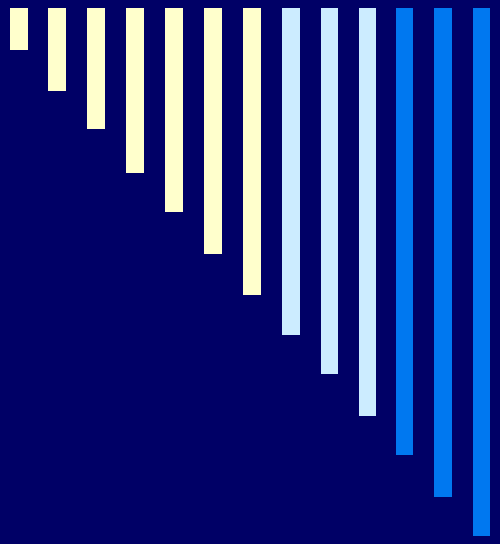
Практическое занятие № 7



Настройка и работа с антивирусными программами на примере пакета прикладных и системных программ ПО «ДОКТОР ВЕБ» (Dr.Web).

Цель: Научиться использовать антивирусное программное обеспечение на примере пакета прикладных и системных программ ПО «ДОКТОР ВЕБ» (Dr.Web).

По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

Содержание:

По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

Теоретическая часть
1. Модуль графического интерфейса сканера

Вид элементов интерфейса описываемой программы и действия пользователя могут изменяться в зависимости от ОС и ее настроек. Описание ведется на примере работы программы под управлением ОС **Linux Fedora Core 3**, графическая среда **GNOME**. Многие операции и настройки программы могут быть осуществлены разными путями (с использованием главного меню, контекстного меню, горячих клавиш и других средств). Как правило, для краткости описывается только одна из предоставляемых возможностей.

1.1. Установка и запуск программы

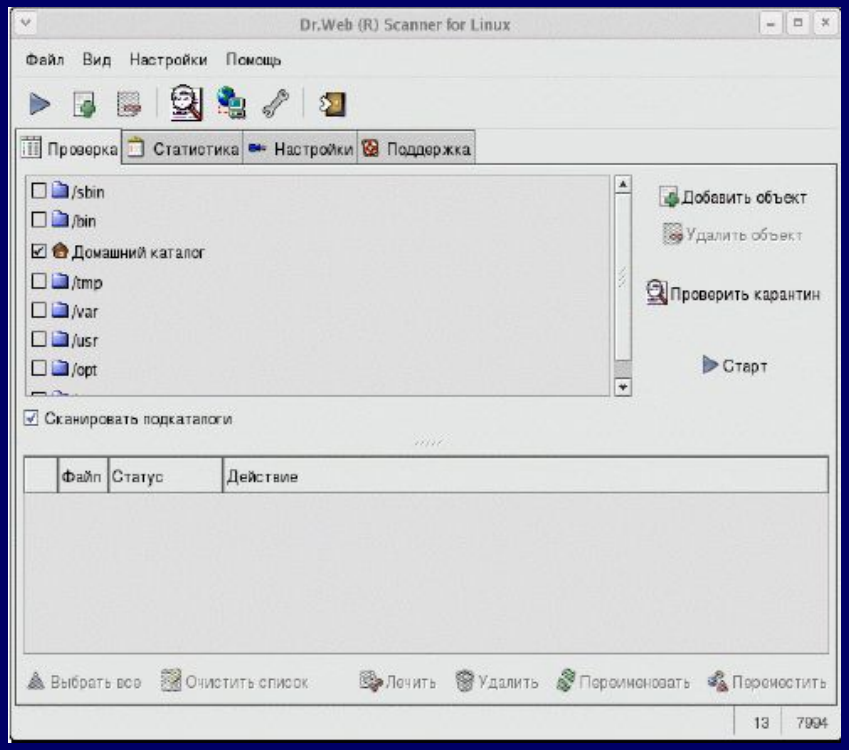


Рисунок 1. - Главное окно модуля графического интерфейса

Перед запуском программы необходимо запустить **X Window Server.**

Способ запуска Модуля графического интерфейса зависит от **ОС** и способа установки модуля. Если для установки использовался менеджер пакетов **RPM**, выполните в консоли команду **xdrweb**.

Независимо от способа установки вы можете также запустить на выполнение файл **drweb-gui** из каталога установки сканера.

Откроется главное окно программы (рисунок 1).

1.1. Установка и запуск программы

Немедленно после запуска программа проверяет настройки путей к ключевому файлу сканера и исполняемому файлу сканера.

При отсутствии по указанному адресу действительного ключевого файла и исполняемого файла сканера выдаются соответствующие предупреждения.

После этого модуль графического интерфейса запускает сканер для получения информации о состоянии антивирусной защиты.

При невозможности запуска сканера выдается соответствующее сообщение.

При необходимости отредактируйте соответствующие настройки программы и проверьте корректность установки сканера.

1.1. Установка и запуск программы

При запуске программы из командной строки можно использовать следующие параметры:

- **-default-settings** – не загружать конфигурационный файл
- **-eng-lng-save=<путь>** - сохранить файлы языковых ресурсов по умолчанию по указанному пути
- **-ini-file=<путь>** - путь к конфигурационному файлу
- **-no-lng-load** – не загружать файлы языковых ресурсов (использовать английский язык, ресурс содержится в самой программе)
- **-d** или **--debug** – запустить в отладочном режиме
- **-v** или **--version** – выдать сведения о версии программы
- **-h** или **--help** – показать краткую подсказку

1.2. Настройки сканера
Редактирование и сохранение настроек. Выбор режима сканирования

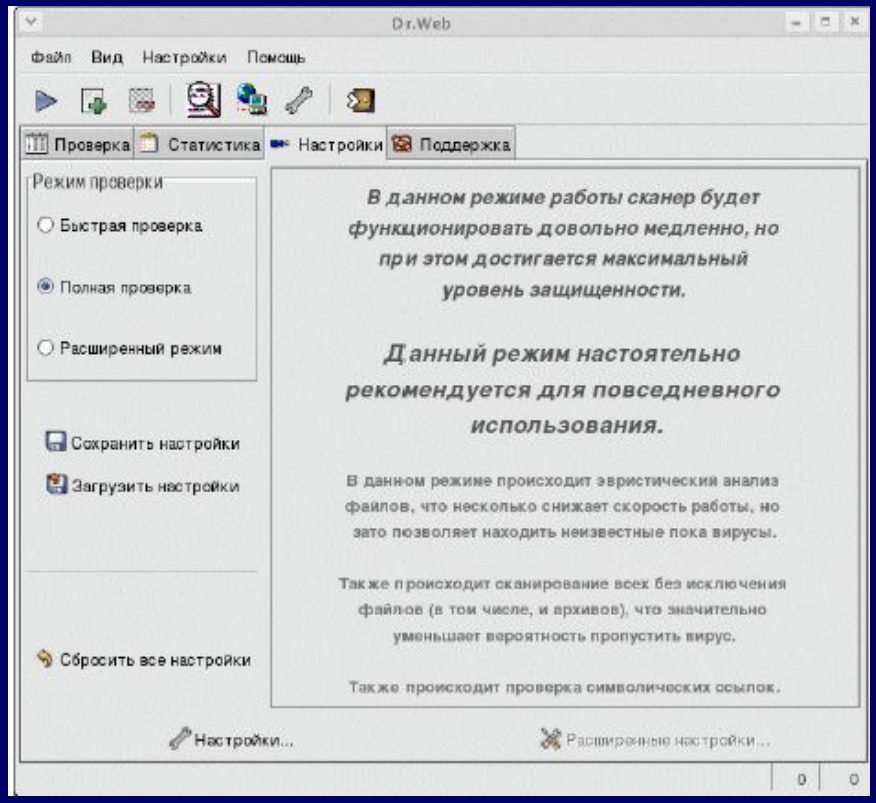


Рисунок 2. - Вкладка Настройка

Для того чтобы перейти к редактированию настроек, перейдите на вкладку Настройка (рисунок. 2).

1.2. Настройки сканера

Редактирование и сохранение настроек. Выбор режима сканирования

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

При запуске программы настройки из конфигурационного файла будут загружены автоматически. Используйте эту кнопку только для отказа от изменений настроек, внесенных вами с помощью Модуля графического интерфейса сканера.

Для того чтобы записать изменения настроек в конфигурационный файл, нажмите на кнопку

Сохранить настройки.

Для того чтобы загрузить в программу настройки по умолчанию, нажмите на кнопку Сбросить все настройки.

Настройки самого Модуля графического интерфейса также хранятся в конфигурационном файле программы в секции [**GUI**].

1.2. Настройки сканера

Редактирование и сохранение настроек. Выбор режима сканирования

Вы также можете настроить режим сканирования (уровень тщательности проверки). Для этого выберите в группе кнопок выбора Режим проверки один из следующих вариантов:

Расширенный режим — в этом режиме вы можете самостоятельно настроить все параметры, определяющие степень тщательность проверки. Смысл этих параметр описывается ниже.

Полная проверка — режим, в котором проверяются все отобранные файлы, в том числе архивные. Режим рекомендуется для повседневной проверки компьютера.

Быстрая проверка — режим, в котором проверяются только файлы, внутренний формат которых позволяет им быть "носителями" вирусов, архивы не проверяются, отключен эвристический анализ. При этом проверка происходит гораздо быстрее, чем в режиме полной проверки, за счет некоторого снижения надежности контроля.

Основные настройки программы

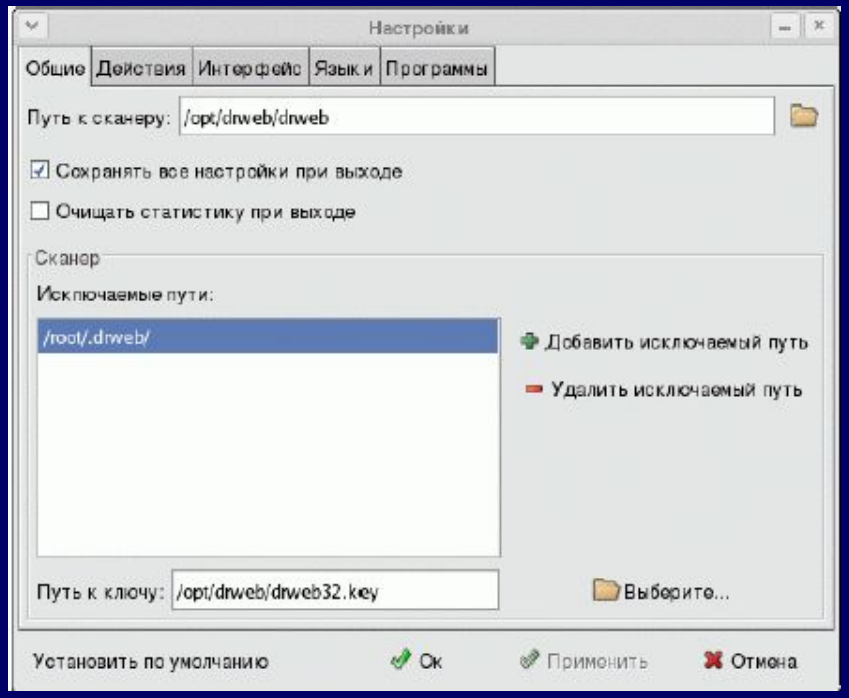


Рисунок 3. - Общие настройки

Независимо от выбранного режима сканирования, вы можете настроить реакцию программы на обнаружение инфицированных объектов, а также параметры взаимодействия с **ОС** и между различными программами антивирусного комплекса.

Для того чтобы просмотреть и при необходимости отредактировать основные настройки, нажмите на вкладке Настройки главного окна на кнопку **Настройки**. Откроется окно Настройки на вкладке **Общие** (рисунок 3).

Основные настройки программы

На этой вкладке вы можете задать путь к сканеру (как правило, при установке программы он указан корректно и в редактировании не нуждается). Для этого введите путь в поле ввода Путь к сканеру или нажмите на кнопку  и выберите его в обозревателе файловой системы.

Аналогично, при необходимости, задайте путь к файлу лицензионного ключа сканера в поле Путь к ключу.

Снимите флажок **Сохранять все настройки при выходе**, если хотите, чтобы настройки сохранялись в конфигурационный файл только при нажатии на соответствующую кнопку.

Основные настройки программы

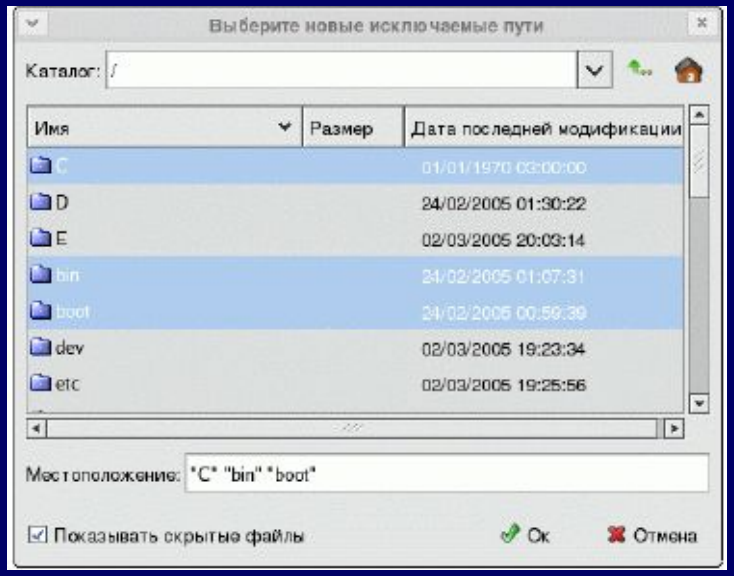


Рисунок 4. - Добавление исключаемого пути

По умолчанию флажок установлен; при этом настройки сохраняются также при закрытии главного окна.

Установите флажок **Очищать** всю статистику при выходе, если хотите вести статистику только на каждый отдельный сеанс.

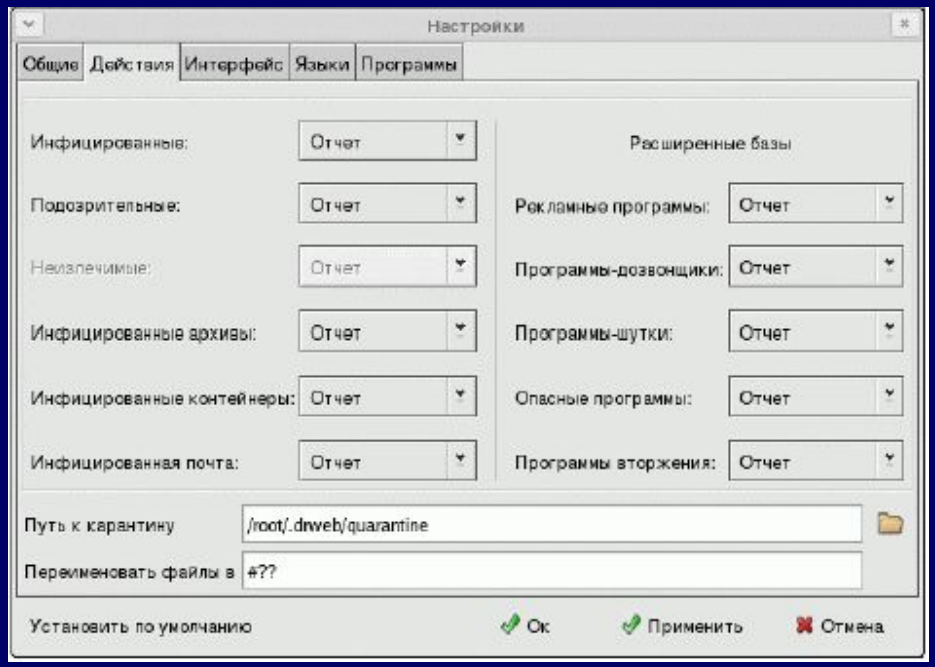
Вы можете задать список исключаемых из сканирования путей.

По умолчанию список содержит только каталог, используемый для размещения карантина.

Для того чтобы добавить в список какой-либо каталог или файл, нажмите на кнопку **Добавить** исключаемый путь.

Откроется окно выбора пути, рисунок 4.

Основные настройки программы



Чтобы выделить нужные файлы или каталоги, удерживая клавишу **Ctrl**, щелкните мышью по соответствующим объектам (если нужно выделить только один объект, дважды щелкните по нему). По окончании выбора нужных объектов нажмите на кнопку **OK**.

Рисунок 5. - Настройка действий

Основные настройки программы

Выберите в раскрывающемся списке **Инфицированные действия**, которое будет предпринято программой при обнаружении файла, зараженного вирусом:

Отчет — выдать информацию об инфекции в отчет. Пользователь сможет задать реакцию программы вручную.

Лечить — пытаться восстановить состояние инфицированного объекта до заражения. При невозможности или не успешности будет применена реакция, заданная для неизлечимых.

Удалить — удалить инфицированный файл.

Карантин — переместить инфицированный файл с каталог карантина (см. ниже).

Переименовать — переименовать инфицированный файл в соответствии с маской переименования.

Основные настройки программы

По умолчанию предусмотрено информирование пользователя (реакция Отчет). Рекомендуется сохранить ее. Информация об обнаруженных файлах сообщается пользователю в специальном поле главного окна. Пользователь может предписать произвести необходимые действия вручную.

Аналогично настраивается реакция на обнаружение файлов, зараженных неизлечимым вирусом или подозрительных на зараженность. В том случае недоступен выбор **Лечить**.

Пункт Неизлечимые доступен только в том случае, когда для инфицированных файлов выбрана настройка **Лечить**.

Основные настройки программы

При обнаружении инфицированных или подозрительных файлов в файловых архивах, почте или файловых контейнерах программа не предпринимает никаких действий в отношении отдельных файлов в архивах этих типов, однако вы можете настроить автоматические действия в отношении архивов каждого типа в целом. Настройка полностью аналогична настройке реакции на обнаружение неизлечимых или подозрительных файлов.

При настройках по умолчанию для архивов любого типа недоступна также реакция

Удалить. Разрешение использования удаления архивов настраивается в расширенных настройках программы.

Основные настройки программы

В правой части окна настраивается реакция на обнаружения файлов, содержащих нежелательные программы следующих видов:

- рекламные программы (демонстрируют рекламу)
- программы - **дозвонщики** (выполняют несанкционированное подключение к платным сайтам, чаще всего порнографическим)
- **программы-шутки** (могут пугать и отвлекать пользователя)
- **опасные программы** (могут использоваться злоумышленниками)
- программы вторжения (средства для несанкционированного доступа на компьютеры и другие электронные устройства)

Настройка реакции в этих случаях аналогична настройке реакции на обнаружение подозрительных или неизлечимых файлов,
однако добавляется также действие **Игнорировать**.

Вы можете отредактировать заданный по умолчанию путь к каталогу для перемещаемых файлов (каталогу карантина).

Основные настройки программы

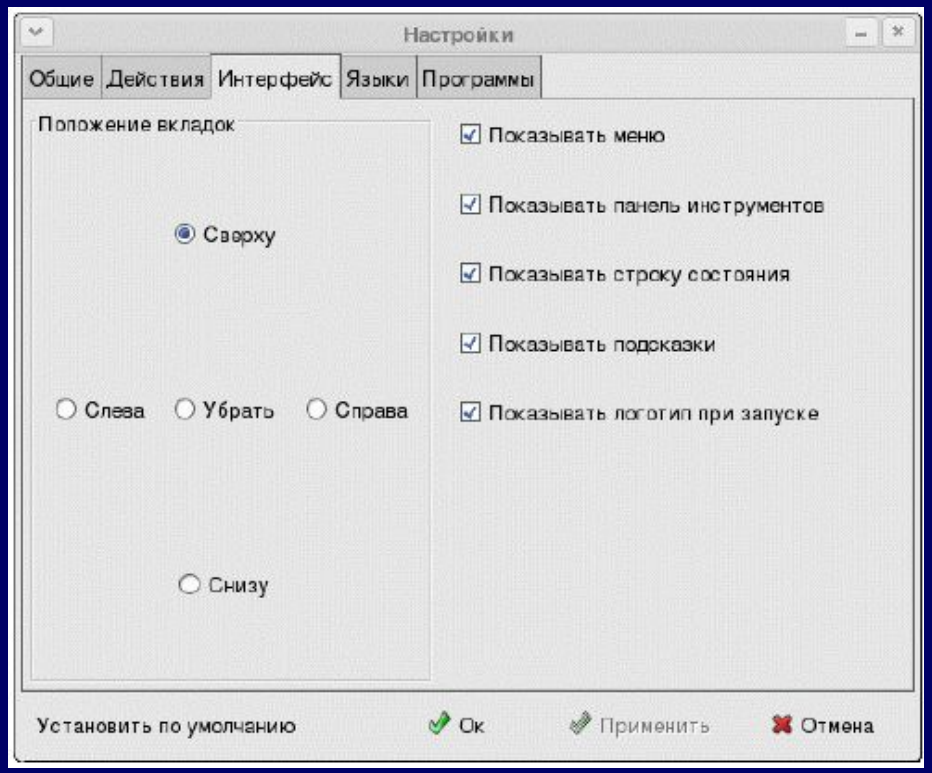


Рисунок 6. - Настройка интерфейса

Отредактируйте путь в поле ввода Путь к карантину или нажмите на кнопку выберите его в обозревателе файловой системы (при этом имеется возможность создать новый каталог).

При переименовании файла расширение имени файла меняется на текст, заданный маской переименования (по умолчанию маска имеет вид **#??**, т. е. первый символ расширения меняется на **#**, остальные не изменяются). Вы можете отредактировать маску в поле ввода Переименовать файлы в.

Перейдите на вкладку **Интерфейс**, чтобы настроить интерфейс программы (рисунок 6).

Основные настройки программы

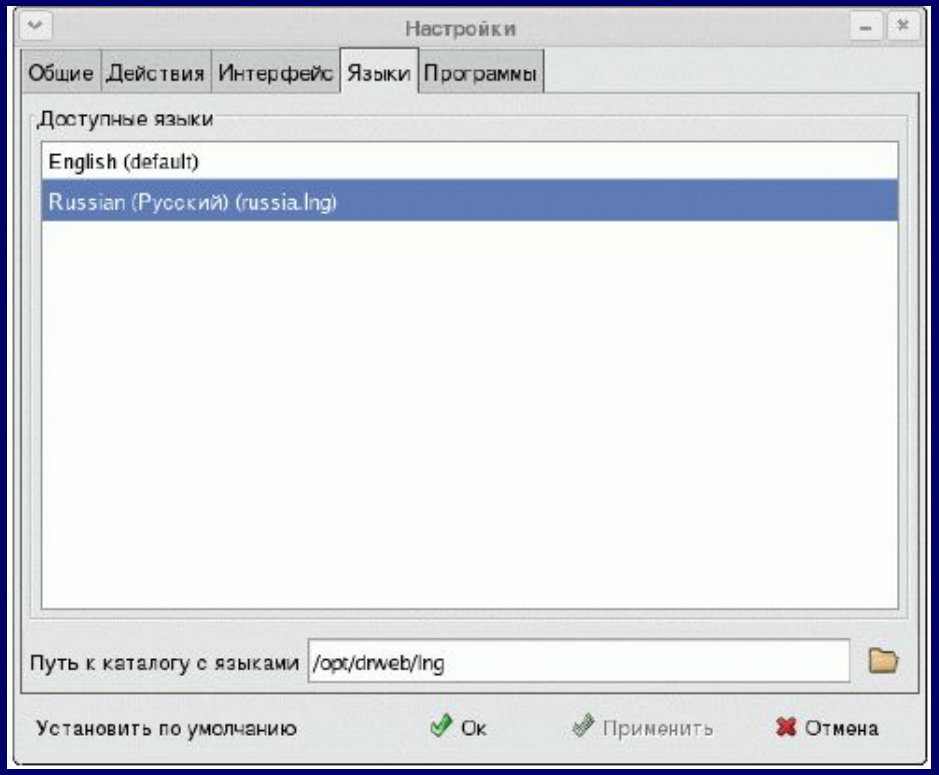


Рисунок 7. - Настройка языка

Перейдите на вкладку **Языки**, чтобы выбрать язык интерфейса программы (рисунок 7).

Основные настройки программы

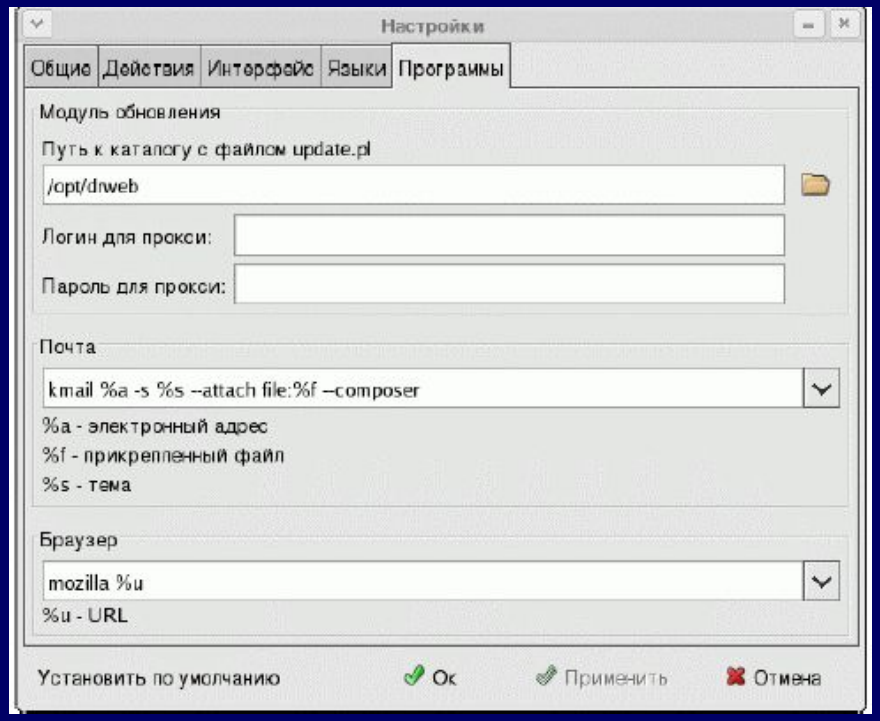


Рисунок 8. - Настройка взаимодействия с программами

Выберите нужный язык в списке **Доступные языки**.

При необходимости отредактируйте путь к файлам языковых ресурсов в поле **Путь к каталогу** с языками или нажмите на кнопку и выберите его в обозревателе файловой системы.

На вкладке **Программы** вы можете настроить параметры взаимодействия с компонентами антивирусного комплекса и другими программами (рисунок 8).

Основные настройки программы

При необходимости отредактируйте в поле **Путь к каталогу с файлом update.pl** путь к каталогу, содержащему **Модуль обновления**, или нажмите на кнопку и выберите его в обозревателе файловой системы.

Если вы используете **прокси** - сервер для получения обновлений, вы можете задавать **логин** и **пароль** на этом сервере в соответствующих полях ввода.

В поле **Почта** выберите и при необходимости отредактируйте командную строку для запуска почтовой программы в пакетном режиме.

В поле **Браузер** выберите и при необходимости отредактируйте командную строку для запуска веб - браузера.

По окончании редактирования настроек нажмите на кнопку **OK**, чтобы сохранить внесенные изменения.

Расширенные настройки

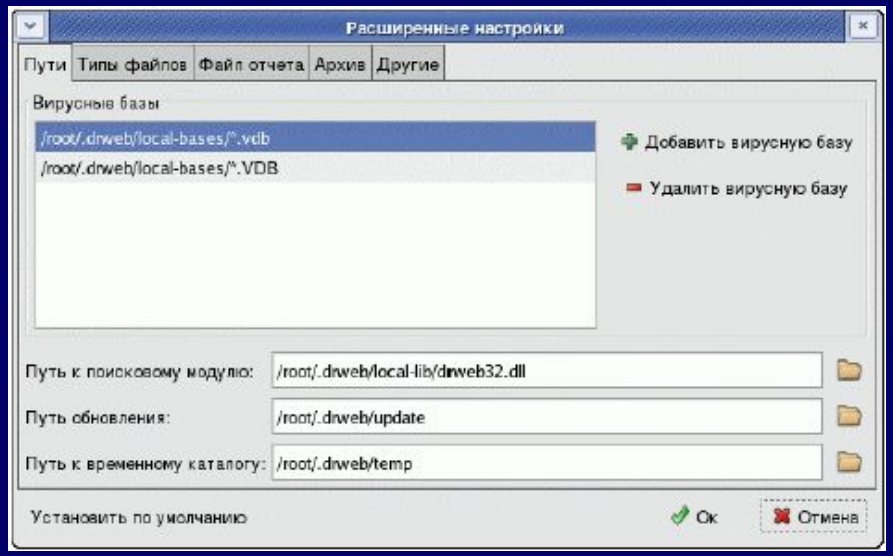


Рисунок 9. - Настройка путей

Опытные пользователи могут выбрать в качестве режима проверки **Расширенный режим**.

При этом делается доступной кнопка **Расширенные настройки** (и одноименный пункт меню **Настройки**).

Нажмите на кнопку **Расширенные настройки**. Откроется окно расширенных настроек на вкладке **Пути** (рисунок 9).

Расширенные настройки

В списке **Вирусные базы** перечислены каталоги и файлы, содержащие базы вирусных сигнатур. По умолчанию, базы размещаются в каталоге, заданном при установке программе в конфигурационном файле. В этот же каталог помещает дополнительные базы **Модуль обновления**. Однако в случае подключения дополнительных баз вручную необходимо указать их в данном списке. Также в тех случаях, когда файлы баз имеют нестандартное расширение (даже если они размещаются в стандартном каталоге), они должны быть включены в данный список.

Для того чтобы добавить элемент в список вирусных баз, нажмите на кнопку **Добавить вирусную базу**. Откроется окно добавления базы рисунок 10).

Расширенные настройки

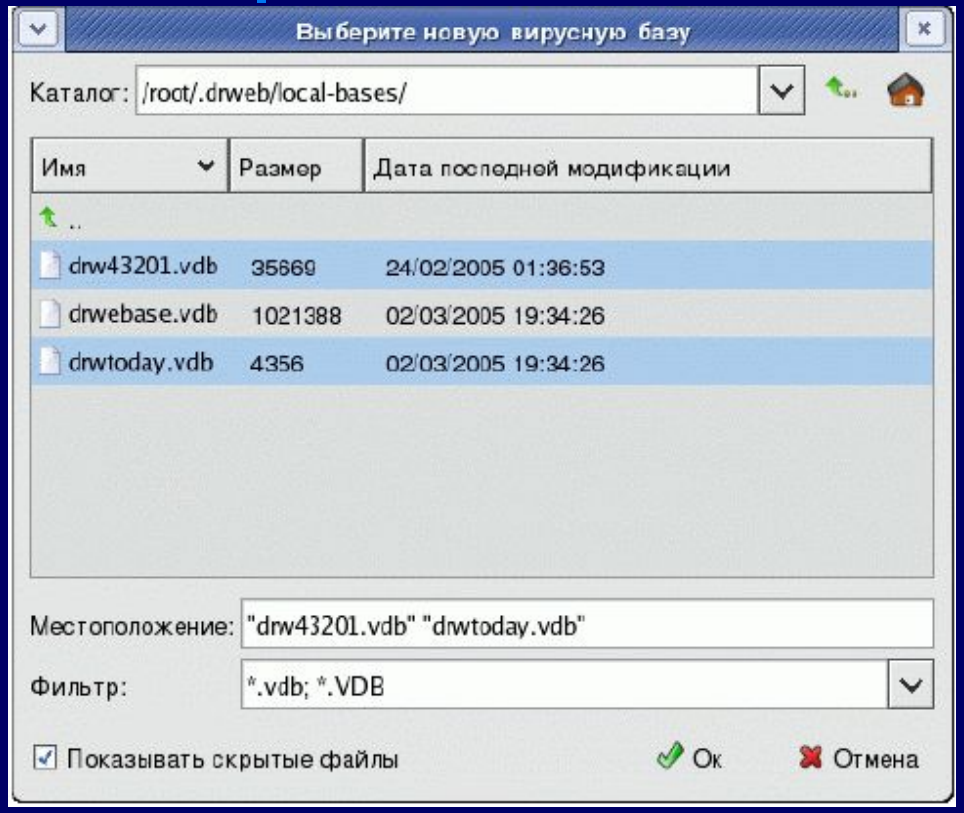


Рисунок 10. - Добавление вирусной базы

Чтобы выделить нужные файлы или каталоги, удерживая клавишу **Ctrl**, щелкните мышью по соответствующим объектам (если нужно выделить только один объект, дважды щелкните по нему). По окончанию выбора нужных объектов нажмите на кнопку **OK**.

По умолчанию, в окне обозревателя отображаются все файлы, в том числе скрытые. Чтобы отменить отображение скрытых файлов, удалите флажок **Показывать скрытые файлы**.

Расширенные настройки

В раскрывающемся списке **Фильтр** содержится маска, которой должны соответствовать имена файлов подключаемых баз.
По умолчанию предполагается список из двух элементов *.**vdb** ;
*.**VDB** (т. е. только файлы с расширениями **vdb** или **VDB**). Вы также можете выбрать в списке значение * (т. е. любые файлы).

Для того чтобы удалить элемент из списка, выберите его в списке и нажмите на кнопку **Удалить вирусную базу**.

При необходимости отредактируйте в соответствующих полях пути к антивирусному движку, каталогу обновления и каталогу временных файлов.

Перейдите на вкладку **Типы файлов**, чтобы настроить ограничение множества проверяемых файлов (рисунок 11).

Расширенные настройки

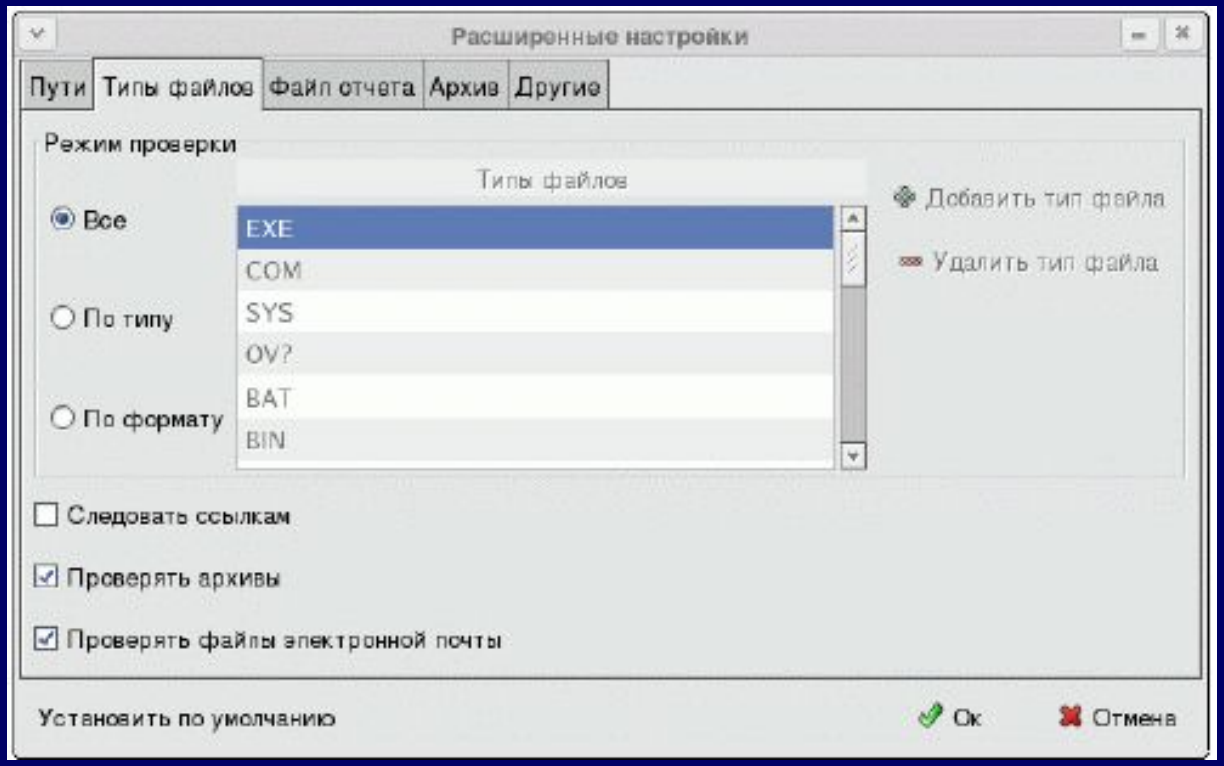


Рисунок 11. - Выбор типов сканируемых файлов

Расширенные настройки

В группе кнопок выбора Режим проверки выберите способ отбора файлов:

• **Все** — при этом проверяются все файлы, независимо от имени и внутренней структуры. Режим по умолчанию при выборе режима Полная проверка

• **По формату** — проверяются (независимо от имени) файлы, которые по внутренней структуре могут быть носителями вирусов. Режим по умолчанию при вы режима Быстрая проверка

• **По типу** — проверяются только файлы с заданными в списке **Типы файлов** расширениями. По умолчанию список содержит расширения исполняемых и макросодержащих файлов. Для добавления расширения в список, нажмите на кнопку **Добавить тип файла** и введите в открывшемся окне добавляемое расширение.

Для удаления расширения из списка пометьте его и нажмите на кнопку **Удалить тип файла.**

Расширенные настройки

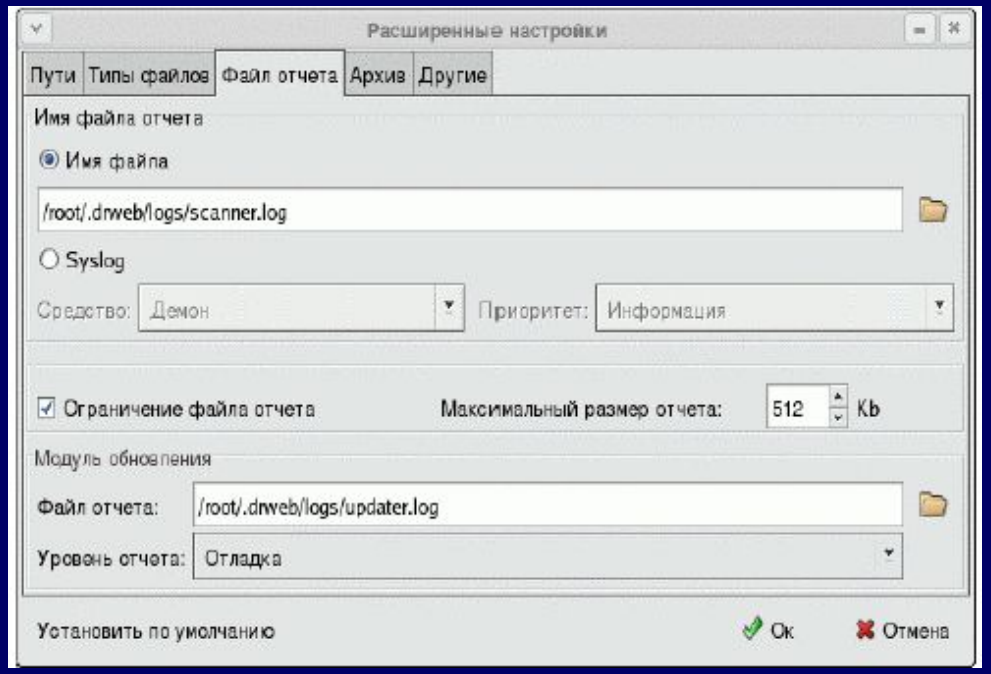
Вкладка **Проверять архивы** предназначена для того, чтобы сканер распаковывал файловые архивы и проверял входящие в них файлы (при установленном режиме **По формату** — если они имеют соответствующий формат, в режиме **По типу** в список типов должны входить и расширение архива, и расширение извлекаемого файла).

Установите флажок **Проверять файлы электронной почты**, чтобы сканер проверял файлы электронной почты, в том числе прикрепленные вложения (при этом автоматически включается проверка архивов).

В режиме **Полная проверка** перечисленные режимы включены, в режиме **Быстрая проверка** — нет.

Перейдите на вкладку **Файл отчета**, чтобы настроить ведение отчета (рисунок 12).

Расширенные настройки



Установите флажок **Следовать ссылкам**, чтобы сканер проверял файлы, символические ссылки на которые число проверяемых.

Рисунок 12. - Настройка ведения отчета

Расширенные настройки

В группе кнопок выбора Имя файла отчета выберите способ протоколирования — в файл (вариант **Имя файла**) или с использованием системной службы **Syslog**. В первом случае можно отредактировать или выбрать путь к файлу отчета, во втором — выбрать средство протоколирования и приоритет режима чтения и задать уровень подробности его ведения.

Перейдите на вкладку **Архив**, чтобы настроить ограничения, налагаемые на действия с архивами по соображениям безопасности (рисунок 13).

Рекомендуется сохранить установленные по умолчанию.

Ограничение файла отчета и значение в поле Максимальный размер файла отчета (по умолчанию **512 Кб**).

В поле **Модуль** обновления можно отредактировать или выбрать имя файла отчета **Модуля** обновления

Расширенные настройки

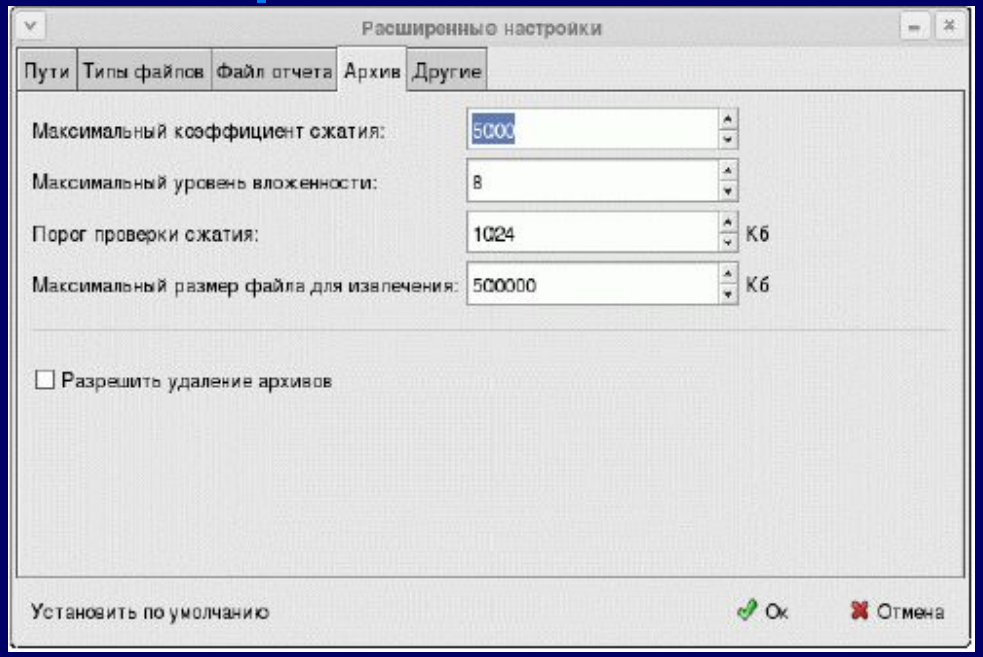


Рисунок 13. - Настройка работы с архивами

По умолчанию, флажок **Разрешить удаление архивов** не установлен.

При этом на вкладке **Действия окна Настройки для всех типов архивов** недоступен вариант **Удалить**

Если вы хотите разрешить выбирать для архивов эту реакцию, установите данный флажок.

Остальные параметры на данной вкладке направлены на защиту сканера от атак "**почтовыми бомбами**". Параметры задают характеристики архивов, при превышении которых их проверка прекращается во избежание исчерпания ресурсов.

Расширенные настройки

При выборе реакции **Удалить сканер** может автоматически удалить архив, содержащий многие тысячи файлов, из-за обнаружения одного инфицированного или даже подозрительного файла. Настоятельно не рекомендуется разрешать удаление архивов.

При необходимости изменить заданные по умолчанию значения отредактируйте значения в следующих полях:

- **Максимальный коэффициент сжатия** (по умолчанию 5000)
- **Максимальный уровень вложенности** (по умолчанию 8)
- **Порог проверки сжатия** (по умолчанию 1024 Кб, архивы меньшего размера проверяются независимо от коэффициента сжатия)
- **Максимальный размер файла для извлечения** (по умолчанию 500000 Кб, при обнаружении файлов большего размера извлечение прекращается) можете задать приоритет. На вкладке (рисунок 14) **Другие** сканирования, **таймаут обновления** и ряд других параметров.

Расширенные настройки

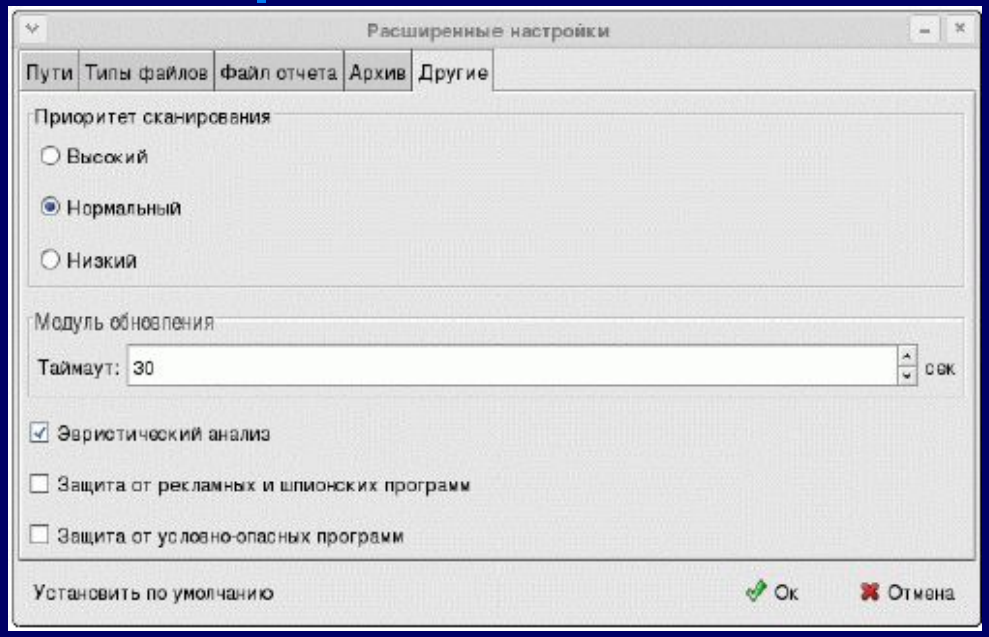


Рисунок 14. - Вкладка Другие

Для того чтобы включить **режим эвристической проверки** (поиск неизвестных вирусов, режим может вызывать ложные срабатывания, обнаруженные файлы имеют статус "**подозрительных**"), установите флажок **Эвристический анализ**. В режиме **Быстрая проверка** данный режим выключен, в режиме **Полная проверка** – включен.

Сканирование под управлением Модуля графического интерфейса

Модуль графического интерфейса может быть использован не только для облегчения настройки параметров сканера, но и для управления самим процессом сканирования.

В главном окне на вкладке **Проверка** (см. выше рисунок 1) вы можете выбрать объекты, подлежащие сканированию.

По умолчанию, список содержит перечень каталогов верхнего уровня и **Домашний каталог** текущего пользователя. При этом для **Домашнего каталога** установлен флажок, предписывающий проверять его, для остальных объектов флажок не установлен.

Для того чтобы включить сканирование для каких-либо объектов из списка, установите флажок возле их наименований.

Вы также можете отредактировать список объектов. Для того чтобы добавить в список объект, нажмите кнопку **Добавить объект**.

Сканирование под управлением Модуля графического интерфейса

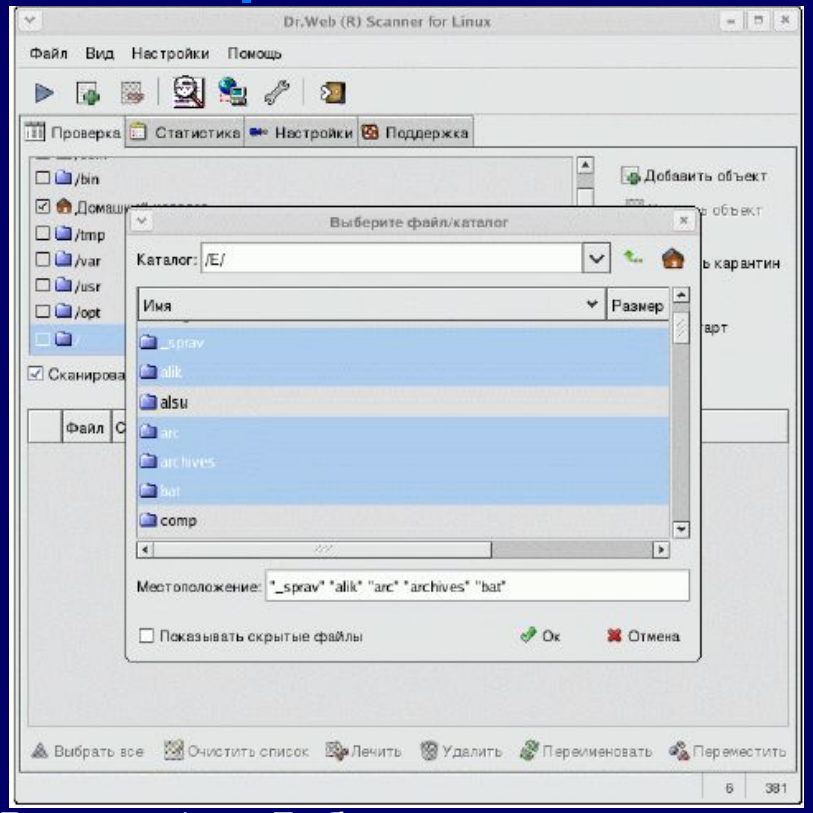


Рисунок 15. - Добавление элемента в список сканирования

Откроется окно выбора объектов сканирования (рисунок 15).

Чтобы выделить нужные файлы или каталоги, удерживая клавишу **Ctrl**, щелкните мышью по соответствующим объектам (если нужно выделить только один объект, дважды щелкните по нему). По окончании выбора нужных объектов нажмите на кнопку **OK**.

Сканирование под управлением Модуля графического интерфейса

По умолчанию, в окне обозревателя не отображаются скрытые файлы. Чтобы отображать также скрыты файлы, установите флажок **Показывать скрытые файлы**.

Для того чтобы удалить объект, выберите его в списке и нажмите на кнопку **Удалить объект** (можно удалять только ранее добавленные вами объекты).

По окончании формирования списка сканируемых объектов нажмите на кнопку **Старт**.

Результаты сканирования отображаются в табличной форме в поле отчета в нижней части главного окна. Если в настройках действий для обнаруженного объекта было задано действие, отличное от информирования, в столбце **Действие** отображается результат предпринятых действий.

Список обнаруженных объектов иерархический; если обнаружен вирус в архиве, инфицированный архив представляется как узел иерархического списка, который можно развернуть или свернуть

Сканирование под управлением Модуля графического интерфейса

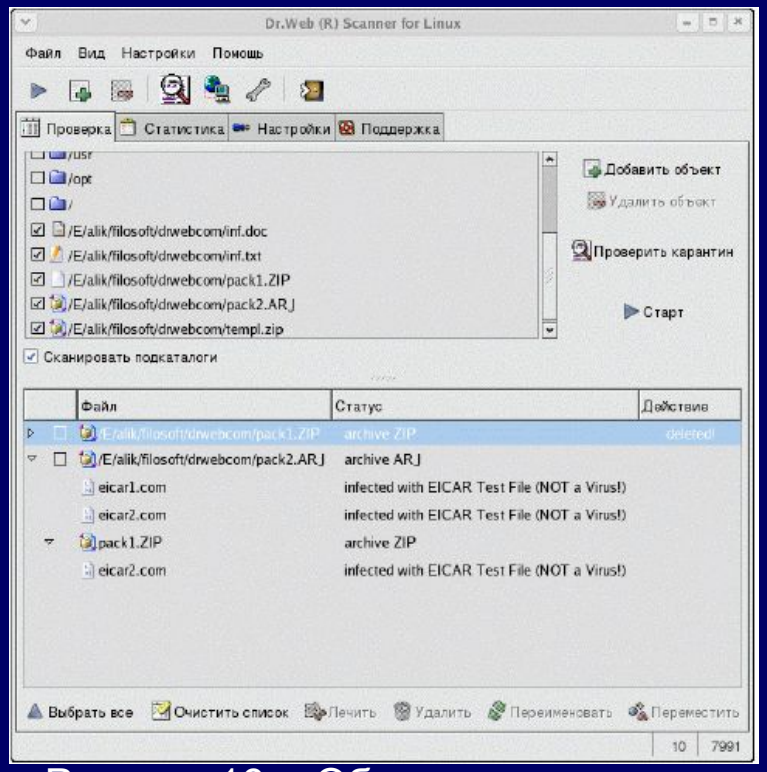


Рисунок 16. - Обнаружен вирус в многоуровневом архиве

Лечить, **Переименовать** или **Переместить** соответственно. При выборе варианта **Лечить** откроется дополнительное окно с запросом о действии в случае неуспешного лечения (рисунок 17).

Для того чтобы вручную произвести необходимые действия с обнаруженным объектом, установите против него флажок (или нажмите на кнопку **Выбрать все**, чтобы пометить все обнаруженные объекты) и нажмите на кнопку **Удалить**.

Сканирование под управлением Модуля графического интерфейса

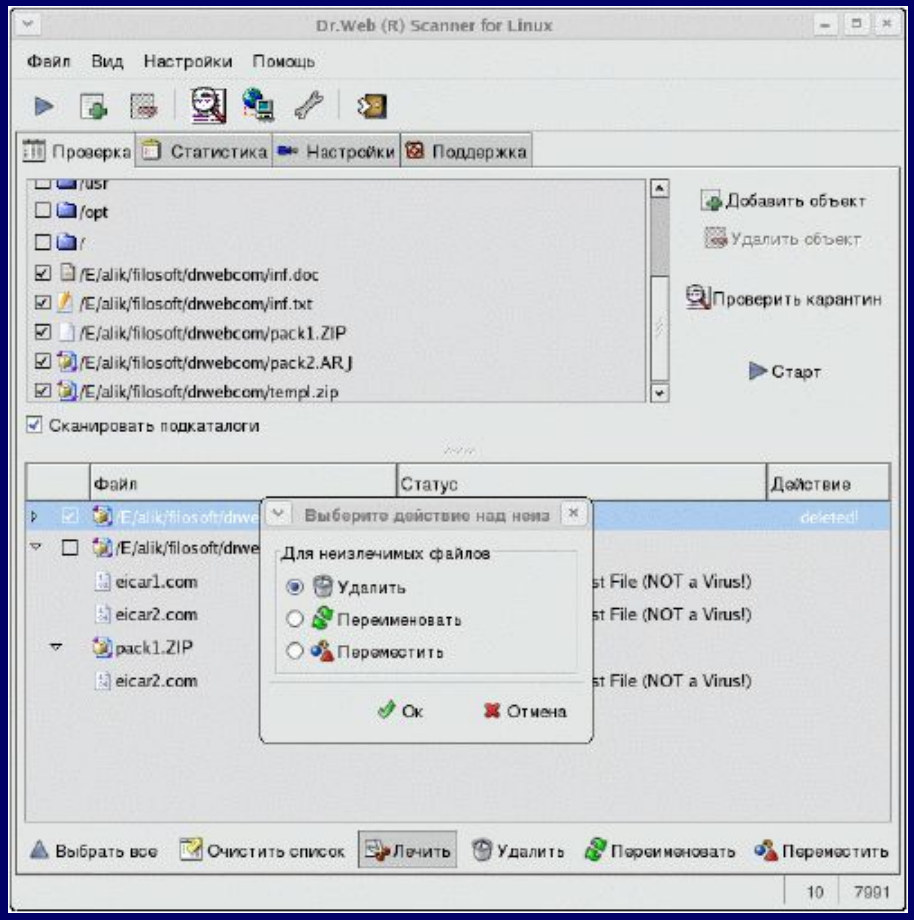


Рисунок 17. - Работа с инфицированными объектами

Сканирование под управлением Модуля графического интерфейса

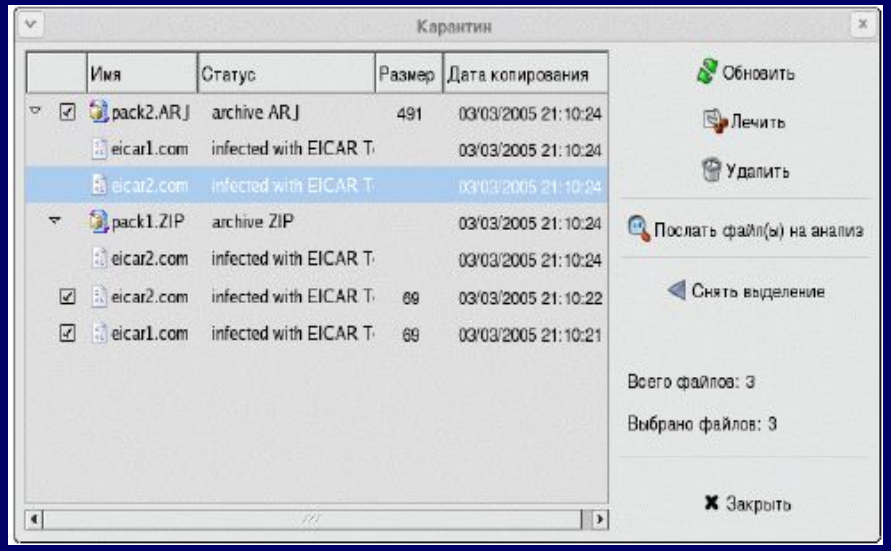


Рисунок 18. - Карантин

Вы можете просматривать файлы, помещенные в карантин, для этого нажмите на кнопку **Проверить карантин**. Откроется окно (рисунок 18):

Сканирование под управлением Модуля графического интерфейса

Установите флажок против файлов, с которыми вы хотите предпринять необходимые действия (или нажмите на кнопку **Выбрать все**). Нажмите на кнопку **Лечить**, чтобы попытаться вылечить файл. Нажмите на кнопку **Удалить**, чтобы удалить файл. Нажмите на кнопку **Послать файл(ы)** на анализ, чтобы послать файлы для проверки (с использованием) в службу поддержки установленного почтового клиента **ООО "Доктор Веб"**.

Если файл не удастся вылечить, он сохраняется в карантине. Вы можете удалить его или послать на анализ, как описано выше.

Статистика работы сканера

Для того чтобы ознакомиться со статистикой работы сканера (в зависимости от настроек программы за текущий сеанс или с момента очередной очистки статистики), перейдите на вкладку **Статистика** (рисунок 19).

Для того чтобы очистить статистику (установить все счетчики в нулевое значение), нажмите на кнопку в правой части окна.

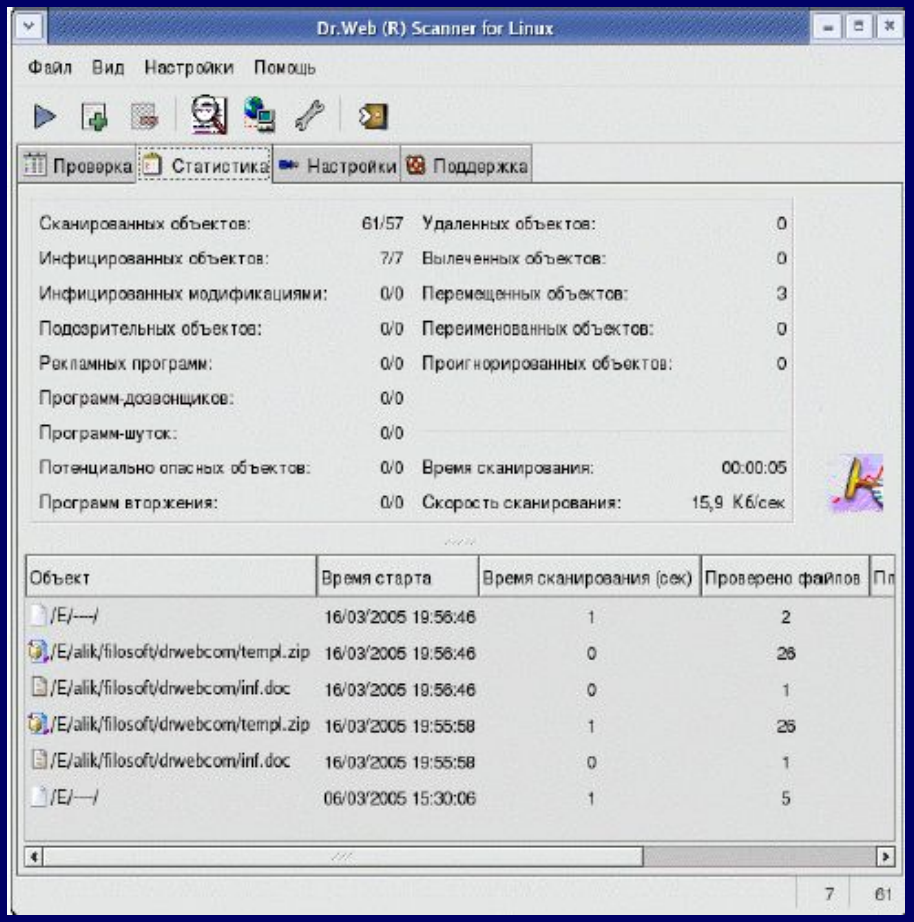


Рисунок 19. - Статистика

Сведения о программе обновлении и техническая поддержка

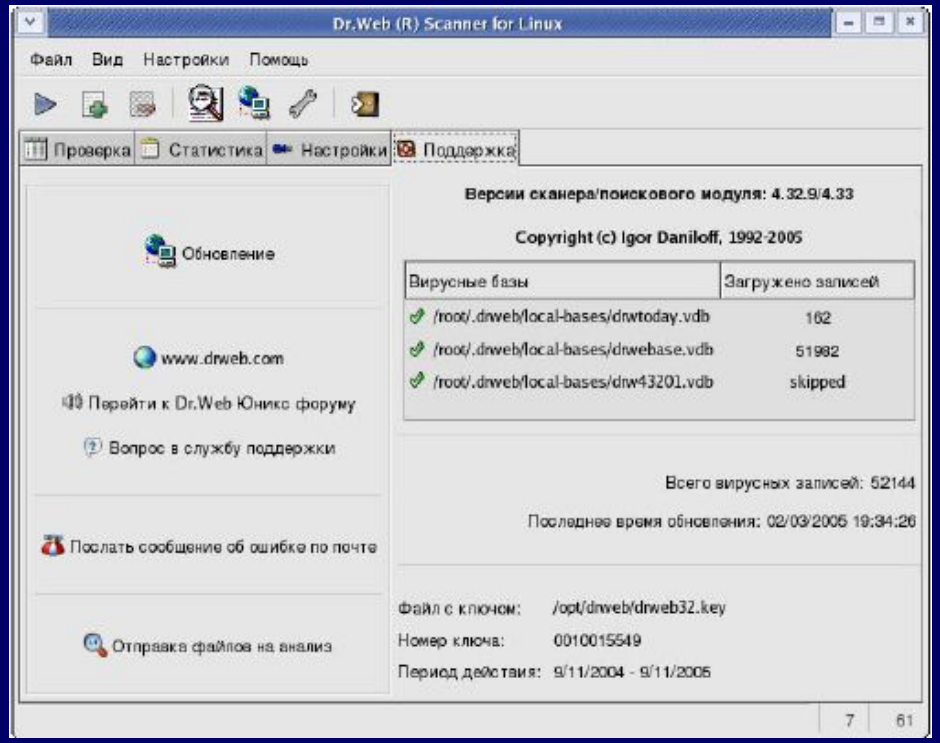


Рисунок 20. - Вкладка **Поддержка**

Использование Модуля графического интерфейса облегчает доступ к технической поддержке. Для того чтобы воспользоваться возможностями, перейдите на вкладку **Поддержка** (рисунок 20).

Сведения о программе обновлении и техническая поддержка

Для того чтобы запустить **Модуль обновления**, нажмите на кнопку **Обновление** в левой части окна.

Для того чтобы загрузить в окно веб - браузера сайт **ООО "Доктор Веб"**, форум **Dr.Web Юникс**, направить (с помощью **HTML**-формы) вопрос в службу поддержки или послать сообщение по почте, выберите соответствующую ссылку в левой части окна.

Для того чтобы послать файлы, предположительно инфицированные неизвестными вирусами, на анализ в **ООО "Доктор Веб"**, нажмите на кнопку

Отправка файлов на анализ. Откроется окно выбора файлов.

Сведения о программе обновлении и техническая поддержка

В правой части окна содержится информация о версии программы, загруженных базах, дате последнего обновления информация о номере ключа. После сеанса обновления эта корректируется.

Если при попытке перейти о ссылке на один из выше указанных 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.

Практическая часть

Выполните настройку антивируса.

Результат: Выполнив работу, вы научитесь использовать антивирусное программное обеспечение «ДОКТОР ВЕБ» на рабочей станции.