Dr.WEB®
LiveUSB

Защити созданное

Руководство пользователя

Dr.Web® LiveUSB
Версия 6.0.0
Руководство пользователя
13.10.2010

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® LiveUSB - 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, клиентов терминальных серверов, клиентов виртуальных серверов и клиентов встроенных систем (**Dr.Web® Desktop Security Suite**);
- защита файловых серверов и серверов приложений (в том числе виртуальных и терминальных) (**Dr.Web® Server Security Suite**);
- защита почты (**Dr.Web® Mail Security Suite**);
- защита интернет-шлюзов и SMTP-шлюзов (**Dr.Web® Gateway Security Suite**);
- защита мобильных устройств (**Dr.Web® Mobile Security Suite**).

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

1.1. Dr.Web® LiveUSB

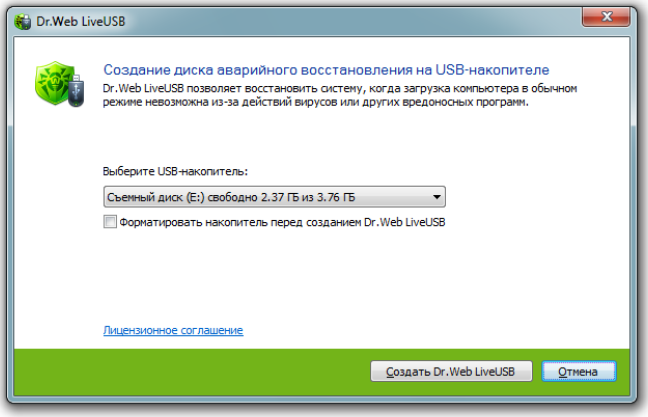
Dr.Web® LiveUSB - это утилита, позволяющая создать загрузочную флэш-карту с переносной операционной системой на базе Linux и встроенным программным обеспечением, предназначенным для проверки и лечения компьютера (антивирусное решение **Dr.Web LiveUSB**), работы с файловой системой, просмотра и редактирования текстовых файлов, просмотра веб-страниц и ведения электронной переписки. С помощью загрузочной флэш-карты можно восстановить систему в тех случаях, когда вследствие вирусной активности не представляется возможным произвести загрузку компьютера с жесткого диска обычным способом.

Dr.Web® LiveUSB поставляется в виде исполняемого файла `drwebliveusb.exe`.

1.2. Создание диска аварийного восстановления

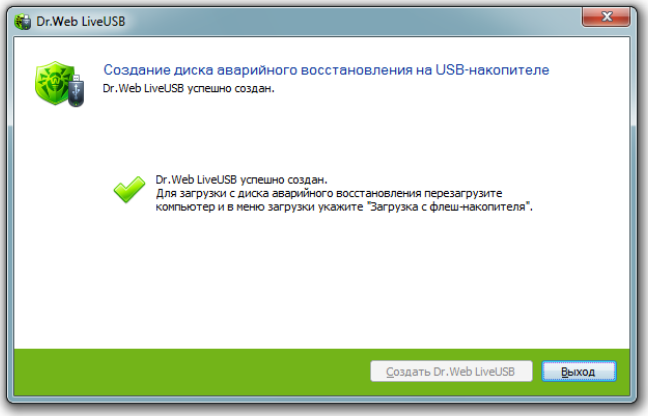
Чтобы создать диск аварийного восстановления на USB-накопителе:

1. Подключите флэш-карту. Регистрация события подключения занимает максимум десять секунд.
2. Запустите приложение `drwebliveusb.exe`.
3. Программа сама определит доступные USB-устройства и предложит вам выбрать нужное. При желании вы сможете отформатировать выбранное устройство (перед форматированием будет выведено окно с предупреждением).



Чтобы ознакомиться с **Лицензионным соглашением**, перейдите по соответствующей ссылке в окне программы (для просмотра текста **Лицензионного соглашения** будет запущен браузер по умолчанию).

4. Для создания загрузочной флеш-карты нажмите кнопку **Создать Dr.Web LiveUSB**.
5. Копирование файлов начнется автоматически.
6. По окончании процесса нажмите кнопку **Выход** для выхода из программы.



1.3. Системные требования

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

- процессор i386;
- 128 МБ оперативной памяти (64 МБ для работы в безопасном режиме);
- флэш-накопитель с объемом памяти не менее 256 МБ.

Для загрузки с флэш-накопителя BIOS вашего компьютера должен поддерживать устройство USB-HDD в качестве загрузочного.

1.4. Запуск антивирусного решения Dr.Web LiveUSB

Убедитесь, что ваш компьютер загружается в первую очередь с флэш-карты, созданной при помощи **Dr.Web® LiveUSB**. При загрузке на экран выводится меню, в котором пользователю предоставляется возможность выбора режима запуска.

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

- чтобы запустить версию антивирусного решения **Dr.Web LiveUSB** с графическим интерфейсом, выберите обычный режим загрузки **Dr.Web-LiveUSB**;
- чтобы запустить антивирусное решение **Dr.Web LiveUSB** с интерфейсом командной строки, выберите режим **DrWeb-LiveUSB (Safe Mode)**;
- выберите **Local HDD**, если вы желаете загрузить компьютер с жесткого диска и не запускать антивирусное решение **Dr.Web LiveUSB** (отменить запуск, произвести загрузку системы 0 раздела 0 диска (hd0,0));
- для проверки памяти (например, если машина работает крайне нестабильно, в случайный момент времени перегружается) выберите вариант **Test Memory**.

Обычный режим является предпочтительным в силу большей наглядности и функциональности. Именно работе в графической оболочке посвящена основная часть руководства. Безопасный режим предназначен для более опытных пользователей, хорошо знакомых с UNIX-подобными операционными системами, и используется при невозможности запуска режима с графическим интерфейсом.

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

2. Графическая оболочка Dr.Web LiveUSB

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

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

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

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

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

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

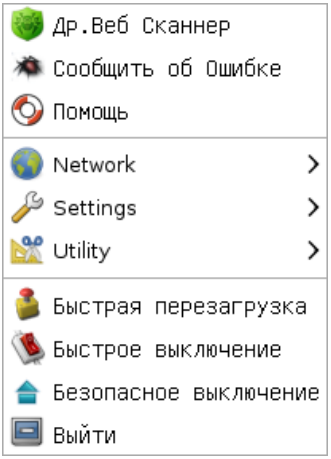
- текстовый редактор **Leafpad**.

Рисунок 1. Графическая оболочка.

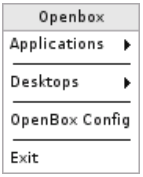
Запуск основных компонентов можно осуществить одним из следующих способов:

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

Системное меню открывается при нажатии на кнопку  на панели задач.



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



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

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

2.1. Настройки

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

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

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

2.1.1. Внешний вид

Эти настройки позволят вам указать параметры графической оболочки Openbox (цветовые темы, рабочий стол и т.п.) (рис. 2).

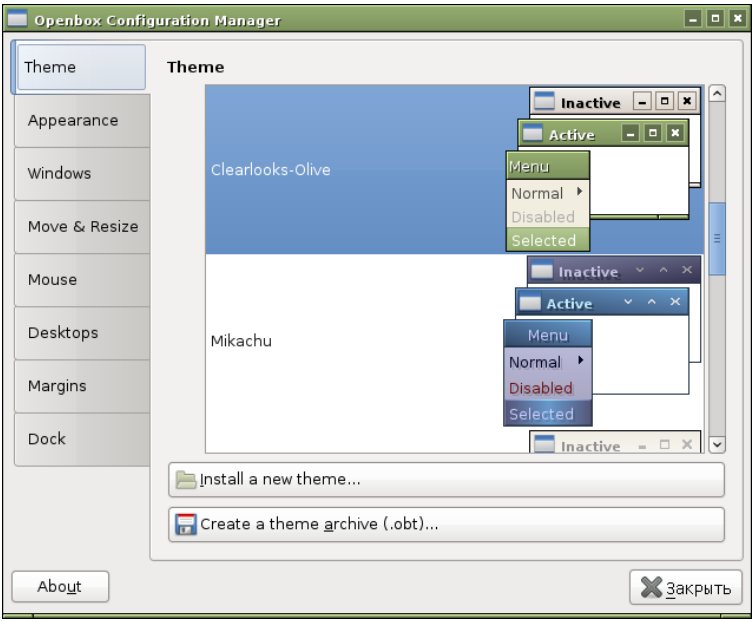


Рисунок 2. Окно настроек графической оболочки.

2.1.2. Графические настройки

Эти настройки позволят вам указать параметры системы X Window (разрешение экрана, тип видеодрайвера, тип мыши, клавиши переключения раскладки клавиатуры) (рис. 3).

Рисунок 3. Окно настроек X Window System.

2.1.3. Конфигурация меню

Эти настройки позволят вам выбрать положение, размер и специальный эффекты отображения панели задач (вкладка **General**), а также задать настройки модулей установленных расширений для графической оболочки (вкладка **Plugins**) (рис. 4).

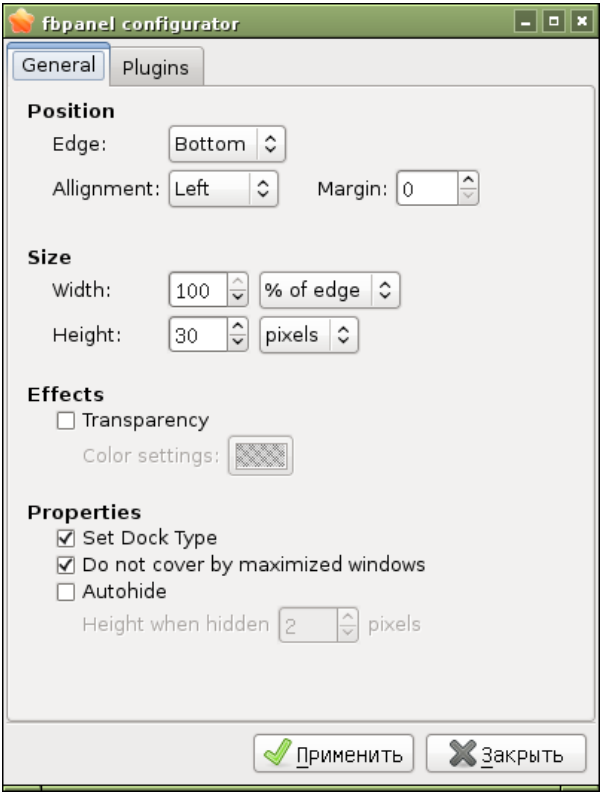


Рисунок 4. Окно настроек панели задач.

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

2.1.4. Конфигурация сети

Эти настройки позволят вам задать параметры подключения к сети вручную, или получить их через DHCP (рис. 5).

Рисунок 5. Окно настроек сети.

2.2. Встроенные приложения

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

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

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

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

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

2.2.1. Браузер

Несмотря на невозможность загрузить компьютер с жесткого диска, интернет-браузер Mozilla Firefox, включенный в состав **Dr.Web LiveUSB**, позволит вам просматривать веб-сайты и сохранять просмотренные страницы (рис. 6). Сохраненные страницы можно будет просмотреть после полного восстановления и загрузки ОС.

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

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

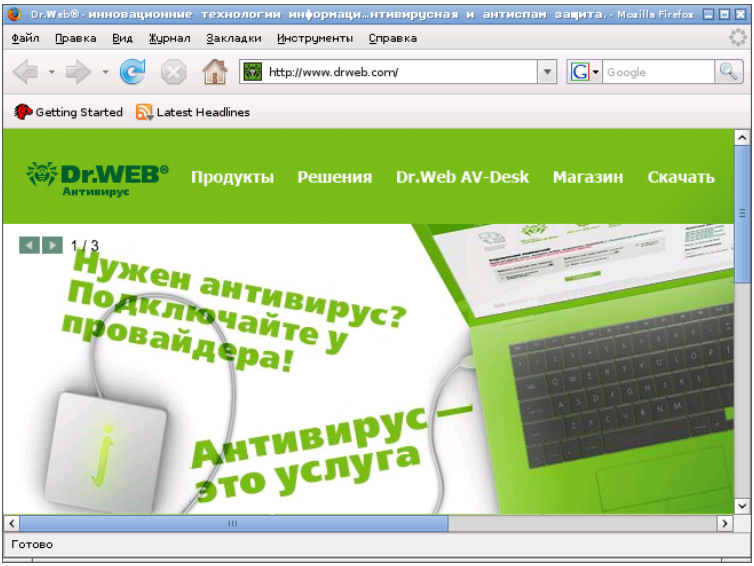


Рисунок 6. Встроенный браузер.

2.2.2. Почтовый клиент

При помощи встроенного почтового клиента **Sylpheed** (рис. 7) вы сможете вести полноценную переписку по электронной почте.

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

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

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

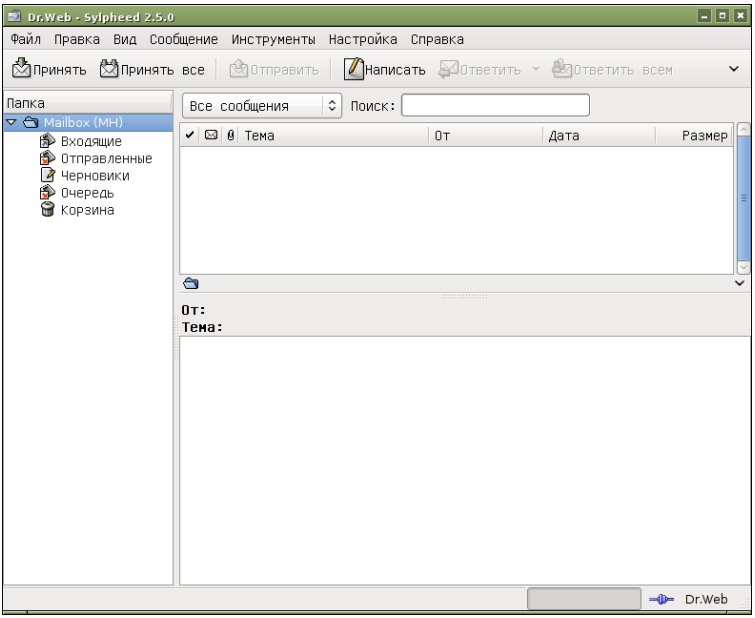


Рисунок 7. Почтовый клиент.

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

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

2.2.3. Файловый менеджер

Встроенный файловый менеджер **Midnight Commander** (рис. 8) аналогичен файловому менеджеру Norton Commander. Используя полноэкранный режим изображения, **Midnight Commander** предоставляет операционной системе интуитивный пользовательский интерфейс и является полезным инструментом для работы с файлами как для опытных пользователей, так и для начинающих.

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

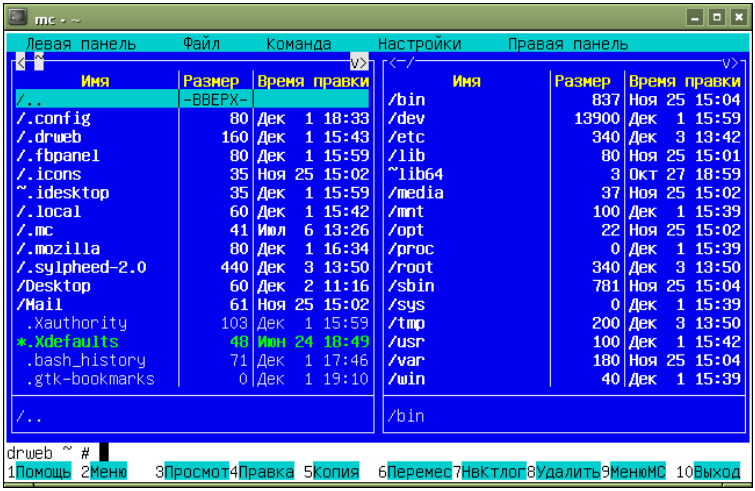


Рисунок 8. Файловый менеджер.

3. Работа со Сканером в графической оболочке

В данном разделе описывается работа со Сканером в графической оболочке Dr.Web Live CD.

3.1 Основные настройки Сканера

Доступ к основным настройкам Сканера осуществляется при помощи кнопки **Изменить установки** на панели инструментов или в меню **Настройка** -> **Настройки** главного окна Сканера. В данном окне настраивается интерфейс программы, реакция на обнаружение зараженных и подозрительных объектов, а также параметры ее взаимодействия с ОС и различными компонентами антивирусного комплекса (рис. 9).

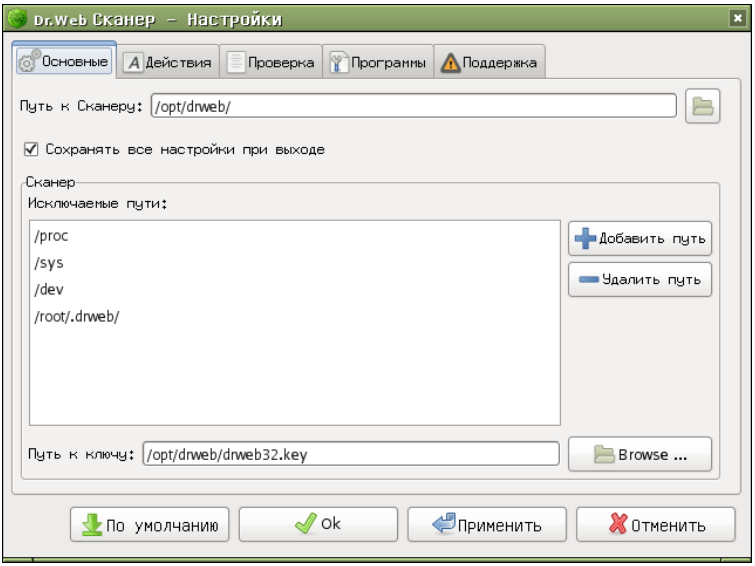


Рисунок 9. Окно настроек Сканера.

Основные настройки Сканера делятся на несколько вкладок:

- Основные - общие настройки Сканера;
- Действия - настройка реакции программы при обнаружении вирусных угроз или какого-либо вредоносного ПО;
- Проверка - настройка режима проверки файлов Сканером, сохранение текущих настроек и загрузка сохраненных настроек;
- Программы - настройка параметров взаимодействия с компонентами антивирусного комплекса и другими программами;
- Поддержка - обновления и техническая поддержка.

В нижней части окна основных настроек Сканера расположены кнопки управления:

- **По умолчанию** - сбросить пользовательские изменения настроек и вернуть настройки по умолчанию;

- **Ok** - сохранить изменения и вернуться в главное окно Сканера;
- **Применить** - сохранить изменения и остаться в окне настроек;
- **Отменить** - вернуться в главное окно Сканера без сохранения изменений в настройках.

3.1.1. Вкладка "Основные"

Окно основных настроек по умолчанию открывается на вкладке **Основные** (рис. 10).

В верхней части этой вкладки задается путь к Сканеру. Для этого необходимо ввести путь в поле ввода **Путь к Сканеру** или нажать на кнопку  и выбрать его в проводнике файловой системы. Аналогично, при необходимости, задайте путь к файлу лицензионного ключа Сканера в поле **Путь к ключу** в нижней части вкладки.

Как правило, заданный по умолчанию путь к Сканеру указан корректно и в редактировании не нуждается.

Для того чтобы измененные настройки сохранялись в конфигурационном файле только при нажатии на кнопку **Сохранить настройки** (см. раздел Вкладка "Проверка"), снимите флажок **Сохранять параметры устройств ввода при выходе**. По умолчанию флажок установлен, и настройки сохраняются при каждом закрытии главного окна Сканера.

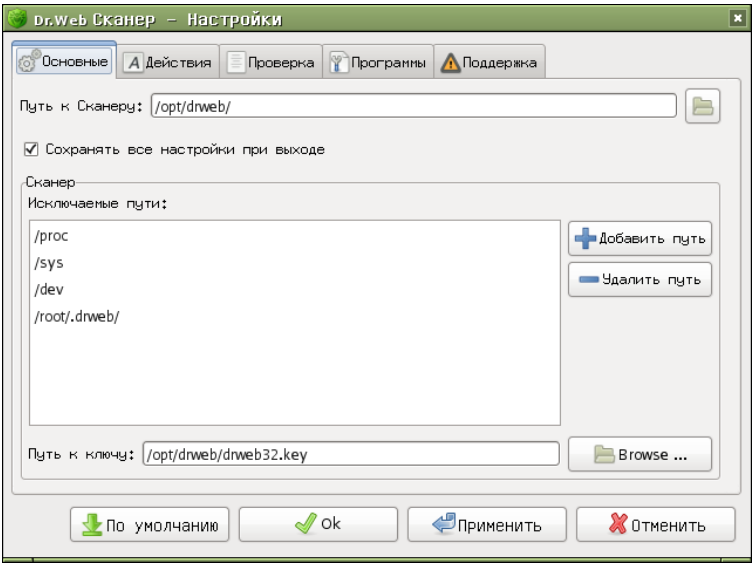


Рисунок 10. Вкладка "Основные"..

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

Панель выбора пути (вверху) изначально содержит кнопки:

- **Введите имя файла** - открыть поле ввода имени файла для добавления (для закрытия поля необходимо повторно нажать кнопку).
- **Файловая система** - открыть список разделов файловой системы **Dr.Web LiveUSB**.

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

Для добавления объектов в закладки для быстрого доступа выберите требуемые директории в проводнике файловой системы и нажмите кнопку **Добавить**. Для удаления объектов из закладок выберите требуемые директории в списке **Места** и нажмите кнопку **Удалить**. В дальнейшем вы можете использовать закладки для быстрой навигации по файловой системе.

После окончания выбора нажмите кнопку **ОК** для добавления выбранной в данный момент директории в список объектов для исключения из сканирования и закрытия окна или кнопку **Отменить** для закрытия окна без совершения какого-либо выбора.

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

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

3.1.2. Вкладка "Действия"

На вкладке **Действия** (рис. 11) настраивается реакция программы при обнаружении вирусных угроз или какого-либо вредоносного ПО.

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

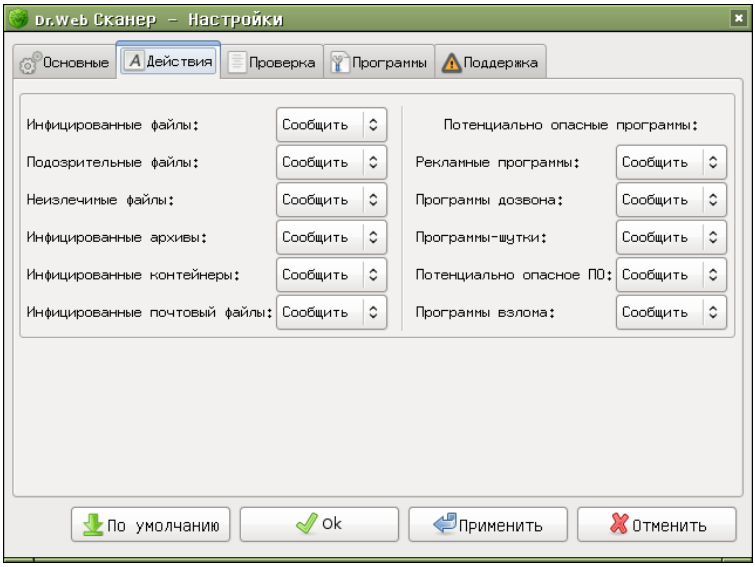


Рисунок 11. Вкладка "Действия".

Вы можете изменить реакцию программы на обнаружение вирусных угроз или вредоносного ПО на вкладке **Действия**. Для этого выберите необходимое действие в выпадающем списке напротив соответствующего типа объекта. В зависимости от типа угрозы списки содержат различный набор возможных действий:

- **Сообщить** - сообщить об обнаруженной угрозе в поле отчета главного окна Сканера.
- **Лечить** - попытаться вылечить файл и восстановить его состояние до заражения. Если лечение невозможно - применить действие, указанное для неизлечимых объектов.
- **Удалить** - удалить файл.

При обнаружении инфицированных или подозрительных файлов в архивах, почте или файловых контейнерах программа применяет указанное действие ко всему объекту в целом, а не к отдельному файлу внутри объекта. Соответственно, если задано действие **Удалить**, то удален будет весь объект со всем своим содержимым, а не только зараженный файл.

Сканер распознает вредоносное ПО следующих видов:

- **Рекламные программы** - используются для демонстрации рекламы;
- **Программы дозвона** - используются для несанкционированного подключения пользователя через dial-up модем к платным службам, чаще всего, порнографическим;
- **Программы-шутки** - могут пугать и отвлекать пользователя;
- **Потенциально опасное ПО** - может быть использовано злоумышленниками;
- **Программы взлома** - средства для несанкционированного доступа к компьютеру.

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

3.1.3. Вкладка "Проверка"

Все основные настройки работы Сканера находятся на вкладке **Проверка** главного окна настроек Сканера (рис. 12). Здесь вы можете сохранить желаемые настройки, загрузить настройки из пользовательского конфигурационного файла `drweb.ini`, а также перейти к секции дополнительных настроек Сканера.

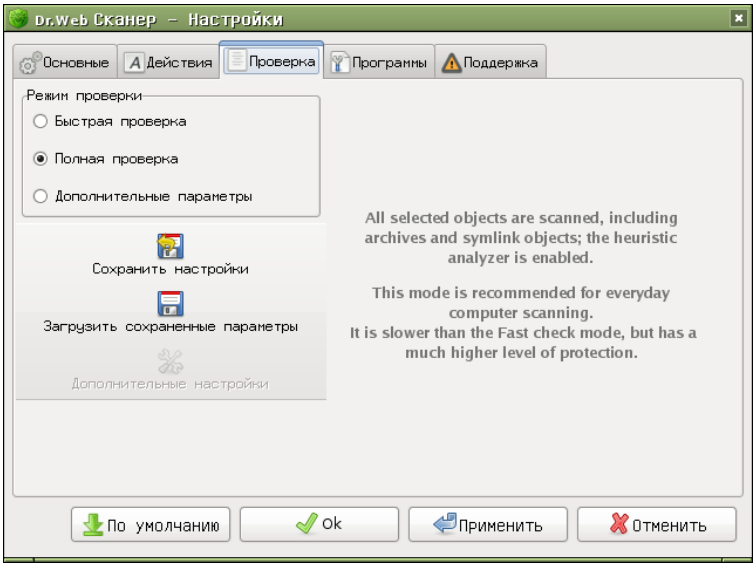


Рисунок 12. Вкладка Checking.

В состав вкладки **Проверка** входят:

- панель **Режим проверки**;
- панель описания режимов проверки;
- кнопки управления настройками.

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

- **Быстрая проверка** - проверяются только файлы, формат которых позволяет им быть «носителями» вирусов; архивы и объекты по символическим ссылкам не проверяются; эвристический анализатор отключен. Проверка происходит гораздо быстрее, чем в режиме полной проверки за счет незначительного снижения надежности.
- **Полная проверка** - режим, в котором проверяются все выбранные объекты, в том числе архивы и объекты по символическим ссылкам; эвристический анализатор

включен. Данный режим рекомендуется для повседневной проверки компьютера. Проверка происходит медленнее, чем в режиме быстрой проверки, но со значительно более высоким уровнем надежности защиты.

- **Дополнительные параметры** - в этом режиме вы можете самостоятельно настроить все параметры, определяющие степень тщательности проверки. Данный режим предназначен в первую очередь для опытных пользователей. При выборе данного режима в левой нижней части окна становится доступной кнопка **Дополнительные настройки**. Для настройки параметров сканирования нажмите данную кнопку (см. раздел Дополнительные настройки).

При выборе любого режима проверки в правой панели вкладки будет показано подробное описание данного режима.

Для того чтобы сохранить изменения настроек в конфигурационном файле, нажмите кнопку **Сохранить настройки**. После этого при каждом запуске программы или загрузке настроек из пользовательского конфигурационного файла будут использованы новые настройки.

Если вы перезагрузите систему без сохранения новых настроек, то любые изменения в конфигурационном файле будут удалены и настройки параметров вернутся в состояние по умолчанию, в котором **Dr.Web LiveUSB** был записан на диск или другой носитель. Обратите внимание, что если флажок **Сохранять параметры устройств ввода при выходе** на вкладке **Основные** установлен, то настройки будут сохраняться при каждом закрытии **Сканера**.

Для того чтобы загрузить настройки из конфигурационного файла программы, нажмите кнопку **Загрузить сохраненные параметры**.

При запуске программы настройки из конфигурационного файла загружаются автоматически. Используйте кнопку **Загрузить сохраненные параметры** только для отказа от внесенных вами свежих изменений в пользу прежнего варианта конфигурации.

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

3.1.4. Вкладка "Программы"

На вкладке **Программы** настраиваются параметры взаимодействия Сканера с компонентами **Dr.Web LiveUSB** (рис. 13).

На вкладке **Программы** расположены три панели:

- **Модуль обновления** - используется для настройки модуля обновлений;
- **Почта** - используется для настройки параметров вызова почтовой программы;
- **Браузер** - используется для настройки параметров вызова браузера.

В верхней панели **Модуль обновления**:

- при необходимости можно отредактировать путь к директории, содержащей модуль обновления. Для этого введите путь в поле **Путь к директории с файлом update.pl** или нажмите на кнопку  для выбора нужной директории в проводнике файловой системы;

- при использовании прокси-сервера для получения обновлений логин и пароль для этого сервера необходимо задать в полях ввода **Логин для прокси** и **Пароль для прокси** соответственно.

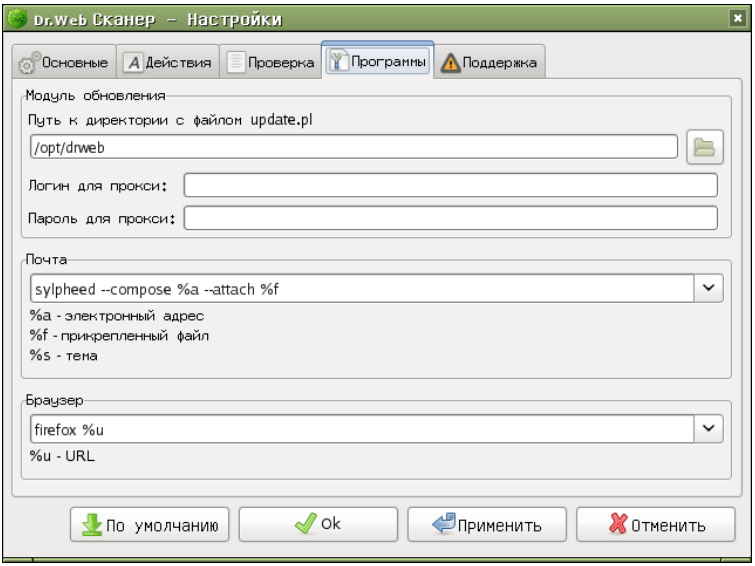


Рисунок 13. Вкладка Programs.

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

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

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

3.1.5. Обновление и техническая поддержка

На вкладке **Поддержка** (рис. 14) можно произвести обновление антивирусных баз, связаться с технической поддержкой, отправить **Dr.Web** информацию о программной ошибке или подозрительный файл на проверку, просмотреть информацию о программе.

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

- Запуск модуля обновления. Осуществляется при нажатии на кнопку **Обновить**.
- Переход на сайт **Dr.Web** в окне веб-браузера. Нажмите кнопку **www.drweb.com**.
- Переход на форум Dr.Web в окне веб-браузера. Нажмите кнопку **Forum** (Форум). Откроется встроенный браузер на странице форума **Dr.Web**.
- Отправка вопроса в службу технической поддержки. Нажмите кнопку **Request to support** (Вопрос в техподдержку). Откроется встроенный браузер на странице технической поддержки **Dr.Web**.
- Отправка сообщения о найденной ошибке по почте. Нажмите кнопку **Bug report** (Сообщить об ошибке). Для отправки почтового сообщения откроется встроенный почтовый клиент.
- Отправка файлов, предположительно инфицированных неизвестными вирусами, на анализ в лабораторию **Dr.Web** . Нажмите на кнопку **Отправить файл на анализ**. Откроется окно выбора файлов.

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

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

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

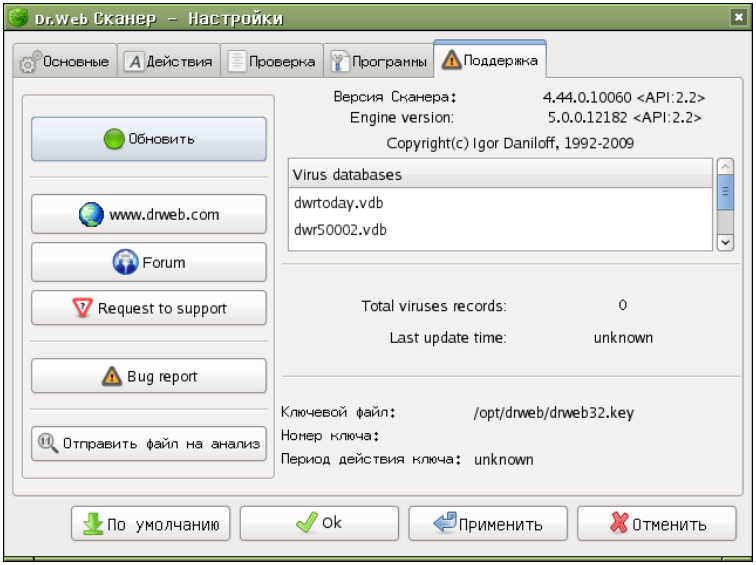


Рисунок 14. Вкладка "Поддержка".

3.2. Дополнительные настройки Сканера

Опытные пользователи могут самостоятельно настроить все

параметры, определяющие степень тщательности проверки, в секции Дополнительных настроек.

Для самостоятельной настройки параметров сканирования:

1. В меню Сканера **Настройка** выберите пункт **Настройки** и перейдите на вкладку **Проверка**.
2. На панели **Режим проверки** выберите **Дополнительные параметры**.
3. При этом становится доступной кнопка **Дополнительные настройки**. Нажмите кнопку для доступа к настройкам.
4. Либо непосредственно в меню Сканера **Настройка** установите флаг напротив пункта **Дополнительные параметры**.
5. При этом станет доступным пункт **Дополнительные опции**. Пройдите по этой ссылке для доступа к секции дополнительных настроек.

Меню расширенных настроек позволяет вручную задать пути к директориям, которые используются различными компонентами программы, указать типы проверяемых файлов, настроить порядок ведения отчетов о работе программы и т.д. (рис. 15).

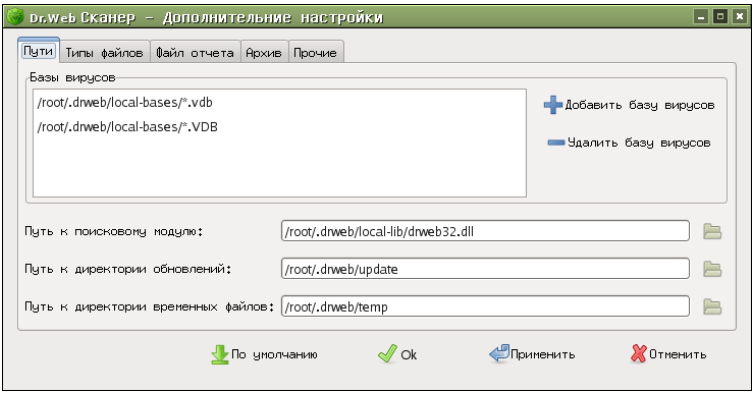


Рисунок 15. Окно дополнительных настроек Сканера.

Дополнительные настройки Сканера делятся на несколько

разделов (вкладок):

- Пути - указание путей к основным модулям Сканера;
- Типы файлов - настройка типов файлов, подлежащих проверке;
- Файл отчета - настройка ведения отчета;
- Архив - настройка ограничений, налагаемых на действия с архивами из соображений безопасности;
- Прочие - задание настроек, влияющих на загруженность компьютера, указание таймаута модуля обновления и включение эвристического анализатора.

В нижней части окна расширенных настроек сканера расположены кнопки управления:

- **По умолчанию** - сбросить пользовательские изменения настроек и вернуть настройки по умолчанию;
- **Ok** - сохранить настройки и вернуться в главное окно Сканера;
- **Применить** - сохранить внесенные изменения и остаться в окне настроек;
- **Отменить** - вернуться в главное окно Сканера без сохранения сделанных изменений.

3.2.1. Вкладка "Пути"

Окно расширенных настроек Сканера по умолчанию открывается на вкладке **Пути** (рис. 16).

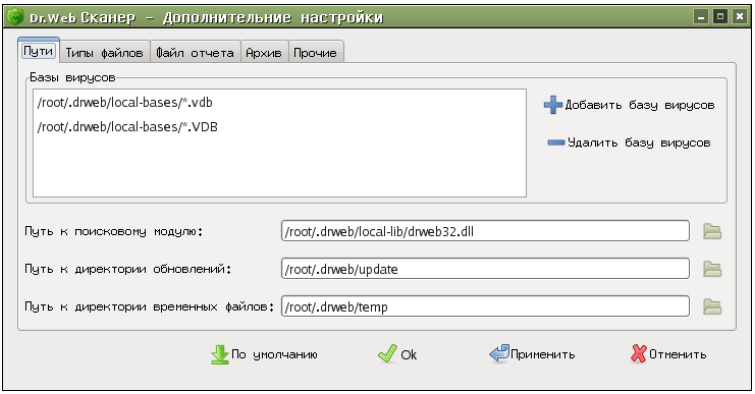


Рисунок 16. Вкладка "Пути".

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

Для того чтобы добавить элемент в список вирусных баз, нажмите на кнопку **Добавить базу вирусов**. Откроется окно добавления базы.

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

Для того чтобы удалить элемент из списка вирусных баз, выберите его и нажмите на кнопку **Удалить базу вирусов**.

При необходимости вы можете отредактировать в соответствующих полях ввода пути к поисковому модулю, директории обновления и директории временных файлов.

Также вы можете задать альтернативные пути, нажав на кнопку  рядом с соответствующей строкой ввода и выбрав их в проводнике файловой системы.

3.2.2. Вкладка "Типы файлов"

На вкладке **Типы файлов** настраиваются ограничения для проверяемых файлов (рис. 17).

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

- **Все** - проверяются все файлы, независимо от типа и внутренней структуры. Данный режим задан по умолчанию при выборе режима **Полная проверка** на вкладке Проверка настроек Сканера.
- **По типу** - проверяются только файлы с расширениями, заданными в списке **Типы файлов**. По умолчанию в список включены исполняемые файлы и файлы, содержащие макросы. Для добавления расширения в список нажмите на кнопку **Добавить тип файла**, введите в открывшемся окне желаемое расширение и нажмите **Применить**. Для удаления расширения из списка отметьте его и нажмите на кнопку **Удалить тип файла**.

  Кнопки **Добавить тип файла** и **Удалить тип файла** активны только при выборе режима проверки **По типу**.

- **По формату** - проверяются все файлы, которые по внутренней структуре могут быть носителями вирусов. Данный режим задан по умолчанию при выборе режима **Быстрая проверка** на вкладке Проверка настроек Сканера.

Ниже на вкладке **Типы файлов** вы можете выбрать следующие флажки, чтобы установить дополнительные ограничения на проверку файлов:

- **Следовать по символическим ссылкам** - устанавливается, чтобы Сканер проверял файлы, символические ссылки на которые попадают в число проверяемых объектов.
- **Проверять архивы** - устанавливается, чтобы Сканер распаковывал файловые архивы и проверял входящие в них файлы (при установленном режиме **По формату** - если они имеют соответствующий формат; при выборе режиме **По типу** - в список расширений должны входить как расширение архива, так и расширение проверяемого файла).
- **Проверять e-mail файлы** - устанавливается, чтобы Сканер проверял файлы, прикрепленные к почтовым сообщениям.

При выборе режима **Полная проверка** на вкладке Проверка настроек Сканера все три вышеперечисленных флажка по умолчанию установлены; при выборе режима **Быстрая проверка** - все они по умолчанию сняты.

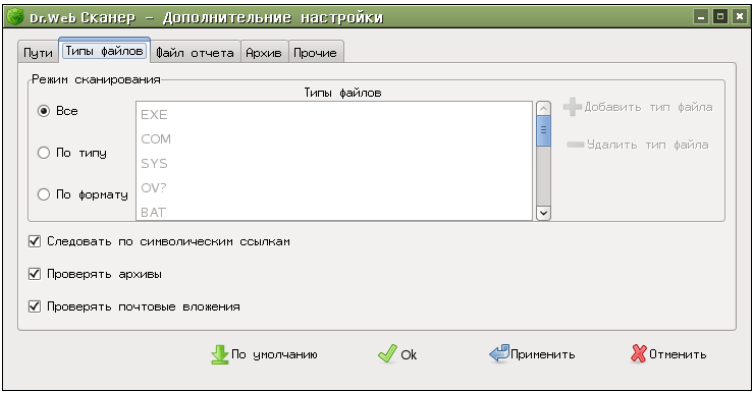


Рисунок 17. Вкладка "Типы файлов".

3.2.3. Вкладка "Файл отчета"

На вкладке **Файл отчета** (рис. 18) настраивается ведение отчета.

На панели **Имя файла отчета** выбирается способ протоколирования - средствами **Dr.Web LiveUSB** или через системную службу:

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

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

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

Установленный флажок **Ограничить размер файла отчета** указывает, что файл отчета не может превышать размер, указанный в поле ввода справа. После достижения файлом отчета максимального размера старые записи из него постепенно стираются, чтобы освободить место для записей новых событий. Снятие флажка убирает ограничение на размер файла отчета.

Рекомендуется сохранить установленный по умолчанию флажок **Ограничить размер файла отчета** и значение по умолчанию в поле **Максимальный размер файла отчета** (512 Кб).

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

В выпадающем списке **Уровень подробности файла отчета** задается требуемый уровень подробности ведения отчета. Доступны следующие уровни ведения отчета: **Debug | Verbose | Info | Warning | Error | Quiet**.

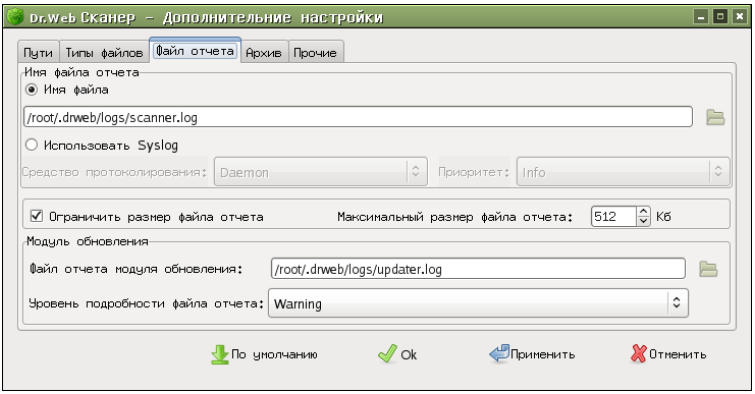


Рисунок 18. Вкладка Log file.

3.2.4. Вкладка "Архив"

На вкладке **Архив** (рис. 19) настраиваются ограничения, накладываемые на действия с архивами из соображений безопасности.

Параметры на данной вкладке направлены на защиту Сканера от

атак «почтовыми бомбами». При превышении заданных численных значений характеристик архивов их проверка прекращается, чтобы не исчерпать ресурсы системы.

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

- **Максимальный коэффициент сжатия** - по умолчанию `5000`;
- **Максимальный уровень вложенности архива** - по умолчанию `8`;
- **Порог проверки сжатия** - по умолчанию `5000 Кб`. Архивы меньшего размера проверяются независимо от коэффициента сжатия;
- **Максимальный размер файла для извлечения** - по умолчанию `1024 Кб`. При обнаружении файлов большего размера архив не распаковывается.

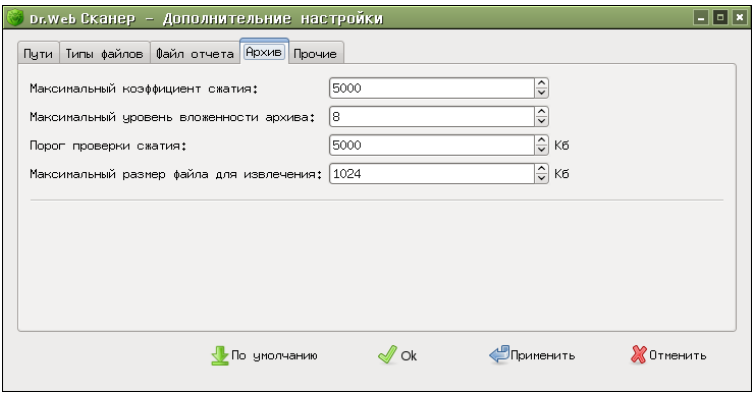


Рисунок 19. Вкладка "Архив".

3.2.5. Вкладка "Прочие"

На вкладке **Прочие** (рис. 20) задаются настройки, влияющие на загруженность компьютера, указывается время ожидания для модуля обновления и производится включение и выключение эвристического анализатора.

На панели **Приоритет сканирования** при помощи кнопок-переключателей задается приоритет процесса сканирования по сравнению с остальными процессами в системе: **Высокий**, **Нормальный**, **Низкий**.

В поле ввода **Максимальное время ожидания** задается максимальное время ожидания в секундах для модуля обновления при соединении с сервером обновлений.

Флажок **Эвристический анализ** включает режим *эвристического анализатора* (режим поиска неизвестных вирусов на основании анализа структуры файла).

В режиме эвристического анализатора возможны ложные срабатывания. Обнаруженные с его помощью файлы всегда имеют статус «подозрительных». При выборе режима **Полная проверка** эвристический анализатор включается по умолчанию. При выборе режима **Быстрая проверка** эвристический анализатор выключен.

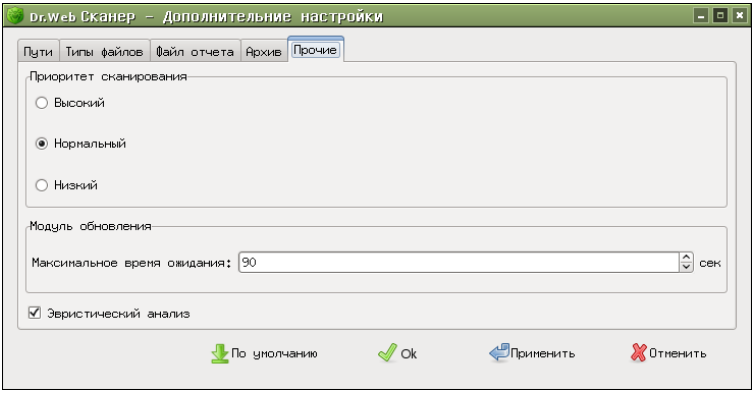


Рисунок 20. Вкладка "Прочие".

3.3. Антивирусная проверка

Данный раздел описывает процесс проверки файловой системы компьютера на наличие вирусов.

3.3.1. Запуск сканирования

Сканер Dr.Web для Linux можно запустить следующими способами:

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

После запуска Сканера откроется главное окно программы (рис. 21).

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

Перед началом сканирования рекомендуется обновить **антивирусные базы Dr.Web**. Для этого воспользуйтесь кнопкой **Обновить базы** в верхней части главного окна Сканера.

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

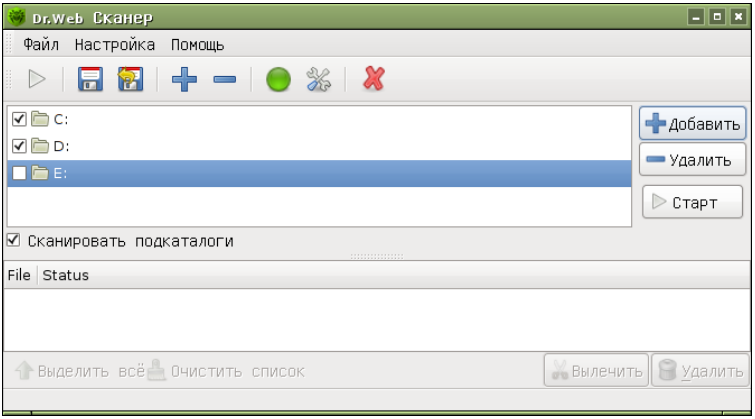


Рисунок 21. Главное окно Сканера.

Чтобы добавить или удалить объект из списка сканируемых объектов, используются кнопки **Добавить** и **Удалить** соответственно.

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

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

При нажатии на кнопку **Добавить** открывается окно выбора объектов для сканирования (рис. 22).

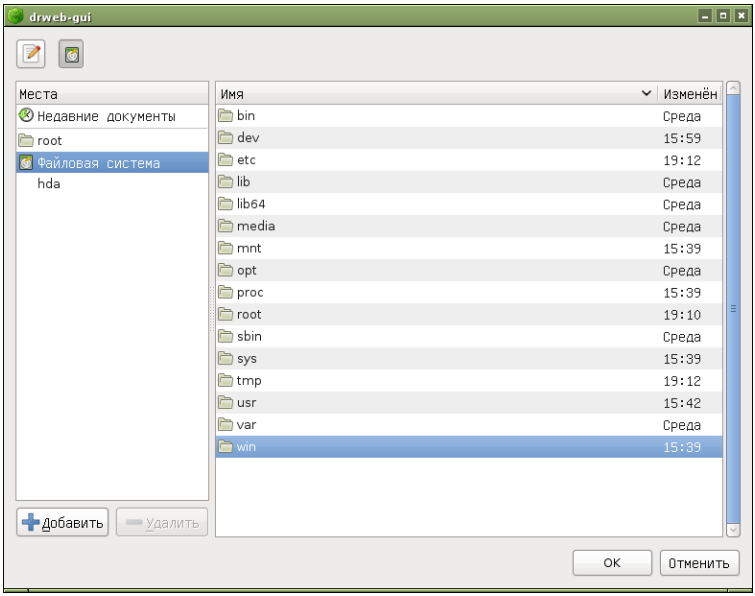


Рисунок 22. Окно выбора объектов для сканирования.

Панель выбора пути (вверху) изначально содержит кнопки:

- **Введите имя файла** - открыть поле ввода имени файла для добавления (для закрытия поля необходимо повторно нажать кнопку).
- **Файловая система** - открыть список разделов

файловой системы **Dr.Web LiveUSB**.

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

Для добавления объектов в закладки для быстрого доступа выберите требуемые директории в проводнике файловой системы и нажмите кнопку **Добавить**. Для удаления объектов из закладок выберите требуемые директории в списке **Места** и нажмите кнопку **Удалить**. В дальнейшем вы можете использовать закладки для быстрой навигации по файловой системе.

После окончания выбора нажмите кнопку **ОК** для добавления выбранной в данный момент директории в список объектов для сканирования и закрытия окна или кнопку **Отменить** для закрытия окна без совершения какого-либо выбора.

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

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

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

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

3.3.2. Результаты сканирования

Результаты сканирования отображаются в виде таблицы (рис. 23) внизу главного окна 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.

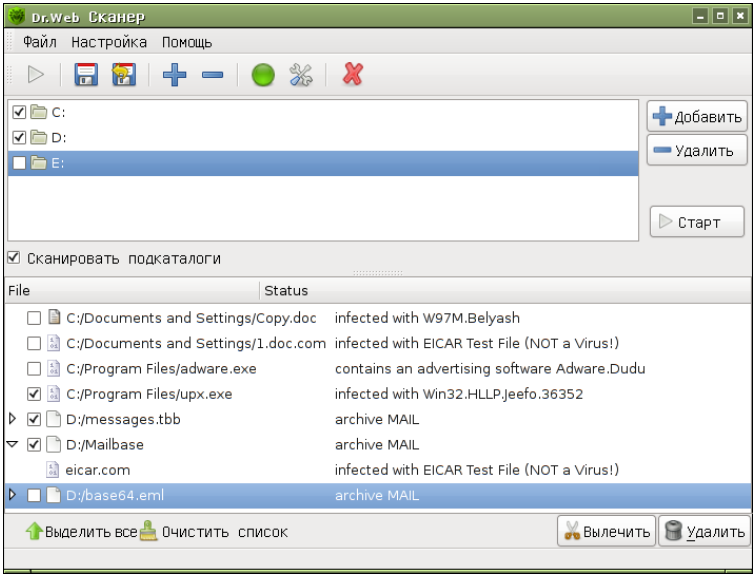


Рисунок 23. Результаты сканирования.

На нижней панели, расположенной под окном отчета, для каждого объекта при помощи соответствующих кнопок выбирается желаемое действие: **Вылечить** или **Удалить**.

Действие **Вылечить** недоступно для архивов, контейнеров и почтовых файлов.

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

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

Для того чтобы вручную произвести необходимые действия с обнаруженным объектом, установите флажок напротив имени этого объекта (или нажмите кнопку **Выделить все**, чтобы отметить все обнаруженные объекты) и нажмите одну из кнопок: **Вылечить** или **Удалить**.

4. Работа с консольным Сканером

В данном разделе описываются особенности работы с консольным Сканером.

4.1. Запуск процесса сканирования

После загрузки **Dr.Web LiveUSB** в безопасном режиме на экран выводится главное меню запуска - **Стартовое Меню** (рис. 24).

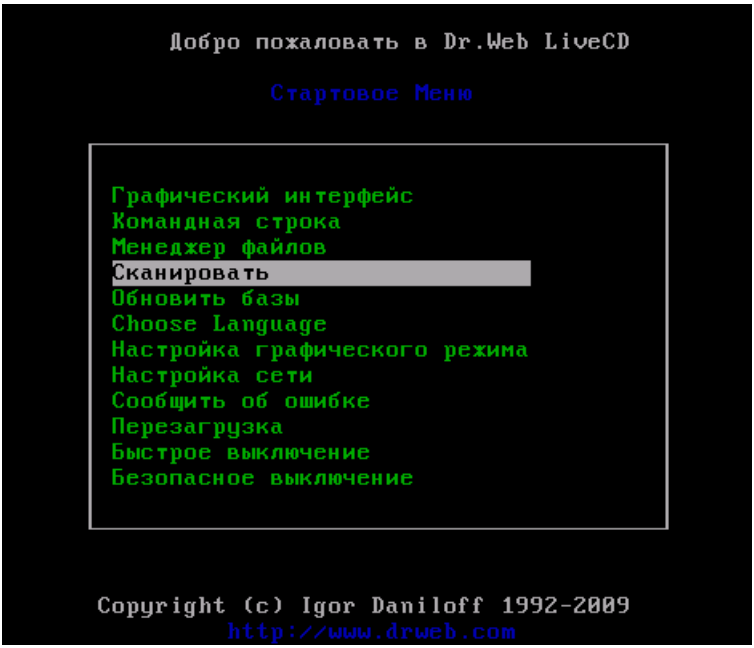


Рисунок 24. Стартовое меню.

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

- **Графический интерфейс** - запустить **Сканер** с графическим интерфейсом;
- **Командная строка** - вывести на экран командную строку;
- **Менеджер файлов** - запустить встроенный файловый менеджер;
- **Сканировать** - сканировать все разделы жесткого диска с настройками по умолчанию;
- **Обновить базы** - обновить вирусные базы;
- **Choose Language** - изменить язык интерфейса;
- **Настройка графического режима** - настроить графический режим, если автоматическое конфигурирование графической оболочки не сработало или сработало неверно;
- **Настройка сети** - настроить сеть, если автоматичекое конфигурирование сети не сработало или сработало неверно;
- **Сообщить об ошибке** - отправить разработчикам информацию об ошибке в ПО;
- **Перезагрузка** - перезагрузить компьютер;
- **Быстрое выключение** - выключить компьютер, не извлекая диска LiveUSB;
- **Безопасное выключение** - извлечь диск и завершить работу компьютера.

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

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

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

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

```
$ /opt/drweb/drweb -path /win/C:
```

4.2. Параметры командной строки

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

Основные параметры программы могут быть сгруппированы следующим образом:

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

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

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

Параметры диагностики, определяющие, какие типы объектов

должны проверяться на вирусы:

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

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

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

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

Параметры интерфейса определяют условия вывода результатов работы программы:

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

указанный файл;

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

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

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

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

```
$ drweb -path <путь> -ha-
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Отправка сообщений об ошибке

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

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

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

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