Dr.WEB®

Антивирус
для Linux

Защити созданное

Руководство пользователя

Антивирус Dr.Web® для Linux
Версия 9.0.0
Руководство пользователя
11.04.2014

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

Условные обозначения и сокращения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов **Dr.Web** или их компонентов.
Зеленое и подчеркнутое начертание	Ссылки на страницы руководства и веб-сайты.
`Моноширинный шрифт`	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
Курсив	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Введение

Благодарим вас за приобретение программного продукта **Антивирус Dr.Web для Linux**. Он позволит вам обеспечить надежную защиту вашего компьютера от компьютерных угроз всех возможных типов, используя наиболее современные технологии обнаружения и обезвреживания угроз.

Данное руководство предназначено для помощи пользователям компьютеров, работающих под управлением операционных систем семейства **GNU/Linux** (далее в документе будет использовано обозначение **Linux**), в установке и использовании продукта **Антивирус Dr.Web для Linux** версии 9.0.0.

Если у вас уже установлен **Антивирус Dr.Web для Linux** версии 6.0.2, и вы желаете обновить его до версии 9.0.0, выполните процедуру перехода на новую версию.

О продукте

Антивирус Dr.Web для Linux создан для защиты от вирусов и всех прочих видов вредоносного программного обеспечения компьютеров, работающих под управлением ОС семейства **Linux.**

Основные компоненты программы (антивирусное ядро **Dr.Web Virus-Finding Engine** и вирусные базы **Dr.Web**) являются не только крайне эффективными и нетребовательными к системным ресурсам, но и кросс-платформенными, что позволяет специалистам компании **«Доктор Веб»** создавать превосходные антивирусные решения для различных операционных систем.

Компоненты **Антивируса Dr.Web для Linux** постоянно обновляются, а вирусные базы **Dr.Web** регулярно дополняются новыми сигнатурами угроз, что обеспечивает актуальный уровень защищенности компьютера, программ и данных пользователей. Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре.

Решаемые задачи (функции)

Основные функции продукта **Антивирус Dr.Web для Linux:**

1. **Поиск и обезвреживание** как непосредственно вредоносных программ всех возможных типов (различные вирусы, включая вирусы, инфицирующие почтовые ящики и загрузочные записи дисков, троянские программы, почтовые черви и т.п.), так и нежелательных программ (рекламные, шуточные, программы автоматического дозвона).

   Для обнаружения вредоносных и нежелательных программ используются:

   - Сигнатурный анализ. Метод проверки, позволяющий обнаружить уже известные угрозы, информация о которых содержится в вирусных базах;

- Эвристический анализ. Набор методов проверки, позволяющих обнаруживать угрозы, которые еще неизвестны.

Обратите внимание, что, как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки двух типов: пропускать неизвестные угрозы или допускать ложные срабатывания для программного обеспечения, не являющегося вредоносным. Поскольку диагноз эвристического анализатора может оказаться ложным, то объекты, содержащие обнаруженные им угрозы, получают специальный статус «подозрительные». Рекомендуется помещать такие файлы в **Карантин**, а также передавать на анализ в **Вирусную лабораторию компании «Доктор Веб»**. Подробнее об методах обезвреживание см. в Приложении Б Устранение компьютерных угроз.

Проверка объектов файловой системы на предмет обнаружения угроз может осуществляться как по запросу пользователя, так и автоматически, в соответствии с заданным расписанием. Имеется возможность выполнять как полную проверку всех доступных пользователю объектов файловой системы (включая не только файлы, но и загрузочные записи), так и только перечень объектов, выбранных пользователем. Кроме того, доступна возможность отдельной проверки исполняемых файлов, из которых запущены процессы, активные в системе в данный момент. При обнаружении угрозы в этом случае выполняется не только обезвреживание вредоносного файла, но и принудительное завершение работы активного процесса.

2. **Мониторинг обращений к файлам.** Отслеживаются обращения к файлам с данными и попытки запуска исполняемых файлов. Это позволяет обнаруживать и нейтрализовывать вредоносные программы непосредственно при попытках инфицирования ими компьютера.
3. **Надежная изоляция инфицированных или подозрительных объектов** в специальном хранилище – **Карантине**, чтобы они не могли нанести ущерба системе. При перемещении объектов в **Карантин** они специальным образом переименовываются, и могут быть восстановлены в исходное место (в случае необходимости) только по команде

пользователя.

4. **Автоматическое обновление** содержимого вирусных баз **Dr.Web** и антивирусного ядра для поддержания высокого уровня надежности защиты от вредоносных программ.
5. **Обеспечение работы под управлением сервера централизованной защиты** (такого, как **Dr.Web Enterprise Server** или в рамках сервиса **Dr.Web AV-Desk**) для применения на защищаемом компьютере единых политик безопасности, принятых в некоторой сети, в состав которой он входит. Это может быть как сеть некоторого предприятия (корпоративная сеть) или частная сеть VPN, так и сеть, организованная провайдером каких-либо услуг, например, доступа к сети Интернет.

Системные требования

Использование **Антивируса Dr.Web для Linux** возможно на компьютере, удовлетворяющем следующим требованиям:

Компонент	Требование
Платформа	Поддерживаются 32-битная **(IA-32, x86)** и 64-битная **(x86-64, x64, amd64)** платформы **Intel.**
Место на жестком диске	Не менее 400 Мбайт свободного дискового пространства на томе, на котором размещаются каталоги **Антивируса**.
Операционная система	**Linux** для платформ **Intel x86/amd64** на основе ядра с версией не ниже 2.6.37 и использующая библиотеку **glibc** версии 2.13 и выше. Перечень протестированных дистрибутивов **Linux** перечислен ниже. В случае использования 64-битной версии операционной системы, должна быть обязательно включена поддержка исполнения 32-битных приложений (для этого, возможно, потребуются дополнительные библиотеки, см.

Компонент	Требование
	ниже).
Прочее	Наличие сетевого подключения: Подключение к сети Интернет для обновления вирусных баз и компонентов **Антивируса Dr. Web для Linux**. При работе в режиме централизованной защиты достаточно только подключения к используемому серверу в рамках локальной сети, доступ в Интернет не требуется.

Работоспособность программного продукта протестирована на следующих дистрибутивах **Linux** (для 32- и 64-битной платформ):

Название дистрибутива Linux	Версии	Требуемые дополнительные библиотеки для 64-битной версии ОС
Debian	7	`libc6-i386`
Fedora	20	`glibc.i686`
Mint	16	`libc6-i386`
Ubuntu	12.04 LTS, 13.04, 13.10	`libc6-i386`

Прочие дистрибутивы **Linux,** соответствующие описанным требованиям, не проходили тестирование на совместимость с **Антивирусом**, но могут быть совместимы. При возникновении проблем с совместимостью с вашим дистрибутивом, обратитесь в техническую поддержку: http://support.drweb.com/request/.

Дополнительные пакеты

- Для работы **Антивируса** в графическом режиме, а также для запуска программ установки и удаления продукта для графического режима требуется наличие графической

подсистемы **X Window System** и любого менеджера окон.

- Для работы в графическом режиме программ установки и удаления продукта, рассчитанных на режим командной строки, необходимо наличие в системе любого эмулятора терминала (например, **xterm** или **xvt**).
- Также в операционной системе должны быть установлены следующие дополнительные пакеты и утилиты: **unzip**, **crond**. Для повышения привилегий достаточно иметь **su** или **sudo**, а также установленный **xterm**. Вместо этого рекомендуется установить (если ещё не установлена) одну из утилит повышения прав из графики: **gksu**, **gksudo**, **kdesu**, **kdesudo**, **beesu**, **beesudo**.

Для удобной работы с **Антивирусом** из командной строки рекомендуется включить автодополнение команд в используемой командной оболочке, если оно не включено.

В случае возникновения проблем с установкой требуемых дополнительных пакетов и компонентов обратитесь к справочным руководствам используемого вами дистрибутива операционной системы.

Структура программного продукта

Антивирус Dr.Web для Linux состоит из следующих компонентов:

Компонент	Описание
Сканер	Компонент, выполняющий по требованию пользователя или по заданному расписанию проверку объектов файловой системы (файлы, каталоги и загрузочные записи) на наличие в них угроз. Пользователь имеет возможность запускать проверку как из графического режима, так и из командной строки.

Компонент	Описание
Монитор файловой системы SpIDer Guard	Компонент, работающий в резидентном режиме и отслеживающий операции с файлами (такие как создание, открытие, закрытие и запуск файла). Посылает **Сканеру** запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ.
Антивирусное ядро	Центральный компонент антивирусной защиты. Используется **Сканером** для поиска и распознавания вирусов и вредоносных программ, а также анализа подозрительного поведения.
Вирусные базы	Автоматически обновляемая база данных, используемая антивирусным ядром, и содержащая информацию для распознавания и лечения известных угроз.
Модуль обновления	Компонент, отвечающий за автоматическую загрузку с серверов **ВСО Dr.Web** обновлений вирусных баз и антивирусного ядра (как автоматически, по расписанию, так и непосредственно по команде пользователя)
Карантин	Компонент, организующий специальное хранилище, используемое **Антивирусом** для надежной изоляции файлов, содержащих угрозы, чтобы они не могли нанести вред системе.
Менеджер лицензий	Компонент, упрощающий работу с лицензиями в графическом режиме. Позволяет активировать лицензию или демонстрационный период, просмотреть данные о текущей лицензии, выполнить ее продление, а также установить и удалить лицензионный ключевой файл.

Кроме перечисленных в таблице, в состав **Антивируса Dr.Web для Linux** входят также дополнительные сервисные компоненты, работающие в фоновом режиме и не требующие вмешательства пользователя.

Каталоги Карантина

Карантин организует систему каталогов, предназначенных для надежной изоляции файлов, содержащих выявленные угрозы, которые в данный момент не могут быть обезврежены по каким-либо причинам. Например, обнаруженная угроза может быть неизлечимой, потому что еще неизвестна **Антивирусу** (например, она была обнаружена эвристическим анализатором, а в вирусных базах ее сигнатура, а следовательно – и метод лечения, отсутствует), или при попытке ее лечения возникают ошибки. Кроме того, файл может быть перемещен в **Карантин** непосредственно по желанию пользователя, в случае если он выбрал соответствующее действие в списке обнаруженных угроз или указал его как реакцию **Сканера** или монитора файловой системы **SpIDer Guard** на угрозы определенного типа.

Когда файл, содержащий угрозу, перемещается в **Карантин**, он специальным образом переименовывается, чтобы предотвратить возможность доступа к нему со стороны пользователей и программ, минуя инструменты работы с **Карантином**, реализованные в **Антивирусе Dr.Web для Linux**.

Каталоги **Карантина** размещаются:

- **в домашнем каталоге пользователя** (если на данном компьютере имеется несколько учетных записей разных пользователей, то в домашнем каталоге каждого из этих пользователей может быть создан свой собственный каталог **Карантина**).
- **в корневом каталоге** каждого логического тома, смонтированного в файловую систему операционной системы.

Каталоги **Карантина Dr.Web** всегда имеют имя **`.com.drweb.quarantine`** и создаются по мере необходимости, в тот момент, когда к какой-либо угрозе применяется действие «Переместить в Карантин» («Изолировать»), т.е. до тех пор, пока угроз не обнаружено, каталоги **Карантина** не создаются. При этом всегда создается только тот каталог **Карантина**, который требуется для

изоляции файла. Для определения, в какой из каталогов требуется изолировать файл, используется имя владельца файла. Если при движении к корню файловой системы / от каталога, содержащего файл, достигается домашний каталог владельца, файл изолируется в каталог **Карантина**, находящийся в нем. В противном случае файл будет изолирован в каталог **Карантина**, созданный в корне тома, содержащего файл (корневой каталог тома необязательно совпадет с корнем файловой системы). Таким образом, любой инфицированный файл, помещаемый в хранилище **Карантина**, всегда остается на том томе, на котором он был обнаружен. Это обеспечивает корректную работу **Карантина** при наличии в системе съемных накопителей и других томов, которые могут монтироваться в файловую систему операционной системы периодически и в различные точки.

Пользователь может управлять содержимым **Карантина** как в графическом режиме работы, так и из командной строки. При этом всегда обрабатывается консолидированный **Карантин,** объединяющий в себе все каталоги с изолированными объектами, доступные в данный момент. С точки зрения пользователя, просматривающего содержимое консолидированного **Карантина**, каталог, располагающийся в его домашнем каталоге, называется Пользовательским Карантином, а все остальные каталоги считаются Системным Карантином.

Работа с **Карантином** возможна даже тогда, когда отсутствует активная лицензия, но в этом случае становится невозможным лечение изолированных объектов.

Полномочия для работы с файлами

При сканировании объектов файловой системы и нейтрализации угроз **Антивирус Dr.Web для Linux** (точнее, пользователь, от имени которого он запущен) должен обладать следующими полномочиями:

Действие	Требуемые полономочия
Вывод всех обнаруженных угроз	Без ограничений. Специальных полномочий не требуется.
Вывод содержимого архива (Отображение только элементов, которые содержат ошибку или угрозу)	Без ограничений. Специальных полномочий не требуется.
Перемещение в **Карантин**	Без ограничений. Пользователь может отправлять в **Карантин** все инфицированные файлы, независимо от наличия у него прав на чтение и запись для перемещаемого файла.
Удаление угроз	Пользователь должен иметь права на запись в удаляемый файл.
Лечение файлов	Без ограничений. После выполнения лечения остается вылеченный файл с исходными правами доступа и владельцем. Обратите внимание, что файл может быть даже удален, если удаление является методом лечения обнаруженной в нем угрозы.
Восстановление файла из **Карантина**	Пользователь должен иметь разрешение на чтение восстанавливаемого файла и иметь разрешение выполнять запись в каталог восстановления.
Удаление файла из **Карантина**	Пользователь должен иметь разрешение на запись в исходный файл, который был перемещен в **Карантин**.

Для временного повышения прав **Антивируса Dr.Web для Linux,** запущенного в графическом режиме, вы можете воспользоваться соответствующей кнопкой, имеющейся на окне **Антивируса** (она доступна и отображается только в тех случаях,

когда повышение прав может потребоваться для успешного выполнения некоторой операции). Для запуска **Антивируса** в графическом режиме или утилиты управления из командной строки с правами суперпользователя вы можете воспользоваться командой смены пользователя **su** или командой выполнения от имени другого пользователя **sudo**.

Обратите внимание, что **Сканер** не может работать с файлами, размер которых больше 4 Гбайт (при попытке проверки таких файлов будет выдаваться ошибка «Файл слишком большой»).

Режимы работы Антивируса

Антивирус Dr.Web для Linux может работать как в одиночном режиме, так и в составе корпоративной или частной антивирусной сети, управляемой каким-либо сервером централизованной защиты. Такой режим работы называется режимом централизованной защиты. Использование этого режима не требует установки дополнительного программного обеспечения, переустановки или удаления **Антивируса Dr.Web для Linux**.

- **В одиночном режиме (standalone mode)** защищаемый компьютер не включен в антивирусную сеть и управляется локально. В этом режиме конфигурационный и лицензионный ключевой файлы находятся на локальных дисках, а **Антивирус Dr.Web для Linux** полностью управляется с защищаемого компьютера. Обновления вирусных баз получаются с серверов **ВСО Dr.Web**.
- **В режиме централизованной защиты (enterprise mode)** защитой компьютера управляет сервер централизованной защиты. В этом режиме некоторые функции и настройки **Антивируса Dr.Web для Linux** могут быть изменены или заблокированы в соответствии с общей (корпоративной) стратегией антивирусной защиты, принятой в антивирусной сети. В этом режиме на компьютере используется особый лицензионный ключевой файл, полученный с выбранного сервера централизованной защиты, к которому подключен **Антивирус**. Лицензионный или демонстрационный ключевой

файл пользователя, если он имеется на локальном компьютере, не используется. На сервер централизованной защиты отсылается статистика работы **Антивируса**, включая статистику вирусных инцидентов. Обновление вирусных баз также выполняется с сервера централизованной защиты.

- **В мобильном режиме (mobile mode)** **Антивирус Dr.Web для Linux** получает обновления вирусных баз с серверов **ВСО Dr.Web**, но использует локально хранящиеся настройки и особый лицензионный ключевой файл, полученные от сервера централизованной защиты.

В случае работы **Антивируса** под управлением сервера централизованной защиты (в том числе и в мобильном режиме) блокируются следующие возможности:

1. Возможность удаления лицензионного ключевого файла в **Менеджере лицензий**;
2. Возможность запуска обновлений вручную и настройки параметров обновления;
3. Возможность настройки параметров проверки объектов файловой системы **Сканером**.

Возможность настройки монитора файловой системы **SpIDer Guard**, а также его включения и выключения при работе **Антивируса** под управлением сервера централизованной защиты зависит от разрешений, заданных на сервере.

Обратите внимание, что если на сервере централизованной защиты включен запрет на запуск проверки файлов пользователем, то страница Проверка окна **Антивируса** будет недоступна. Кроме того, в этом случае **Сканер** не будет выполнять проверки файлов по расписанию, если они настроены.

Принципы централизованной защиты

Решения компании **Dr.Web** по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см.

иллюстрацию ниже).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз *локальными антивирусными компонентами* (в данном случае – **Антивирусом Dr.Web для Linux**), которые обеспечивают антивирусную защиту и поддерживают соединение с сервером централизованной защиты.

Рисунок 1. Логическая структура антивирусной сети.

Обновление и конфигурация локальных компонентов производится через сервер централизованной защиты. Весь поток команд, данных и статистической информации в антивирусной

сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и сервером централизованной защиты может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Все необходимые обновления загружаются на сервер централизованной защиты с серверов **ВСО Dr.Web.**

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется сервером централизованной защиты по указанию администраторов антивирусной сети. Администраторы управляют конфигурацией сервера централизованной защиты и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также, при необходимости, задают настройки работы конкретных локальных антивирусных компонентов.

Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями **Dr.Web**, не поддерживающими режим централизованной защиты (например **Антивирус Dr.Web для Linux** версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Подключение к антивирусной сети

Антивирус Dr.Web для Linux может быть подключен к антивирусной сети следующими способами:

- При активации **Антивируса Dr.Web для Linux** – в **Менеджере лицензий**;
- На вкладке **Режим** страницы настроек окна **Антивируса Dr.Web для Linux**;
- При помощи команды `esconnect` утилиты управления из командной строки **`drweb-ctl`**.

Если **Антивирус Dr.Web для Linux** подключен к антивирусной сети, то имеется возможность перевести его в мобильный режим и вернуть назад в режим централизованной защиты. Для этого необходимо использовать команду `esmobile` утилиты управления из командной строки **`drweb-ctl`**.

Отключение от антивирусной сети

Антивирус Dr.Web для Linux может быть отключен от антивирусной сети следующими способами:

- На вкладке **Режим** страницы настроек окна **Антивируса Dr. Web для Linux**;
- При помощи команды `esdisconnect` утилиты управления из командной строки **`drweb-ctl`**.

Проверка работоспособности Антивируса

Имеется стандартный тест, позволяющий проверить работоспособность антивирусных программ, использующих сигнатурные методы обнаружения угроз. Для этого применяется специальный тест `EICAR` (European Institute for Computer Anti-Virus Research), разработанный одноименной организацией. Этот тест разработан для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса.

Программа, используемая для теста `EICAR`, не является вредоносной, но специально определяется большинством антивирусных программ как вирус. Антивирусные продукты **Dr. Web** называют этот «вирус» следующим образом: **`EICAR Test File (Not a Virus!)`**. Примерно так его называют и другие антивирусные программы. Тестовая программа EICAR представляет собой последовательность из 68 байт, образующую тело исполняемого COM-файла для ОС MS DOS/MS Windows, в результате исполнения которого на консоль выводится текстовое сообщение

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Тело тестовой программы состоит только из текстовых символов, которые формируют следующую строку:

```
X5O! P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-
ANTIVIRUS-TEST-FILE!$H+H*
```

Если вы создадите файл, содержащий приведенную выше строку, то в результате получится программа, которая и будет описанным «вирусом».

В случае корректной работы **Антивируса Dr.Web для Linux**, этот файл должен обнаруживаться при проверке объектов файловой системы любым доступным способом, с уведомлением об обнаружении угрозы **EICAR Test File (Not a Virus!)**.

Лицензирование

Права пользователя на использование копии программного продукта **Антивирус Dr.Web для Linux** подтверждаются и регулируются лицензией, приобретенной пользователем у компании **«Доктор Веб»** или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с **Лицензионным соглашением**, условия которого принимаются пользователем при установке программного продукта на свой компьютер. В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии продукта, в частности:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование **Антивируса**;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать приобретенную копию **Антивируса**).

Имеется также возможность активировать для приобретенной копии **Антивируса** демонстрационный период. В этом случае, если не нарушены условия активации демонстрационного периода, пользователь получает право на полноценное использование **Антивируса** в течение демонстрационного периода.

Каждой лицензии на использование программных продуктов компании **«Доктор Веб»** сопоставлен уникальный серийный номер, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу компонентов **Антивируса** в соответствии с параметрами лицензии. Он называется лицензионным ключевым файлом. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый демонстрационным.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов **Антивируса** блокируются, кроме того, недоступен сервис регулярных обновлений вирусных баз с серверов **Всемирной Системы Обновлений Dr.Web** (**ВСО Dr. Web**). Однако имеется возможность активировать **Антивирус**, подключив его к серверу централизованной защиты антивирусной сети предприятия или сети, организованной Интернет-провайдером. В этом случае управление антивирусными функциями и обновлениями копии продукта, установленной на компьютере, включенном в состав антивирусной сети, возлагается на сервер централизованной защиты.

Приобретение и регистрация лицензий

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов **ВСО Dr.Web**, а также получать стандартную техническую поддержку компании **«Доктор Веб»** и ее партнеров.

Приобрести любой антивирусный продукт **Dr.Web** или серийный номер для него вы можете у наших партнеров или через интернет-магазин. Дополнительную информацию о сроках и типах лицензирования можно найти на официальном сайте компании **«Доктор Веб»** http://www.drweb.com/.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем **Антивируса Dr.Web для Linux** и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки. Приобретенная лицензия может быть активирована любым из указанных ниже способов:

- при помощи мастера регистрации, входящего в состав **Менеджера лицензий**;
- непосредственно на сайте компании **«Доктор Веб»** по адресу http://products.drweb.com/register/.

При активации приобретенной лицензии необходимо указать ее серийный номер. Этот номер может поставляться вместе с продуктом или по электронной почте, при покупке или продлении лицензии онлайн.

В случае регистрации лицензии, продлевающей лицензию, срок годности которой истек, требуется указать серийный номер или лицензионный ключевой файл предыдущей лицензии, в противном случае срок действия новой лицензии будет сокращен на 150 дней.

Если имеется комплект лицензий, выданных для использования **Антивируса** на нескольких компьютерах, то при регистрации имеется возможность указать, что **Антивирус** будет использоваться только на одном компьютере. В этом случае все лицензии из комплекта будут объединены в одну, и срок ее действия будет автоматически увеличен.

Запрос демонстрационного периода

Пользователям продуктов **Dr.Web** доступно два типа демонстрационного периода:

- сроком на 3 месяца;
- сроком на 1 месяц.

Чтобы получить демонстрационный период сроком на 3 месяца, необходимо пройти процедуру регистрации на официальном сайте компании **«Доктор Веб»** и указать свои персональные данные. В этом случае вы получите по электронной почте серийный номер для активации вашей копии **Антивируса**. Демонстрационный период сроком на 1 месяц можно получить непосредственно в окне мастера регистрации **Менеджера лицензий,** не указывая персональных данных.

Вы можете в любой момент запустить процесс регистрации или запроса демонстрационного периода из окна **Менеджера лицензий**, нажав кнопку **Активировать лицензию** на странице просмотра информации о текущей лицензии.

Для активации при помощи серийного номера, а также для запроса демонстрационного периода требуется подключение к сети Интернет.

Демонстрационный период использования **Антивируса** не может быть предоставлен для одного и того же компьютера чаще, чем 1 раз в год.

В случае активации лицензии или демонстрационного периода при помощи **Менеджера лицензий**, ключевой файл (лицензионный или демонстрационный) будет сформирован на локальном компьютере и установлен в надлежащее место автоматически. При получении ключевого файла по электронной почте в результати регистрации на сайте, вам необходимо выполнить его установку вручную.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации необходимо указать те же персональные данные, которые вы ввели при первой регистрации лицензии. Допускается использовать другой адрес электронной почты – в таком случае лицензионный ключевой файл будет выслан по новому адресу.

Количество запросов на получение лицензионного ключевого файла ограничено – регистрация лицензии с одним и тем же серийным номером допускается не более 25 раз. Если это число превышено, лицензионный ключевой файл не будет выслан. В этом случае обратитесь в службу технической поддержки (в запросе следует подробно описать ситуацию, указать персональные данные, введенные при регистрации, и серийный номер лицензии). Лицензионный ключевой файл будет выслан службой технической поддержки по электронной почте.

Ключевой файл

Ключевой файл – это специальный файл, который хранится на локальном компьютере и соответствует приобретенной лицензии или активированному демонстрационному периоду для программного продукта **Антивирус Dr.Web для Linux**. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

Ключевой файл имеет расширение `.key` и является действительным при одновременном выполнении следующих условий:

- срок действия лицензии или демонстрационного периода, которым он соответствует, не истек;
- разрешение, определяемое лицензией или активным демонстрационным периодом, распространяется на все используемые модули;
- целостность файла не нарушена.

При нарушении любого из этих условий ключевой файл становится недействительным.

При работе **Антивируса Dr.Web для Linux** ключевой файл по умолчанию должен находиться в каталоге `/etc/opt/drweb.com` и иметь имя **`drweb32.key`**.

Компоненты **Антивируса** регулярно проверяют наличие и корректность ключевого файла. Его содержимое защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

При отсутствии действительного ключевого файла (лицензионного или демонстрационного), а также по истечении срока его действия, антивирусные функции всех компонентов блокируются до установки действующего ключевого файла.

Рекомендуется сохранять имеющийся лицензионный ключевой файл до истечения срока его действия. В этом случае при переустановке продукта или переносе его на другой компьютер повторная регистрация серийного номера лицензии не потребуется, и вы сможете использовать лицензионный ключевой файл, полученный при первом прохождении процедуры регистрации.

Установка ключевого файла

В случае если уже имеется ключевой файл, соответствующий действующей лицензии на этот продукт (например, он был получен от продавца по электронной почте после регистрации или **Антивирус Dr.Web для Linux** переносится на другой компьютер), имеется возможность активировать **Антивирус**, просто указав путь к имеющемуся ключевому файлу.

Это можно сделать следующим образом:

- В **Менеджере лицензий**, перейдя на первом шаге мастера регистрации по ссылке **Другие виды активации** и указав путь к имеющемуся ключевому файлу.
- Вручную, для этого:
  1. Распакуйте ключевой файл, если он был вами получен в архиве;
  2. Скопируйте его в каталог `/etc/opt/drweb.com` и переименуйте в **`drweb32.key`**

Вы можете так же воспользоваться командой:

```
# drweb-ctl cfset Root.KeyPath </путь/к/ключевому/файлу>
```

Обратите внимание, что в последнем случае ключевой файл не будет скопирован в каталог `/etc/opt/drweb.com`, а останется в своем исходном каталоге. В этом случае пользователь сам несет ответственность за сохранность ключевого файла. Такой способ установки ключевого файла не рекомендуется из-за возможности его случайного удаления (например, если он был размещен в каталоге, подвергающемся автоматической очистке системой).

Файл настроек подключения

Файл настроек подключения представляет собой специальный файл, хранящий внутри себя параметры подключения **Антивируса Dr.Web для Linux** к серверу централизованной защиты.

Этот файл может быть предоставлен администратором антивирусной сети или Интернет-провайдером (если он обеспечивает поддержку услуги централизованной антивирусной защиты).

Вы можете использовать этот файл для активации **Антивируса Dr.Web для Linux** через подключение его к серверу централизованной защиты (в этом случае вы не сможете использовать **Антивирус** в автономном режиме, не приобретя дополнительно лицензию).

Активация через подключение к серверу централизованной защиты

В случае если провайдер или администратор сети предприятия предоставил файл настроек подключения к серверу централизованной защиты, вы можете активировать **Антивирус**, просто указав путь к имеющемуся файлу настроек подключения.

Это можно сделать следующим образом:

- В **Менеджере лицензий** на первом шаге мастера регистрации перейти по ссылке **Другие виды активации** и указать путь к имеющемуся файлу настроек подключения.

Установка и удаление Антивируса

Ниже описывается процедура установки и удаления программного комплекса **Антивирус Dr.Web для Linux** версии 9.0.0. Также в этом разделе рассмотрена процедура перехода на новую версию, если на вашем компьютере уже установлен **Антивирус Dr.Web для Linux** версии 6.0.2.

Для осуществления этих операций необходимы права суперпользователя (пользователя `root`). Для получения прав суперпользователя при установке и удалении продукта воспользуйтесь командой смены пользователя **`su`** или командой выполнения от имени другого пользователя **`sudo`**.

Переход на новую версию

Если вы используете **Антивирус Dr.Web для Linux** версии 6.0.2, которую хотите обновить до версии 9.0.0, то вам следует переустановить продукт.

Обратите внимание, что переход на новую версию **Антивируса Dr.Web для Linux** следует выполнять тем же способом, который был использован при установке **Антивируса Dr.Web для Linux** версии 6.0.2:

- Если предыдущая версия продукта была установлена из репозитория, то переход на новую версию рекомендуется выполнять обновлением версии из репозитория.
- Если предыдущая версия продукта была установлена из универсального пакета, то обновление следует производить установкой универсального пакета, содержащего новую версию продукта.

В случае если вы не имеете возможности обновить продукт тем же способом, каким он был установлен изначально, вам следует предварительно удалить **Антивирус Dr.Web для Linux** версии 6.0.2, а потом выполнить установку новой версии продукта доступным для вас способом. Способы установки и удаления продукта **Антивирус Dr.Web для Linux** версии 6.0.2 аналогичны способам установки и удаления, рассмотренным в данном руководстве для версии 9.0.0. Для дополнительной информации обратитесь к Руководству пользователя **Антивируса Dr.Web для Linux** версии 6.0.2.

- При установке **Антивируса Dr.Web для Linux** версии 9.0.0 из универсального пакета вам будет предложено автоматически удалить старую версию продукта, установленную из универсального пакета, при установке новой версии.
- Для обновления **Антивируса Dr.Web для Linux** версии 6.0.2, установленного из репозитория компании **«Доктор Веб»,** вам необходимо выполнить:
  - Смену используемого репозитория (с репозитория пакетов версии 6.0.2 на репозиторий пакетов версии 9.0.0. Имя

репозитория см. в разделе Установка из репозитория);

- Обновление продукта. Для этого необходимо выполнить команды

  В случае использования пакетов RPM:

```
# yum update
```

  В случае использования пакетов DEB:

```
# apt-get update
# apt-get dist-upgrade
```

При любом способе обновления **Антивируса** имеющийся у вас лицензионный ключевой файл будет автоматически установлен в надлежащее место для использования новой версией (либо в процессе работы программы установки, либо при первом запуске **Антивируса** в графическом режиме).

В случае возникновения проблем с автоматической установкой ключевого файла вы можете выполнить его установку вручную. Лицензионный ключевой файл **Антивируса Dr.Web для Linux** 6.0.2 находится в каталоге `/home/<user>/.drweb` (каталог имеет атрибут «скрытый»).

В случае утраты действующего лицензионного ключевого файла обратитесь в службу технической поддержки компании **«Доктор Веб»**.

Антивирус Dr.Web для Linux версии 9.0.0 не поддерживает **Карантин Антивируса Dr.Web для Linux** версии 6.0.2! При наличии в **Карантине** старой версии антивируса изолированных файлов, вы можете извлечь их оттуда или окончательно удалить вручную. **Карантин Антивируса Dr.Web для Linux** версии 6.0.2 использует для изоляции файлов следующие каталоги:

- `/var/drweb/infected` – системный;
- `/home/<user>/.drweb/quarantine` – пользовательский (где `<user>` – имя пользователя).

Для упрощения обработки **Карантина** рекомендуется произвести ревизию его содержимого непосредственно из **Антивируса Dr.Web для Linux** версии 6.0.2 перед началом перехода на новую версию.

При обновлении продукта из репозитория при работающем **Антивирусе Dr.Web для Linux** версии 6.0.2, после завершения установки пакетов новой версии **Антивируса**, процессы старой версии **Антивируса** **останутся запущенными до выхода пользователя из системы,** в том числе – в области уведомлений рабочего стола (если вы работаете в графическом режиме) может быть доступен значок старой версии продукта.

Установка Антивируса

Вы можете установить **Антивирус Dr.Web для Linux** одним из двух способов:

1. Загрузив с сайта компании **«Доктор Веб»** установочный файл, содержащий универсальный пакет для UNIX-систем, снабженный программами установки в графическом режиме и режиме командной строки (при начале установки будет запущена одна из них, в зависимости от возможностей окружения).
2. Выполнив установку продукта в виде набора нативных пакетов (для этого потребуется подключиться к соответствующему репозиторию пакетов компании **«Доктор Веб»**).

После установки **Антивируса Dr.Web для Linux** любым из указанных в данном руководстве способов, в начале работы, вам потребуется активировать лицензию или установить ключевой файл. Кроме того, вы можете подключить **Антивирус** к серверу централизованной защиты.

До тех пор пока вы этого не сделаете, **функции антивирусной защиты будут отключены.**

Установка универсального пакета

Программный комплекс **Антивирус Dr.Web для Linux** распространяется в виде инсталляционного файла с именем **drweb-workstations_<версия>~linux_<платформа>.run**, где **<версия>** – это строка, включающая в себя версию и дату выпуска продукта, а **<платформа>** – строка, указывающая тип платформы, для которой предназначен продукт (**x86** для 32-битных платформ и **amd64** для 64-битных платформ). Например:

```
drweb-workstations_9.0.0.0-1404011200~linux_x86.run
```

Обратите внимание, что далее в данном разделе руководства имя

установочного файла, соответствующее формату, указанному выше, указывается как **<имя_файла>.run**.

Чтобы автоматически установить компоненты программного комплекса **Антивирус Dr.Web для Linux**:

1. Скачайте инсталляционного файла с официального сайта компании **«Доктор Веб»**.
2. Сохраните его на жесткий диск компьютера.
3. Разрешите исполнение файла, например, командой:

   ```
   # chmod +x <имя_файла>.run
   ```

4. Запустите его на исполнение командой:

   ```
   # ./<имя_файла>.run
   ```

   или воспользуйтесь стандартным файловым менеджером вашей графической оболочки как для изменения свойств файла, так и для его запуска.

   При этом будет создан каталог с именем `<имя_файла>`, с набором файлов внутри, и автоматически запустится программа установки. Если запуск был осуществлен не с правами суперпользователя, то программа установки попытается повысить свои права.

   В зависимости от возможностей текущего окружения, в котором произведен запуск дистрибутива, запустится одна из программ установки, входящих в состав дистрибутива:

   - программа установки для графического режима;
   - программа установки для режима командной строки.

   При этом программа установки для режима командной строки запустится автоматически, если невозможно запустить программу установки для графического режима.

5. Следуйте инструкциям программы установки.

Пожалуйста, обратите внимание, что если ваш дистрибутив **Linux** оснащен подсистемой безопасности **SELinux,** то возможно возникновение ситуации, когда работа программы установки будет прервана подсистемой безопасности. В этом случае вам необходимо временно перевести **SELinux** в разрешающий (`Permissive`) режим, для чего выполните команду

```
# setenforce 0
```

После этого перезапустите программу установки.

Также в этом случае по окончании процесса установки необходимо выполнить настройку политик безопасности **SELinux** для того, чтобы в дальнейшем антивирусные компоненты работали корректно.

После завершения установки, в графической оболочке рабочего стола, в меню **Приложения,** появится группа **Dr.Web,** содержащая два пункта:

- **Dr.Web для Linux** для запуска **Антивируса Dr.Web для Linux** в графическом режиме
- **Удалить компоненты Dr.Web** для его удаления.

После успешной установки продукта вы можете удалить каталог с установочными файлами <имя_файла>.

Установка в графическом режиме

После запуска программы установки, работающей в графическом режиме, на экране появится окно мастера установки. На странице приветствия вы можете выбрать язык, который будет использоваться в процессе работы мастера. Для этого выберите нужный язык в выпадающем списке, расположенном в правом верхнем углу страницы приветствия.

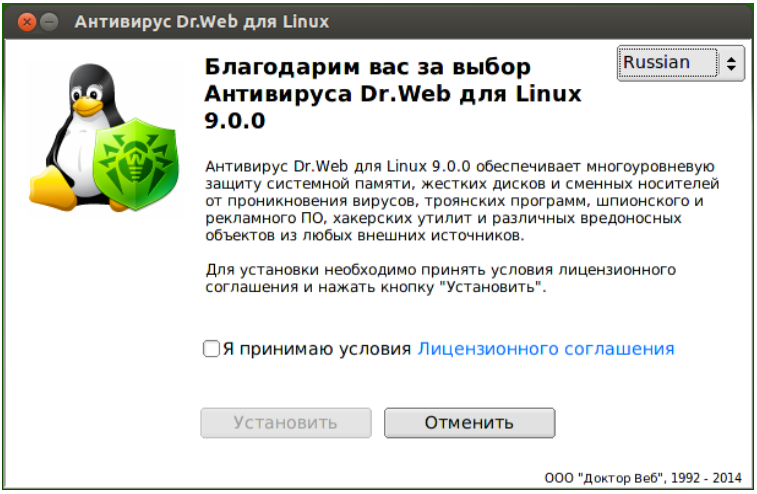

Рисунок 2. Страница приветствия мастера установки

Для установки **Антивируса Dr.Web для Linux** на свой компьютер необходимо последовательно выполнить следующие действия:

1. Ознакомиться с условиями **Лицензионного соглашения** компании **«Доктор Веб»**. Для чего нужно щелкнуть по соответствующей ссылке в надписи "Я принимаю условия Лицензионного соглашения". После этого откроется страница мастера установки, позволяющая ознакомиться с текстом **Лицензионного соглашения** и сведениями об авторских правах на компоненты, которые будут установлены на ваш компьютер.

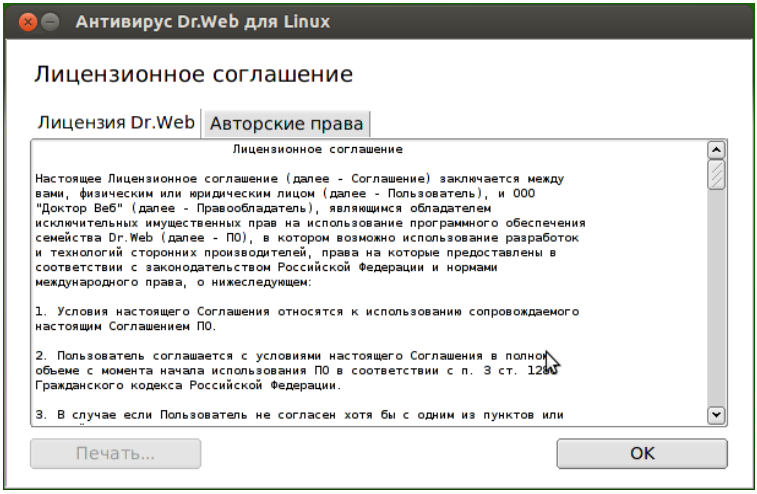

Рисунок 3. Просмотр Лицензионного соглашения

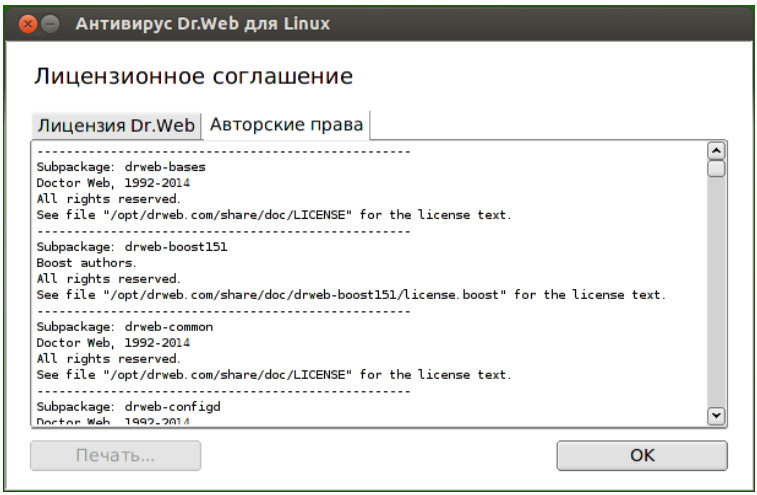

Рисунок 4. Просмотр сведений об авторских правах

При необходимости, если в вашей системе установлен и настроен принтер, вы можете распечатать текст

Лицензионного соглашения и сведения об авторских правах. Для этого необходимо открыть нужную вкладку на странице ознакомления с **Лицензионным соглашением** и авторскими правами и нажать кнопку **Печать...**.

Для закрытия страницы ознакомления с **Лицензионным соглашением** и авторскими правами нажмите кнопку **ОК**.

2. Для начала установки вы должны подтвердить, что принимаете условия **Лицензионного соглашения** компании **«Доктор Веб»**, для чего следует установить флажок **Я принимаю условия Лицензионного соглашения.**

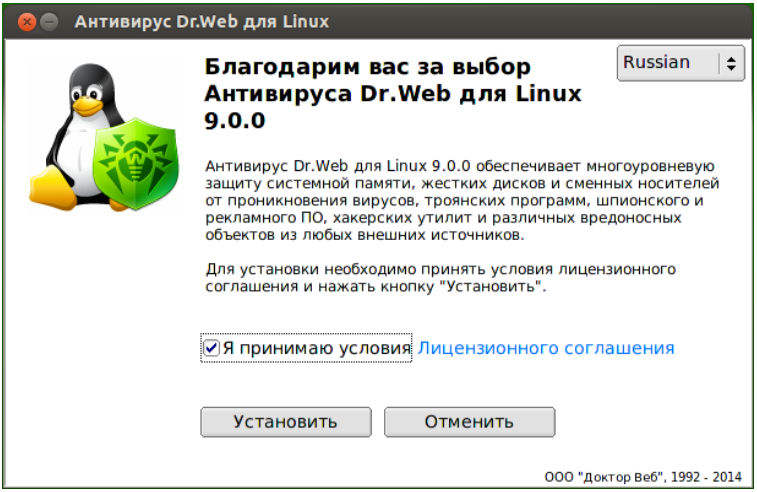

Рисунок 5. Подтверждение принятия условий Лицензионного соглашения

Если вы решили отказаться от установки **Антивируса** на свой компьютер, нажмите кнопку **Отмена** для отказа от установки и завершения работы мастера установки. В противном случае нажмите кнопку **Установить** для начала процесса установки продукта.

3. После начала установки откроется страница мастера,

содержащая индикатор, показывающий прогресс процесса установки. При необходимости вы можете нажать кнопку **Подробнее** для просмотра сообщений журнала установки.

Рисунок 6. Индикатор процесса установки

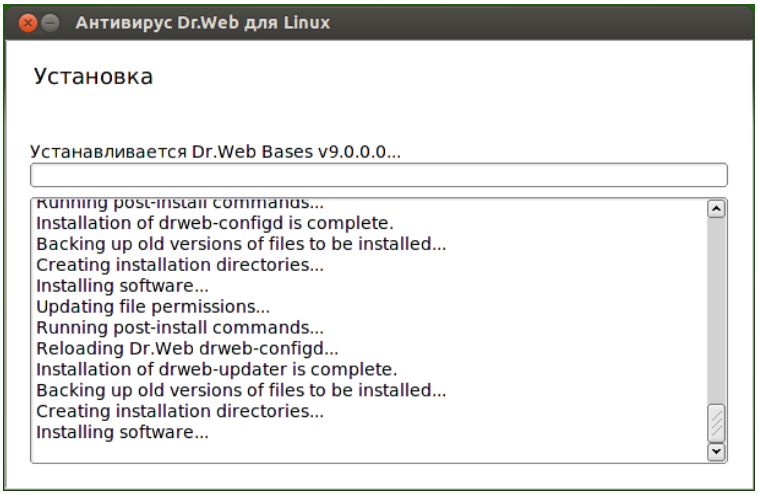

Рисунок 7. Просмотр журнала установки

4. После успешного окончания процесса копирования файлов программы и внесений необходимых изменений в системные файлы, откроется финальная страница мастера, отображающая результат установки.

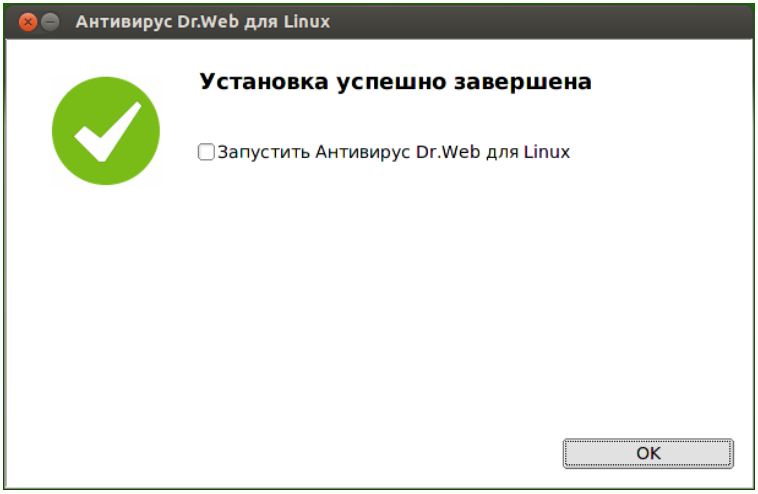

Рисунок 8. Результаты установки

5. Чтобы закрыть окно мастера установки, необходимо нажать кнопку **OK.** Если вы хотите сразу по окончании установки запустить **Антивирус Dr.Web для Linux** в графическом режиме, установите предварительно флажок **Запустить Антивирус Dr.Web для Linux.**

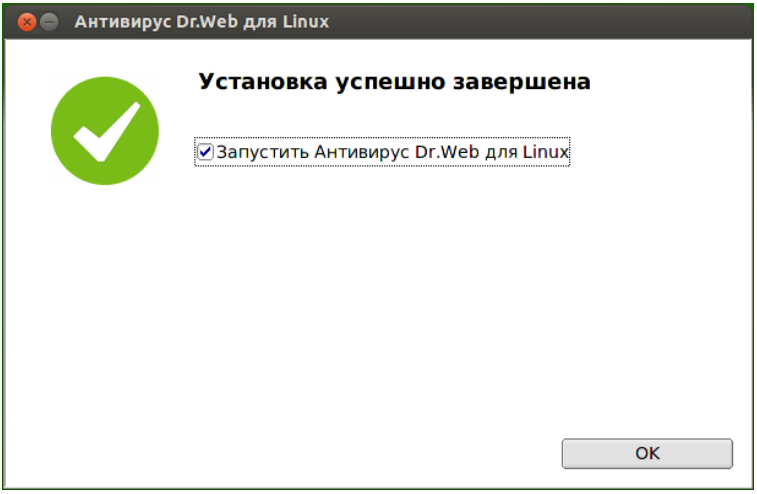

Рисунок 9. Требование запуска Антивируса поле окончания установки

Если установка была прервана из-за ошибки, финальная страница мастера будет содержать соответствующее сообщение. В этом случае также следует закрыть мастер установки, нажав кнопку **OK.** После этого устраните проблемы, вызвавшие ошибку установки, и повторите установку заново.

Установка в режиме командной строки

После запуска программы установки, работающей с режиме командной строки, на экране появится текст приглашения к установке.

1. Для начала установки ответьте **Yes** или **Y** на запрос «Вы хотите продолжить?». Чтобы отказаться от установки, введите **No** или **N.** В этом случае работа программы установки будет завершена.

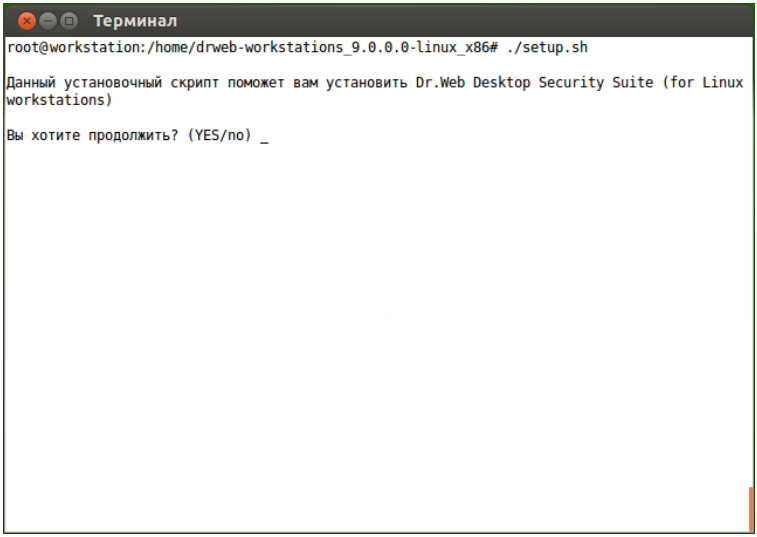

Рисунок 10. Приглашение к установке

2. Далее перед началом установки вам необходимо ознакомиться с текстом **Лицензионного соглашения** компании **«Доктор Веб»**, который будет выведен на экран. Для пролистывания текста лицензионного соглашения пользуйтесь клавишами ENTER (пролистывание текста на одну строчку вниз) и ПРОБЕЛ (пролистывание текста вниз на экран). Обратите внимание, что пролистывание текста **Лицензионного соглашения** назад (вверх) не предусмотрено.

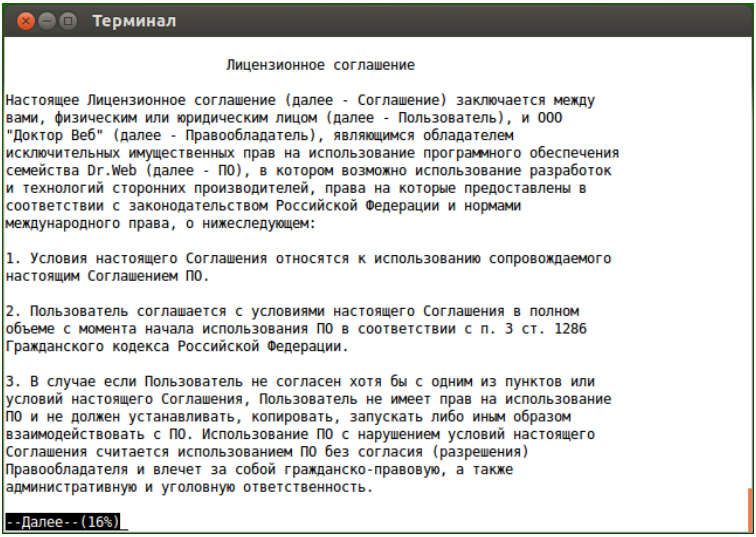

Рисунок 11. Просмотр текст Лицензионного соглашения

3. После прочтения **Лицензионного соглашения** вам будет предложено принять его условия. Введите **`Yes`** или **`Y`**, если вы принимаете условия, и **`No`** или **`N`**, если вы не согласны с условиями **Лицензионного соглашения**. В случае отказа от принятия условий **Лицензионного соглашения** работа программы установки будет завершена.

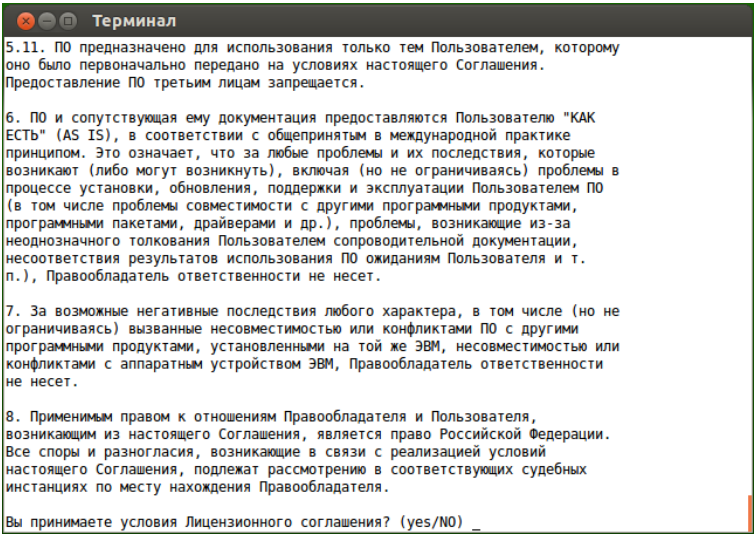

Рисунок 12. Принятие условий Лицензионного соглашения

4. После соглашения с условиями **Лицензионного соглашения** автоматически будет запущен процесс установки на компьютер компонентов **Антивируса Dr.Web для Linux.** При этом на экран будет выводиться информация о ходе установки, включающая в себя перечень устанавливаемых компонентов.

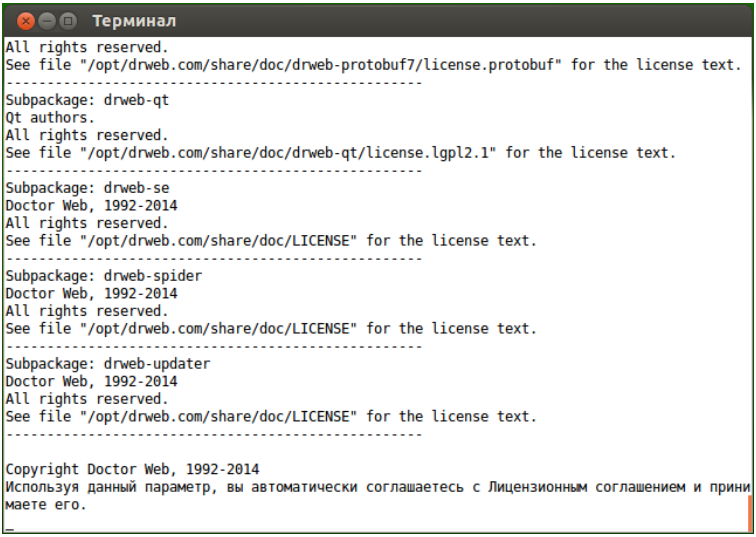

Рисунок 13. Протокол установки компонентов

5. В случае успешного окончания процесса установки на экран будет выведено сообщение «Установка завершена» и программа установки завершит свою работу. В случае возникновения ошибки на экран будет выведено соответствующее сообщение с описанием ошибки, после чего работа программы установки также будет завершена.

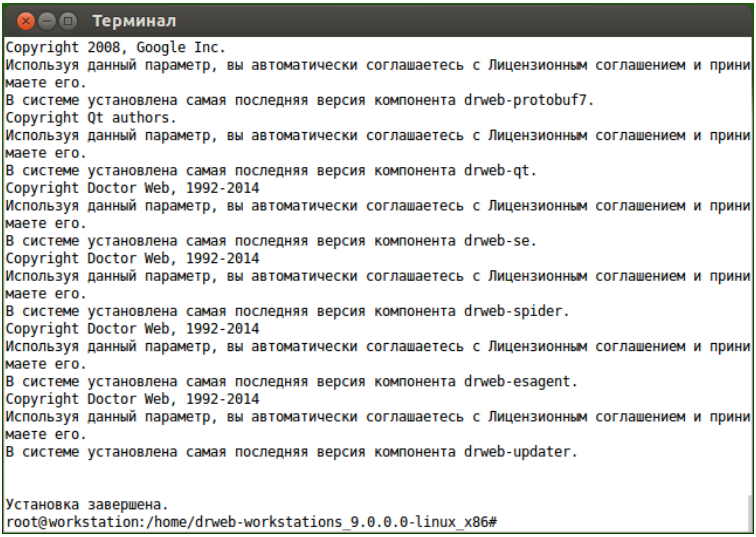

Рисунок 14. Сообщение об окончании установки

6. Для начала работы с установленным **Антивирусом** воспользуйтесь любым удобным для вас способом запуска.

Если установка была прервана из-за ошибки, следует устранить проблемы, вызвавшие ошибку установки, и повторить процесс установки заново.

Установка из репозитория

Нативные пакеты продукта **Антивирус Dr.Web для Linux** находятся в официальном репозитории **Dr.Web** http://repo.drweb.com/drweb/. После добавления репозитория **Dr.Web** в список репозиториев, используемых менеджером пакетов вашей операционной системы, вы сможете устанавливать его в виде нативных пакетов для операционной системы так же, как и любые другие программы из репозиториев вашей операционной системы. Необходимые зависимости будут разрешаться автоматически.

Все нижеприведенные команды для подключения репозиториев, импортирования ключей, установки и удаления пакетов должны быть выполнены с правами суперпользователя. Для этого используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Все команды обращения к репозиториям записываются в одну строчку. Символ "↵" в данном документе используется только для обозначения принудительного переноса на новую строку части длинной строки.

Debian, Mint, Ubuntu (apt)

Репозиторий для этих ОС защищен с помощью механизма цифровой подписи. Для корректной работы нужно импортировать ключ цифровой подписи командой

```
wget -O - http://repo.drweb.com/drweb/drweb.key ↵
| apt-key add -
```

или

```
curl http://repo.drweb.com/drweb/drweb.key ↵
| apt-key add -
```

Чтобы подключить репозиторий, добавьте следующую строку в файл `/etc/apt/sources.list`:

```
deb http://repo.drweb.com/drweb/debian 9.0.0 ↵
non-free
```

Кроме того, вы можете выполнить автоматическое получение ключа и подключение к репозиторию версии 9.0.0, скачав и установив специальный DEB-пакет. Ссылка на скачивание пакета: http://repo.drweb.com/drweb-repo9.deb.

Для установки **Антивируса Dr.Web для Linux** из репозитория выполните команды:

```
apt-get update
apt-get install drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **Synaptic** или **aptitude**). Кроме того, альтернативные менеджеры, такие как **aptitude,** рекомендуется использовать для разрешения конфликта пакетов, если он возникнет.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

Добавьте файл со следующим содержимым в каталог `/etc/yum.repos.d`:

Для 32-разрядной версии:

```
[drweb]
name=DrWeb - 9.0.0
baseurl=http://repo.drweb.com/drweb/el5/9.0.0/i386/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

Для 64-разрядной версии:

```
[drweb]
name=DrWeb - 9.0.0
baseurl=http://repo.drweb.com/drweb/el5/9.0.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

Кроме того, вы можете выполнить автоматическое подключение к репозиторию версии 9.0.0, скачав и установив специальный RPM-пакет. Ссылка на скачивание пакета: http://repo.drweb.com/drweb-repo9.rpm.

Для установки **Антивируса Dr.Web для Linux** из репозитория выполните команду:

```
yum install drweb-workstations
```

Установка также может осуществляться с помощью альтернативных менеджеров (например **PackageKit** или **Yumex**).

Настройка политик безопасности для SELinux

Если используемый вами дистрибутив **Linux** оснащен подсистемой безопасности **SELinux** (`Security-Enhanced Linux` – **Linux** с улучшенной безопасностью), то для того, чтобы компоненты ядра продукта (такие как сканирующее ядро) работали корректно после установки компонентов приложения, вам потребуется внести изменения в политики безопасности, используемые **SELinux.**

Кроме того, при включенном **SELinux** установка продукта в виде универсального пакета из установочного файла (`.run`) может окончиться неудачей, поскольку будет заблокирована попытка создания в системе специального пользователя `drweb`, с полномочиями которого работают модули **Антивируса Dr.Web для Linux.**

Перед началом установки рекомендуется проверить режим работы **SELinux,** для этого выполните команду **`getenforce`**. Эта команда выводит на экран текщуий режим зашиты:

- **`Permissive`** – защита активна, но используется разрешающая стратегия: действия, нарушающие политики безопасности, не запрещаются, а только фиксируются в журнале аудита.
- **`Enforced`** – защита активна, используется запрещающая стратегия: действия, нарушающие политики безопасности, регистрируются в журнале аудита и блокируются.
- **`Disabled`** – **SELinux** установлен, но неактивен.

Если **SELinux** работает в режиме `Enforced`, следует временно (на период установки продукта и последующей настройки политик безопасности) перевести ее в режим `Permissive`. Для этого выполните команду **`setenforce 0`**, которая временно (до первой перезагрузки системы) переведет **SELinux** в режим `Permissive`. Чтобы вернуть систему в режим `Enforced`, следует выполнить команду **`setenforce 1`**.

Обратите внимание, что, какой бы режим защиты вы ни установили при помощи команды **setenforce**, после перезагрузки операционной системы **SELinux** вернется в режим защиты, заданный в ее настройках (обычно файл настроек **SELinux** находится в каталоге `/etc/selinux`).

В общем случае, при использовании в системе демона **audit**, журнал аудита располагается в файле `/var/log/audit/audit.log`. В противном случае сообщения о запрете операции записываются в общий файл журнала `/var/log/messages`.

Чтобы при работающем **SELinux** антивирусные компоненты могли успешно функционировать, необходимо скомпилировать специальные политики безопасности сразу после установки программного продукта.

Пожалуйста, обратите внимание, что в некоторых дистрибутивах **Linux** указанные ниже утилиты могут быть по умолчанию не установлены. В этом случае вам, возможно, потребуется дополнительно установить содержащие их пакеты.

Чтобы создать необходимые политики:

1. Создайте новый файл с исходным кодом политики **SELinux** (файл с расширением `.te`). Данный файл определяет ограничения, относящиеся к описываемому модулю. Исходный файл политики может быть создан двумя способами:

    1) **С помощью утилиты audit2allow.** Это наиболее простой способ. Данная утилита генерирует разрешающие правила на основе сообщений об отказе в доступе в файлах системных журналов. Возможно задать автоматический поиск сообщений в файлах журналов или указать путь к файлу журнала вручную.

Утилита **audit2allow** находится в пакете `policycoreutils-python` или `policycoreutils-devel` (для ОС **RedHat Enterprise Linux, CentOS, Fedora,** в зависимости от версии) или в пакете `python-sepolgen` (для ОС **Debian, Ubuntu**).

Обратите внимание, что для ОС **Fedora** версии 19 дополнительно обязательно требуется установить пакет `checkmodule`, иначе вызов утилиты **audit2allow** завершится ошибкой.

Пример использования:

```
# audit2allow -M drweb -i /var/log/audit/
audit.log
```

или

```
# cat /var/log/audit/audit.log |
audit2allow  -M drweb
```

В данном примере утилита **audit2allow** производит поиск сообщений об отказе в доступе в файле `audit.log`.

```
# audit2allow -a -M drweb
```

В данном примере утилита **audit2allow** ищет сообщения об отказе в доступе в файлах журналов автоматически.

В обоих случаях в результате работы утилиты создаются два файла: исходный файл политики `drweb.te` и готовый к установке модуль политики `drweb.pp`.

В большинстве случаев вам не потребуется вносить изменения в файл политики, созданный этой утилитой. Поэтому рекомендуется сразу переходить к пункту 4 для установки полученного модуля политики `drweb.pp`. Обратите внимание, что по умолчанию утилита

audit2allow в качестве результата своей работы выводит на экран готовый вызов команды **semodule**. Скопировав его в командную строку и выполнив, вы выполните пункт 4. Перейдите к пункту 2, только если вы хотите внести изменения в политики, автоматически сформированные для компонентов **Антивируса Dr.Web для Linux**.

2) **С помощью утилиты policygentool.** Для этого укажите в качестве параметров имя модуля, работу с которым вы хотите настроить, и полный путь к его исполняемому файлу.

Обратите внимание, что утилита **policygentool**, входящая в состав пакета `selinux-policy` для ОС **RedHat Enterprise Linux** и **CentOS Linux,** может работать некорректно. В таком случае воспользуйтесь утилитой **audit2allow**.

Пример создания политик при помощи **policygentool**:

- Для модуля **drweb-se** (используется антивирусным ядром):

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- Для модуля **drweb-filecheck** (входит в состав **Сканера**):

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Вам будет предложено указать несколько общих характеристик домена, после чего для каждого модуля будут созданы три файла, определяющих политику:

`<module_name>.te`, `<module_name>.fc` и `<module_name>.if`.

2. При необходимости отредактируйте сгенерированный

исходный файл политики `<module_name>.te`, а затем, используя утилиту **checkmodule**, создайте бинарное представление (файл с расширением `.mod`) исходного файла локальной политики.

Обратите внимание, что для успешной работы этой команды в системе должен быть установлен пакет `checkpolicy`.

Пример использования:

```
# checkmodule -M -m -o drweb.mod drweb.te
```

3. Создайте устанавливаемый модуль политики (файл с расширением `.pp`) с помощью утилиты **semodule_package**.

   Пример:

   ```
   # semodule_package -o drweb.pp -m drweb.mod
   ```

4. Для установки созданного модуля политики воспользуйтесь утилитой **semodule**.

   Пример:

   ```
   # semodule -i drweb.pp
   ```

После перезагрузки операционной системы подсистема безопасности **SELinux** будет настроена для корректной работы **Антивируса Dr.Web для Linux.**

Для получения дополнительной информации о принципах работы и настройки **SELinux** обратитесь к документации по используемому вами дистрибутиву **Linux.**

Расположение файлов продукта

Файлы программного комплекса **Антивирус Dr.Web для Linux** после установки размещаются в каталогах `/opt`, `/etc` и `/var` дерева файловой системы.

Структура используемых каталогов:

Каталог	Содержимое
/opt/drweb.com	Исполняемые файлы компонентов продукта и основные библиотеки, необходимые для работы **Антивируса Dr.Web для Linux**
/etc/opt/drweb.com	Файлы настроек компонентов (по умолчанию) и лицензионный ключевой файл для работы **Антивируса Dr.Web для Linux** в режиме Standalone
/var/opt/drweb.com	Вирусные базы, Антивирусное ядро, а также временные файлы и дополнительные библиотеки, необходимые для работы **Антивируса Dr.Web для Linux**

Удаление Антивируса

В зависимости от способа установки, вы можете удалить **Антивирус Dr.Web для Linux** одним из двух способов:

1. Запустив программу удаления универсального пакета (для графического режима или режима командной строки, в зависимости от возможностей окружения).
2. Удалив пакеты продукта, установленные из репозитория компании **«Доктор Веб»,** используя системный менеджер пакетов.

Удаление универсального пакета

Удаление продукта **Антивирус Dr.Web для Linux,** установленного из универсального пакета, можно выполнить как через меню приложений окружения графического рабочего стола, так и при помощи командной строки.

Удаление продукта через меню приложений

Для этого выберите в меню приложений группу **Dr.Web,** в которой выберите пункт меню **Удалить компоненты Dr.Web.**

Далее будет запущена программа удаления для графического режима.

Удаление продукта из командной строки

Запуск программы удаления осуществляется скриптом **remove.sh,** расположенным в каталоге `/opt/drweb.com/bin`. Таким образом, чтобы запустить удаление продукта, необходимо выполнить следующую команду:

```
# /opt/drweb.com/bin/remove.sh
```

Далее запустится программа удаления (использующая графический режим или режим командной строки, в зависимости от возможностей текущего окружения).

Чтобы непосредственно запустить программу удаления для режима командной строки, используйте следующую команду:

```
# /opt/drweb.com/bin/uninst.sh
```

Процедура удаления **Антивируса Dr.Web для Linux** рассмотрена в соответствующих разделах:

- Удаление в графическом режиме;
- Удаление в режиме командной строки.

Удаление в графическом режиме

После запуска программы удаления для графического режима, на экране появится окно мастера удаления. На странице приветствия вы можете выбрать язык, который будет использоваться в процессе работы мастера. Для этого выберите нужный язык в выпадающем списке, расположенном в правом верхнем углу страницы приветствия.

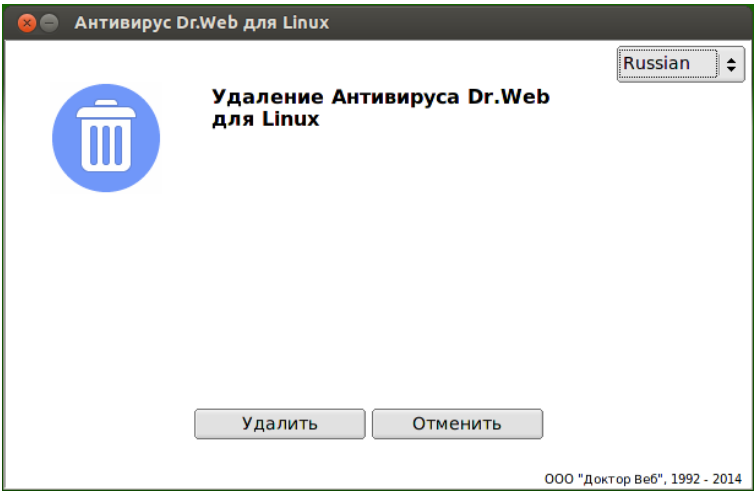

Рисунок 15. Страница приветствия мастера удаления

Для удаления **Антивируса Dr.Web для Linux** необходимо нажать кнопку **Удалить**. Чтобы прекратить работу мастера удаления и отказаться от удаления **Антивируса**, нажмите кнопку **Отменить.**

После начала процесса удаления откроется страница мастера, отражающая ход процесса удаления и содержащая соответствующий индикатор прогресса. При необходимости вы можете нажать кнопку **Подробнее** для просмотра сообщений журнала удаления.

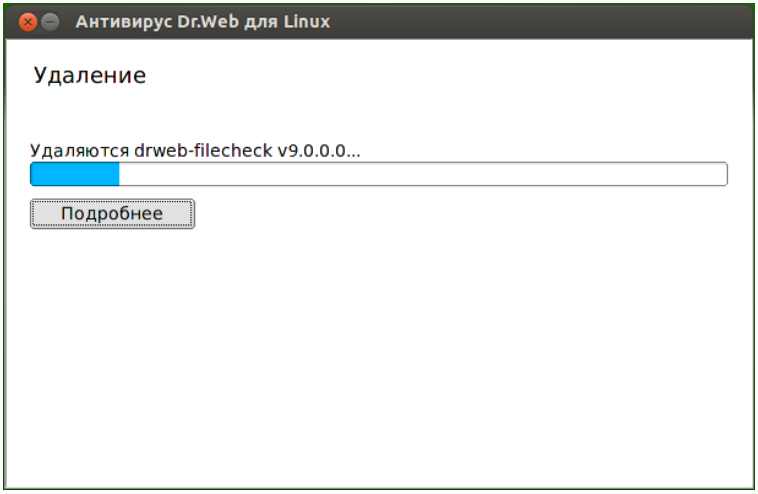

Рисунок 16. Индикатор процесса удаления

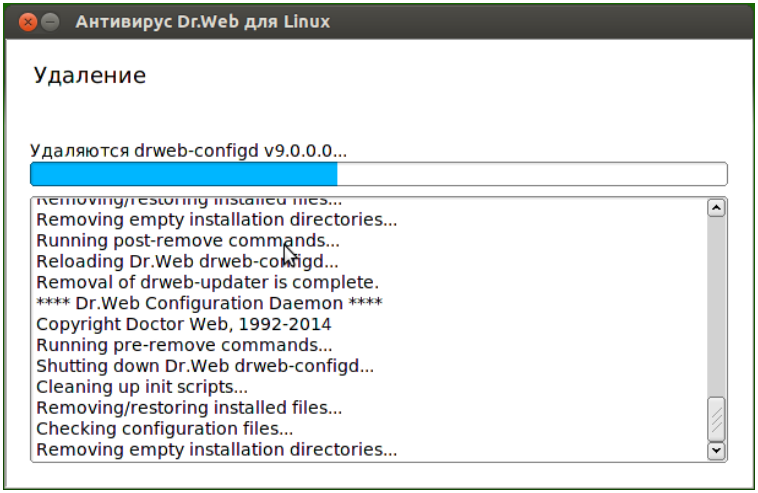

Рисунок 17. Просмотр журнала удаления

После успешного окончания процесса удаления файлов **Антивируса Dr.Web для Linux** и внесений необходимых

изменений в системные файлы, откроется финальная страница мастера с сообщением об успешном удалении.

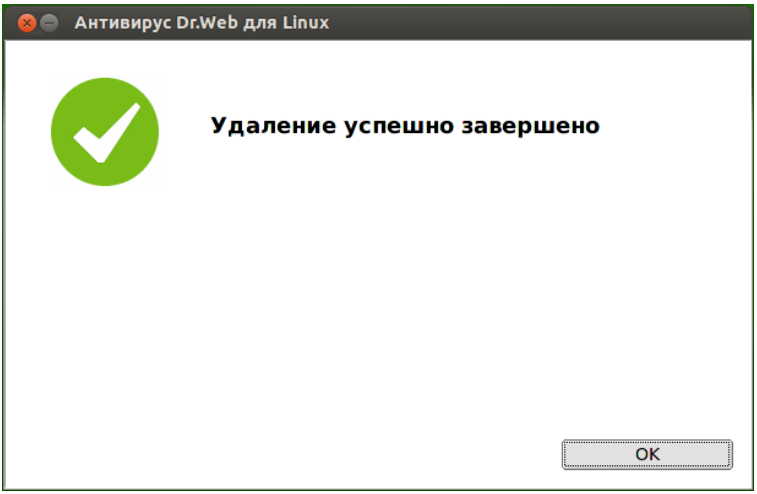

Рисунок 18. Результаты работы мастера удаления

Для закрытия окна мастера удаления необходимо нажать кнопку **OK.**

Удаление в режиме командной строки

После запуска программы удаления, работающей в режиме командной строки, на экране появится текст приглашения к удалению.

1. Для начала удаления ответьте **Yes** или **Y** на запрос «Вы хотите продолжить?». Чтобы отказаться от удаления **Антивируса**, введите **No** или **N.** В этом случае работа программы удаления будет завершена.

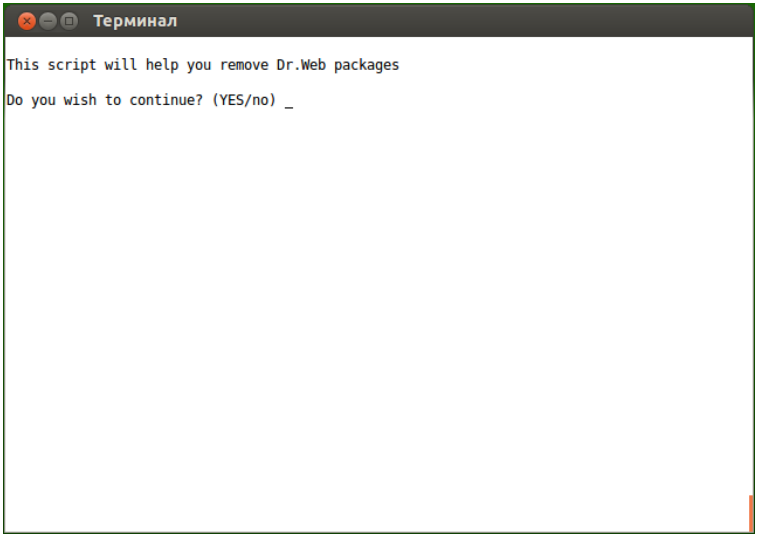

Рисунок 19. Приглашение к удалению

2. Далее на экран будет выведен перечень установленных компонентов **Антивируса Dr.Web для Linux**.

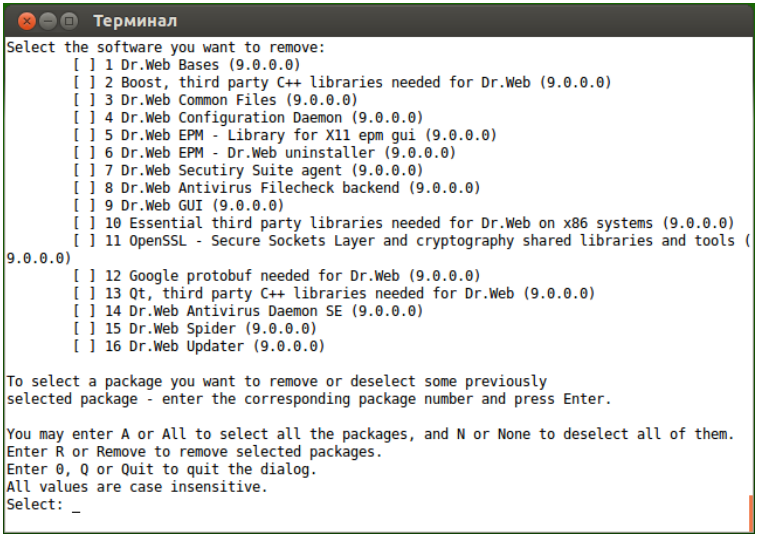

Рисунок 20. Просмотр перечня имеющихся компонентов

3. Для продолжения удаления следует отметить компоненты, подлежащие удалению. Для отметки конкретного пакета необходимо ввести его номер. Обратите внимание, что в случае если от пакета, отмеченного к удалению, зависят какие-то другие пакеты, они также будут отмечены автоматически.
   - Чтобы отметить сразу все имеющиеся компоненты, введите вместо номера слово **All** или **A**.
   - Чтобы сбросить выделение пакетов, введите вместо номера слово **None** или **N**.
   - Чтобы отказаться от удаления, введите вместо номера **0**, **Q** или **Quit**. Это приведет к завершению работы программы удаления.

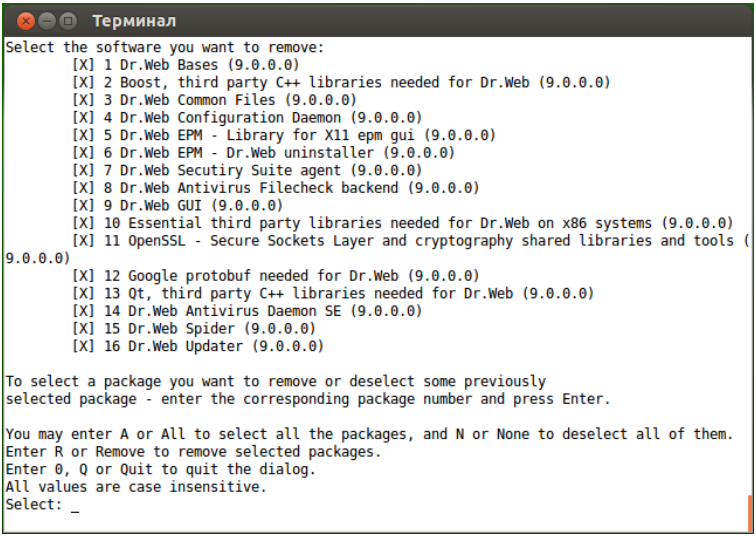

Рисунок 21. Выбор компонентов для удаления

4. После отметки всех подлежащих удалению компонентов, для начала процесса удаления, введите слово **Remove** или **R**.

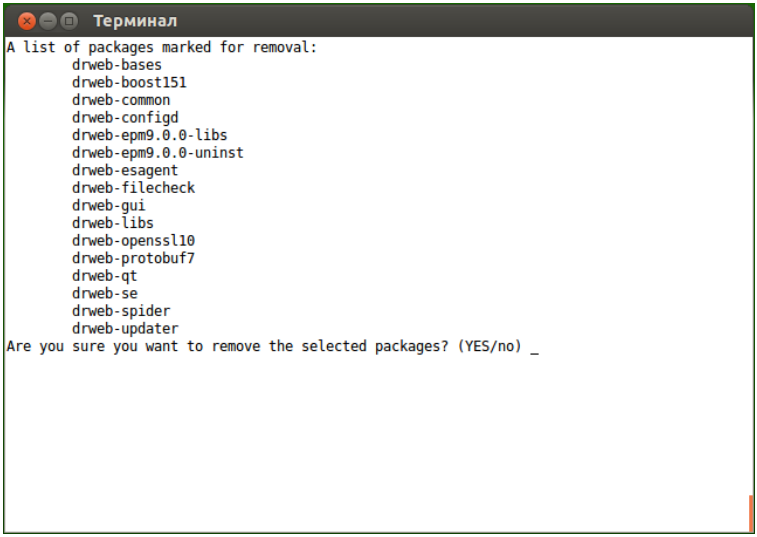

Рисунок 22. Подтверждение удаления отмеченных компонентов

5. На следующем экране необходимо просмотреть список пакетов, отмеченных для удаления, и подтвердить удаление, введя **Yes** или **Y**. Чтобы отказаться от удаления, следует ввести **No** или **N**. Это приведет к завершению работы программы удаления.

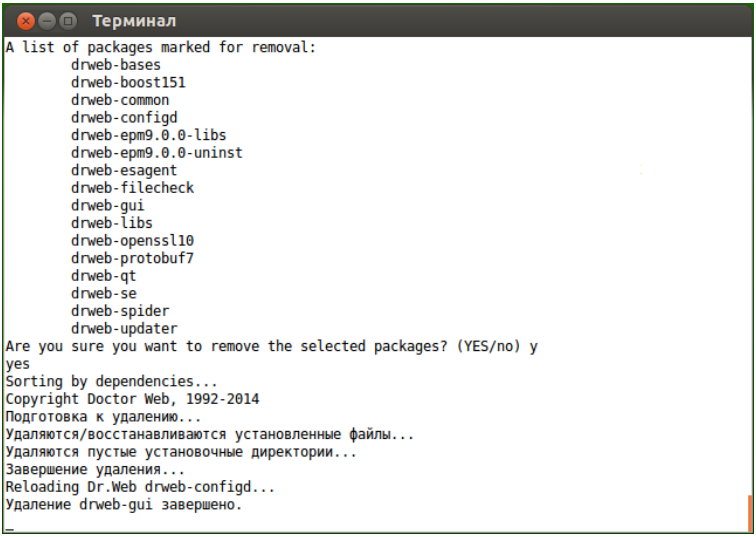

Рисунок 23. Протокол удаления

6. После запуска удаления отмеченных ранее пакетов на экран будут выдаваться записи, фиксируемые в журнал удаления и отражающие ход процесса удаления.

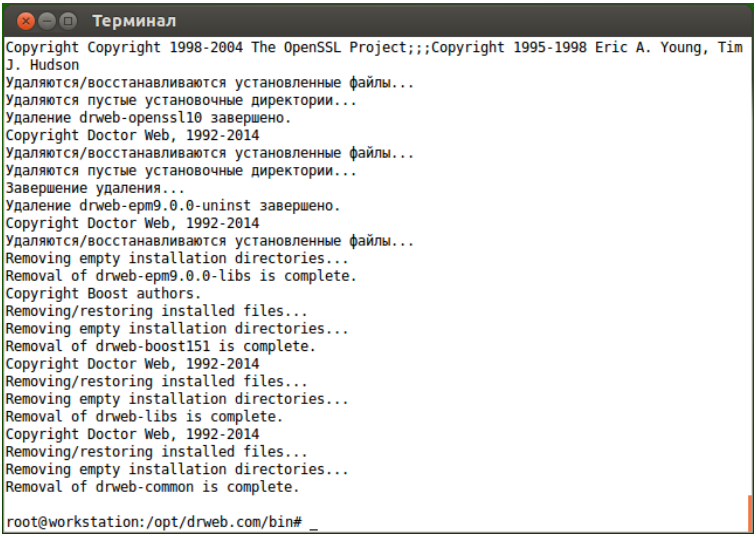

Рисунок 24. Сообщение об окончании удаления

7. По окончанию процесса программа удаления выведет на экран соответствующее сообщение и завершит свою работу.

Удаление продукта, установленного из репозитория

Все нижеприведенные команды для удаления пакетов должны быть выполнены с правами суперпользователя. Для этого используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Debian, Mint, Ubuntu (apt)

Для удаления **Антивируса Dr.Web для Linux** выполните команду:

```
apt-get remove drweb-workstations
```

Для удаления всех установленных пакетов **Dr.Web** выполните команду (в некоторых системах символ '*' требуется экранировать: '*'):

```
apt-get remove drweb*
```

Для автоматического удаления из системы всех более не используемых пакетов можно воспользоваться командой:

```
apt-get autoremove
```

Обратите внимание на следующие особенности удаления с использованием **apt-get**:

1. Первый вариант команды удалит только пакет `drweb-workstations`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы все пакеты, название которых начинается на "`drweb`" (стандартное наименование для пакетов программных продуктов **Dr.Web**). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта **Антивирус Dr.Web для Linux**.
3. Третий вариант команды удалит из системы все пакеты, которые были автоматически установлены для удовлетворения зависимостей других пакетов, но более не требуемые (например, ввиду удаления исходного пакета). Обратите внимание, что эта команда удалит из системы все более не требуемые пакеты, а не только пакеты продукта **Антивирус Dr.Web для Linux**.

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например **Synaptic** или **aptitude**).

Red Hat Enterprise Linux, Fedora, CentOS (yum)

Для удаления **Антивируса Dr.Web для Linux** выполните команду:

```
yum remove drweb-workstations
```

Для удаления всех установленных пакетов **Dr.Web** выполните команду (в некоторых системах символ '*' требуется экранировать: '*'):

```
yum remove drweb*
```

Обратите внимание на следующие особенности удаления с использованием **yum**:

1. Первый вариант команды удалит только пакет `drweb-workstations`, а остальные пакеты, которые могли быть автоматически установлены при установке этого пакета для удовлетворения его зависимостей, останутся в системе.
2. Второй вариант команды удалит из системы все пакеты, название которых начинается на "`drweb`" (стандартное наименование для пакетов программных продуктов **Dr.Web**). Обратите внимание, что эта команда удалит из системы все пакеты с таким именем, а не только пакеты продукта **Антивирус Dr.Web для Linux**.

Удаление пакетов продукта также может осуществляться с помощью альтернативных менеджеров (например **PackageKit** или **Yumex**).

Работа с Антивирусом

Работа пользователя с **Антивирусом Dr.Web для Linux** может производиться любым из следующих способов:

- При помощи графического интерфейса – в графическом режиме;
- Из командной строки, включая работу через эмуляторы терминала в графического режиме.

Для запуска **Антивируса** в графическом режиме необходимо выбрать пункт **Dr.Web для Linux** в меню приложений, или выполнить в командной строке операционной системы команду

```
$ drweb-gui
```

В этом случае, если окружение графического рабочего стола доступно, **Антивирус Dr.Web для Linux** будет запущен в графическом режиме.

Управление работой **Антивируса** из командной строки рассмотрено в разделе Работа из командной строки.

В штатном режиме работы **Антивируса Dr.Web для Linux** все его сервисные компоненты запускаются автоматически (некоторые – при старте операционной системы, а другие только по запросу от других компонентов) и не требуют ручного вмешательства в свою работу.

После установки **Антивируса Dr.Web для Linux** любым из указанных в данном руководстве способов, в начале работы, вам потребуется активировать лицензию, либо установить ключевой файл, если он у вас уже имеется, или подключить **Антивирус** к серверу централизованной защиты. (см. раздел Управление лицензиями).

До тех пор, пока вы этого не сделаете, **функции антивирусной защиты будут отключены.**

Работа в графическом режиме

Графический интерфейс **Антивируса Dr.Web для Linux** работает в окружении графического рабочего стола и используется для управления работой **Антивируса.**

Назначение

Главное окно **Антивируса** позволяет решать следующие задачи:

1. Просмотр состояния работы **Антивируса Dr.Web для Linux,** включая актуальность имеющихся вирусных баз и срока действия лицензии.
2. Запуск и остановка монитора файловой системы **SpIDer Guard.**
3. Запуск проверки файлов по требованию, в том числе:
   - **Быстрая проверка** системных файлов и наиболее уязвимых системных объектов;
   - **Полная проверка** всех файлов системы;
   - **Выборочная проверка** только указанных файлов и каталогов или специализированных объектов (загрузочных записей дисков, активных процессов).

   Выбор файлов для проверки выполняется как указанием целевых каталогов или файлов перед запуском проверки, так и их перетаскиванием («drag and drop») мышью из окна файлового менеджера на главную страницу (см. ниже) или страницу **Проверка** окна **Антивируса**.
4. Обзор всех угроз, обнаруженных **Антивирусом Dr.Web для Linux** во время текущего сеанса работы в графическом режиме, включая обзор нейтрализованных и пропущенных угроз, а также объектов, перемещенных в **Карантин.**
5. Обзор объектов, перемещенных в **Карантин,** с возможностью их окончательного удаления или восстановления.
6. Настройка параметров работы компонентов **Антивируса Dr. Web для Linux,** включая следующие параметры:
   - Действия, которые **Сканеру** и **SpIDer Guard** следует

автоматически применять к обнаруженным угрозам (в зависимости от их типа);

- Перечень каталогов и файлов, которые не должны проверяться **Сканером** и не должны контролироваться монитором файловой системы **SpIDer Guard**;
- Расписание плановых проверок файловой системы, включая периодичность и тип производимой проверки, а также перечень объектов, подлежащих выборочной проверке;
- Режим работы (подключение к серверу централизованной защиты и отключение от него).

8. Управление лицензиями (выполняется через **Менеджер лицензий**).

Для корректной работы **Антивируса** необходимо, чтобы предварительно были запущены его сервисные компоненты, в противном случае он завершит свою работу непосредственно после запуска, выдав соответствующее предупреждение.

В штатном режиме все необходимые сервисные компоненты запускаются автоматически и не требуют вмешательства пользователя.

Внешний вид

Вид главного окна **Антивируса Dr.Web для Linux** представлен на рисунке ниже.

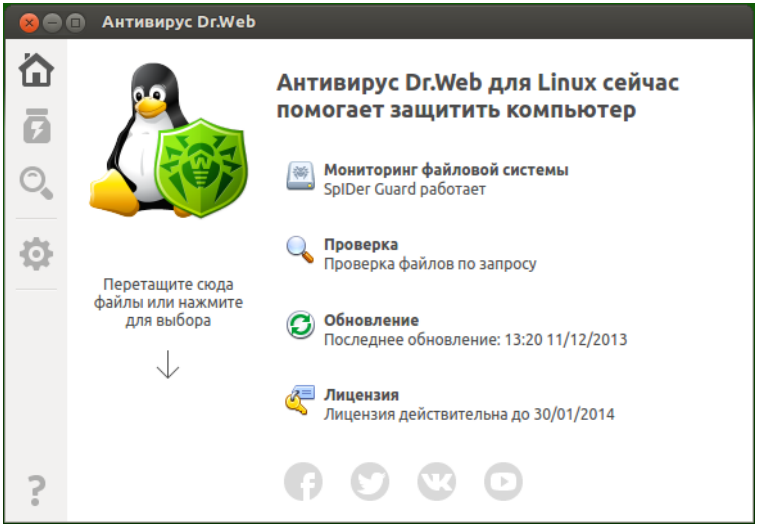

Рисунок 25. Главное окно Антивируса Dr.Web для Linux

В левой части окна расположена навигационная панель, кнопки которой позволяют выполнить следующие действия.

Кнопка	Описание
Постоянно доступные	
	Открывает главную страницу, на которой имеется возможность: • включить или выключить монитор файловой системы **SpIDer Guard**; • запустить проверку объектов файловой системы (файлов, загрузочных записей) и запущенных процессов; • просмотреть состояние актуальности вирусных баз и выполнить их обновление при необходимости; • запустить **Менеджер лицензий** для просмотра состояния текущей лицензии и регистрации новой, при необходимости.

Кнопка	Описание
	Открывает страницу работы с **Карантином,** позволяющую просмотреть файлы, помещенные в **Карантин,** а также выполнить их удаление или восстановление из **Карантина.**
	Открывает страницу запуска проверки файлов, на которой можно выбрать режим проверки, а также, при необходимости, перечень объектов, подлежащих проверке, включая запущенные в данный момент процессы.
	Открывает страницу настройки работы **Антивируса,** в частности: • **Сканера** объектов файловой системы; • Монитора файловой системы **SpIDer Guard**; • Запуска проверок по расписанию. Кроме того, здесь может быть настроена работа в режиме централизованной защиты.
	Предоставляет доступ к справочным материалам и вспомогательным ресурсам компании **«Доктор Веб»:** • Информация о продукте; • Руководство пользователя; • Официальный форум; • Техническая поддержка; • Персональный кабинет пользователя **Мой Dr.Web.** Все ссылки открываются в браузере, установленном в системе.
Появляющиеся в зависимости от условий	
	Открывает страницу списка задач проверки файлов, в котором имеются незавершенные (выполняющиеся) задачи проверки. Присутствует на навигационной панели только в случае, если хотя бы одна проверка выполняется.
	Открывает страницу списка результатов законченных проверок. Окрашивается в зависимости от результата: 1) Зеленая – все проверки закончились успешно, все найденные угрозы, если найдены, обезврежены.

Кнопка	Описание
 	2) Красная – имеются необезвреженные угрозы. 3) Желтая – какая-либо из проверок завершилась вследствие ошибки. Присутствует на навигационной панели только в случае, если запускалась хотя бы одна проверка.
	Открывает страницу просмотра угроз, обнаруженных при проверке файлов сканером или монитором файловой системы **SpIDer Guard.** Присутствует на навигационной панели только в случае, если имеются обнаруженные угрозы.
	Открывает страницу управления **SpIDer Guard.** Присутствует на навигационной панели только в случае, если ранее страница управления **SpIDer Guard** была открыта с главной страницы.
	Открывает страницу управления обновлением. Присутствует на навигационной панели только в случае, если ранее страница управления обновлениями была открыта с главной страницы.
	Открывает страницу **Менеджера лицензий.** Присутствует на навигационной панели только в случае, если ранее страница **Менеджера лицензий** была открыта с главной страницы.

Главная страница

На главной странице окна **Антивируса** расположена целевая область («мишень») для перетаскивания файлов и каталогов, подлежащих проверке. Она отмечена надписью **Перетащите сюда файлы или нажмите для выбора** и изображением стрелки, направленной вниз. При перетаскивании и отпускании файлов и каталогов из окна файлового менеджера на главную страница окна **Антивируса** запускается их выборочная проверка (в случае, если **Сканер** уже выполняет какую-либо проверку, то задача проверки указанных файлов ставится в очередь).

Также на главной странице окна **Антивируса** управления расположены следующие кнопки:

- **Мониторинг файловой системы** – отображает текущее состояние, в котором находится монитор файловой системы **SpIDer Guard.** При нажатии открывает страницу управления, на которой можно запустить или остановить **SpIDer Guard,** а также просмотреть статистику его работы.
- **Проверка** – позволяет открыть страницу запуска проверки файлов, каталогов и других объектов файловой системы (например, загрузочные записи).
- **Обновление** – отображает текущее состояние обновления вирусных баз. При нажатии открывает страницу управления обновлением, на которой можно запустить процесс обновления по требованию.
- **Лицензия** – отображает состояние текущей лицензии. При нажатии открывает страницу **Менеджера лицензий**, на которой можно ознакомиться с более детальной информацией о текущей лицензии, а также выполнить процедуру приобретения и регистрации новой лицензии, если это требуется.

Индикатор в области уведомлений

Когда **Антивирус Dr.Web для Linux** работает в графическом режиме, в области уведомлений рабочего стола доступен индикатор состояния, используемый для показа всплывающих уведомлений и доступа к контекстному меню приложения.

Запуск и завершение работы

Запуск Антивируса в графическом режиме

Для запуска **Антивируса Dr.Web для Linux** в графическом режиме необходимо выбрать в меню приложений пункт **Dr.Web для Linux.**

Кроме того, вы можете запустить **Антивирус Dr.Web для Linux** в графическом режиме из командной строки. Это возможно только в том случае, если графическое окружение доступно при работе с

командной строкой, например – из окна эмулятора терминала.

Завершение работы Антивируса

Для завершения работы **Антивируса Dr.Web для Linux** необходимо закрыть его окно, используя стандартную кнопку закрытия, расположенную в заголовке окна.

Обратите внимание, что при завершении работы графического интерфейса **Антивируса** сервисные компоненты продолжают свою работу. Это же относится и к монитору файловой системы **SpIDer Guard,** но при этом теряется возможность взаимодействия с ним через индикатор в области уведомлений. Поэтому не рекомендуется закрывать окно **Антивируса** при работающем **SpIDer Guard** (вместо этого используйте сворачивание окна).

В штатном режиме все необходимые сервисные компоненты не требуют вмешательства пользователя.

Индикатор в области уведомлений

Когда **Антивирус Dr.Web для Linux** запущен в графическом режиме, в области уведомлений рабочего стола (если она поддерживается используемой графической средой) отображается индикатор, имеющий вид пиктограммы с логотипом **Антивируса.** Индикатор используется для отображения статуса приложения, а также доступа к контекстному меню **Антивируса.** При наличии каких-либо проблем (например, устарели вирусные базы или заканчивается срок действия лицензии) в индикаторе поверх логотипа **Антивируса Dr.Web для Linux** отображается символ восклицательного знака.

Индикатор используется также для отображения всплывающих уведомлений, информирующих пользователя о важных событиях в работе **Антивируса,** таких, как:

- Обнаружена угроза (в том числе – резидентным монитором файловой системы **SpIDer Guard**);

- Заканчивается срок действия лицензии.

При нажатии клавишей мыши на пиктограмму приложения на экране отображается контекстное меню **Антивируса Dr.Web для Linux.**

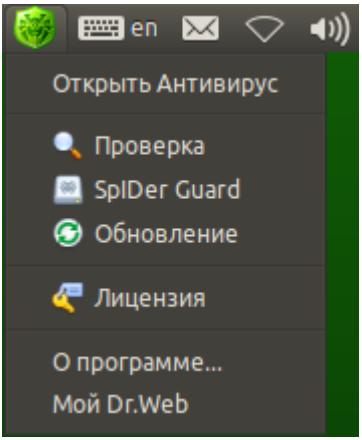

Рисунок 26. Контекстное меню Антивируса Dr.Web для Linux

При выборе пунктов меню **Открыть Антивирус, Проверка, SpIDer Guard, Обновление** или **Лицензия** на экране появляется главное окно **Антивируса,** на котором отображается соответствующая страница. Выбор пункта **О программе...** отображает на экране окно с краткой информацией о производителе, версии и названии продукта. Выбор пункта меню **Мой Dr.Web** открывает в браузере персональную страницу пользователя продукта на официальном сайте компании **«Доктор Веб»** (требуется наличие подключения к сети Интернет).

В случае если индикатор указывает на наличие проблем в функционировании **Антивируса,** то в меню пиктограмма соответствующего пункта, вызвавшего проблему, окрашивается в красный цвет (на приведенном рисунке восклицательный знак в индикаторе указывает на отключенный монитор файловой системы **SpIDer Guard** и истекший срок действия лицензии). Тем самым имеется возможность устранить проблему, вызвав на экран

окно **Антивируса** и совершив требуемые действия на соответствующей странице окна.

При закрытии окна **Антивируса** индикатор также удаляется из области уведомлений, вследствие чего работающий монитор файловой системы **SpIDer Guard** не сможет выводить свои уведомления. Поэтому не рекомендуется закрывать окно **Антивируса** при работающем **SpIDer Guard** (вместо этого используйте сворачивание окна).

В некоторых окружениях рабочего стола внешний вид и поведение индикатора могут отличаться от описанного, например, могут не отображаться пиктограммы в выпадающем меню.

Поиск и обезвреживание угроз

Поиск и обезвреживание угроз осуществляется как **Сканером**, по требованию пользователя или по заданному расписанию, так и в процессе работы монитора файловой системы **SpIDer Guard.**

- Включение и выключение **SpIDer Guard** осуществляется на соответствующей странице управления его работой.
- Обзор текущих задач на проверку **Сканером** объектов файловой системы и управление ими осуществляется на странице управления списком проверок.
- Все угрозы, обнаруженные **Сканером** или монитором файловой системы **SpIDer Guard,** отображаются в виде списка на странице просмотра обнаруженных угроз.
- Управление угрозами, помещенными в **Карантин,** осуществляется на странице работы с Карантином.
- Настройка реакции **Антивируса Dr.Web для Linux** на обнаруженные угрозы осуществляется на странице настроек. Там же имеется возможность включить и настроить расписание периодических проверок.

Если **Антивирус** работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то страница Проверка окна **Антивируса** будет недоступна.

Кроме того, в этом случае **Сканер** не будет запускать проверки по расписанию, если они настроены.

Проверка объектов по требованию

Типы выполняемых проверок

По требованию пользователя **Сканер** может выполнять следующие типы проверок:

- Быстрая проверка – проверка только жестко определенного набора критических системных объектов, подверженных наибольшему риску (загрузочные записи дисков, системные файлы и т.п.).
- Полная проверка – проверка всех объектов локальной файловой системы, доступных пользователю, от имени которого запущен **Антивирус.**
- Выборочная проверка – проверка объектов файловой системы, или некоторых объектов специального типа, непосредственно указанных пользователем.

Если **Антивирус** работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то эта страница окна **Антивируса** будет недоступна.

При проверке объектов увеличивается нагрузка на процессор, что, в случае использования мобильных устройств, может привести к быстрой разрядке аккумулятора. Поэтому на портативных компьютерах рекомендуется проводить проверку системы при питании от сети.

Запуск проверки

Запустить процесс проверки объектов файловой системы вы

можете любым из указанных ниже способов:

- Нажав кнопку  на навигационной панели.
- Нажав кнопку **Проверка** на главной странице окна.

При этом откроется страница выбора типа проверки. Чтобы инициировать Быструю или Полную проверку, следует нажать соответствующую кнопку. После этого проверка начнется автоматически.

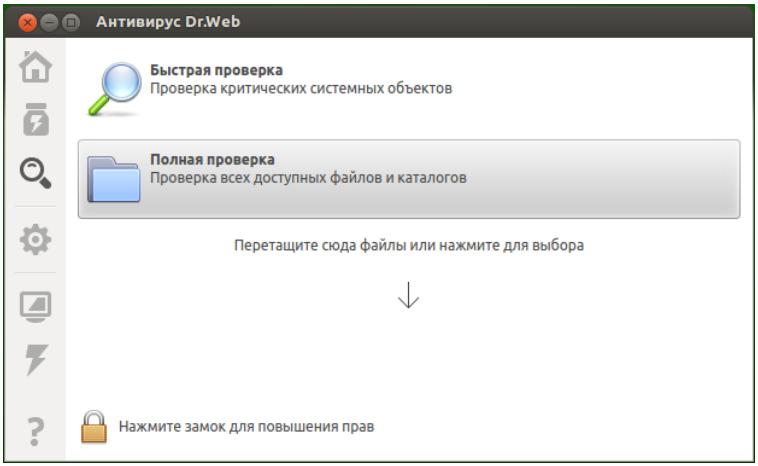

Рисунок 27. Страница выбора типа проверки

Проверка объектов всегда выполняется **Сканером** с текущими правами приложения. Если приложение не обладает правами суперпользователя, то при проверке будут пропущены все файлы и каталоги, недоступные пользователю. Чтобы обеспечить проверку всех требуемых файлов, владельцем которых вы не являетесь, следует перед началом проверки повысить права приложения, если они не повышены. См. Управление правами приложения.

Если требуется выполнить Выборочную проверку только требуемых файлов и каталогов, то это можно сделать любым из

способов, указанных ниже:

- **Перетаскивание курсором.**

  Файлы и каталоги, подлежащие проверке, можно перетащить мышью из окна файлового менеджера на открытую страницу выбора типа проверки (в зону, отмеченную надписью **Перетащите сюда файлы или нажмите для выбора** и стрелкой, направленной вниз). Также можно перетащить их на главную страницу окна **Антивируса**.

  При наведении перемещаемых файлов и/или каталогов курсором мыши на окно, на нем отображается мишень, ограниченная пунктирной линией и надписью **Поместите файлы сюда**. Для начала проверки выбранных файлов достаточно «бросить» их на страницу, отпустив кнопку мыши. После этого проверка начнется автоматически.

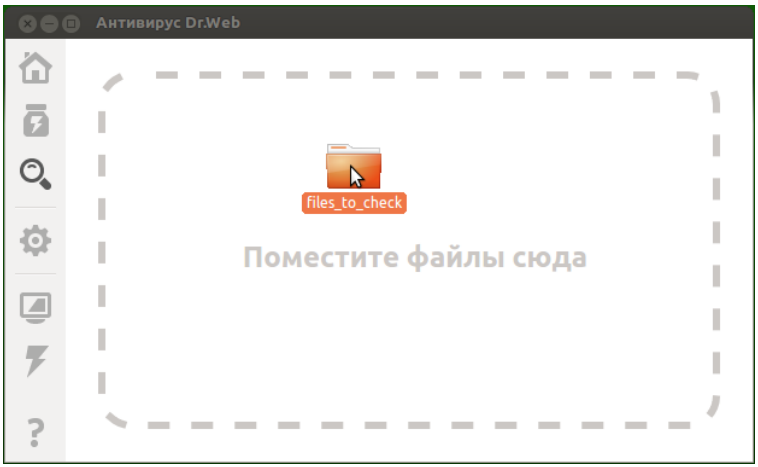

Рисунок 28. Мишень для файлов, подлежащих проверке

- **Формирование списка объектов для выборочной проверки.**

  Для формирования списка объектов для выборочной проверки необходимо щелкнуть мышью по мишени для выбора файлов. В этом случае на экране откроется список объектов для выборочной проверки.

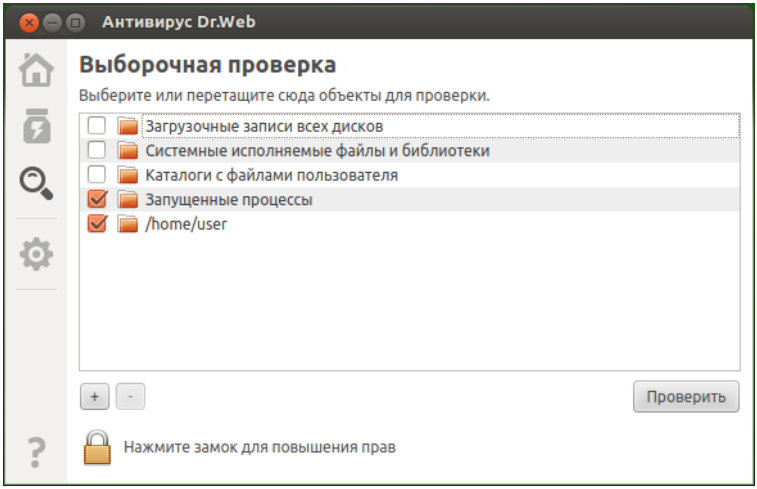

Рисунок 29. Список объектов для выборочной проверки

В списке также имеется четыре специальных пункта, задающие предопределенные группы объектов:

- Загрузочные записи всех дисков. При выборе этого пункта автоматически выделяются для проверки все загрузочные записи всех доступных в системе дисков;
- Системные файлы и библиотеки. При выборе этого пункта автоматически выбираются для проверки все каталоги, содержащие системные исполняемые файлы (`/bin`, `/sbin` и т.д.);
- Каталоги с файлами пользователя. При выборе этого пункта автоматически выбираются для проверки каталоги, содержашие файлы пользователя и текущего сеанса работы (домашний каталог `/home/<username>` (`~`), `/tmp`, `/var/mail`, `/var/tmp`).
- Запущенные процессы. При выборе этого пункта автоматически проверяются исполняемые файлы, из которых были запущены процессы, активные в системе в данный момент. При этом, если в исполняемом файле обнаруживается угроза, то все процессы, запущенные из

этого файла, принудительно завершаются, а к файлу применяются меры по нейтрализации угрозы.

Добавление и удаление объектов из списка выборочной проверки

При необходимости вы можете добавить в список выборочной проверки собственные пути для проверки. Для этого перетащите требуемые объекты мышью (пути, ведущие к указанным объектам, автоматически будут добавлены в список выборочной проверки), или нажмите кнопку «+», расположенную под списком. В этом случае откроется стандартное окно выбора файлов и каталогов. Выберите требуемый объект (файл или каталог) и нажмите кнопку **Открыть.** Кнопка «–», расположенная под списком, удаляет из списка все пути, отмеченные флажками.

Файлы и каталоги с установленным атрибутом «скрытый» по умолчанию не отображаются в окне выбора файлов и каталогов. Чтобы отобразить их, щелкните в списке файлов окна выбора файлов правой кнопкой мыши и выберите в контекстном меню пункт **Показать скрытые файлы.**

Нельзя удалить из списка первые четыре предопределенных пункта, даже если они отмечены флажками. Более того, если среди элементов списка, отмеченных флажками, имеется хотя бы один предопределенный пункт, то кнопка «–» недоступна.

Запуск выборочной проверки из списка

Чтобы начать выборочную проверку, вам следует отметить флажками в списке все объекты, подлежащие проверке, и нажать кнопку **Проверить.** После этого запустится проверка.

После запуска созданная задача проверки помещается в очередь, которая содержит все проверки, выполнявшиеся **Сканером** в текущем сеансе работы, как завершенные, так и выполняющиеся в данный момент или еще только ожидающие своего выполнения. Просмотр списка задач проверки и управление им осуществляется на странице просмотра списка задач проверки.

Управление списком проверок

Перечень созданных и выполняющихся **Сканером** задач проверки объектов файловой системы и их результатов доступен на специальной странице окна **Антивируса Dr.Web для Linux.** При наличии в очереди **Сканера** хотя бы одной задачи, на навигационной панели окна появляется специальная кнопка, нажатие на которую приводит к открытию страницы обзора списка задач проверки. В зависимости от состояния задач проверки, эта кнопка имеет следующий вид:

	В списке задач имеются незавершенные проверки (используется анимация).
	Все проверки, имеющиеся в списке, завершены или были остановлены пользователем, угроз не найдено, или все найденные угрозы обезврежены.
	Все проверки, имеющиеся в списке, завершены или были остановлены пользователем, имеются необезвреженные угрозы.
	Все проверки, имеющиеся в списке, завершены или были остановлены пользователем. Имеются проверки, завершившиеся из-за ошибки.

Задачи в списке упорядочены по мере их создания сверху вниз (от самой первой к самой последней).

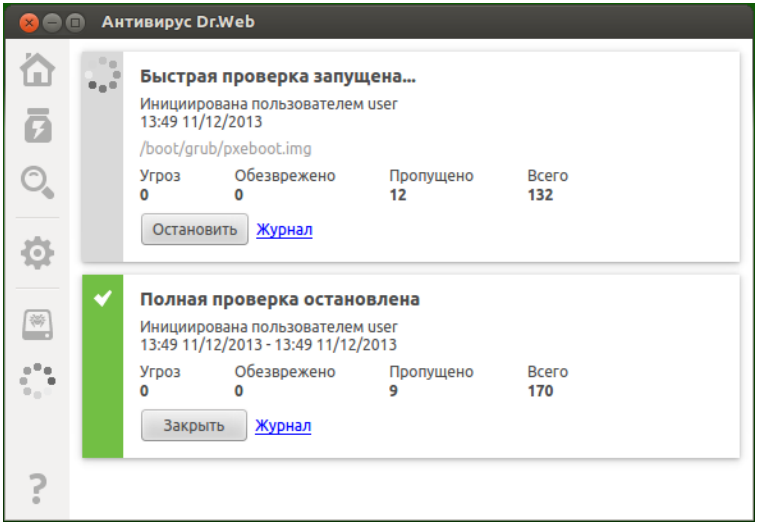

Рисунок 30. Страница просмотра списка проверок

Для каждой задачи выводится следующая информация:

- Тип проверки (кроме Быстрой, Полной и Выборочной проверок в списке могут присутствовать проверки дополнительных типов, см. ниже);
- Имя пользователя, инициировавшего проверку (если имя пользователя неизвестно, выводится его системный UID);
- Дата создания задачи и ее окончания, если она уже завершена;
- Количество обнаруженных угроз, обезвреженных угроз, пропущенных файлов и общее количество проверенных объектов.

Состояние, в котором находится задача, указывается при помощи цветовой метки, присвоенной задаче в списке. Используются следующие цвета:

 – Проверка еще не завершена или дожидается своей очереди.

 – Проверка завершена или остановлена пользователем, угроз не найдено, или все найденные угрозы обезврежены.

 – Проверка остановлена из-за возникшей ошибки.

 – Проверка завершена или остановлена пользователем, имеются необезвреженные угрозы.

Обратите внимание, что в списке отображаются все проверки, выполняемые **Сканером** в текущем сеансе работы, а не только те, которые были непосредственно инициированы пользователем в окне **Антивируса.** Это могут быть проверки следующих дополнительных типов:

- Консольная проверка – проверка, инициированная пользователем или какой-либо другой внешней программой через командную строку;
- Централизованная проверка – проверка, инициированная сервером централизованной защиты;
- Проверка по расписанию – проверка, запущенная автоматически в соответствии с расписанием, заданным в настройках.

На области описания задачи может располагаться одна из следующих кнопок:

- **Отменить** – отменить проверку, дожидающуюся своей очереди. Доступна, если задача ожидает выполнения. После нажатия задача завершается. Информация о задаче остается в списке.
- **Остановить** – остановить начатую проверку без возможности ее возобновления. Доступна, если задача выполняется. После нажатия задача завершается, а в списке остается информация о задаче, содержашая результаты проверки, полученные к моменту остановки.

- **Закрыть** – закрыть информацию о завершенной задаче и удалить её из списка. Доступна, если задача завершена и не имеется необезвреженных угроз.
- **Обезвредить** – выполнить обезвреживание угроз. Доступна, если задача проверки завершена и имеются необезвреженные угрозы.
- **Подробнее** – перейти к просмотру списка угроз. Доступна, если по результатам обезвреживания некоторые угрозы остались необезвреженными.

Нажатие на ссылку **Журнал** открывает на экране окно журнала проверки, содержащего подробную информацию о проверке, включающую в себя как общую информацию о задаче, так и перечень обнаруженных угроз, если они были обнаружены в ходе этой проверки.

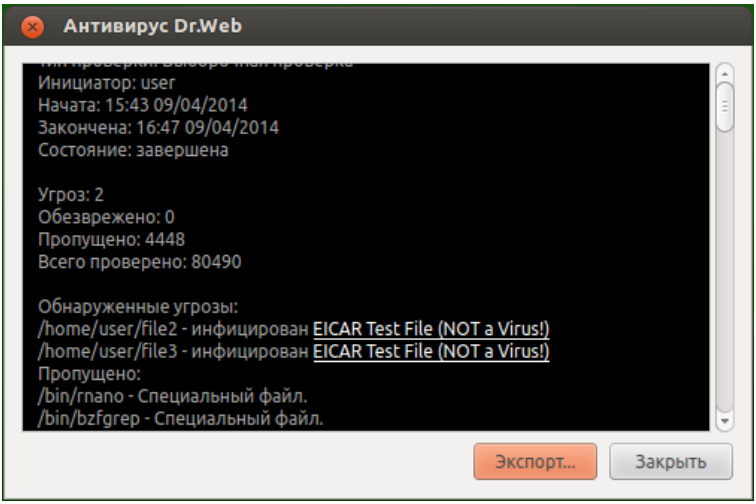

Рисунок 31. Детальная информация о проверке

Примечание: В файловой системе операционных систем семейства UNIX, к которым относится ОС **Linux,** могут встречаться специальные объекты, которые выглядят как файлы, и имеют имя, но по своей природе не являющиеся файлами, содержащими данные (например, это символические ссылки, сокеты,

именованные каналы и файлы устройств). В противоположность к обычным (регулярным) файлам такие объекты носят название специальных файлов. Специальные файлы всегда пропускаются **Антивирусом** при проверке.

Нажатие кнопки **Экспорт...** позволяет сохранить журнал проверки в текстовый файл. Нажатие на ссылку с названием обнаруженной угрозы откроет в браузере страницу с информацией об угрозе (производится переход на сайт компании **«Доктор Веб»,** требуется наличие подключения к сети Интернет).

К угрозам, обнаруженным **Сканером** в процессе любой проверки, запущенной через окно **Антивируса** (включая проверку по расписанию), применяются действия по их обезвреживанию в соответствии с настройками, указанными на вкладке **Сканер.**

Обратите внимание, что настройки обезвреживания угроз, заданные на вкладке **Сканер,** не используются для Централизованной и Консольной проверок.

Общий список всех обнаруженных угроз доступен на странице Просмотра обнаруженных угроз.

Мониторинг файловой системы

Функция постоянного мониторинга за объектами файловой системы реализуется монитором файловой системы **SpIDer Guard.**

Окно **Антивируса Dr.Web для Linux** позволяет управлять работой **SpIDer Guard,** а именно:

- Запускать и останавливать монитор файловой системы;
- Просматривать статистику работы компонента и перечень обнаруженных угроз;
- Настраивать следующие параметры работы монитора файловой системы:
  - Реакция на обнаружение угроз;

- Перечень исключений из проверки.

Управление работой монитора файловой системы

Запуск и остановка монитора файловой системы **SpIDer Guard,** а также просмотр статистики его работы производятся со специальной страницы окна **Антивируса.** Чтобы перейти на страницу управления мониторингом, необходимо нажать кнопку **Мониторинг файловой системы** на главной странице.

Аналогичное действие выполняет кнопка  на навигационной панели (она доступна, только если страница управления мониторингом уже ранее была открыта с главной страницы).

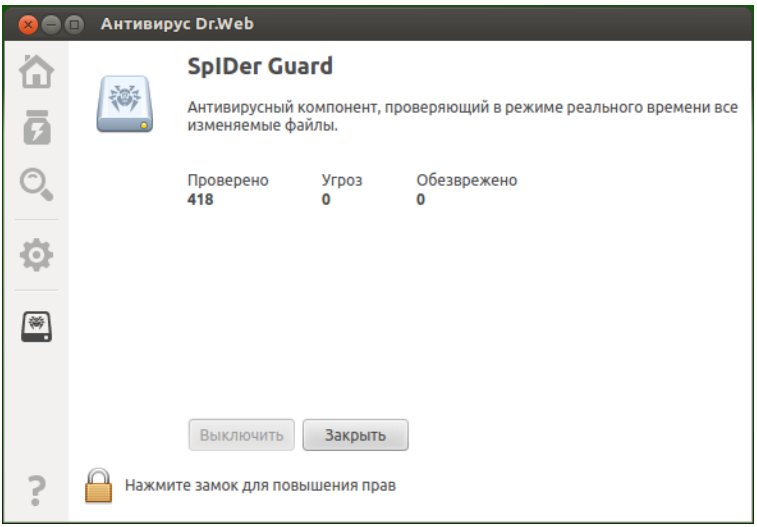

Рисунок 32. Страница управления работой SpIDer Guard

На странице управления мониторингом файловой системы выводится следующая информация:

- Состояние монитора файловой системы **SpIDer Guard**

(включен или выключен), а также, возможно, сведения о произошедших ошибках запуска.

- Статистика мониторинга файловой системы (количество проверенных объектов, количество обнаруженных и обезвреженных угроз).

Чтобы включить мониторинг, если он выключен, следует нажать кнопку **Включить.** Чтобы выключить мониторинг, если он включен, следует нажать кнопку **Выключить.**

Для выключения мониторинга файловой системы необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Возможность включения и выключения монитора файловой системы **SpIDer Guard** при работе **Антивируса** под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Состояние **SpIDer Guard** (выключен он или включен) иллюстрируется цветом индикатора:

 – монитор файловой системы **SpIDer Guard** включен и защищает файловую систему.

 – монитор файловой системы **SpIDer Guard** выключен и не защищает файловую систему.

Нажатие кнопки **Закрыть** закрывает страницу управления мониторингом файловой системы.

Перечень угроз, обнаруженных **SpIDer Guard** в текущем сеансе работы **Антивируса Dr.Web для Linux,** отображается на странице просмотра обнаруженных угроз (эта страница доступна только в том случае если имеются обнаруженные угрозы).

Настройка работы монитора файловой системы

Настройка работы монитора файловой системы **SpIDer Guard** производится на странице настроек:

- на вкладке **SpIDer Guard** – реакция на обнаруженные угрозы;
- на вкладке **Исключения** – исключение объектов из наблюдения.

Просмотр обнаруженных угроз

Список угроз, обнаруженных **Сканером** и монитором файловой системы **SpIDer Gurad** во время текущего сеанса работы **Антивируса,** отображается на специальной странице окна, которая доступна только в том случае, если была обнаружена хотя бы одна угроза.

В случае если были обнаружены угрозы, то, чтобы открыть страницу со списком угроз, необходимо нажать кнопку  на навигационной панели.

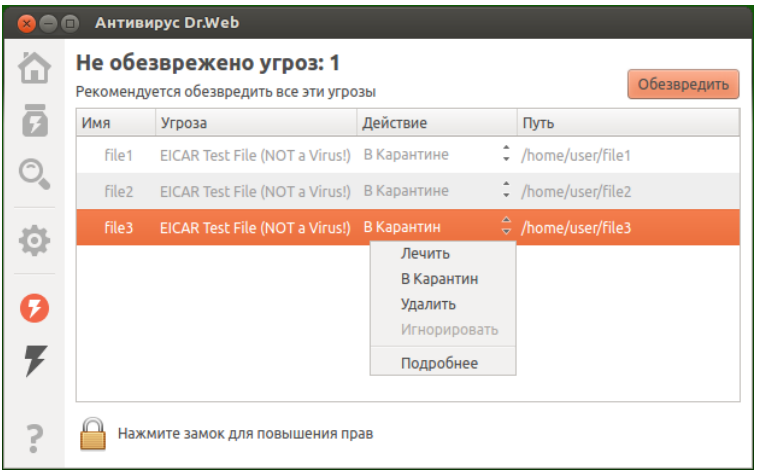

Рисунок 33. Страница обзора угроз

В списке для каждой обнаруженной угрозы выводится следующая информация:

- Имя объекта, содержащего угрозу;
- Имя угрозы, содержащейся в объекте (по классификации **«Доктор Веб»**);
- Действие, которое будет применено к объекту для нейтрализации угрозы (или уже было применено, если угроза нейтрализована);
- Путь к объекту файловой системы, в котором эта угроза была обнаружена.

Уже обезвреженные угрозы в списке представлены в списке неактивными строками.

Обезвреживание обнаруженных угроз

В случае если в списке имеются необезвреженные угрозы, на странице, непосредственно над списком, доступна кнопка **Обезвредить,** при нажатии на которую ко всем угрозам, представленным в списке, будут применены действия по их обезвреживанию, указанные в поле **Действие** у каждой необезвреженной угрозы. В случае если угроза обезвреживается успешно, ее строка в таблице становится неактивной. В случае если попытка оказывается неудачной, строка, содержащая сведения об угрозе, остается активной, текст в строке окрашивается в красный цвет, а в поле **Действие** выводится информация об ошибке.

По умолчанию в списке в качестве действий выбираются действия, заданные в качестве реакций на угрозу в настройках компонента, обнаружившего угрозу. Действия, которые по умолчанию выбираются для угроз, обнаруживаемых **Сканером** и монитором файловой системы **SpIDer Guard,** могут быть изменены на соответствующих вкладках страницы настроек.

Если требуется применить к угрозе действие, отличное от представленного в списке, следует кликнуть мышью по полю **Действие** в строке угрозы и выбрать требуемое действие в появившемся контекстном меню.

Имеется возможность выделения набора угроз в списке. Для этого нужно выделять их мышью, удерживая нажатой клавишу CTRL или SHIFT.

- При удержании CTRL угрозы будут добавляться в список выделения по одной;
- При удержании клавиши SHIFT угрозы выделяются непрерывным списком.

После выбора угроз, для применения к ним некоторого действия, нажмите правую кнопку мыши в области списка и выберите требуемое действие в появившемся выпадающем меню. Действие, выбранное в меню, будет применено ко всем выделенным угрозам.

Обратите внимание, что:

- Если угроза была обнаружена в составном объекте (архив, сообщение электронной почты и т.п.), то выбранное действие применяется не ко вложенному инфицированному объекту, а ко всему контейнеру целиком;
- Действие **Лечить** может быть применено не ко всем типам угроз;
- Если файл содержит только угрозу и не содержит никакого полезного содержимого, то действие **Лечить** равносильно действию **Удалить.**

В случае необходимости, для успешного применения действий к угрозам, повысьте права приложения.

Просмотр информации об угрозах

Для получения детальной информации о любой обнаруженной угрозе необходимо нажать правую кнопку мыши в строке информации об угрозе и выбрать в появившемся контекстном меню пункт **Подробнее.** После этого на экране появится окно, содержащее подробную информацию об угрозе и содержащем ее объекте. Если требуется получить подробную информацию сразу о нескольких угрозах, их следует перед вызовом контекстного меню выделить в списке мышью, удерживая нажатой клавишу CTRL.

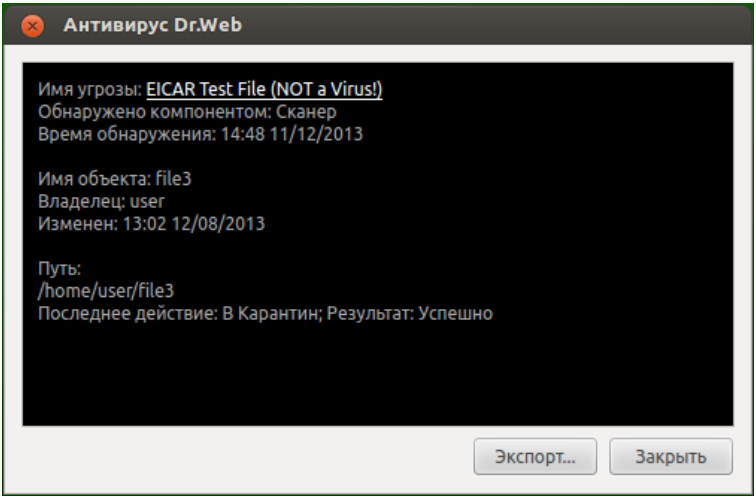

Рисунок 34. Информация об угрозе

В этом окне отображается следующая информация:

- Имя угрозы (по классификации **«Доктор Веб»**);
- Название компонента **Антивируса Dr.Web для Linux,** обнаружившего угрозу;
- Дата и время обнаружения угрозы;
- Информация об объекте файловой системы, в котором эта угроза была обнаружена: Имя, пользователь-владелец объекта, дата последнего изменения и путь к объекту в файловой системе.
- Последнее действие, которое применялось к угрозе, и его результат (если в настройках компонента, обнаружившего угрозу, задано автоматическое применение действий, например, для **Сканера** оно может быть задано на странице настроек).

Нажатие на ссылку с именем угрозы откроет в браузере веб-страницу с описанием угрозы (происходит переход на сайт компании **«Доктор Веб»,** требуется подключение к сети Интернет). При помощи нажатия кнопки **Экспорт...** имеется

возможность сохранить информацию, показанную в окне, в текстовый файл (по нажатию кнопки откроется окно выбора файла для сохранения информации).

Чтобы закрыть окно подробной информации об угрозе и содержащем ее объекте, нажмите кнопку **Закрыть.**

Управление Карантином

Список объектов, изолированных **Антивирусом Dr.Web для Linux** в **Карантин,** отображается на специальной странице.

Чтобы ее открыть, необходимо нажать кнопку  на навигационной панели.

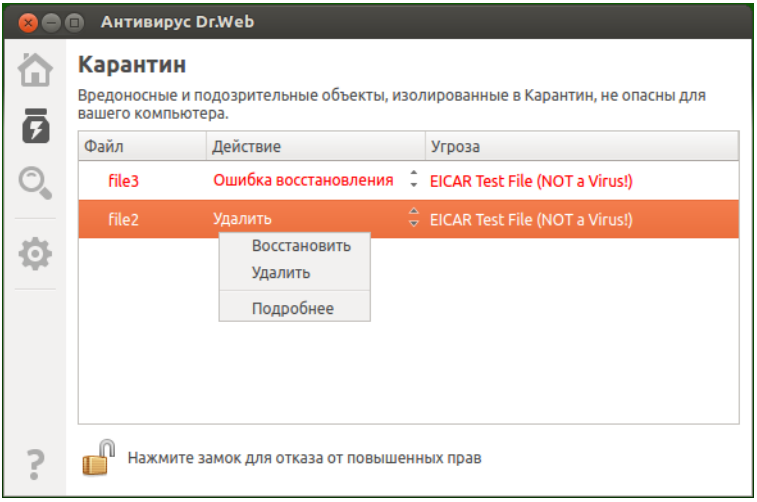

Рисунок 35. Страница управления Карантином

Если **Карантин** не пуст, в списке для каждой обнаруженной угрозы выводится следующая информация:

- Имя объекта, содержащего угрозу;

- Действие, которое следует применить к объекту в **Карантине**;
- Имя угрозы, содержащейся в объекте (по классификации **«Доктор Веб»**).

Применение действий к изолированным объектам

Для выполнения какого-либо действия с изолированным в **Карантин** объектом, следует кликнуть правой кнопкой мыши в строке, содержащей информацию об объекте, и выбрать требуемое действие в появившемся контекстном меню. Если требуется совершить некоторое действие с несколькими изолированными объектами, их следует перед вызовом контекстного меню выделить в списке. Выделение осуществляется мышью при нажатой клавише CTRL или SHIFT.

- При удержании CTRL изолированные объекты будут добавляться в список выделения по одному;
- При удержании клавиши SHIFT изолированные объекты выделяются непрерывным списком.

В меню доступны следующие действия:

- **Восстановить** – восстановление изолированного объекта в исходное место в файловой системе;
- **Удалить** – необратимое удаление изолированного объекта.

В случае если выбранное действие применяется к объекту успешно, его строка исчезает из таблицы. В случае если попытка оказывается неудачной, строка, содержащая сведения об изолированном объекте, остается активной, текст в строке окрашивается в красный цвет, а в поле **Действие** выводится информация об ошибке.

В случае необходимости, для успешного применения действий к изолированным объектам, повысьте права приложения.

Просмотр информации об изолированных объектах

Для получения детальной информации о любом изолированном объекте необходимо нажать правую кнопку мыши в строке информации об этом объекте и выбрать в появившемся контекстном меню пункт **Подробнее.** После этого на экране появится окно, содержащее подробную информацию об объекте. Если требуется получить подробную информацию сразу о нескольких изолированных объектах, их следует перед вызовом контекстного меню выделить в списке мышью, удерживая нажатой клавишу CTRL.

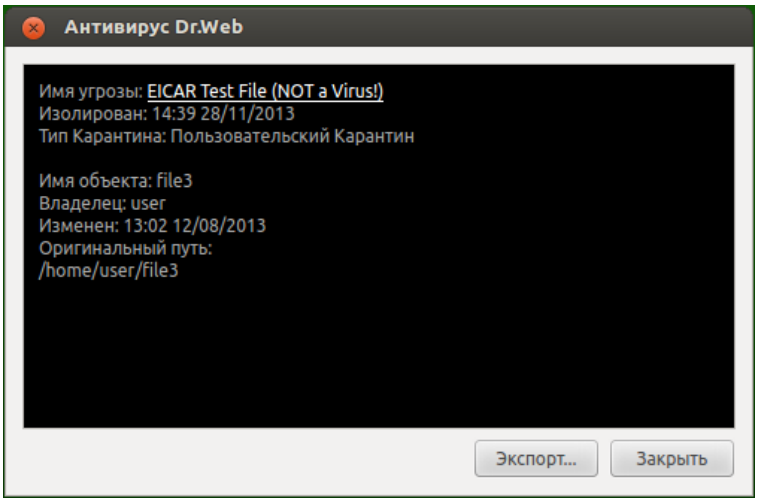

Рисунок 36. Информация об изолированном объекте

В этом окне отображается следующая информация:

- Имя угрозы (по классификации **«Доктор Веб»**);
- Дата и время изоляции объекта в **Карантин**;
- Тип Карантина, в который изолирован объект;
- Наименование и результат последнего действия, которое применялось к объекту;

- Информация об изолированном объекте файловой системы: Имя, пользователь-владелец объекта, дата последнего изменения и путь к объекту в файловой системе.

Нажатие на ссылку с именем угрозы откроет в браузере веб-страницу с описанием угрозы (происходит переход на сайт компании **«Доктор Веб»,** требуется подключение к сети Интернет). При помощи нажатия кнопки **Экспорт...** имеется возможность сохранить информацию, показанную в окне, в текстовый файл (по нажатию кнопки откроется окно выбора файла для сохранения информации).

Чтобы закрыть окно подробной информации об объекте, нажмите кнопку **Закрыть.**

Обновление вирусных баз

Периодическое обновление вирусных баз и антивирусного ядра производится **Модулем обновления** автоматически. Просмотр состояния обновлений и принудительное обновление вирусных баз производятся со специальной страницы окна **Антивируса.** Чтобы перейти на страницу управления обновлением, необходимо нажать кнопку **Обновление** на главной странице. Аналогичное действие выполняет кнопка  на навигационной панели (она доступна только в том случае, если страница управления обновлением уже ранее была открыта с главной страницы).

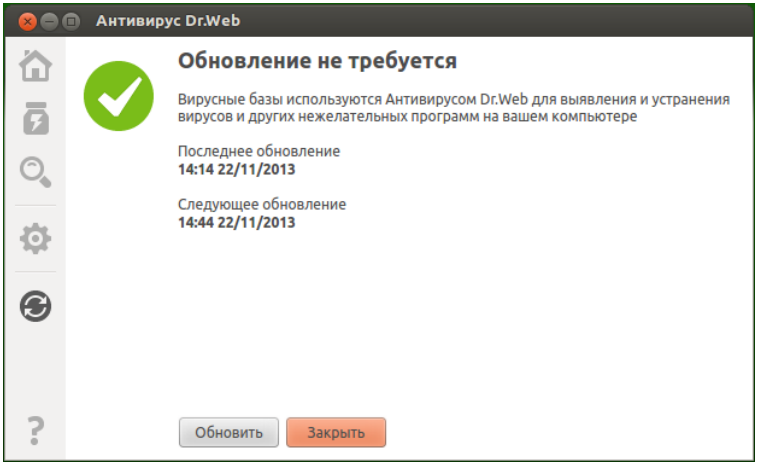

Рисунок 37. Страница управления обновлением

На странице управления обновлением выводится следующая информация:

- Состояние вирусных баз.
- Информация о последнем произведенном обновлении и время следующего планового обновления.

Чтобы выполнить принудительное обновление, следует нажать кнопку **Обновить.** Нажатие кнопки **Закрыть** закрывает страницу управления обновлением.

Если **Антивирус Dr.Web для Linux** работает в режиме централизованной защиты, эта страница будет заблокирована.

Настройка обновлений

Настройка обновлений **Антивируса Dr.Web для Linux** производится на странице настроек, на вкладке **Основные.**

Менеджер лицензий

Менеджер лицензий позволяет просмотреть в графическом режиме информацию о текущей лицензии, которая выдана пользователю **Антивируса Dr.Web для Linux.** Данные лицензии, выданной пользователю, хранятся в лицензионном ключевом файле, обеспечивающем работу **Антивируса** на компьютере пользователя. В случае отсутствия на компьютере лицензионного или демонстрационного ключевого файла все антивирусные функции **Антивируса Dr.Web для Linux** (проверка и мониторинг объектов файловой системы, обновление вирусных баз) будут заблокированы.

Запуск Менеджера лицензий

Менеджер лицензий интегрирован в окно **Антивируса Dr.Web для Linux.** Чтобы открыть страницу **Менеджера лицензий,** необходимо нажать кнопку **Лицензия** на главной странице окна.

Аналогичное действие выполняет кнопка  на навигационной панели (она доступна только в том случае, если страница менеджера лицензий уже ранее была открыта с главной страницы).

В случае если на компьютере имеется ключевой файл, связанный с некоторой лицензией на использование **Антивируса Dr.Web для Linux,** выданной пользователю, или с активным демонстрационным периодом, то на начальной странице **Менеджера лицензий** отображаются данные о лицензии, такие, как ее номер, имя владельца, а также срок действия, извлеченные из ключевого файла.

Вид страницы просмотра данных о лицензии представлен на рисунке ниже.

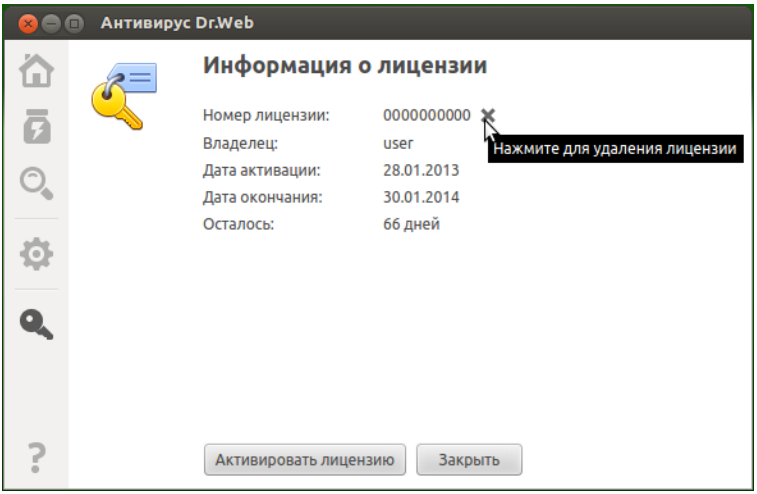

Рисунок 38. Информация о лицензии

Нажатие на символ крестика, изображенный сбоку от номера лицензии, позволяет выполнить удаление ключевого файла.

Вы можете закрыть **Менеджер лицензий** на любом этапе работы с ним, нажав кнопку **Закрыть**, расположенную в нижней части страницы. В этом случае откроется главная страница окна **Антивируса Dr.Web для Linux.**

Активация лицензии

Для того чтобы при помощи **Менеджера лицензий**

активировать лицензию (в том числе – приобрести новую лицензию или продлить текущую) или демонстрационный период, и получить на компьютер соответствующий ключевой файл, обеспечивающий работу **Антивируса Dr.Web для Linux,** необходимо нажать кнопку **Активировать лицензию.** После этого на экране появится мастер регистрации. Обратите внимание, что мастер регистрации отображается также автоматически при первом запуске **Антивируса** после его инсталляции.

На первом этапе активации необходимо выбрать способ активации. Доступно четыре способа:

1. Активация лицензии или демонстрационного периода по имеющемуся серийному номеру;
2. Получение демонстрационного периода;
3. Установка ключевого файла, полученного ранее;
4. Активация **Антивируса** через подключение к серверу централизованной защиты.

Для регистрации серийного номера и для получения демонстрационного периода требуется наличие подключения к сети Интернет.

1) Активация лицензии или демонстрационного периода при помощи серийного номера

Для активации лицензии или демонстрационного периода при помощи имеющегося у вас серийного номера следует выбрать на первом шаге работы мастера регистрации пункт **Активировать лицензию,** после чего ввести в появившееся поле ввода, разделенное на 4 секции, символы имеющегося у вас серийного номера и нажать кнопку **Далее.**

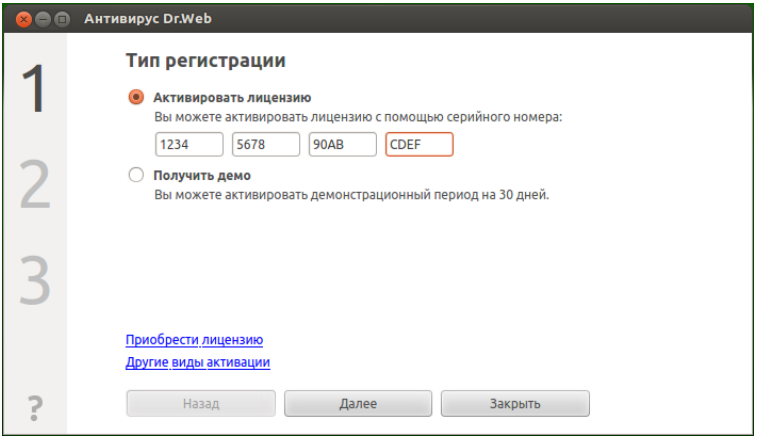

Рисунок 39. Регистрация при помощи серийного номера

Если у вас нет серийного номера или действующего ключевого файла, то вы можете приобрести лицензию в онлайн-магазине компании **«Доктор Веб»,** перейдя по ссылке **Приобрести лицензию.**

О дополнительных способах приобретения лицензии на продукты **Dr.Web** см. в разделе Лицензирование.

После нажатия кнопки **Далее** будет произведено подключение к серверу регистрации компании **«Доктор Веб».**

Если указанный вами серийный номер был получен на сайте компании **«Доктор Веб»** для активации демонстрационного периода сроком на 3 месяца, то дополнительных шагов для активации не потребуется.

Если указанный на первом шаге серийный номер входит в комплект из двух серийных номеров, то далее вам нужно выбрать, на каком количестве компьютеров вы планируете использовать продукт. Если вы выберете вариант **на двух компьютерах,** то второй серийный номер из этого комплекта вы сможете активировать на еще одном компьютере и получить второй лицензионный ключевой файл. При этом для

обоих компьютеров выданные лицензии будут действительны в течение одинакового срока (например, на год). Если же вы выберете вариант **на одном компьютере,** то в появившемся поле (разделено на 4 секции) вам необходимо указать второй серийный номер из комплекта. В дальнейшем вы уже не сможете зарегистрировать этот серийный номер на другом компьютере (также как и использовать на нем копию лицензионого ключевого файла, полученного вами в результате активации объединенной лицензии), но для текущего компьютера срок действия лицензии будет увеличен вдвое (например, до двух лет, если лицензия была выдана сроком на год).

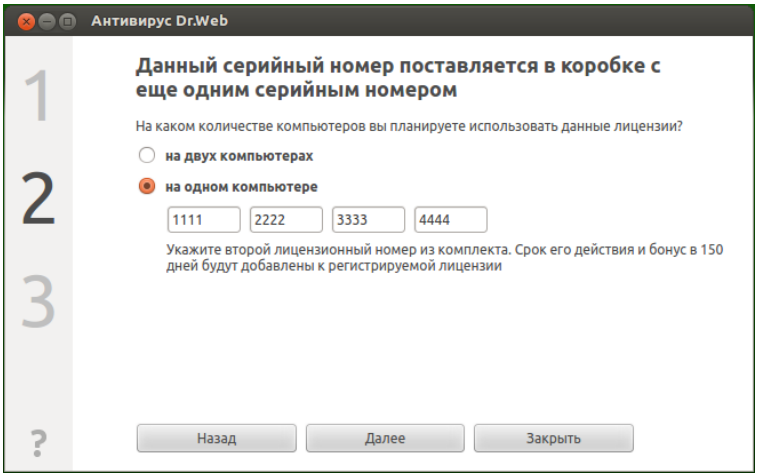

Рисунок 40. Выбор количества компьютеров

После выбора количества компьютеров, для которого может быть активирована лицензия, нажмите кнопку **Далее**.

Далее вам будет предложено получить бонус в 150 дней к сроку действия активируемой лицензии. Для этого будет необходимо указать предыдущую приобретенную вами лицензию, если она у вас имеется.

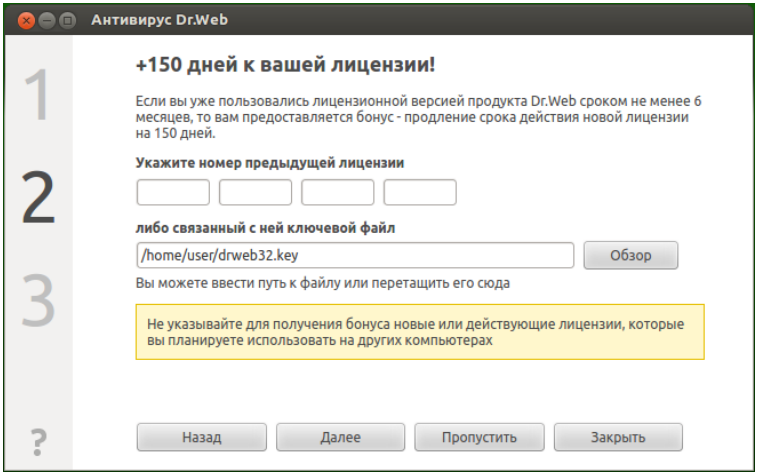

Рисунок 41. Продление лицензии

Если вы укажете на этом шаге лицензию, срок действия которой еще не истек, то срок действия активируемой лицензии будет дополнительно продлен и на остаток срока действия старой лицензии. Вы можете пропустить этот шаг (нажав кнопку **Пропустить**), но в этом случае вы потеряете остаток срока действия старой лицензии, а срок действия активируемой лицензии не будет увеличен. В случае активации комплекта из двух серийных номеров, порядок обработки бонуса зависит от того, какой вариант использования был выбран на предыдущем шаге мастера регистрации:

- **На двух компьютерах,** и это первый компьютер. Для получения бонуса для первого активируемого серийного номера вы должны использовать на данном шаге предыдущую лицензию, выданную для этого компьютера, если она имеется. Второй серийный номер из комплекта здесь указывать нельзя.
- **На двух компьютерах,** и это второй компьютер. Для получения бонуса для второго активируемого серийного номера вы можете использовать на данном шаге серийный номер, активированный на первом компьютере, или предыдущую лицензию, выданную для этого компьютера,

если она имеется.

- **На одном компьютере.** В этом случае не только удваивается срок действия активируемой лицензии, но к нему также автоматически прибавляется бонус (первый серийный номер дает бонус для второго номера). Кроме этого, если вы на данном шаге дополнительно укажете предыдущую лицензию, выданную для этого компьютера, если она имеется, то к удвоенному сроку действия активируемой лицензии также прибавится бонус и остаток срока действия указанной лицензии, если он имеется.

Если вы активируете специальную лицензию продления, то, нажав на этом шаге кнопку **Пропустить,** вы не только потеряете остаток срока действия старой лицензии, но и уменьшите срок действия новой лицензии на 150 дней.

Для указания на предыдущую лицензию можно ввести ее серийный номер в соответствующее поле или указать связанный с ней ключевой файл. Для указания ключевого файла вы можете:

- ввести путь к нему непосредственно в строку ввода;
- воспользоваться стандартным окном выбора файлов графической оболочки, нажав кнопку **Обзор**;
- перетащить его мышью на страницу мастера из окна файлового менеджера.

Обратите внимание, что вместо ключевого файла вы можете указать файл zip-архива, содержащего ключевой файл, распаковки архива при этом не требуется.

После указания предыдущей лицензии, для продолжения регистрации нажмите кнопку **Далее**.

На следующем шаге требуется указать корректную информацию о себе, которая включает следующие данные:

- Регистрационное имя пользователя;
- Регион (страна) нахождения, выбирается из списка;
- Корректный адрес электронной почты.

Все поля регистрационной формы являются обязательными для заполнения. Кроме того, вы можете подписаться на новостную рассылку компании **«Доктор Веб»** (новости будут приходить на указанный при регистрации адрес электронной почты), установив соответствующий флажок.

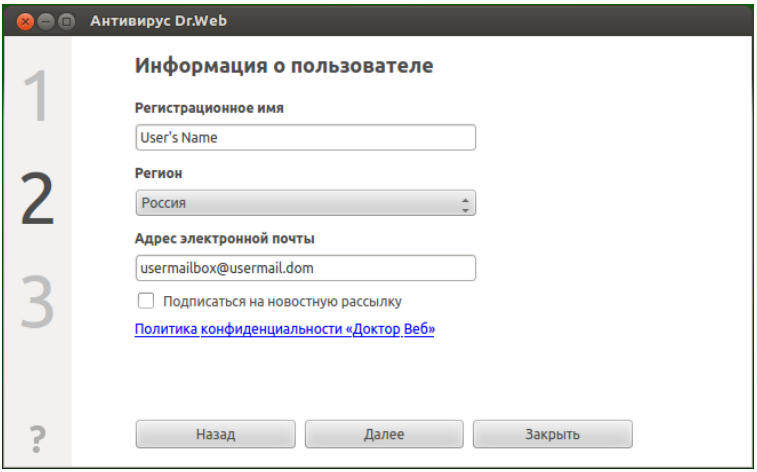

Рисунок 42. Регистрационная информация пользователя

Чтобы ознакомиться с политикой конфиденциальности, которую применяет компания **«Доктор Веб»** в отношении персональной информации пользователя, перейдите по имеющейся на этой странице мастера ссылке **Политика конфиденциальности «Доктор Веб»** (ссылка откроется в браузере).

После корректного заполнения всех полей формы нажмите кнопку **Далее** для подключения к серверу и получения лицензионного ключевого файла (обратите внимание, что тем самым вы одновременно соглашаетесь с политикой конфиденциальности **«Доктор Веб»** в отношении персональной информации пользователя). При необходимости вы сможете перенести полученный лицензионный ключевой файл на любой компьютер при условии, что вы перестанете использовать его на этом компьютере.

2) Получение демонстрационного периода

Если требуется получить демонстрационный период для работы **Антивируса Dr.Web для Linux** в течение 30 дней, выберите пункт **Получить демо** и нажмите кнопку **Далее.**

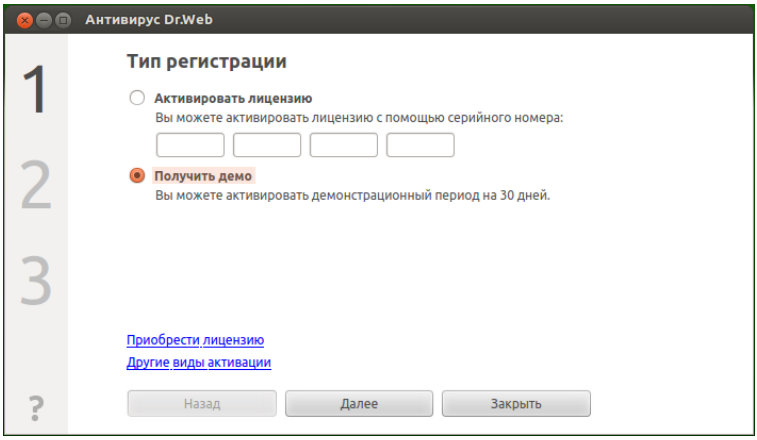

Рисунок 43. Запрос получения демо

При получении демонстрационного периода сроком на 1 месяц через **Менеджер лицензий** вам не требуется указывать свои персональные данные. Однако вы можете зарегистрироваться на официальном сайте компании **«Доктор Веб»** и получить серийный номер, предоставляющий демонстрационный период сроком на 3 месяца.

Демонстрационный период для одного и того же компьютера не может быть выдан чаще, чем 1 раз в год.

Подробнее см. в разделе Лицензирование.

3) Установка имеющегося ключевого файла

Если вы уже имеете действующую лицензию и связанный с ней ключевой файл (возможно, полученный от компании **«Доктор Веб»** или ее партнеров по электронной почте), то вы можете активировать **Антивирус Dr.Web для Linux,** установив этот ключевой файл. Для этого на первом шаге активации

перейдите по ссылке **Другие виды активации,** после чего укажите в появившемся поле ввода путь к имеющемуся у вас ключевому файлу и нажмите кнопку **Далее.**

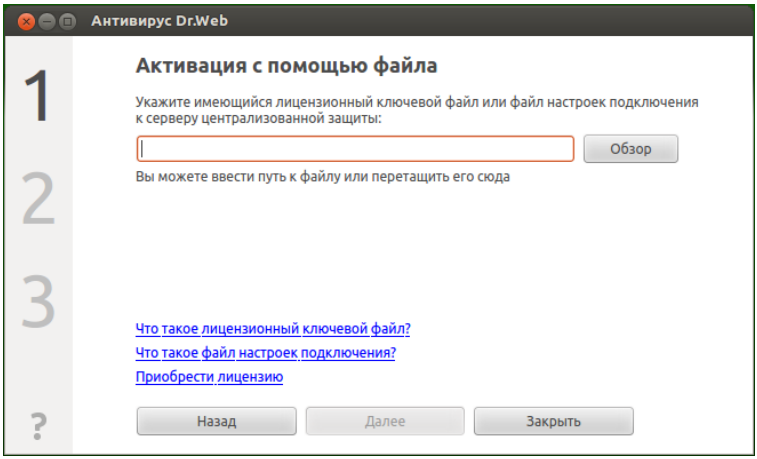

Рисунок 44. Активация с помощью ключевого файла

Обратите внимание, что:

- можно ввести путь к файлу непосредственно в строку ввода;
- можно указать путь к файлу, воспользовавшись стандартным окном выбора файлов графической оболочки, нажав кнопку **Обзор**;
- можно указать путь к файлу, перетащив его мышью на страницу мастера из окна файлового менеджера.

Обратите внимание, что вместо ключевого файла вы можете указать файл zip-архива, содержащего ключевой файл, распаковки архива при этом не требуется.

После указания пути к ключевому файлу (или содержащему его архиву) нажмите кнопку **Далее** для автоматической установки ключевого файла. Ключевой файл будет при необходимости распакован и скопирован в каталог служебных файлов **Антивируса.** Подключения к сети Интернет в данном

случае не требуется.

4) Активация Антивируса через подключение к серверу централизованной защиты

Если ваш провайдер или администратор вашей корпоративной сети предоставили вам файл настроек подключения вашей копии **Антивируса** к серверу централизованной защиты, обеспечивающему централизованное управление антивирусной защитой компьютеров, входящих в сеть, то вы можете активировать **Антивирус** при помощи этого файла, подключив его к серверу защиты. В этом случае сервер защиты сам сформирует для вашего экземпляра **Антивируса** требуемый ключевой файл.

Чтобы выполнить подключение **Антивируса** к серверу централизованной защиты, на первом шаге активации перейдите по ссылке **Другие виды активации,** после чего укажите в появившемся поле ввода путь к предоставленному вам файлу настроек подключения к серверу защиты и нажмите кнопку **Далее.**

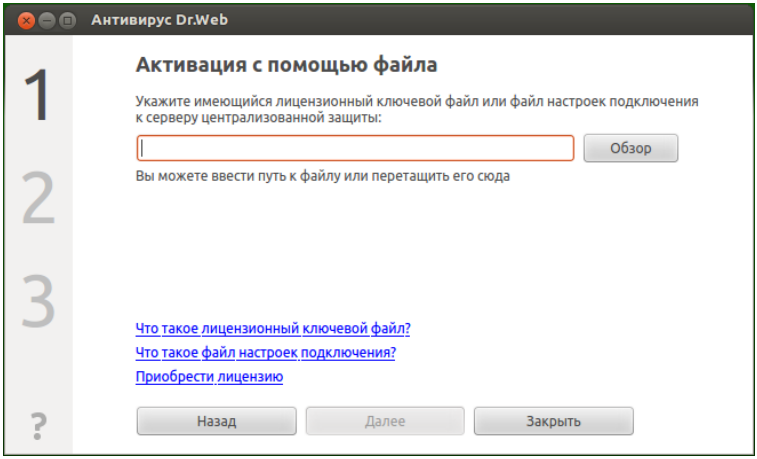

Рисунок 45. Активация с помощью файла настроек подключения

Обратите внимание, что:

- можно ввести путь к файлу непосредственно в строку ввода;
- можно указать путь к файлу, воспользовавшись стандартным окном выбора файлов графической оболочки, нажав кнопку **Обзор**;
- можно указать путь к файлу, перетащив его мышью на страницу мастера из окна файлового менеджера.

Обратите внимание, что вместо файла настроек подключения вы можете указать файл содержащего его zip-архива, распаковки архива при этом не требуется.

После указания пути к файлу настроек подключения (или содержащему его архиву) нажмите кнопку **Далее** для попытки подключения к серверу централизованной защиты (требуется наличие сетевого соединения).

В случае успешного завершения процесса регистрации (любым из описанных выше способов) на экране будет показана финальная страница мастера регистрации с сообщением об успешной регистрации. Нажмите кнопку **Готово** для закрытия мастера регистрации и возвращения на главную страницу окна **Антивируса Dr.Web для Linux.**

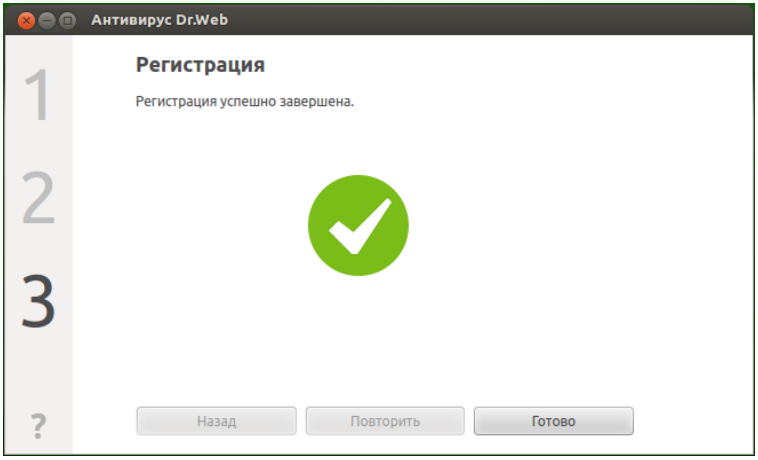

Рисунок 46. Сообщение об успешной регистрации

В случае если на каком-либо из этапов регистрации возникнет ошибка, появится страница с соответствующим сообщением и кратким описанием ошибки. Пример такой страницы показан ниже.

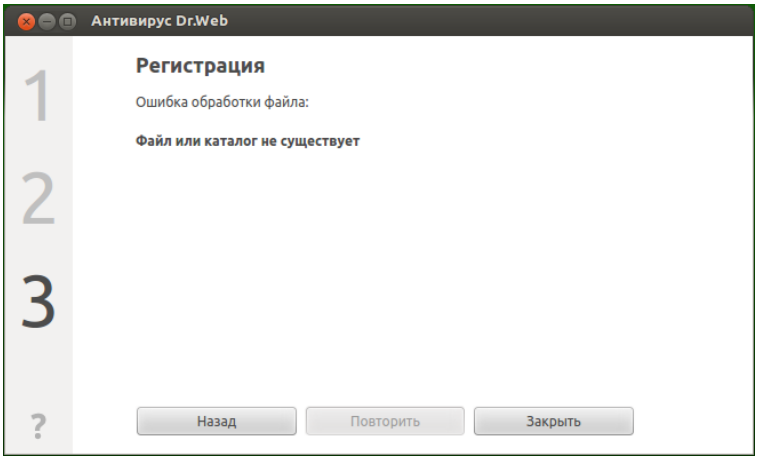

Рисунок 47. Сообщение об ошибке

В этом случае вы имеете возможность вернуться на предыдущий шаг регистрации, чтобы внести исправления (например, исправить серийный номер или указать правильный путь к файлу). Для этого нажмите кнопку **Назад.** В случае если ошибка связана с временной неполадкой, например, временным сбоем в сети, то вы можете попытаться повторить этот шаг, нажав кнопку **Повторить.** В случае необходимости вы можете нажать кнопку **Закрыть,** чтобы прервать регистрацию и закрыть мастер регистрации. В этом случае вам придется позднее повторить процедуру регистрации заново.

В любой момент работы с мастером регистрации вы можете получить доступ к справочным материалам, нажав кнопку  . Кроме того, на некоторых страницах мастера доступны гиперссылки, перейдя по которым, вы получите дополнительную информацию.

Обратите внимание, что при активации новой лицензии и формировании нового ключевого файла, предыдущий ключевой файл, который использовался **Антивирусом,** автоматически сохраняется в виде файла резервной копии в каталоге `/etc/opt/drweb.com`.

В случае необходимости вы можете вернуться к его использованию, выполнив процедуру установки ключевого файла.

Удаление лицензионного ключевого файла

В случае необходимости (например, вы решили больше не использовать **Антивирус Dr.Web для Linux** на этом компьютере, а перенести его на другой компьютер) можно удалить установленный на компьютере лицензионный ключевой файл, управляющий работой **Антивируса.** Для этого необходимо открыть страницу информации о лицензии (начальная страница **Менеджера лицензий**) и кликнуть мышью по символу крестика, расположенному справа от номера текущей лицензии.

После этого вам необходимо в появившемся окне подтвердить удаление лицензионного ключевого файла с данного компьютера. Для этого нажмите кнопку **Да.** Если вы решили отказаться от удаления с данного компьютера лицензионного ключевого файла, нажмите кнопку **Нет.**

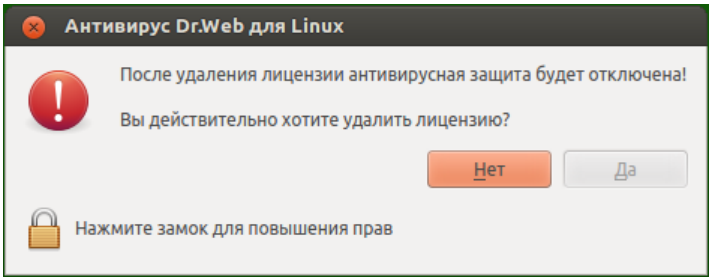

Рисунок 48. Окно подтверждения удаления лицензионного ключевого файла

Для удаления лицензионного ключевого файла приложение должно обладать правами суперпользователя. Если в момент попытки удаления права приложения не повышены, кнопка **Да** будет недоступна. При необходимости вы можете повысить права приложения, и в случае успешного их повышения кнопка **Да** станет доступной.

Удаление с компьютера лицензионного ключевого файла не влияет на срок действия лицензии. Если срок действия лицензии еще не истек, то вы сможете получить новый ключевой файл для этой лицензии на оставшийся срок.

После удаления лицензионного ключевого файла и до момента активации новой лицензии или демонстрационного периода все антивирусные функции **Антивируса Dr.Web для Linux** (проверка файлов, обновление вирусных баз, мониторинг файловой системы) будут заблокированы.

Управление правами приложения

Некоторые действия в окне **Антивируса Dr.Web для Linux** можно выполнить только в том случае, если приложение имеет повышенные права, соответствующие правам специального пользователя системы – суперпользователя (пользователя `root`). В частности, обладания повышенными правами требуют следующие функции:

1. Управление объектами, помещенными в системный **Карантин** (т.е. в каталог **Карантина,** не принадлежащий пользователю, запустившему **Антивирус**);
2. Проверка файлов и каталогов, принадлежащих другим пользователям (в частности – суперпользователю);
3. Выключение монитора файловой системы **SpIDer Guard**;
4. Удаление лицензионного ключевого файла, подключение и отключение от сервера централизованной защиты.

На всех страницах окна **Антивируса Dr.Web для Linux,** функциональность которых зависит от наличия у приложения полномочий суперпользователя, расположена специальная кнопка с изображением замка. Состояние замка показывает, обладает ли в данный момент окно **Антивируса Dr.Web для Linux** правами суперпользователя:

– Приложение не обладает повышенными правами суперпользователя.

Нажатие замка приведет к попытке повышения прав приложения до прав суперпользователя.

– Права приложения повышены до прав суперпользователя.

Нажатие замка приведет к понижению прав приложения, т.е. отказа от прав суперпользователя и возврат к исходным правам пользователя, запустившего приложение.

В случае попытки повышения прав, после нажатия на изображение замка появляется всплывающее меню, предлагающее выбрать метод повышения прав.

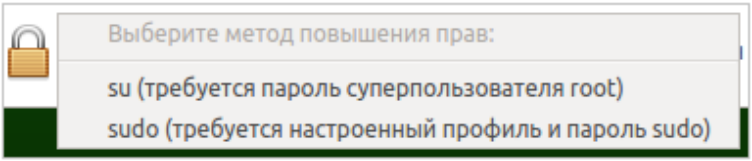

Рисунок 49. Меню повышения прав приложения

Доступны два метода повышения прав – вызов команды смены пользователя **su** или использование настроенного профиля команды **sudo**. При выборе любого из способов повышения прав, в зависимости от настроек, вам может быть показано окно для ввода пароля. При отказе от прав суперпользователя ввода пароля не требуется.

Для повышения привилегий достаточно иметь **su** или **sudo**, а также установленный **xterm**.

Вместо этого рекомендуется установить (если ещё не установлена) одну из утилит повышения прав из графического окружения: **gksu**, **gksudo**, **kdesu**, **kdesudo**, **beesu**, **beesudo**.

В случае если приложение изначально было запущено с правами суперпользователя, то замок всегда находится в разомкнутом состоянии и не доступен для выбора, то есть в этом случае понижение прав приложения невозможно.

Справочные материалы

Для доступа к справочным материалам используйте кнопку  на навигационной панели окна **Антивируса Dr.Web для Linux.**

При нажатии на эту кнопку на экране появляется выпадающее меню, содержащее следующие пункты:

- **Помощь** – открытие краткого Руководства пользователя **Антивируса Dr.Web для Linux**;
- **Официальный форум Dr.Web** – открытие в браузере страницы форума пользователей продуктов компании **«Доктор Веб»** (требуется подключение к сети Интернет);
- **Техническая поддержка** – открытие в браузере страницы службы технической поддержки компании **«Доктор Веб»** (требуется подключение к сети Интернет);
- **Мой Dr.Web** – открытие в браузере персональной страницы пользователя продуктов компании **«Доктор Веб»** (требуется подключение к сети Интернет);
- **О программе** – открытие окна с краткой информацией об **Антивирусе Dr.Web для Linux** и его версии.

Настройка работы

Настройка параметров работы приложения, таких, как:

- Периодичность выполнения обновлений;
- Реакции **Антивируса** на обнаруженные угрозы при проверках по требованию **Сканером** и при обнаружении их монитором файловой системы **SpIDer Guard**;
- Перечень объектов, исключаемых **Сканером** и **SpIDer Gurad** из проверки;
- Расписание периодических проверок объектов **Сканером**;
- Режим защиты (одиночная, централизованная);

выполняется на странице настроек окна **Антивируса Dr.Web для Linux.**

Для доступа к странице настроек необходимо нажать кнопку  на навигационной панели.

На странице настроек доступны следующие вкладки:

- Основные – позволяет настроить использование уведомлений, а также периодичность автоматических обновлений.
- Сканер – позволяет настроить реакцию **Антивируса** на угрозы, обнаруживаемые **Сканером** в процессе проверки по требованию и по расписанию.
- SpIDer Guard – позволяет настроить реакцию **Антивируса** на угрозы, обнаруживаемые монитором файловой системы **SpIDer Guard.**
- Исключения – позволяет настроить список объектов, которые следует исключать из проверки по требованию и по расписанию, а также из перечня объектов, наблюдаемых **SpIDer Guard.**
- Планировщик – позволяет настроить периодический запуск проверок по заданному расписанию.
- Режим – позволяет выбрать режим защиты (одиночная, централизованная), в котором работает **Антивирус Dr.Web для Linux.**

Все изменения, вносимые в настройки, представленные на этих вкладках, применяются немедленно.

Если **Антивирус Dr.Web для Linux** работает в режиме централизованной защиты, то некоторые настройки могут быть заблокированы и недоступны для изменения.

Основные настройки

На вкладке **Основные** вы можете настроить основные параметры работы приложения.

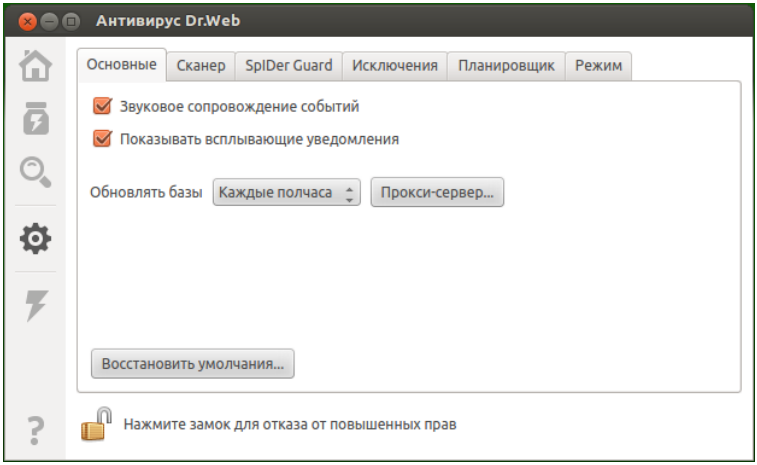

Рисунок 50. Вкладка основных настроек

Элемент управления	Действие
Флажок **Звуковое сопровождение событий**	Установка этого флажка предписывает **Антивирусу** проигрывать звуковые уведомления при возникновении таких событий, как: • Обнаружена угроза (как **Сканером** так и **SpIDer Guard**) • Ошибка проверки объекта • и т.п.
Флажок **Показывать всплывающие уведомления**	Установка этого флажка предписывает **Антивирусу** при работе в режиме графического рабочего стола отображать на экране всплывающие уведомления при возникновении таких событий, как: • Обнаружена угроза • Ошибка проверки • и т.п.
Выпадающий список	Позволяет выбрать периодичность

Элемент управления	Действие
Обновлять базы	автоматического обновления вирусных баз и антивирусного ядра **Модулем обновлений.**
Кнопка **Прокси-сервер...**	Открывает окно настройки использования **Модулем обновлений** прокси-сервера для получения обновлений (использование прокси-сервера может понадобиться в том случае если обращение к внешним серверам запрещено политиками безопасности сети).
Кнопка **Восстановить умолчания...**	Позволяет сбросить настройки в значения по умолчанию.

Для управления параметрами получения обновлений и сброса настроек в значения по умолчанию необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Настройки прокси-сервера, используемого для получения обновлений

В окне настройки использования **Модулем обновлений** прокси-сервера для получения обновлений вы можете настроить следующие параметры:

- Использовать или нет прокси-сервер для получения обновлений;
- Адрес прокси-сервера, который следует использовать для получения обновлений;
- Порт для подключения к прокси-серверу;
- Имя пользователя и пароль, используемые для аутентификации на прокси-сервере.

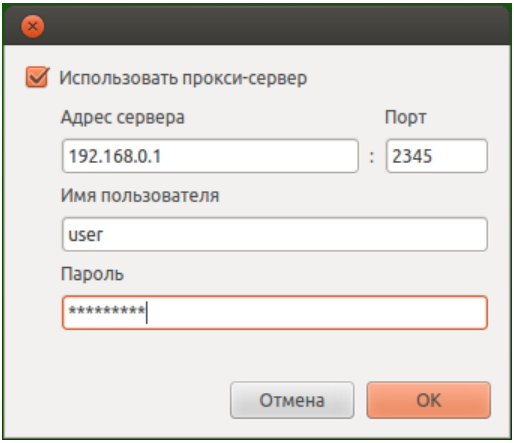

Рисунок 51. Настройки прокси-сервера

Нажатие кнопки **OK** закрывает окно настройки с сохранением внесенных изменений, нажатие кнопки **Отмена** закрывает окно без сохранения внесенных изменений.

Настройки сканирования

На вкладке **Сканер** вы можете настроить действия, которые **Антивирус Dr.Web для Linux** должен применять к угрозам в случае обнаружения их **Сканером** в процессе проверки файлов по требованию пользователя или по расписанию.

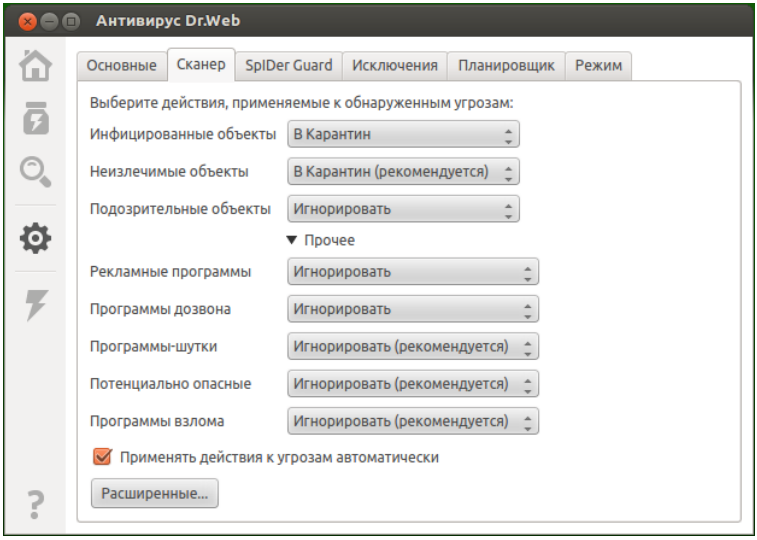

Рисунок 52. Вкладка настроек сканирования

В выпадающих списках следует выбрать действие, которое **Антивирус Dr.Web для Linux** должен применить к объекту в случае обнаружения в нем угрозы определенного типа.

Включение флажка **Применять действия к угрозам автоматически** предписывает **Антивирусу** применять указанное действие к объекту, содержащему угрозу сразу в момент ее обнаружения **Сканером** в ходе проверки по требованию или по расписанию (пользователь будет проинформирован о нейтрализации угрозы, а информация об ней будет доступна в списке угроз). В случае если флажок отключен, угроза, обнаруженная **Сканером,** будет только добавлена в список обнаруженных угроз, в котором пользователю придется самостоятельно выбрать, какое действие к ней следует применить.

Для обеспечения наилучшего уровня безопасности рекомендуется назначить для всех типов угроз действия, отмеченные в списках как рекомендуемые, и оставить включенным флажок **Применять действия к угрозам автоматически.**

Нажатие на кнопку **Расширенные...** открывает окно дополнительных настроек проверки файлов.

Расширенные настройки сканирования

В окне дополнительных настроек проверки вы можете настроить следующие параметры работы **Сканера**:

- Включить и отключить проверку содержимого контейнеров:
  - Архивов;
  - Почтовых файлов;
- Задать ограничение на время проверки одного файла.

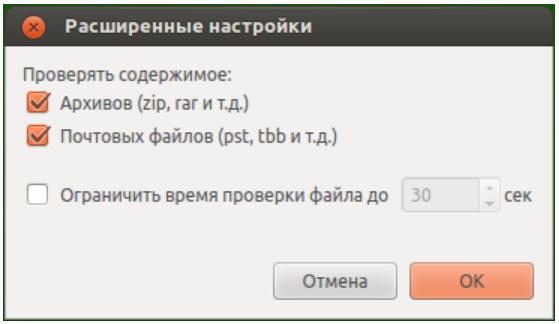

Рисунок 53. Расширенные настройки сканирования

Если флажки проверки содержимого контейнеров не включены, то это означает, что файлы-контейнеры все равно проверяются **Сканером,** но без отдельной проверки вложенных в них файлов.

Нажатие кнопки **OK** закрывает окно настройки с сохранением

внесенных изменений, нажатие кнопки **Отмена** закрывает окно без сохранения внесенных изменений.

Настройки мониторинга

На вкладке **SpIDer Guard** вы можете настроить действия, которые **Антивирус Dr.Web для Linux** должен применять к угрозам в случае обнаружения их монитором файловой системы **SpIDer Guard.**

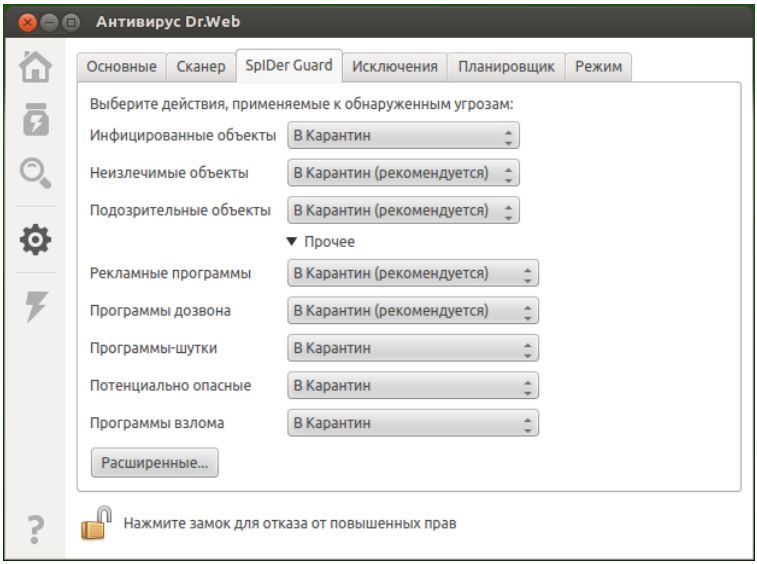

Рисунок 54. Вкладка настроек мониторинга файловой системы

Эта вкладка, включая окно расширенных настроек, аналогична вкладке настроек сканирования.

Для изменения настроек монитора файловой системы **SpIDer Guard** необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Возможность настройки **SpIDer Guard** при работе **Антивируса** под управлением сервера централизованной защиты может быть заблокирована, если это запрещено сервером.

Настройка исключений

На вкладке **Исключения** вы можете указать перечень путей к объектам, которые следует исключать из проверки по требованию пользователя и/или по расписанию, и от наблюдения их монитором файловой системы **SpIDer Guard.**

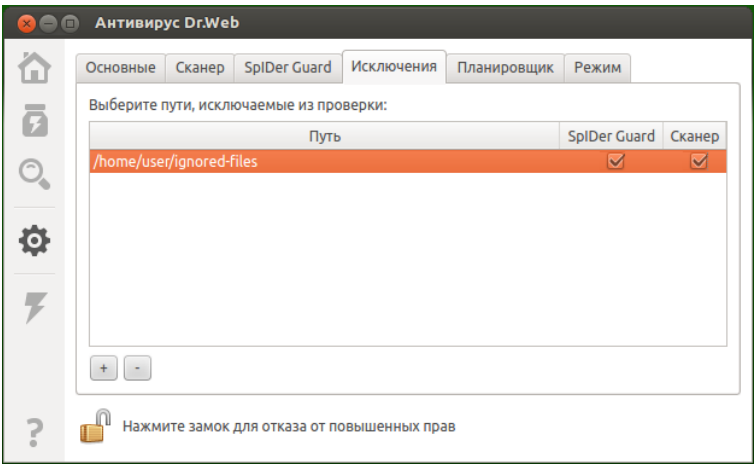

Рисунок 55. Вкладка настройки исключений

Один и тот же объект вы можете добавить в список исключений как для проверки **Сканером** (по запросу и/или по расписанию), так и для наблюдения монитором файловой системы **SpIDer Guard.** Отметка, для какого компонента объект из списка добавлен в исключения, изображается флажком в соответствующем столбце таблицы.

Добавление и удаление объектов из списков исключений

Чтобы добавить объект, присутствующий в списке, в перечень исключаемых объектов для **Сканера** или для **SpIDer Guard,** необходимо включить соответствующий флажок в строке объекта. Чтобы исключить объект, представленный в списке, из перечня объектов исключаемых из проверки **Сканером** или **SpIDer Guard,** необходимо отключить соответствующий флажок в строке объекта.

Чтобы добавить в список новый объект, следует нажать кнопку «+», расположенную под списком объектов, и выбрать объект в появившемся окне выбора каталогов и файлов. Кроме этого, вы можете добавить объекты в этот список, перетащив их мышью из окна файлового менеджера.

Чтобы удалить объект из списка, следует выделить его строчку в списке и нажать кнопку «–», расположенную под списком.

Для добавления и удаления объектов из перечня исключений монитора файловой системы **SpIDer Guard** необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Обратите внимание, что объект нельзя удалить из списка, если он добавлен в перечень исключений для **SpIDer Guard,** и приложение не обладает правами на корректировку этого перечня.

Настройка расписания

На вкладке **Планировщик** вы можете включить использование системного планировщика для автоматического запуска проверки

по расписанию, задать расписание запуска и выбрать тип проверки.

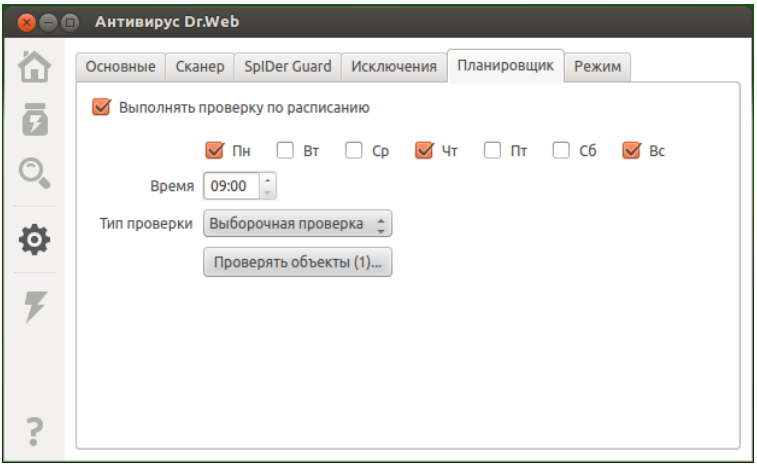

Рисунок 56. Вкладка настройки расписания

Для включения автоматической проверки по расписанию следует включить флажок **Выполнять проверку по расписанию**. В этом случае **Антивирус Dr.Web для Linux** создаст для системного планировщика **cron** задачу периодического запуска проверки.

Проверки по заданному расписанию будут запускаться системным планировщиком **cron** с указанной периодичностью вне зависимости от того, запущен **Антивирус,** или нет.

Если **Антивирус** работает под управлением сервера централизованной защиты, на котором включен запрет на запуск проверки файлов пользователем, то **Сканер** не будет запускать проверки по расписанию, если они настроены.

Для проверок, запускаемых по расписанию, как и для проверок по требованию, действуют настройки проверки, заданные на вкладке **Сканер.**

Настройка проверки по расписанию

Включив проверку по расписанию, вы можете настроить следующие параметры:

- Выбрать дни недели, в которые следует запускать проверку (включив соответствующие флажки);
- Установить время (часы и минуты) начала проверки.
- Задать тип проверки (Быстрая, Полная или Выборочная).
- Для Выборочной проверки по расписанию вы можете задать перечень объектов, подлежащих проверке. Для этого следует нажать кнопку **Проверять объекты...** (в скобках указывается количество объектов, выбранных для проверки по расписанию).

  После этого на экране откроется окно выбора объектов для выборочной проверки объектов по расписанию, аналогичное окну выбора объектов для выборочной проверки по требованию. Вы можете добавить объекты в список, как используя кнопку «+», так и перетаскивая их в список мышью из окна файлового менеджера.

Для отключения автоматической проверки объектов по расписанию следует отключить флажок **Выполнять проверку по расписанию.** Соответствующая задача системного планировщика **cron,** запускающая проверку, будет автоматически удалена.

Настройка режима работы

На вкладке **Режим** вы можете подключить **Антивирус Dr.Web для Linux** к серверу централизованной защиты (переведя его в режим централизованной защиты) или отключиться от сервера централизованной защиты (в этом случае **Антивирус Dr.Web для Linux** будет работать в одиночном режиме).

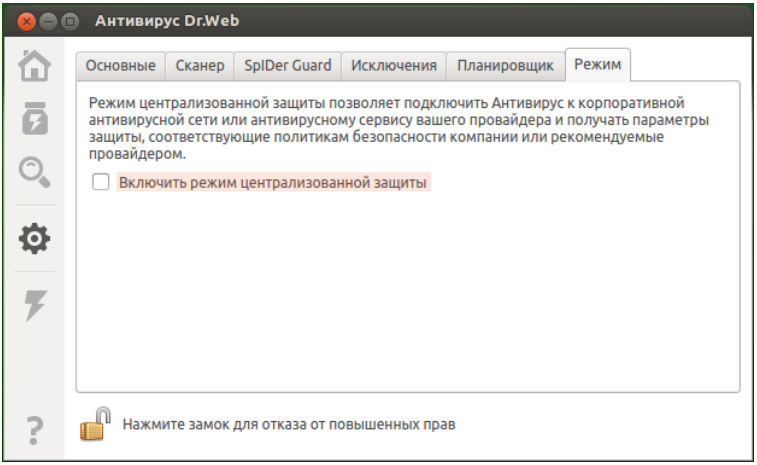

Рисунок 57. Вкладка управления режимом работы

Чтобы подключить **Антивирус Dr.Web для Linux** к серверу централизованной защиты или отключиться от него, используйте соответствующий флажок.

Для подключения **Антивируса Dr.Web для Linux** к серверу централизованной защиты или отключения от него необходимо, чтобы приложение обладало повышенными правами. См. Управление правами приложения.

Подключение к серверу централизованной защиты

При попытке подключения к серверу централизованной защиты на экране появится окно, в котором требуется указать параметры подключения к серверу.

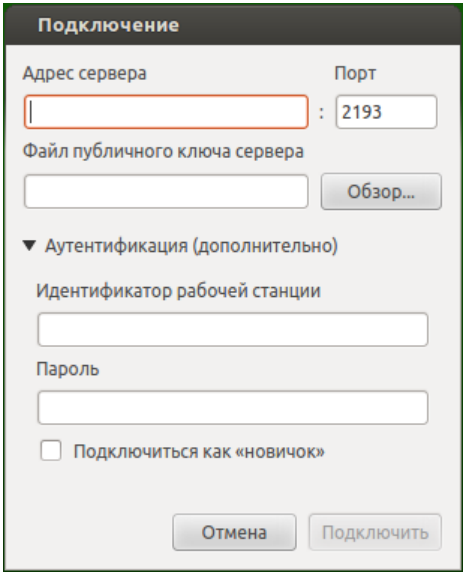

Рисунок 58. Окно подключения к серверу централизованной защиты

Для подключения к серверу централизованной защиты следует указать следующие параметры (они должны быть предоставлены вам администратором антивирусной сети или провайдером):

- Адрес сервера централизованной защиты;
- Порт, используемый для подключения к серверу централизованной защиты;
- Путь к файлу публичного ключа сервера.

Дополнительно, в разделе **Аутентификация,** вы можете указать идентификатор рабочей станции и пароль для аутентификации на сервере, если они вам известны. Если эти поля заполнены, то подключение к серверу будет успешным только при указании правильной пары идентификатор/пароль. Если эти поля оставить пустыми, то подключение к серверу будет успешным только в случае его одобрения на сервере (автоматически или администратором антивирусной сети, в зависимости от настроек

сервера).

Кроме того, вы можете установить флажок **Подключиться как «новичок»**. Если опция «новичок» разрешена на сервере, то после одобрения подключения он автоматически сгенерирует уникальную пару идентификатор/пароль, которая в дальнейшем будет использоваться для подключения вашего компьютера к этому серверу. Обратите внимание, что при подключении как «новичок», новая учетная запись для вашего компьютера будет сгенерирована сервером централизованной защиты даже в том случае, если ранее он уже имел учетную запись на этом сервере.

Для подключения к серверу, после указания всех параметров, следует нажать кнопку **Подключить** и дождаться окончания процесса подключения. Чтобы закрыть окно без подключения к серверу, нажмите кнопку **Отмена.**

После того, как вы подключили **Антивирус Dr.Web для Linux** к серверу централизованной защиты, он будет работать под его управлением до тех пор, пока вы его не отключите. В режиме централизованной защиты подключение к серверу будет происходить автоматически каждый раз при запуске операционной системы. Подробнее см. раздел Режимы работы Антивируса.

Обратите внимание, что если на сервере централизованной защиты включен запрет на запуск проверки файлов пользователем, то страница Проверка окна **Антивируса** будет недоступна. Кроме того, в этом случае **Сканер** не будет запускать проверки по расписанию, если они настроены.

Дополнительно

Аргументы командной строки

Для запуска **Антивируса Dr.Web для Linux** в графическом режиме из командной строки операционной системы используется следующая команда:

```
$ drweb-gui [options]
```

Команда допускает использование следующих параметров:

Короткий вариант	Полный вариант	Аргументы
-h	--help	
Описание: Вывод на экран краткой справки по имеющимся параметрам командной строки и завершение работы модуля.		
-v	--version	
Описание: Вывод на экран информации о версии модуля и завершение работы		
-d	--debug	
Описание: Включение вывода на экран расширенной отладочной информации в процессе работы приложения.		
-t	--tray	
Описание: Запустить приложение свернутым в область системных уведомлений (tray).		

Пример:

```
$ drweb-gui --debug --tray
```

Данная команда запустит **Антивирус Dr.Web для Linux** в графическом режиме с включением вывода расширенной отладочной информации и окном, свернутым в область системных уведомлений (tray).

Работа из командной строки

Антивирус Dr.Web для Linux позволяет осуществлять управление своей работой из командной строки операционной системы, для чего в его состав входит специальная утилита **drweb-ctl**.

Имеется возможность выполнять из командной строки следующие действия:

- Запуск проверки файлов, загрузочных записей дисков и исполняемых файлов активных процессов;
- Запуск обновления вирусных баз.
- Просмотр и изменение параметров конфигурации **Антивируса**.
- Просмотр состояния компонентов программного комплекса и статистики обнаруженных угроз.
- Просмотр **Карантина** и управление его содержимым.
- Подключение к серверу централизованной защиты и отключение от него.

Для того, чтобы команды управления **Антивирусом,** вводимые пользователем, имели эффект, должны быть запущены сервисные компоненты **Антивируса** (по умолчанию они автоматически запускаются при старте операционной системы).

Обратите внимание, что для выполнения некоторых управляющих команд требуются полномочия суперпользователя.

Для получения полномочий суперпользователя используйте команду смены пользователя **su** или команду выполнения от имени другого пользователя **sudo**.

Утилита **drweb-ctl** поддерживает стандартное автодополнение команд управления **Антивирусом**, если функция автодополнения включена в используемой вами командной оболочке. В случае если командная оболочка не поддерживает автодополнение, вы можете настроить ее при необходимости. Для этого обратитесь к справочному руководству по используемому вами дистрибутиву операционной системы.

Формат вызова

1. Формат вызова утилиты управления из командной строки

Утилита управления работой **Антивируса Dr.Web для Linux** имеет следующий формат вызова:

```
$ drweb-ctl [<общие опции> | <команда> [<аргумент>]
[<опции команды>]]
```

Где:

- `<общие опции>` – опции, которые могут быть использованы при запуске без указания команды или для любой из команды. Не являются обязательными для запуска.
- **<команда>** – команда, которая должна быть выполнена **Антивирусом** (например, запустить проверку файлов, вывести содержимое **Карантина** и т.п.).
- `<аргумент>` – аргумент команды. Зависит от указанной команды. У некоторых команд аргументы отсутствуют.
- `<опции команды>` – опции, управляющие работой указанной команды. Зависит от команды. У некоторых команд опции отсутствуют.

2. Общие опции

Доступны следующие общие опции:

Опция	Описание
`-h`, `--help`	Вывести на экран краткую общую справку и завершить работу. Для вывода справки по любой команде используйте вызов: **`drweb-ctl -h <команда>`** или **`drweb-ctl <команда> -h`**
`-v`, `--version`	Вывести на экран версию модуля и завершить работу
`-d`, `--debug`	Предписывает выводить на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов **`drweb-ctl -d <команда>`**

3. Команды

Команды управления **Антивирусом** разделены на следующие группы:

- Команды антивирусной проверки.
- Команды управления обновлением и работой в режиме централизованной защиты.
- Команды управления конфигурацией.
- Команды управления угрозами и **Карантином.**
- Информационные команды.

3.1. Команды антивирусной проверки

Доступны следующие команды антивирусной проверки файловой системы:

Команда	Описание
`scan` `<путь>`	**Назначение:** Инициировать проверку **Сканером** указанного файла или каталога.

Команда	Описание
	Аргументы: `<путь>` – путь к файлу или каталогу, который нужно проверить. Этот аргумент может быть опущен в случае использования опции `--stdin` или `--stdin0`. Для проверки перечня файлов, выбираемых по некоторому условию, рекомендуется использовать утилиту **find** (см. примеры) и опции `--stdin` или `--stdin0`. **Опции:** `-a [--Autonomous]` – запустить отдельную копию антивирусного ядра и **Сканера** для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). `--stdin` – получить список путей для проверки из стандартного потока ввода (stdin). Пути в списке должны быть разделены символом новой строки ('\n'). `--stdin0` – получить список путей для проверки из стандартного потока ввода (stdin). Пути в списке должны быть разделены нулевым символом NUL ('\0'). Обратите внимание, что при использовании обеих этих опций пути в списке не должны содержать шаблонов.

Команда	Описание
	Предпочтительное использование опций `--stdin` и `--stdin0` – обработка в команде **`scan`** списка путей, сформированного внешней утилитой, например, **`find`** (см. примеры). `--Report <BRIEF| DEBUG>` – установить тип отчета о проверке. Возможные значения: • `BRIEF` – краткий отчет. • `DEBUG` – подробный отчет. Значение по умолчанию: `BRIEF` `--ScanTimeout <число>` – установить тайм-аут на проверку одного файла в мс. Значение `0` указывает, что время проверки не ограничено. Значение по умолчанию: `0` `--PackerMaxLevel <число>` – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8` `--ArchiveMaxLevel <число>` – установить максимальный уровень вложенности объектов при проверке архивов (zip, rar и т.п.). Значение `0` указывает, что вложенные объекты будут пропущены. Значение по умолчанию: `8` `--MailMaxLevel <число>` – установить максимальный уровень вложенности объектов при проверке почтовых сообщений (pst, tbb и т.п.).

Команда	Описание
	Значение 0 указывает, что вложенные объекты будут пропущены. Значение по умолчанию: 8 --ContainerMaxLevel <число> – установить максимальный уровень вложенности объектов при проверке прочих контейнеров (HTML и т.п.). Значение 0 указывает, что вложенные объекты будут пропущены. Значение по умолчанию: 8 --MaxCompressionRatio <степень> – установить максимальную допустимую степень сжатия проверяемых объектов. Должна быть не менее 2. Значение по умолчанию: 3000 --HeuristicAnalysis <On| Off> – использовать ли Эвристический анализ. Значение по умолчанию: On --OnKnownVirus <действие> – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: REPORT, CURE, QUARANTINE, DELETE. Значение по умолчанию: REPORT --OnIncurable <действие> – действие, которое следует выполнить в случае если лечение (CURE) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: REPORT, QUARANTINE, DELETE. Значение по умолчанию: REPORT

Команда	Описание
	`--OnSuspicious <действие>` – действие, которое следует выполнить в случае если Эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT, QUARANTINE, DELETE`. Значение по умолчанию: `REPORT` `--OnAdware <действие>` – действие, которое следует выполнить в случае если обнаружена рекламная программа. Возможные действия: `REPORT, QUARANTINE, DELETE`. Значение по умолчанию: `REPORT` `--OnDialers <действие>` – действие, которое следует выполнить в случае если обнаружена программа дозвона. Возможные действия: `REPORT, QUARANTINE, DELETE`. Значение по умолчанию: `REPORT` `--OnJokes <действие>` – действие, которое следует выполнить в случае если обнаружена шуточная программа. Возможные действия: `REPORT, QUARANTINE, DELETE`. Значение по умолчанию: `REPORT` `--OnRiskware <действие>` – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа. Возможные действия: `REPORT, QUARANTINE, DELETE`. Значение по умолчанию: `REPORT`

Команда	Описание
	`--OnHacktools <действие>` – действие, которое следует выполнить в случае если обнаружена программа взлома. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`
bootscan `<устройство> | ALL`	**Назначение:** Инициировать проверку **Сканером** загрузочной записи на указанных дисковых устройствах. Проверяются как записи MBR, так и записи VBR. **Аргументы:** `<устройство>` – путь к блочному файлу дискового устройства, загрузочная запись на котором подлежит проверке. Может быть указано несколько дисковых устройств через пробел. Если вместо файла устройства указано `ALL`, будут проверены все загрузочные записи на всех доступных дисковых устройствах. Обязательный аргумент. **Опции:** `-a [--Autonomous]` – запустить отдельную копию антивирусного ядра и **Сканера** для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой `threats` (см. ниже). `--Report <BRIEF| DEBUG>` – установить тип отчета о проверке. Возможные значения:

Команда	Описание
	• BRIEF – краткий отчет. • DEBUG – подробный отчет. Значение по умолчанию: BRIEF --ScanTimeout <число> – установить тайм-аут на проверку одного файла в мс. Значение 0 указывает, что время проверки не ограничено. Значение по умолчанию: 0 --HeuristicAnalysis <On| Off> – использовать ли Эвристический анализ. Значение по умолчанию: On --Cure <Yes| No> – требуется ли делать попытки лечения обнаруженных угроз. Если указано no, то производится только информирование об обнаруженной угрозе. Значение по умолчанию: No --ShellTrace – включить вывод дополнительной отладочной информации при проверке загрузочной записи.
procscan	**Назначение:** Инициировать проверку **Сканером** содержимого исполняемых файлов, содержащих код процессов, запущенных в системе. **Аргументы:** Нет. **Опции:**

Команда	Описание
	-a [--Autonomous] – запустить отдельную копию антивирусного ядра и **Сканера** для выполнения заданной проверки, завершив их работу после окончания проверки. Обратите внимание, что угрозы, обнаруженные при автономном сканировании, не будут добавлены в общий список обнаруженных угроз, выводимый командой threats (см. ниже). --Report <BRIEF| DEBUG> – установить тип отчета о проверке. Возможные значения: • BRIEF – краткий отчет. • DEBUG – подробный отчет. Значение по умолчанию: BRIEF --ScanTimeout <число> – установить тайм-аут на проверку одного файла в мс. Значение 0 указывает, что время проверки не ограничено. Значение по умолчанию: 0 --HeuristicAnalysis <On| Off> – использовать ли Эвристический анализ. Значение по умолчанию: On --PackerMaxLevel <число> – установить максимальный уровень вложенности объектов при проверке запакованных объектов. Значение 0 указывает, что вложенные объекты будут пропущены. Значение по умолчанию: 8

Команда	Описание
	`--OnKnownVirus <действие>` – действие, которое следует выполнить в случае если методами сигнатурного анализа обнаружена известная угроза. Возможные действия: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnIncurable <действие>` – действие, которое следует выполнить в случае если лечение (`CURE`) обнаруженной угрозы окончилось неудачей или оно невозможно. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnSuspicious <действие>` – действие, которое следует выполнить в случае если Эвристический анализ обнаружит подозрительный объект. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnAdware <действие>` – действие, которое следует выполнить в случае если обнаружена рекламная программа. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT` `--OnDialers <действие>` – действие, которое следует выполнить в случае если обнаружена программа дозвона. Возможные действия: `REPORT`, `QUARANTINE`, `DELETE`. Значение по умолчанию: `REPORT`

Команда	Описание
	`--OnJokes <действие>` – действие, которое следует выполнить в случае если обнаружена шуточная программа. Возможные действия: `REPORT, QUARANTINE, DELETE.` Значение по умолчанию: `REPORT` `--OnRiskware <действие>` – действие, которое следует выполнить в случае если обнаружена потенциально опасная программа. Возможные действия: `REPORT, QUARANTINE, DELETE.` Значение по умолчанию: `REPORT` `--OnHacktools <действие>` – действие, которое следует выполнить в случае если обнаружена программа взлома. Возможные действия: `REPORT, QUARANTINE, DELETE.` Значение по умолчанию: `REPORT` Обратите внимание, что при обнаружении угроз в исполняемом файле все запущенные из него процессы принудительно завершаются **Антивирусом.**

3.2. Команды управления обновлением и работой в режиме централизованной защиты

Доступны следующие команды управления обновлением и работой в режиме централизованной защиты:

Команда	Описание
`update`	**Назначение:**

Команда	Описание
	Инициировать процесс обновления **Модулем обновлений** вирусных баз и антивирусного ядра с серверов обновлений **ВСО Dr.Web,** или прервать уже запущенный процесс обновления. Команда не имеет эффекта, если **Антивирус** работает под управлением сервера централизованной защиты. **Аргументы:** Нет. **Опции:** `--Stop` – прервать уже идущий процесс обновления.
esconnect `<сервер>[:порт]`	**Назначение:** Подключить **Антивирус Dr.Web для Linux** к указанному серверу централизованной защиты (например, **Dr.Web Enterprise Server**) и перевести его в режим централизованной защиты. О режимах работы **Антивируса** см. в разделе Режимы работы Антивируса. **Аргументы:** • `<сервер>` – IP-адрес или имя хоста в сети, на котором располагается сервер централизованной защиты. Обязательный аргумент. • `<порт>` – номер порта, используемого сервером централизованной защиты. Необязательный аргумент, указывается только в случае, если сервер централизованной защиты использует нестандартный порт). **Опции:**

Команда	Описание
	`--Key <путь>` – путь к файлу публичного ключа сервера централизованной защиты, к которому производится подключение. Обратите внимание, что это обязательный параметр! `--Login <ID>` – логин (идентификатор рабочей станции) для подключения к серверу централизованной защиты. `--Password <пароль>` – пароль для подключения к серверу централизованной защиты. `--Compress <On| Off>` – разрешить сжатие передаваемых данных. Значение по умолчанию: `Off` `--Encrypt <On| Off>` – разрешить шифрование передаваемых данных. Значение по умолчанию: `Off` `--Newbie` – подключиться как «новичок» (получить новую учетную запись на сервере). Обратите внимание, что для выполнения этой команды требуется, чтобы **`drweb-ctl`** была запущена от имени суперпользователя.
`esmobile`	**Назначение:** Перевести **Антивирус Dr.Web для Linux**, находящийся в режиме централизованной защиты, в мобильный режим, или выполнить возврат из мобильного режима в режим централизованной защиты. Команда не имеет смысла, если **Антивирус** находится в автономном режиме. **Аргументы:** Нет. **Опции:**

Команда	Описание
	`--Disable` – выполнить возврат из мобильного режима в режим централизованной защиты.
`esdisconnect`	**Назначение:** Отключить **Антивирус Dr.Web для Linux** от сервера централизованной защиты и перевести его в автономный режим работы. Команда не имеет смысла, если **Антивирус** находится в автономном режиме. **Аргументы:** Нет. **Опции:** Нет. Обратите внимание, что для выполнения этой команды требуется, чтобы **`drweb-ctl`** была запущена от имени суперпользователя.

3.3. Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
`cfset` `<секция>.<параметр> <значение>`	**Назначение:** Изменить активное значение указанного параметра текущей конфигурации. Обратите внимание, что знак равенства не используется. **Аргументы:** • `<секция>` – имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент.

Команда	Описание
	• <параметр> – имя изменяемого параметра. Обязательный аргумент. • <значение> – значение, которое следует присвоить изменяемому параметру. Обязательный аргумент. Для задания значения параметров всегда используется формат <секция>.<параметр> <значение> Описание конфигурационного файла доступно в документации man drweb.ini(5). **Опции:** -a [--Add] – не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). -e [--Erase] – не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). -r [--Reset] – сбросить параметр в значение по умолчанию. <значение> в этом случае в команде не указывается, а если указано – игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе – список значений) заменяется на указанное значение.

Команда	Описание
	Для опции `-r` предусмотрен также особый синтаксис вызова команды **cfset**: **cfset** <секция>.* -r В этом случае все параметры указанной секции сбрасываются в значения по умолчанию. Обратите внимание, что для выполнения этой команды требуется, чтобы **drweb-ctl** была запущена от имени суперпользователя.
cfshow [<секция>][.<параметр>]	**Назначение**: Вывести на экран параметры текущей конфигурации программного комплекса. Для вывода параметров по умолчанию используется формат <секция>.<параметр> = <значение>. Секции и параметры не установленных компонентов по умолчанию не выводятся. **Аргументы**: • <секция> – имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла.

Команда	Описание
	• <параметр> – имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла. **Опции**: --Uncut – вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. В противном случае выводятся только те параметры, которые используются имеющимися компонентами. --Ini – вывести значения параметров в формате INI-файла: сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции, перечисляются в виде пар <параметр> = <значение> (по одному в строке).

3.4. Команды управления угрозами и Карантином

Доступны следующие команды управления угрозами и **Карантином**:

Команда	Описание
threats [<действие> <объект>]	**Назначение**:

Команда	Описание
	Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. **Аргументы:** Нет. **Опции:** `-f [--Follow]` – выполнять ожидание поступления новых сообщений об угрозах и выводить их сразу, как только они будут поступать (**^C** прерывает ожидание). `--Cure <список угроз>` – выполнить попытку лечения перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Quarantine <список угроз>` – выполнить перемещение в **Карантин** перечисленных угроз (идентификаторы угроз перечисляются через запятую) `--Delete <список угроз>` – выполнить удаление перечисленных угроз (идентификаторы угроз перечисляются через запятую). `--Ignore <список угроз>` – игнорировать перечисленные угрозы (идентификаторы угроз перечисляются через запятую). Если требуется применить данную команду ко всем обнаруженным угрозам, вместо `<список угроз>` следует указать `all`.

Команда	Описание
	Например, команда **drweb-ctl** threats --Quarantine all перемещает в **Карантин** все обнаруженные объекты с угрозами.
quarantine [<действие> <объект>]	**Назначение**: Применить действие к указанному объекту, находящемуся в **Карантине.** Если действие не указано, то вывести на экран информацию об объектах, находящихся в **Карантине,** с указанием их идентификаторов и краткой информации об исходных файлах, перемещенных в **Карантин.** **Аргументы**: Нет. **Опции**: --Delete <объект> – удалить указанный объект из **Карантина.** Обратите внимание, что удаление из **Карантина** – необратимая операция. --Restore <объект> – восстановить указанный объект из **Карантина** в исходное место. В качестве <объект> используется идентификатор объекта в **Карантине.** Если требуется применить данную команду ко всем объектам, находящимся в **Карантине,** вместо <объект> следует указать all. Например, команда **drweb-ctl** quarantine --Restore all

Команда	Описание
	восстанавливает из **Карантина** все имеющиеся в нем объекты.

3.5. Информационные команды

Доступны следующие информационные команды:

Команда	Описание
`appinfo`	**Назначение**: Вывести на экран информацию о работающих модулях **Антивируса.** **Аргументы**: Нет. **Опции**: `-f [--Follow]` – выполнять ожидание поступления новых сообщений об изменении состояния модулей и выводить их на экран сразу, как только они будут поступать (**^C** прерывает ожидание).
`baseinfo`	**Назначение**: Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. **Аргументы**: Нет. **Опции**: Нет.
`license`	**Назначение**: Вывести на экран информацию об активной лицензии. **Аргументы**: Нет. **Опции**: Нет.

Примеры использования

Примеры использования утилиты **drweb-ctl**:

1) Запустить проверку каталога `/home` с параметрами по умолчанию:

```
$ drweb-ctl scan /home
```

2) Выполнить проверку списка путей, перечисленных в файле `daily_scan` (по одному пути в строке файла):

```
$ drweb-ctl scan --stdin < daily_scan
```

3) Запустить проверку загрузочной записи на диске **sda**:

```
$ drweb-ctl bootscan /dev/sda
```

4) Вывести на экран все параметры из секции `[Root]` активной конфигурации:

```
$ drweb-ctl cfshow Root
```

5) Задать значение `'No'` для параметра **Start** из секции `[LinuxSpider]` (это приведет к остановке работы **SpIDer Guard** – монитора файловой системы **Linux**):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Обратите внимание на то, что в данном случае требуются полномочия суперпользователя. Пример вызова этой же команды с использованием **sudo** для временного повышения полномочий:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

Примеры использования утилиты **find** для формирования выборки файлов, подлежащих проверке (команда **drweb-ctl** `scan --stdin`):

1) Проверить все файлы всех каталогов, начиная с корневого, находящихся на одном разделе файловой системы:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

2) Проверить все файлы всех каталогов, начиная с корневого, кроме файлов, находящихся в каталогах `/var/log/messages` и `/var/log/syslog`:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog | drweb-ctl scan -stdin
```

3) Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователю `root`:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

4) Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям `root` и `admin`:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

5) Проверить во всех каталогах, начиная с корневого, файлы, принадлежащие пользователям с `UID` из диапазона `1000 - 1005`:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

6) Проверить файлы во всех каталогах, начиная с корневого, но находящихся не более чем на пятом уровне вложенности относительно корневого каталога:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

7) Проверить файлы в корневом каталоге, не заходя во вложенные каталоги:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

8) Проверить файлы во всех каталогах, начиная с корневого, при этом следовать по встречающимся символическим ссылкам:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

9) Проверить файлы во всех каталогах, начиная с корневого, при этом не следовать по встречающимся символическим ссылкам:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

10) Проверить во всех каталогах, начиная с корневого, файлы, созданные не позже, чем 03.07.2013:

```
$ find / -type f -newermt 2013-07-03 | drweb-ctl scan --stdin
```

Приложения

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 также могут нанести вред пользователю.

В продуктах и документации компании **«Доктор Веб»** 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 **«Доктор Веб»** 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 инфицированному файлу;
- **макро-вирусы** инфицируют документы, которые используют программы из пакета **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 инфицируют 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** инфицируют 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 инфицировании, что затрудняет его обнаружение 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 инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, 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 языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т.д.) и по инфицируемым ими операционным системам.

Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии, но при этом они не инфицируют 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 **«Доктор Веб»** 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 **«Доктор Веб»** 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** переопределяют 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, брандмауэрах) 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. Файлы, содержащие подозрительные объекты, рекомендуется помещать в **Карантин,** а также их следует отправлять на анализ специалистам **Вирусной лаборатории компании «Доктор Веб».**

Приложение Б. Устранение компьютерных угроз

Все антивирусные продукты, разработанные компанией **Dr.Web**, применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. Сигнатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в **Вирусных базах Dr.Web** составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология **Dr.Web**, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы заражения и нанесения ущерба. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения **Dr.Web** от таких угроз, как троянская программа-вымогатель **Trojan.Encoder.18** (также известная под названием **gpcode**). Кроме того, использование технологии

Origins Tracing™ позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи **Origins Tracing™,** добавляется постфикс . `Origin`.

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 и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (буфером эмуляции). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

Работа эвристического анализатора основывается на наборе эвристик (предположений, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного и, наоборот, безопасного исполняемого кода. Каждый признак кода имеет определенный вес (т.е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию **FLY-CODE™** – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о

наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта **Dr.Web**, но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов **Dr.Web** используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты **Антивирусной Лаборатории Dr.Web** обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту **Dr.Web**, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

Действия с угрозами

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:

- **Ignore (Игнорировать, Пропустить)** – Пропустить обнаруженную угрозыу, не предпринимая никаких действий;

- **Report (Информировать)** – Уведомить о наличии угрозы, но ничего не делать с инфицированным объектом;
- **Cure (Лечить)** – Попытаться вылечить инфицированный объект, удалив из него вредоносное содержимое, и оставив в целости полезное содержимое. Обратите внимание, что это действие применимо не ко всем видам угроз;
- **Quarantine (Переместить в Карантин, Изолировать)** – Переместить инфицированный объект (если он допускает эту операцию) в специальный каталог **Карантина** с целью его изоляции;
- **Delete (Удалить)** – Безвозвратно удалить инфицированный объект.

Приложение В. Техническая поддержка

Страница службы технической поддержки компании **«Доктор Веб»** 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/;
- 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 представительство компании **«Доктор Веб»** и всю информацию, необходимую пользователю, вы можете по адресу http://company.drweb.com/contacts/moscow.