Dr.WEB®
LiveCD

Защити созданное

Руководство пользователя

Антивирус Dr.Web LiveCD
Версия 5.0.0
Руководство администратора
20.02.2009

ООО "Доктор Веб", 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.

ООО "Доктор Веб"

ООО "Доктор Веб" - российский разработчик средств информационной безопасности.

Компания предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные продукты ООО "Доктор Веб" 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

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 компьютеров, 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 флэш-накопителя для Dr.Web LiveCD).

Dr.Web LiveCD загружается в одном из двух режимов:

- в обычном режиме с графическим интерфейсом;
- в безопасном режиме (safe 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. Безопасный режим предназначен для более опытных пользователей, хорошо знакомых с Unix-подобными системами, и используется при невозможности запуска режима с графическим интерфейсом. Работа с консольной оболочкой описана в последнем разделе руководства.

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 **Dr.Web®** 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 **Dr.Web** для постоянной защиты от вирусов, вредоносного ПО и спама присутствуют такие решения, как:

- защита корпоративных сетей (**Dr.Web Enterprise Suite**)
- защита рабочих станций (**Dr.Web Security Space 5.0**, **Dr.Web для Windows 5.0**, **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 ООО «Доктор Веб».

Системные требования

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

- процессор i386;
- 128 МБ оперативной памяти (64 МБ для работы в безопасном режиме);
- CD-ROM, DVD-ROM или флэш-накопитель с объемом памяти не менее 64 МБ.

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**;
- чтобы запустить **Dr.Web LiveCD** с интерфейсом командной строки (консольный сканер), выберите режим **DrWeb-LiveCD (Safe Mode)**;
- выберите **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 **Test Memory**.

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;
- системные часы (в правом углу).

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

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

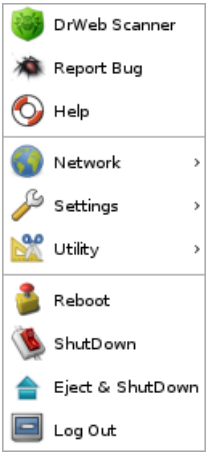
- текстовый редактор **Leafpad**.

Рисунок 1. Графическая оболочка.

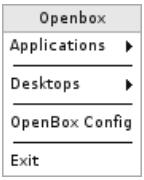
Запуск основных компонентов можно осуществить одним из следующих способов:

- 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.



Чтобы получить информацию о том, как пользоваться сканером **Dr.Web для Linux**, выберите пункт **Help** системного меню или в главном окне сканера выберите в меню **Help** пункт **Help**.

После запуска графической оболочки по умолчанию открывается главное окно **сканера Dr.Web для Linux**. С помощью **сканера Dr.Web для Linux** вы можете проверить на вирусы все корневые разделы ОС Windows.

Настройки

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

- Menu Configuration - настройка панели графической оболочки;
- NetWorks Configuration - настройка сетевых взаимодействий;
- Openbox Configuration Manager - настройка параметры графической оболочки.

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

Настройки панели

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

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 (**Margine**) в пикселах.
Size	Задайте размер панели: • ширину (**Width**) в процентах от ширины рабочего стола (% of edge), пикселах (**pixel**) или (**dynamic**); • высоту (**Height**) в пикселах (**pixel**).

Effects	Задайте эффекты отображения панели: • прозрачность (**Transparency**) и соответствующие цветовые настройки (**Color**).
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 пикселах.

Настройки сети

Эти настройки позволяют вам указать используемый сетевой интерфейс (**Interface**), задать параметры подключения к сети (вкладка **Static IP**) и указать путь к конфигуационным файлам сети (вкладка **System wide**).

Настройка сети

1. В окне настроек сети задайте интерфейс (**Interface**), используемый для подключения.
2. На вкладке **Static IP** задайте следующие настройки:

Настройка	Комментарий
Host	Имя компьютера.
IP	IP-адрес компьютера.
Netmask	Маска подсети.
Gateway	Шлюз.
Name server	Сервер имен.
Use DHCP	Выберите эту опцию, чтобы получать настройки сети автоматически с использованием протокола DHCP.

3. Чтобы сохранить изменения, нажмите кнопку **Update**. Чтобы выключить сеть, нажмите **Stop**.

4. На вкладке **System wide** задайте пути к конфигурационным файлам сети.

Чтобы открыть файл для редактирования, нажмите кнопку справа от поля ввода.

5. Чтобы перезапустить сеть, нажмите кнопку **Restart**.
6. Для выхода из окна настроек нажмите кнопку **Exit**.

Настройки графической оболочки

Эти настройки позволяют вам указать параметры графической оболочки Openbox (цветовые темы, рабочий стол и т.п.).

Сканирование файловой системы

Данный раздел описывает процесс сканирования файловой системы компьютера.

Запуск процесса сканирования

Перед началом сканирования рекомендуется обновить антивирусные базы. Для этого воспользуйтесь кнопкой в верхней части главного окна сканера.

Сканер Dr.Web® для Linux можно запустить следующими способами:

- автоматически после загрузки графической оболочки;
- при помощи значка на рабочем столе;
- при помощи соответствующего пункта системного меню.

После запуска сканера откроется главное окно программы (рис. 2).

Сканер позволяет проверять на вирусы все типы разделов, поддерживаемых операционной системой Windows (FAT, FAT32, NTFS). По умолчанию для проверки выбраны все доступные разделы жесткого диска.

По умолчанию сканируются все подкаталоги в выбранных каталогах. Если вам требуется проверка только файлов в отдельных указанных директориях и разделах диска, без содержимого вложенных каталогов (несмотря на то, что оно также может быть инфицировано), то снимите флажок **Scan subdirectories** (Сканировать подкаталоги).

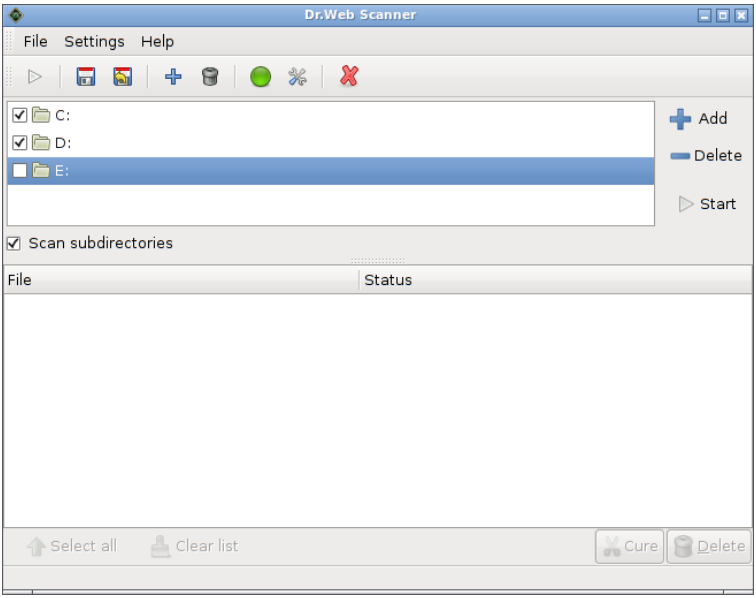


Рисунок 2. Главное окно программы.

Чтобы добавить или удалить объект из списка сканируемых объектов, используются кнопки **Add** (Добавить) и **Delete** (Удалить), либо клавиши **Insert** и **Delete** соответственно.

Кнопка **Delete** (Удалить) становится активной, если выбран какой-либо объект.

Чтобы исключить из проверки какой-либо объект, не удаляя его из списка сканируемых, достаточно снять флажок рядом с этим объектом.

При нажатии на кнопку **Add** (Добавить) открывается окно выбора объектов для сканирования.

Панель выбора пути (вверху) изначально содержит кнопки:

-  **Type a file name** - открыть поле ввода имени файла для добавления (для закрытия поля необходимо повторно нажать кнопку).
-  **File System** - открыть список разделов файловой системы **Dr.Web LiveCD**.
-  **Win** - открыть содержимое раздела операционной системы Windows.

В процессе просмотра объектов файловой системы на панели выбора пути (верхняя часть окна) появляется набор кнопок, соответствующих пройденным по порядку директориям («хлебные крошки»). При нажатии на кнопку осуществляется переход в соответствующую ей директорию.

Для добавления объектов в закладки для быстрого доступа выберите требуемые директории в проводнике файловой системы и нажмите кнопку **Add** (Добавить). Для удаления объектов из закладок выберите требуемые директории в списке **Places** (Пути) и нажмите кнопку **Remove** (Удалить).

После окончания выбора нажмите кнопку **OK** для подтверждения создания закладки и закрытия окна; кнопку **Cancel** (Отмена) - для закрытия окна без создания закладок.

Закладки файловой системы автоматически добавляются в список объектов для сканирования. В дальнейшем вы можете

использовать закладки для быстрой навигации по файловой системе.

Чтобы начать процесс сканирования выбранных объектов, нажмите на кнопку **Start** (Старт) (она превратится в кнопку **Stop** (Стоп) и начнется сканирование).

Во время сканирования текущее действие отображается на строке состояния в нижней части главного окна, например, загрузка вирусных баз или полный путь к сканируемому в данный момент файлу.

Чтобы остановить сканирование, нажмите кнопку **Stop** (Стоп) (она превратится в кнопку **Start** (Старт) и сканирование прекратится).

Перед началом сканирования можно установить дополнительные параметры проверки, например: режим проверки (степень тщательности), действия над обнаруженными объектами и др. Более подробную информацию о настройках сканера можно получить в разделе Основные настройки сканера.

Результаты сканирования

Результаты сканирования отображаются в виде таблицы (рис. 3) внизу главного окна сканера. Там представлены сведения о найденных в ходе сканирования инфицированных и подозрительных объектах, их статусе, пути, а также о действиях, произведенных программой над этими объектами.

Список обнаруженных объектов отображается в виде иерархической структуры. Так, если обнаружен вирус в архиве, то инфицированный архив будет показан в окне отчета в виде узла, который можно свернуть или развернуть для отображения его содержимого.

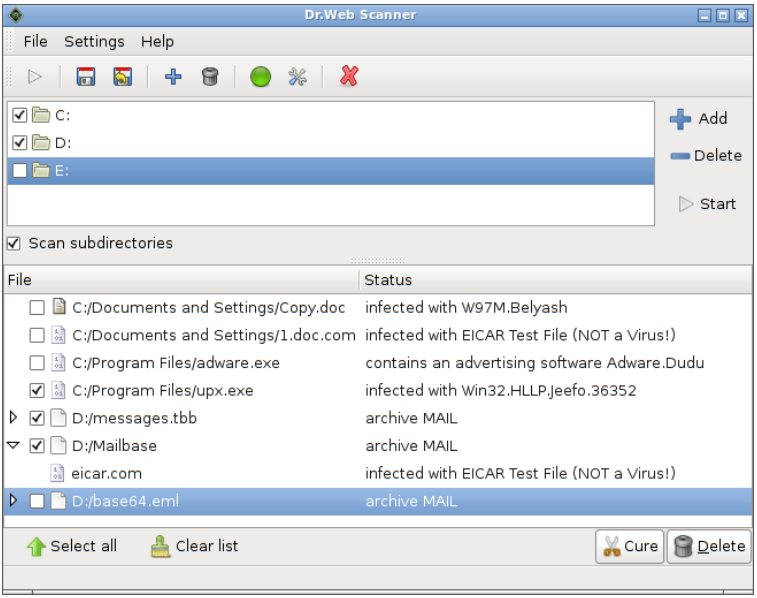


Рисунок 3. Результаты сканирования.

На нижней панели, расположенной под окном отчета, для каждого объекта при помощи соответствующих кнопок выбирается желаемое действие: **Cure** (Лечить) или **Delete** (Удалить). Действие **Cure** (Лечить) недоступно для архивов, контейнеров и почтовых файлов.

Если на вкладке Действия настроек сканера в настройках действий для данного типа обнаруженных объектов было задано действие, отличное от информирования, то в столбце **Status** (Статус) будет отображаться результат произведенных действий.

При выборе варианта **Cure** (Лечить), если файл окажется неизлечимым, выполняется действие, указанное для неизлечимых объектов на вкладке Действия настроек сканера.

Для того чтобы вручную произвести необходимые действия с обнаруженным объектом, установите флажок напротив имени этого объекта (или нажмите кнопку **Select all** (Выбрать все), чтобы пометить все обнаруженные объекты) и нажмите одну из кнопок: **Cure** (Лечить) или **Delete** (Удалить).

Настройки сканера

В данном разделе описываются настройки сканера.

Основные настройки сканера

Доступ к основным настройкам сканера осуществляется при помощи кнопки  (Настройки) на панели инструментов или в меню **Settings** -> **Options** (Настройки -> Опции) главного окна сканера. В данном окне настраивается интерфейс программы, реакция на обнаружение инфицированных и подозрительных объектов, а также параметры ее взаимодействия с ОС и различными программами антивирусного комплекса.

Основные настройки сканера делятся на несколько вкладок:

- Genera (Общие) - общие настройки сканера;
- Actions (Действия) - настройка реакции программы при обнаружении вирусных угроз или какого-либо вредоносного ПО;
- Checking (Проверка) - настройка режима проверки файлов сканером, сохранение текущих настроек/восстановление настроек по умолчанию;
- Programs (Программы) - настройка параметров взаимодействия с компонентами антивирусного комплекса и другими программами;
- Support (Поддержка) - обновления и техническая поддержка.

В нижней части окна основных настроек сканера расположены кнопки управления:

- **Set default** (Установить по умолчанию) - сбросить пользовательские изменения настроек и вернуть настройки по умолчанию;
- **OK** - сохранить настройки и вернуться в главное окно сканера;
- **Apply** (Применить) - сохранить настройки и остаться в окне настроек;
- **Cancel** (Отмена) - вернуться в главное окно сканера без сохранения изменения настроек.

Вкладка Общие

Окно основных настроек по умолчанию открывается на вкладке **General** (Общие) (рис. 4).

В верхней части этой вкладки задается путь к сканеру. Для этого необходимо ввести путь в поле ввода **Path to Scanner** (Путь к сканеру) или нажать на кнопку  и выбрать его в проводнике по файловой системе. Аналогично, при необходимости, задайте путь к файлу лицензионного ключа сканера в поле **Path to key** (Путь к ключу) в нижней части вкладки.

Как правило, указанный по умолчанию путь к сканеру указан корректно и в редактировании не нуждается.

Для того чтобы измененные настройки сохранялись в конфигурационном файле только при нажатии на кнопку **Save Settings** (Сохранить настройки) (см. раздел Вкладка Проверка), снимите флажок **Save all settings at exit** (Сохранять все настройки при выходе). По умолчанию флажок установлен, при этом настройки сохраняются при каждом закрытии главного окна сканера.

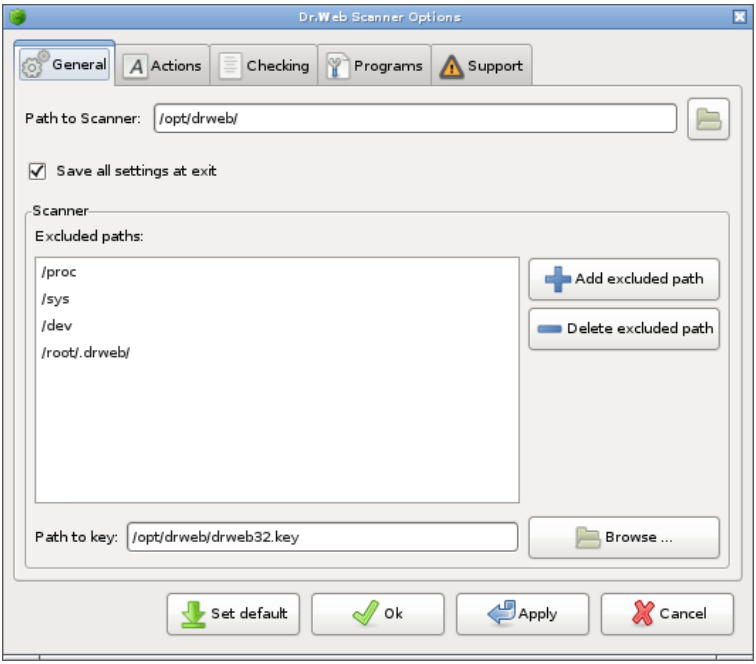


Рисунок 4. Вкладка General..

Вы можете задать список исключаемых из сканирования путей. Для того чтобы добавить в список какую-либо директорию, нажмите на кнопку **Add excluded path** (Добавить исключаемый путь). Откроется окно выбора пути.

Панель выбора пути (вверху) изначально содержит кнопки:

- **Type a file name** - открыть поле ввода имени файла для добавления (для закрытия нажмите кнопку повторно);
- **File System** - открыть список разделов файловой системы **Dr.Web LiveCD;**
- **Win** - открыть содержимое раздела ОС Windows.

В процессе просмотра объектов файловой системы на панели выбора пути (верхняя часть окна) появляется набор кнопок, соответствующих пройденным по порядку директориям («хлебные крошки»). При нажатии на кнопку осуществляется переход в соответствующую ей директорию.

Для добавления объектов в закладки для быстрого доступа выберите требуемые директории в проводнике файловой системы и нажмите кнопку **Add** (Добавить). Для удаления объектов из закладок выберите требуемые директории в списке **Places** (Пути) и нажмите кнопку **Remove** (Удалить).

После окончания выбора нажмите кнопку **OK** для подтверждения создания закладки и закрытия окна; кнопку **Cancel** (Отмена) - для закрытия окна без создания закладок.

Закладки файловой системы автоматически добавляются в список исключаемых путей. В дальнейшем вы можете использовать закладки для быстрой навигации по файловой системе.

Для того чтобы удалить какой-либо путь из списка, выберите его в списке исключаемых путей и нажмите на кнопку **Delete excluded path** (Удалить исключаемый путь).

По окончании редактирования настроек нажмите на кнопку **Apply** (Применить), чтобы сохранить внесенные изменения, не закрывая окно основных настроек.

Вкладка Действия

На вкладке **Actions** (Действия) (рис. 5) настраивается реакция программы при обнаружении вирусных угроз или какого-либо вредоносного ПО.

По умолчанию для всех типов объектов установлено действие **Report** (Отчет). Информация обо всех обнаруженных объектах отображается в поле отчета главного окна (см. раздел Результаты сканирования). Пользователь может выбрать необходимые действия вручную, при помощи кнопок под полем отчета.

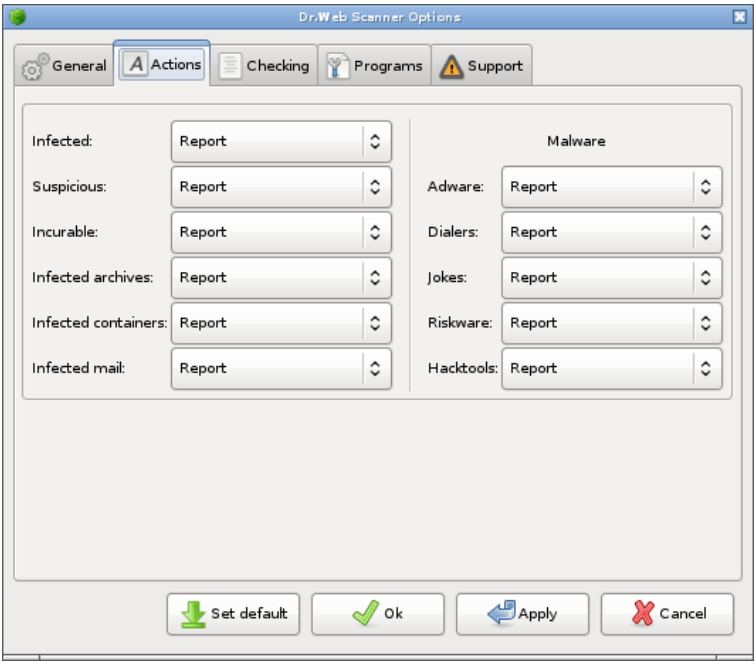


Рисунок 5. Вкладка Actions.

Вы можете изменить реакцию программы на обнаружение вирусных угроз или вредоносного ПО на вкладке **Actions** (Действия). Для этого выберите необходимое действие в выпадающем списке напротив соответствующего типа объекта. В зависимости от типа обнаруженной угрозы списки включают различный состав возможных действий над объектами:

- **Report** (Отчет) - сообщить о файле в поле отчета главного окна сканера.
- **Cure** (Лечить) - попытаться вылечить файл и восстановить его состояние до заражения. В случае если лечение невозможно, применить действие, выбранное для неизлечимых объектов.
- **Delete** (Удалить) - удалить файл.

При обнаружении инфицированных или подозрительных файлов в архивах, почте или файловых контейнерах программа применяет указанное действие в отношении всего объекта, а не отдельного файла внутри объекта.

Сканер распознает вредоносное ПО следующих видов:

- **adware** (рекламные программы) - используются для демонстрации рекламы;
- **dialers** (программы дозвона) - используются для накручивания оплаты за телефон жертве или для незаметного несанкционированного подключения пользователя через модем к дорогостоящим платным службам, чаще всего порнографическим;
- **jokes** (программы-шутки) - могут пугать и отвлекать пользователя;
- **riskware** (потенциально опасные программы) - невредоносные программы, которые могут использоваться во вредоносных целях;
- **hacktools** (программы взлома) - средства для несанкционированного доступа к компьютеру и другим электронным устройствам.

По окончании редактирования настроек нажмите на кнопку **Apply** (Применить), чтобы сохранить внесенные изменения, не закрывая окно основных настроек.

Вкладка Проверка

Все основные настройки работы сканера находятся на вкладке **Checking** (Проверка) главного окна настроек сканера (рис. 6). Здесь вы можете сохранить желаемые настройки, загрузить настройки из конфигурационного файла, а также восстановить настройки по умолчанию.

Рисунок 6. Вкладка Checking.

В состав вкладки **Checking** (Проверка) входят:

- панель **Check mode** (Режим проверки);
- панель описания режимов проверки;
- кнопки управления настройками.

На панели **Check mode** (Режим проверки) настраивается режим сканирования (уровень тщательности проверки):

- **Fast check** (Быстрая проверка) - проверяются только файлы, формат которых позволяет им быть «носителями» вирусов; архивы и объекты символических ссылок не проверяются; эвристический анализатор отключен. Проверка происходит гораздо быстрее, чем в режиме полной проверки за счет незначительного снижения надежности.

- **Full check** (Полная проверка) - режим, в котором проверяются все выбранные объекты, в том числе архивы и объекты символических ссылок. Данный режим рекомендуется для повседневной проверки компьютера. Проверка происходит медленнее, чем в режиме быстрой проверки, но со значительно более высоким уровнем надежности защиты.
- **Advanced mode** (Расширенный режим) - в этом режиме вы можете самостоятельно настроить все параметры, определяющие степень тщательности проверки. Данный режим предназначен в первую очередь для опытных пользователей. При выборе данного режима в правой нижней части окна становится доступной кнопка **Advanced Options** (Расширенные настройки). Для настройки параметров сканирования нажмите данную кнопку (см. раздел Расширенные настройки).

При выборе любого режима проверки правая панель вкладки содержит подробное описание данного режима.

Для того чтобы сохранить изменения настроек в конфигурационном файле, нажмите кнопку **Save Settings** (Сохранить настройки) (либо воспользуйтесь комбинацией клавиш CTRL+S). После этого при каждом запуске программы или загрузке настроек из конфигурационного файла будут использованы новые настройки.

Если вы перезагрузите систему без сохранения внесенных настроек, то любые изменения в конфигурационном файле будут удалены и настройки параметров вернутся в состояние по умолчанию, в котором **Dr.Web LiveCD** был записан на диск или другой носитель. Обратите внимание, что если флажок **Save all settings at exit** (Сохранять все настройки при выходе) на вкладке **General** (Общие) установлен, то настройки будут сохраняться при каждом закрытии **Сканера**.

Для того чтобы загрузить настройки из конфигурационного файла программы, нажмите кнопку **Load Settings** (Загрузить настройки) (либо воспользуйтесь комбинацией клавиш CTRL+L).

При запуске программы настройки из конфигурационного файла загружаются автоматически. Используйте кнопку **Load Settings** (Загрузить настройки) только для отказа от внесенных вами изменений настроек.

В конфигурационном файле программы в секции `[GUI]` также хранятся настройки самого модуля графического интерфейса. Подробную информацию о конфигурационном файле можно найти в Руководстве пользователя **Антивируса Dr.Web для Linux**.

Вкладка Программы

На вкладке **Programs** (Программы) настраиваются параметры взаимодействия с компонентами **Dr.Web LiveCD** (рис. 7).

На вкладке **Programs** (Программы) расположены три панели:

- **Updater** (Модуль обновлений) - содержит информацию, необходимую для модуля обновлений;
- **Mail** (Почта) - для настройки почтовой программы;
- **Browser** (Браузер) - для настройки браузера.

В верхней панели **Updater** (Модуль обновлений)

- при необходимости можно отредактировать путь к директории, содержащей модуль обновления. Для этого введите путь в поле **Path to directory with file update.pl** (Путь к каталогу с файлом update.pl) или нажмите на кнопку  для выбора нужной директории в проводнике по файловой системе;
- при использовании прокси-сервера для получения обновлений логин и пароль для этого сервера необходимо задать в полях ввода **Proxy login** (Логин для прокси) и **Proxy password** (Пароль для прокси) соответственно.

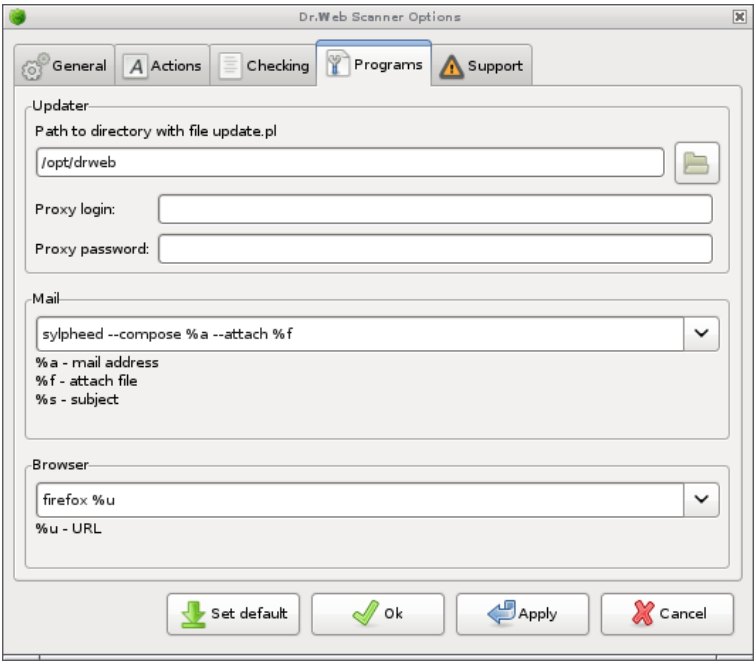


Рисунок 7. Вкладка Programs.

На панели **Mail** (Почта) выбирается и при необходимости редактируется в соответствующем поле команда для запуска почтовой программы в пакетном режиме. Под полем ввода указаны допустимые параметры команды запуска с описанием их значения.

На панели **Browser** (Браузер) выбирается и при необходимости редактируется в соответствующем поле команда для запуска веб-браузера. Под полем ввода приводятся допустимые параметры команды запуска с описанием их значения.

После окончания редактирования настроек нажмите на кнопку **Apply** (Применить), чтобы сохранить внесенные изменения, не закрывая окно основных настроек.

Обновление и техническая поддержка

На вкладке **Support** (Поддержка) (рис. 8) можно произвести обновление антивирусных базы, связаться с технической поддержкой, отправить **ООО «Доктор Веб»** информацию о программной ошибке или подозрительный файл на проверку, просмотреть информацию о программе.

Левая панель вкладки **Support** (Поддержка) содержит кнопки для выполнения следующих действий:

- Запуск модуля обновления. Осуществляется при нажатии на кнопку **Update** (Обновление).
- Переход на сайт ООО «Доктор Веб» в окне веб-браузера. Нажмите кнопку **www.drweb.com**.
- Переход на форум Dr.Web для Unix в окне веб-браузера. Нажмите кнопку **Forum** (Форум). Откроется встроенный браузер на странице форума **ООО «Доктор Веб»**.
- Отправка вопроса в службу технической поддержки. Нажмите кнопку **Request to support** (Вопрос в техподдержку). Откроется встроенный браузер на странице технической поддержки **ООО «Доктор Веб»**.
- Отправка сообщения о найденной ошибке по почте. Нажмите кнопку **Bug report** (Отправить сообщение об ошибке). Для отправки почтового сообщения откроется встроенный почтовый клиент.
- Отправка файлов, предположительно инфицированных неизвестными вирусами, на анализ в лабораторию **ООО «Доктор Веб"**. Нажмите на кнопку **Send file for check** (Отправка файлов на анализ). Откроется окно выбора файлов.

Правая панель вкладки **Support** (Поддержка) содержит информацию о версии программы, загруженных вирусных базах, дате последнего обновления и номере лицензионного ключа. Эта информация корректируется после каждого сеанса обновления.

Для обновления антивирусных баз, перехода на вышеуказанные веб-ресурсы, а также для отправки сообщений и файлов требуется выход в Интернет.

Если при попытке перейти по ссылке на один из вышеуказанных веб-сайтов или отправить сообщение по электронной почте вы получите сообщение о том, что браузер или почтовая программа не найдены, настройте пути к почтовой программе и браузеру. Для этого в меню сканера **Settings** (Настройки) выберите пункт **Options** (Опции) -> вкладку Programs (Программы) и введите необходимые данные.

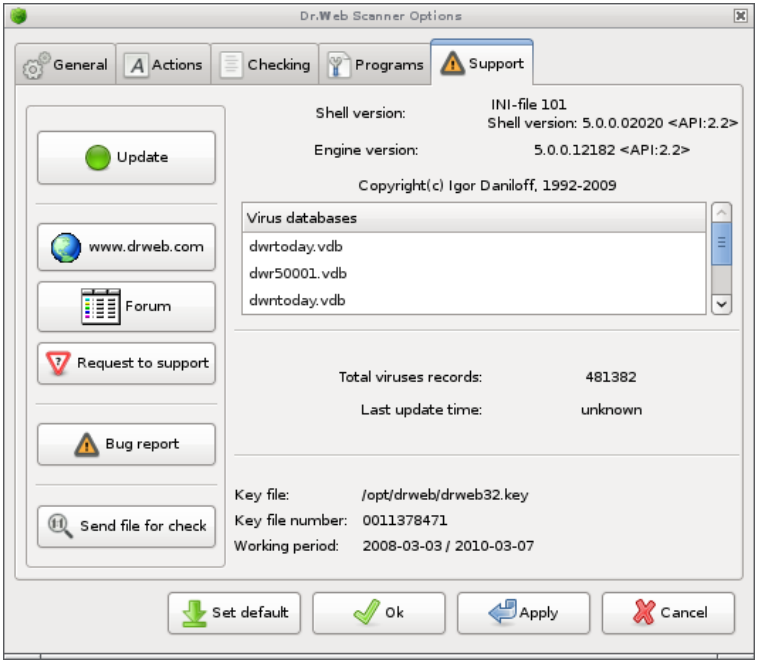


Рисунок 8. Вкладка Support.

Расширенные настройки сканера

Опытные пользователи могут выбрать Расширенный режим сканирования компьютера.

Для самостоятельной настройки параметров сканирования:

1. В меню сканера **Settings** (Настройки) выберите пункт **Options** (Опции) и перейдите на вкладку **Checking** (Проверка).
2. На панели **Check mode** (Режим проверки) выберите **Advanced mode** (Расширенный режим).
3. При этом становится доступной кнопка **Advanced Options** (Расширенные настройки). Нажмите кнопку для доступа к настройкам.

Меню расширенных настроек позволяет вручную задать пути к директориям, которые используются программой, типы проверяемых файлов, режимы ведения файлов отчета и т.д.

Расширенные настройки сканера делятся на несколько разделов (вкладок):

- Paths (Пути) - указание путей к основным модулям сканера.
- File types (Типы файлов) - настройка типов файлов, подлежащих проверке.
- Log file (Файл отчета) - настройка ведения отчета.
- Archive (Архив) - настройка ограничений, налагаемых на действия с архивами из соображений безопасности.
- Other (Прочие) - задание настроек, влияющих на загруженность компьютера, указание тайм-аута модуля обновления и включение эвристического анализатора.

В нижней части окна расширенных настроек сканера расположены кнопки управления:

- **Set default** (Установить по умолчанию) - сбросить пользовательские изменения настроек и вернуть настройки по умолчанию;

- **OK** - сохранить настройки и вернуться в главное окно сканера;
- **Apply** (Применить) - сохранить настройки и остаться в окне настроек;
- **Cancel** (Отмена) - вернуться в главное окно сканера без сохранения изменения настроек.

Вкладка Пути

Окно расширенных настроек сканера по умолчанию открывается на вкладке **Paths** (Пути) (рис. 9).

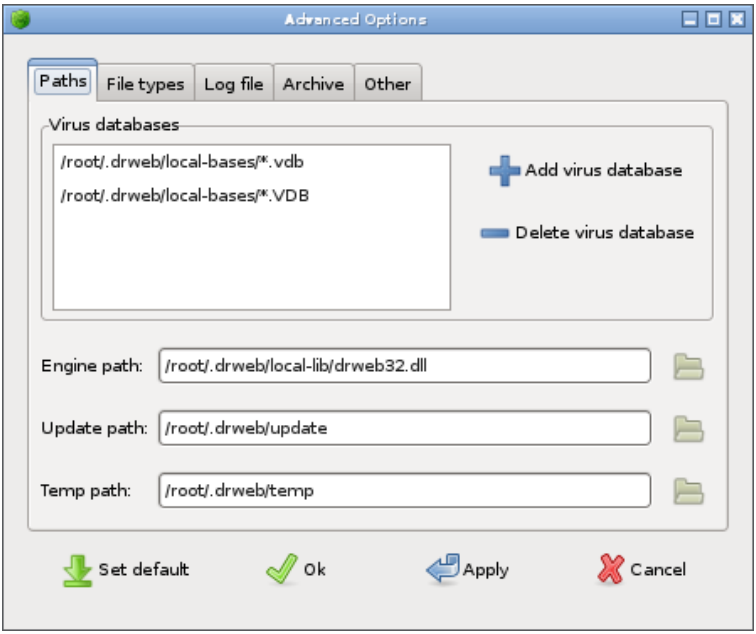


Рисунок 9. Вкладка Paths.

В списке **Virus databases** (Вирусные базы) указано нахождение баз с вирусными записями. По умолчанию базы размещаются в

директории, заданной при установке программы. Модуль обновления по умолчанию помещает обновленные базы в ту же директорию. Однако в случае подключения дополнительных баз вручную необходимо указать их в данном списке. Если файлы баз имеют нестандартное расширение (даже если они размещаются в стандартной директории), они также должны быть включены в список вирусных баз.

Для того чтобы добавить элемент в список вирусных баз, нажмите на кнопку **Add virus database** (Добавить вирусную базу). Откроется окно добавления базы.

По умолчанию в списке указаны две маски файлов: `*.vdb`; `*.VDB` (т.е. только файлы с расширениями `.vdb` или `.VDB`). Вы также можете выбрать значение `*` (т.е. файлы с любым расширением).

Для того чтобы удалить элемент из списка вирусных баз, выберите его и нажмите на кнопку **Delete virus database** (Удалить вирусную базу).

При необходимости вы можете отредактировать в соответствующих полях пути к поисковому модулю, директории обновления и директории временных файлов либо выберите их в проводнике по файловой системе, нажав на кнопку  рядом с соответствующей строкой под списком вирусных баз.

Вкладка Типы файлов

На вкладке **File types** (Типы файлов) настраиваются ограничения для проверяемых файлов (рис. 10).

На панели **Scan mode** (Режим сканирования) при помощи кнопок-переключателей выбирается способ отбора файлов для сканирования:

- **All** (Все) - проверяются все файлы, независимо от имени и внутренней структуры. Данный режим задан по умолчанию при выборе **Full check** (Полная проверка) на вкладке Checking (Проверка) настроек сканера.

- **By type** (По типу) - проверяются только файлы с расширениями, заданными в списке **File types** (Типы файлов). По умолчанию в список включены исполняемые файлы и файлы, содержащие макросы. Для добавления расширения в список нажмите на кнопку **Add file type** (Добавить тип файла), введите в открывшемся окне желаемое расширение и нажмите **OK**. Для удаления расширения из списка отметьте его и нажмите на кнопку **Delete file type** (Удалить тип файла).

Кнопки **Add file type** (Добавить тип файла) и **Delete file type** (Удалить тип файла) активны только при выборе режима проверки **By type** (По типу).

- **By format** (По формату) - независимо от имени и расширения проверяются файлы, которые по внутренней структуре могут быть носителями вирусов. Данный режим задан по умолчанию при выборе **Fast check** (Быстрая проверка) на вкладке Checking (Проверка) настроек сканера.

Ниже на вкладке **File types** (Типы файлов) вы можете выбрать следующие флажки, чтобы установить дополнительные ограничения к файлам:

- **Follow symlinks** (Следовать символическим ссылкам) - устанавливается, чтобы сканер проверял файлы, символические ссылки на которые попадают в число проверяемых.
- **Check archives** (Проверять архивы) - устанавливается, чтобы сканер распаковывал файловые архивы и проверял входящие в них файлы (при установленном режиме **By format** (По формату) - если они имеют соответствующий формат; в режиме **By type** (По типу) в список типов должны входить как расширение архива, так и расширение проверяемого файла).
- **Check e-mail files** (Проверять файлы электронной почты) - устанавливается, чтобы сканер проверял файлы, прикрепленные к почтовым сообщениям.

При выборе режима **Full check** (Полная проверка) на вкладке Checking (Проверка) настроек сканера три вышеперечисленных

флажка устанавливаются по умолчанию; при выборе режима **Fast check** (Быстрая проверка) - снимаются.

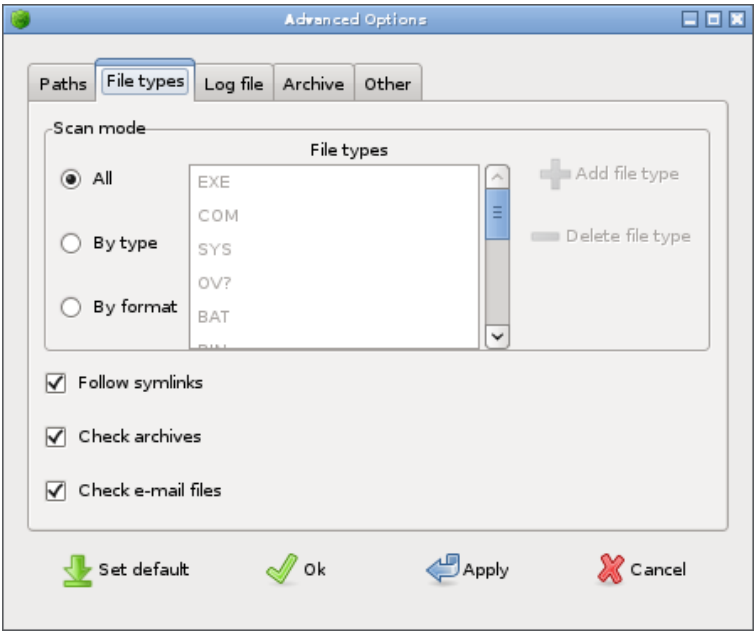


Рисунок 10. Вкладка File types.

Вкладка Файл отчета

На вкладке **Log file** (Файл отчета) (рис. 11) настраивается ведение отчета.

На панели **Log File Name** (Имя файла отчета) выбирается способ протоколирования - средствами **Dr.Web LiveCD** или через системную службу:

- **File name** (Имя файла) - **Dr.Web LiveCD** записывает отчеты в указанный в поле ввода файл. Путь к файлу отчета можно отредактировать в поле ввода или выбрать его при помощи проводника по файловой системе, нажав на кнопку  .
- **Syslog** - файл отчета ведется при помощи системной службы протоколирования Syslog. При выборе этого варианта вы можете указать средство протоколирования и приоритет в выпадающих списках ниже .

Доступны следующие средства протоколирования: **Daemon | Local0 .. Local7 | Kern | User | Mail**

В качестве приоритета событий может быть выбран один из следующих вариантов: **Info | Notice | Alert | Warning**

Установленный флажок **Limit log file size** (Ограничить размер файла отчета) указывает, что файл отчета не может превышать размер, указанный в поле ввода слева. После достижения максимального размера старые записи постепенно стираются, чтобы освободить место для записей новых событий. Снятие флажка убирает ограничение на размер файла отчета.

Рекомендуется сохранить установленный по умолчанию флажок **Limit log file size** (Ограничить размер файла отчета) и значение по умолчанию в поле **Max log file size** (Предельный размер файла отчета) (512 КБ).

На панели **Updater** (Модуль обновления) при необходимости можно отредактировать имя файла отчета модуля обновления. Имя и путь указываются в поле ввода **Updater log** (Файл отчета), либо выбираются при помощи проводника по файловой системе, открываемого по кнопке  .

В выпадающем списке **Level of log** (Уровень отчета) задается требуемый уровень подробности ведения отчета. Доступны следующие уровни ведения отчета: **Debug | Verbose | Info | Warning | Error | Quiet**

Рисунок 11. Вкладка Log file.

Вкладка Архив

На вкладке **Archive** (Архив) (рис. 12) настраиваются ограничения, накладываемые на действия с архивами из соображений безопасности.

Параметры на данной вкладке направлены на защиту сканера от атак «почтовыми бомбами». При превышении заданных численных значений характеристик архивов их проверка прекращается для исключения возможности исчерпать ресурсы системы.

При необходимости изменения заданных по умолчанию настроек отредактируйте значения в следующих полях:

- **Max compression ratio** (Максимальный коэффициент сжатия) (по умолчанию 5000);

- **Max archive nesting level** (Максимальный уровень вложенности архива) (по умолчанию 8);
- **Compression check threshold** (Порог проверки сжатия) (по умолчанию 5000 КБ) - архивы меньшего размера проверяются независимо от коэффициента сжатия;
- **Max file size to extract** (Максимальный размер файла для извлечения) (по умолчанию 1024 КБ) - при обнаружении файлов большего размера архив не распаковывается.

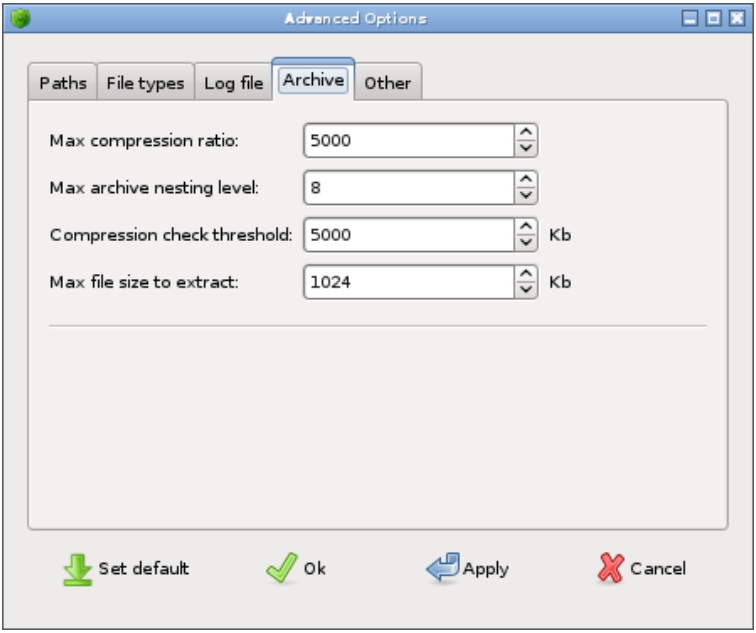


Рисунок 12. Вкладка Archive.

Вкладка Прочие

На вкладке **Other** (Прочие) (рис. 13) задаются настройки, влияющие на загруженность компьютера, указывается тайм-аут модуля обновления и производится включение/ выключение эвристического анализатора.

На панели **Scan priority** (Приоритет сканирования) при помощи кнопок-переключателей задается приоритет процесса сканирования по сравнению с остальными процессами в системе: **High** (Высокий), **Normal** (Нормальный), **Low** (Низкий).

В поле ввода **Timeout** (Тайм-аут) задается максимальное время ожидания в секундах для модуля обновления при соединении с сервером обновлений.

Флажок **Heuristic analysis** (Эвристический анализ) включает режим эвристического *анализатора* (режим поиска неизвестных вирусов на основании анализа действий, присущих вирусам).

В режиме эвристического анализатора возможны ложные срабатывания. Обнаруженные с его помощью файлы всегда имеют статус «подозрительных». При выборе режима **Full check** (Полная проверка) эвристический анализатор включается по умолчанию. При выборе режима **Fast check** (Быстрая проверка) - выключается.

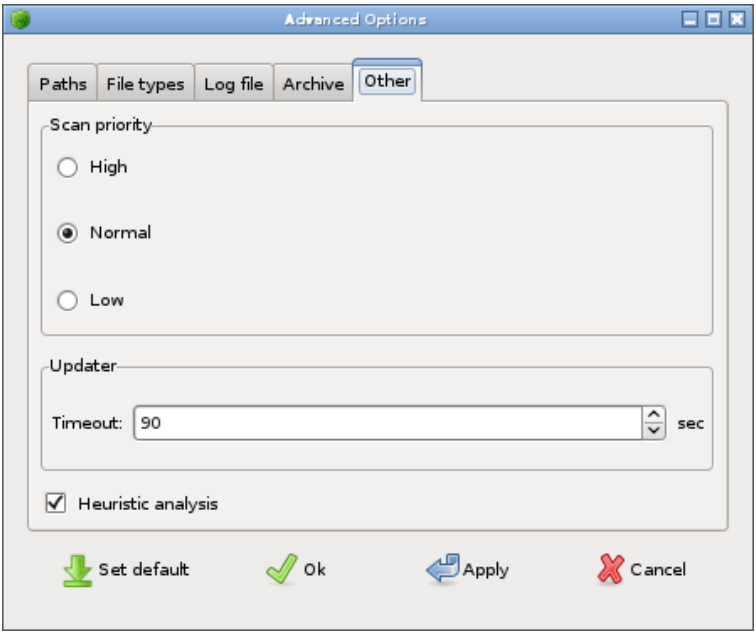


Рисунок 13. Вкладка Other.

Встроенные приложения

В данном разделе описываются приложения, входящие в состав **Dr.Web LiveCD**.

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. 14). 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 **ООО «Доктор Веб»**.

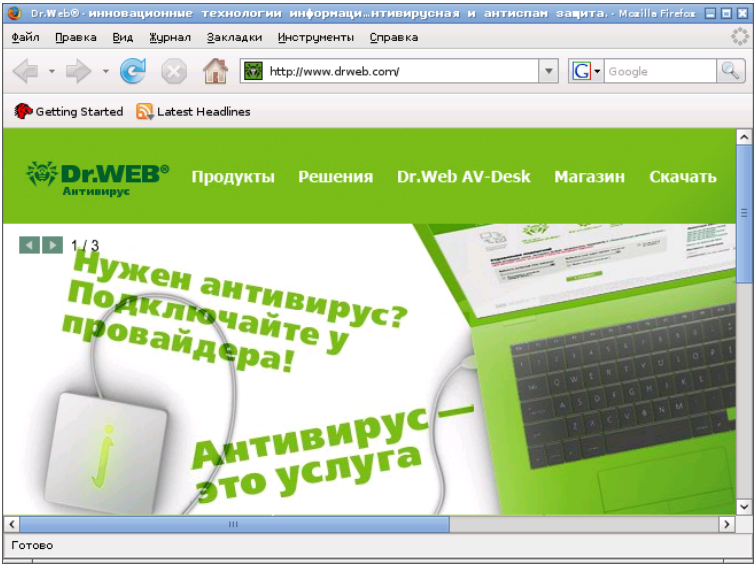


Рисунок 14. Встроенный браузер.

Почтовый клиент

При помощи встроенного почтового клиента **Sylpheed** (рис. 15) 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 **Configuration** -> **Create new account**. 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 **File** -> **Mailbox** -> **Add mailbox**. В свойствах почтового ящика необходимо указать, какая учетная запись будет использоваться: в контекстном меню ящика выбрать **Properties** -> вкладка **Compose** -> выпадающий список **Account** -> указать требуемую запись.

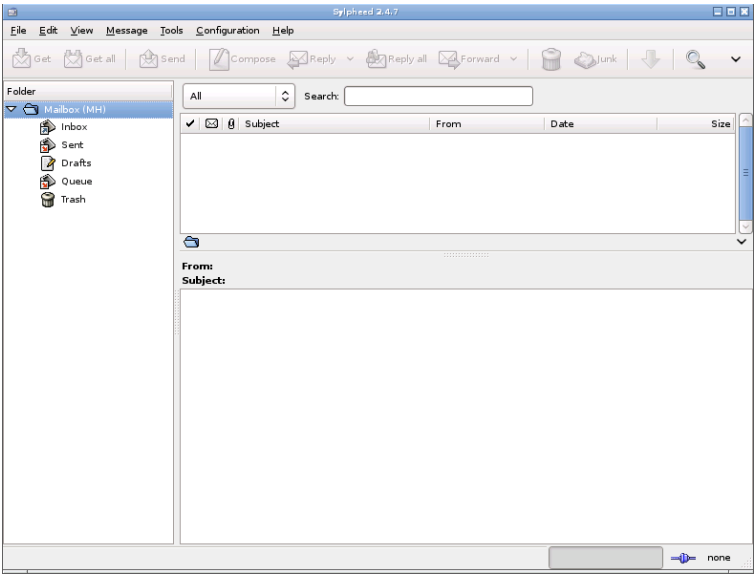


Рисунок 15. Почтовый клиент.

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.

Файловый менеджер

Встроенный файловый менеджер **Midnight Commander** (рис. 16) 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/.

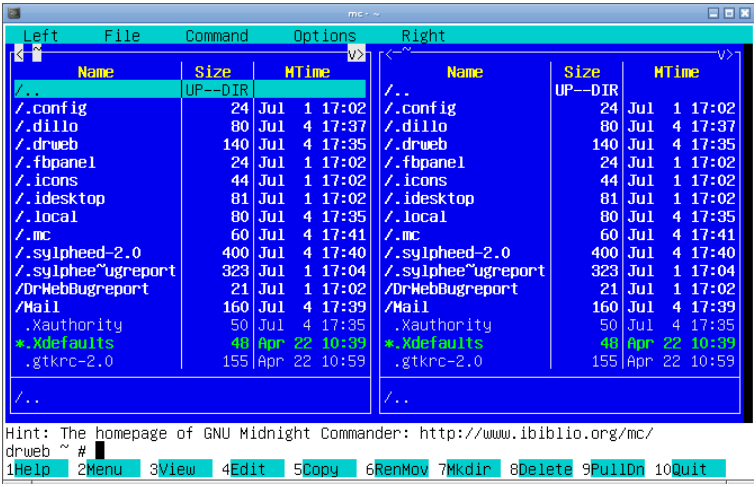


Рисунок 16. Файловый менеджер.

Работа с консольным сканером

В данном разделе описываются особенности работы с консольным сканером.

Запуск процесса сканирования

После загрузки **Dr.Web LiveCD** в безопасном режиме на экран выводится главное меню запуска - **Start Menu**.

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

- **Start Xorg** - запустить сканер с графическим интерфейсом;
- **Start Shell** - вывести на экран командную строку;
- **Start Midnight Commander** - запустить встроенный файловый менеджер;
- **Start Dr.Web Scanner** - сканировать все разделы жесткого диска с настройками по умолчанию;
- **Start Dr.Web Update** - обновить вирусные базы;
- **Bugreport** - отправить разработчикам информацию об ошибке в ПО;
- **Restart** - перезагрузить компьютер;
- **Shut Down** - выключить компьютер, не открывая привод;
- **Eject & Shut Down** - извлечь диск и завершить работу компьютера.

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

`/opt/drweb/drweb -path=<`*путь*`> [ `*опции*`]`

где <*путь*> — путь к проверяемому каталогу или маска тестируемых файлов.

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

```
drweb -path=/win/C:
```

Опции командной строки

Как и для любой Unix-программы, для сканера **Dr.Web** предусматриваются многочисленные опции командной строки (ключи, задающие дополнительные параметры команды). Они отделяются от указания пути пробелом и предваряются символом «-» (дефис). Полный список опций можно получить, запустив команду `drweb` со следующими опциями:

`-?` или `-help`

Основные опции программы могут быть сгруппированы следующим образом:

- опции области проверки
- опции диагностики
- опции действий
- опции интерфейса

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

- `@[+]<файл>` — проверка объектов, перечисленных в данном файле; символ «+» (плюс) предписывает не удалять файл списка объектов по окончании проверки; файл списка может содержать пути к периодически проверяемым каталогам или просто список подлежащих регулярной проверке файлов;
- `sd` — рекурсивный поиск и сканирование файлов в подкаталогах, начиная с текущего;

- `fl` — следовать ссылкам, как для файлов, так и для каталогов; при этом ссылки, приводящие к «зацикливанию», игнорируются.

Опции диагностики, определяющие, какие типы объектов должны проверяться на вирусы, включают:

- `al` — диагностика всех файлов на заданном устройстве или в указанном в качестве аргумента каталоге;
- `ar[d/m/r][n]` — проверка файлов в архивах (ARJ, CAB, GZIP, RAR, TAR, ZIP);
  `d` – удаление, `m` – перемещение, `r` – переименование архивов, содержащих инфицированные объекты; `n` – отключение вывода имен архиваторов;
  под архивами в данном случае понимаются не только собственно архивы (например, вида `*.tar`), но и их компрессированные формы (в частности, компрессированные TAR-архивы вида `*.tar.gz` и `*.tgz`);
- `cn[d/m/r][n]` – проверка файлов в контейнерах (HTML, RTF, PowerPoint);
  `d` – удаление, `m` – перемещение, `r` – переименование контейнеров, содержащих инфицированные объекты; `n` – отключение вывода типа контейнера;
- `ml[d/m/r][n]` — проверка 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 (задаются в строке конфигурационного файла `FilesTypes`);
- `fm` — диагностика файлов с внутренней структурой программных модулей;
- `ha` — эвристический анализ файлов, поиск неизвестных вирусов.

Опции действий определяют действия, которые должен выполнять сканер в отношении инфицированных и подозрительных файлов. Доступны следующие опции:

- cu[d/m/r] — лечение инфицированных файлов; дополнительные опции предписывают: d — удаление, m — перемещение, r — переименование инфицированных файлов;
- ic[d/m/r] — определяет действия для неизлечимых файлов: d — удаление, m — перемещение, r — переименование неизлечимых файлов;
- sp[d/m/r] — определяет действия для подозрительных файлов: d — удаление, m — перемещение, r — переименование подозрительных файлов;
- adw[d/m/r/i] — определяет действия для файлов, содержащих рекламные программы: d — удаление, m — перемещение, r — переименование, i — игнорирование;
- dls[d/m/r/i] — определяет действия для файлов, содержащих программы дозвона (аналогично рекламным программам, см. выше);
- jok[d/m/r/i] — определяет действия для файлов, содержащих программы-шутки (аналогично рекламным программам, см. выше);
- rsk[d/m/r/i] — определяет действия для файлов, содержащих потенциально опасные программы (аналогично рекламным программам, см. выше);
- hck[d/m/r/i] — определяет действия для файлов, содержащих программы взлома (аналогично рекламным программам, см. выше).

Опции интерфейса определяют условия вывода результатов работы программы. К ним относятся:

- ot — вывод информации на stdout, то есть стандартный вывод;
- oq — отключить вывод информации;
- ok — вывод сообщения 'Ok' для неинфицированных файлов;
- log=<файл> — запись протокола работы в указанный файл;
- ini=<файл> — использование альтернативного INI-файла;

- `lng=<файл>` — использование альтернативного файла языка.

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

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

Например, при запуске сканера командой вида:

```
drweb -path=<путь> -ha-
```

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

По умолчанию (то есть без указания опций), если не изменялся конфигурационный файл программы, сканер запускается с опциями:

```
-ar -fm -ha -fl- -ml -sd -up
```

Эти опции считаются наиболее приемлемыми для повседневной проверки системы. Однако они не предусматривают никаких автоматических действия для зараженных, подозрительных и неизлечимых файлов. Для таких файлов вы можете задать множество различных действий, но рекомендуемыми являются приведенные ниже:

- `cu` — лечение инфицированных файлов и системных областей, без удаления, перемещения или переименования инфицированных файлов;
- `icd` — удаление неизлечимых файлов;
- `spm` — перемещение подозрительных файлов;
- `spr` — переименование подозрительных файлов (по умолчанию расширение заменяется на `.#??`, т.е. первый символ расширения заменяется символом `#`, а остальные символы остаются неизменными).

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 флэш-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 флэш-накопителя на другом носителе.

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

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

Создание загрузочного флэш-накопителя автоматически

1. В графической оболочке нажмите значок программы **Create Live USB** на рабочем столе: 

   Программа перейдет в режим ожидания подключения устройства через USB-порт.

2. Подключите флэш-накопитель. Регистрация события подключения занимает максимум десять секунд.

Копирование файлов начнется автоматически. Если на подключенном флэш-накопителе несколько разделов, файлы **LiveCD** будут записаны на тот раздел, который является загружаемым, у остальных разделов флаг bootable снимается.

Создание загрузочного флэш-накопителя вручную

1. Откройте терминал для работы в командной строке одним из следующих способов:
   - в графической оболочке нажмите значок терминала на рабочем столе;
   - в safe mode выберите в главном меню пункт **Start Shell**.
2. (Необязательно.) Для проверки подключенных к компьютеру дисков, а также разделов на флэш-накопителях запустите команду `mount: /bin/mount` или просто `mount`.
3. Выполните команду `create_usb [device]` или `CreateLiveUSB [device]`.
   Например, `create_usb sda1`

   Команда работает в двух режимах:

   - запуск команды с явным указанием устройства, на которое нужно произвести запись. В этом режиме необходимо указать имя флэш-накопителя и раздел, на который записывается **LiveCD**.
   - запуск команды без указания устройства. Программа перейдет в режим ожидания подключения устройства через USB-порт. Регистрация события подключения занимает максимум десять секунд. Если на подключенном флэш-накопителе несколько разделов, файлы **LiveCD** будут записаны на тот раздел, который является загружаемым, у остальных разделов флаг bootable снимается.