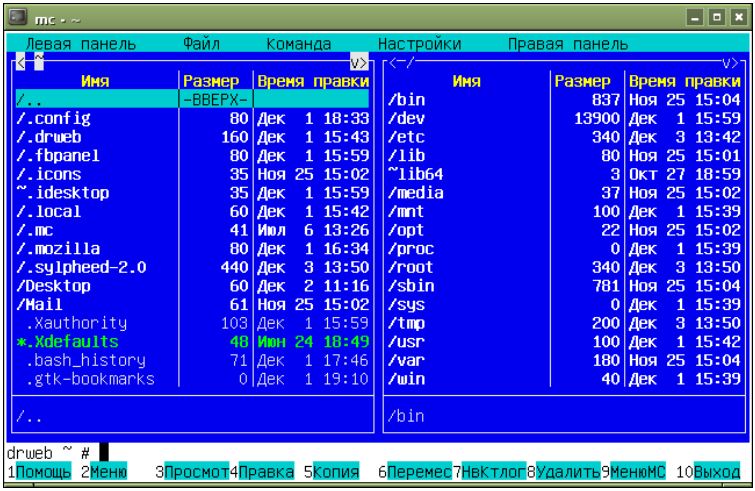


Рисунок 9. Файловый менеджер.

3. Работа в текстовом режиме

В текстовом режиме вы можете сканировать вашу систему из командной строки. Этот режим потребляет меньше системных ресурсов и позволяет использовать снапшоты.

3.1. Снапшоты

С помощью снапшотов вы можете сохранять все изменения, файлы отчета и временные файлы, создаваемые при сканировании системы, на локальных дисках или флеш-накопителях. Использование снапшотов позволяет снизить нагрузку на системные ресурсы и избежать сбоев при сканировании больших архивов.

В графическом режиме снапшоты не используются и **Dr.Web LiveCD** сохраняет все настройки и временные файлы только в оперативной памяти.

При загрузке LiveCD в текстовом режиме доступные диски будут автоматически проверены на наличие снапшотов и вам будет предложено выбрать снапшот или создать новый (рис. 10).

Если при загрузке не обнаружено доступных разделов диска или флеш накопителей, список снапшотов выводится не будет.

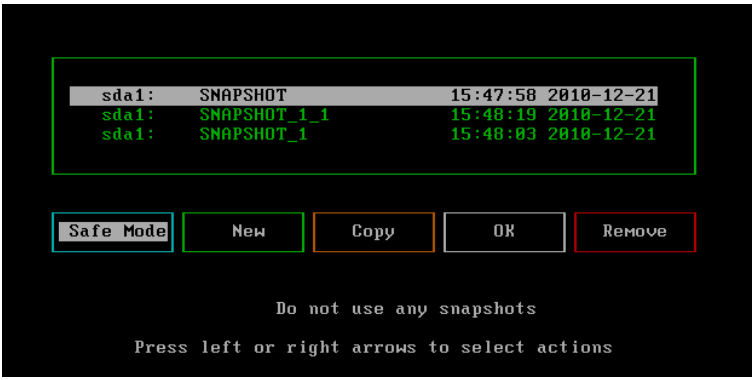


Рисунок 10. Список снапшотов.

Используйте клавиши ВВЕРХ и ВНИЗ для выбора снапшота. Клавиши ВЛЕВО и ВПРАВО для выбора действий. Доступные действия:

- **Safe Mode** - загрузить **LiveCD** без поддержи снапшотов;
- **New** - создать новый снапшот;
- **Copy** - скопировать выбранный снапшот в другой раздел;
- **OK** - загрузить **LiveCD** с использованием выбранного снапшота;
- **Remove** - удалить выбранный снапшот;

Чтобы создать новый снапшот

- загрузитесь с **Dr.Web LiveCD** в тектовом режиме;
- выберите **Add snapshot** в меню выбора снапшота;
- выберите раздел, на котором будет размещен новый снапшот (рис. 11);

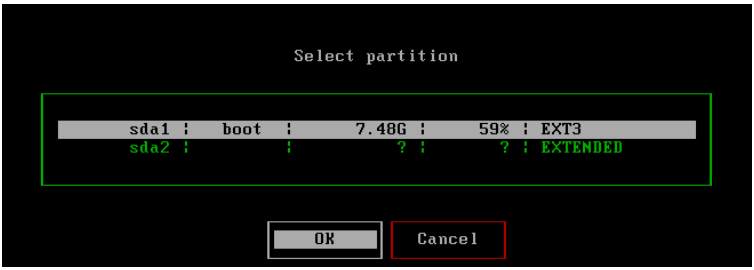


Рисунок 11. Выбор раздела.

- укажите имя снапшота (рис. 12).

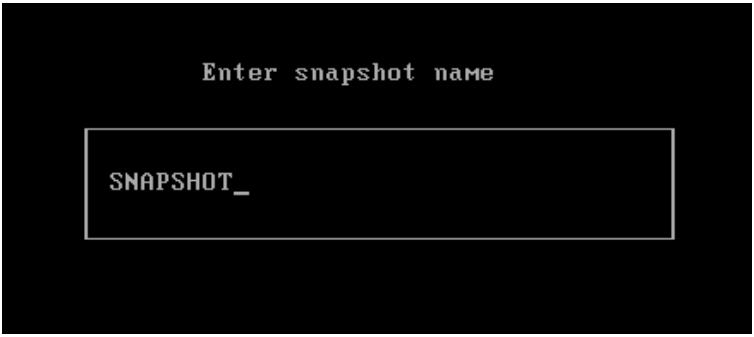


Рисунок 12. Имя снапшота.

3.2. Запуск процесса сканирования

После загрузки **Dr.Web LiveCD** в текстовом режиме на экран выводится главное меню запуска - **Стартовое Меню** (рис. 13).

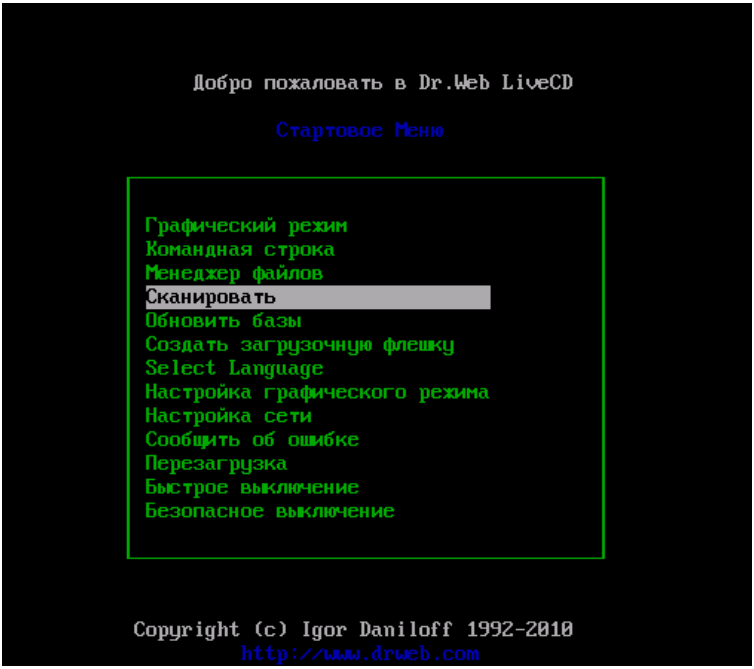


Рисунок 13. Стартовое меню.

С помощью стрелок на клавиатуре выберите нужный пункт меню и нажмите **ENTER**:

- **Графический режим** - загрузить графический интерфейс **Dr.Web LiveCD**;
- **Командная строка** - вывести на экран командную строку;
- **Менеджер файлов** - запустить встроенный файловый менеджер Midnight Commander;
- **Сканировать** - сканировать все разделы жесткого диска с

настройками по умолчанию;

- **Обновить базы** - обновить вирусные базы данных;
- **Select Language** - изменить язык интерфейса;
- **Настройка графического режима** - настроить графический режим, если автоматическое конфигурирование графической оболочки не сработало или сработало неверно;
- **Настройка сети** - настроить сеть, если автоматичекое конфигурирование сети не сработало или сработало неверно;
- **Сообщить об ошибке** - отправить разработчикам информацию об ошибке в ПО;
- **Перезагрузка** - перезагрузить компьютер;
- **Быстрое выключение** - выключить компьютер, не извлекая диска LiveCD;
- **Безопасное выключение** - извлечь диск и завершить работу компьютера.

Если вы желаете сканировать с особыми настройками, то выберите пункт **Командная строка**. В нижней части экрана появится командная строка. Общий формат запуска сканирования следующий:

```
$ /opt/drweb/drweb <путь> [параметры командной строки]
```

где *<путь>* — путь к проверяемой директории или маска проверяемых файлов.

Сканер, запущенный без параметров, только с указанием пути в качестве аргумента, осуществляет проверку указанной директории, используя набор параметров по умолчанию. В следующем примере показано, как в командной строке запустить проверку диска **C:** с настройками по умолчанию:

```
$ /opt/drweb/drweb /mnt/disk/sda1
```

Файлы отчета находятся в директории `/var/drweb/log/`:

- `drweb.log` - файл отчета **Сканера**;
- `updater.log` - файл отчета утилиты обновления;

3.3. Параметры командной строки

Сканер Dr.Web может быть настроен с помощью многочисленных параметров командной строки. Они отделяются от указания пути пробелом и начинаются с символа «-» (дефис). Полный список параметров командной строки можно получить, запустив программу `drweb` с параметрами `-?`, `-h` или `-help`.

Основные параметры программы могут быть сгруппированы следующим образом:

- параметры области проверки
- параметры диагностики
- параметры действий
- параметры интерфейса

Параметры области проверки указывают, где следует проводить проверку на вирусы. К ним относятся:

- `path` - задание пути для сканирования. В одном параметре может быть задано несколько путей;
- `@[+]<файл>` - проверка объектов, перечисленных в указанном файле. Символ «+» (плюс) предписывает не удалять файл со списком объектов по окончании проверки. Этот файл может содержать пути к периодически проверяемым директориям или просто список подлежащих регулярной проверке файлов;
- `sd` - рекурсивный поиск и проверка файлов в поддиректориях, начиная с текущей;
- `fl` - указание следовать символическим ссылкам, как для файлов, так и для директорий. Ссылки, приводящие к «зацикливанию», игнорируются;
- `mask` - указание игнорировать маски имен файлов.

Параметры диагностики, определяющие, какие типы объектов должны проверяться на вирусы:

- `al` - диагностика всех файлов на заданном устройстве или в указанной в качестве аргумента директории;
- `ar[ d/m/r][ n]` - проверка файлов в архивах (ARJ, CAB, GZIP, RAR, TAR, ZIP и др.).
  `d` - удаление, `m` - перемещение, `r` - переименование архивов, содержащих зараженные объекты; `n` - отключение вывода имен архиваторов.
  Под архивами в данном случае понимаются не только собственно архивы (например, вида `*.tar`), но и их сжатые формы (в частности, сжатые TAR-архивы вида `*.tar.bz2` и `*.tbz`);
- `cn[ d/m/r][ n]` – проверка файлов в контейнерах (HTML, RTF, PowerPoint).
  `d` - удаление, `m` - перемещение, `r` - переименование контейнеров, содержащих зараженные объекты; `n` - отключение вывода типа контейнера;
- `ml[ d/m/r][ n]` - проверка файлов почтовых программ.
  `d` - удаление, `m` - перемещение, `r` - переименование файлов почтовых программ, содержащих зараженные объекты; `n` - отключение вывода типа файлов почтовых программ;
- `up[ n]` – проверка исполняемых файлов, упакованных LZEXE, DIET, PKLITE, EXEPACK;
  `n` – отключение вывода имен утилит упаковки;
- `ex` - диагностика файлов, имена которых соответствуют заданным маскам (см. параметр конфигурационного файла `FilesTypes`);
- `ha` - эвристический анализ файлов, поиск неизвестных вирусов.

Параметры действия определяют, какие манипуляции должны быть выполнены в отношении зараженных (или подозрительных) файлов:

- `cu[ d/m/r]` - лечение зараженных файлов. Дополнительные параметры: `d` - удаление, `m` – перемещение, `r` – переименование зараженных файлов;
- `ic[ d/m/r]` - действия для неизлечимых файлов: `d` –

удаление, m - перемещение, r - переименование неизлечимых файлов;

- sp[d/m/r] – действия для подозрительных файлов: d - удаление, m - перемещение, r - переименование подозрительных файлов;
- adw[d/m/r/i] – действия для файлов, содержащих рекламные программы: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- dls[d/m/r/i] - действия для файлов, содержащих программы дозвона: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- jok[d/m/r/i] - действия для файлов, содержащих программы-шутки: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- rsk[d/m/r/i] - действия для файлов, содержащих потенциально опасные программы: d - удаление, m - перемещение, r - переименование, i - игнорирование;
- hck[d/m/r/i] - действия для файлов, содержащих программы, используемые для взлома: d - удаление, m - перемещение, r - переименование, i - игнорирование.

Параметры интерфейса определяют условия вывода результатов работы программы:

- v, version - вывод информации о версии продукта и версии антивирусного ядра;
- ki - вывод информации о ключе и его владельце (только в кодировке UTF8);
- foreground[yes| no] - запуск **Сканера** в приоритетном или в фоновом режиме;
- ot - вывод информации на stdout, то есть стандартный вывод;
- oq - отключение вывода информации;
- ok - вывод сообщения «Ok» для не зараженных вирусами файлов;
- log=<путь к файлу> - запись отчета о работе в указанный файл;

- `ini=<путь к файлу>` - использование альтернативного конфигурационного файла;
- `lng=<путь к файлу>` - использование альтернативного языкового файла.

Некоторые из параметров отменяют соответствующее им действие, если оканчиваются символом «-» (дефис). К ним относятся следующие параметры:

```
-ar -cu -ha -ic -fl -ml -ok -sd -sp
```

Например, при запуске **Сканера** командой вида:

```
$ drweb -path <путь> -ha-
```

проверка будет производиться без эвристического анализа файлов, который обычно по умолчанию включен.

Если не производились действия по перенастройке программы, то по умолчанию (то есть без отдельного указания параметров) **Сканер** запускается с параметрами:

```
-ar -ha -fl- -ml -sd
```

Этот набор параметров по умолчанию (включающий проверку архивов и упакованных файлов, файлов почтовых программ, рекурсивный поиск, эвристический анализ и т.д.) достаточно целесообразен для целей диагностики и может использоваться в большинстве типичных случаев. Если какой-либо из параметров по умолчанию не нужен в конкретной ситуации, его можно отключить, указав после него символ «-» (дефис), как это было показано выше на примере параметра `-ha` (эвристический анализ).

Следует добавить, что отключение проверки архивированных и упакованных файлов резко снижает уровень антивирусной защиты, т.к. именно в виде архивов (часто самораспаковывающихся) распространяются файловые вирусы в виде почтовых вложений. Документы прикладных программ, потенциально подверженные заражению макровирусами (Word, Excel и др.), также обычно пересылаются по электронной почте в архивированном и упакованном виде.

При запуске **Сканера** с параметрами по умолчанию не осуществляется лечение зараженных файлов. Не предусмотрены также действия в отношении неизлечимых файлов и подозрительных файлов. Все эти действия требуют указания дополнительных параметров командной строки - параметров действия.

Наборы параметров действия могут различаться в каждом конкретном случае, однако обычно представляются целесообразными следующие:

- `cu` - лечение зараженных файлов и системных областей, без удаления, перемещения или переименования зараженных файлов;
- `icd` - удаление неизлечимых файлов;
- `spm` - перемещение подозрительных файлов;
- `spr` - переименование подозрительных файлов.

Запуск **Сканера** с параметром лечения означает, что программа предпримет попытку восстановить состояние зараженного объекта. Это возможно только тогда, когда обнаружен известный вирус, причем необходимые инструкции по излечению имеются в вирусных базах, однако и в этих случаях попытка излечения может не быть успешной, например, если зараженный файл уже серьезно поврежден.

Если при проверке архивов в их составе были обнаружены зараженные файлы, лечение последних, как и удаление, перемещение или переименование, не производится. Для уничтожения вирусов в таких объектах архивы должны быть вручную распакованы соответствующими программными средствами, желательно, в отдельную директорию, которая и будет указана как аргумент при повторном запуске **Сканера**.

При запуске с параметром удаления программа уничтожит зараженный файл на диске. Этот параметр целесообразен для неизлечимых (необратимо поврежденных вирусом) файлов.

Параметр переименования вызывает замену расширения имени файла на некое установленное (по умолчанию «`*.#??`», т.е. первый символ расширения заменяется символом «`#`»). Этот

параметр целесообразно применять для файлов других ОС (например, DOS/Windows), выявленных при эвристическом анализе как подозрительные. Переименование сделает невозможным случайный запуск исполняемых модулей в этих системах, загрузку документов Word или Excel без дальнейшей проверки и таким образом предотвратит заражение возможным вирусом и дальнейшее его распространение.

Параметр перемещения переместит зараженный (или подозрительный) файл в предназначенную для этого директорию карантина.

4. Создание загрузочного флэш-накопителя

Dr.Web LiveCD можно использовать как переносную операционную систему, настроенную под конкретные задачи пользователя, для доступа к данным любого компьютера независимо от установленных на нем ОС и ПО. Чтобы индивидуальные настройки, создаваемые в процессе сеанса работы в **Dr.Web LiveCD**, сохранялись, файлы **Dr.Web LiveCD** записываются на флеш-память. Для этого используется команда `CreateLiveUSB`.

Несмотря на то, что команда `CreateLiveUSB` не изменяет и не удаляет содержимое устройств, рекомендуется перед запуском команды сохранить все файлы используемого флеш-накопителя на другом носителе.

Для загрузки **Dr.Web LiveCD** запись продукта на CD-диск и наличие привода необязательны. Вы можете использовать виртуальную машину с эмулятором CD-привода.

Все файлы **Dr.Web LiveCD** записываются в директорию `/boot`. При необходимости, программа изменяет конфигурацию разделов на флеш-накопителе, оригинальная конфигурация сохраняется в файле `/boot/partition.backup`. Программа копирует MBR на флеш-накопитель, оригинальная главная загрузочная запись сохраняется в файле `/boot/mbr.backup` .

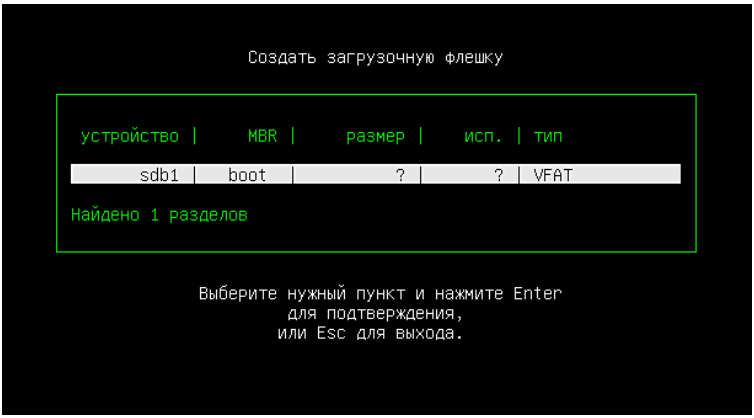


Рисунок 14. Меню Create LiveUSB.

Создание загрузочного флеш-накопителя автоматически:

1. Подключите флеш-накопитель. Регистрация события подключения занимает не больше десяти секунд.
2. В графической оболочке нажмите значок программы **Создать загрузочную флешку** на рабочем столе или наберите в консоли команду `create_usb`.
3. Программа **Create Live USB** сама определит все разделы на флеш-накопителе .
4. Выберите подходящий раздел (рис. 14) и нажмите клавишу ENTER.
5. Копирование файлов начнется автоматически.

5. Отправка сообщений об ошибке

Если вы работаете в графической оболочке, то для отправки сообщения об ошибке вам потребуется:

- перейти к секции основных настроек **Сканера** при помощи кнопки **Изменить установки** на панели инструментов или воспользовавшись меню **Настройка** -> **Настройки** главного окна **Сканера**;
- в секции основных настроек выбрать вкладку **Поддержка**;
- на этой вкладке нажать на кнопку **Сообщить об ошибке**;
- после этого будет запущен встроенный почтовый клиент, и откроется шаблон сообщения;
- в поле **Subject** письма изложите краткое описание проблемы, а в теле письма - дайте наиболее полное описание возникшей ошибки и шагов, приведших к ней;
- затем отправьте письмо, воспользовавшись учетной записью, настроенной по умолчанию.

Если вы работаете из консоли, то для отправки сообщения об ошибке воспользуйтесь следующим алгоритмом:

- с помощью стрелок на клавиатуре выберите в **Стартовом Меню** пункт **Сообщить об ошибке** и нажмите **ENTER**;
- откроется окно консольного текстового редактора nano, в котором вы сможете описать возникшую проблему;
- после того, как вы закончите с описанием проблемы, нажмите **CTRL+X** для выхода из редактора;
- перед выходом вам будет предложено выбрать, хотите ли вы отправить сообщение об ошибке, или нет (введите **Y**, если сообщение должно быть отправлено, и **N**, если вы не хотите отправлять сообщение).