Dr.WEB®
LiveCD

Защити созданное

Руководство пользователя

Dr.Web® LiveCD
Версия 6.0.2
Руководство пользователя
25.09.2012

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** для систем GNU/Linux. 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, а также выполнить восстановление и редактирование реестра Windows.

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 расширенном режиме (advanced mode) с большим количеством возможностей, а также доступом к интерфейсу командной строки или к графическому режиму по выбору.

Обычный режим является предпочтительным в силу большей наглядности и функциональности. Именно работе в графической оболочке посвящена основная часть руководства. Интерфейс командной строки предназначен для более опытных пользователей, хорошо знакомых с Unix-подобными

операционными системами, и используется при невозможности запуска режима с графическим интерфейсом.

Пожалуйста, обратите внимание, что в процессе работы **Dr. Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все изменения, внесенные в настройки программ, входящих в состав диска, будут утеряны при перезагрузке компьютера.

Каталог **Карантина** также создается на RAM-диске, поэтому резервные копии файлов, сохраненные в **Карантине**, будут утрачены, если их не сохранить на один из жестких (физических) дисков компьютера.

Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

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 системными требованиями являются:

Параметр	Требование
Процессор (CPU)	архитектура i386
Оперативная память (RAM)	не менее 256 МБ (512 МБ, если нет возможности использовать виртуальную память на жестком диске)
Место на жестком диске (HDD)	при использовании снапшотов необходимо наличие на любом из жестких дисков не менее 512 MB свободного места
Приводы	CD-ROM, DVD-ROM или накопитель USB-flash с объемом памяти не менее 200 МБ
Прочее	наличие видеокарты, монитора, клавиатуры и мыши

1.3. Антивирус Dr.Web для Linux

Антивирус Dr.Web для Linux создан с целью помочь пользователям компьютеров, работающих под управлением GNU/Linux, защитить свои рабочие машины от вирусов и прочих типов угроз.

Основные компоненты программы (**Антивирусное ядро** и **Антивирусные базы**) являются не только крайне эффективными и нетребовательными к ресурсам, но и кросс-платформенными, что позволяет специалистам **Dr.Web** создавать превосходные антивирусные решения для различных операционных систем (ОС). Компоненты **Антивируса Dr.Web для Linux** постоянно обновляются, а антивирусные базы дополняются новыми сигнатурами, что обеспечивает защиту на наиболее современном уровне. Для дополнительной защиты от неизвестных вирусов используется эвристический анализатор.

Антивирус Dr.Web для Linux состоит из следующих компонентов, каждый из которых выполняет свой набор функций:

Компонент	Функции
Пульт управления	Модуль управления функциями **Антивируса Dr.Web для Linux** в среде Linux с графической оболочкой. Позволяет настраивать параметры сканирования, запускать и останавливать его, инициировать обновления, работать с **Карантином**
Сканер	Это основной компонент для обнаружения вирусов, который может выполнять: • полную или выборочную проверку системы по запросу пользователя; • обезвреживание обнаруженных угроз (лечение, удаление, помещение в **Карантин**); Пользователь может вручную выбрать необходимое действие, либо задать автоматическое применение действия, указанного для данного типа угроз в настройках антивируса)

Карантин	Это специальный каталог, который используется для изоляции зараженных файлов и других угроз, чтобы они не могли нанести вред системе
Модуль обновления	Данный компонент используется для обновления антивирусных баз и других компонентов антивируса через сеть Интернет
Менеджер лицензий	Данный компонент упрощает работу с ключевыми файлами: он позволяет получить демонстрационный или лицензионный ключевой файл, просмотреть информацию о нем, а также продлить лицензию

Гибкие и удобные настройки **Антивируса Dr.Web для Linux** позволяют задать звуковые уведомления для различных событий, максимальный размер **Карантина**, а также составить список файлов и папок, которые следует исключить из проверки.

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

Для обеспечения максимальной эффективности сканирования **Антивирус Dr.Web для Linux** не забывайте своевременно обновлять вирусные базы. Обратите внимание, что для обновления вирусных баз требуется доступ в Интернет. Подробности настройки сетевого подключения приведены в разделе Конфигурация сети.

1.4. Что нового в Dr.Web® LiveCD

В **Dr.Web® LiveCD** версия 6.0.2 внесены следующие улучшения:

1. Добавлена возможность правки реестра **Windows**. Реестр **Windows** находится автоматически и монтируется в виде каталога в корень файловой системы при запуске **Dr.Web® LiveCD**, после чего разделы и ключи реестра становятся доступны для редактирования файловому

менеджеру в виде каталогов и файлов;

2. Добавлена утилита автоматического исправления неисправностей реестра **Windows**, вызываемых вредоносными программами;
3. Обновлен антивирусный **Сканер**:
   - Сканирование теперь выполняется одновременно в несколько потоков;
   - Отсутствие необходимости загрузки вирусных баз при каждой проверке позволяет обрабатывать запрос на сканирование гораздо быстрее;
   - Добавлена позможность проверки загрузочных секторов диска.
4. При выборе пункта главного меню **Сообщить об ошибке** (**Report Bug**) автоматически создаётся письмо с сообщением об ошибке, включающее в себя в том числе и дампы MBR, которые также копируются в каталог файловой системы `/tmp`;
5. Появилась возможность выбора используемого языка интерфейса прямо в стартовом меню. В данный момент доступны 2 языка: русский и английский.
6. Общие улучшения:
   - Версия ядра ОС обновлена с 2.6.30 до 3.2.12;
   - Добавлен модуль для работы с файловой системой **exFat**;
   - Добавлена поддержка накопителей USB-flash с файловой системой **NTFS**;
   - Добавлена поддержка **NTFS ADS**;
   - Обновлен и увеличен список устройств, поддерживаемых **Dr.Web® LiveCD**;
   - Обновлены драйвера графических карт, благодаря чему новая версия **Dr.Web® LiveCD** поддерживает большее количество видеоадаптеров.

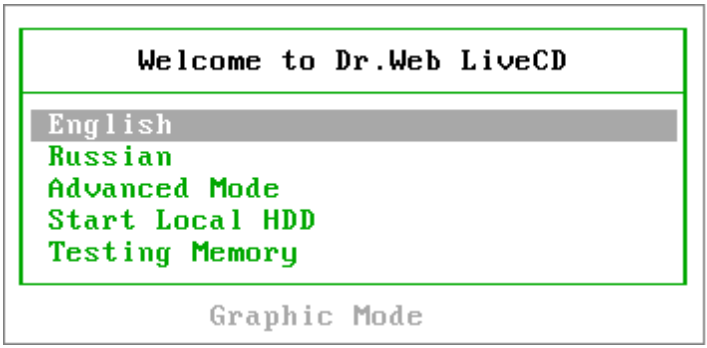
2. Запуск Dr.Web LiveCD

Предварительные замечания

Убедитесь, что ваш компьютер загружается в первую очередь с CD-привода, в котором находится диск **Dr.Web LiveCD**, либо с другого носителя (например, USB-flash), на котором записан **Dr.Web LiveCD**. Вставьте носитель **Dr.Web LiveCD** в привод и включите или перезагрузите компьютер.

Основное загрузочное меню

При загрузке компьютера на экран выводится меню, в котором пользователю предоставляется возможность выбора режима запуска. Вид стартового меню показан на рисунке ниже.



С помощью стрелок ⇧ и ⇩ клавиатуры выберите один из следующих вариантов загрузки и нажмите ENTER:

- Чтобы запустить **Dr.Web LiveCD** в режиме графического интерфейса, выберите требуемый язык:
  - **English** – английский;
  - **Russian** – русский.
- Чтобы запустить **Dr.Web LiveCD** в расширенном режиме, выберите пункт **Advanced Mode**;
- Выберите **Start Local HDD**, если вы желаете загрузить

операционную систему, установленную на жестком диске компьютера и не запускать **Dr.Web LiveCD** (производится попытка загрузки операционной системы с нулевого раздела нулевого диска (hd0,0));

- Для проверки памяти выберите вариант **Testing Memory**. Тестирование памяти рекомендуется выполнять, если компьютер работает крайне нестабильно, в случайный момент времени перегружается. После выбора этого пункта будет запущена программа тестирования памяти. После завершения тестирования компьютер будет перезагружен.

В случае если в течение 15 секунд вы не выберете нужный пункт меню, по умолчанию **Dr.Web LiveCD** запустится в режиме графического интерфейса с использованием английского языка (по умолчанию в меню выбран пункт **English**).

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

Пожалуйста, обратите внимание, что в процессе работы **Dr.Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все изменения, внесенные в настройки программ, входящих в состав диска, будут утеряны при перезагрузке компьютера.

Каталог **Карантина** также создается на RAM-диске, поэтому резервные копии файлов, сохраненные в **Карантине**, будут утрачены, если их не сохранить на один из жестких (физических) дисков компьютера.

Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

3. Графическая оболочка Dr.Web LiveCD

Программный продукт **Dr.Web® LiveCD** содержит графическую оболочку с оконным интерфейсом, аналогичную GUI ОС Linux. При запуске **Dr.Web LiveCD** в режиме графического интерфейса после загрузки среды на экране отображается стандартный рабочий стол.

Структура рабочего стола

Вид рабочего стола графической оболочки **Dr.Web® LiveCD** показан на рисунке ниже.

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 следующие компоненты:

	Кнопка открытия системного меню
	Значки быстрого запуска встроенных приложений
	Значки для переключения между рабочими столами (доступно 4 рабочих стола)
	Значки открытых в данный момент приложений
	Иконка **Антивирус Dr.Web для Linux** и системные часы

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;
- текстовые редакторы **Leafpad** и **nano**;
- средство просмотра файлов PDF;
- Утилиты:
  - Утилита лечения реестра;
  - Утилита конфигурирования сети;
  - Утилита создания загрузочной USB-flash.

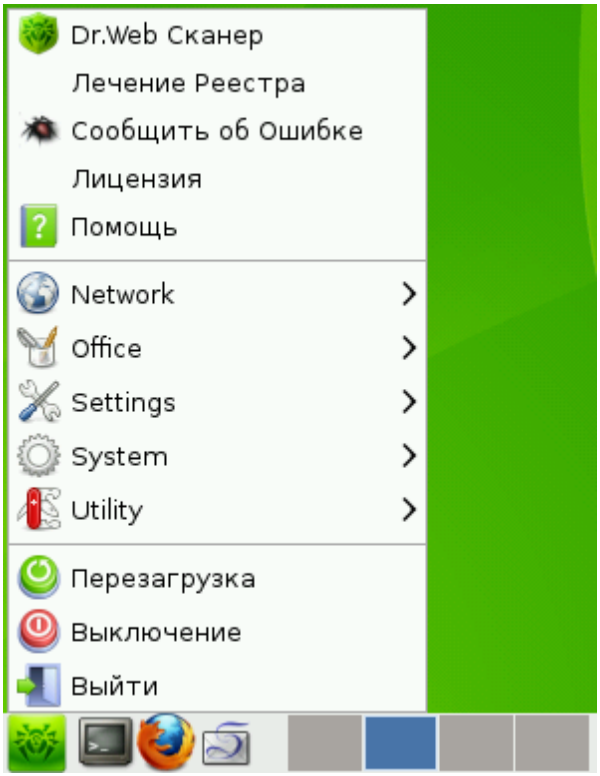
Запуск основных компонентов можно осуществить одним из следующих способов:

- 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;

- выбрав требуемый компонент в системном меню оболочки.

Структура системного меню

Системное меню открывается при нажатии на кнопку  на панели задач. Вид системного меню представлен на рисунке ниже.



Пункты системного меню:

Пункт	Назначение
Dr.Web Сканер	Запуск окна **Пульта Управления Антивируса Dr.Web для Linux**
Лечение реестра	Запуск утилиты лечения реестра **Windows**
Сообщить об ошибке	Запуск почтового приложения **Sylpheed** и формирование заготовки письма для описания ошибки (в качестве адресата письма автоматически указывается команда разработчиков **«Доктор Веб»**)
Лицензия	Запуск текстового редактора **nano** и открытие в нем текста лицензионного договора с конечным пользователем
Помощь	Запуск браузера **Firefox** и открытие в нем справочных материалов по продукту **Dr.Web LiveCD**
Network	Содержит подменю, позволяющее запустить следующие приложения: • Браузер **Firefox** • Почтовая программа **Sylpheed**
Office	Содержит подменю, позволяющее запустить: • Средство просмотра файлов PDF
Settings	Содержит подменю, позволяющее запустить следующие утилиты: • Настройка плеера **Adobe flash player** • Настройка внешнего вида оконного интерфейса графической оболочки • Настройка системного меню • Конфигурирование сети
System	Содержит подменю, позволяющее запустить следующие приложения: • **Антивирус Dr.Web для Linux** • Терминал для доступа к командной консоли
Utility	Содержит подменю, позволяющее запустить следующие утилиты: • Текстовый редактор **Leafpad**

	• Файловый менеджер **Midnight Commander** • **Утилита создания загрузочного носителя USB-flash**
Перезагрузка	Выполнение перезагрузки компьютера
Выключение	Выполнение выключения компьютера
Выйти	Завершение работы графической оболочки и переход в меню расширенного режима.

Запуск антивируса

После запуска графической оболочки по умолчанию открывается окно **Пульта управления Антивируса Dr.Web для Linux**. С помощью **Антивируса Dr.Web для Linux** вы можете проверить на вирусы все диски вашего компьютера.

Чтобы получить информацию о том, как пользоваться **Антивирусом Dr.Web для Linux**, выберите пункт **Помощь** системного меню или в окне **Пульта управления** выберите в меню **Помощь** пункт **Справка**.

3.1. Решение типовых задач

В графическом режиме работы Вы можете выполнить следующие действия:

1. Проверка системы на вирусы

Проверка системы на наличие вирусов и вредоносного ПО выполняется при помощи **Антивируса Dr.Web для Linux**.

Работа с **Антивирусом Dr.Web для Linux** рассмотрена в следующих разделах:

- В режиме графической оболочки – в разделе 3.2;
- В режиме командной строки – в разделе 5.

2. Восстановление реестра Windows

Восстановление реестра Windows в автоматическом режиме выполняется при помощи специальной утилиты восстановления

реестра, входящей в состав **Dr.Web LiveCD**.

Работа с утилитой восстановления реестра рассмотрена в разделе 6.2.

3. Просмотр, редактирование, создание и удаление файлов

Работа с каталогами и файлами, в том числе просмотр, редактирование, создание и удаление файлов выполняются при помощи файлового менеджера **Midnight Commander**.

Работа с файловым менеджером **Midnight Commander** рассмотрена в разделе 3.4.3.

4. Создание, просмотр и редактирование текстовых файлов

Работа с текстовыми файлами, в том числе их просмотр и редактирование выполняются при помощи текстовых редакторов **nano** (тектовый режим) и **Leafpad**.

Работа с текстовым редактором **Leafpad** рассмотрена в разделе 3.4.5.

Работа с текстовым редактором **nano** рассмотрена в разделе 3.4.6.

5. Редактирование реестра Windows

Просмотр и редактирование ключей реестра Windows выполняются при помощи файлового менеджера **Midnight Commander**. Ветви реестра Windows автоматически монтируются в файловую систему (используется каталог `/reg`) при загрузке **Dr.Web LiveCD**, после чего с ключами реестра можно работать как с обычными файлами (просматривать содержимое ключей и вносить в них изменение при необходимости).

Работа с файловым менеджером **Midnight Commander** рассмотрена в разделе 3.4.3.

Не смотря на то, что работа с содержимым реестра Windows ведется так же, как с каталогами и файлами, следует помнить, что ветви реестра не являются каталогами, а потому в них нельзя копировать обычные файлы и каталоги.

Также крайне не рекомендуется удалять, перемещать и переименовывать ветви и ключи реестра, поскольку это может привести к тому, что его структура окажется не читаемой в системе Windows, из-за чего операционная система (или некоторые ее компоненты) окажется полностью или частично неработоспособной.

6. Создание загрузочного носителя USB-flash

В состав сборки **Dr.Web LiveCD** входит специальная утилита автоматического создания загрузочной USB-flash, которая в дальнейшем может быть использована для аварийной загрузки компьютера аналогично **Dr.Web LiveCD**.

Работа с утилитой создания загрузочного носителя USB-flash рассмотрена в разделе 6.1.

7. Конфигурирование сетевых настроек

Изменение сетевых настроек компьютера (необходимо для подключения к интернету с целью загрузки обновлений вирусных баз) выполняется при помощи специальной утилиты, работающей в текстовом режиме. Изменение сетевых настроек следует выполнять только в том случае, когда конфигурация, автоматически созданная при загрузке **Dr.Web LiveCD**, не работает.

Работа утилиты конфигурирования сетевых настроек рассмотрена в разделе 6.3.

8. Конфигурирование внешнего вида графической оболочки

Изменение внешнего вида графического интерфейса и основного системного меню выполняется при необходимости при помощи специальной утилиты графической оболочки.

Работа с утилитой конфигурирования графического интерфейса рассмотрена в разделе 3.3.

9. Просмотр Интернет-сайтов

Просмотр интернет-сайтов, а также страниц справки по продукту **Dr.Web LiveCD** производится при помощи браузера **Firefox**.

Работа с браузером **Firefox** рассмотрена в разделе 3.4.1.

10. Отправка сообщений электронной почты

Работа с сообщениями электронной почты (создание, просмотр, прием и отправка), в том числе с сообщениями в службу поддержки компании **«Доктор Веб»**, выполняется при помощи приложения электронной почты **Sylpheed**.

Работа с приложением **Sylpheed** рассмотрена в разделе 3.4.2.

11. Работа с командной консолью Linux

Доступ к командной консоли ОС Linux осуществляется при помощи **Терминала**.

Работа с **Терминалом** рассмотрена в разделе 3.4.4.

12. Завершение работы, перезагрузка компьютера

Команды завершения работы с **Dr.Web LiveCD** расположены в основном системном меню графической оболочки. Системное меню открывается при нажатии на кнопку  на панели задач. Для завершения работы могут быть использованы следующие пункты системного меню:

Пункт	Назначение
Перезагрузка	Выполнение перезагрузки компьютера
Выключение	Выполнение выключения компьютера
Выйти	Завершение работы графической оболочки и возврат в основное загрузочное меню

3.2. Работа с Антивирусом Dr.Web в графической оболочке

В данном разделе описывается работа с **Антивирусом Dr.Web для Linux** в графической оболочке **Dr.Web LiveCD**.

Работа с **Антивирусом Dr.Web для Linux** в графической оболочке осуществляется через **Пульт управления**, имеющий графический интерфейс.

Запуск антивируса

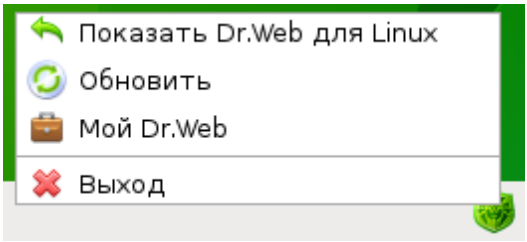
По умолчанию запуск **Пульта управления Dr.Web для Linux** осуществляется автоматически при начале работы с графической оболочкой **Dr.Web LiveCD**.

В случае если требуется запустить **Пульт управления** вручную (например, в случае если ранее его работа была завершена), то это можно сделать одним из следующих способов:

1. Двойной щелчок левой кнопкой мыши по иконке **Dr.Web Сканер** на рабочем столе графической оболочки;
2. Выбрать пункт  **Dr.Web Сканер** или **System → Dr.Web для Linux** в главном системном меню графической оболочки.

В случае если **Пульт управления Dr.Web для Linux** уже запущен, то в правом нижнем углу рабочего стола (в области уведомлений, рядом с индикатором системных часов) выводится иконка запущенного приложения:

Щелчок правой кнопкой мыши по иконке в области уведомления открывает на экране контекстное меню:

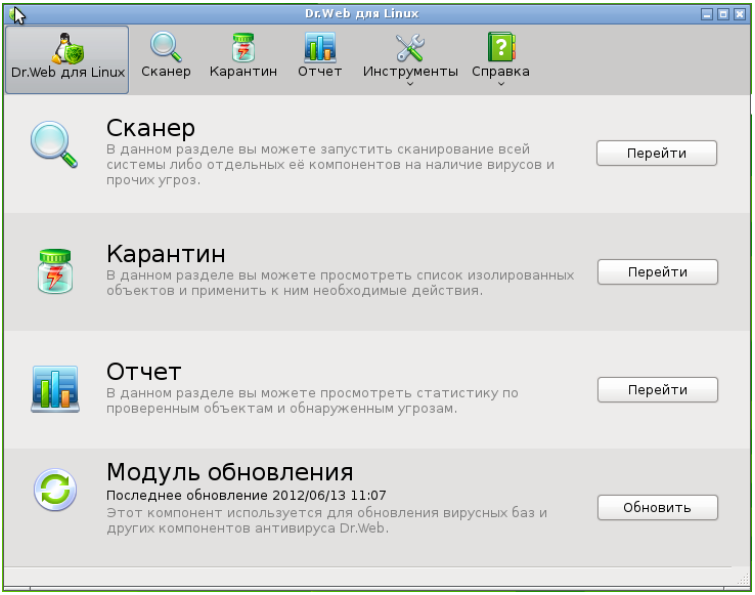


Контекстное меню имеет следующие пункты:

Пункт	Назначение
Показать/Скрыть Dr.Web для Linux	Показ или скрытие окна **Пульта управления Dr.Web для Linux**. Аналогичное действие – одиночный щелчок по иконке в области уведомлений
Обновить	Принудительный запуск обновления вирусных баз
Мой Dr.Web	Запуск браузера **Firefox** и открытие страницы персонального кабинета пользователя антивирусного продукта компании **«Доктор Веб»**
Выход	Завершение работы **Пульта управления Dr.Web для Linux**

Основное окно Пульта управления Dr.Web для Linux

Вид основного окна **Пульта управления** показан на рисунке ниже.



В верхней части окна расположена панель инструментов, предоставляющая доступ к основным функциям **Антивируса Dr.Web для Linux**.

На панели инструментов имеются следующие кнопки:

Кнопка	Назначение
Dr.Web для Linux	Переход к основной странице **Пульта управления** (показана на рисунке выше)
Сканер	Переход к странице управления **Сканером**
Карантин	Переход к странице просмотра **Карантина**
Отчет	Открытие окна просмотра отчета о работе **Сканера**
Инструменты	Открытие контекстного меню дополнительных инструментов **Антивируса Dr.Web для Linux** • **Настройки** – настройка работы **Антивируса Dr.Web для Linux** • **Журнал** – просмотр журнала работы **Антивируса Dr.Web для Linux**

	• **Менеджер лицензий** – просмотр имеющихся лицензий и работа с ключевыми файлами • **Послать подозрительный файл** – возможность отправить на проверку в компанию **«Доктор Веб»** подозрительный файл
Справка	Открытие контекстного меню справки и помощи: • **Справка** – открытие в браузере справки по продукту **Антивирус Dr.Web для Linux** • **Форум** – открытие в браузере страницы форума компании **«Доктор Веб»** • **Что нового** – открытие в браузере страницы новостей об антивирусных продуктах компании **«Доктор Веб»** • **О программе** – открытие окна с краткой информацией об наименовании и версии продукта

Задачи Пульта управления Dr.Web для Linux

При помощи **Пульта управления** Вы можете:

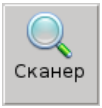
- Перейти к сканированию файлов, расположенных на компьютере;
- Просмотреть содержимое **Карантина**;
- Просмотреть отчеты о работе **Сканера**;
- Выполнить обновление антивирусных баз;
- Произвести настройку работы **Антивируса Dr.Web для Linux**;
- Просмотреть сведения об имеющейся лицензии;
- Послать на проверку подозрительный файл;
- Просмотреть справку и обратиться за технической поддержкой.

3.2.1. Антивирусная проверка

В данном разделе описывается процесс выполнения антивирусной проверки файлов компьютера **Антивирусом Dr. Web для Linux** в графической оболочке **Dr.Web LiveCD**.

Для начала сканирования необходимо:

1. Запустить **Пульт управления Dr.Web для Linux**, если он не запущен;

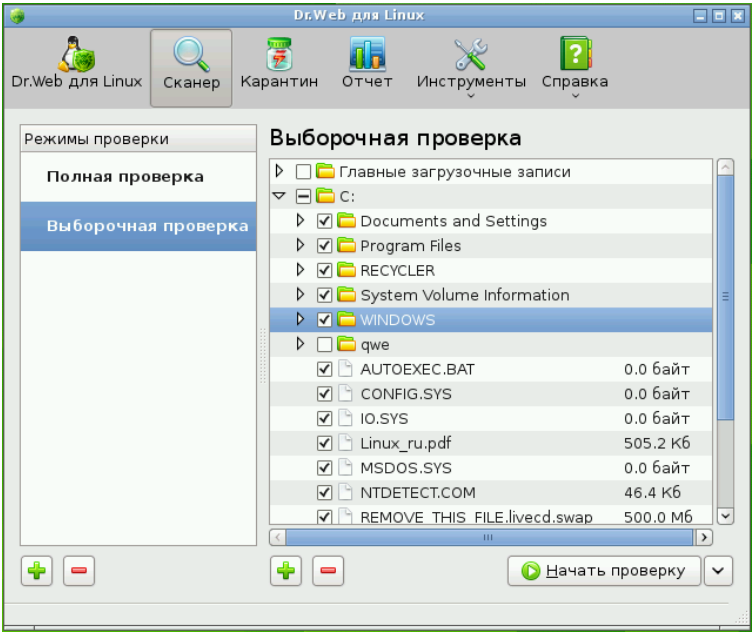
2. Перейти на страницу сканера, нажав кнопку 

на панели инструментов, или нажав кнопку **Перейти** в разделе **Сканер** главной страницы **Пульта управления**.

Перед началом сканирования рекомендуется обновить вирусные базы.

Запуск сканирования

Вид страницы запуска сканирования **Пульта управления Dr. Web** показан на рисунке ниже.



Выбор режима сканирования

В левой части страницы настроек сканирования расположен список основных режимов проверки, а в правой части – дерево выбора каталогов и файлов, подлежащих сканированию. Сканером предусмотрены следующие режимы проверки:

Режим сканирования	Описание
Полная проверка	В окне выбора каталогов и файлов для сканирования автоматически выбираются все файлы и все главные загрузочные записи (MBR), имеющиеся на всех дисках компьютера, исключая диск **Dr.Web LiveCD**. При этом пользователю становится недоступной возможность добавлять или исключать загрузочные записи, файлы и каталоги из проверки
Выборочная проверка	Окно выбора каталогов и файлов становится доступным для выбора пользователем загрузочных записей, дисков, каталогов и файлов, подлежащих сканированию

В случае если Ваш компьютер заражен вирусами, рекомендуется запускать **Сканер** в режиме **Полная проверка**. Диск **Dr.Web LiveCD** автоматически исключается из проверки в этом режиме для сокращения времени полного сканирования файлов, поскольку файлы системы **Dr.Web LiveCD** считаются заведомо не зараженными. Если вы все же хотите включить их в проверку, выберите режим **Выборочная проверка** и отметьте галочкой все диски, включая диск **Dr.Web LiveCD** (про выбор объектов для сканирования см. ниже).

Создание собственных режимов сканирования

Расположенные под списком режимов сканирования кнопки  и  позволяют редактировать список режимов сканирования, добавляя или удаляя из него собственные режимы сканирования, содержащие только объекты, выбранные пользователем.

Для добавления в список нового режима следует нажать кнопку  , ввести имя режима в появившемся окне, и нажать кнопку **ОК**. При добавлении нового режима сканирования в список он по умолчанию будет пустым (не будет выбран ни один объект для сканирования). Если выделить добавленный режим в списке режимов, а затем отметить в дереве выбора файлы и каталоги, сделанные отметки будут запомнены и будут автоматически выделяться при выборе данного режима в списке режимов.

Нажатие кнопки  позволяет удалить из списка режимов выделенный режим сканирования.

Двойной щелчок по названию режима в списке позволяет переименовать его (после изменения названия нужно нажать клавишу `ENTER`).

Стандартные режимы сканирования **Полная проверка** и **Выборочная проверка** переименовать и удалить из списка режимов сканирования невозможно.

Выбор файлов и каталогов для сканирования

Выбор загрузочных записей, дисков, каталогов и файлов, подлежащих сканированию, производится в дереве выбора каталогов и файлов. Выбор доступен только в случае если в списке режимов проверки выбран режим **Выборочная проверка** , или один из режимов сканирования, созданный Вами.

В корне дерева выбора изначально имеется отдельная ветвь **Главные загрузочные записи**, содержащая все загрузочные записи (*MBR – Master boot record*), расположенные на всех дисках, подключенных к компьютеру. Загрузочные записи содержат программный код, производящий запуск операционной системы, и могут подвергаться изменению и заражению со стороны ряда вирусов. Поэтому рекомендуется подвергать их обязательной проверке.

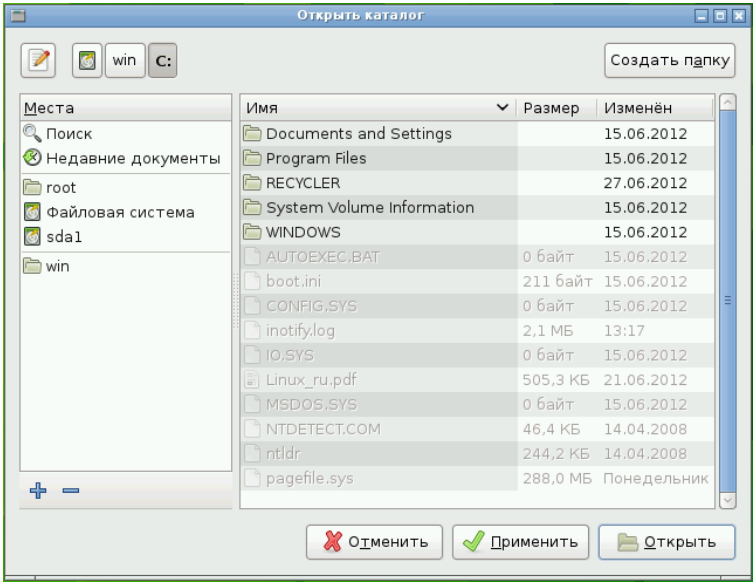
Помимо ветви **Главные загрузочные записи**, в корне дерева размещаются все диски, обнаруженные системой **Dr.Web LiveCD**. Обратите внимание, что система **Dr.Web LiveCD** автоматически распознает все диски и разделы, отформатированные в файловых системах FAT и NTFS, которые имеются на Вашем компьютере, и присваивает им соответствующие буквенные обозначения (`C:` , `D:` и т.п.), как это принято в операционных системах DOS и Windows.

Для разворачивания диска или каталога и просмотра его содержимого следует нажать на символ треугольника ▷, расположенный слева от названия диска или каталога. После этого ниже каталога в дереве, с отступом вправо, будут выведены каталоги и файлы, находящиеся в раскрытом каталоге. Если каталог развернут, треугольник принимает вид ▽. Чтобы свернуть развернутый каталог и скрыть его содержимое, достаточно снова щелкнуть по треугольнику ▽.

Для того чтобы выбрать элемент в дереве для последующей проверки, необходимо отметить флажок, находящийся в дереве слева от его имени. Повторный щелчок по флажку отключает его, убирая элемент из списка проверки. Включение флажка напротив имени каталога автоматически включает в проверку все содержимое каталога, включая вложенные каталоги со всем их содержимым. Если флажок слева от имени каталога или диска имеет вид ▪, то это означает, что не все файлы, содержащиеся в нем, выбраны для сканирования.

Кнопки  и  , расположенные под деревом выбора каталогов и файлов, позволяют добавлять в корень дерева выбора собственные пути для проверки конкретных каталогов.

Для добавления в список нового пути следует нажать кнопку  . После этого на экране откроется окно выбора каталогов. Вид окна выбора каталогов приведен на рисунке ниже:



В левой части окна расположена панель **Места**, позволяющая перейти к следующим начальным точкам для поиска каталогов:

- **Поиск** – поиск файла или каталога по всей имеющейся файловой системе;
- **Недавние документы** – открывает список документов и файлов, которые открывались программами;
- **root** – открывает домашний каталог суперпользователя Linux (окружение **Dr.Web LiveCD** работает с правами суперпользователя Linux);
- **Файловая система** – открывает корневой каталог файловой системы Linux (каталог /).

- **hdX*** или **sdX*** (где **X** – латинская буква (a, b, ...), а * – номер) – открывает содержимое диска, примонтированного к файловой системе Linux, как точка монтирования `/mnt/disk/hdX*` или `/mnt/disk/sdX*` соответственно.
- **win** – открывает список найденных дисков Windows (FAT, NTFS) с их буквенными обозначениями (`C:` , `D:` и т.п.), как это принято в операционных системах DOS и Windows (каждый из этих дисков соответствует своей логической точке монтирования `/mnt/disk/hdX*` или `/mnt/disk/sdX*`).

Содержимое выбранного каталога отображается в правой части окна в виде списка. Двойной щелчок по названию каталога в списке открывает его содержимое. Путь к текущему обозреваемому каталогу отображается в верхней части окна на панели выбора пути в виде набора кнопок, соответствующих пройденным по порядку каталогам («хлебные крошки»). При нажатии на кнопку осуществляется переход в соответствующий ей каталог.

Кнопки  и , расположенные под панелью **Места**, используются для добавления и удаления текущего каталога в эту панель. Для добавления каталога в список мест для быстрого доступа выберите его в файловой системе и нажмите кнопку  . Для удаления каталога из списка мест выберите его в списке **Места** и нажмите кнопку .

Для занесения выбранного каталога в список проверки следует нажать кнопку **Применить**. Для отмены добавления каталога в список проверки следует нажать кнопку **Отменить**.

Выбранный каталог всегда добавляется в корень дерева выбора каталогов и файлов для сканирования.

Нажатие кнопки  , расположенной под деревом выбора каталогов и файлов для сканирования, позволяет удалить из дерева выбора каталогов и файлов выделенный добавленный путь к каталогу. При этом физически каталог с диска не удаляется, а только отменяется его проверка, если он не выделен в стандартной части дерева (в качестве одного из каталогов, проверяемых на диске).

Обратие внимание, что файлы и каталоги, добавленные в настройках Сканера в список исключений, проверяться не будут.

Запуск сканирования

После выбора проверяемых дисков, каталогов и файлов для запуска процесса их проверки **Сканером** следует нажать кнопку **Начать проверку**.

Перед началом проверки рекомендуется определить, какие действия **Сканер** будет применять к подозрительным и зараженным файлам. Для этого необходимо нажать кнопку  , находящуюся справа от кнопки **Начать проверку**. При этом на экране появится выпадающее меню, содержащее два пункта:

Пункт меню	Описание
Действия применяются автоматически	При обнаружении опасностей различного вида **Сканер** будет автоматически выполнять действия, заданные в настройках
Действия выбираются вручную	При обнаружении опасностей **Сканер** будет выводить предупреждающее сообщение и предлагать пользователю выбрать, какое действие следует применить к опасному объекту

Для выбора требуемого поведения **Сканера** выберите соответствующий пункт меню. По умолчанию при сканировании **Сканер** будет использовать стратегию **Действия выбираются вручную**.

Результаты сканирования

В процессе работы **Сканера** на странице сканирования отображаются:

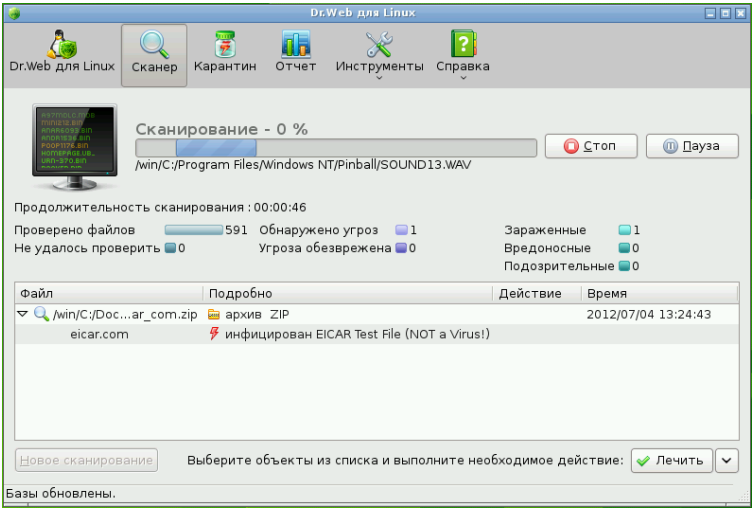
- Общий прогресс сканирования;

- Имя сканируемого в данный момент файла;
- Статистика сканирования по видам событий.

В любой момент времени сканирование можно остановить или поставить на паузу, нажав соответствующую кнопку справа от индикатора общего прогресса сканирования. В случае нажатия кнопки **Стоп** сканирование будет прервано и для начала нового сканирования потребуется нажать кнопку **Новое сканирование**. Нажатие кнопки **Пауза** позволяет выполнить временную приостановку сканирования, чтобы продолжить его через некоторое время. Результаты и настройки текущего сканирования при этом сброшены не будут и при возобновлении сканирование продолжится с прерванного места.

Результаты текущего (продолжающегося) или ранее завершенного сканирования отображаются в виде таблицы в нижней части страницы **Сканера**. Там представлены сведения о найденных в ходе сканирования зараженных и подозрительных объектах: об их местонахождении, о причине включения объекта в выборку, а также о действиях, произведенных программой над этими объектами.

Список обнаруженных объектов отображается в виде иерархической структуры. Например, 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. Вид страницы сканирования в процессе сканирования изображен на рисунке ниже.



На панели, расположенной под списком опасных объектов имеется кнопка, при помощи которой можно применить некоторое действие к объектам, выделенным в списке. Для выделения объекта в списке щелкните по нему мышью (удерживайте клавишу SHIFT, чтобы выделить несколько объектов подряд, или CTRL, чтобы выделить несколько разрозненных объектов).

После этого сначала нажатием кнопки  выбирается из выпадающего меню требуемое действие. Для применения выбранного действия нажимается кнопка действия (надпись и иконка на кнопке всегда совпадают с действием, которое было выбрано в выпадающем меню).

Перечень возможных действий:

Режим сканирования	Описание
Лечить	Применяется только к файлам, пораженным вирусами. Попытка извлечения вируса из тела файла без нарушения целостности самого файла
Переместить в Карантин	Перемещение файла из исходного места в каталог **Карантина** (невозможно, если файл доступен только для чтения)
Удалить	Безвозвратное удаление файла (невозможно, если файл доступен только для чтения)

Существуют следующие ограничения на возможные действия:

- лечение подозрительных объектов невозможно;
- перемещение, переименование или удаление объектов, не являющихся файлами (загрузочных секторов), невозможно;
- любые действия для отдельных файлов внутри архивов, контейнеров или в составе писем невозможны – действие в таких случае применяется только ко всему объекту целиком.

Если на вкладке **Действия** настроек **Сканера** в настройках действий для данного типа обнаруженных объектов было задано действие, отличное от **Сообщить**, то в столбце **Действие** будет отображаться результат действий, произведенных с файлом.

Если при попытке применить действие **Лечить** файл оказывается неизлечимым, то выполняется действие, указанное для неизлечимых объектов на вкладке **Действия** настроек **Сканера**.

Подозрительные файлы, перемещенные в карантин, рекомендуется передавать для дальнейшего анализа в антивирусную лабораторию **Dr.Web**, используя специальную форму на веб-сайте http://vms.drweb.com/sendvirus/.

Чтобы перейти к окну запуска сканирования, нажмите кнопку **Новое сканирование** (в процессе сканирования она недоступна, необходимо либо дождаться завершения сканирования, либо прервать его, нажав кнопку **Стоп**).

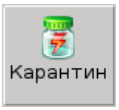
3.2.2. Просмотр карантина

В данном разделе описывается процесс работы с **Карантином**, хранящим подозрительные или зараженные объекты, выявленные в процессе антивирусной проверки файлов компьютера **Антивирусом Dr.Web для Linux**.

Карантин представляет собой специальный каталог в файловой системе, в который **Сканер** перемещает подозрительные или опасные объекты, которые не были вылечены, удалены или пропущены в процессе сканирования. В дальнейшем пользователь может просмотреть содержимое **Карантина** и принять решение, какие действия применить к объектам, попавшим в каталог **Карантина**.

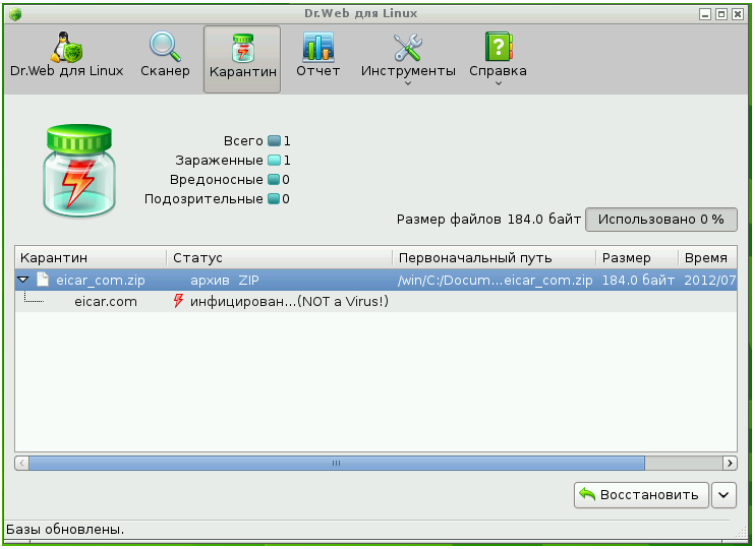
Для доступа к просмотру Карантина необходимо:

1. Запустить **Пульт управления Dr.Web для Linux**, если он не запущен;

2. Перейти на страницу карантина, нажав кнопку 

на панели инструментов, или нажав кнопку **Перейти** в разделе **Карантин** главной страницы **Пульта управления**.

Вид страницы просмотра **Карантина** показан на рисунке ниже.



Объекты, попавшие в **Карантин**, отображаются в виде таблицы в нижней части страницы. Там представлены следующие сведения о зараженных и подозрительных объектах:

- Название объекта;
- Статус (причина перемещения в **Карантин**);
- Первоначальное местоположение, из которого был перемещен объект;
- Размер объекта;
- Время перемещения в **Карантин**.

Список объектов отображается в виде иерархической структуры. Например, если в **Карантин** помещен архив, то инфицированный архив будет показан в списке в виде узла, который можно свернуть или развернуть для отображения его содержимого.

В **Карантине** хранятся:

1. Временные файлы, обозначенные иконкой . Это резервные копии заражённых и подозрительных файлов, для которых было выбрано действие **Лечить.** Также к временным файлам относятся резервные копии удалённых файлов (действие **Удалить**), что позволяет при необходимости восстановить удалённый файл.
2. Постоянные файлы, обозначенные иконкой . Это зараженные и подозрительные файлы, перемещённые в **Карантин** согласно соответствующим настройкам (действие **Переместить**). Поскольку алгоритмы лечения постоянно совершенствуются, данные файлы могут быть вылечены позднее.

Файлы первого типа хранятся в **Карантине** в течение ограниченного времени (указываемого в настройках), по истечении которого удаляются безвозвратно. Также они удаляются по исчерпании **Карантином** всего отведенного ему свободного места в разделе (на их место записываются новые файлы). Файлы второго типа могут быть удалены только пользователем (действие **Удалить**).

По умолчанию **Карантин** находится в подкаталоге `.drweb` домашнего каталога пользователя.

Работа с содержимым Карантина

На панели, расположенной под списком объектов, имеется кнопка, при помощи которой можно применить некоторое действие к объектам, выделенным в списке. Для выделения объекта в списке щелкните по нему мышью (удерживайте клавишу `SHIFT`, чтобы выделить несколько объектов подряд, или `CTRL`, чтобы выделить несколько разрозненных объектов).

После выделения объектов сначала нажатием кнопки выбирается из выпадающего меню требуемое действие. Для применения выбранного действия нажимается кнопка действия (надпись и иконка на кнопке всегда совпадают с действием, которое было выбрано в выпадающем меню).

Перечень возможных действий:

Режим сканирования	Описание
Восстановить	Файл из каталога **Карантина** будет перемещен в исходное место
Восстановить в ...	Файл из каталога **Карантина** будет перемещен в указанный каталог
Удалить	Безвозвратное удаление файла из каталога **Карантина**

Подозрительные файлы, перемещенные в карантин, рекомендуется передавать для дальнейшего анализа в антивирусную лабораторию **Dr.Web**, используя специальную форму на веб-сайте http://vms.drweb.com/sendvirus/.

Пожалуйста, обратите внимание, что каталог **Карантина** создается на временном RAM-диске, поэтому резервные копии файлов, сохраненные в **Карантине**, будут утрачены, если их не сохранить на один из жестких (физических) дисков компьютера.

Чтобы обеспечить сохранность файлов, попавших в **Карантин**, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться утилитой создания снапшотов (доступна только в расширенном режиме).

3.2.3. Просмотр отчета

В данном разделе описывается процесс работы с отчетом о результатах антивирусной проверки файлов компьютера **Антивирусом Dr.Web для Linux**. В отчете хранится информация о вредоносных объектах и прочих информационных угрозах, обнаруженных на вашем компьютере **Сканером**. Инструмент **Отчет** позволяет вам просмотреть статистику обнаружения и, при необходимости, удалить устаревшие данные.

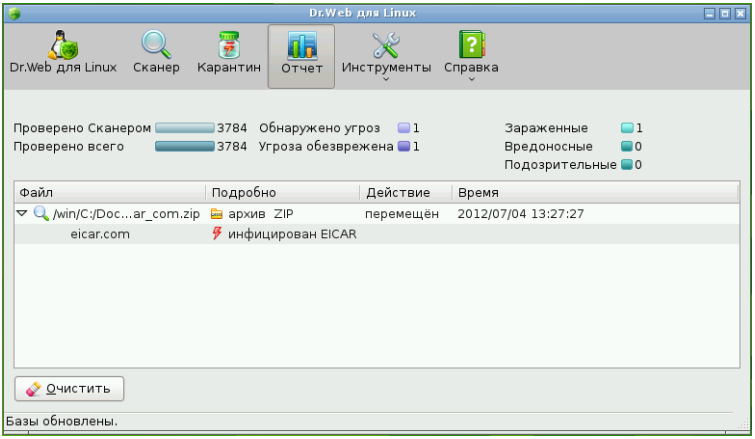
Для доступа к просмотру отчета необходимо:

1. Запустить **Пульт управления Dr.Web для Linux**, если он не запущен;

2. Перейти на страницу отчета, нажав кнопку 

на панели инструментов, или нажав кнопку **Перейти** в разделе **Отчет** главной страницы **Пульта управления**.

Вид страницы просмотра отчета о работе **Антивируса Dr.Web для Linux**, приведен на рисунке ниже.



В верхней части окна отображается общая статистика по обнаруженным угрозам.

В нижней части окна расположена кнопка **Очистить**, с помощью которой можно удалить все данные из **Отчета**.

Средняя часть окна содержит таблицу обнаруженных объектов, представляющих угрозу информации на вашем компьютере:

Колонка	Описание
Файл	Указывает путь и имя файла, содержащего угрозу.
Подробно	Содержит информацию об угрозе (например, название или тип угрозы).
Действие	Содержит информацию о действии, которое было применено для устранения угрозы (пустое поле означает, что действие к данному объекту применено не было).
Время	Указывает время обнаружения угрозы.

3.2.4. Обновление вирусных баз

По всему миру постоянно появляются новые типы компьютерных угроз с более совершенными маскировочными функциями. Обновление антивирусных баз и других компонентов **Антивируса Dr.Web для Linux** гарантирует соответствие защиты вашего компьютера современным требованиям и ее готовность к новым угрозам. Обновление выполняет специальный компонент, называемый **Модулем обновления**.

Рекомендуется периодически запускать **Модуль обновления**.

Запуск обновления

1. Запустить **Пульт управления Dr.Web для Linux**, если он не запущен;

2. Нажать кнопку **Обновить** в разделе **Модуль обновления** главной страницы **Пульта управления**, или щелкнуть правой кнопкой мыши по значку **Антивируса**  в области уведомлений панели задач графической оболочки и выбрать пункт меню **Обновить**.

3.2.5. Настройка работы Антивируса Dr.Web

Доступ к настройке работы **Антивируса Dr.Web для Linux** осуществляется следующим образом:

1. Запустить **Пульт управления Dr.Web для Linux**, если он не запущен;

2. Перейти на страницу управления настройками, нажав на панели инструментов **Пульта управления** кнопку 

, и выбрав в выпадающем меню пункт **Настройки**.

Страница управления настройками **Антивируса Dr.Web для Linux** делится на несколько вкладок:

- **Сканер** – Настройка работы **Сканера**;
- **Карантин** – Настройка работы **Карантина**;
- **Обновления** – Настройка работы **Модуля обновления**;
- **Уведомления** – Настройка уведомлений.

В нижней части окна управления настройками **Антивируса Dr.Web для Linux** расположены следующие кнопки:

- **По умолчанию** – сбросить пользовательские изменения настроек и вернуть настройки по умолчанию;
- **ОК** – сохранить изменения и вернуться в главное окно **Пульта управления Dr.Web для Linux**;
- **Применить** – сохранить изменения и остаться в окне настроек;
- **Отменить** – вернуться в главное окно **Пульта управления Dr.Web для Linux** без сохранения изменений в настройках.

Пожалуйста, обратите внимание, что в процессе работы **Dr.Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все изменения, внесенные в настройки программ, входящих в состав диска, будут утеряны при перезагрузке компьютера.

Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

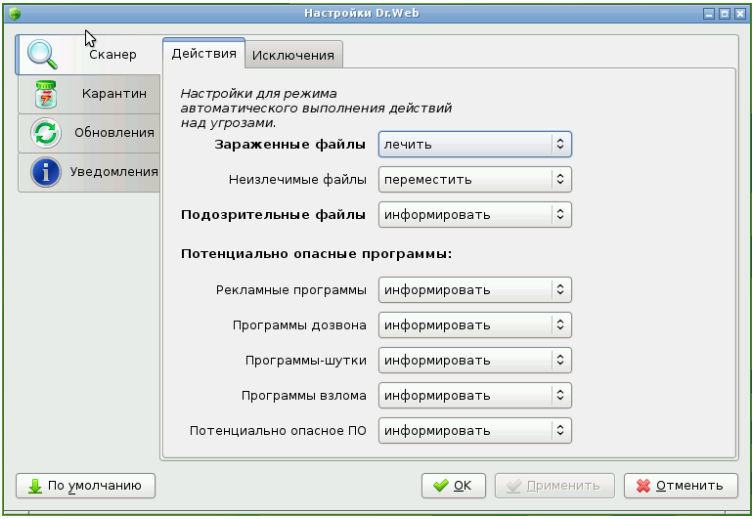
Настройки Сканера

На странице настроек **Сканера** имеется две вкладки:

- **Действия** – Настройка действий, применяемых **Сканером** при обнаружении подозрительных и вредоносных объектов в автоматическом режиме проверки;
- **Исключения** – Настройка исключения файлов и каталогов из проверки **Сканером**.

Вкладка Действия

Вид вкладки **Действия** показан на рисунке ниже.



На этой вкладке Вы можете задать действия, которые должны применяться к различным типам компьютерных угроз автоматически, если не требуется выбрать необходимое действие вручную.

Для различных типов угроз можно выбрать одно из следующих действий:

- **Лечить** (доступно только для **зараженных файлов**) – попытаться излечить объект, зараженный известным вирусом, а в случае невозможности (например, если вирус неизлечим) – отработать реакцию, заданную для **неизлечимых файлов**. Данное действие используется по умолчанию для всех инфицированных файлов.
- **Удалить** – удалить зараженный или подозрительный файл.
- **Переместить** – переместить зараженный или подозрительный файл в каталог Карантина. Данное действие используется по умолчанию для **неизлечимых файлов**.
- **Информировать** – информировать пользователя об обнаружении угрозы в поле отчета. В таком случае действия над файлами необходимо выполнить вручную. По умолчанию данное действие используется для

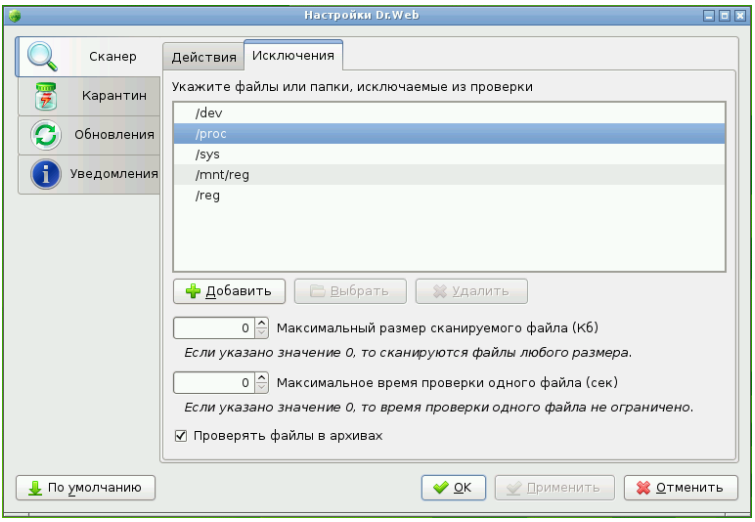
подозрительных файлов и **потенциально опасных программ**, таких как программы для взлома, программы-шутки и т.п.

- **Игнорировать** (доступна для **подозрительных файлов** и всех **потенциально опасных программ**) – пропустить файл (при этом в журнал будет выведена запись о том, что данный файл заражен).

Настройки, заданные на вкладке **Действия** по умолчанию, являются оптимальными для полноценной защиты вашего компьютера. Не рекомендуется изменять настройки без необходимости.

Вкладка Исключения

Вид вкладки **Исключения** показан на рисунке ниже.



На этой вкладке вы при необходимости можете сформировать список файлов и каталогов, которые следует исключить из проверки. Поскольку каталог **Карантина** предназначен для изоляции опасных объектов и доступ к нему заблокирован, то он исключается из проверки автоматически, и его добавлять в

список исключений не требуется.

Настройка списка исключений

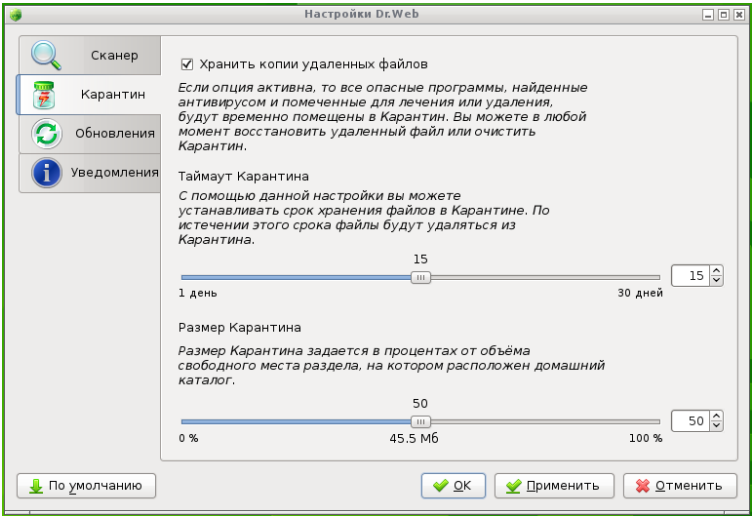
1. Чтобы добавить файл или каталог в список исключений:
   - Нажмите кнопку **Добавить**.
   - В появившемся окне выбора каталогов и файлов укажите нужный объект и нажмите **Применить**.
2. Чтобы изменить каталог и/или файл из списка, выделите его в списке и нажмите **Выбрать**.
3. Чтобы удалить файл или каталог из списка исключений, выберите его в списке и нажмите **Удалить**.
4. Также имеется возможность ограничить максимальный размер проверяемых файлов (файлы больше указанного размера будут пропускаться без проверки), а также максимальное время проверки одного файла, чтобы антивирус не "зависал" при проверке очень больших и поврежденных файлов. Для этого укажите соответствующие значения в полях-счетчиках. Значение 0 в поле снимает соответствующее ограничение.
5. Чтобы исключить из проверки содержимое архивов всех типов, отключите флажок **Проверять файлы в архивах**.

Предустановленные настройки исключений являются оптимальными для большинства применений, их не следует изменять без необходимости. Кроме того, некоторые каталоги, внесенные в список исключений, удалить из этого списка невозможно.

Обратите внимание, что файлы, включенные в список исключений, не будут проверяться, даже если они будут выбраны для сканирования при старте сканирования.

Настройки Карантина

На странице настроек **Карантина** имеется возможность задать размер калога, отведенного для хранения файлов, помещенных в карантин, а также длительность хранения файлов в карантине. Вид вкладки **Карантин** показан на рисунке ниже.

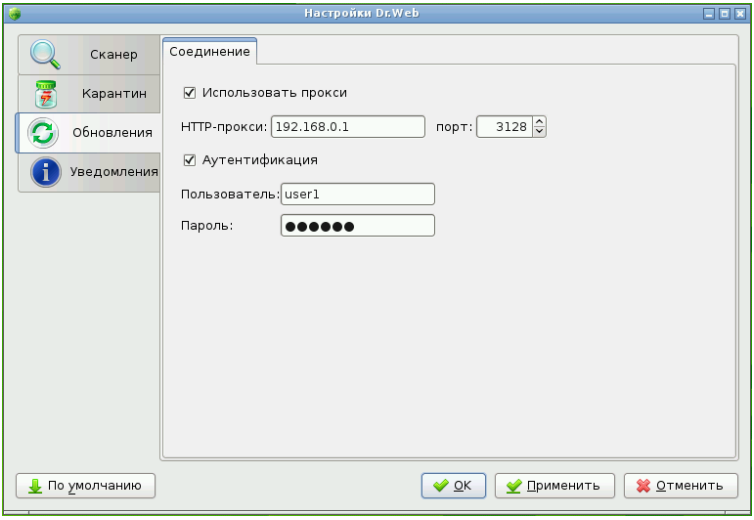


Для различных типов угроз можно выбрать одно из следующих действий:

- Установка флажка **Хранить копии удаленных файлов** предписывает **Сканеру** при удалении любого зараженного или вредоносного объекта помещать его копию в **Карантин**. Если флажок не установлен, удаляемые объекты будут удаляться безвозвратно.
- При помощи ползунка **Таймаут Карантина** имеется возможность задания срока хранения в **Карантине** копий удаленных файлов (файлы, перемещенные в **Карантин**, хранятся там постоянно, пока не будут восстановлены или окончательно удалены пользователем);
- При помощи ползунка **Размер Карантина** определяется максимально разрешенный объем места на диске (в процентах от общего объема), который может занимать каталог **Карантина**. При достижении этого размера из **Карантина** удаляются копии удаленных файлов.

Настройки Модуля Обновления

На странице настроек **Модуля Обновления** имеется вкладка **Соединение**, вид которой показан на рисунке ниже.



На этой вкладке вы при необходимости можете включить использование прокси-сервера для обращения к серверам обновления и задать настройки подключения к нему.

Для использования прокси-сервера установите флажок **Использовать прокси**. При включении режима использования прокси-сервера требуется указать следующие данные:

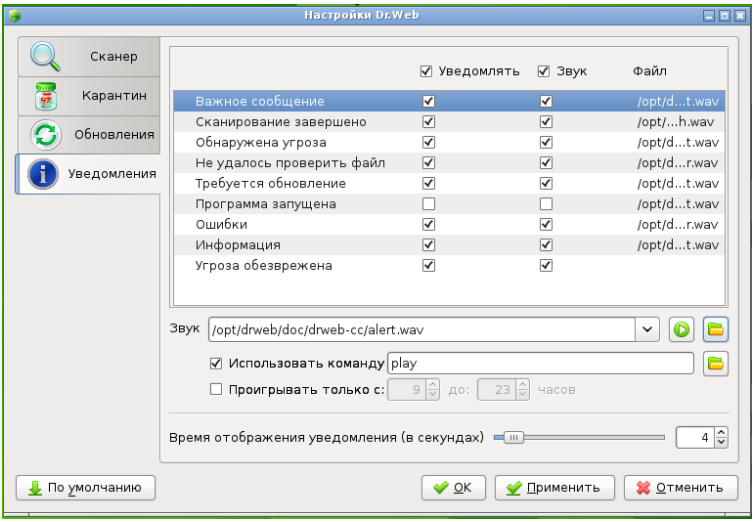
- **HTTP-прокси** – укажите имя или IP-адрес используемого прокси-сервера;
- **порт** – укажите номер используемого порта;
- **Аутентификация** – если используемый прокси-сервер требует аутентификации, то включите этот флажок и укажите имя пользователя (логин) и пароль в полях **Пользователь** и **Пароль** соответственно.

Использование прокси-сервера может потребоваться только в том случае, если политикой вашей локальной сети запрещено обращение ко всем внешним серверам или только к серверам обновления компании **«Доктор Веб»**.

Настройки уведомлений

На этой вкладке имеется возможность настройки уведомлений, при помощи **Антивирус Dr.Web для Linux** будет уведомлять пользователя о различных событиях, происходящих в ходе работы антивируса.

Вид вкладки **Уведомления** показан на рисунке ниже.



Уведомления бывают двух типов:

- **Экранные** – при возникновении события на экране появляется всплывающее окно с текстовым сообщением
- **Звуковые** – при возникновении события раздается звуковой сигнал.

Настройка уведомлений

1. При необходимости поменяйте настройки звуковых уведомлений:
   - Чтобы отключить или включить все звуковые оповещения, снимите или установите флажок **Звук** в верхней части вкладки.
   - Чтобы отключить или включить звуковые оповещения для определённых событий, снимите или установите соответствующий флажок в столбце **Звук**.
   - Чтобы сопоставить событию определенный звук, выделите название события в списке, а затем выберите один из имеющихся звуков в выпадающем списке **Звук**. Чтобы добавить к выпадающему списку новую мелодию, нажмите кнопку **Выбрать** и выберите звуковой файл. При необходимости вы также можете задать команду для проигрывания файла и интервал в течение дня, во время которого разрешено использование звукового оповещения. Чтобы проиграть выбранный файл, нажмите кнопку **Воспроизводить звук**.
2. При необходимости поменяйте настройки экранных уведомлений:
   - Используйте ползунок, чтобы установить время, в течение которого сообщение должно отображаться на экране.
   - По умолчанию экранные оповещения включены. Чтобы отключить или включить все экранные оповещения, снимите или установите флажок **Уведомлять** в верхней части вкладки.
   - Чтобы отключить или включить экранные оповещения для определённых событий, снимите или установите соответствующий флажок **Уведомлять** в столбце.

3.2.6. Просмотр журнала событий

В данном разделе описывается процесс работы с журналом, содержащим сообщения, возникающие в процессе работы **Антивируса Dr.Web для Linux**. В журнал помещается информация о пропущенных вредоносных объектах, об ошибках

и уведомлениях, возникшим в процессе работы антивируса. Инструмент **Журнал** позволяет вам просмотреть содержимое журнала и, при необходимости, экспортировать записи из журнала и удалить устаревшие данные.

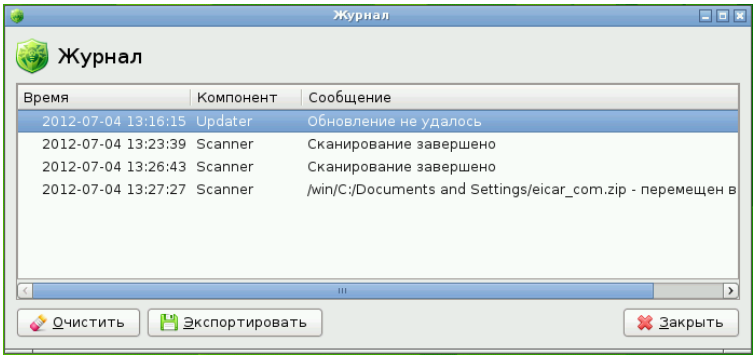
Для доступа к просмотру журнала необходимо:

1. Запустить **Пульт управления Dr.Web для Linux**, если он не запущен;

2. Перейти в окно просмотра журнала, нажав кнопку 

на панели инструментов и выбрав в появившемся выпадающем меню пункт **Журнал**.

Вид окна просмотра журнала **Антивируса Dr.Web для Linux** приведен на рисунке ниже.



В нижней части окна расположены:

- кнопка **Очистить**, с помощью которой можно удалить все записи из **Журнала**.
- кнопка **Экспортировать**, при помощи которой можно сохранить записи журнала в текстовый файл (имя и местоположение файла выбираются в открывающемся окне сохранения файла).

Средняя часть окна содержит таблицу сообщений журнала. Для

каждого сообщения указывается:

Колонка	Описание
Время	Время формирования записи
Компонент	Имя компонента **Антивируса**, сгенерировавшего данное сообщения
Сообщения	Текст сообщения, сформированного компонентом, или описание возникшего события

Нажатие кнопки **Закрыть** закрывает окно просмотра журнала.

3.2.7. Просмотр сведений о лицензии

Разрешенные режимы работы **Антивируса Dr.Web для Linux** и перечень доступных функций определяются активной лицензией. При скачивании программного продукта **Dr.Web LiveCD** с сайта компании **«Доктор Веб»** пользователю автоматически предоставляется лицензия на использование **Антивируса Dr.Web для Linux** в базовой конфигурации, достаточной для выполнения задач антивирусной проверки компьютера.

Параметры действующей лицензии хранятся в ключевом файле, располагающемся на **Dr.Web LiveCD**.

Номер выданной лицензии и сроки ее действия можно просмотреть в специальном окне **Пульта управления Dr.Web для Linux**.

Обратите внимание, что лицензия, предоставленная при получении **Dr.Web LiveCD** с сайта компании, имеет срок действия 2 года. По истечению срока действия лицензии вам придется или скачать новую версию продукта **Dr.Web LiveCD**, или приобрести новый ключ к этой лицензии.

Подробнее о приобретении и продлении лицензий см. на сайте компании **«Доктор Веб»**: www.drweb.com

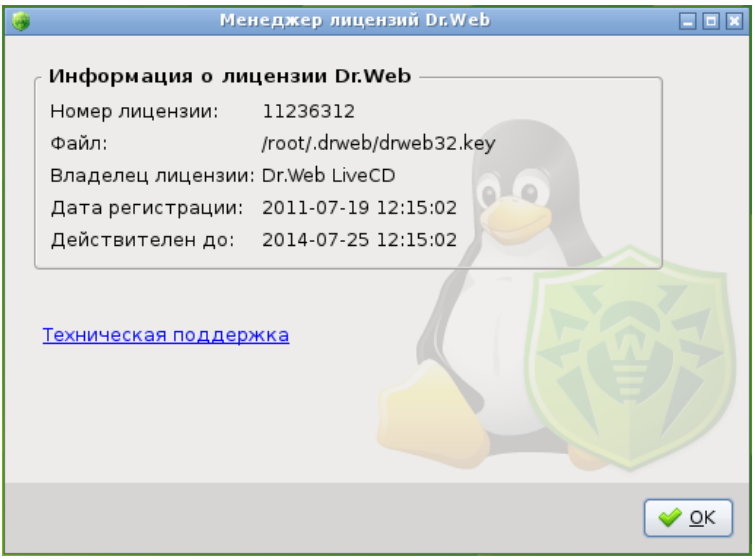
Для просмотра сведений о лицензии:

1. Запустите **Пульт управления Dr.Web для Linux**, если он не запущен;

2. Откройте окно просмотра сведений о лицензии, нажав кнопку 

на панели инструментов и выбрав в появившемся выпадающем меню пункт **Менеджер лицензий**.

Вид окна просмотра сведений о лицензии на **Антивирус Dr.Web для Linux** приведен на рисунке ниже.



Нажатие кнопки **ОК** закрывает окно просмотра сведений о лицензии.

Нажатие на ссылку **Техническая поддержка** открывает в браузере **Firefox** страницу обращения в техническую поддержку компании **«Доктор Веб»**.

3.2.8. Отправка файлов на анализ

В случае если **Антивирус Dr.Web для Linux** обнаружил неизвестный вирус или пометил какой-либо файл как подозрительный, рекомендуется отправлять такой файл на анализ в антивирусную лабораторию компании **«Доктор Веб»**.

Для этого необходимо, чтобы в процессе проверки **Сканер** переместил подозрительный файл в каталог **Карантина**, или удалил его с помещением копии в **Карантин** (см. соответствующие настройки Сканера и Карантина). Кроме того, можно в процессе проверки разрешить **Сканеру** пропустить файл, и запомнить путь к нему (или посмотреть его в Отчете).

Для отправки подозрительного файла на анализ:

1. Откройте в браузере страницу отправки файлов http://vms.drweb.com/sendvirus/. Например, это можно сделать, нажав на панели **Пульта управления Dr.Web для Linux** кнопку 

и выбрав в появившемся выпадающем меню пункт **Послать подозрительный файл**.

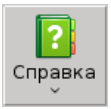
2. Следуйте инструкциям, представленным на странице отправки вируса.

Обратите внимание, что путь к каталогу **Карантина** имеет вид:

`~/.drweb/quarantine` или `/root/.drweb/quarantine` (поскольку работа ведется в режиме суперпользователя Linux **root**).

3.2.9. Получение помощи и просмотр справки

В случае если Вам требуется помощь по работе с продуктом **Антивирус Dr.Web для Linux**, доступ к справочным материалам осуществляется на панели **Пульта управления Dr.Web для Linux**.

Для этого нажмите на панели инструментов кнопку 

и выберите в появившемся выпадающем меню требуемый пункт:

- **Справка** – открытие в браузере справки по продукту **Антивирус Dr.Web для Linux**.
- **Форум** – открытие в браузере страницы форума компании **«Доктор Веб»**.
- **Что нового** – открытие в браузере страницы новостей об

антивирусных продуктах компании **«Доктор Веб»**.

- **О программе** – открытие окна с краткой информацией об наименовании и версии продукта.

Для обращения в службу технической поддержки воспользуйтесь ссылкой support.drweb.com.

3.3. Настройка графической оболочки

Настройка вида графической оболочки **Dr.Web LiveCD** доступна через пункт **Settings** системного меню и включают следующие опции:

- Adobe Flash Player – настройка параметров мультимедиа-плеера **Adobe Flash Player**;
- Внешний Вид – настройка параметров графической оболочки;
- Конфигурация Меню – настройка панели задач графической оболочки;
- Конфигурация сети – настройка сетевого соединения с Интернет.

Чтобы задать настройки, откройте системное меню, нажав кнопку  в углу панели задач, и выберите интересующий пункт в подменю **Settings**. На экране откроется соответствующее окно настроек.

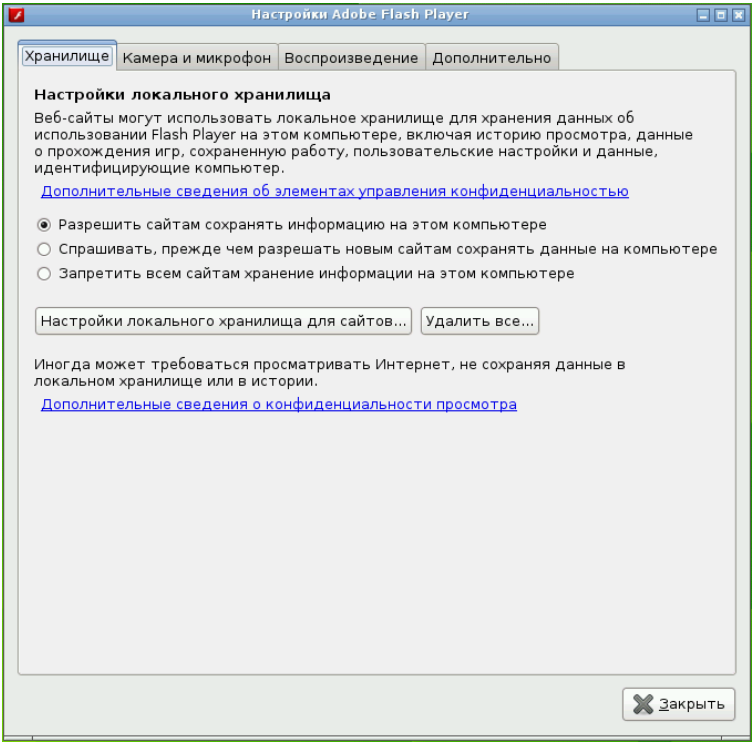
Пожалуйста, обратите внимание, что в процессе работы **Dr.Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все изменения, внесенные в настройки программ, входящих в состав диска, будут утеряны при перезагрузке компьютера.

Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

3.3.1. Настройки Adobe Flash Player

Adobe Flash Player – это плеер, предназначенный для воспроизведения мультимедиа (видео, аудио), встраиваемого в веб-страницы. Кроме того он используется некоторыми веб-приложениями. Окно настройки параметров **Adobe Flash Player** позволяет настроить параметры хранения персональных данных, используемых flash-приложениями, а также параметры доступа к видеокамере и микрофону, имеющимся на компьютере.

Вид окна настройки параметров **Adobe Flash Player** показан на рисунке ниже.



При помощи данного окна вы можете настроить следующие параметры **Adobe Flash Player**:

- Вкладка **Хранилище**. На этой вкладке вы можете разрешить или запретить сайтам, которые вы будете посещать в браузере, сохранять на локальном компьютере данные Adobe Flash. Вы можете разрешить сайтам сохранять информацию безусловно, или по запросу (перед попыткой сохранить данные будет выдаваться запрос, который можно будет подтвердить или отвергнуть). Режим разрешения выбирается пометкой соответствующего переключателя. Нажатие кнопки **Настройки локального хранилища для сайтов...** позволяет задать режим хранения данных для разных сайтов индивидуально. Нажатие кнопки **Удалить все...** позволяет выполнить полную очистку хранилища.
- Вкладка **Камера и микрофон**. На этой вкладке вы можете задать разрешение на использование сайтами видеокамеры и микрофона, подключенных к этому компьютеру (разрешать безусловно или по запросу). Нажав кнопку **Настройки камеры и микрофона для веб-сайта...**, можно настроить параметры разрешения для разных сайтов индивидуально.
- Вкладка **Воспроизведение**. На этой вкладке вы можете разрешить сайтам использовать при воспроизведении видео пиринговые сети (безусловно или по запросу). Дополнительно можно настроить разрешение на использование пиринговых сетей для разных сайтов индивидуально.
- Вкладка **Дополнительно**. На этой вкладке вы можете выполнить дополнительную настройку **Adobe Flash Player**:
  - Удалить все настройки хранилища, очистить все разрешения для сайтов;
  - Выполнить проверку наличия обновлений для **Adobe Flash Player**;
  - Выполнить деавторизацию компьютера, удалив с него всю персональную информацию, используемую **Adobe Flash Player**;
  - Настроить перечень доверенных папок для тестовых целей (не рекомендуется).

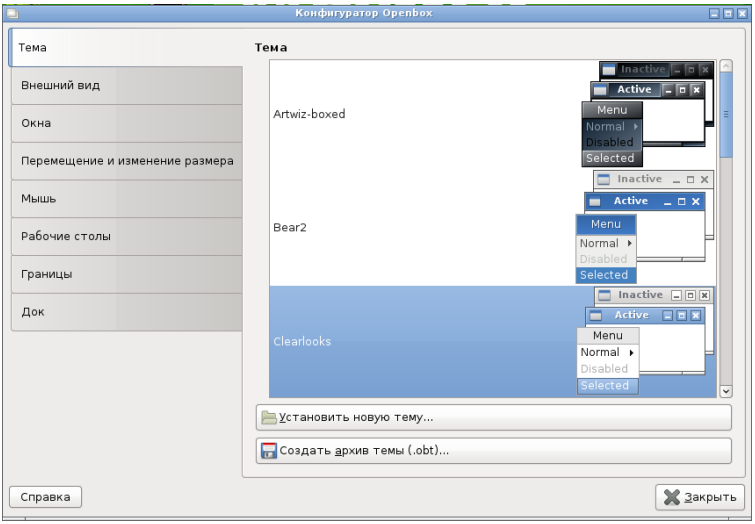
Нажатие на ссылки **Дополнительные сведения о ...**, расположенные на вкладках окна настройки, приведет к открытию в браузере страниц с дополнительной информацией о настройке **Adobe Flash Player**.

Любое изменение параметров **Adobe Flash Player**, внесенное в данном окне, применяется сразу. Нажатие кнопки **Закрыть** закрывает окно настройки.

3.3.2. Внешний вид

Графическая оболочка **Dr.Web LiveCD** основана на облегченной графической оболочке Openbox Linux-систем.

Вид окна настройки параметров графической оболочки **Dr.Web LiveCD** представлен на рисунке ниже.



При помощи данного окна вы можете настроить следующие параметры графической оболочки:

- Вкладка **Тема**. На этой вкладке вы можете выбрать общий стиль оформления всех окон оболочки (цвета фона, заголовков и т.п.).

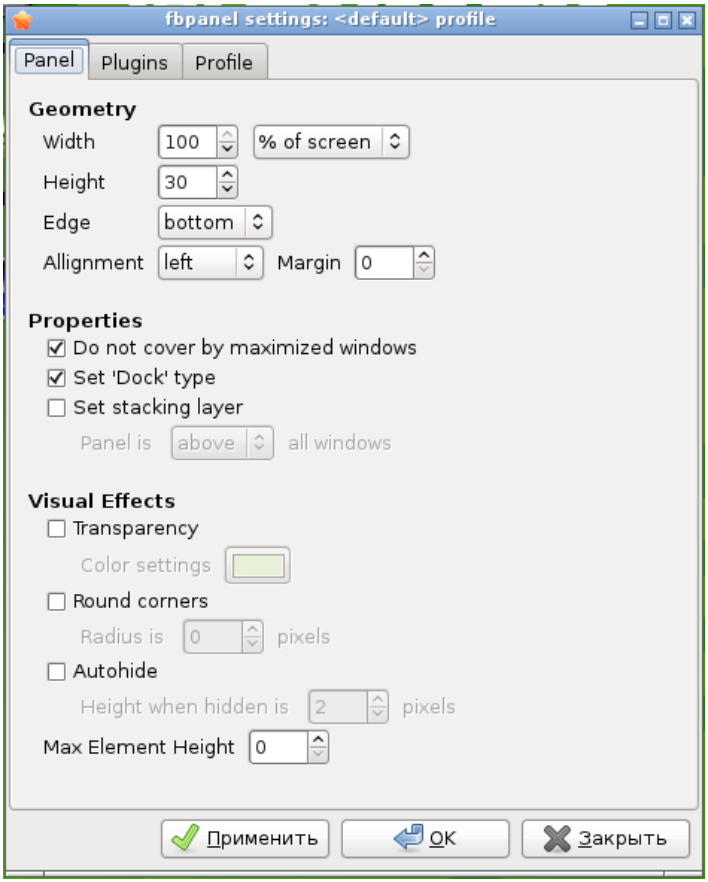
- Вкладка **Внешний вид**. На этой вкладке вы можете задать параметры окон (вид и оформление строки заголовка, используемые шрифты и т.п.).
- Вкладка **Окна**. На этой вкладке вы можете настроить поведение окон при их открытии (таких как получение фокуса ввода, расположение по центру экрана и т.п).
- Вкладка **Перемещение и изменение размера**. На этой вкладке вы можете настроить параметры изменения размеров окон и их перемещения.
- Вкладка **Мышь**. На этой вкладке вы можете настроить реакцию окон приложений на перемещение курсора мыши (такую, как получение фокуса).
- Вкладка **Рабочие столы**. На этой вкладке вы можете настроить количество используемых рабочиих столов (по умолчанию четыре) и параметры переключения между ними.
- Вкладка **Границы**. На этой вкладке вы можете указать размеры (ширину) границ рабочего стола.
- Вкладка **Док**. На этой вкладке вы можете настроить параметры дока – специальной области на краю экрана, к которой "прицепляются" графические модули "док-приложений" (типа часов. клендаря и т.п.).

Любое изменение параметров графической облочки, внесенное в данном окне, применяется сразу. Нажатие кнопки **Закрыть** закрывает окно настройки.

3.3.3. Конфигурация меню

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

Вид окна настройки панели задач показан на рисунке ниже.



При помощи этого окна вы можете задать следующие параметры:

- Геометрию панели (раздел **Geometry**):
  - **Width**: Ширина в точках или относительно ширины экрана в процентах,
  - **Height**: Высота в точках;
  - **Edge**: Положение панели на экране (слева, справа, сверху, снизу);
  - **Alignment**: Выравнивание элементов на панели (по левому краю, по правому краю, по центру);
  - **Margin**: Отступ от края рабочего стола в пикселях.
- Свойства панели (раздел **Properties**):
  - **Do not cover by maximized windows** – положение поверх всех окон;
  - **Set 'Dock' Type** – использование док-панели;
  - **Set stacking layer** – разрешение панели задач размещаться над или под окнами (с выбором режима расположения);
- Визуальные эффекты (**Visual Effects**):
  - **Transparency** – эффект прозрачности панели и соответствующие цветовые настройки (**Color settings**);
  - **Round corners** – эффект загругленных углов (и радиусы соответствующих окружностей **Radius is**);
  - **Autohide** – автоматическое скрытие панели при отведении курсора мыши (дополнительно указывается высота панели в "скрытом" состоянии);
  - **Max Element Height** – максимальная высота элемента на панели задач.

На вкладке **Plugins** имеется возможность просмотреть состав плагинов (компонентов), отображаемых на панели задач, и при необходимости настроить его (изменить порядок следования плагинов, добавить или удалить компонент).

На вкладке **Profile** выводится информация о файле, в котором хранятся все настройки профиля, отображаемые в окне настройки панели задач (этот файл находится в каталоге `/root/.config/fbpanel` и называется `default`).

Нажатие кнопки **Применить** позволяет применить внесенные изменения немедленно, не закрывая окно. Нажатие кнопки **ОК** применяет изменения и закрывает окно. Нажатие кнопки **Закрыть** закрывает окно без внесения изменений в настройки панели.

3.4. Встроенные приложения

В данном разделе описываются приложения, входящие в состав **Dr.Web LiveCD**. Доступ к ним осуществляется с помощью иконок, находящихся на рабочем столе графической оболочки, пунктов системного меню, а также пунктов меню расширенного режима.

3.4.1. 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. 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»**.

Запуск браузера в графической оболочке

Для запуска браузера выполните любое из следующих действий:

- Выполните двойной щелчок левой кнопкой мыши по иконке  **Firefox** на рабочем столе;

- Кликните мышью по иконке  на панели задач;
- Выберите пункт **Network → Mozilla Firefox** в главном системном меню графической оболочки.

Запуск браузера в текстовом режиме

Запуск браузера в текстовом режиме невозможен. Для просмотра веб-сайтов перейдите сначала в режим графической оболочки.

Пожалуйста, обратите внимание, что в процессе работы **Dr. Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все страницы, сохраненные на него, а также история просмотра браузера будут утеряны при перезагрузке компьютера. Если вам требуется сохранить посещенные страницы, сохраняйте их на жесткий диск.

Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

Подробнее о работе с браузером **Mozilla Firefox** вы можете ознакомиться на сайте разработчика: http://support.mozilla.org/.

3.4.2. Почтовый клиент

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

Запуск почтового клиента в графической оболочке

Для запуска почтовой программы выполните любое из следующих действий:

- Выполните двойной щелчок левой кнопкой мыши по иконке  **Sylpheed** на рабочем столе;

- Кликните мышью по иконке  на панели задач;
- Выберите пункт **Network → Почта** в главном системном меню графической оболочки.

Запуск почтового клиента в текстовом режиме

Запуск почтового клиента **Sylpheed** в текстовом режиме невозможен. Для запуска почтовой программы перейдите сначала в режим графической оболочки.

Если вам необходимо отправить почтовое сообщение в текстовом режиме, воспользуйтесь утилитой **ssmtp**.

Работа с почтовым клиентом

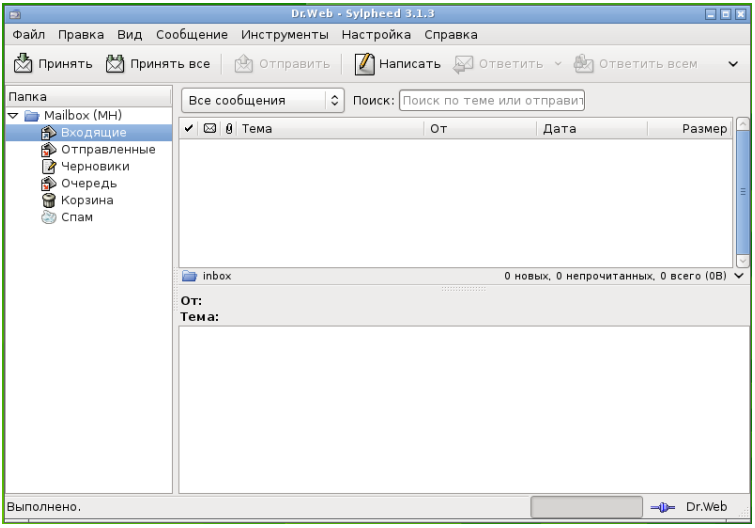
Обратите внимание, что у почтового клиент изначально настроена учетная запись на сервере `mail.drweb.com`, через которую вы сможете отправлять сообщения только в почтовый домен `drweb.com` (на адреса вида `<mailbox>@drweb.com`). Поэтому при необходимости отправки писем на длугие адреса (например, на `gmail.com`, `yandex.ru` и т.п.) необходимо создать дополнительные учетные записи для ведения переписки. Для этого можно использовать данные любой из имеющихся у вас учетных записей почты, при условии, что почтовые сервера, обслуживающие эту учетную запись, доступны по сети.

Для создания новой учетной записи выберите меню **Настройка → Создать новую учетную запись**. Введите всю необходимую для отправки почты информацию:

- Адрес электронной почты (почтовый ящик) отправителя,
- Параметры для отправки почты (подключение по протоколу SMTP: сервер, порт, аутентификация);
- Параметры для получения почты (подключение по протоколу POP3: сервер, порт, аутентификаци);
- Укажите также дополнительную 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.



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.

Пожалуйста, обратите внимание, что в процессе работы **Dr.Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все письма, сохраненные на него, будут утеряны при перезагрузке компьютера. Если вам требуется сохранить письма, сохраняйте их на жесткий диск.

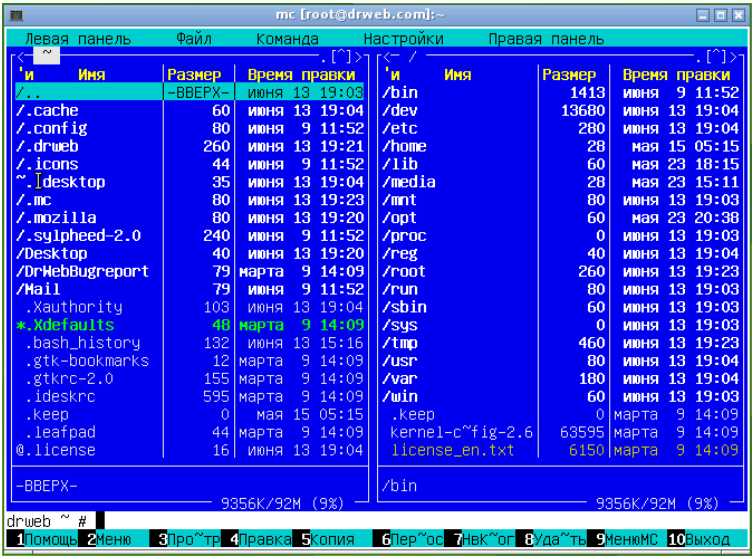
Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

Подробнее с информацией о работе с почтовой программой **Sylpheed** вы можете ознакомиться на сайте разработчика: http://sylpheed.sraoss.jp/en/ (на английском языке).

3.4.3. Файловый менеджер

Консольный файловый менеджер **Midnight Commander** аналогичен файловым менеджерам **Norton Commander**, **FAR** и **Total Commander**, используемым в среде ОС MS-DOS и Windows. Файловый менеджер **Midnight Commander** работает в консольном режиме, а потому может быть запущен не только в графической оболочке, но и в текстовом режиме работы **Dr.Web LiveCD**.

Вид экрана файлового менеджера (в оконном режиме) представлен на рисунке ниже:



Запуск файлового менеджера в графической оболочке

Для запуска файлового менеджера в графической оболочке выполните любое из следующих действий:

- Выполните двойной щелчок левой кнопкой мыши по иконке  **Midnight Commander** на рабочем столе;
- Выберите пункт **Utility** → **Менеджер файлов** в главном системном меню графической оболочки.

Запуск файлового менеджера в текстовом режиме

Для запуска файлового менеджера из консоли операционной системы введите команду

```
mc
```

Использование для работы с файлами

Помимо панелей навигации по файловой системе, файловый менеджер также содержит встренный текстовый редактор, позволяющий просматривать и редактировать содержимое файлов.

- Для просмотра файла выделите его и нажмите клавишу `F3`, для редактирования нажмите клавишу `F4`.
- Для удаления выделенного файла воспользуйтесь клавишей `F8`.
- Действия, назначенные фукнциональным клавишам клавиатуры, представлены в виде меню в нижней строке экрана.
- Дополнительные функции менеджера доступны в главном меню программы, доступ к которому осуществляется по нажатию клавиши `F9`.

Между нижним меню и панелями навигации по файлам и каталогам расположена строка ввода команд, при помощи которой можно вводить команды, передаваемые операционной системе (аналогично режиму работы в консоли).

Дополнительные сведения о программе можно получить по адресу: https://www.midnight-commander.org/ (на английском языке).

Использование для просмотра и редактирования реестра Windows

Ветви реестра Windows автоматически монтируются в файловую систему (используется каталог `/reg`) при загрузке **Dr.Web LiveCD**, после чего с ключами реестра можно работать как с обычными файлами (просматривать содержимое ключей и вносить в них изменение при необходимости).

Не смотря на то, что работа с содержимым реестра Windows ведется так же, как с каталогами и файлами, следует помнить, что ветви реестра не являются каталогами, а потому в них нельзя копировать обычные файлы и каталоги.

Также крайне не рекомендуется удалять, перемещать и переименовывать ветви и ключи реестра, поскольку это может привести к тому, что его структура окажется не читаемой в системе Windows, из-за чего операционная система (или некоторые ее компоненты) окажется полностью или частично неработоспособной.

Завершение работы файлового менеджера

Для завершения работы файлового менеджера нажмите клавишу `F10`.

3.4.4. Терминал

При помощи программы **Терминал** вы можете получить доступ к командной консоли ОС Linux для ввода команд и работы в текстовом режиме.

Запуск Терминала в графической оболочке

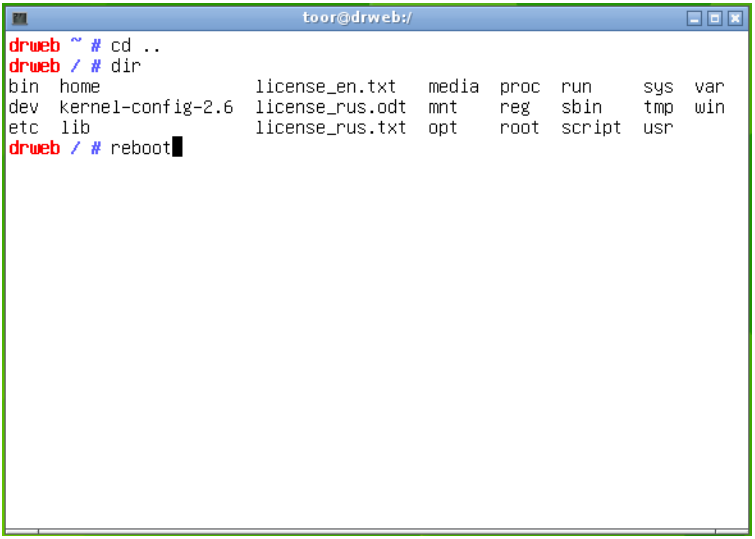
Для запуска **Терминала** выполните любое из следующих действий:

- Выполните двойной щелчок левой кнопкой мыши по иконке  **Терминал** на рабочем столе;
- Кликните мышью по иконке  на панели задач;
- Выберите пункт **System** → **Терминал** в главном системном меню графической оболочки.

Работа с Терминалом

Вид окна запущенного терминала в графической оболочке

приведен на рисунке ниже.



Команды вводятся пользователем с клавиатуры в активную строку, отмеченную символом приглашения **#**. В начале строки, перед символом приглашения, выводятся имя пользователя и путь к текущему активному каталогу файловой системы. При выводе текста содержимое окна прокручивается снизу вверх по принципу телетайпа.

Работа с консолью требует знания основ работы с операционными системами семейства UNIX и рекомендуется только опытным пользователям.

Завершение работы терминала

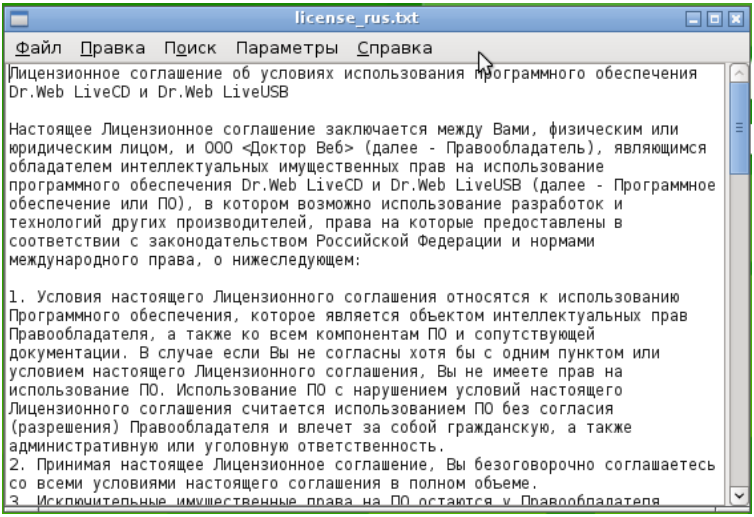
Для завершения работы терминала закройте окно или введите команду **exit**.

3.4.5. Графический текстовый редактор Leafpad

Оконный текстовый редактор **Leafpad**, входящий в состав программ, доступных в графической оболочке, аналогичен текстовому редактору **Notepad** (**Блокнот**), используемому в среде ОС Windows.

Leafpad – простой, легковесный, быстрый текстовый редактор для Unix-подобных систем. Его достоинством является малое время запуска на большинстве современного оборудования. Последние версии поддерживают печать при наличие установленного в системе принтера. **Leafpad** работает с текстами без возможности форматирования (использование различных шрифтов, управления выравниванием и т.п.).

Вид окна текстового редактора **Leafpad** представлен на рисунке ниже:



Запуск текстового редактора в графической оболочке

Для запуска текстового редактора в графической оболочке выберите в главном системном меню пункт **Utility → Leafpad**.

Запуск текстового редактора в текстовом режиме

Запуск текстового редактора в текстовом режиме невозможен. Для просмотра текстовых файлов перейдите сначала в режим графической оболочки, или воспользуйтесь текстовым редактором **nano**.

Использование для работы с текстовыми файлами

Работа производится стандартным для текстовых редакторов образом:

- Пункты меню **Файл** позволяют выполнять создание нового файла, открывать имеющиеся текстовые файлы и выбирать имя файла для сохранения.
- В меню **Правка** располагаются пункты работы с буфером обмена (копировать, вырезать, вставить, выделить все).
- При помощи пунктов меню **Поиск** можно осуществлять поиск и замену в тексте заданного фрагмента текста, а также осуществить переход к конкретной строке текста, указав ее номер.
- В меню **Параметры** можно настроить параметры редактора, такие как
  - Используемый шрифт (включая его размер);
  - Автоперенос длинных строк;
  - Нумерация строк текста.

Дополнительные сведения о программе можно получить по адресу: http://tarot.freeshell.org/leafpad/ (на английском языке).

Завершение работы

Для завершения работы текстового редактора необходимо закрыть окно или выбрать в меню пункт **Файл** → **Выход**.

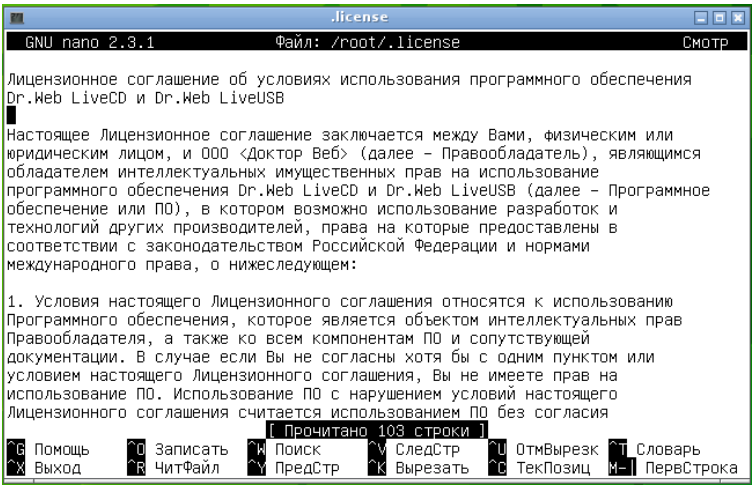
3.4.6. Консольный текстовый редактор nano

Текстовый редактор **nano**, входящий в состав программ **Dr.Web LiveCD**, работает в консольном (текстовом) режиме, и доступен как в графической оболочке, так и в текстовом режиме работы **Dr.Web LiveCD**.

nano – простой текстовый редактор для Unix-подобных систем. **nano** работает с текстами без возможности форматирования (использование различных шрифтов, управления выравниванием и т.п.).

Вид текстового редактора **nano** с открытым в нем текстом лицензионного соглашения **Dr.Web LiveCD** представлен на

рисунке ниже (в оконном режиме):



Запуск текстового редактора в графической оболочке

Запуск текстового редактора **nano** в графической оболочке при помощи пункта меню или щелчка по иконке не предусмотрен. Однако выбор пункта **Лицензия** в главном системном меню открывает текст лицензионного соглашения в редакторе **nano**.

Запуск текстового редактора в текстовом режиме

Для запуска текстового редактора из консоли операционной системы введите команду

```
nano
```

Для открытия в текстовом редакторе **nano** текстового файла из консоли операционной системы введите команду

```
nano <filename>
```

где `<filename>` - путь к файлу, включающий его имя. Например, чтобы открыть для просмотра текст лицензионного соглашения, введите команду:

```
nano /license_rus.txt
```

В графическом режиме для доступа к консоли вы можете воспользоваться **Терминалом**.

Использование для работы с текстовыми файлами

При запуске текстового редактора nano область экрана делится на три части:

- **Строка заголовка**, в которой выводится имя и версия редактора, имя открытого файла и режим работы редактора. Занимает верхнюю строку экрана.
- **Область просмотра и редактирования текста**. Занимает весь экран, за исключением строки заголовка и области уведомления.
- **Строка уведомления и подсказки доступных команд**. Занимает три последних строки экрана.

Работа производится стандартным для текстовых редакторов образом:

- Текст вводится в позицию, отмеченную курсором.
- Перемещение курсора по редактируемому тексту производится при помощи клавиш клавиатуры со стрелками, а также `PgUP` и `PgDn`.
- Доступные сочетания клавищ, и действия, которые они производят, перечисляются в области уведомления.

Дополнительные сведения о программе можно получить в справке (сочетание клавиш `Ctrl` + `G`).

Завершение работы

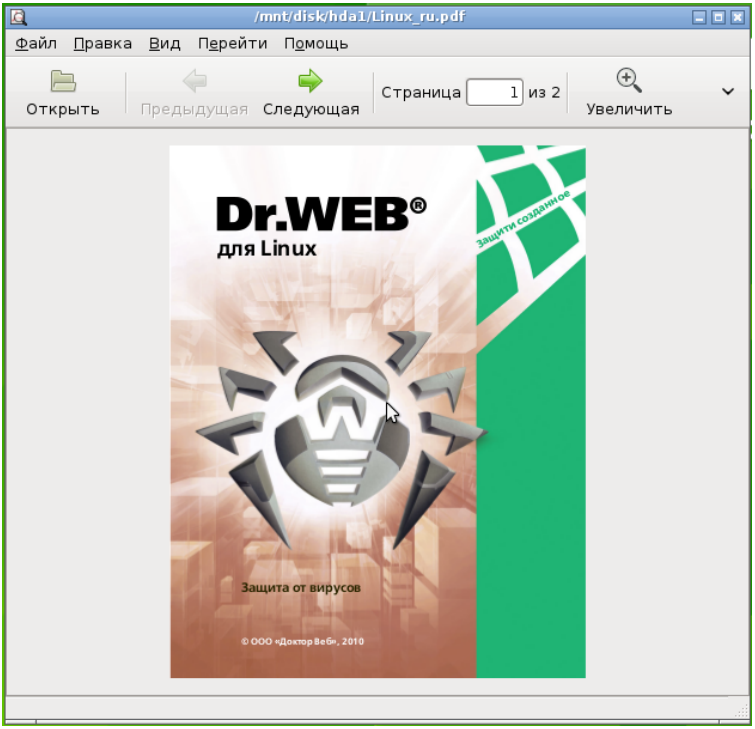
Для завершения работы текстового редактора необходимо нажать сочетание клавиш `Ctrl` + `X`.

3.4.7. Средство просмотра файлов PDF

Средство просмотра документов в формате PDF **ePDFViewer**, входящее в состав программ **Dr.Web LiveCD**, позволяет

открывать PDF-файлы в режиме просмотра (только для чтения) при работе в режиме графической оболочки.

Вид окна **ePDFViewer** с открытым в нем PDF-документом представлен на рисунке ниже:



Запуск средства просмотра PDF-файлов в графической оболочке

Запуск средства просмотра PDF-файлов **ePDFViewer** в графической оболочке осуществляется при помощи выбора в главном системном меню графической оболочки пункта **Office → ePDFViewer**.

Запуск средства просмотра PDF-файлов в текстовом режиме

Запуск средства просмотра PDF-файлов **ePDFViewer** в текстовом режиме невозможен. Для просмотра PDF-файлов перейдите сначала в режим графической оболочки.

Использование для просмотра PDF-файлов

- При помощи пунктов меню **Файл** можно выбрать и открыть документ, перезагрузить открытый документ, сохранить его копию в новый файл, а также завершить работу приложения. Также открыть файл для просмотра можно нажатием кнопки **Открыть** на панели инструментов.
- При помощи пункта меню **Поиск**, расположенном в меню **Правка**, включается панель поиска текста в открытом документе. Также в меню **Правка** можно выбрать режим просмотра документа (прокрутка или выделение текста).
- Пункты меню **Вид** управляют видимостью дополнительных панелей приложения (панель меню, инструментов и просмотра оглавления). Также в этом меню можно выбрать параметры отображения документа (масштаб и поворот).
- Пункты меню **Переход** позволяют осуществлять навигацию по страницам документа (переход к предыдущей, следующей, первой и последней странице документа).
- Кнопки панели инструментов реализуют основной функционал навигации (перелистывание страниц), а также масштабирования просматриваемого документа.

Завершение работы

Для завершения работы средства просмотра PDF-файлов необходимо закрыть окно или выбрать в меню **Файл** пункт **Выход**.

4. Расширенный режим

Для загрузки **Dr.Web LiveCD** в расширенном режиме (Advanced mode) следует в главном загрузочном меню выбрать пункт **Advanced Mode**.

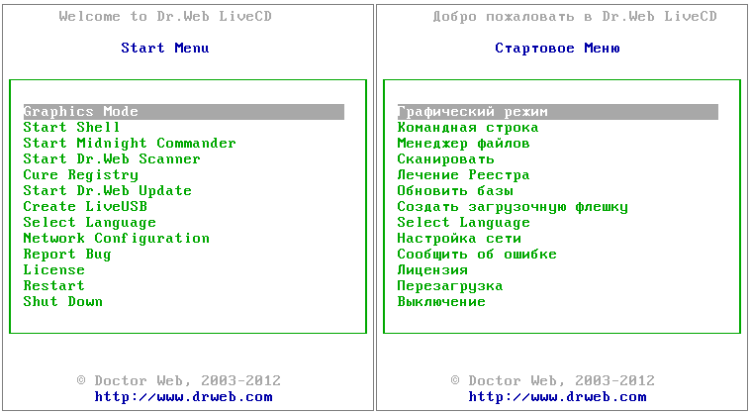
При загрузке системы в расширенном режиме произойдет следующее:

1. Загрузка в память ядра операционной системы Linux, используемой **Dr.Web LiveCD**;
2. Загрузка **утилиты работы со снимками**, в меню которой можно выбрать один из ранее сохраненных снимков, создать новый снимок, или отказаться от использования снимков.
3. Запуск меню расширенного режима работы.

Также в меню расширенного режима можно попасть из режима графической оболочки, если выбрать в главном меню графической оболочки пункт **Выход**.

4.1. Меню расширенного режима

Меню расширенного режима работы **Dr.Web LiveCD** представлено на рисунке ниже. Слева – вид меню при выборе английского языка (по умолчанию при загрузке **Dr.Web LiveCD**), а справа – при выборе русского языка интерфейса.



С помощью стрелок ⇧ и ⇩ клавиатуры и нажатия клавиши ENTER имеется возможность выбора следующих режимов работы:

- Пункт **Graphics mode** (**Графический режим**) позволяет запустить **Dr.Web LiveCD** в режиме графического интерфейса (после выбора пункта **Выход** в главном меню графического режима будет осуществлен возврат к главному меню расширенного режима). В графическом режиме будет использоваться текущий язык расширенного режима. Для смены языка следует предварительно выбрать в главном меню пункт **Select Language**.
- Пункт **Start Shell** (**Командная строка**) позволяет запустить командную консоль операционной системы **Linux** (для выхода из нее и возврата в меню расширенного режима используйте команду **exit**).
- Пункт **Start Midnight Commander** (**Менеджер файлов**) позволяет запустить файловый менеджер **Midnight Commander**, работающий в текстовом режиме. По завершению работы программы будет осуществлен возврат в главное меню расширенного режима.

- Пункт **Start Dr.Web Scanner** (**Сканировать**) позволяет запустить **Антивирусный сканер Dr.Web** в текстовом режиме с настройками по умолчанию. По завершению работы программы будет осуществлен возврат в главное меню расширенного режима. Если вы желаете запустить **Антивирусный сканер** с особыми настройками, воспользуйтесь командной строкой или менеджером файлов.
- Пункт **Cure registry** (**Лечение реестра**) позволяет запустить **утилиту восстановления реестра Windows.** По завершению работы утилиты будет осуществлен возврат в главное меню расширенного режима.
- Пункт **Start Dr.Web Update** (**Обновить базы**) позволяет запустить процесс обновления баз **Антивирусного сканера Dr.Web**. По завершению обновления будет осуществлен возврат в главное меню расширенного режима.
- Пункт **Create LiveUSB** (**Создать загрузочную флешку**) позволяет запустить **утилиту создания загрузочного накопителя USB-flash** с продуктом **Dr.Web LiveUSB**. По завершению работы утилиты будет осуществлен возврат в главное меню расширенного режима.
- Пункт **Select Language** позволяет выбрать язык, используемый при работе в расширенном режиме, включая наименование пунктов главного меню расширенного режима. Доступны русский и английский язык. По умолчанию используется английский язык. После выбора языка будет осуществлен возврат в главное меню расширенного режима.
- Пункт **Network Configuration** (**Настройка сети**) позволяет запустить **утилиту конфигурирования настроек сети.** Наличие правильной сетевой конфигурации сети необходимо для возможности обновления антивирусных баз. По завершению работы утилиты будет осуществлен возврат в главное меню расширенного режима.

- Пункт **Report Bug** (**Сообщить об ошибке**) позволяет запустить текстовый редактор **nano** для составления сообщения об ошибке **Dr.Web LiveCD** и ее последующей отправке по электронной почте команде разработчиков компании **«Доктор Веб»**. По завершению работы текстового редактора будет осуществлен возврат в главное меню расширенного режима.
- Пункт **License** (**Лицензия**) позволяет открыть в текстовом редакторt **nano** текст лицензионного соглашения с конечным пользователем на использование продукта **Dr.Web LiveCD**. Текст лицензии всегда выводится на текущем выбранном языке. По завершению работы текстового редактора будет осуществлен возврат в главное меню расширенного режима.
- Пункт **Restart** (**Перезагрузка**) позволяет выполнить перезагрузку компьютера.
- Пункт меню **Shut Down** (**Выключение**) используется для того, чтобы завершить работу **Dr.Web LiveCD** и выключить компьютер.

Пожалуйста, обратите внимание, что в процессе работы **Dr.Web LiveCD** использует временный диск, создаваемый в памяти (RAM-диск) при загрузке, в связи с чем все изменения, внесенные в настройки программ, входящих в состав диска, будут утеряны при перезагрузке компьютера.

Каталог **Карантина** также создается на RAM-диске, поэтому резервные копии файлов, сохраненные в **Карантине**, будут утрачены, если их не сохранить на один из жестких (физических) дисков компьютера.

Чтобы обеспечить сохранность внесенных изменений, следует либо создать и использовать загрузочный флеш-накопитель, либо воспользоваться инструментом создания снапшотов (доступен только в расширенном режиме).

4.2. Работа со снимками (snapshots)

Предварительные замечания

С помощью снимков системы (снапшотов) вы можете сохранять

все изменения настроек **Dr.Web LiveCD**, файлы отчета, временные файлы, а также **Карантин** антивируса, создаваемые при сканировании системы, на локальных жестких дисках компьютера или съемных накопителях USB-flash. Использование снапшотов позволяет снизить нагрузку на системные ресурсы, в частности – уменьшить используемый объем оперативной памяти, и избежать сбоев при сканировании больших архивов.

Снимки сохраняются в виде файлов в каталог `.DrWebLive` в корневой каталог выбранного диска. В случае если вам в дальнейшем не нужны сохраненные снимки, этот каталог можно удалить с диска вручную. Кроме того, каталог можно переместить, к примеру, на носитель USB-flash и использовать при последующих загрузках **Dr.Web LiveCD**, настроенного по вашему вкусу, на других компьютерах.

Обратите внимание, что для использования снапшотов на выбранном для их хранения диске должно быть не менее 512 MB свободного места

Запуск утилиты

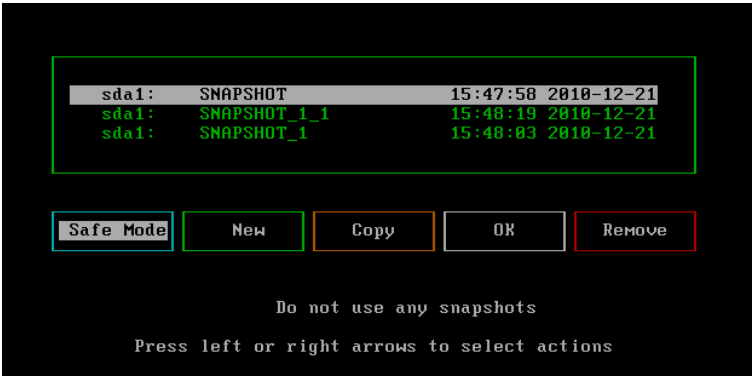
Запуск утилиты работы со снапшотами производится автоматически, при загрузке **Dr.Web LiveCD** в расширенном режиме.

Запуск утилиты производится единственный раз, при старте расширенного режима. Если выбран другой режим запуска, или при старте расширенного режима вы отказались от использования снапшотов, запустить утилиту вам в этом сеансе работы больше не удастся. Для запуска утилиты вам потребуется выполнить перезагрузку компьютера.

При запуске утилита автоматически просканирует ваш компьютер в поиске дисков, подходящих для хранения снимков, а также построит список снимков, уже созданных и сохраненных ранее. Если при загрузке не будет обнаружено дисков или накопителей USB-flash, подходящих для хранения снапшотов, список выводится не будет, а утилита автоматически завершит свою работу.

Работа со снимками

В случае если утилита нашла набор уже имеющихся снимков, их список выводится на экране. Если на дисках, имеющихся в компьютере (включая подключенные накопители USB-flash), снимков не будет обнаружено, в списке будет выведена надпись "**Snapshots not found**". Вид экрана при старте утилиты (с заполненным списком ранее созданных снимков) показан на рисунке ниже.



Для каждого снимка в списке указываются:

- Диск (устройство), на котором он хранится;
- Имя снимка, присвоенное ему при создании;
- Дата и время создания снимка.

С помощью стрелок ⇧ и ⇩ клавиатуры производится выбор нужного снимка в списке. Снимок, выделенный в списке, подсвечивается светлой полосой.

Под списком снимков расположены команды работы утилиты:

- **Safe Mode** – загрузить **Dr.Web LiveCD** без использования снимков (все имеющиеся снимки будут сохранены).

  Обратите внимание, что в этом случае для использования снапшотов вам придется перезагрузить компьютер.
- **New** – создать новый снимок.

- **Copy** – скопировать снимок, выделенный в списке, на другой диск.
- **OK** – загрузить **Dr.Web LiveCD** с использованием снимка, выбранного в списке.
- **Remove** – удалить снимок, выделенный в списке.

  Помните, что удаление снимка – необратимая операция.

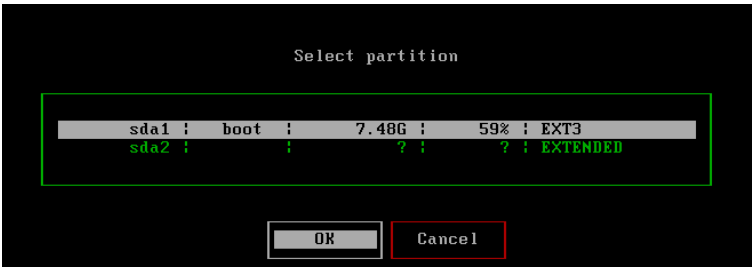
Выбор требуемой команды осуществляется с помощью стрелок ⇦ и ⇨ клавиатуры. Активация выбранной команды производится нажатием клавиши ENTER. Текст активной (выделенной) команды подсвечивается светлым фоном.

Создание нового снимка

- Загрузите **Dr.Web LiveCD** в расширенном режиме;
- Выберите команду **New** под списком снимков и нажмите ENTER;
- Выберите из появившегося списка диск, на котором будет размещен новый снапшот. Требуемый диск в списке выбирается клавишами ⇧ и ⇩ клавиатуры.
- Для создания снимка выберите команду **OK**. Если вы решили отказаться от создания снимка, выберите команду **Cancel**.

Так же, как и на экране выбора снимков, выбор требуемой команды осуществляется с помощью стрелок ⇦ и ⇨ клавиатуры. Активация выбранной команды производится нажатием клавиши ENTER. Текст активной (выделенной) команды подсвечивается светлым фоном.

Вид экрана выбора диска показан на рисунке ниже:



- После того, как выбран диск, на следующем экране укажите имя создаваемого снимка. Имя может быть любым. Вид экрана задания имени нового снимка показан на рисунке ниже. После ввода имени нажмите клавишу ENTER.

Загрузка системы без использования снимков

- Загрузите **Dr.Web LiveCD** в графическом режиме, или
- Загрузите **Dr.Web LiveCD** в расширенном режиме, выберите команду **Safe Mode** под списком снимков и нажмите ENTER.

Загрузка системы с использованием ранее сохраненного снимка

- Загрузите **Dr.Web LiveCD** в расширенном режиме.
- Выберите снимок в списке.
- Выберите команду **OK** под списком снимков и нажмите ENTER.

Копирование снимков

- Загрузите **Dr.Web LiveCD** в расширенном режиме.
- Выберите снимок в списке.
- Выберите команду **Copy** под списком снимков и нажмите ENTER.
- Выберите в появившемся списке диск, на который будет скопирован снимок, нажмите ENTER.
- Укажите имя копии снимка, нажмите ENTER.

После создания копии на экране снова появится основной экран утилиты со списком имеющихся снимков.

Удаление снимков

- Загрузите **Dr.Web LiveCD** в расширенном режиме.
- Выберите снимок в списке.
- Выберите команду **Remove** под списком снимков и нажмите `ENTER`.

После удаления снимка на экране снова появится основной экран утилиты со списком имеющихся снимков.

5. Работа с Антивирусом Dr.Web в текстовом режиме

При необходимости вы можете работать со **Сканером Антивируса Dr.Web для Linux** непосредственно в текстовом (консольном режиме). В этом режиме для запуска сканирования необходимо ввести команду:

```
drweb <путь> [параметры командной строки]
```

где `<путь>` — путь к проверяемому каталогу или маска имен проверяемых файлов.

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

```
drweb /mnt/disk/sda1
```

Файлы отчетов, формируемых **Сканером**, находятся в каталоге `/var/drweb/log`.

- Для доступа к консоли в расширенном режиме выберите в меню пункт **Start Shell** (**Командная строка**).
- Для доступа к консоли в режиме графической оболочки воспользуйтесь **Терминалом**.

Перечень параметров, которые можно задавать в команде запуска **Сканера**, перечислен в разделе 5.1.

5.1. Параметры командной строки

Использование параметров при запуске Сканера

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, введя команду `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

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 каталогам или просто список файлов, подлежащих регулярной проверке;
- `sd` – рекурсивный поиск и проверка файлов в подкаталог, начиная с текущей;
- `fl` – указание следовать символическим ссылкам, как для файлов, так и для каталогов. Ссылки, приводящие к «зацикливанию», игнорируются;
- `mask` – указание игнорировать маски имен файлов.

Параметры диагностики

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

- `al` – диагностика всех файлов на заданном устройстве или в каталоге, указанном в качестве аргумента;
- `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 действий

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

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 (на экран);
- `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.

Особые параметры

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.

Набор параметров по умолчанию

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).

Замечания по использованию параметров

Следует отметить, 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 отдельный каталог, который и будет указан 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 предназначенный для этого каталог **Карантина**.

6. Служебные утилиты

В состав **Dr.Web LiveCD** помимо **Антивируса** входит набор служебных утилит, выполняющих ряд полезных действий:

- **Утилита создания загрузочного носителя USB-flash**. Предназначена для создания копии **Dr.Web LiveCD** для загрузки компьютера через USB.
- **Утилита лечения реестра Windows**. Утилита предназначена для автоматического сканирования реестра Windows и устранения в нем следов вирусной активности.
- **Утилита конфигурирования сети**. Предназначена для настройки соединения компьютера с сетью, необходимого, в том числе, для обновления баз **Антивируса**.
- **Утилита отправки сообщений об ошибках**. Используется для отправки по электронной почте разработчикам программного продукта **Dr.Web LiveCD** сообщений об обнаруженных ошибках.

Все утилиты запускаются как в графическом, так и в текстовом режиме работы **Dr.Web LiveCD**.

6.1. Создание загрузочного накопителя USB-flash

Вводные замечания

Dr.Web LiveCD позволяет создать свою полноценную копию на накопителе USB-flash, который может быть использован аналогично диску **Dr.Web LiveCD** на любом компьютере, на котором поддерживается загрузка с USB-накопителей. В этом случае **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.

Преимущество использования в качестве носителя накопителя

USB-flash заключается в том, что на нем будут сохраняться все изменения, внесенные в настройки системы в процессе работы, в отличие от CD/DVD-носителя. При этом не требуется использования снапшотов.

Требования к носителю USB-flash

Для создания загрузочной копии **Dr.Web LiveCD** подойдет любой накопитель USB-flash, обладающей достаточным количеством свободного места (желательно не менее 512 MB).

Несмотря на то, что утилита создания загрузочного USB-flash **CreateLiveUSB** не изменяет и не удаляет файлы, содержащиеся на накопителе, рекомендуется перед запуском утилиты сохранить все файлы используемого накопителя на другом носителе.

Все файлы системы **Dr.Web LiveCD** записываются на носителе в каталог `/boot`. При необходимости утилита изменяет конфигурацию разделов на флеш-накопителе, оригинальная конфигурация сохраняется в файле `/boot/partition.backup`. Также утилита создает на флеш-накопителе новую загрузучную запись MBR. При этом оригинальная главная загрузочная запись, если она была, сохраняется в файле `/boot/mbr.backup`.

Создание загрузочного накопителя USB-flash

1. Подключите накопитель к USB-порту компьютера. Регистрация события подключения занимает не больше десяти секунд.
2. Запустите утилиту создания загрузочного накопителя **CreateLiveUSB**. Это можно сделать следующим образом:
   a) В графической оболочке:
      - Выполнив двойной щелчок мышью по иконке  **Создать загрузочную флешку** на рабочем столе;
      - Выбрав в системном меню пункт **Utility → Создать**

загрузочную флешку.

b) В расширенном режиме:

- Выбрав в меню пункт **Create LiveUSB** (**Создать загрузочную флешку**).

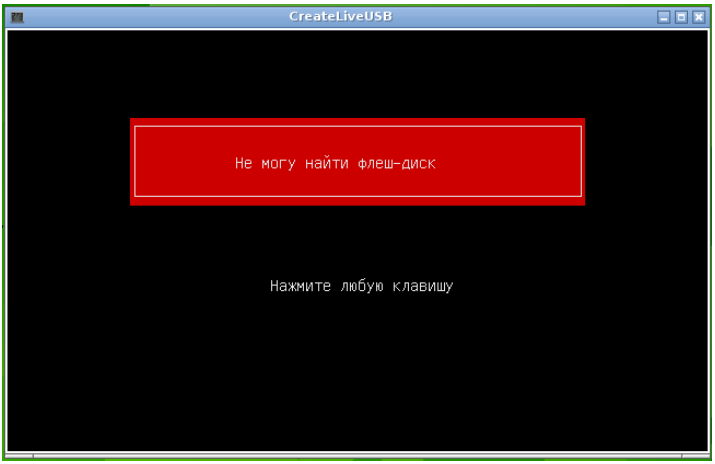
c) В консоли:

- Введите команду

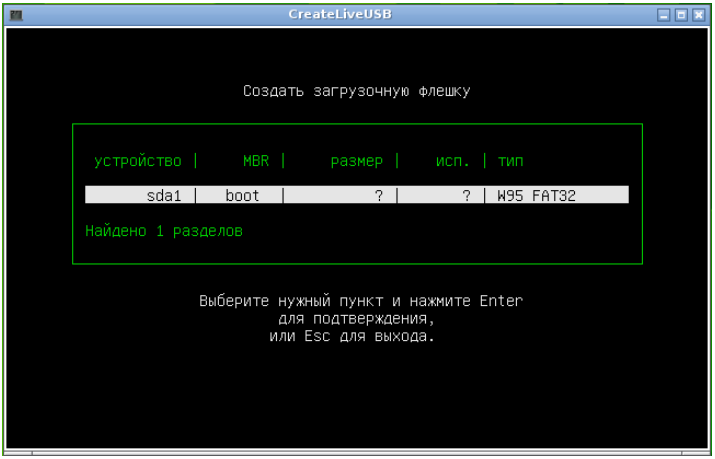
```
CreateLiveUSB
```

- Для доступа к консоли в расширенном режиме выберите в меню пункт **Start Shell** (**Командная строка**).
- Для доступа к консоли в режиме графической оболочки воспользуйтесь **Терминалом**.

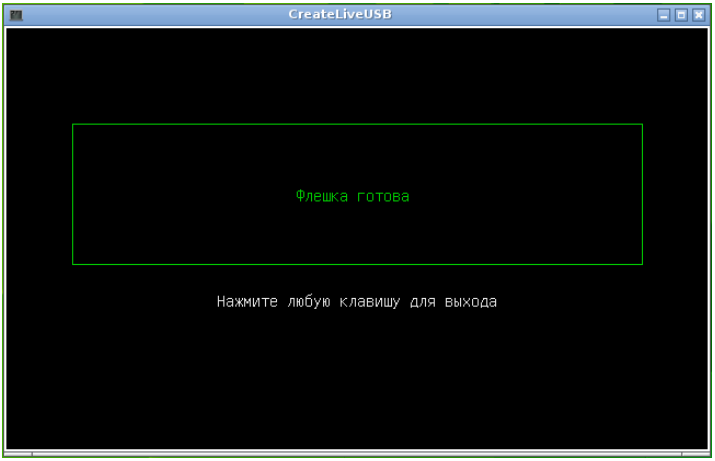
3. Утилита создания загрузочного носителя сама обнаружит все имеющиеся в системе накопители USB-flash. Если ни одного устройства обнаружено не будет, утилита выведет соответствующее сообщение:



4. Выберите подходящий раздел и нажмите клавишу `ENTER`. Вид экрана утилиты при выборе требуемого накопителя показан на рисунке ниже (в оконном режиме).



5. После выбора устройства копирование файлов начнется автоматически. По окончанию работы утилиты на экран будет выведено соответствующее сообщение.



6. Для завершения работы нажмите любую клавишу на клавиатуре.

6.2. Лечение реестра

Вводные замечания

Утилита лечения реестра Windows позволяет в автоматическом режиме выполнить сканирование реестра Windows (если он был обнаружен на данном компьютере). В процессе сканирования утилита автоматически устраняет все ошибки и нарушения в реестре, появившиеся вследствие вирусной активности.

При загрузке **Dr.Web LiveCD** автоматически обнаруживает реестр Windows и монтирует его к своей файловой системе как каталог `/reg`. В случае если вы желаете вручную внести некоторые изменения в реестр (изменить значение ключей, добавить или удалить ключ), воспользуйтесь файловым менеджером.

Обратите внимание, что **Утилита лечения реестра Windows** выполняет только ряд стандартных проверок реестра (перечень выполняемых действий приведен ниже). Эта утилита не предназначена для восстановления произвольно удаленных или измененных ветвей и ключей реестра.

Также обратите внимание, что утилита восстанавливает значения проверяемых ключей в состояние, принятое по умолчанию в ОС Windows, или взятое из файла резервной копии реестра. Поэтому если некоторые значения в реестре, контролируемые данной утилитой, были изменены вами, то эти изменения будут утеряны.

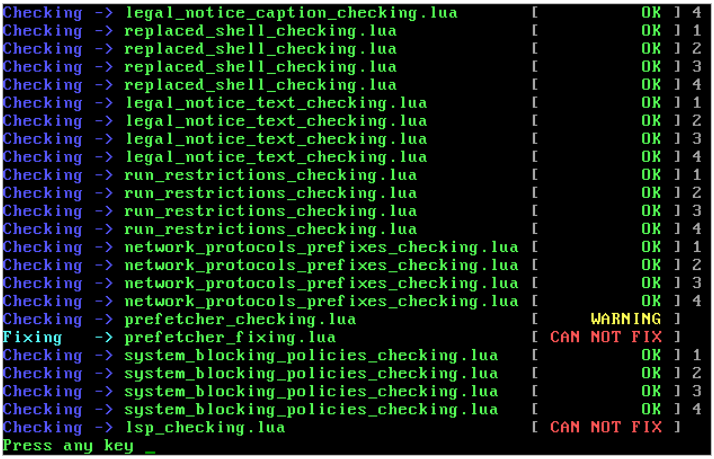
Лечение реестра

1. Запустите **Утилиту лечения реестра Windows**. Это можно сделать следующим образом:
   a) В графической оболочке:
      - Выбрав в системном меню пункт **Лечение реестра**.

   b) В расширенном режиме:
      - Выбрав в меню пункт **Cure registry** (**Лечение**

реестра)

2. **Утилита лечения реестра Windows** сама обнаружит реестр. Если реестр обнаружен не будет, утилита выведет соответствующее сообщение. В противном случае утилита начнет проверять ветви реестра. Отчет о выполняемых проверках и их результате будет выводиться на экран. Пример отчета, сформированного в ходе проверки, показан на рисунке ниже.



3. Для завершения работы утилиты, после того, как весь реестр проверен, нажмите любую клавишу на клавиатуре.

Перечень проверок, выполняемых утилитой лечения реестра

Восстановление значений ключей всегда производится либо в естественные значнеия, принятые в ОС Windows по умолчанию, либо значения восстанавливаются из файла резервной копии реестра (`System.sav`).

Утилита выполняет следующие проверки реестра:

1. Проверка и восстановление ассоциаций важных файлов ОС (`exe`, `com`, `bat`, `cmd`, `pif`, `scr`, `lnk`, `reg`);
2. Проверка и восстановление параметров загрузки Windows в безопасном режиме;
3. Обнаружение и удаление записей об отладчиках

процессов;

4. Обнаружение и устранение следующих изменений настройки браузера **Internet Explorer**:
   1) Заблокирована настройка домашней страницы;
   2) Задан нестандартный заголовок окна браузера **Internet Explorer**;
   3) Блокирована возможность закрытия окна браузера;
   4) Блокированы кнопки навигации;
   5) Заблокировано контекстное меню;
   6) Заблокирован доступ к настройкам браузера;
   7) Заблокирована возможность выбора каталога для сохранения файлов;
   8) Заблокирован просмотр HTML-кода страниц;
   9) Отключено отображение адресной панели;
   10) Заблокированы различные настройки.
5. Обнаружение и удаление политик, блокирующих работу системы:
   1) Блокировка панели управления;
   2) Сокрытие всех элементов на рабочем столе;
   3) Заблокировано изменение свойств экрана;
   4) Заблокирована закладка **Рабочий стол** в окне свойств экрана;
   5) Заблокирована закладка **Заставка** в окне свойств экрана;
   6) Заблокирована закладка **Параметры** в окне свойств экрана;
   7) Заблокирована закладка **Оформление** в окне свойств экрана;
   8) Заблокированы настройки системы **Windows Update**;
   9) Заблокированы настройки системы **System Restore**;
   10) Заблокирован доступ к настройкам сети;
   11) Заблокирована настройка автоматического обновления;
   12) Заблокирован интерфейс командной строки (`cmd.exe`);
   13) Заблокировано отображение иконки **Мой компьютер**;

14) Установлены запреты на запуск программ из реестра;
15) Отключена возможность управлять установленными приложениями;
16) Заблокирована вкладка **Обои** в окне свойств экрана.

6. Обнаружение и устранение изменений в параметрах запуска сеанса работы пользователя:
   1) Изменены параметры запуска графической оболочки пользователя (**Проводника**);
   2) Задано сообщение, выводимое при загрузке системы;
   3) Изменены параметры инициализации сеанса (запуска `userinit.exe`).
7. Восстановление настроек **Проводника**:
   1) Ограничено отображение дисков в **Проводнике**;
   2) Заблокирована возможность закрытия окон **Проводника**;
   3) Заблокирован доступ к сетевому окружению;
   4) Заблокирована возможность завершения сеанса;
   5) Заблокирован пункт меню **Управление** в папке **Мой компьютер**;
   6) Отключено контекстное меню панели задач;
   7) Отключено контекстное меню кнопки **Пуск**;
   8) Заблокировано меню **Пуск** → **Поиск**;
   9) Заблокировано меню **Пуск** → **Выполнить**;
   10) Отключено отображение значков в системном трее;
   11) Заблокирована возможность монтирования сетевых дисков;
   12) Заблокировано отображение вложенных папок в меню **Пуск**;
   13) Заблокирован доступ к настройкам принтеров;
   14) Заблокированы элементы меню **Пуск**;
   15) Заблокирован доступ к свойствам папки;
   16) Заблокирован доступ к свойствам панели задач и меню **Пуск**;
   17) Заблокирован пункт меню **Справка и техподдержка**.
8. Обнаружение и устранение блокировки диспетчера задач;

9. Обнаружение и устранение блокировки редактора реестра;
10. Обнаружение и устранение модификации файла `hosts`.
11. Обнаружение и устранение повреждений цепочки LSP.
12. Обнаружение и устранение блокировки известных сайтов в списке статических маршрутов.
13. Обнаружение и устранение подмены диспетчера задач.
14. Обнаружение и устранение ограничений на запуск программ.
15. Обнаружение и устранение изменений префиксов сетевых протоколов.
16. Обнаружение и устранение отключения или неоптимальной настройки **Prefetcher**.

6.3. Конфигурация сети

Вводные замечания

Dr.Web LiveCD использует сетевое подключение, имеющееся на вашем компьютере, для подключения к Интернету. Подключение к Интернету используется в первую очередь для обновления вирусных баз **Антивируса**. Кроме того при наличии подключения к Интернету вы можете вести переписку по электронной почте и просматривать веб-сайты при помощи почтовой программы и браузера, входящих в состав **Dr.Web LiveCD** (только в режиме графической оболочки).

Dr.Web LiveCD автоматически определяет параметры подключения к сети при загрузке. В большинстве случаев эти параметры определяются верно и не требуют ручной корректировки. Однако если подключение к сети не распознано, или доступ к сети отсутствует, при помощи утилиты конфигурации сети можно попытаться задать правильные параметры соединения вручную.

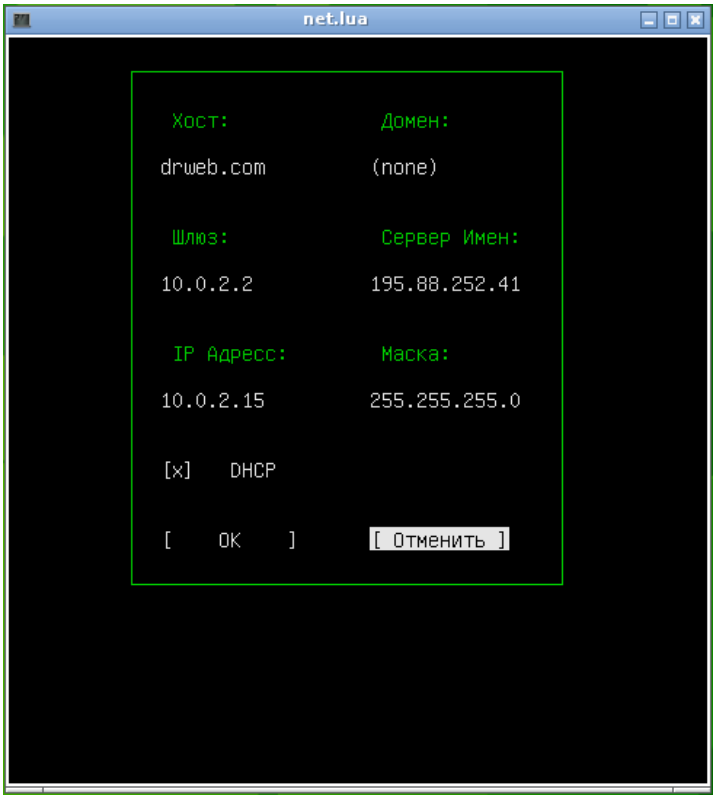
Конфигурирование подключения к сети

1. Убедитесь, что компьютер подключен к сети (что сетевой кабель воткнут в разъем).
2. Запустите утилиту конфигурирования сети. Это можно сделать следующим образом:

a) В графической оболочке:
   - Выбрав в системном меню пункт **Settings** → **Конфигурация сети**.

b) В расширенном режиме:
   - Выбрав в меню пункт **Network Configuration (Настройка сети)**.

3. Вид экрана при работе утилиты конфигурирования сети показан на рисунке ниже (в оконном режиме):



4. При помощи этой утилиты вы можете задать следующие параметры сетевого соединения:
   - **Имя хоста** (сетевое имя компьютера). По умолчанию –

drweb.com;

- **Имя домена**. Не используется и не задается;
- IP-адрес или имя хоста используемого **шлюза** (компьютера, через который производится подключение к интернету);
- IP-адрес или имя хоста используемого **сервера имен** (компьютера, на котором работает сервер DNS);
- **IP-адрес** и **маска** сети, используемые этим компьютером.
- Флажок использования **DHCP** (автоматического получения IP-адреса и параметров подключения от шлюза). По умолчанию **DHCP** включен. Когда **DHCP** включен, никакие параметры, кроме имени хоста, недоступны для настройки.

5. Для перемещения курсора между полями ввода используйте клавишу TAB. Активное поле подсвечивается белым фоном. Включение и выключение флажка DHCP (когда на него установден фокус ввода) осуществляется нажатием клавиши ENTER.
6. Для завершения работы утилиты и сохранения внесенных изменений "нажмите кнопку" **ОК** (активируйте ее при помощи клавиши TAB и нажмите ENTER). Для завершения работы утилиты без сохранения внесенных изменений "нажмите кнопку" **Отменить**.

6.4. Отправка сообщений об ошибке

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

- Выбрать в системном меню пункт **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;
- Отправьте письмо, воспользовавшись учетной записью, настроенной по умолчанию.

Если вы работаете в расширенном режиме, то для отправки сообщения об ошибке выполните следующие действия:

- Выберите в меню расширенного режима пункт **Report Bug** (**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).

Приложение А. Виды компьютерных угроз

Под термином *«угроза»* в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они могут нанести вред пользователю.

В продуктах и документации компании **Dr.Web** угрозы принято разделять на два типа в соответствии с уровнем опасности:

- **значительные угрозы** – классические компьютерные угрозы, которые сами по себе способны выполнять различные деструктивные и незаконные действия в системе (удаление и кража важной информации, нарушение работы сети и т.д.). Этот тип компьютерных угроз состоит из программ, которые традиционно называют вредоносными (вирусы, черви и троянские программы);

- **незначительные угрозы** – компьютерные угрозы, которые считаются менее опасными по сравнению со значительными угрозами, но могут быть использованы третьими лицами для совершения вредоносных действий. Помимо этого, само присутствие незначительных угроз в системе является несомненным свидетельством низкого уровня ее защищенности. Специалисты в области информационной безопасности иногда называют этот тип компьютерных угроз «серым» программным обеспечением или потенциально нежелательными программами. К незначительным угрозам относятся рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

Значительные угрозы

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании **Dr.Web** вирусы делят по типу файлов, которые они инфицируют:

- **файловые вирусы** инфицируют файлы операционной системы (обычно, исполняемые файлы и динамические библиотеки) и активизируются при обращении к зараженному файлу;
- **макро-вирусы** инфицируют документы, которые используют программы Microsoft® Office (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). Макросы – это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в Microsoft® Word макросы могут запускаться при открытии, закрытии или сохранении документа);

- **скрипт-вирусы** пишутся на языках сценариев (скриптов) и в большинстве случаев заражают другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях;
- **загрузочные вирусы** заражают загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- **шифрованные вирусы** шифруют свой код при каждом новом заражении, что затрудняет его обнаружения в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры;
- **полиморфные вирусы** используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур;
- **стелс-вирусы** (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в зараженных объектах. Такой вирус снимает перед заражением объекта его характеристики, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на ассемблере, высокоуровневых языках программирования, языках сценариев и т.д.) и по поражаемым операционным системам.

Компьютерные черви

В последнее время черви стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии, но при этом они не заражают другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через сеть Интернет) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании **Dr.Web** червей делят по способу (среде) распространения:

- **сетевые черви** распространяются посредством различных сетевых протоколов и протоколов обмена файлами;
- **почтовые черви** распространяются посредством почтовых протоколов (POP3, SMTP и т.д.);
- **чат-черви** распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т.д.).

Троянские программы

Этот тип вредоносных программ не способен к

саморепликации. Троянские программы подменяют какую-либо из часто запускаемых программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т.д.), либо делая возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловых сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании **Dr.Web** выделяют в отдельные классы:

- **бэкдоры** – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы; они прописывают себя в реестре, модифицируя ключи;
- **руткиты** предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (User Mode Rootkits (UMR)), и руткиты, работающие в

режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (Kernel Mode Rootkits (KMR));

- **клавиатурные перехватчики** (кейлоггеры) используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т.д.);
- **кликеры** переопеделяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак);
- **прокси-трояны** предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы.

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Незначительные угрозы

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (фаерволах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

Это специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-сервера и т.д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типов компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Подозрительные объекты следует отправлять на анализ специалистам **Вирусной лаборатории компании Dr.Web**.

Приложение Б. Устранение компьютерных угроз

Существует множество методов обнаружения и устранения компьютерных угроз. Многие из них объединены в продуктах **Dr.Web** с их гибкими и удобными настройками для обеспечения надежной всесторонней защиты компьютеров и сетей.

Методы обнаружения

Поиск по контрольным суммам сигнатур

Данный метод является разновидностью сигнатурного анализа. *Сигнатура* – это непрерывная конечная последовательность байтов, являющаяся уникальной для определенной компьютерной угрозы. Если в коде проверяемой программы встречается сигнатура из антивирусной базы, то фиксируется факт обнаружения компьютерной угрозы.

Поиск по контрольным суммам сигнатур подразумевает сравнение контрольных сумм, а не самих сигнатур, что позволяет значительно сократить размер антивирусных баз при сохранении надежности традиционного метода сигнатурного анализа.

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* – программной модели процессора (а также, отчасти, компьютера и операционной системы). Эмулятор оперирует с защищенной областью памяти (*буфером эмуляции*). При этом инструкции не передаются на центральный процессор для

реального исполнения. Если код, обрабатываемый эмулятором, заражен вирусом, то результатом его эмуляции станет расшифрованное тело вируса, которое далее легко поддается определению методом поиска по контрольным суммам сигнатур.

Эвристический анализ

Эвристический анализ используется для обнаружения новых, ранее неизвестных угроз, информации о которых нет в антивирусных базах. Принцип эвристического анализа основан на определении, присутствуют ли у объекта часто встречающиеся признаки (характерные особенности) угроз. Каждому признаку при этом сопоставляется некоторое число, называемое его *весом*, которое характеризует важность (или серьезность) этого признака. Вес может быть как положительным, если признак указывает на наличие вредоносного кода, так и отрицательным, если признак не свойственен компьютерным угрозам. Если сумма весов всех обнаруженных в объекте признаков превышает определенное значение, то эвристический анализатор выдает заключение о том, что анализируемый объект может представлять угрозу, и определяет его как подозрительный.

Как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки первого рода (пропуск неизвестной угрозы) и второго рода (ложное срабатывание).

Origins Tracing™

Origins Tracing™ – это уникальный несигнатурный алгоритм обнаружения компьютерных угроз, разработанный специалистами компании **Dr.Web** и используемых только в продуктах **Dr.Web.** Дополняя традиционные методы сигнатурного и эвристического анализа, этот алгоритм значительно увеличивает вероятность обнаружения неизвестных угроз. К названиям угроз, обнаруженных при помощи **Origins Tracing**, добавляется постфикс **.Origin**.

Действия

В продуктах **Dr.Web** реализована возможность применять определенные действия к обнаруженным объектам для обезвреживания компьютерных угроз. Пользователь может оставить автоматически применяемые к определенным типам угроз действия, заданные по умолчанию, изменить их или выбирать нужное действия для каждого обнаруженного объекта отдельно. Ниже приведен список доступных действий:

- **Лечение** – это действие, применимое только к значительным угрозам (вирусам, червям и троянским программам). Оно подразумевает удаление вредоносного кода из инфицированных объектов и, по возможности, восстановление их структуры и работоспособности. Иногда объект состоит только из вредоносного кода и не содержит полезной информации (как, например, троянские программы или функциональные копии компьютерных червей), и в таком случае под лечением понимается удаление самого объекта целиком. Не все зараженные файлы можно вылечить, но алгоритмы лечения постоянно развиваются;
- **Карантин** (перемещать в **Карантин**) – это действие, при котором обнаруженный объект помещается в специальную папку, изолированную от остальной системы. Данное действие можно применять в случаях, когда лечение невозможно, а также для подозрительных объектов. Подобные объекты рекомендуется посылать на анализ в **Вирусную лабораторию компании Dr.Web**;
- **Удаление** является наиболее эффективным способом устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу (или его содержимого). При этом удаление может иногда применяться к объектам, для которых выбрано действие **Лечение**. Подобное «лечение удалением» производится, если файл целиком состоит из вредоносного кода и не содержит никакой полезной информации (например, под лечением компьютерного червя подразумевается удаление всех его функциональных копий);

- **Переименование** – это действие, при котором расширение имени файла изменяется в соответствии с некоторым заданным шаблоном (по умолчанию первый символ расширения заменяется символом «#»); это действие целесообразно применять для файлов других операционных систем (например, MS-DOS® или семейства Microsoft® 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;
- **Игнорирование** (Пропускать) – это действие, применимое только к незначительным угрозам (рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома), при котором ни действий для устранения обнаруженной угрозы, ни оповещения пользователя не производится;
- **Информирование** означает, что к объекту не применяется никакое действие, но информация об обнаруженной угрозе все равно отображается в отчетной таблице результатов сканирования.

Приложение В. Техническая поддержка

Страница службы технической поддержки компании **Dr.Web** находится по адресу http://support.drweb.com/.

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу http://download.drweb.com/;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/;
- попытаться найти ответ в **базе знаний Dr.Web** по адресу http://wiki.drweb.com/;
- посетить **форумы Dr.Web** по адресу http://forum.drweb.com/.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела http://support.drweb.com/.

Найти ближайшее к вам представительство компании **Dr.Web** и всю информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.