



Dr.WEB®
Enterprise Security Suite

Защити созданное

Dr.Web® для файловых серверов Windows

Версия 8.0

Методическое пособие для практических занятий по курсу DWCERT-003

«Защита файловых серверов на базе антивирусного решения Dr.Web для файловых серверов Windows»

Версия программного обеспечения 8.0

Версия документа 1.0

Дата последнего изменения 28 апреля 2014 года

Внимание! Материалы, представленные в настоящем документе, являются собственностью ООО «Доктор Веб». Защита авторских прав на данный документ осуществляется в соответствии с текущим законодательством РФ. Ни одна из частей данного документа не может быть сфотографирована, размножена или распространена другим способом без согласия ООО «Доктор Веб». Если вы собираетесь использовать, копировать или распространять материалы настоящего курса, свяжитесь, пожалуйста, с представителями ООО «Доктор Веб» через специальную форму, расположенную на официальном сайте: <http://support.drweb.com/new/feedback>

Dr.Web®, SpIDer Guard®, SpIDer Mail®, Dr.Web CureIt! и логотип Dr.WEB — зарегистрированные товарные знаки ООО «Доктор Веб» в России и/или других странах.

Другие названия продуктов, упоминаемые в тексте курса, являются товарными знаками или зарегистрированными товарными знаками соответствующих фирм.

Ограничение ответственности

Ни при каких обстоятельствах Dr.Web® и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Возможности Dr.Web для файловых серверов Windows не ограничиваются функционалом, описанным в данном документе. Для ознакомления с возможностями решения используйте документацию к продуктам.

Внимание! В программные продукты, выпускаемые ООО «Доктор Веб», могут вноситься изменения, не отраженные в данном документе. Со всеми изменениями, вносимыми в программные продукты ООО «Доктор Веб», можно ознакомиться на сайте: <http://www.drweb.com>.

Содержание

1. Введение.....	4
2. Требования к специалисту, изучающему курс.....	4
3. Назначение продукта	5
4. Получение дистрибутива и документации устанавливаемого продукта	7
5. Установка продукта.....	11
5.1. Установка из командной строки.....	11
5.2. Установка с помощью мастера	11
6. Удаление продукта.....	19
7. Проверка работоспособности продукта.....	20
8. Знакомство с Dr.Web для файловых серверов Windows.....	21
9. Задание настроек с Dr.Web для файловых серверов Windows	25
10. Обновление продукта	27
10.1. Проверка актуальности обновлений.....	29
10.2. Проведение обновлений вручную	30
10.3. Настройка обновлений.....	32
10.4. Настройки, которые можно задать только в командной строке.....	36
11. Продление лицензии. Замена ключевого файла.....	38
11.1. Замена ключевого файла.....	38
12. Настройка параметров постоянной антивирусной защиты	39
12.1. Настройка файлового сторожа	39
12.2. Настройки, которые можно задать только в реестре	46
12.3. Настройки Dr.Web Scanning Engine.....	48
12.4. Антируткит Dr.Web.....	49
12.5. Превентивная защита. Защита от неизвестных угроз.....	50
13. Антивирусная проверка.....	52
13.1. Проверка с правами другого пользователя	55
14. Управление Карантином.....	56
15. Управление антивирусной защитой удаленного компьютера.....	57
16. Включение и отключение самозащиты.....	58
17. Создание отчета.....	60
18. Перевод антивирусного решения в режим централизованно управляемой защиты.....	61
19. Приложение 1. «Мой Dr.Web» — личный кабинет пользователя.....	62
20. Приложение 2. Получение услуг службы технической поддержки.....	63
20.1. Запрос в службу технической поддержки	63
20.2. Сбор информации о системе	68
20.3. Отсылка образцов на анализ	69
21. Приложение 3. Работа со справкой о программе.....	69
22. Приложение 4. Поисковый модуль Dr.Web	71

1. Введение

Данный документ содержит сведения, описывающие:

- детали реализации комплексной антивирусной защиты серверов компании с помощью Dr.Web для файловых серверов Windows.

Обращаем ваше внимание, что данный документ не содержит сведений о следующем:

- общие принципы организации антивирусной защиты,
- основные угрозы в области информационной безопасности,
- принципы выбора мер и средств защиты на основе анализа актуальности угроз безопасности.

Актуальные пути реализации современных вредоносных угроз, а также необходимые меры, позволяющие предотвратить реализацию данных угроз, описаны в курсе DWCERT-070-3 «Антивирусная система защиты предприятия».

Внимание! Сдача экзамена по курсу DWCERT-007 «Централизованно управляемая защита банкоматов, терминалов и иных встраиваемых систем на базе решения Dr.Web ATM Shield» возможна только после сдачи экзамена по курсу DWCERT-070-3 «Антивирусная система защиты предприятия».

В данном пособии описаны основные возможности решения Dr.Web для файловых серверов Windows, входящие в него компоненты, а также последовательности шагов по выполнению наиболее распространенных действий по настройке продукта, контролю его состояния и поддержанию безопасного состояния защищаемого им сервера.

Все разделы снабжены иллюстрациями, с помощью которых администратор может легко освоить продукт и выполнять все необходимые ему задачи. Информации, приведенной в пособии, достаточно, чтобы разобраться в настройках продукта с нуля.

Внимание! В настоящем пособии описаны только самые важные возможности и настройки Dr.Web для файловых серверов Windows, наиболее часто использующиеся процедуры выполнения действий. Полная информация о возможностях продукта приведена в документации на него.

Внимание! Перед прочтением документа убедитесь, что это последняя версия. Актуальную версию можно найти на официальном веб-сайте компании «Доктор Веб» <http://download.drweb.com/esuite>, а также в разделе <https://training.drweb.com/external>.

Данный документ адресован *администратору антивирусной сети* — сотруднику организации, которому поручено руководство антивирусной защитой компьютеров (рабочих станций и серверов) этой сети.

Администратор антивирусной сети должен иметь полномочия системного администратора или сотрудничать с администратором локальной сети, быть компетентным в вопросах стратегии антивирусной защиты и детально знать антивирусные пакеты **Dr.Web** для всех используемых в сети ОС.

Ряд начальных глав будет полезен руководителю организации, принимающему решение о приобретении и установке системы комплексной антивирусной защиты.

2. Требования к специалисту, изучающему курс

Предполагается, что обучающийся обладает следующими знаниями и навыками:

- базовые знания по установке, подключению и использованию компьютерной техники;
- знания и практические навыки администрирования локальных сетей на базе ОС Windows Server версий 2000/2003/2008/2012;
- знакомство с документацией по продукту Dr.Web® для файловых серверов Windows версия 8.0.

3. Назначение продукта

Dr.Web для файловых серверов Windows обеспечивает многоуровневую защиту всех компонентов защищаемых серверов: системной памяти, жестких дисков и сменных носителей от проникновений вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов из любых внешних источников.

Важной особенностью программы Dr.Web для файловых серверов Windows является модульная архитектура. Dr.Web для файловых серверов Windows использует программное ядро и вирусные базы, общие для всех программных продуктов компании «Доктор Веб», на какой бы платформе они ни работали. Во многом именно благодаря этому продукты Dr.Web позволяют организовать эффективную антивирусную защиту в различных операционных системах, на базе различных платформ — эффективную не только по качеству защиты, но и с точки зрения минимизации системных требований и затрат на сопровождение.

Dr.Web Для файловых серверов Windows предлагает пользователю комплекс настроек компонентов, с помощью которых можно защитить файловую систему:

- **Сканер Dr.Web** — антивирусный сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера.
- **SpIDer Guard** — антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку файлов и памяти «на лету», а также обнаруживая проявления вирусной активности.

Dr.Web для файловых серверов Windows использует удобные и эффективные механизмы обновления вирусных баз и используемых компонентов программного обеспечения, что делает незаметной всю процедуру обновления и снижает до нуля необходимость вмешательства в нее конечного пользователя, избавляя его от «головной боли» необходимости контроля за антивирусом.

Для обнаружения вредоносных объектов в Dr.Web для файловых серверов Windows используются уникальные технологии, многие из которых не имеют аналогов.

- **Сигнатурный анализ.** Выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов — соответствия признакам, позволяющим идентифицировать тот или иной вирус. Вирусные базы Dr.Web составлены так, что, имея одну запись, можно обнаруживать целые классы угроз.

Заблуждение

Антивирусы ловят вирусы по сигнатурам (записям в вирусных базах) — если бы это было так, антивирус был бы беспомощен перед лицом **неизвестных** угроз.

Однако антивирус не перестал быть лучшим и **единственным** эффективным средством защиты от всех типов вредоносных угроз — и что особенно важно — как **известных**, так и **неизвестных** вирусной базе антивируса — в продуктах Dr.Web для обнаружения и обезвреживания неизвестного вредоносного ПО применяется множество эффективных несигнатурных технологий, сочетание которых позволяет обнаруживать новейшие (неизвестные) угрозы до внесения записи в вирусную базу.

- **Традиционный эвристический анализатор** — содержит механизмы обнаружения неизвестных вредоносных программ. Работа эвристического анализатора опирается на знания (эвристики) об определенных особенностях (признаках) вирусов — как характерных именно для вирусного кода, так и наоборот, крайне редко встречающихся в вирусах. Каждый из таких признаков характеризуется своим «весом» — числом, модуль которого определяет важность, серьезность данного признака, а знак, соответственно, указывает на то, подтверждает он или опровергает гипотезу о возможном наличии неизвестного вируса в анализируемом коде.

- **Модуль эмуляции исполнения** — технология эмуляции исполнения программного кода необходима для обнаружения полиморфных и сложношифрованных вирусов, когда непосредственное применение поиска по контрольным суммам невозможно либо крайне затруднено (из-за невозможности построения надежных сигнатур). Метод состоит в имитации исполнения анализируемого кода эмулятором — программной моделью процессора (и отчасти компьютера и ОС).
- **Технология FLY-CODE** — обеспечивает качественную проверку упакованных исполняемых объектов, распаковывает любые (даже нестандартные) упаковщики методом виртуализации исполнения файла, что позволяет обнаружить вирусы, упакованные даже неизвестными антивирусному ПО Dr.Web упаковщиками.
- **Технология анализа структурной энтропии** — обнаруживает неизвестные угрозы по особенностям расположения участков кода в защищенных криптоупаковщиками проверяемых объектах.
- **Технология ScriptHeuristic** — предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов. Защищает от заражения неизвестными вирусами через веб-браузер. Работает независимо от состояния вирусной базы Dr.Web совместно с любыми веб-браузерами.
- **Origins Tracing**. Технология позволяет определить новые вирусы или модификации имеющихся, которые используют известные механизмы заражения. Origins Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. При сканировании исполняемого файла он рассматривается как некий образец, построенный характерным образом, после чего производится сравнение полученного образа с базой известных вредоносных программ.
Именно постоянная работа над повышением качества обнаружения и лечения (антивирус должен лечить!) вредоносных объектов любого типа выделяет решения компании «Доктор Веб».

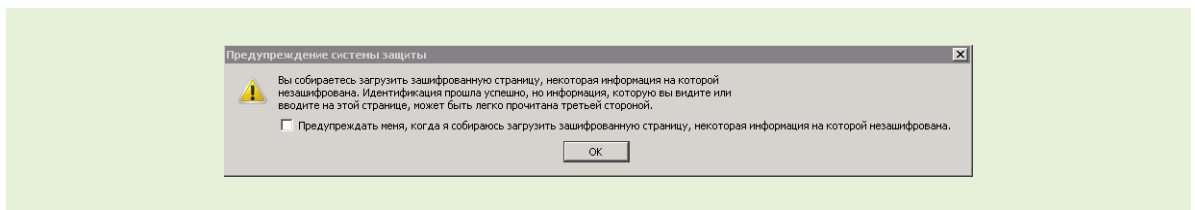
Dr.Web для файловых серверов Windows очень прост в управлении, и для его освоения не понадобятся какие-либо дополнительные навыки. При богатстве возможностей продукта все его настройки интуитивно понятны и расположены так, что путь к ним не занимает времени. Однако в настоящее время мало простого наличия возможностей у продукта — в мире постоянно возникающих новых угроз надо уметь пользоваться продуктом максимально эффективно. О том, как это сделать, и пойдет речь в данном пособии.

4. Получение дистрибутива и документации устанавливаемого продукта

Для получения установочного файла (дистрибутива) антивируса зайдите на сайт компании «Доктор Веб» по адресу <http://www.drweb.com> и на открывшейся странице сайта выберите пункт меню **Скачать**, а в появившемся списке — **Для бизнеса**.

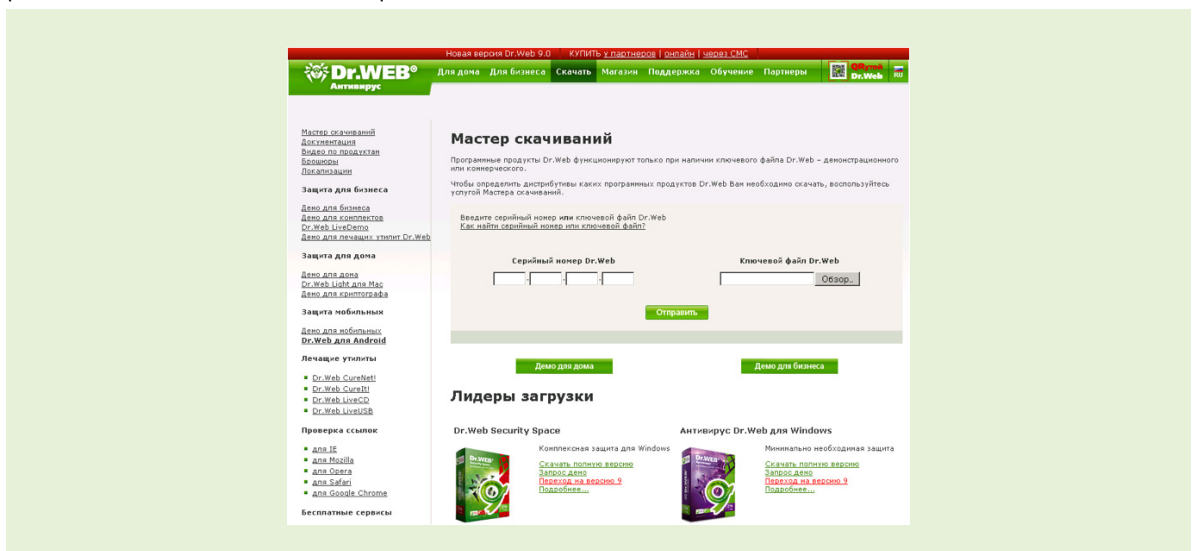


В зависимости от настроек вашей операционной системы вам может быть показано информационное сообщение.



Нажмите **Ок**.

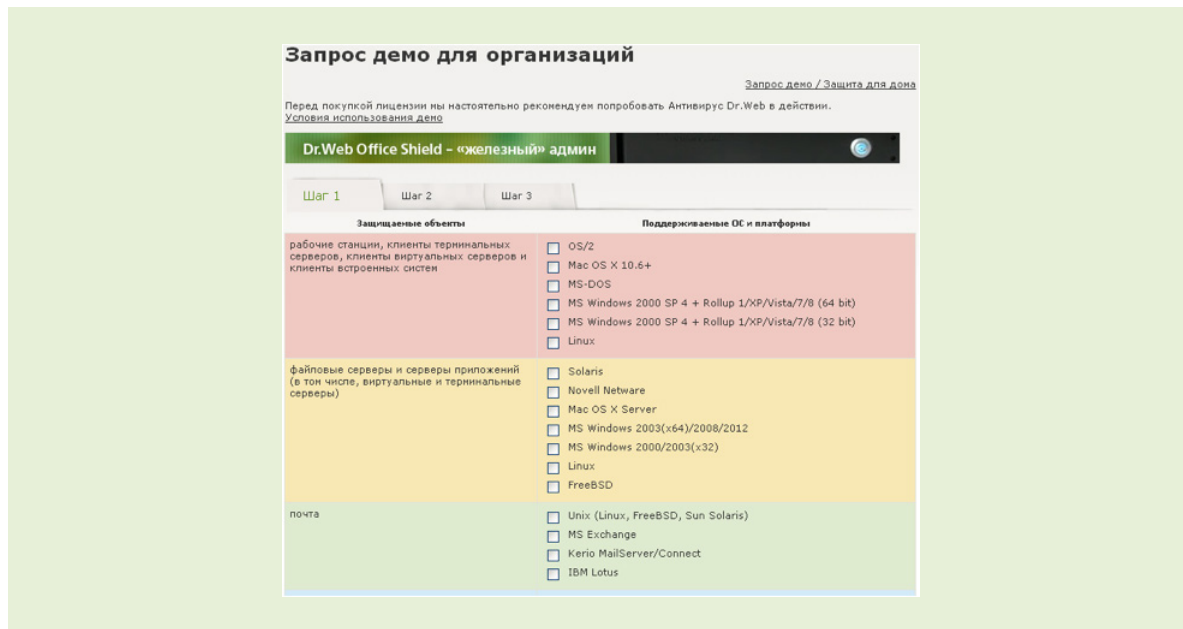
Если вы уже имеете серийный номер или ключевой файл интересующего вас продукта, то вы можете указать их в соответствующих полях ввода — Мастер скачиваний автоматически выберет необходимые для установки дистрибутивы. Если вы еще не получили серийный номер или ключ продукта, то в открывшемся окне Мастера скачиваний вы можете заказать демоверсию продукта, установить ее и оценить возможности выбранного решения, а в дальнейшем продлить лицензию.



Также на эту страницу вы можете попасть, зайдя на сайт компании «Доктор Веб» по адресу <http://download.drweb.com>.

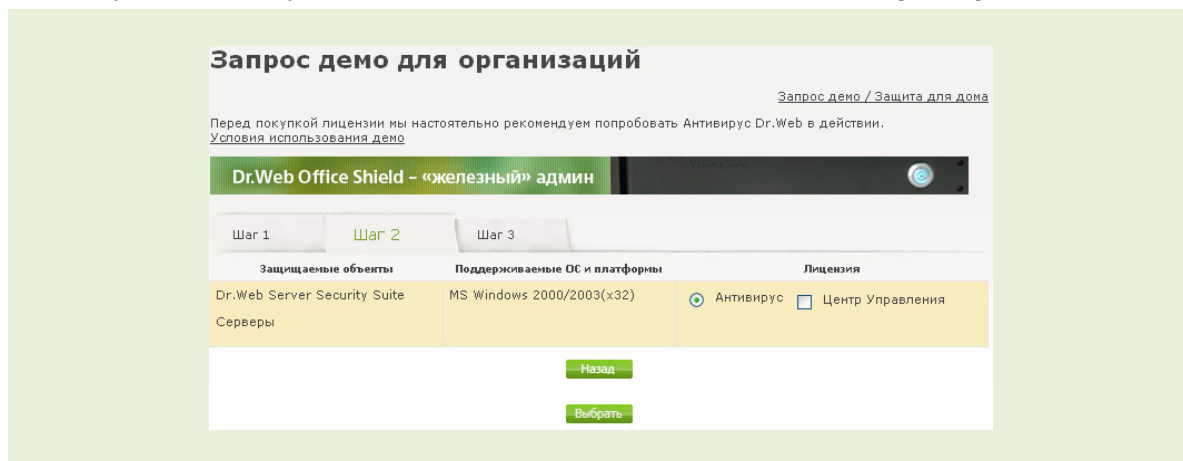
Рассмотрим вариант получения демоверсии.

Нажмите кнопку **Демо для бизнеса**.

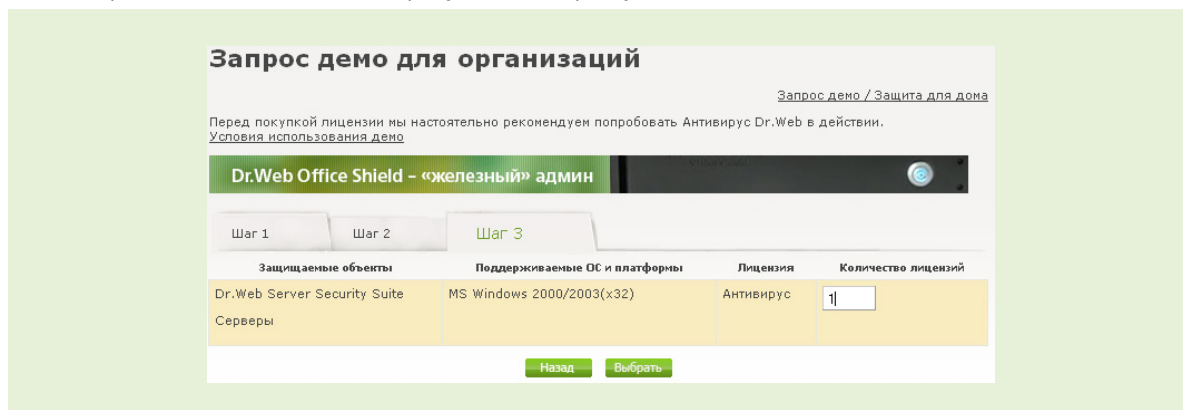


В открывшемся окне выберите тип защищаемого объекта и необходимую операционную систему — и нажмите **Выбрать**.

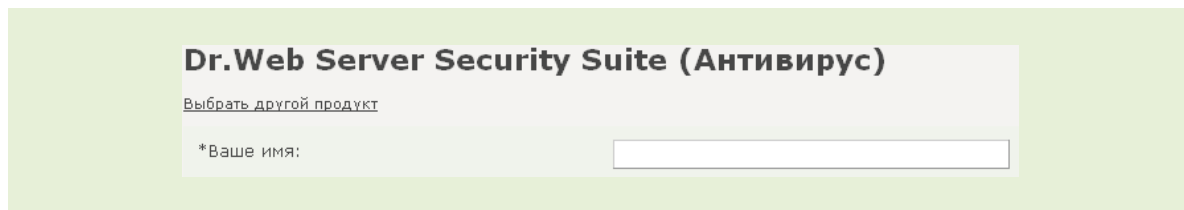
На следующем шаге укажите необходимость использования **Центра Управления**.



На завершающем шаге Мастера укажите требуемое число лицензий.



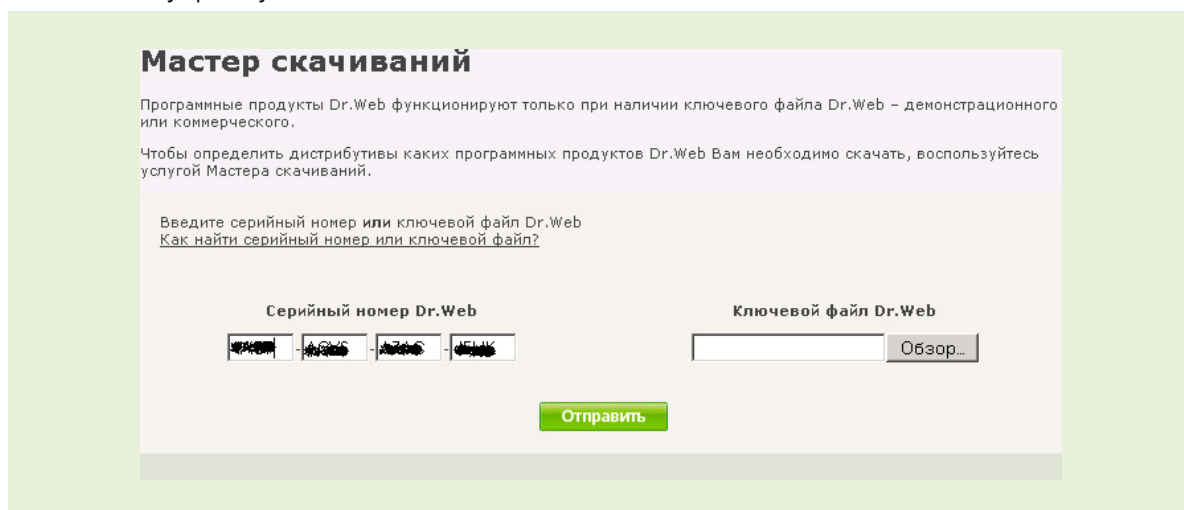
Для получения серийного номера необходимо указать данные, на которые он будет зарегистрирован.



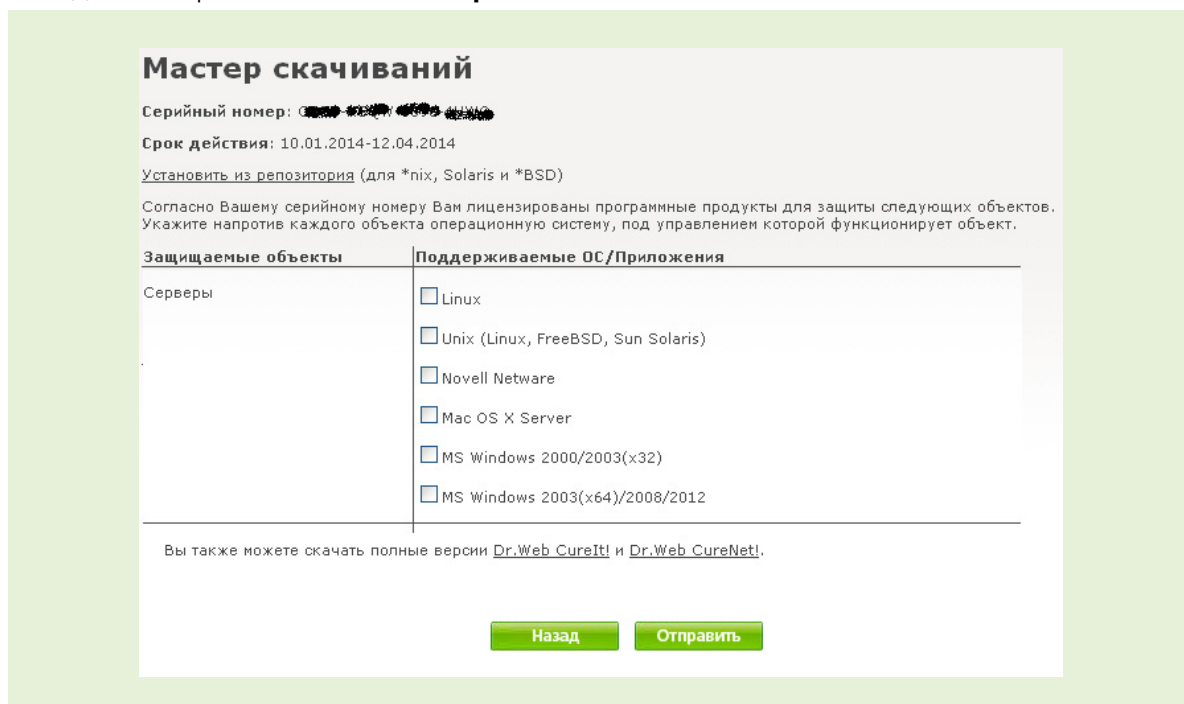
Серийный номер придет на указанный вами почтовый адрес.

Теперь рассмотрим случай получения дистрибутива, если у вас уже имеется серийный номер или ключ продукта.

В окне Мастера скачиваний укажите в соответствующих полях серийный номер или путь к ключевому файлу.



В связи с тем, что для различных операционных систем могут потребоваться различные файлы дистрибутивов, в следующем окне Мастера необходимо отметить операционные системы, на которые вы хотите произвести установку антивирусной защиты. Отметьте необходимые строки и нажмите **Отправить**.



Защищаемые объекты	Поддерживаемые ОС/Приложения
Серверы	<input type="checkbox"/> Linux
	<input type="checkbox"/> Unix (Linux, FreeBSD, Sun Solaris)
	<input type="checkbox"/> Novell Netware
	<input type="checkbox"/> Mac OS X Server
	<input type="checkbox"/> MS Windows 2000/2003(x32)
	<input type="checkbox"/> MS Windows 2003(x64)/2008/2012

В следующем окне для получения дистрибутива нажмите **Скачать Dr.Web для серверов Windows**.

Dr.Web Server Security Suite, Антивирус

[Описание](#) | [Карточка продукта](#)

Поддерживаемые ОС

- Windows Server 2000* / 2003 (x32 и x64*) / 2008 / 2012 (x64)

* Поддерживаются только для версии 7.0.

Номер версии	Программы	Документация
7.0	<p>Dr.Web для серверов Windows</p> <p>Скачать Dr.Web для серверов Windows</p>	<p>выберите язык: <input type="text" value="русский"/></p> <p>Документация Dr.Web для Windows, русская версия</p>

Наиболее подробная информация об установке и настройке продукта содержится в документации. Документацию можно получить из Мастера скачиваний – нажав на ссылку **Документация Dr.Web для Windows**, зайдя на сайт «Доктор Веб» и перейдя по ссылке **Скачать** в разделе **Документация** или в браузере открыть страницу <http://download.drweb.com/doc>. В последних двух случаях документацию можно либо скачать в формате PDF, либо просмотреть онлайн (в окне браузера). Для скачивания необходимо выбрать в меню продукт **Dr.Web® Server Security Suite** и в графе **Поддерживаемые ОС** выбрать **Windows**.

Документация

<p>Центр Управления (Dr.Web Enterprise Security Suite)</p>	<p>Руководство администратора <input type="text" value="русский"/> Скачать Открыть</p> <p>Руководство пользователя <input type="text" value="русский"/> Скачать Открыть</p> <p>Руководство по быстрому запуску Ru Kz Uz Видео</p>
-----------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Продукт	Поддерживаемые ОС и платформы	Документация	Онлайн-документация
<p>Dr.Web® Home Security Suite Защита домашнего ПК/ноутбука/нетбука и мобильных устройств</p>	Windows 8/7/Vista (32- и 64-битные системы), XP (32-битные системы)	Антивирус <input type="text" value="русский"/> Скачать Security space <input type="text" value="русский"/> Скачать Краткое руководство по установке RU EN DE FR ES	Открыть
	Windows 8/7/Vista (32- и 64-битные системы), XP (32-битные системы)	Антивирус <input type="text" value="русский"/> Скачать Security space <input type="text" value="русский"/> Скачать	Открыть
<p>Dr.Web® Desktop Security Suite Защита рабочих станций, клиентов терминальных и виртуальных серверов, клиентов встроенных систем</p>	Mac OS X	<input type="text" value="русский"/> Скачать	Открыть
	Linux	<input type="text" value="русский"/> Скачать	Открыть
	MS-DOS, OS/2	Поставляется вместе с программами	
<p>Dr.Web® Server Security Suite Защита файловых серверов и серверов приложений (в том числе, терминальных и виртуальных серверов)</p>	Windows	7.0 <input type="text" value="русский"/> Скачать 8.0 <input type="text" value="русский"/> Скачать	7.0 Открыть 8.0 Открыть
	Novell NetWare	<input type="text" value="русский"/> Скачать	
	Unix (Samba)	<input type="text" value="русский"/> Скачать	Открыть
	Linux (NSS)	<input type="text" value="русский"/> Скачать	Открыть
	Mac OS X Server	<input type="text" value="русский"/> Скачать	Открыть

5. Установка продукта

Внимание! Установка продукта должна производиться в режиме администратора — только в этом режиме антивирус может противостоять вирусным угрозам. Установка может производиться:

- в обычном (рекомендуемом) режиме (с помощью мастера);
- в фоновом режиме (из командной строки).

Внимание! На компьютере, подключенном к сети Интернет, должны быть установлены все исправления безопасности, причем не только для операционной системы, но и для всех используемых программ — современной тенденцией является использование для проникновения на локальный компьютер уязвимостей именно в программах, а не в операционной системе. Использование всех обновлений безопасности является необходимым условием обеспечения безопасности, так как данные обновления закрывают для вирусописателей доступ в систему через известные уязвимости. Рекомендуется установить эти обновления до начала установки Dr.Web для файловых серверов Windows.

Внимание! На время установки антивирусной защиты компьютер не является защищенным. Не рекомендуется в это время заниматься веб-серфингом, скачивать файлы, проверять личную почту. Как правило, фактическим окончанием установки служит только перезагрузка компьютера, которую требует установка системных компонентов. Начиная с этого момента ваша безопасность будет гарантироваться.

Внимание! Рекомендуется до начала установки удалить ранее используемые антивирусные или антишпионские программы, так как одновременная работа нескольких антивирусов может привести к проблемам в работе некоторых приложений. Dr.Web для файловых серверов Windows способен самостоятельно находить и удалять антивирусные программы, но лучше проделать эту операцию с помощью штатного инсталлятора — в том числе и потому, что деинсталляция может быть защищена паролем, который знаете только вы.

Внимание! Если вы не используете русифицированную версию операционной системы, убедитесь в том, что на ней установлены все необходимые для отображения русских символов компоненты.

5.1. Установка из командной строки

Для запуска установки Dr.Web для файловых серверов Windows в фоновом режиме в командной строке введите имя исполняемого файла с необходимыми вам параметрами.

Рассмотрим вариант команды, при запуске которой будет проведена установка Dr.Web для файловых серверов Windows и проведена перезагрузка после установки (в данном примере дистрибутив продукта расположен в `C:\Documents and Settings`):

```
C:\Documents and Settings\drweb-800-winsrv.exe /silent yes /reboot yes
```

Если необходимо установить Dr.Web для файловых серверов Windows на определенном языке, то дополнительно необходимо задать следующий параметр:

```
/lang <код _ языка>
```

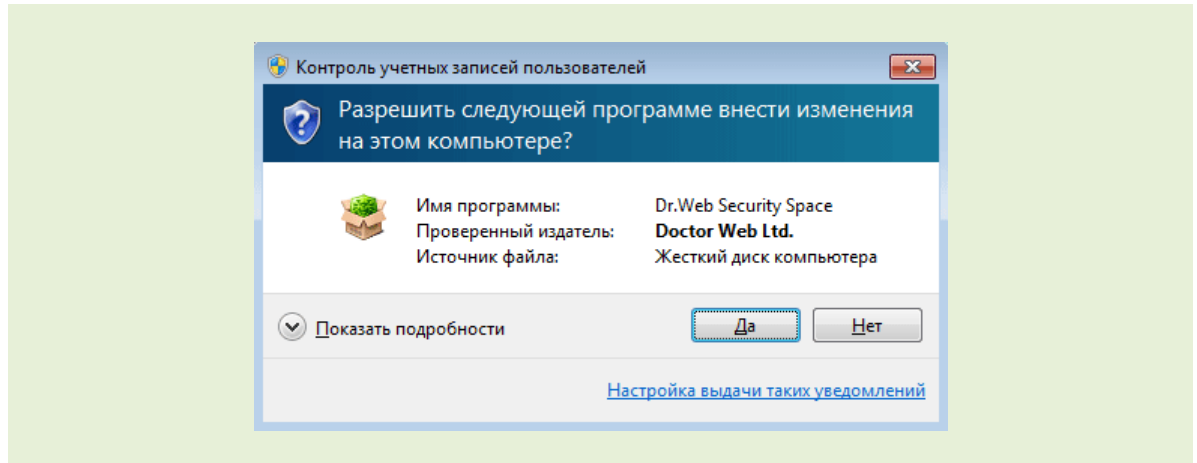
Для русского языка значение кода — `ru`.

Ознакомиться с параметрами командной строки можно в документации по продукту.

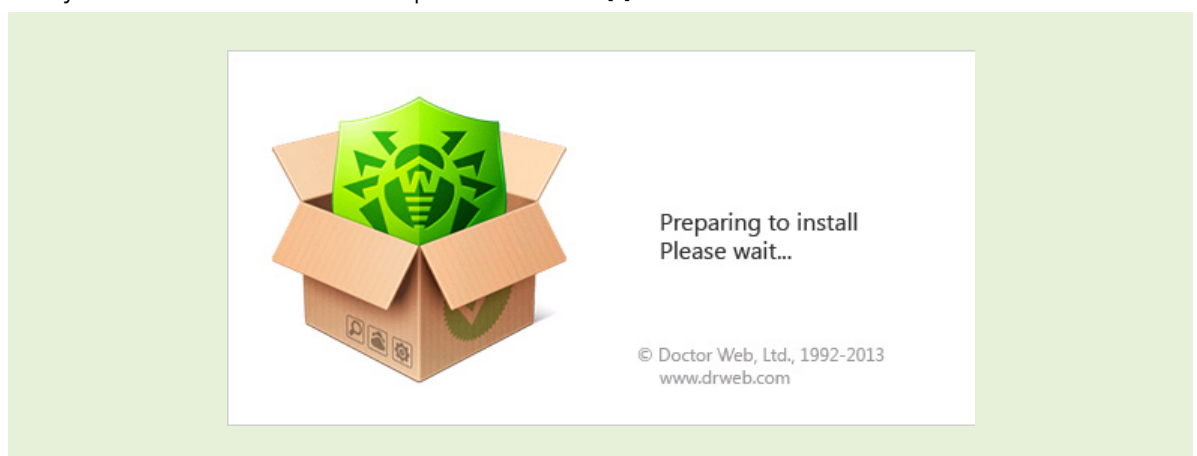
5.2. Установка с помощью мастера

Запустите файл установки и следуйте инструкциям Мастера установки.

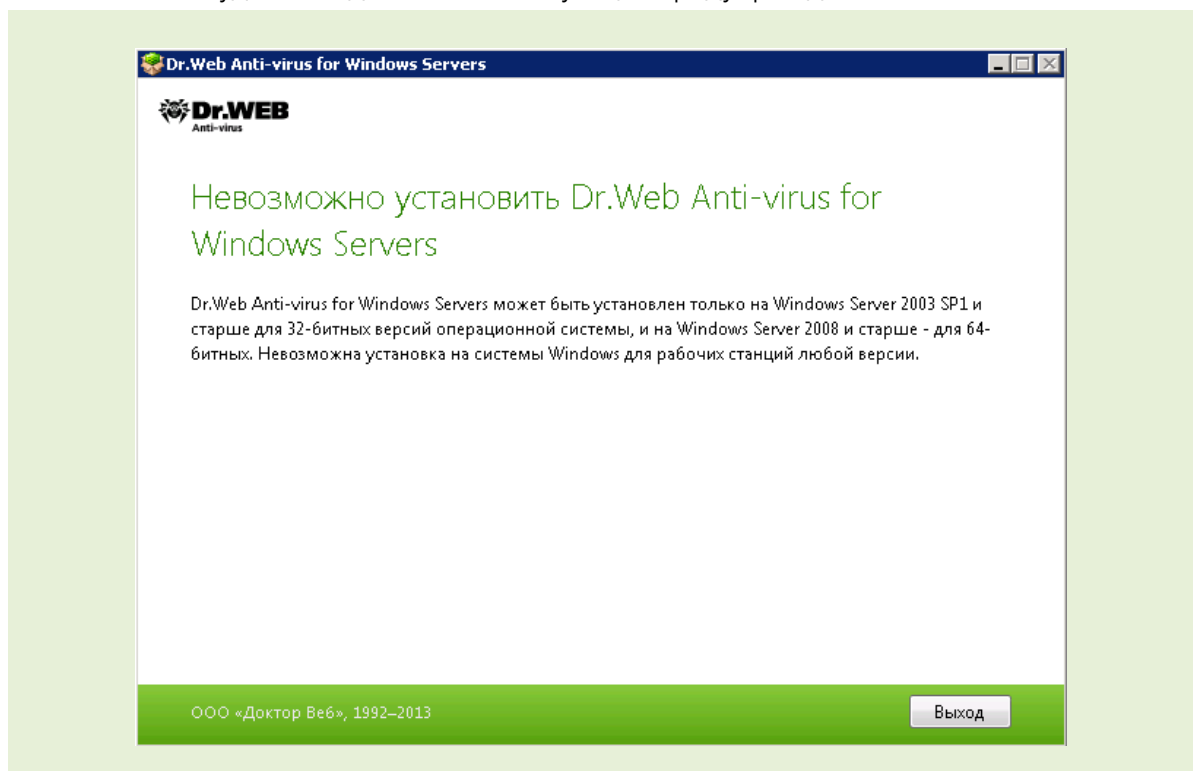
Если установка производится на операционных системах Windows Vista и выше, то в зависимости от настроек вашей операционной системы может появиться запрос системы контроля учетных записей (UAC).



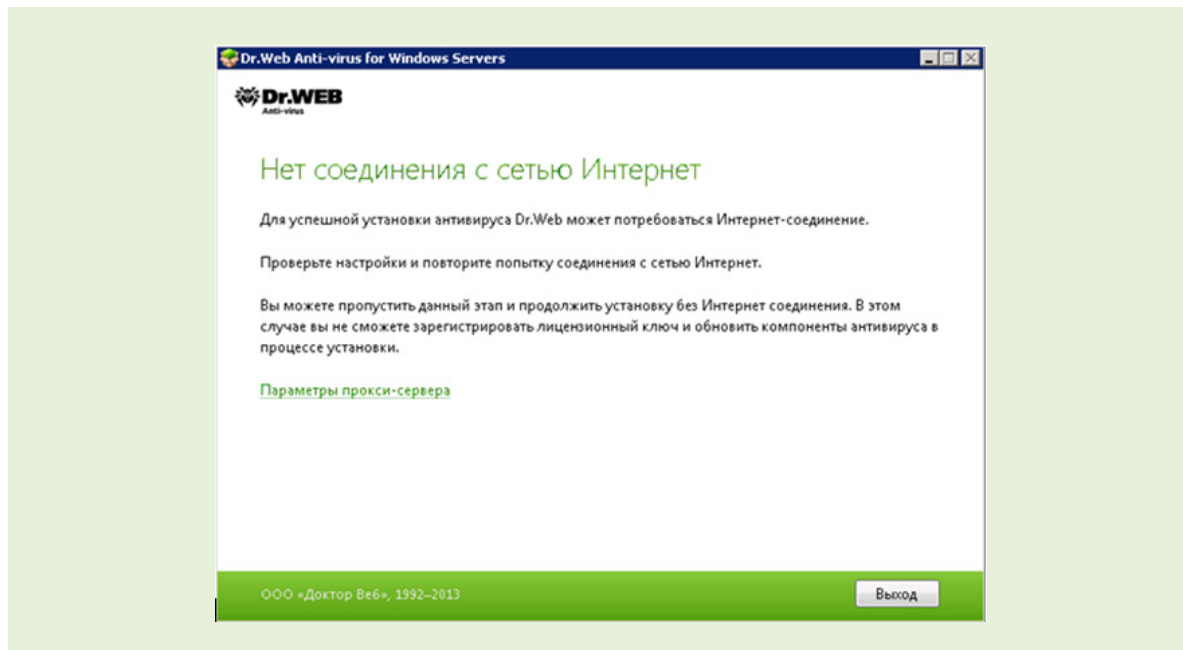
В случае появления такого запроса нажмите **Да**.



Внимание! Установка Dr.Web для файловых серверов Windows возможна только на серверные операционные системы. В случае запуска инсталляционного файла на неподдерживаемой ОС будет выведено соответствующее предупреждение:



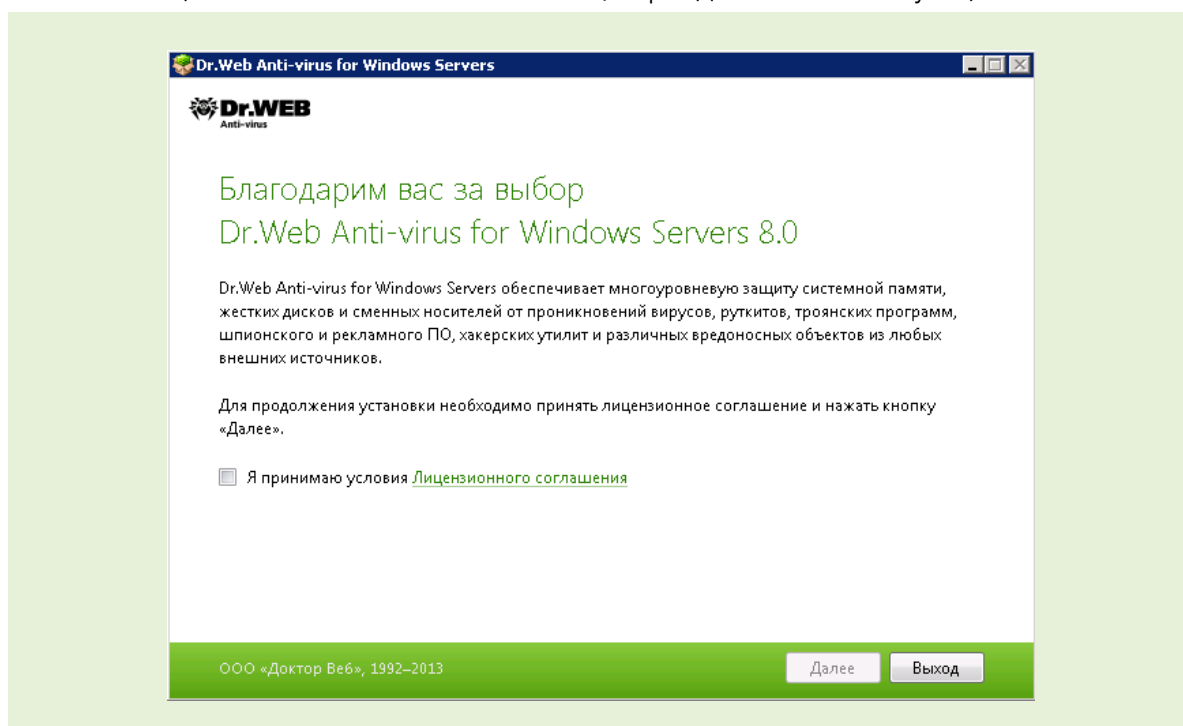
Внимание! Для выполнения ряда операций в ходе установки (в том числе обновления) требуется доступ в сеть Интернет. Если такой доступ отсутствует по тем или иным причинам — в ходе установки будет показано следующее сообщение:

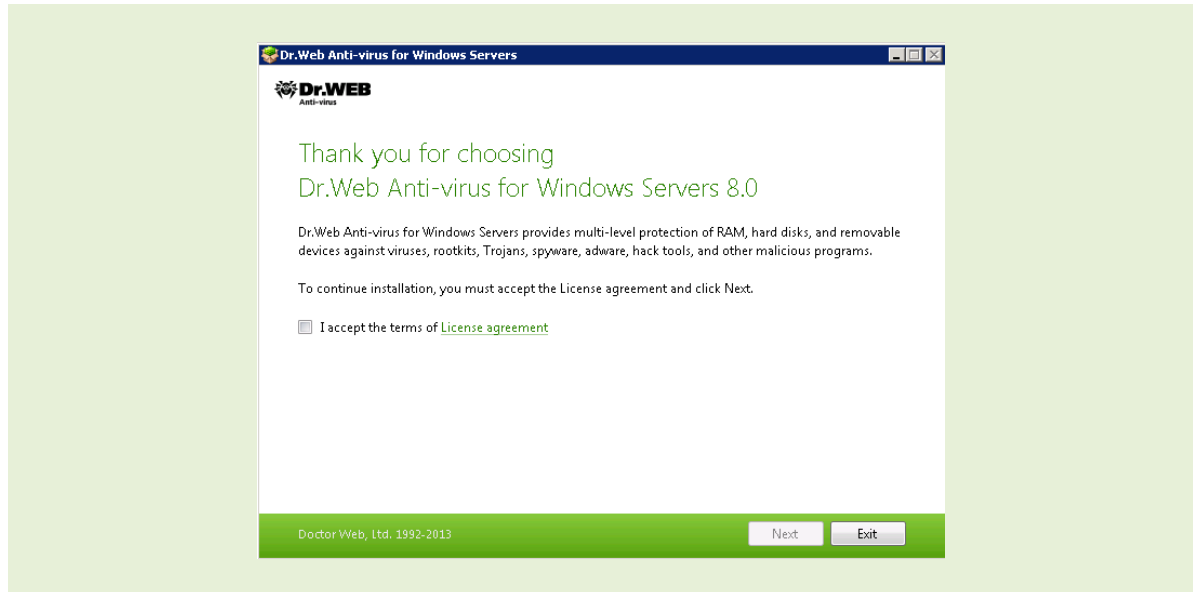


Если у вас ранее была установлена предыдущая версия продукта, то Мастер установки предложит ее удалить. Нажмите **Удалить**.

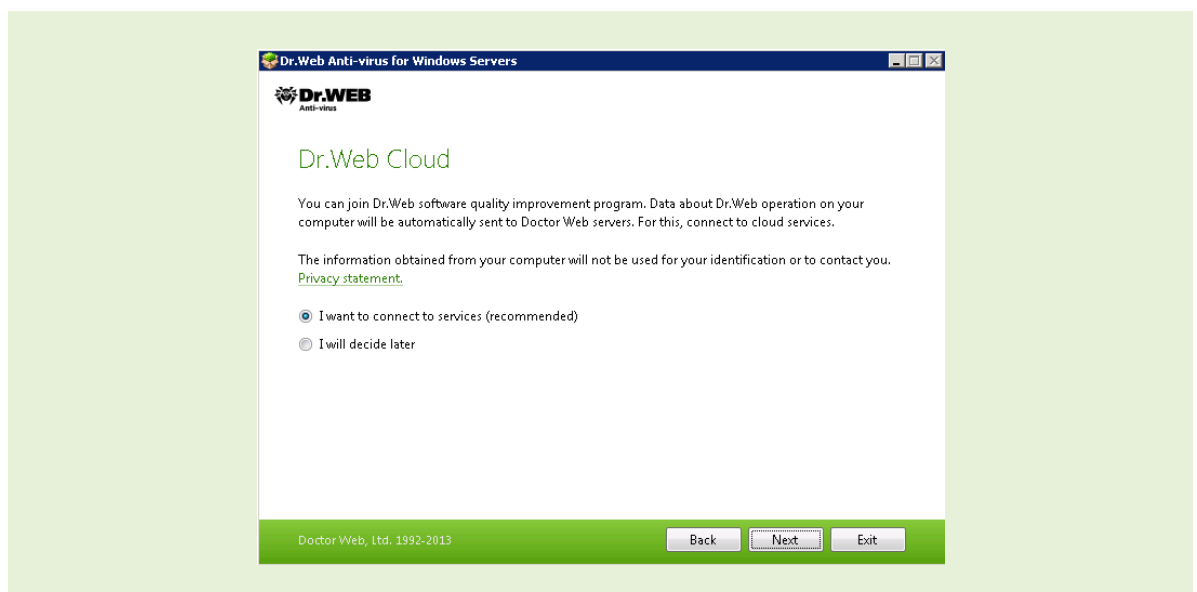
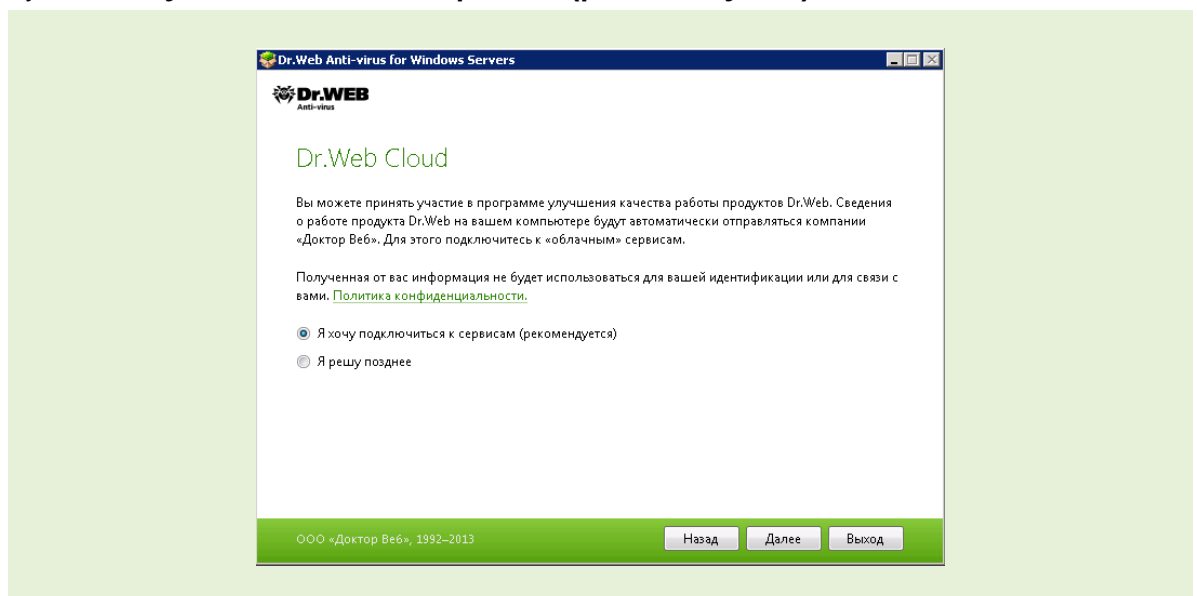
Если в ходе удаления предыдущей версии возникают ошибки и удалить антивирус не удастся, воспользуйтесь утилитой для аварийного удаления «остатков» от некорректных/поврежденных инсталляций Dr.Web, скачать которую можно по ссылке: http://download.geo.drweb.com/pub/drweb/tools/drw_remover.exe. Либо обратитесь в службу технической поддержки по адресу <https://support.drweb.com>.

В начале установки новой версии откроется окно мастера установки. Отметьте флажком пункт **Я принимаю условия лицензионного соглашения** и нажмите **Далее**. Ознакомиться с текстом лицензионного соглашения можно, перейдя по соответствующей ссылке.

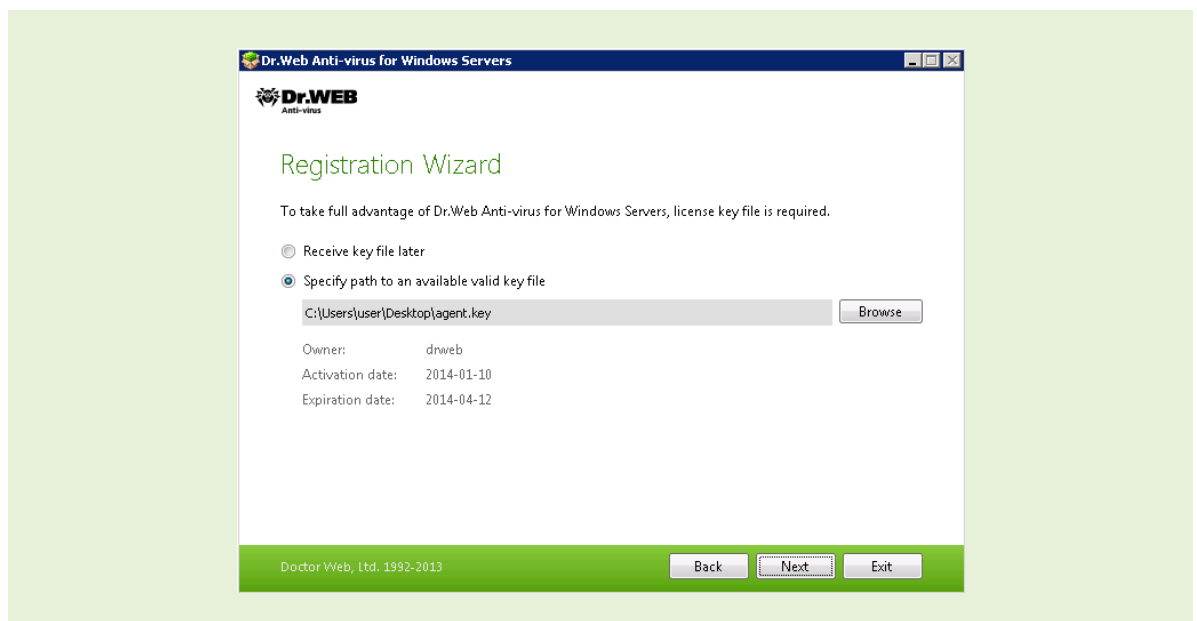
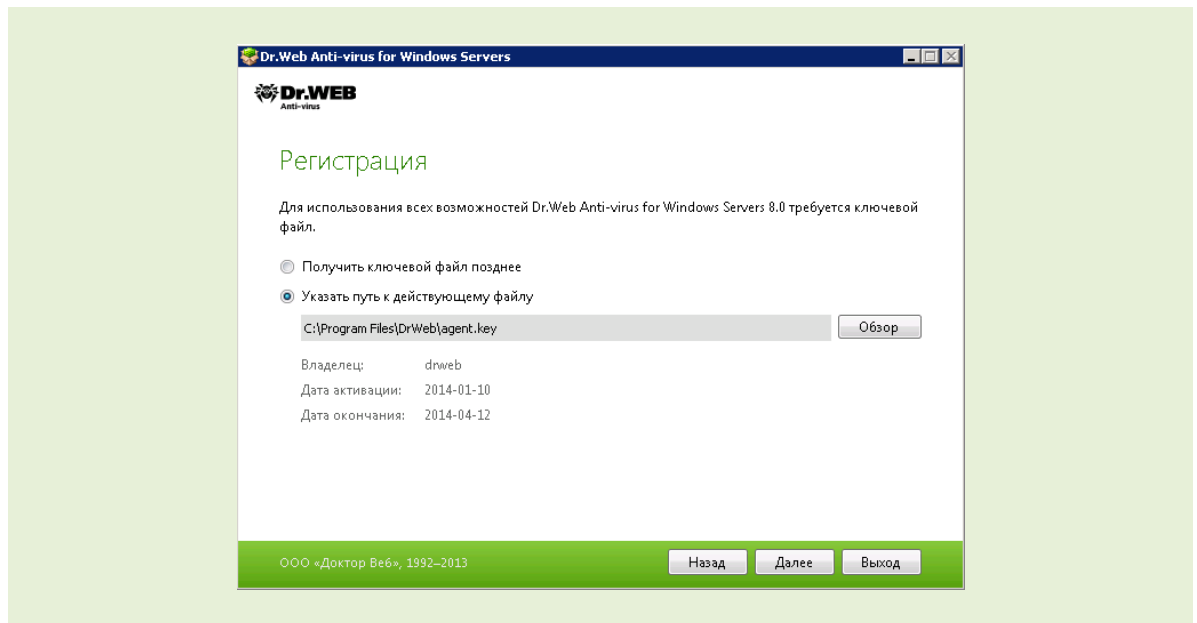




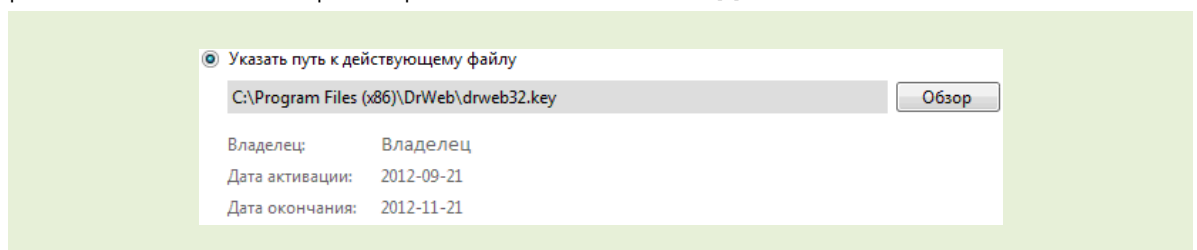
Если требуется подключиться к облачным сервисам Dr.Web, в следующем окне отметьте пункт **Я хочу подключиться к сервисам (рекомендуется)** и нажмите **Далее**.



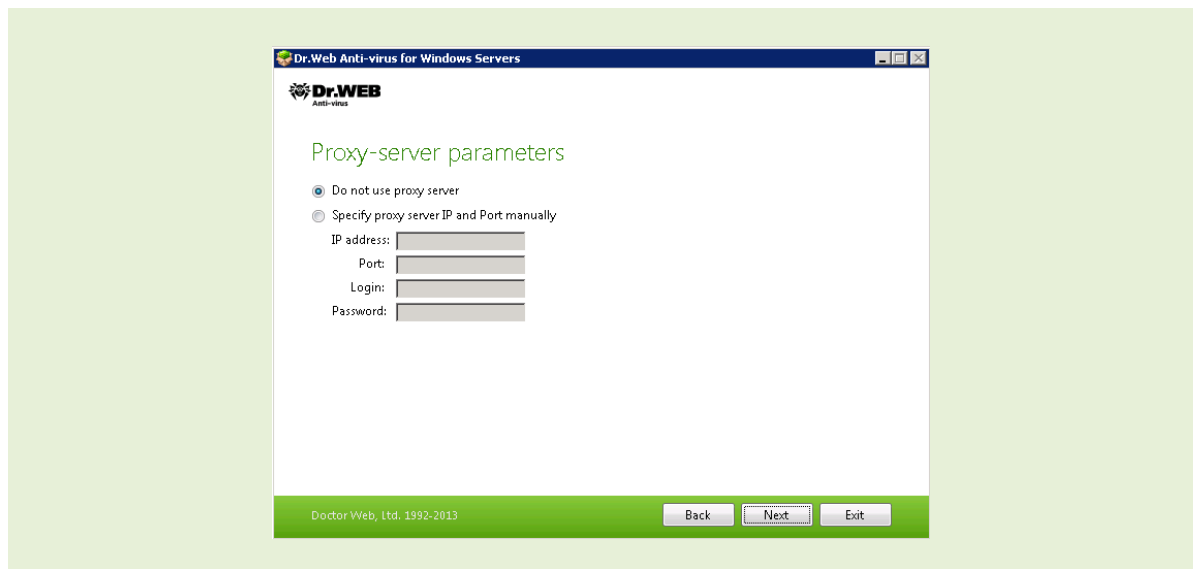
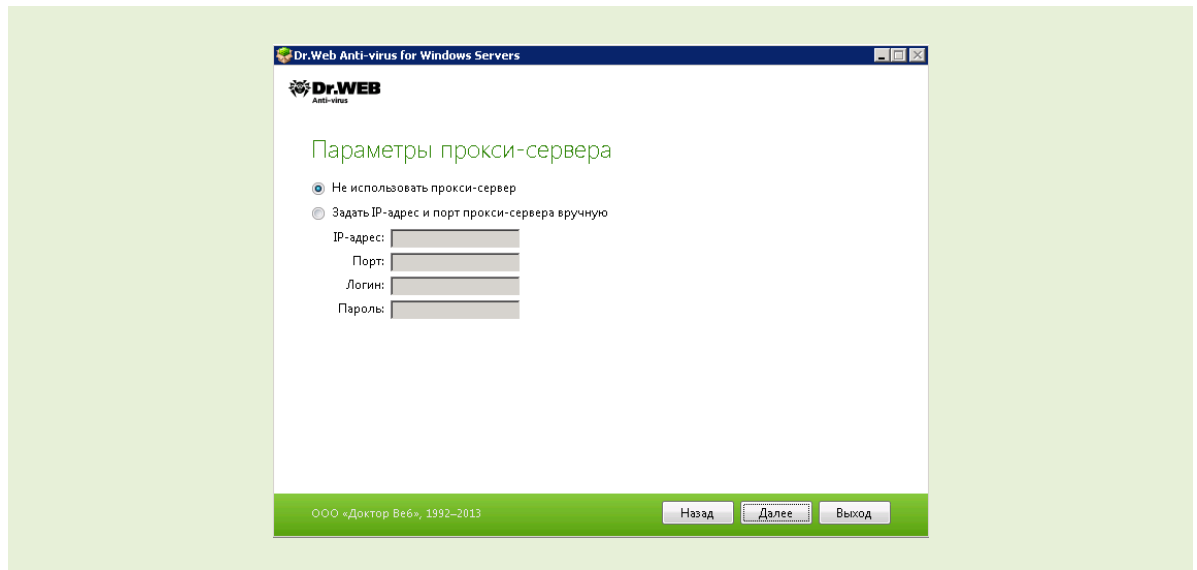
В следующем окне вам будет необходимо указать серийный номер или ключевой файл – в том случае, если они у вас имеются. Если у вас уже есть лицензионный или демонстрационный ключевой файл, выберите пункт **Указать путь...** В том случае, если у вас нет серийного номера или ключевого файла и вы хотите оценить возможности продукта – нажмите **Получить ключевой файл позднее** – после завершения установки продукта, в этом случае вы можете начать работу с временным ключевым файлом.



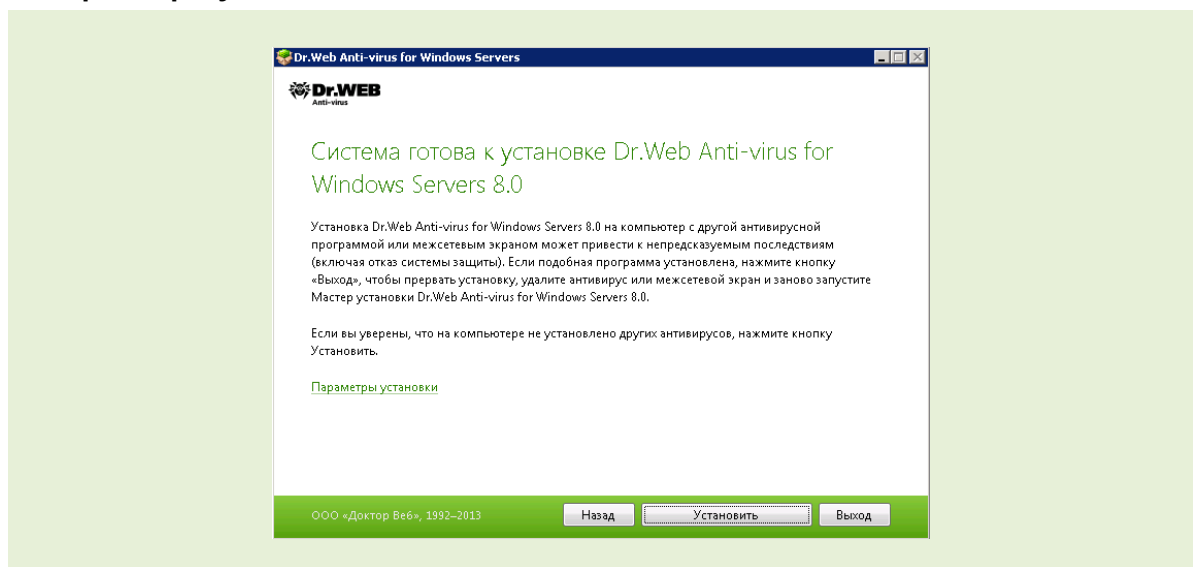
Если у вас ранее уже был установлен антивирус Dr.Web, то при переходе на новую версию с более ранних антивирус при установке автоматически находит ключевой файл. Если файл не найден, нажмите **Обзор** и укажите путь к имеющемуся ключевому файлу (который использовался старой версией). Затем нажмите **Далее**.

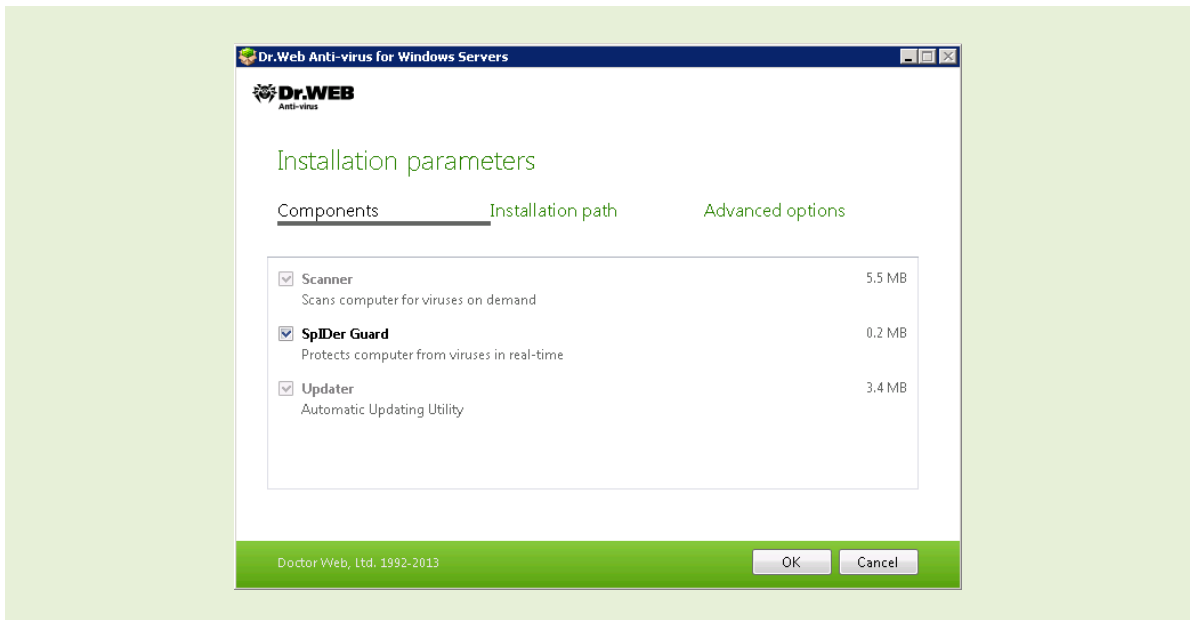
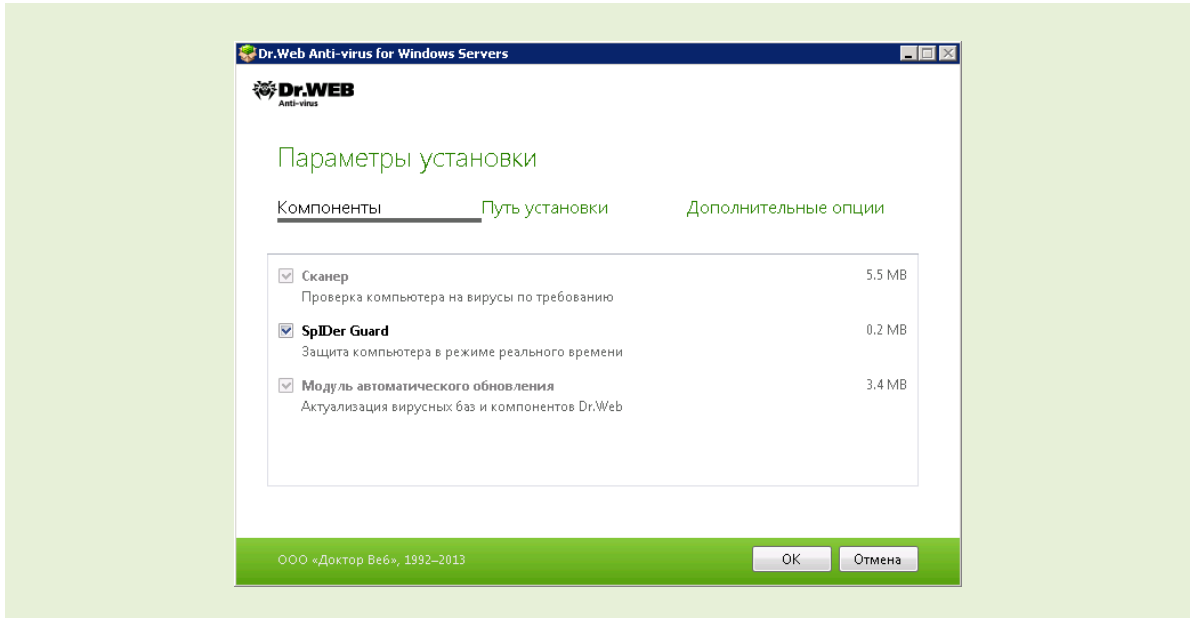


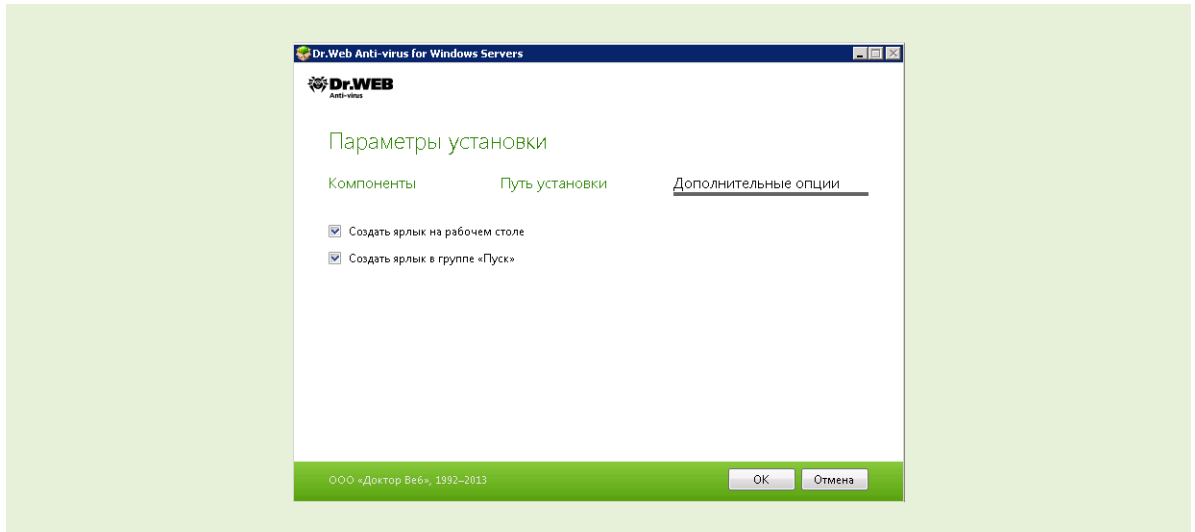
На следующем шаге укажите параметры используемого прокси-сервера.



Для завершения установки антивируса нажмите **Установить** на следующем окне Мастера. В том же окне вы можете просмотреть и изменить настройки — для этого щелкните по ссылке **Параметры установки**.



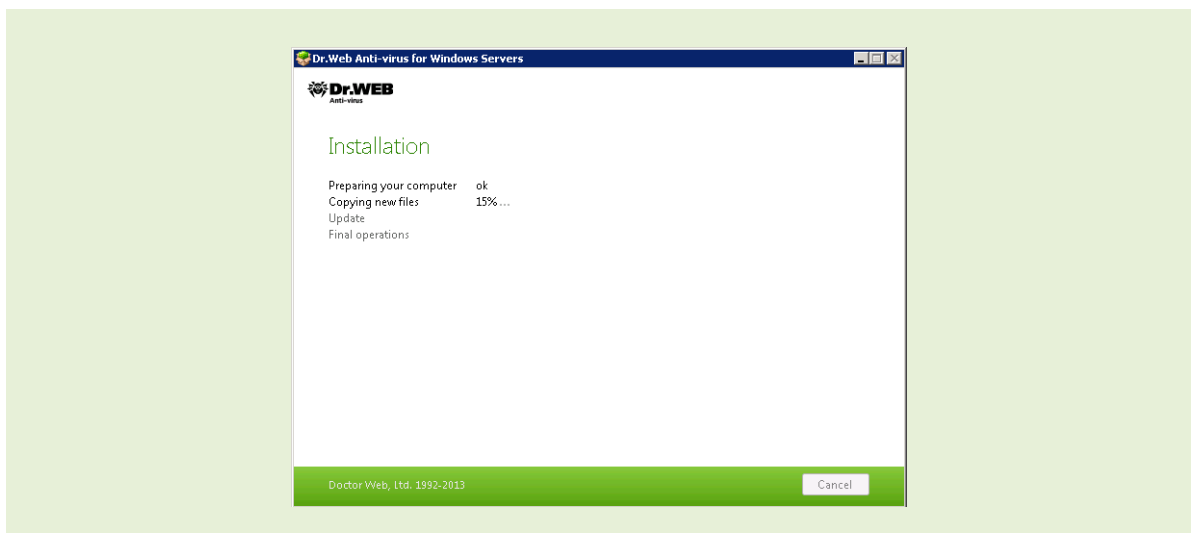
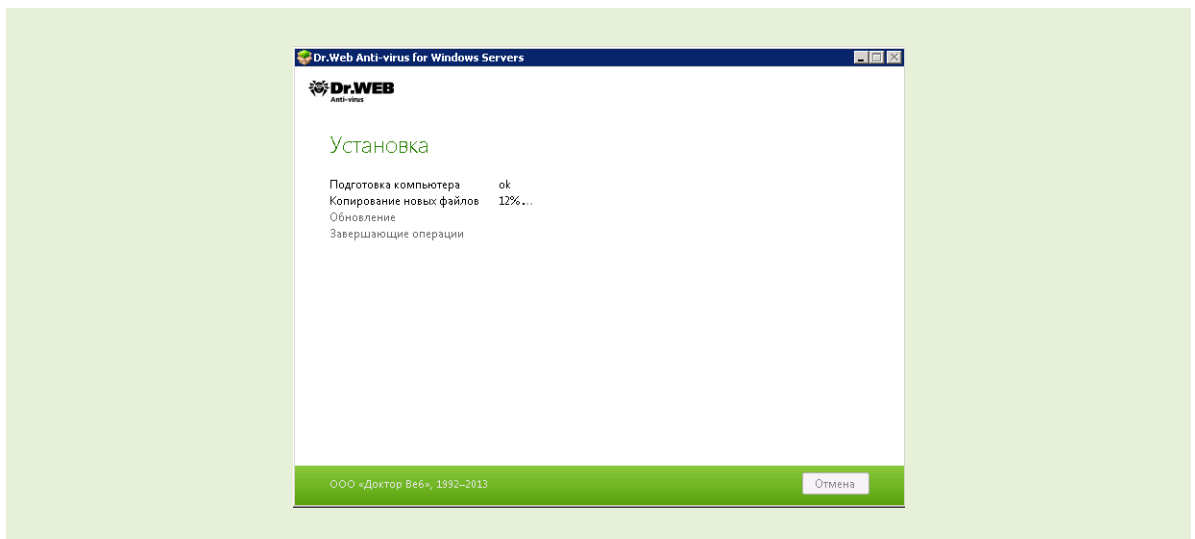




Состав опций зависит от ранее выбранных параметров установки. Так, если ранее был указан действующий ключевой файл, то на вкладке **Дополнительные опции** будет предложено загрузить обновления во время установки.

Рекомендуется использовать установку по умолчанию — все продукты компании «Доктор Веб» поставляются с оптимизированными для комфортной работы настройками.

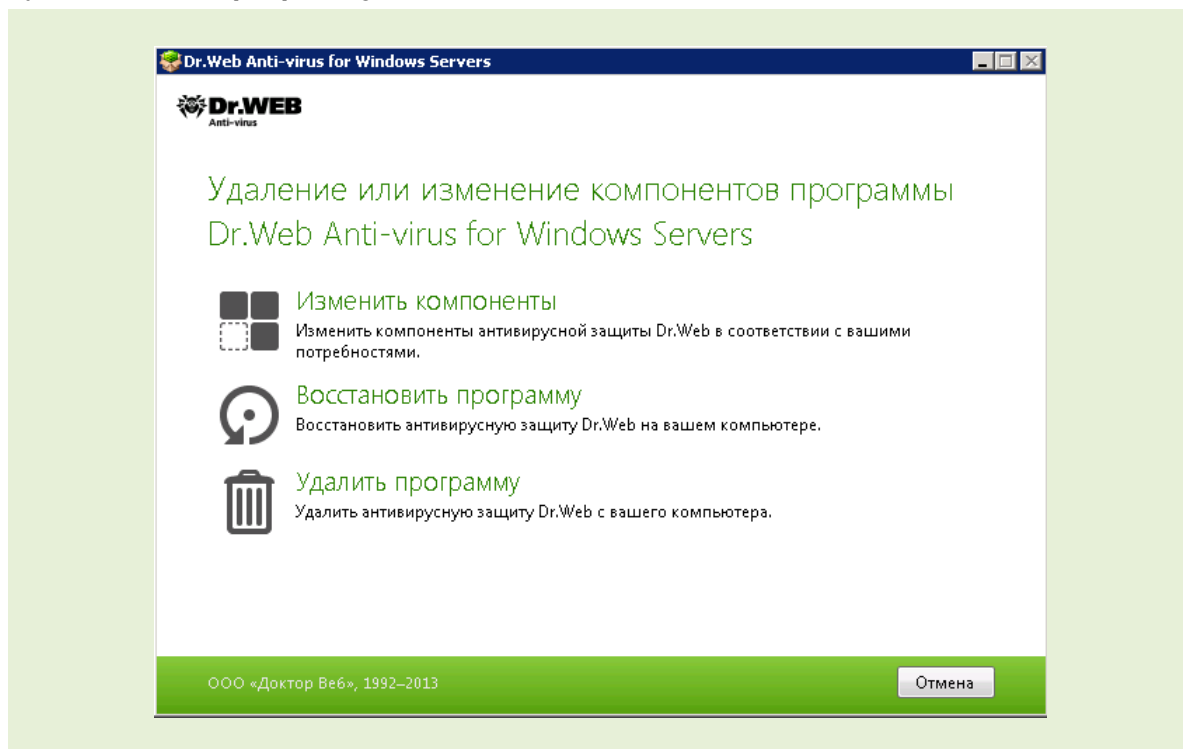
Ход установки также отображается в Мастере.



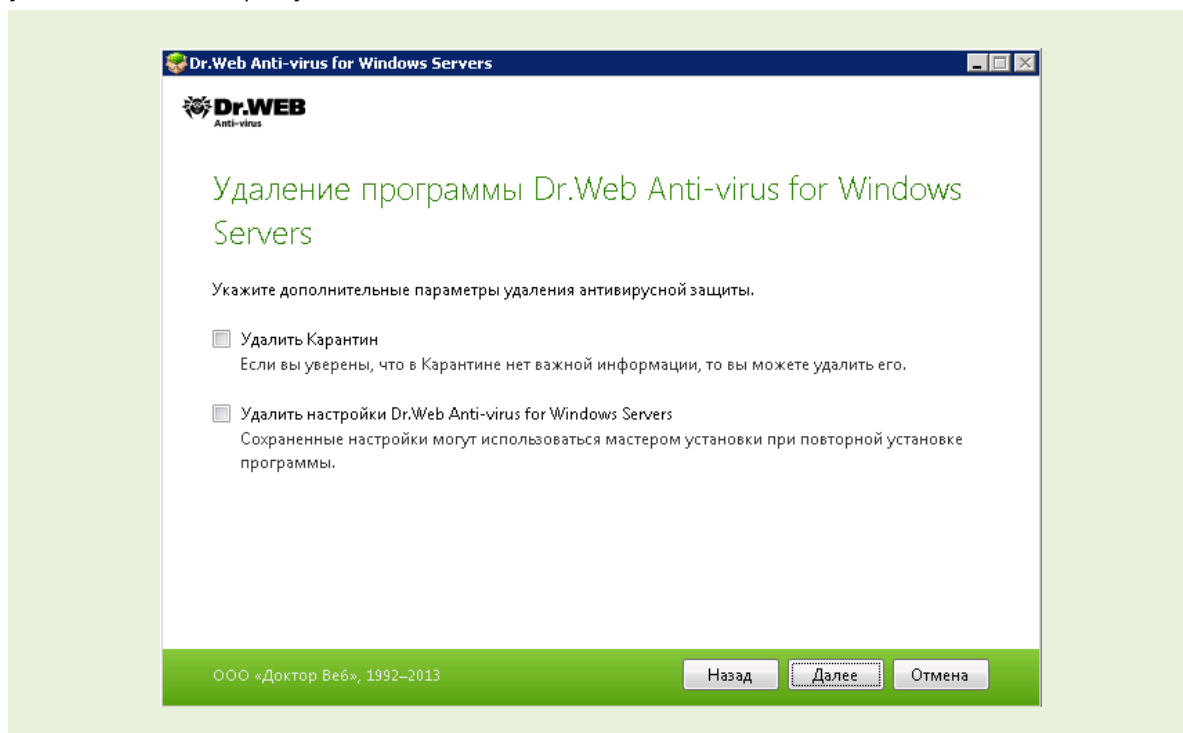
После выполнения всех необходимых действий мастер установки запросит разрешение на перезагрузку. Перезагрузка необходима, в частности, для того, чтобы можно было гарантировать, что ни один вирус не был загружен до антивируса — что крайне важно для борьбы с руткитами. Сохраните все необходимые данные и перезагрузите ПК.

6. Удаление продукта

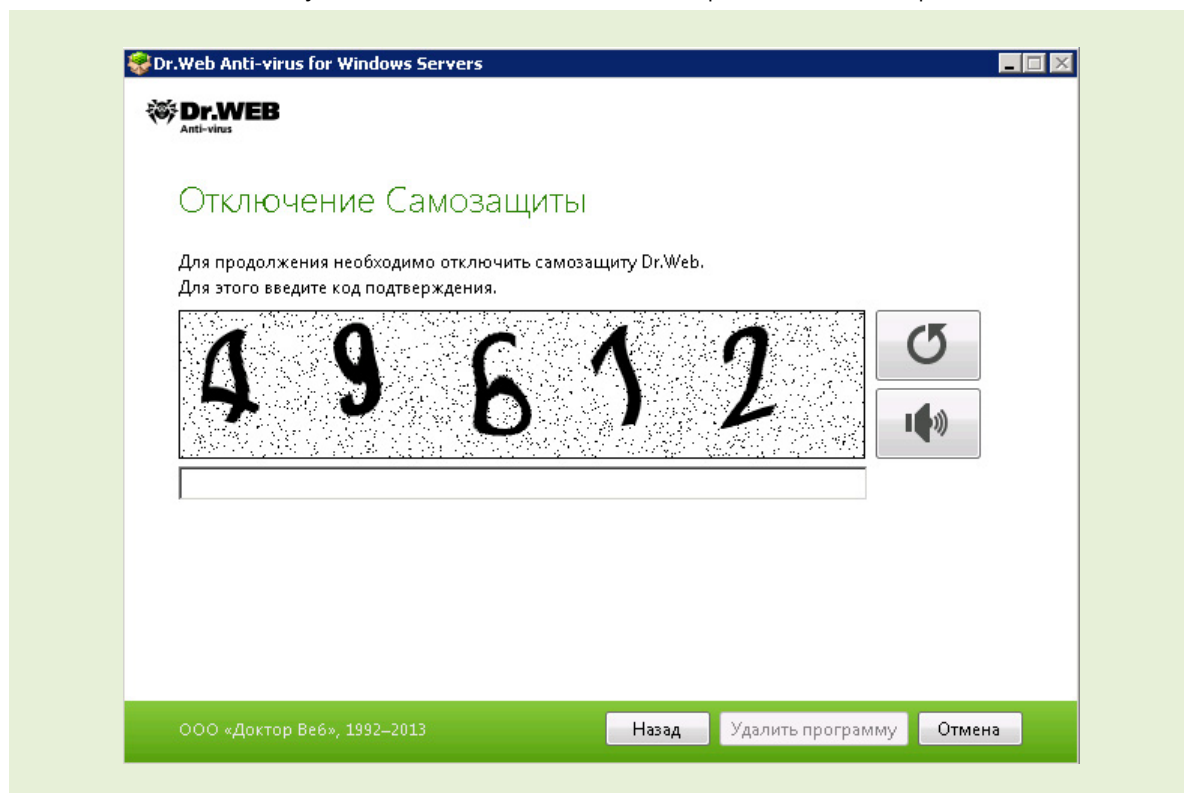
Чтобы удалить продукт, необходимо еще раз запустить установочный файл и выбрать пункт **Удалить программу**.



На следующем шаге определите необходимость удаления настроек и карантина ранее установленного продукта.



Для удаления Dr.Web для файловых серверов Windows программе установки потребуется отключить самозащиту. Для этого введите код, изображенный в открывшемся окне.



При необходимости по просьбе программы перезагрузите компьютер для завершения процедуры удаления.

7. Проверка работоспособности продукта

Чтобы удостовериться в том, что с текущими настройками ваш антивирус функционирует нормально и обеспечивает максимальную защиту от вирусов и спама, вы можете провести небольшое тестирование с использованием тестового файла EICAR — European Institute for Computer Anti-Virus Research.

Многими разработчиками антивирусов принято для этой цели использовать одну и ту же стандартную программу `EICAR.com`. Эта «программа» была специально разработана для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса. Программа `test.com` не является сама по себе вредоносной, но специально обрабатывается большинством антивирусных программ как вирус. Антивирусный продукт Dr.Web называет этот «вирус» следующим образом: EICAR Test File (Not a Virus!). Примерно так его называют и другие антивирусные программы. Программа `test.com` представляет собой 68-байтный COM-файл, в результате исполнения которого на консоль выводится текстовое сообщение EICAR-STANDARDANTIVIRUS-TEST-FILE!

Файл `test.com` состоит только из текстовых символов, которые формируют следующую строку:

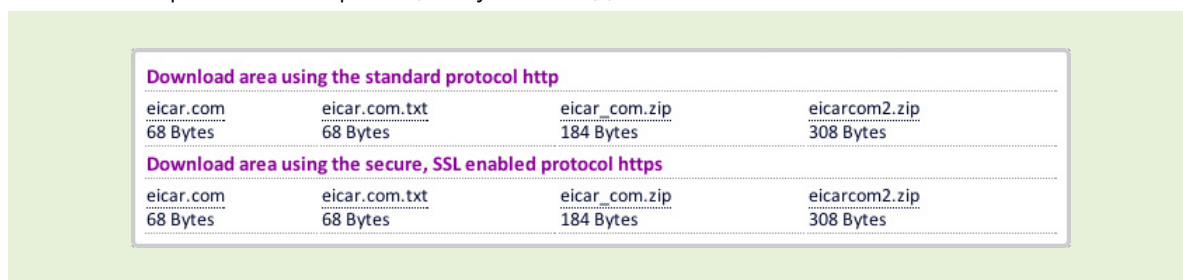
```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Если вы создадите файл, содержащий приведенную выше строку, и сохраните его под именем `test.com`, то в результате получится программа, которая и будет описанным «вирусом».

Если вы хотите проверить работу файлового монитора, сделайте следующее.

1. Откройте браузер и перейдите по адресу <http://www.eicar.org/85-0-Download.html>

2. На открывшейся странице опуститесь до текста




3. Выберите для скачивания любой из предложенных вариантов, например первый — `eicar.com`, и попытайтесь загрузить тестовый вирус. Итогом попытки должно стать окно с сообщением об обнаружении тестового вируса.

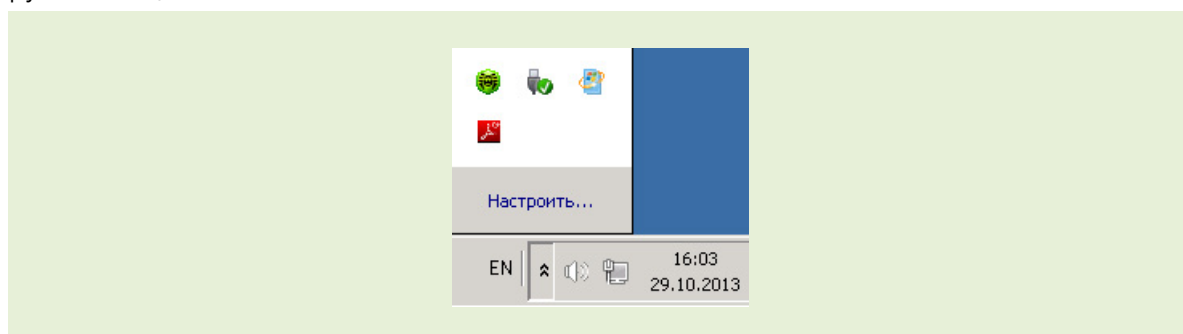
8. Знакомство с Dr.Web для файловых серверов Windows

Одной из особенностей продукта является современная модульная архитектура. Продукт включает в себя следующие компоненты:

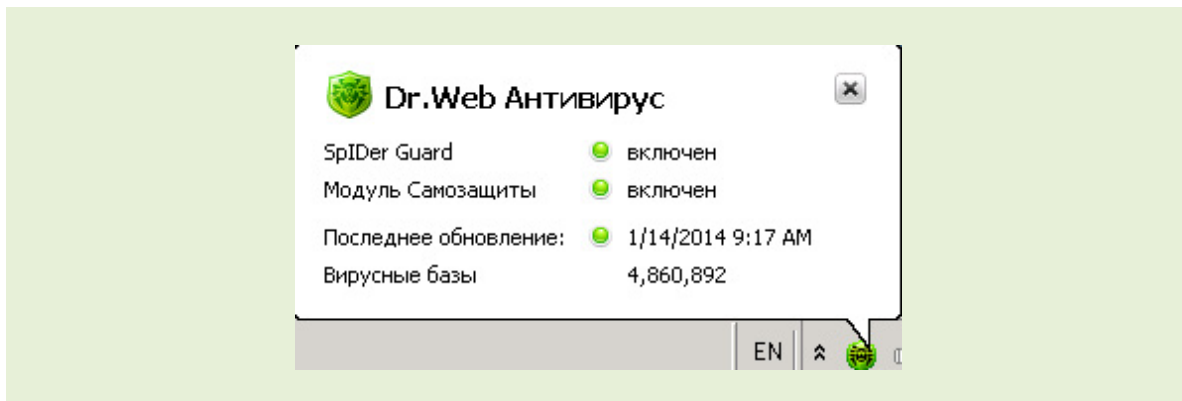
- **Сканер Dr.Web** — антивирусный сканер с графическим интерфейсом, который запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера. Один из основных компонентов антивируса. Первое, что запускается после установки продукта, — это Сканер. Имеет несколько режимов работы, что позволяет оптимизировать процесс сканирования.
- **SplDer Guard** — антивирусный сторож, который постоянно находится в оперативной памяти, осуществляя проверку файлов и памяти «на лету», а также обнаруживая проявления вирусной активности.
- **Модуль обновления Dr.Web** — компонент, который позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов Dr.Web, а также производит их автоматическую установку. Постоянное обновление позволяет вашему антивирусу противостоять самым современным угрозам.
- **SplDer Agent** — модуль управления, с помощью которого осуществляется запуск и настройка компонентов антивирусного продукта. Удобный интерфейс позволяет всегда иметь доступ ко всем группам настроек из одного меню, значок которого находится в правом нижнем углу экрана.

Сразу после установки **Dr.Web для файловых серверов Windows** в правом нижнем углу экрана появляется значок **Агента**, с помощью которого можно осуществлять управление всеми настройками антивируса.

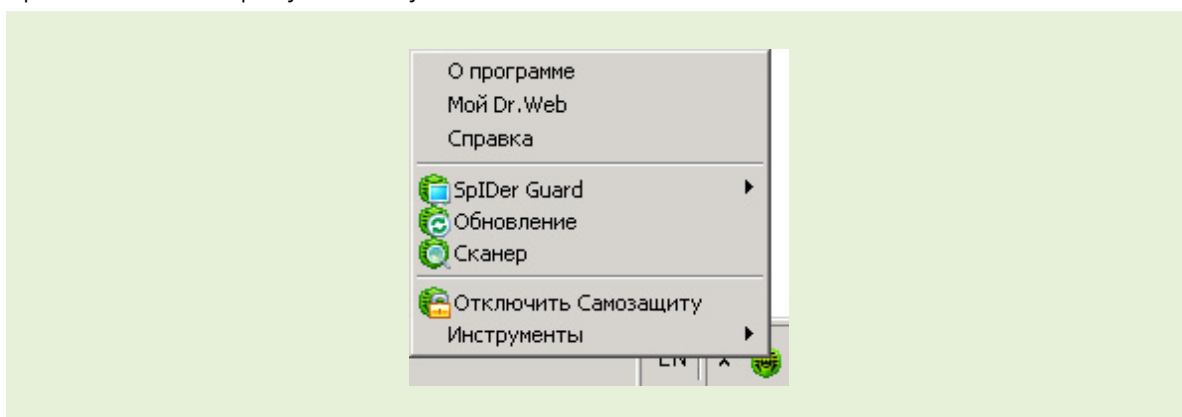
Внимание! Особенностью Windows 7/8 и выше является то, что она не показывает иконку антивируса в системном трее. Рекомендуется включить отображение иконки (щелкнуть на значок  на тулбаре, выбрать пункт **Customize** и настроить желательный вид отображения иконки), так как по изменению ее вида можно контролировать состояние антивирусной защиты.



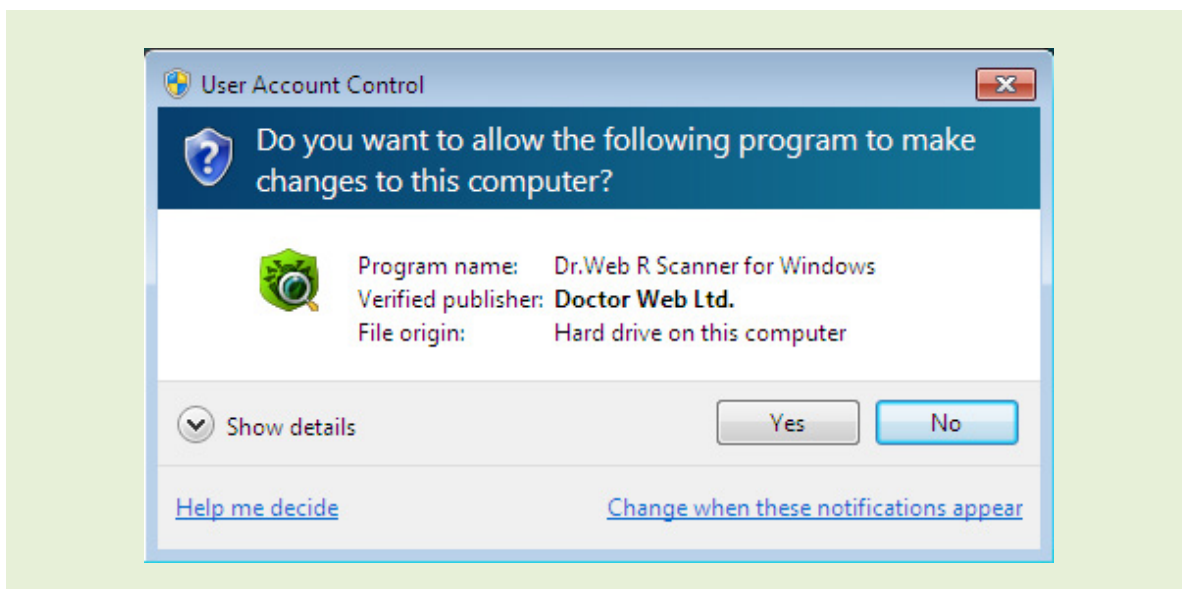
При наведении курсора мыши на значок появляется всплывающая подсказка с информацией о запущенных компонентах, а также датой последнего обновления антивируса и количеством записей в вирусных базах.

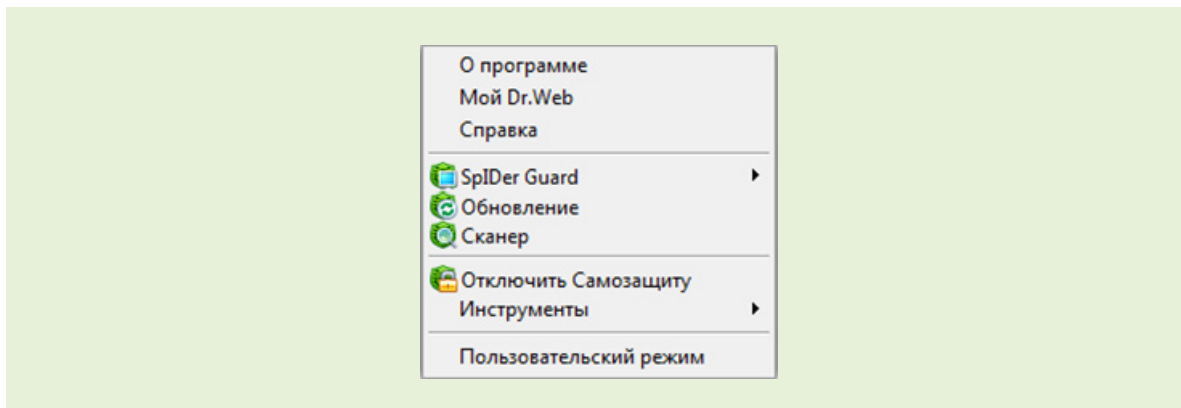


Если настройки уведомлений не были изменены, над значком могут появляться сообщения-подсказки. Запуск и настройка компонентов Dr.Web для файловых серверов Windows осуществляется с помощью контекстного меню значка модуля управления, появляющегося при нажатии на правую кнопку мыши.



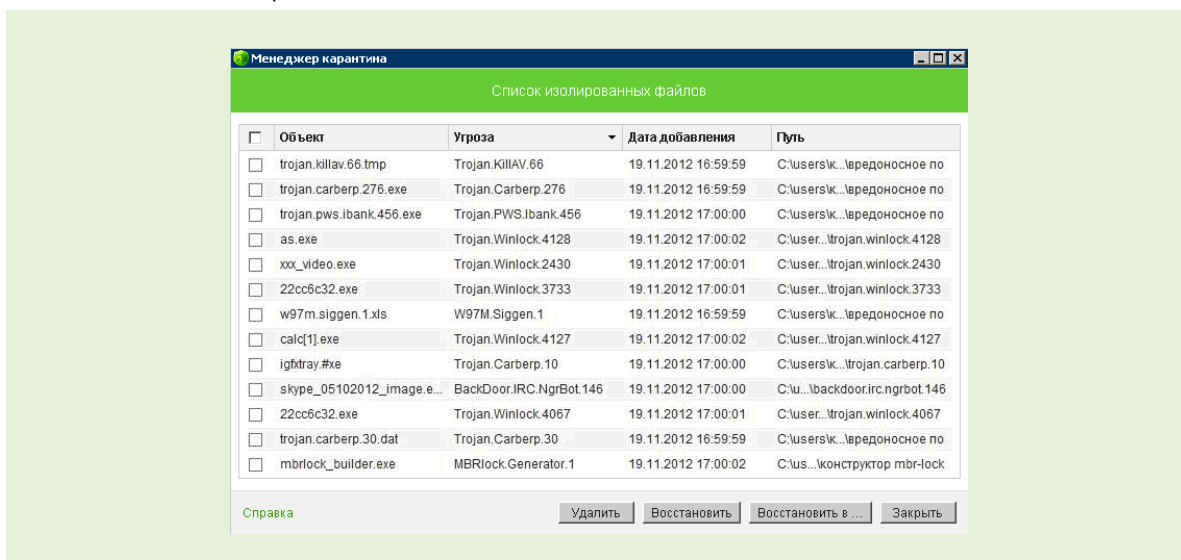
По умолчанию – сразу после старта – в меню показываются возможности, доступные обычному пользователю. Для перехода в полнофункциональный режим необходимо выбрать пункт **Административный режим**. Если вы используете Windows 7/8 и выше, то для перехода в **Административный режим** вам нужно будет подтвердить разрешение, нажав на **Yes**.



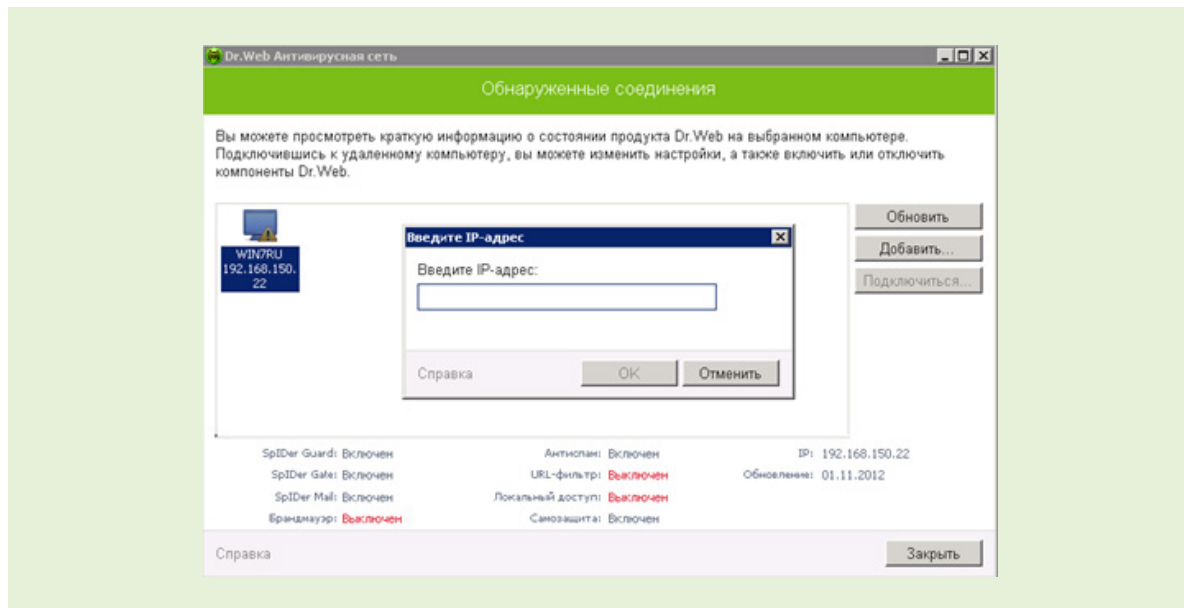


Опишем кратко назначение каждого пункта меню.

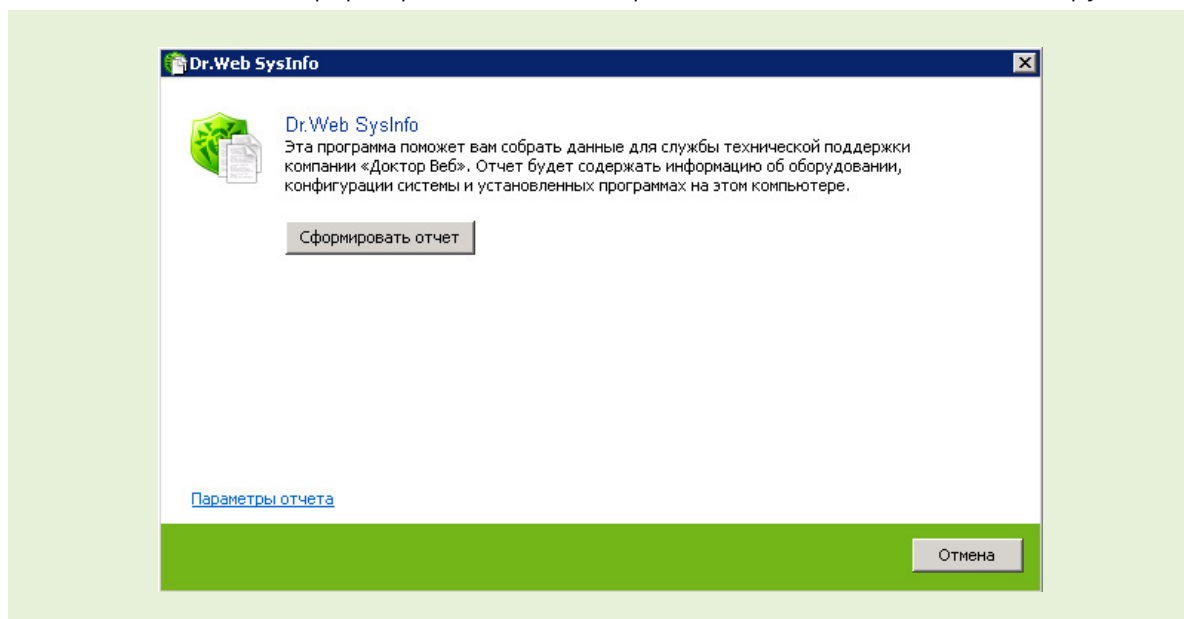
- **О программе** — открывает окно с информацией о версиях компонентов Dr.Web для файловых серверов Windows, а также о текущей версии вирусных баз.
- **Мой Dr.Web** — открывает вашу персональную страницу на сайте компании «Доктор Веб».
- **Справка** — открывает файл справки Dr.Web для файловых серверов Windows.
- **SpIDer Guard** — открывает доступ к настройкам и управлению компонента, позволяет запустить или остановить его работу.
- **Обновление** — позволяет начать процесс обновления
- **Сканер** — запускает **Сканер** Dr.Web. Можно произвести быструю (проверка только наиболее часто используемых разделов памяти компьютера), полную или выборочную (только для выбранных компонентов) проверку.
- **Отключить/Включить Самозащиту** — позволяет отключить/включить защиту файлов, веток реестра и запущенных процессов Dr.Web от повреждений и удаления вредоносными программами. Чтобы отключить **Самозащиту**, необходимо ввести защитный код, который будет выведен на экран.
- **Инструменты** — открывает подменю, предоставляющее доступ к следующим пунктам:
 - **Менеджер лицензий**
 - **Настройка** общих параметров работы Dr.Web для файловых серверов Windows
 - **Статистика** работы компонентов решения
 - **Менеджер карантина**. В этом окне вы можете просматривать и управлять содержимым Карантина, куда отправляются выбранные вами или потенциально опасные файлы.



- **Антивирусная сеть.** С помощью этого компонента вы можете управлять настройками антивирусных продуктов Dr.Web на компьютерах, доступных по локальной сети.



- **Мастер отчетов.** При обращении в службу технической поддержки может потребоваться формирование отчета о работе всех компонентов антивируса.



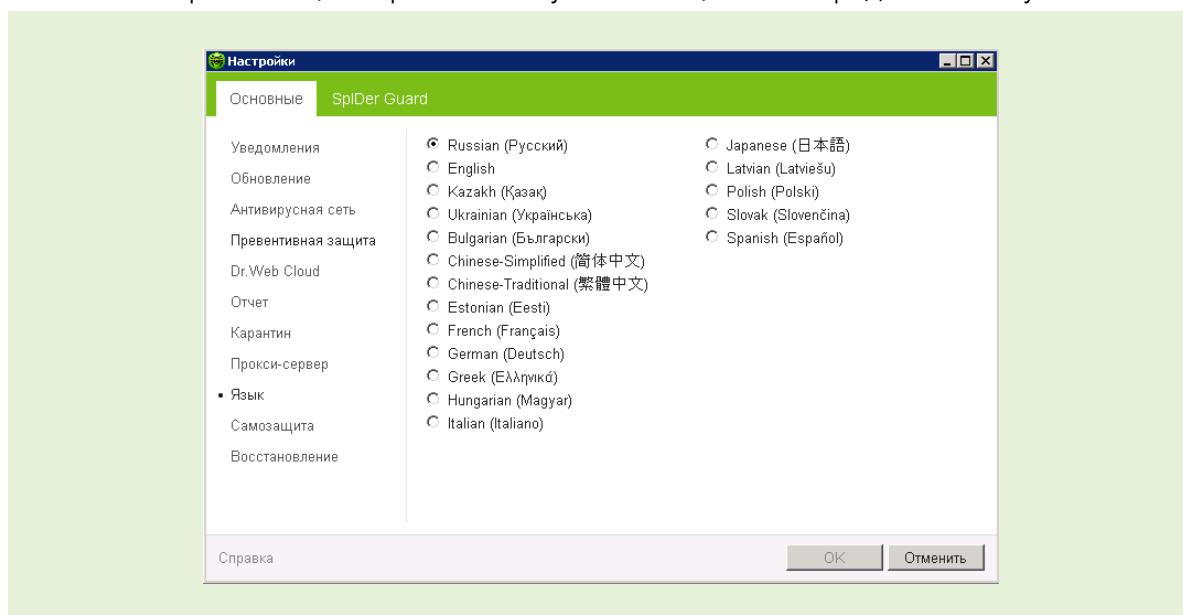
- **Административный/Пользовательский режим** — позволяет переключаться между полнофункциональным **Административным режимом** и ограниченным **Пользовательским режимом** работы с Dr.Web для файловых серверов Windows. В Пользовательском режиме действуют некоторые ограничения:
 - Недоступны настройки компонентов и пункт **Менеджер лицензий**.
 - Недоступны функции отключения всех компонентов и самозащиты.

Для переключения в **Административный режим** необходимы права администратора. Данный пункт отображается только при отсутствии административных привилегий. Например, при работе в среде операционных систем Microsoft Windows 2000 в пользовательском режиме или в среде Microsoft Windows 8 и выше при включенной системе контроля учетной записи UAC. В противном случае данный пункт недоступен и антивирус постоянно работает в полнофункциональном режиме.

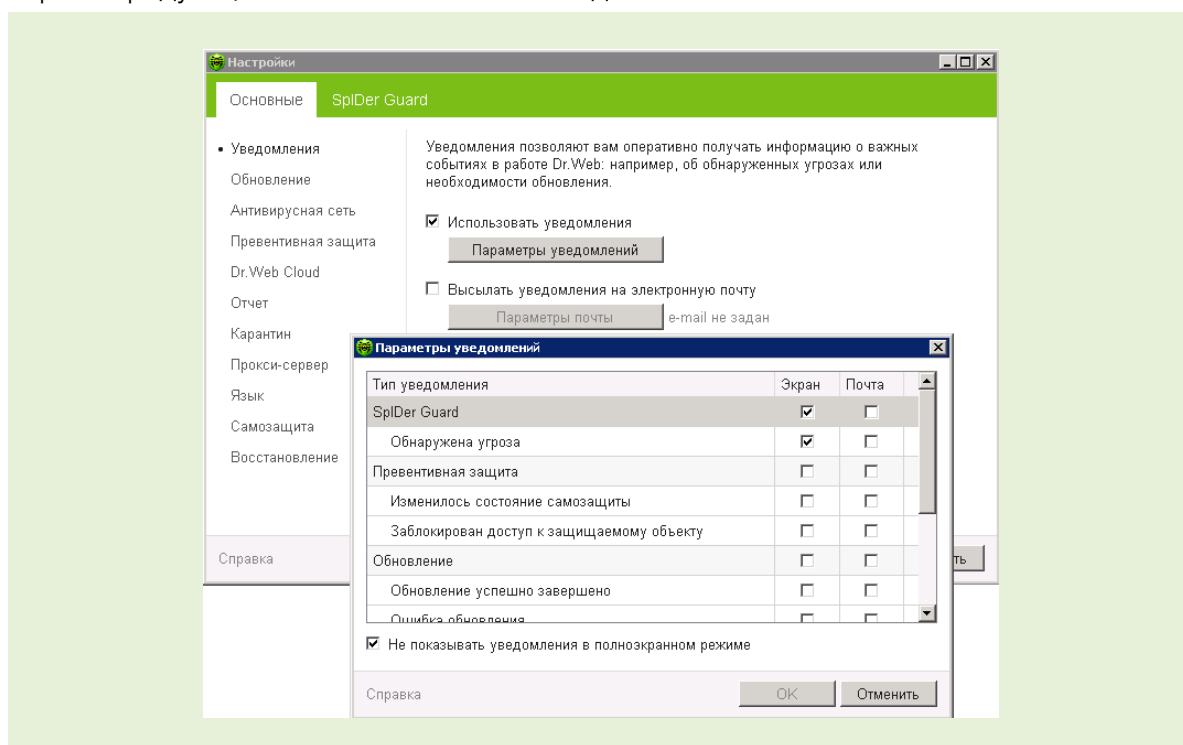
9. Задание настроек с Dr.Web для файловых серверов Windows

Окно настроек модуля управления **SpIDer Agent** позволяет задать общие параметры работы Dr.Web. Чтобы изменить их, щелкните значок **SpIDer Agent** в области уведомлений Windows. В подменю **Инструменты** выберите пункт **Настройки**. Откроется окно настроек.

Вы можете указать язык интерфейса Dr.Web, выбрав необходимый пункт в меню **Основные**. Если вы выберете язык, который не был установлен, Dr.Web предложит его установить.

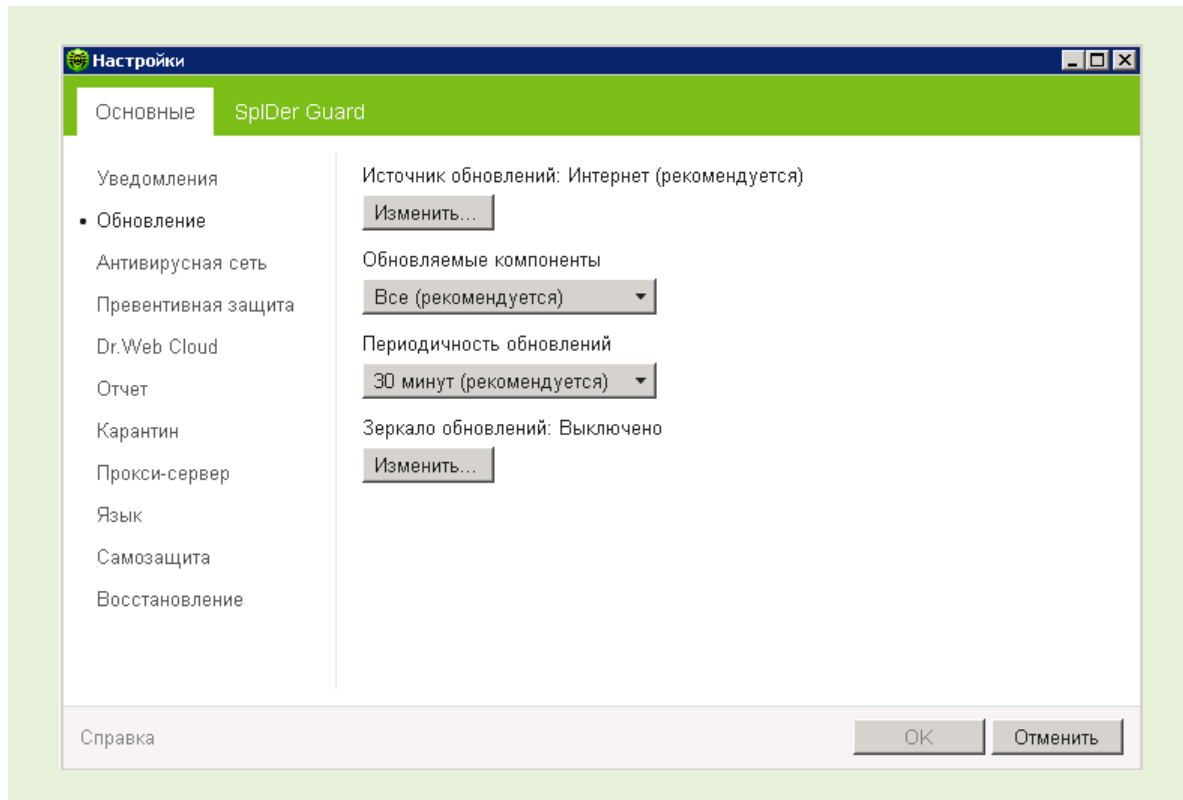


В разделе **Уведомления** можно задать типы и методы уведомлений, появляющихся в виде всплывающего окна над значком **SpIDer Agent** в области уведомлений Windows или приходящих в виде письма. Компоненты, перечисленные в группе **Типы уведомлений**, посылают уведомления в случае срабатывания соответствующей защиты. Также уведомления могут появляться при каждом обновлении вирусных баз, выходе новых версий продукта, ошибках обновления и т. д.

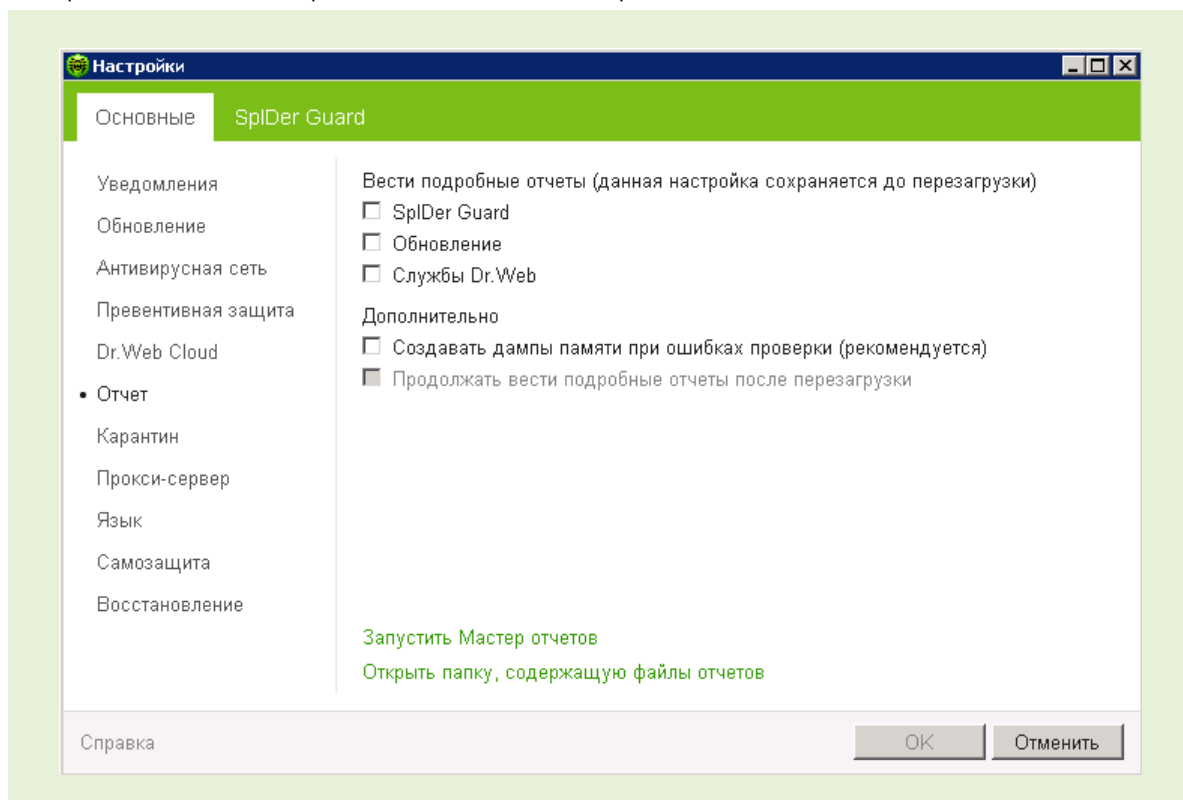


Опция **Не показывать уведомления в полноэкранном режиме** позволяет не получать уведомления при работе с приложениями в полноэкранном режиме (просмотр фильмов, графики и т. д.).

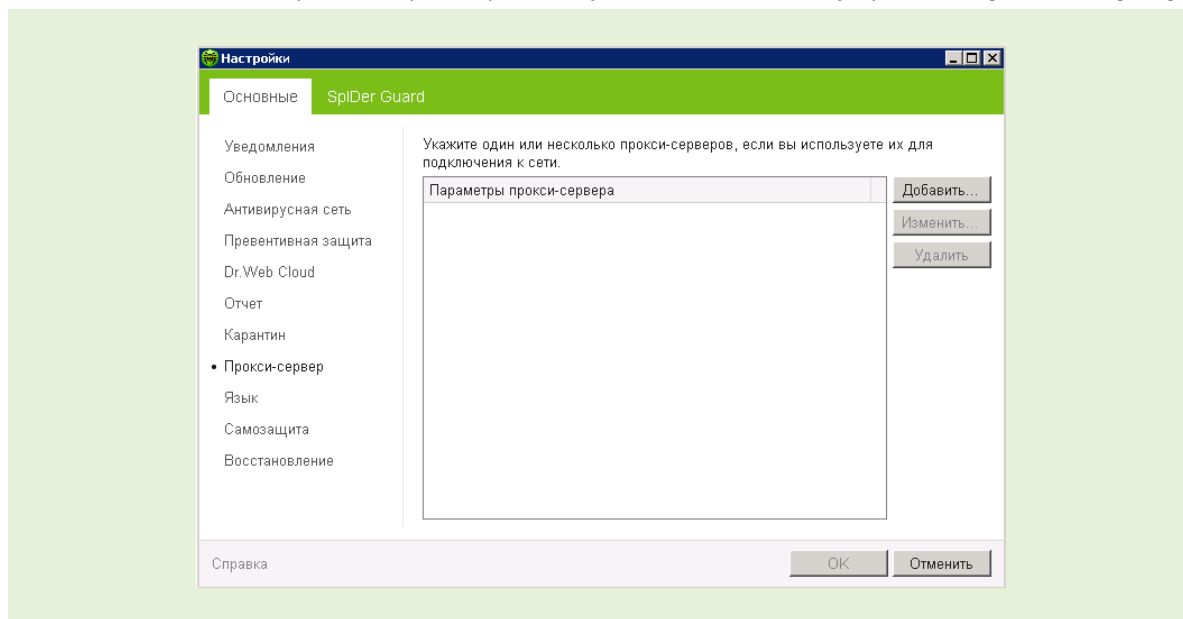
В разделе **Обновление** задаются параметры обновления компонентов и вирусных баз Dr.Web.



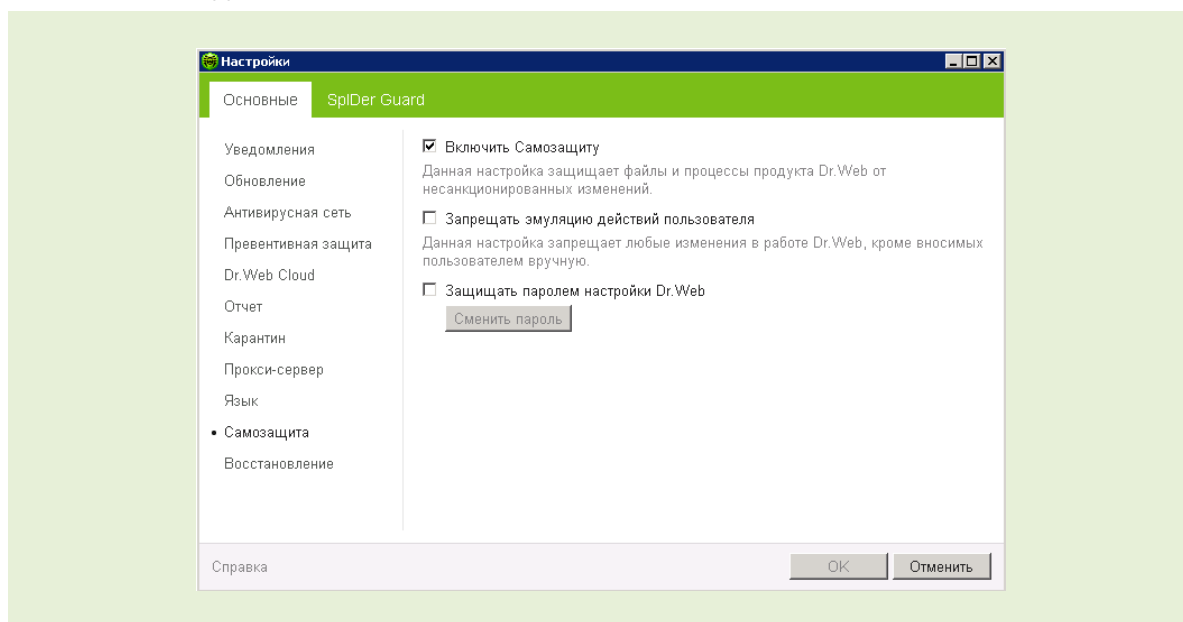
В случае необходимости получения подробной информации о работе продукты вы можете настроить степень подробности отчетов на странице **Отчет**.



Также вы можете настроить параметры доступа к сети, используя раздел **Прокси-сервер**.



Раздел **Самозащита** дает возможность настроить степень самозащиты продукта Dr.Web от внешних воздействий.



Настройка **Запрещать эмуляцию действий пользователя** позволяет предотвратить любые изменения в работе Dr.Web, производимые автоматизированно. В том числе будет запрещено исполнение скриптов, эмулирующих работу пользователя с программой Dr.Web, запущенных самим пользователем.

Настройка **Защищать паролем...** позволяет установить пароль для доступа к настройкам Dr.Web на вашем компьютере. Задайте пароль, который будет запрашиваться при обращении к настройкам Dr.Web.

10. Обновление продукта

Внимание! Для обнаружения вредоносных объектов антивирусы компании «Доктор Веб» используют специальные вирусные базы Dr.Web, в которых содержится информация обо всех известных вредоносных программах. В связи с постоянным появлением новых угроз и разработкой алгоритмов, реализованных в виде исполняемых файлов

и программных библиотек противодействия им, эти базы требуют периодического обновления. Обновление позволяет обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев — излечивать ранее неизлечимые зараженные файлы. Автоматическое обновление необходимо для поддержания выбранного вами в ходе настройки уровня безопасности компьютера.

Благодаря опыту эксплуатации антивирусов Dr.Web исправляются обнаруженные в программах ошибки, обновляется система помощи и документация, выпускаются усовершенствованные модули, позволяющие осуществлять поиск и лечение вредоносных программ с меньшими затратами системных ресурсов.

Для поддержания актуальности вирусных баз и программных алгоритмов компанией «Доктор Веб» реализована система распространения обновлений через сеть Интернет. Модуль обновления позволяет вам в течение срока действия лицензии загружать и устанавливать дополнения к вирусным базам и обновленные программные модули. Важно помнить, что для использования **Модуля обновления** необходимо иметь доступ в сеть Интернет.

Вы можете запустить обновление одним из следующих способов:

- из командной строки,
- с помощью **Модуля обновления SplDer Agent**.

При автоматическом запуске обновление проводится в «невидимом» режиме, отчет **Модуля обновления** записывается в файл `dwupdater.log` в каталоге `%allusersprofile%\Application Data\Doctor Web\Logs` (в Windows 8, `%allusersprofile%\Doctor Web\Logs`).

Работа модуля обновления определяется структурой вирусных баз и методикой обновления баз и комплекса в целом:

- В состав программного комплекса входит основная вирусная база (файл `drwebase.vdb`) и ее расширения (файлы `drw700xx.vdb`). Все вместе они содержат вирусные записи, известные в момент выпуска данной версии программного комплекса.
- Еженедельно выпускаются дополнения — файлы с вирусными записями для обнаружения и обезвреживания вирусов, выявленных за время, прошедшее с выпуска предыдущего еженедельного обновления. Еженедельные дополнения представлены файлами, наименование которых выглядит так: `drwXXXYY.vdb`, где `XXX` — номер текущей версии антивируса, а `YY` — порядковый номер еженедельного дополнения.
- По мере необходимости (обычно несколько раз в сутки) выпускаются горячие дополнения, содержащие вирусные записи для обнаружения и обезвреживания всех вирусов, выявленных после выхода последнего еженедельного дополнения. Эти дополнения выпускаются в виде файла с именем `drwtoday.vdb`. В конце дня содержимое этого файла добавляется в файл накопительного обновления `drwdaily.vdb`. Содержимое файла `drwdaily.vdb` в конце недели выпускается в виде очередного еженедельного обновления.
- В состав программного комплекса входят дополнительные базы вредоносных программ `drwnasty.vdb` и `drwrisky.vdb`. Записи, предназначенные для обнаружения рекламных программ и программ дозвона, включаются в состав вирусной базы `drwnasty.vdb`. Записи для обнаружения программ-шуток, потенциально опасных программ и программ несанкционированного доступа включаются в состав вирусной базы `drwrisky.vdb`.
- Время от времени выпускаются кумулятивные дополнения баз вредоносных программ. Горячие дополнения для этих баз могут выпускаться значительно реже, чем для основной вирусной базы.
- Время от времени выпускаются радикальные обновления самих компонентов антивирусной защиты.

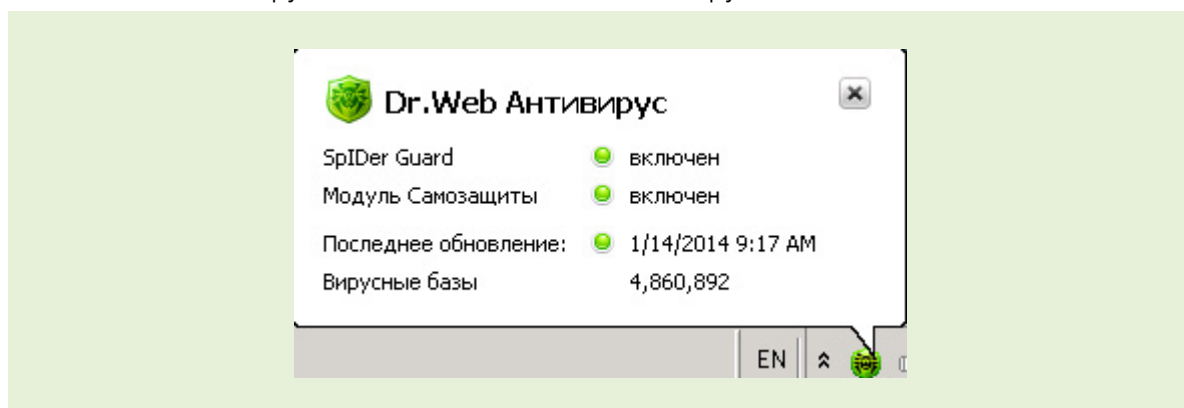
Для запуска обновления можно:

- в режиме командной строки вызвать исполняемый файл `drwupsrv.exe` из каталога установки программы;
- выбрать пункт **Обновление** контекстного меню значка **SpIDer Agent** в области уведомлений Windows.

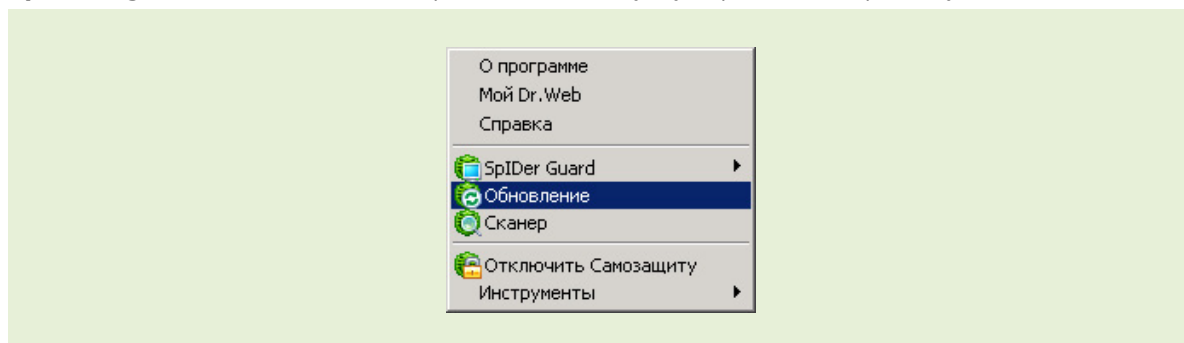
После запуска **Модуля обновления** появится диалоговое окно, в котором отображается информация об актуальности вирусных баз и компонентов, а также дата последнего обновления. При необходимости из этого окна вы можете запустить обновление. Настроить необходимые параметры вы можете в разделе **Обновление** основных настроек работы программы.

10.1. Проверка актуальности обновлений

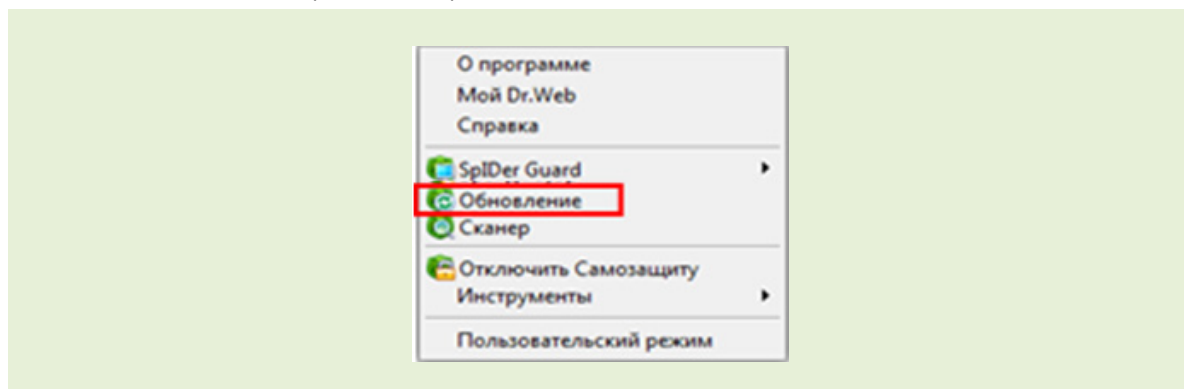
При наведении курсора мыши на значок в правом нижнем углу экрана появляется всплывающая подсказка с информацией о запущенных компонентах, а также датой последнего обновления антивируса и количеством записей в вирусных базах.



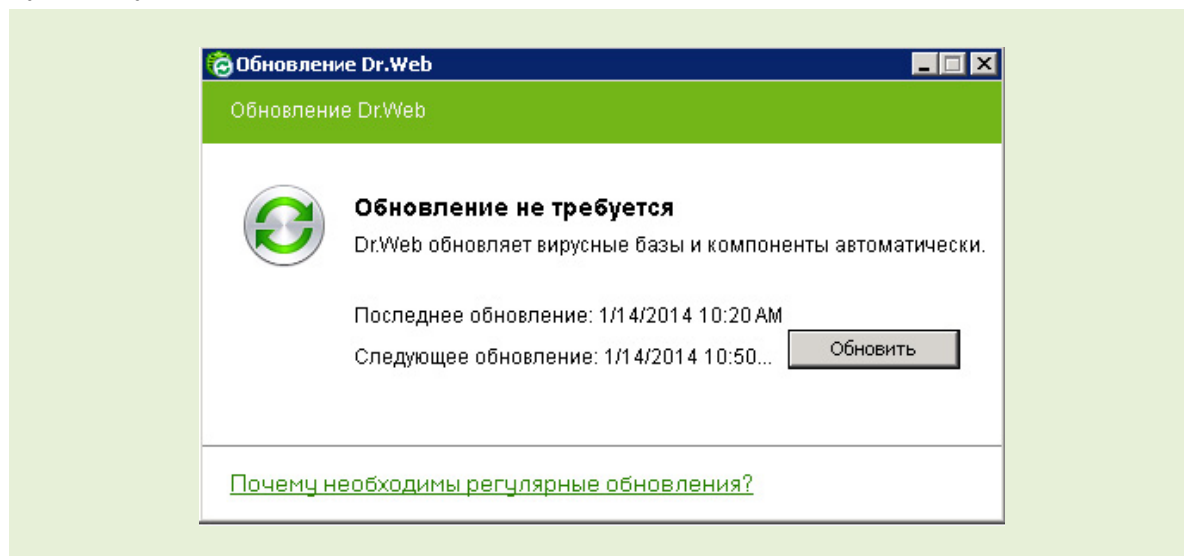
Чтобы проверить актуальность обновлений и обновить продукт вручную, из меню значка **SpIDer Agent** (значок Dr.Web в правом нижнем углу экрана) выберите пункт **Обновление**.



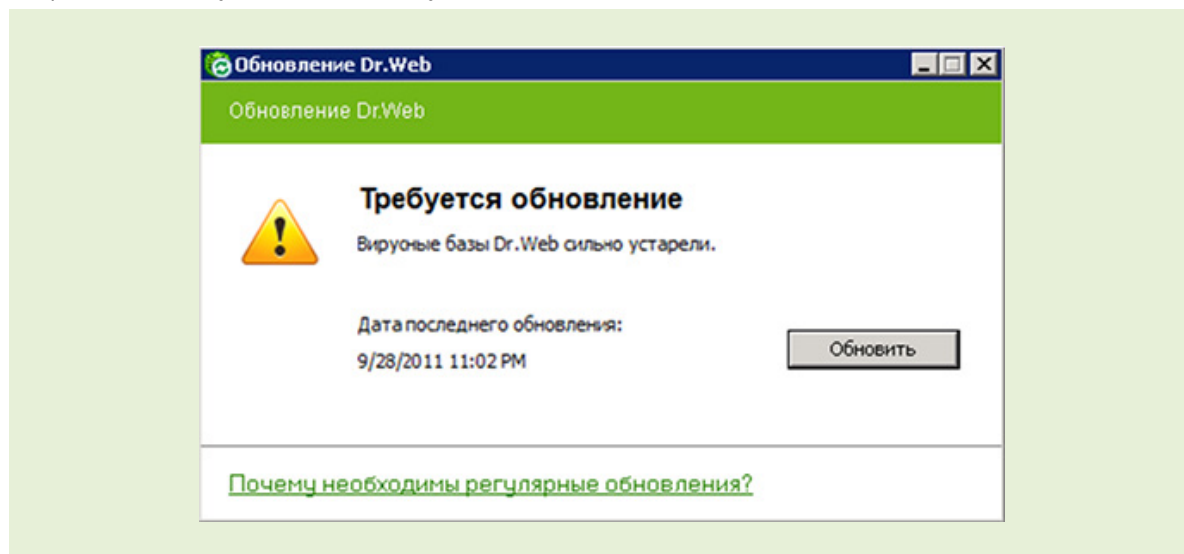
То же окно в административном режиме:



Появится диалоговое окно, в котором отображается информация об актуальности вирусных баз и компонентов, а также дата последнего обновления. Если обновления не требуются, будет показано окно:



В противном случае вид окна будет иным:



10.2. Проведение обновлений вручную

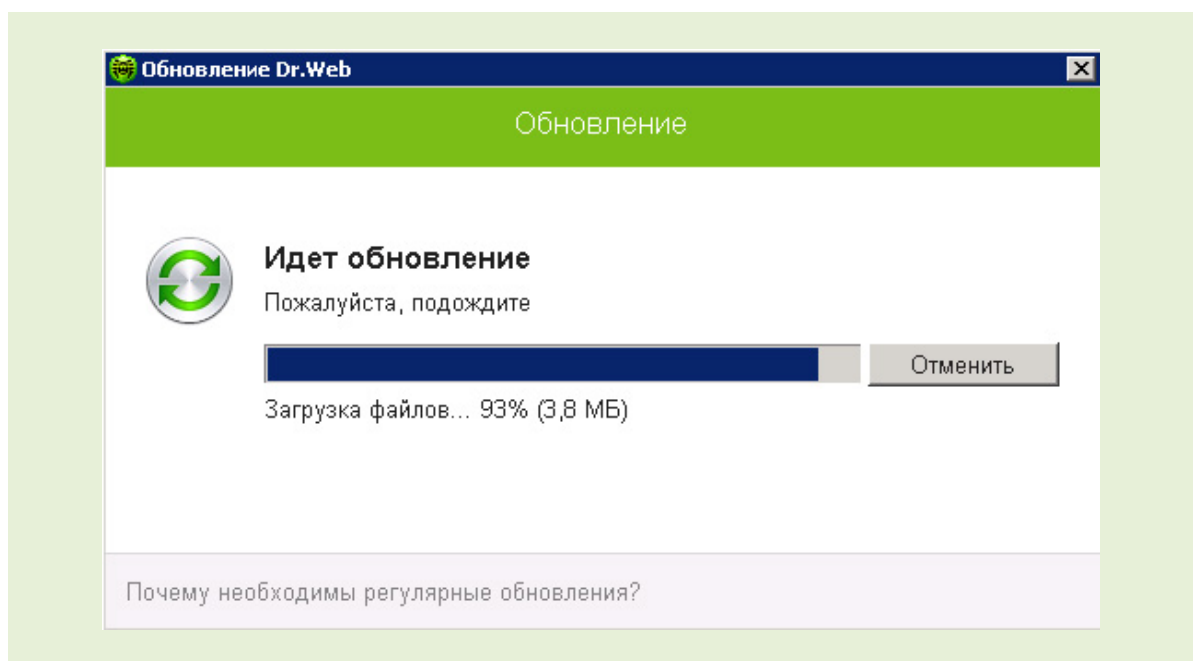
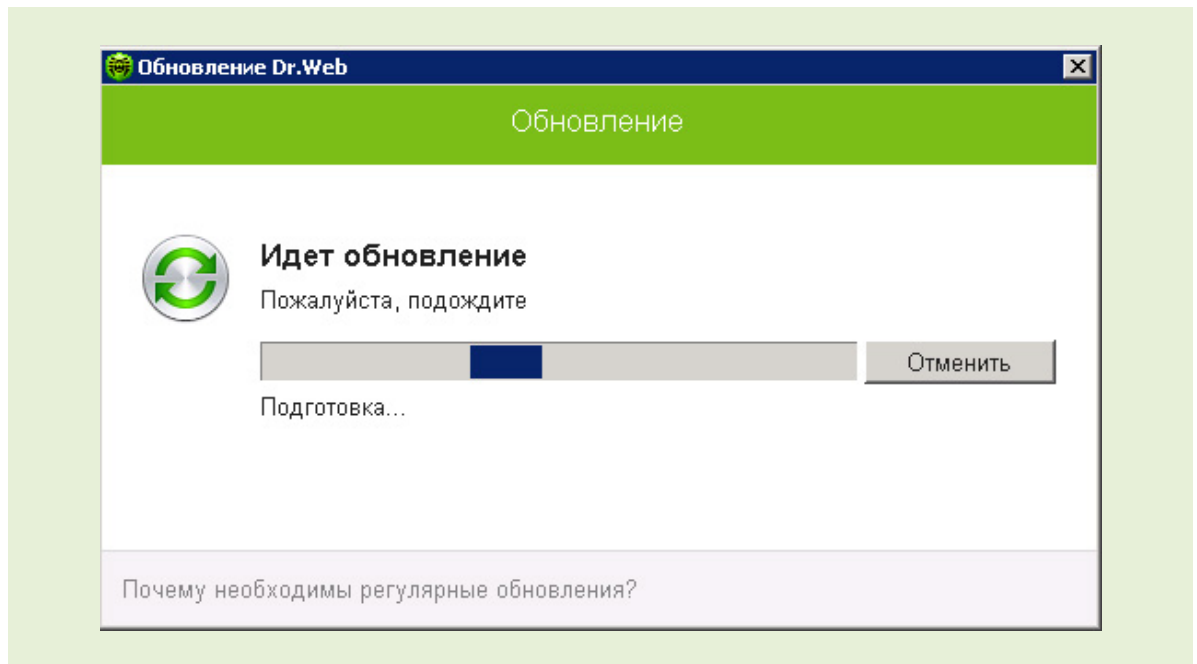
Внимание! При отсутствии ключевого файла обновление Dr.Web невозможно.

При наличии ключевого файла **Модуль обновления** проверяет, не является ли имеющийся у вас ключевой файл заблокированным на сайте компании «Доктор Веб». В случае блокировки вам выдается соответствующее сообщение, обновление не производится, а компоненты программы могут быть заблокированы. Если ваш ключевой файл был заблокирован по ошибке, свяжитесь с продавцом, у которого вы приобрели Dr.Web.

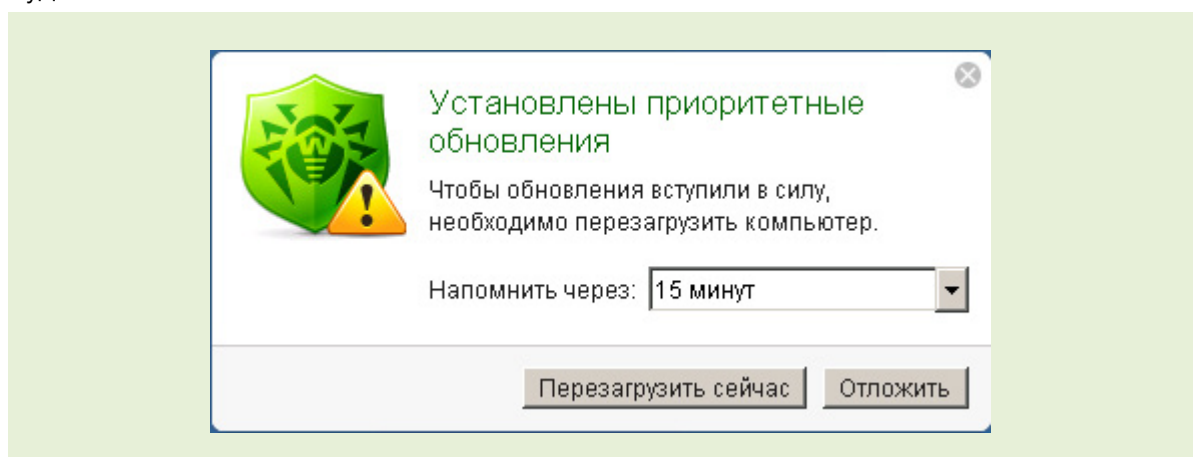
После успешной проверки ключевого файла **Модуль обновления** автоматически загружает все обновленные файлы, соответствующие вашей версии Dr.Web.

При обновлении исполняемых файлов и библиотек может потребоваться перезагрузка компьютера. Пользователь извещается об этом при помощи информационного окна. **Сканер** и **SpIDer Guard** начинают использовать обновленные базы автоматически.

Для запуска обновления необходимо из меню значка **SpIDer Agent** (значок Dr.Web в правом нижнем углу экрана) выбрать пункт **Обновление** и затем нажать на кнопку **Обновить**.

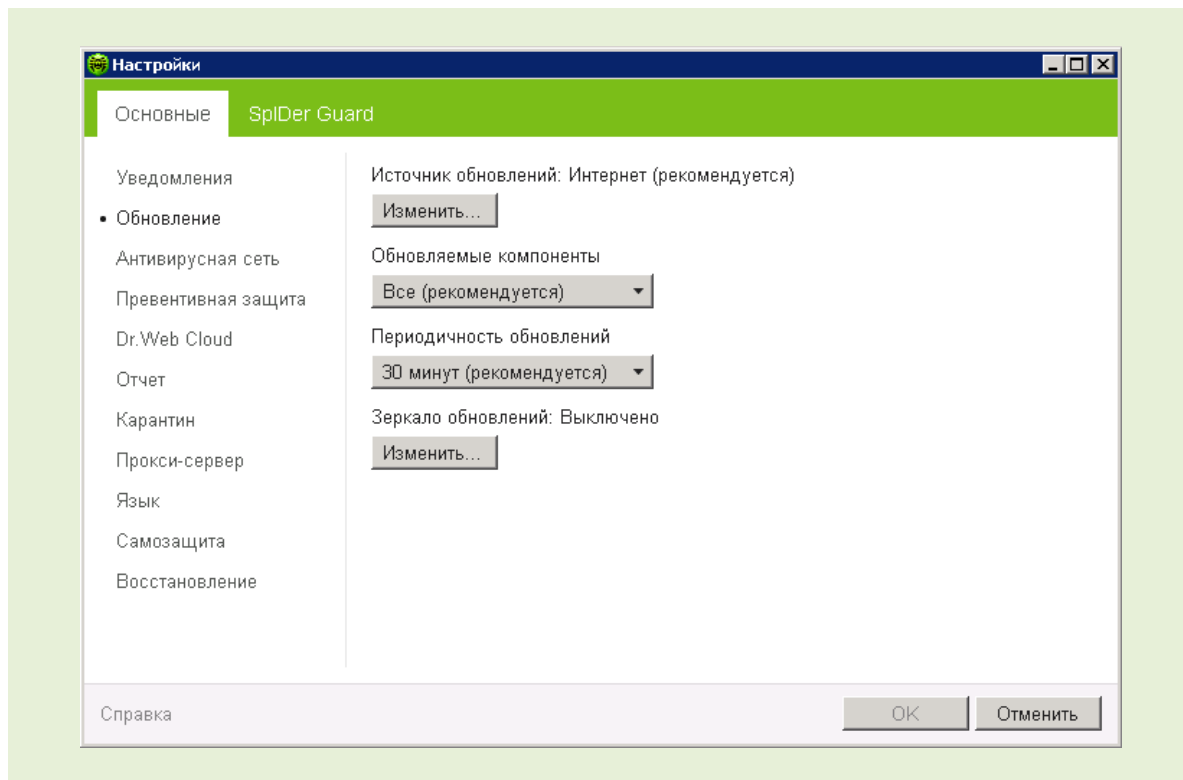


В том случае, если полученные обновления требуют для своей установки перезагрузки, будет показано окно:



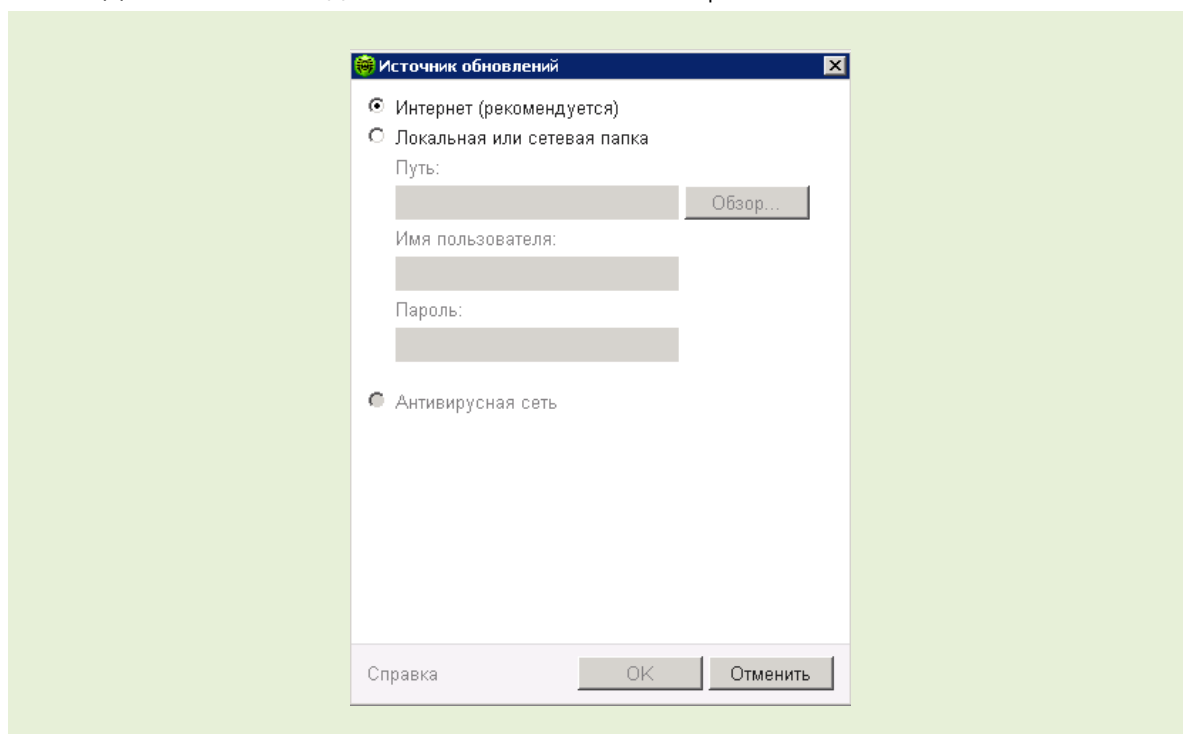
10.3. Настройка обновлений

Для настройки необходимых параметров обновлений необходимо из меню значка **SplDer Agent** (значок Dr.Web в правом нижнем углу экрана) выбрать пункт **Инструменты** → **Настройки** и перейти на пункт меню **Обновление**:

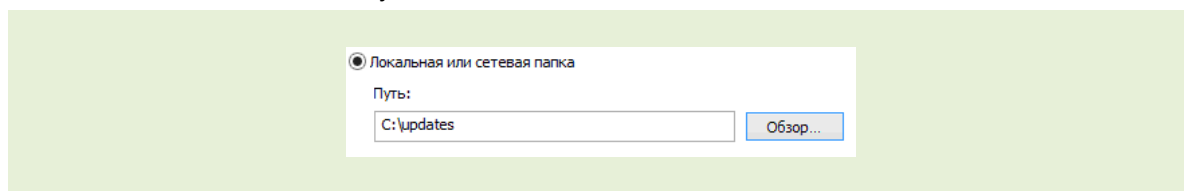


В данном разделе вы можете настроить параметры обновления Dr.Web — указать, какие компоненты необходимо обновлять, источник обновлений, а также периодичность, с которой будут происходить обновления.

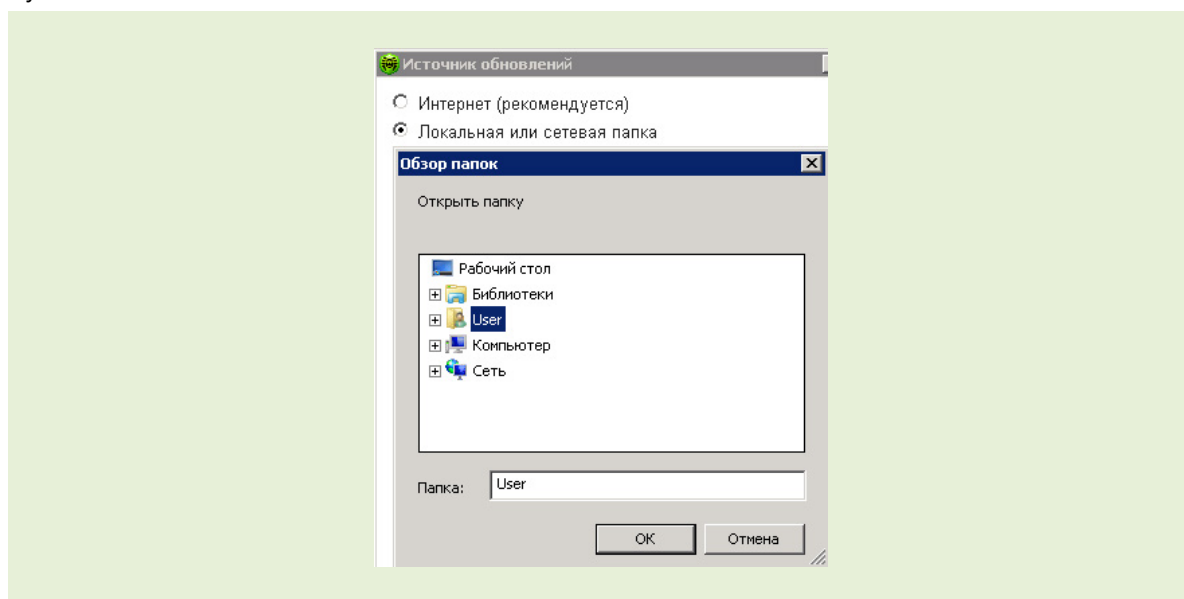
Если обновления не планируется получать с ВСО, можно указать локальный источник обновлений. Для этого необходимо нажать **Изменить**. Откроется окно **Источник обновлений**.



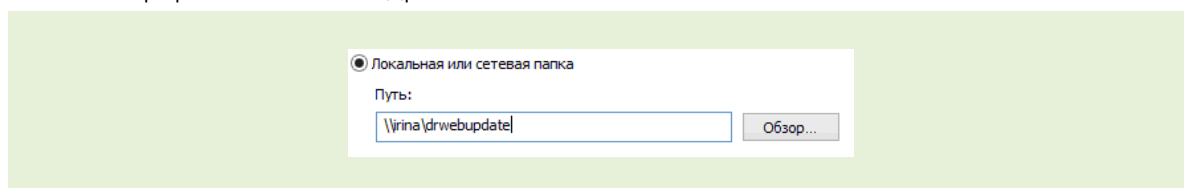
Программа может получать обновления из локальной или сетевой папки.
Источники обновления могут быть локальными и сетевыми.



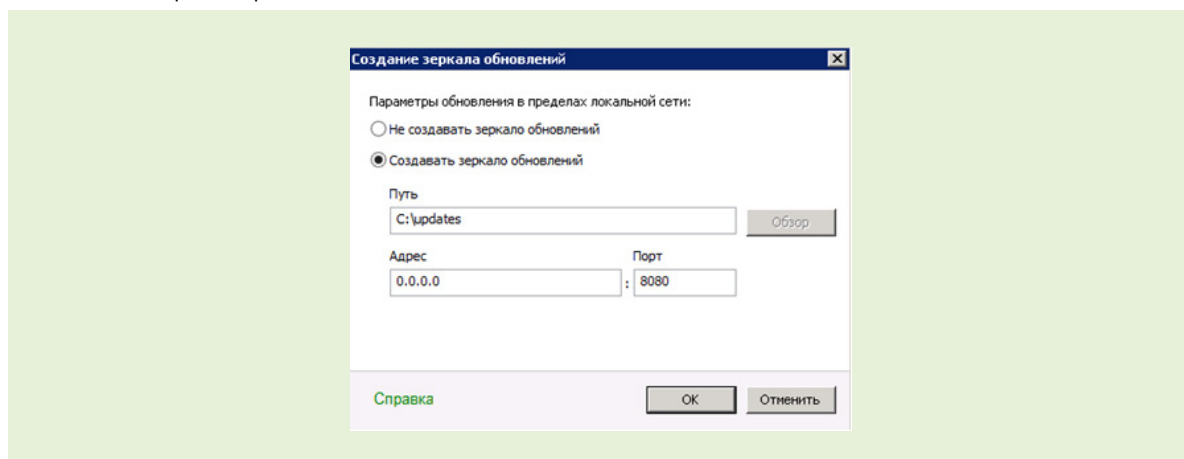
Чтобы установить в качестве источника обновлений локальную папку, включите опцию **Локальная или сетевая папка** и нажмите **Обзор**. Выберите место размещения источника обновления — папку или сетевой ресурс и нажмите **ОК**. В поле **Путь** отобразится полный путь к папке с обновлениями.



В случае нахождения источника обновления на разделяемом общем ресурсе задайте путь к папке в формате сетевых адресов.

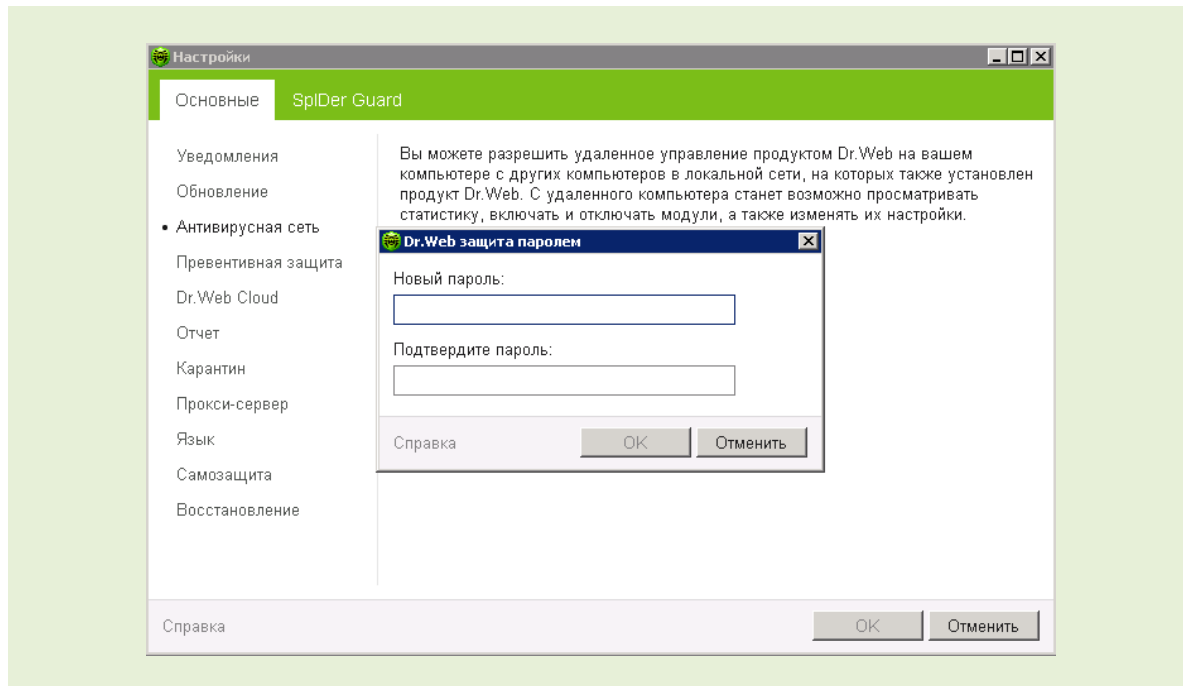


Если обновления в сети предполагается проводить с локально созданного зеркала, то можно задать параметры его создания.



При загрузке необходимых файлов с одного из компьютеров в сети на компьютере, с которого будет производиться обновление, необходимо включить поддержку удаленного управления по сети и функцию создания локального зеркала обновлений. В окне **Настройки** перейдите в пункт **Антивирусная сеть** и включите опцию **Разрешить удаленное управление**.

В открывшемся окне **Dr.Web защита паролем** введите пароль, который будет использоваться для удаленного доступа к настройкам Dr.Web по сети, и нажмите **OK**.

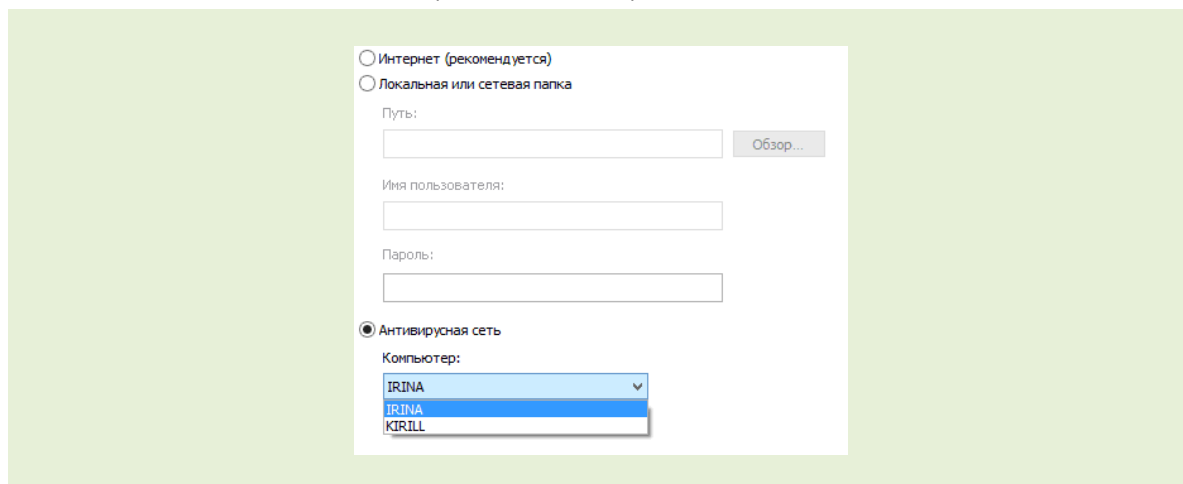


После определения параметров зеркала вернитесь в пункт **Обновление**. Нажмите **Изменить** и в окне **Создание зеркала обновлений** в поле **Путь** пропишите путь к предварительно созданной папке для загрузки обновлений. Эту папку также можно найти с помощью кнопки **Обзор**. Нажмите **OK**.

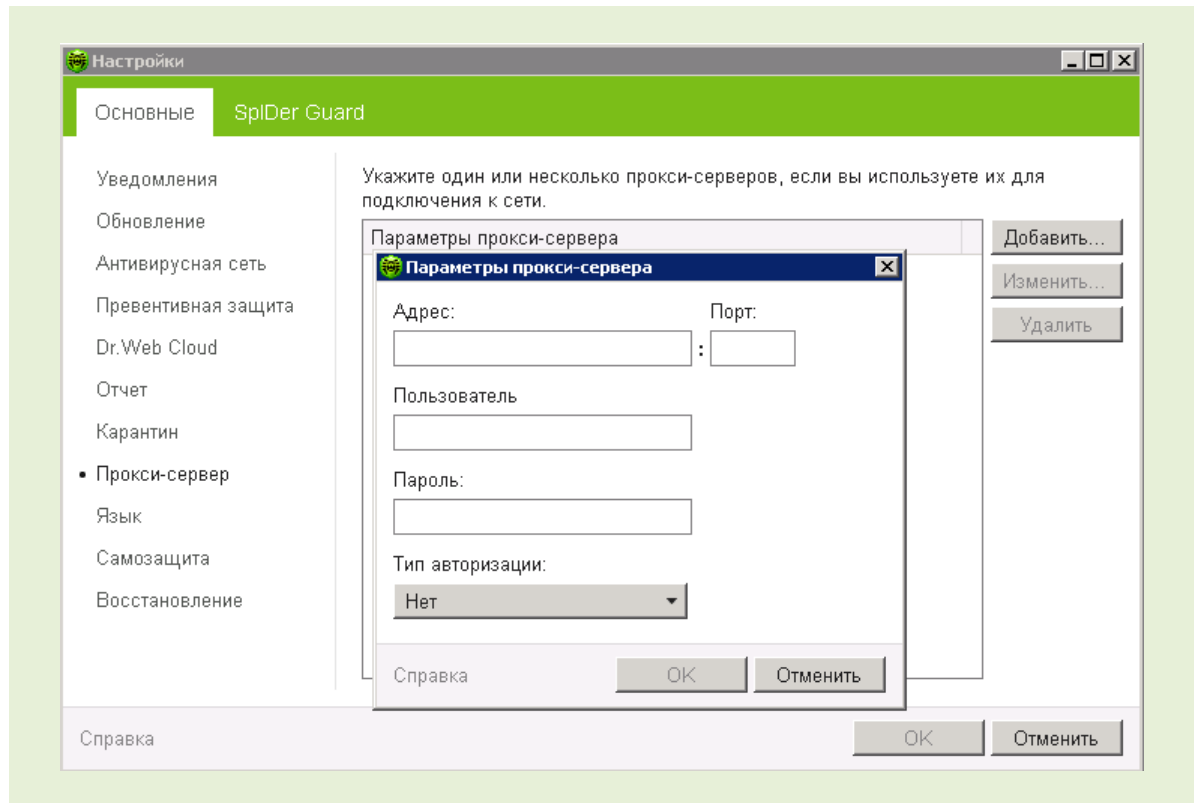
Наведите курсор мыши на значок **Dr.Web** в системном трее, нажмите правую клавишу мыши и выберите пункт **Обновление**.

Начнется процесс обновления программы, в ходе которого будет создан локальный репозиторий.

На всех компьютерах, которые должны получать обновления из компьютера — источника обновлений, сделайте следующие настройки. Перейдите в пункт **Обновление** и нажмите **Изменить**. В окне **Источник обновлений** отметьте опцию **Антивирусная сеть**. С помощью выпадающего списка выберете компьютер-источник:

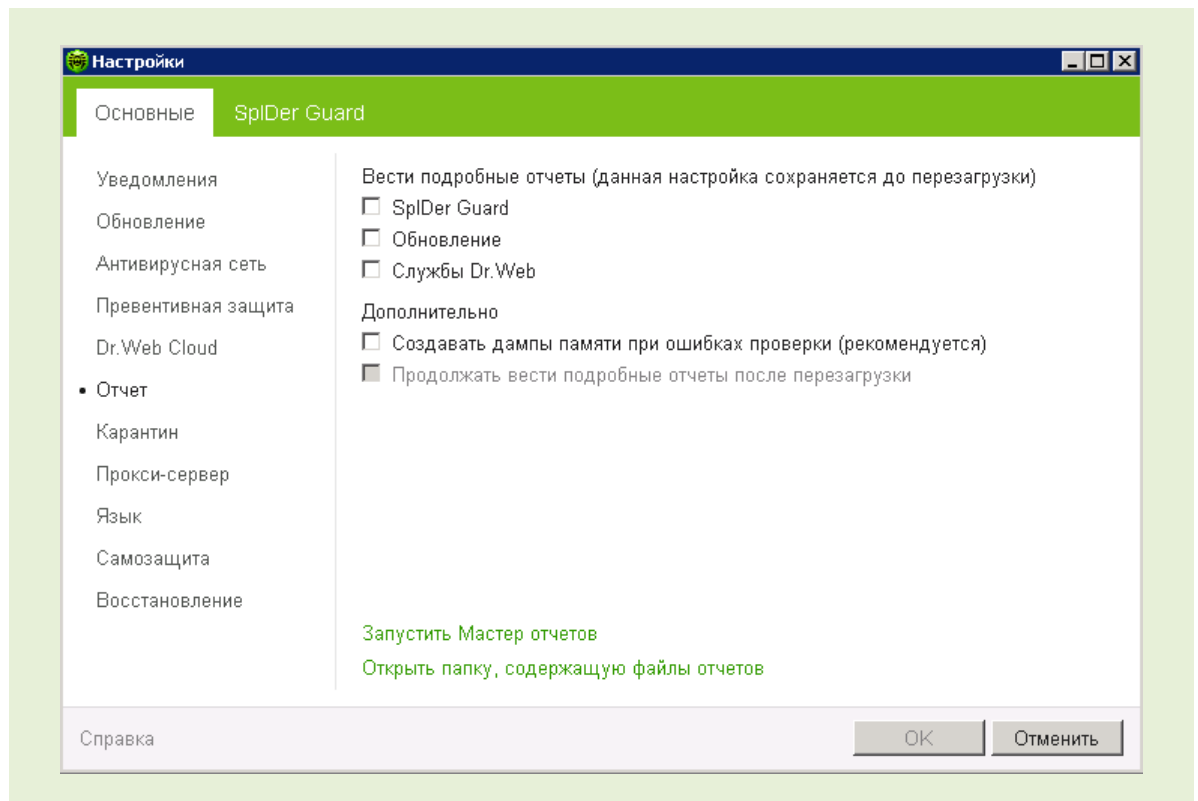


Также вы можете настроить параметры доступа к сети. Для этого перейдите к пункту меню **Прокси-сервер** и в случае его наличия нажмите кнопку **Добавить**.



Если не возникло проблем с подключением к Интернету, настройки на этой странице рекомендуется оставить без изменений.

Также в разделе настроек отчетов вы можете установить флаг **Вести подробные отчеты** для интересующих вас компонентов, для того чтобы отчет об изменениях содержал более подробную информацию.



10.4. Настройки, которые можно задать только в командной строке

Если запуск Dr.Web Updater происходит с использованием ключей командной строки, то соответствующие настройки реестра игнорируются.

Общие параметры:

- `-h [--help]` Вывести на экран краткую справку о работе с программой.
- `-v [--verbosity] arg` Уровень детализации отчета: `error` (стандартный), `info` (расширенный), `debug` (отладочный).
- `-d [--data-dir] arg` Каталог, в котором размещены репозиторий и настройки.
- `--log-dir arg` Каталог, в котором будет сохранен отчет.
- `--log-file arg (=dwupdater.log)` Имя файла отчета.
- `-r [--repo-dir] arg` Каталог репозитория, (по умолчанию `<data_dir>/repo`).
- `-t [--trace]` Включить трассировку.
- `-c [--command] arg (=update)` Выполняемая команда: `getversions` – получить версии, `getcomponents` – получить компоненты, `init` – инициализация, `update` – обновление, `uninstall` – удалить, `exec` – выполнить, `keyupdate` – обновить ключ, `download` – скачать.
- `-z [--zone] arg` Список зон, который будет использоваться вместо заданных в конфигурационном файле.

Параметры команды инициализации (init):

- `-s [--version] arg` Номер версии.
- `-p [--product] arg` Название продукта.
- `-a [--path] arg` Путь, по которому будет установлен продукт. Этот каталог будет использоваться по умолчанию в качестве каталога для всех компонентов, включенных в продукт. Модуль обновления будет проверять наличие ключевого файла именно в этом каталоге.
- `-n [--component] arg` Имя компонента и каталог установки в формате `<name>`, `<install path>`.
- `-u [--user] arg` Имя пользователя прокси-сервера.
- `-k [--password] arg` Пароль пользователя прокси-сервера.
- `-g [--proxy] arg` Прокси-сервер для обновления в формате `<адрес>: <порт>`.
- `-e [--exclude] arg` Имя компонента, который будет исключен из продукта при установке.

Параметры команды обновления (update):

- `-p [--product] arg` Название продукта. Если название указано, то будет произведено обновление только этого продукта. Если продукт не указан и не указаны конкретные компоненты, будет произведено обновление всех продуктов. Если указаны компоненты, будет произведено обновление указанных компонентов.
- `-n [--component] arg` Перечень компонентов, которые необходимо обновить до определенной модификации. Формат: `<name>`, `<target revision>`.
- `-x [--selfrestart] arg (=yes)` Перезапуск после обновления модуля обновления. По умолчанию значение `yes`. Если указано значение `no`, то выводится предупреждение о необходимости перезапуска.
- `--geo-update` Получить список IP-адресов `update.drweb.com` перед обновлением.
- `--type arg (=normal)` В зависимости от аргумента может выполнять следующие действия:

- `reset-all` – принудительное обновление всех компонентов;
- `reset-failed` – сбросить все изменения для поврежденных компонентов;
- `normal-failed` – попытаться обновить компоненты, включая поврежденные, до последней либо до указанной версии;
- `update-revision` – обновить компоненты в пределах текущей ревизии;
- `normal` – обновить все компоненты.
- `-g [--proxy] arg` Прокси-сервер для обновления в формате `<адрес>: <порт>`.
- `-u [--user] arg` Имя пользователя прокси-сервера.
- `-k [--password] arg` Пароль пользователя прокси-сервера.
- `--param arg` Передать дополнительные параметры в скрипт. Формат: `<имя>: <значение>`.
- `-l [--progress-to-console]` Вывести на консоль информацию о загрузке и выполнении скрипта.

Особые параметры команды исполнения (`exec`):

- `-s [--script] arg` Выполнить указанный скрипт.
- `-f [--func] arg` Выполнить функцию скрипта.
- `-p [--param] arg` Передать дополнительные параметры в скрипт. Формат: `<имя>: <значение>`.
- `-l [--progress-to-console]` Вывести на консоль информацию о прогрессе выполнения скрипта.

Параметры команды получения компонентов (`getcomponents`):

- `-s [--version] arg` Номер версии.
- `-p [--product] arg` Укажите имя продукта, чтобы увидеть, какие компоненты он включает. Если продукт не указан, будут выведены все компоненты этой версии.

Параметры команды получения изменений (`getrevisions`):

- `-s [--version] arg` Номер версии.
- `-n [--component] arg` Имя компонента.

Параметры команды удаления (`uninstall`):

- `-n [--component] arg` Имя компонента, который необходимо удалить.
- `-l [--progress-to-console]` Вывести информацию о выполнении команды на консоль.
- `--param arg` Передать дополнительные параметры в скрипт. Формат: `<имя>: <значение>`.
- `-e [--add-to-exclude]` Компоненты, которые будут удалены и их обновление производиться не будет.

Параметры команды автоматического обновления ключа (`keyupdate`):

- `-m [--md5] arg` Контрольная сумма md5 старого ключевого файла.
- `-o [--output] arg` Имя файла.
- `-b [--backup]` Резервное копирование старого ключевого файла, если он существует.
- `-g [--proxy] arg` Прокси-сервер для обновления в формате `<адрес>: <порт>`.
- `-u [--user] arg` Имя пользователя прокси-сервера.
- `-k [--password] arg` Пароль пользователя прокси-сервера.
- `-l [--progress-to-console]` Вывести на консоль информацию о загрузке ключевого файла.

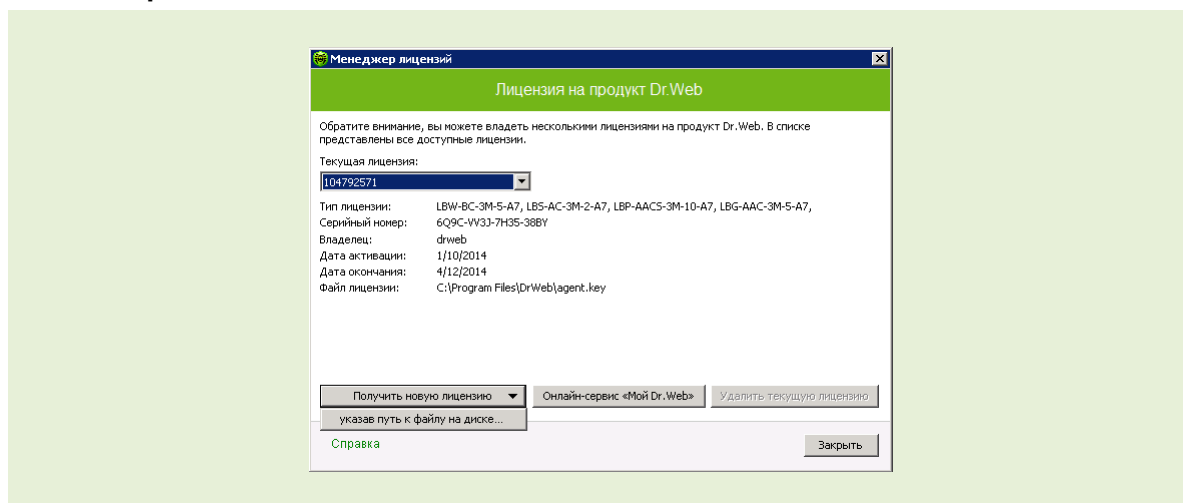
Параметры команды скачивания (download):

- `--zones arg` Файл, содержащий список зон.
- `--key-dir arg` Каталог, в котором находится ключевой файл.
- `-l [--progress-to-console]` Вывести информацию о выполнении команды на консоль.
- `-g [--proxy] arg` Прокси-сервер для обновления в формате <адрес>: <порт>.
- `-u [--user] arg` Имя пользователя прокси-сервера.
- `-k [--password] arg` Пароль пользователя прокси-сервера.
- `-s [--version] arg` Имя версии
- `-p [--product] arg` Название продукта, который необходимо скачать.

11. Продление лицензии. Замена ключевого файла

Внимание! Ключевой файл поставляется в виде файла с расширением `.key` или в виде ZIP-архива, содержащего этот файл. В файле содержится информация об используемом продукте, он необходим для нормальной работы антивируса.

В некоторых случаях ключевой файл необходимо заменить. Это может понадобиться, например, при истечении срока действия имеющейся лицензии или приобретении лицензионного ключевого файла после использования демонстрационного. Чтобы узнать параметры вашей лицензии или продлить ее срок действия, зайдите в меню **Инструменты** → **Менеджер лицензий**.



11.1. Замена ключевого файла

Вы можете получить ключевой лицензионный файл одним из следующих способов:

- при помощи регистрации продукта вручную на официальном сайте «Доктор Веб»;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в комплект поставки;
- на отдельном носителе.

Рассмотрим случай, когда ключевой файл необходимо заменить. Это может понадобиться, например, при истечении срока действия имеющейся лицензии (чтобы проверить, сколько осталось, просто зайдите в раздел **Менеджер лицензий**).

Чтобы продлить лицензию, используйте **Менеджер лицензий**. Для приобретения новой лицензии или продления текущей лицензии вы также можете воспользоваться вашей персональной страничкой на официальном сайте компании «Доктор Веб», которая

открывается в окне интернет-браузера по умолчанию при выборе пункта **Мой Dr.Web** как в **Менеджере лицензий**, так и в меню **SpIDer Agent**. Если текущий ключевой файл недействителен, Dr.Web переключится на использование нового ключевого файла.

12. Настройка параметров постоянной антивирусной защиты

12.1. Настройка файлового сторожа

Антивирусный сторож **SpIDer Guard** постоянно находится в оперативной памяти компьютера, осуществляя проверку файлов «на лету», а также обнаруживая проявления вирусной активности.

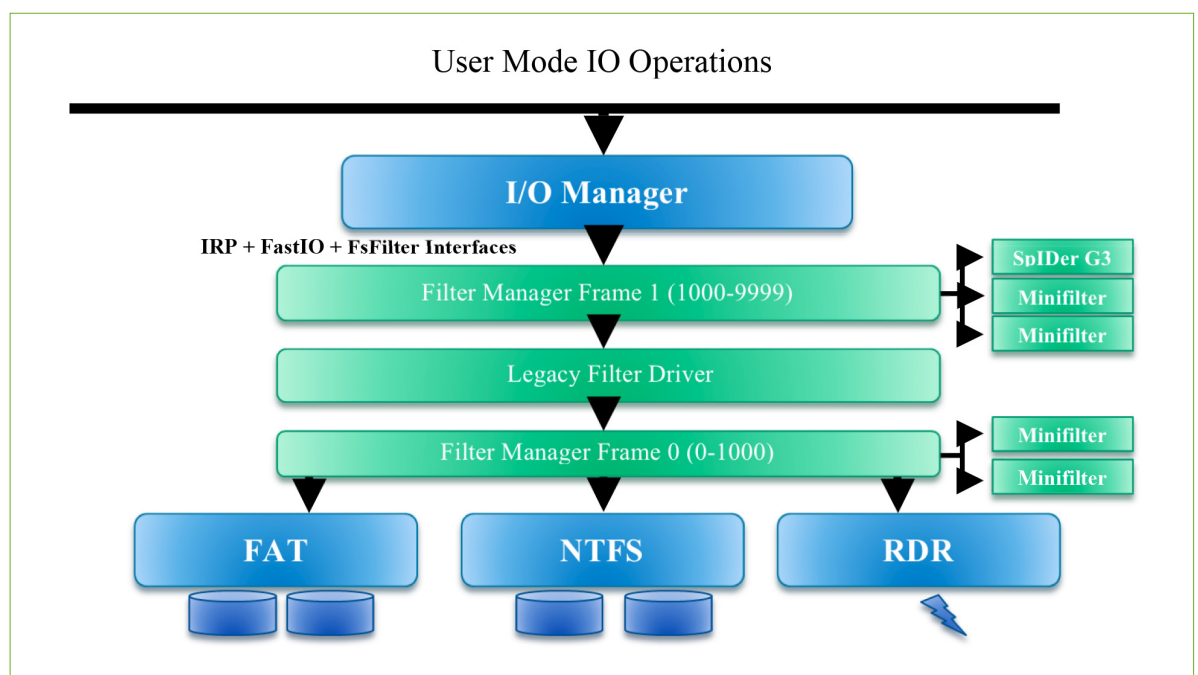
Все настройки SpIDer Guard G3 хранятся в системном реестре Windows, в ветке:

```
HKKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\Scanning Engine\SpIDer Guard\Settings.
```

Внимание! Изменение ключей реестра влияет на систему, подразделения на пользователей не предусмотрено. Если опция может быть активной или неактивной, значение ключа "0" — выключает ее, значение "1" — включает. Значение, стоящее по умолчанию, указано первым.

Файловый монитор — наиболее гибкий из компонентов антивирусной системы в смысле количества настроек, которые можно задать в реестре. Большинство настроек, которые можно произвести через интерфейс SpIDer Guard, применяются сторожем без перезагрузки.

В отличие от предыдущей версии, в SpIDer Guard G3 разработана новая архитектура, базирующаяся на технологии мини-фильтров (Minifilter). Суть построения фильтра: имеется фильтр-менеджер и два фрейма. Только фильтр-менеджер обрабатывает все запросы, что в разы ускоряет работу системы. Все остальное, в том числе SpIDer Guard, — это мини-фильтры. Всеми поступающими запросами управляет фильтр-менеджер, распределяя их по соответствующим мини-фильтрам. Плюсы архитектуры: нет конфликтов между фильтрами, все основные операции по обработке запросов на себя берет фильтр-менеджер, а все остальные (в том числе SpIDer Guard) используют ресурсы самой ОС.



Архитектура SpIDer Guard G3

SplDer Guard запускается автоматически при каждой загрузке операционной системы, при этом запущенный сторож не может быть выгружен в течение текущего сеанса работы операционной системы. При необходимости (например, в случае выполнения критически чувствительного к загрузке процессора задания в реальном масштабе времени) вы можете временно отключить сканирование файлов «на лету».

При настройках по умолчанию сторож **SplDer Guard** «на лету» проверяет все создаваемые или изменяемые файлы и загрузочные секторы, а на сменных носителях — также все открываемые файлы. Сканирование проводится аналогично тому, как работает **Сканер Dr.Web**, однако с более «мягкими» условиями проверки. Кроме того, сторож **SplDer Guard** постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при обнаружении угроз безопасности блокирует соответствующие процессы.

По умолчанию файлы внутри архивов и почтовые ящики не проверяются. Если какой-либо файл в архиве или почтовом вложении инфицирован, то вредоносный объект будет обнаружен сторожем при извлечении файла до появления возможности заражения компьютера. Включение проверки архивов или почтовых файлов значительно увеличивает нагрузку на компьютер.

При обнаружении зараженных объектов сторож **SplDer Guard** применяет к ним действия согласно установленным настройкам. Соответствующим изменением настроек вы можете изменить автоматическую реакцию сторожа на вирусные события. Результаты работы сторожа отражаются в окне статистики и файле отчета.

Следует помнить, что настройки программы по умолчанию являются оптимальными для большинства применений, их не следует изменять без необходимости.

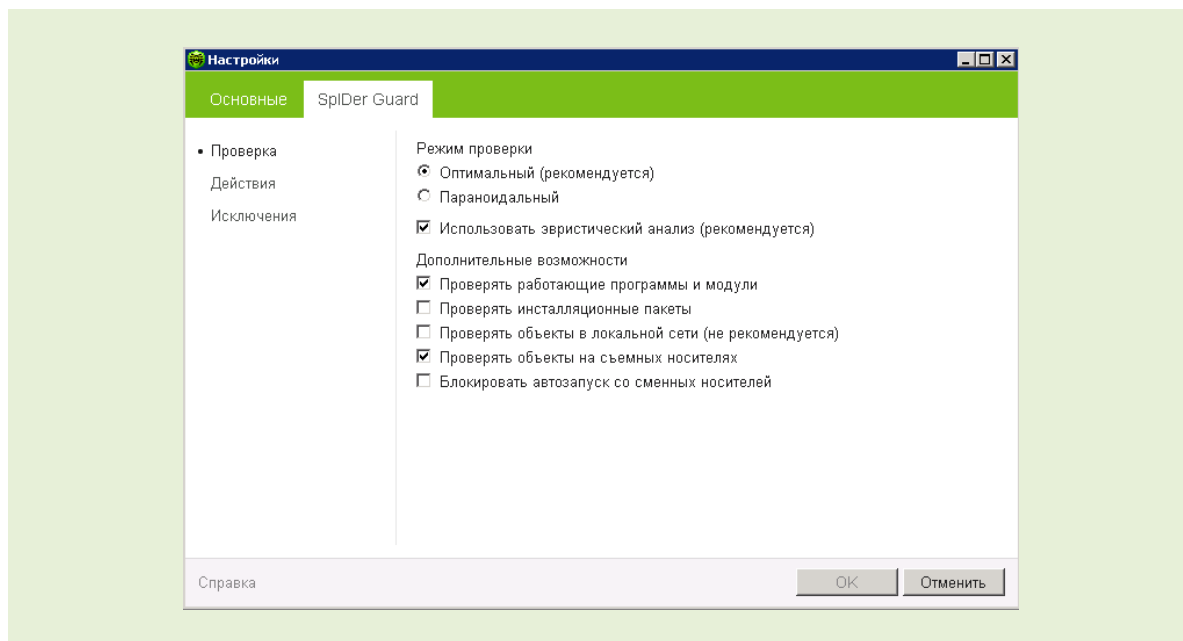
Основные средства настройки и управления сторожем SplDer Guard сосредоточены в группе **SplDer Guard** контекстного меню **SplDer Agent**. Группа **SplDer Guard** включает следующие пункты:

- **Статистика** — открывает окно, содержащее сведения о работе сторожа в течение текущего сеанса (количество проверенных, зараженных и подозрительных объектов, предпринятые действия и др.). В этом же окне можно посмотреть статистику и по другим модулям антивируса, для этого нужно кликнуть на соответствующий модуль в левой части окна.
- **Настройки** (данный пункт недоступен в пользовательском режиме) — предоставляет доступ к основной части настраиваемых параметров сторожа **SplDer Guard**.
- **Отключить/Включить** (данный пункт недоступен в пользовательском режиме) — позволяет временно отключить сканирование файлов в режиме реального времени с помощью сторожа SplDer Guard. Пункт **Включить** появляется в меню в том случае, когда сканирование файлов было приостановлено.

Вы можете временно отключать антивирусную проверку, выполняемую сторожем **SplDer Guard**. При этом снимается блокировка файлов, установленная сторожем в соответствии с настройками реакций на вирусные события. Будьте осторожны: в период отключения функций сторожа не следует подключаться к сети Интернет, а также считывать файлы с носителей, не проверенных **Сканером Dr.Web**. Чтобы отключить функции сторожа, откройте контекстное меню значка **SplDer Agent**, затем в подменю **SplDer Guard** выберите пункт **Отключить**. При отключении **SplDer Guard** запрашивается код подтверждения или пароль (если на вкладке **Дополнительно** настроек **SplDer Agent** вы установили флажок **Защищать паролем настройки Dr.Web**). Не забудьте после выполнения необходимых действий снова включить **Сторож**.

Чтобы приступить к настройке сторожа, откройте контекстное меню значка **SplDer Agent**. В подменю **SplDer Guard** выберите пункт **Настройки**. Откроется окно настроек, содержащее следующие разделы:

- Раздел **Проверка**, в котором задается режим проверки файлов и процессов защищаемого компьютера.



В группе настроек **Режим проверки** задается, при каких действиях с объектом должна производиться его проверка сторожем **SplDer Guard**.

По умолчанию установлен режим проверки **Оптимальный**: сканирование на жестких дисках — только запускаемых, создаваемых или изменяемых файлов, на сменных носителях и сетевых дисках — всех открываемых файлов.

В режиме **Параноидальный** производится проверка всех открываемых, создаваемых или изменяемых файлов на жестких дисках, сменных носителях и сетевых дисках. При включенной опции любое обращение к файлу будет заблокировано и проверено **SplDer Guard**. Включать не рекомендуется, поскольку очень резко возрастает нагрузка на систему.

Группа настроек **Дополнительные возможности** позволяет задать параметры проверки «на лету», которые будут применяться вне зависимости от выбранного режима работы сторожа SplDer Guard.

Опция **Проверять объекты в локальной сети** включает/отключает проверку на чтение файлов с сетевых дисков и ресурсов **SplDer Guard**. Запускаемые процессы и модули на сетевых дисках и ресурсах проверяются независимо от состояния опции.

Опция **Проверять объекты на съемных носителях** включает/отключает проверку на чтение и запись файлов на сменных носителях **SplDer Guard**. Отключать не рекомендуется. Запускаемые процессы и модули на сменных носителях проверяются независимо от состояния опции.

Также вы можете запретить автоматический запуск активного содержимого внешних носителей данных (CD/DVD-дисков, флеш-памяти и т. д.), установив флажок **Блокировать автозапуск со сменных носителей**. Опция блокирует обращение к файлам `autorun.inf` на всех дисках в корневых каталогах, в том числе на сменных носителях. Включение опции позволяет избежать заражения сменного носителя, если поражена ОС, и системы, если инфицирован носитель. Использование этой настройки помогает предотвратить заражение вашего компьютера через внешние носители.

Вы можете задать проверку:

- файлов запускаемых процессов вне зависимости от их расположения,
- установочных файлов,
- файлов на сетевых дисках,
- файлов и загрузочных секторов на съемных носителях.

В случае возникновения проблем при установке программ, обращающихся к файлу `autorun.inf`, рекомендуется временно снять флажок **Блокировать автозапуск со сменных носителей**.

- Раздел **Исключения**, в котором задается список каталогов и файлов, исключаемых из проверки сторожем **SpIDer Guard**. В поле **Список исключаемых путей и файлов** приводится список каталогов и файлов, которые не проверяются сторожем **SpIDer Guard**. В таком качестве могут выступать каталоги карантина антивируса, рабочие каталоги некоторых программ, временные файлы (файлы подкачки) и т. п.

По умолчанию список пуст. Вы можете добавить к исключениям конкретные каталоги и файлы или использовать маски, чтобы запретить проверку определенной группы файлов.

Можно формировать список исключений следующим образом:

- Чтобы указать конкретный существующий каталог или файл, необходимо нажать кнопку **Обзор** и выбрать каталог или файл в стандартном окне открытия файла. Также можно вручную ввести полный путь к файлу или каталогу в поле ввода.
- Чтобы исключить из проверки все файлы или каталоги с определенным именем, требуется ввести это имя в поле ввода. Указывать путь к каталогу или файлу при этом не требуется.
- Чтобы исключить из проверки файлы или каталоги определенного вида, следует ввести определяющую их маску в поле ввода. Маска задает общую часть имени объекта. При этом:
 - символ «*» заменяет любую, возможно, пустую последовательность символов;
 - символ «?» заменяет любой, но только один символ;
 - остальные символы маски ничего не заменяют и означают, что на данном месте в имени файла или каталога должен находиться именно этот символ.

Пример:

- `отчет*.doc` — маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т. д.;
- `*.exe` — маска, задающая все исполняемые файлы с расширением EXE, например `setup.exe`, `iTunes.exe` и т. д.;
- `photo????09.jpg` — маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например, `photo121209.jpg`, `photомама09.jpg` или `photo---09.jpg`.

Кнопка **Добавить** позволяет добавить к списку исключение, указанное в поле ввода.

Кнопка **Удалить** позволяет удалить из списка выбранное исключение.

Разделы реестра также служат для добавления различных типов исключений в **SpIDer Guard**. При этом настройки реестра значительно шире, нежели в графическом интерфейсе.

Исключения файлов и процессов:

- `[HKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\Scanning Engine\SpIDer Guard\Settings\Exclude/Files]` — в данный раздел добавляются файлы и маски, которые следует исключить из проверки **SpIDer Guard**.
- `[HKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\Scanning Engine\SpIDer Guard\Settings\Exclude/Paths]` — в данный раздел добавляются пути, которые следует исключить из проверки **SpIDer Guard**.
- `[HKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\Scanning Engine\SpIDer Guard\Settings\Exclude/Processes]` — данный раздел наиболее опасен

в плане заражения вирусами, но позволяет задействовать мощную возможность **SpiDer Guard** — здесь можно задать список файлов процессов, для которых **SpiDer Guard** будет игнорировать любую активность данного процесса. Применяется как инструмент устранения конфликтов, если они имеются в системе.

Параметры имеют вид:

- 0= [строка]
- 1= [строка]
- ...
- n= [строка]

Пример использования опции — зададим 0=c:\windows\system32\notepad.exe. Теперь любые манипуляции с файлами, процессами, запущенными из c:\windows\system32\notepad.exe, будут игнорироваться **SpiDer Guard** и не попадать на проверку.

Исключения на размер проверяемых объектов по типам:

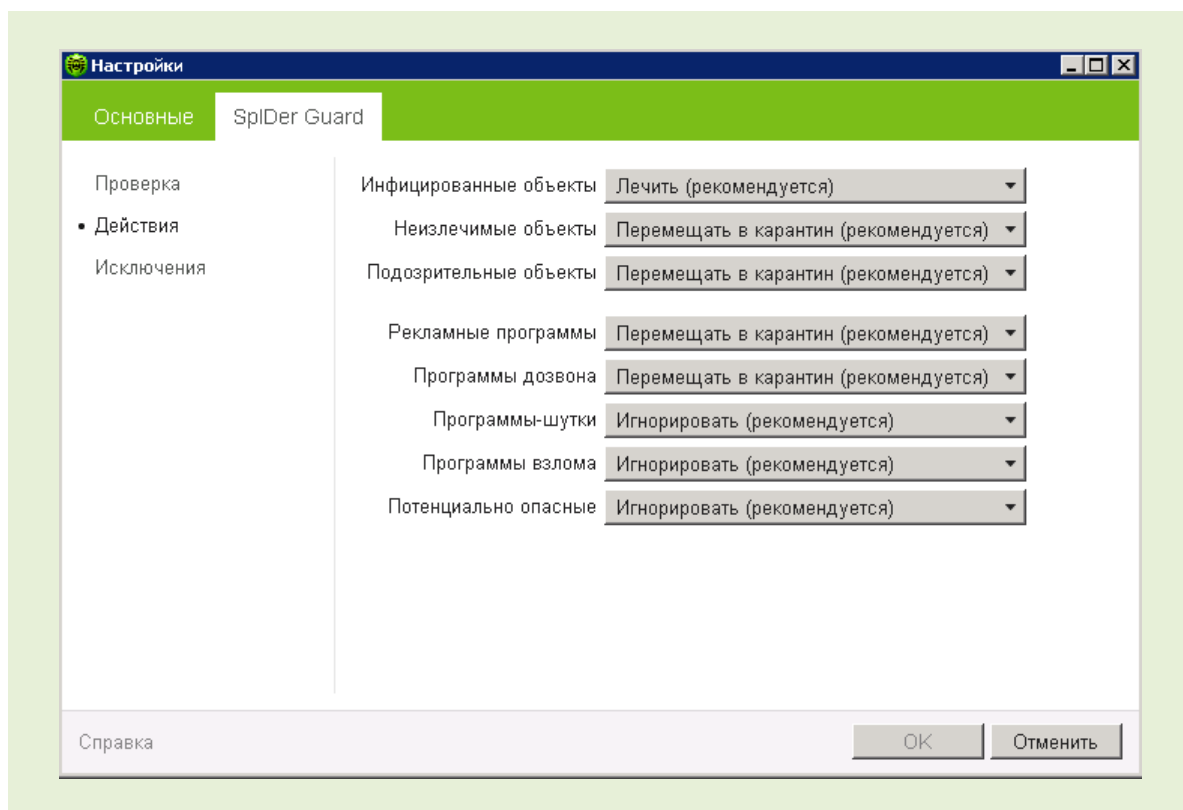
- Scan/AlwaysCheck/Limit/OLEEXPL=dword: [размер:0],
Scan/AlwaysCheck/Limit/PPT=dword: [размер:0]
Scan/AlwaysCheck/Limit/VISIO=dword: [размер:0]
Scan/AlwaysCheck/Limit/RTF=dword: [размер:0]
Scan/AlwaysCheck/Limit/HTML=dword: [размер:0]
Scan/AlwaysCheck/Limit/CHM=dword: [размер:1024]
Scan/AlwaysCheck/Limit/EMBEDOBJ=dword: [размер:0]
Scan/AlwaysCheck/Limit/HTMLVBA=dword: [размер:0]
Scan/AlwaysCheck/Limit/MSGVBA=dword: [размер:0]
Scan/AlwaysCheck/Limit/BINARYRES=dword: [размер:0]
Scan/AlwaysCheck/Limit/DOC1C=dword: [размер:0]
Scan/AlwaysCheck/Limit/PDF=dword: [размер:0]
Scan/AlwaysCheck/Limit/AUTOIT=dword: [размер:0] — набор опций позволяет тонко настроить ограничения на проверку различных типов файлов. Этот метод намного безопаснее, чем создание исключений по имени или маске. По умолчанию лимит установлен только для CHM файлов и равен 1 МБ. В некоторых ситуациях может потребоваться ограничить и другие типы, например DOC1C, что избавит от проблем при проверке больших файлов 1С у некоторых пользователей, не снижая уровень безопасности. 1С-файлы проверяются очень долго, но уже давно не используются для распространения вирусов, поэтому исключение крупных файлов разумнее исключить. Размер файлов задается в КБ.

Системные исключения:

- Exclude/SystemFiles=dword:1/0 — параметр включает/отключает игнорирование проверки специальных системных путей и файлов, согласно рекомендации Microsoft. Внутренние базы данных, системные журналы и т. д. Набор строк и файлов зависит от версии ОС, типа ОС (рабочая станция, сервер, контролер домена). Включение данной опции позволяет избавиться от возможных конфликтов и снижения производительности на серверах и доменных контроллерах.
- Exclude/PrefetcherDB=dword:0/1 — параметр позволяет исключить из проверки файлы базы данных префетчера (эта база данных создается системой) и служит для ускорения повторного запуска приложений методом кеширования файлов. Включение данной опции позволяет повысить производительность системы, поскольку **SpiDer Guard** не тратит время на перепроверку при изменениях базы данных. Учтявая, что опция также позволяет исключить часть возможных конфликтов, быстроедействие системы может возрасти еще сильнее.

- Exclude/SearchDB=dword:0/1 – параметр позволяет исключить из проверки файлы базы данных системной службы индексирования файлов на дисках Windows. Включение данной опции может повысить производительность системы, при условии что в ОС включено индексирование файлов.
- Раздел **Действия**, в котором задается реакция сторожа **SPiDer Guard** на обнаружение зараженных или подозрительных файлов и вредоносных программ. Реакция задается отдельно для каждой категории объектов:
 - Инфицированные файлы, зараженные известным и (предположительно) излечимым вирусом
 - Неизлечимые объекты, зараженные неизлечимым вирусом
 - Подозрительные файлы, предположительно зараженные вирусом или содержащие вредоносный объект
 - Различные потенциально опасные объекты

Вы можете изменить реакцию сторожа **SPiDer Guard** на обнаружение каждого типа объектов в отдельности. Состав доступных реакций при этом зависит от типа вирусного события.



Следующие настройки доступны только в реестре:

- Scan/Action/Archive, Scan/Action/Mail, Scan/Action/Container=dword: [действие] – параметры определяют действие соответственно для файлов в архивах, почтовых файлов и инсталляторов. Возможные действия:
 - 0 – информировать,
 - 2 – переместить в карантин,
 - 4 – удалить,
 - 8 – игнорировать.

По умолчанию сторож **SPiDer Guard** пытается вылечить файлы, зараженные известными и потенциально излечимыми вирусами, остальные наиболее опасные объекты перемещает в **Карантин**. Программы-шутки, программы взлома и неблагонадежные объекты по умолчанию игнорируются. Реакции сторожа **SPiDer Guard**

аналогичны соответствующим реакциям **Сканера** Dr.Web. Существуют следующие действия, применяемые к обнаруженным объектам:

- **Лечить** — восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, будет отработана реакция, заданная для неизлечимых вирусов. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
- **Удалить** — удалить объект. Для загрузочных секторов никаких действий производиться не будет.
- **Перемещать в карантин** — переместить объект в специальный каталог **Карантина**. Для загрузочных секторов никаких действий производиться не будет.
- **Игнорировать** — пропустить объект без выполнения каких-либо действий и не выводить оповещения. Данное действие возможно только для вредоносных программ: рекламных программ, программ дозвона, программ-шуток, потенциально опасных программ и программ взлома.

Сторож **SpIDer Guard** не проверяет составные объекты (архивы, файлы электронной почты или файловые контейнеры), поэтому никакие действия над ними или входящими в их состав файлами не производятся. После выполнения предписанного действия сторож **SpIDer Guard** по умолчанию выводит соответствующее оповещение в область уведомлений Windows.

Отчет сторожа **SpIDer Guard** хранится в файле `spiderg3.log`, расположенном в каталоге `%allusersprofile%\Application Data\Doctor Web\Logs\` (в Windows 8, `%allusersprofile%\Doctor Web\Logs`). Рекомендуется периодически анализировать файл отчета. Подробность отчета задается в разделе Отчет, меню Основные.

В файле отчета SpIDer Guard G3 буквы в квадратных скобках обозначают источник, из которого файл попал на сканирование:

- [NA] — неизвестно (информация не сохранилась);
- [CR] — создание/открытие;
- [CL] — закрытие;
- [RN] — переименование;
- [PR] — сканирование процессов;
- [FB] — пакетные задачи, которые выполняются через фоновое сканирование, если нет более точной информации;
- [BG] — фоновое сканирование.

Настройки журналов действий в реестре:

- `Log/File=[путь]` — параметр задает полный путь к log-файлу SpIDer Guard.
- `Log/Buffered=dword:0/1` — параметр включает/отключает буферизированный вывод. В режиме буферизированного вывода строки пишутся в лог группами, а не по одной, что повышает производительность системы из-за меньшего числа обращений к диску.
- `Log/Verbose=dword:1/0` — параметр включает/отключает дополнительно детализированный вывод в log-файл.
- `Log/Debugging=dword:0/1` — параметр включает/выключает полный отладочный вывод в log-файл.

Примечание. При одновременном включении опций `Log/Verbose` и `Log/Debugging` получается максимально подробный отладочный отчет.

- `Log/SizeInKB=dword:[размер в КБ]` — параметр задает допустимый размер файла журнала. При значении "-1" объем не лимитирован, "0" — журнал не ведется.

- Log/Show/Archiver=dword:1/0 – параметр включает/отключает вывод в журнал информации об архивах и их содержанием.
- Log/Show/Packer=dword:1/0 – параметр включает/отключает вывод в журнал информации о упаковщиках и их содержанием.
- Log/Show/OK=dword:1/0 – параметр включает/отключает вывод в журнал информации о чистых проверенных файлах.
- Log/Show/Milliseconds=dword:0/1 – параметр включает/отключает вывод в журнал миллисекунд (обычно время указывается с точностью до секунд).
- Log/Show/Skipped=dword:0/1 – параметр включает/отключает вывод в журнал информации об исключенных из проверки файлах. Параметр позволяет проверить, работают ли заданные исключения.

12.2. Настройки, которые можно задать только в реестре

Основные настройки:

- Core/LicensePath=[папка] – параметр позволяет указать папку, в которой находится лицензионный ключ. Обычно это папка установки антивируса.
- Core/Watcher/Disable=dword:0/1 – параметр включает/отключает использование **Scanning Engine** второй копии своего процесса (т. н. Сторожевого пса). Вторая копия при запуске подключается к основному процессу **Scanning Engine** как отладчик и контролирует его работу. При активном Сторожевом псе невозможно подключиться к **Scanning Engine** и перехватить управление или уничтожить процесс.

Настройка лимитов проверки:

- Core/Limit/Engines=dword:[кол-во движков:0] – параметр ограничивает для **SpIDer Guard** количество используемых антивирусных движков. При значении "0" (установлено по умолчанию) автоматически рассчитывается из возможностей ОС и аппаратной части ПК.
- Core/Limit/Cores=dword:[кол-во ядер:0] – параметр ограничивает для **SpIDer Guard** число используемых ядер процессора на многоядерных системах. При значении "0" количество задействованных ядер автоматически рассчитывается, исходя из конфигурации ПК и ОС.
- Core/Limit/BgScan=dword:[кол-во потоков:0] – параметр ограничивает количество потоков, используемых для фонового сканирования (BG).

Настройки проверки объектов:

- Scan/Check/Archive=dword:0/1 – параметр включает/отключает проверку архивов в **SpIDer Guard**. Данную опцию включать крайне не рекомендуется, поскольку это значительно увеличит нагрузку на систему и снизит быстродействие компьютера.
- Scan/Check/Mail=dword:0/1 – параметр включает/отключает проверку почтовых файлов и баз в **SpIDer Guard**. Крайне не рекомендуется включать данную опцию ввиду сильной нагрузки на систему.

Настройки карантина:

- Quarantine/EnableBackup=dword:1/0 – параметр включает/отключает создание в карантине резервной копии файла при любой манипуляции с файлом (изменение/удаление). Отключать не рекомендуется.
- Quarantine/MaximumSize=dword:[размер] – параметр задает максимальный размер карантина для использования **SpIDer Guard**, в процентах от размера диска. По умолчанию 10%.
- Quarantine/StoragePeriod=dword:[период] – параметр задает период, указывающий, как долго должны храниться файлы в карантине. По умолчанию 30 дней.

Все более старые файлы автоматически удаляются, при нехватке места первыми удаляются наиболее старые файлы.

Настройка лимитов на проверку:

Эти параметры предназначены для оптимизации проверки. Любые изменения данных параметров приводят к ослаблению безопасности — без крайней необходимости менять их не следует.

- `Scan/Misc/Maximum/Time=dword: [число]` — параметр позволяет ограничить максимальное время на проверку одного файла **SpIDer Guard**. Параметр задается в секундах, при значении "0" лимита на время проверки нет. Менять опцию не рекомендуется.
- `Scan/Misc/Maximum/PackingLevel=dword: [число]` — параметр позволяет установить лимит на количество итераций распаковки запакованных файлов движком. По умолчанию 1000 итераций. Опция предназначена для исключения закливания при распаковке.
- `Scan/Misc/Archive/Maximum/Level=dword: [число]` — параметр позволяет установить лимит на количество уровней распаковки архива движком. По умолчанию 16 уровней вложенности.
- `Scan/Misc/Archive/Maximum/Size=dword: [размер]` — параметр позволяет ограничивать максимальный размер архива, проверяемого **SpIDer Guard**. Параметр задается в КБ. При установке значения "0" — ограничений на размер нет.
- `Scan/Misc/CureLimit=dword: [число]` — параметр позволяет установить лимит на количество итераций лечения файла. По умолчанию используется значение от `Scanning Engine` и равное 500.

Настройки, управляющие ресурсами системы:

- `Scan/Resource/High=dword: [число]` — параметр позволяет задать процент доступных ресурсов для высокоприоритетного сканирования (сканирование при запуске процессов и загрузке модулей). По умолчанию 0.
- `Scan/Resource/Normal=dword: [число]` — параметр позволяет задать процент доступных ресурсов для обычного сканирования (проверка файлов). По умолчанию 0.
- `Scan/Resource/Low=dword: [число]` — параметр позволяет задать процент доступных ресурсов для низкоприоритетного сканирования (фоновая проверка, повторное сканирование после обновления баз). По умолчанию 100.

Значения данных параметров задаются от 0 до 100 следующим образом: 0 — используются все доступные ресурсы, 100 — активируется только простое системы. Можно изменить значение для нормального режима работы (проверка файлов).

Дополнительные параметры проверки:

- `Scan/Processes/OnCreate=dword: 1/0` — при значении "1" проверка процессов происходит в момент создания процесса или в момент загрузки модуля в процесс, а сам процесс заблокирован на время проверки. При значении "0" запускаемые процессы и загрузка модулей не блокируются **SpIDer Guard**, и их проверка осуществляется в фоновом режиме. Значение по умолчанию менять не рекомендуется, поскольку это значительно снижает уровень безопасности. Исключение можно сделать на старых ПК, поскольку на них включение данной опции может существенно замедлить систему.
- `Rescan/ResultSet=dword: 1/0` — параметр включает/отключает фоновое пересканирование файлов всех загруженных процессов и модулей при обновлении баз **SpIDer Guard**. Фоновое сканирование имеет низкий приоритет.

12.3. Настройки Dr.Web Scanning Engine

Dr.Web Scanning Engine – базовый компонент антивируса Dr.Web, антивирусный движок, который используется всеми компонентами антивируса, в том числе новым SplDer Guard G3, созданным на его основе.

Исполняемый файл **Scanning Engine** – `dwengine.exe` – это системный сервис, который запускается одновременно с операционной системой и загружает в себя антивирусный движок и базы. Также `dwengine.exe` предоставляет интерфейс для удаленной проверки файлов любым модулем антивируса (SplDer Gate, SplDer Mail, Сканер и плагины для различных программ).

Кроме этого, `dwengine.exe` служит управляющим сервисом для SplDer G3 и является интерфейсом для интеграции в Центр безопасности Windows. Он отвечает за сигналы о статусе антивируса (какие компоненты активны/неактивны) и актуальности вирусных баз. Этот же файл предоставляет API и интерфейсы для проверки файлов и буферов памяти на вирусы и спам (в зависимости от лицензии).

Все настройки Scanning Engine хранятся в системном реестре Windows, в ветке

```
HKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\Scanning Engine\Machine\  
DrWebEngine\Settings
```

Внимание! Изменение ключей реестра влияет на систему, подразделения на пользователей не предусмотрено. Если опция может быть активной или неактивной, значение ключа "0" – выключает ее, "1" – включает. Значение, стоящее по умолчанию, указано первым.

Основные настройки:

- `Scan/DllPath=[папка]` – параметр указывает папку, в которой находится антивирусное ядро (файл `drweb32.dll`),
- `Scan/VdbPath=[папка]` – параметр указывает папку, в которой хранятся антивирусные базы.
- `Core/OldBases=dword:[сек:86400]` – параметр задает время в секундах, по истечении которого **Scanning Engine** начинает сообщать в Центр безопасности Windows о том, что базы устарели и нужно произвести обновление. По умолчанию значение равно 86400 секунд (1 сутки).
- `WSC/Enable=dword:1/0` – параметр включает/отключает интеграцию в Центр безопасности Windows.
- `SpIDer/Enable=dword:1/0` – параметр включает/отключает интеграцию **Scanning Engine** в **Dr.Web File System Monitor**. При отключении данной опции **Scanning Engine** не подключается к драйверу и не обрабатывает от него никакие события, драйвер же по достижению лимита на события (~30 МБ памяти ~ несколько миллионов событий) перестает отслеживать активность в системе и переходит в режим ожидания, чтобы не спровоцировать системный сбой в ОС.

Настройки по проверке файлов:

- `Scan/Engines=dword:[кол-во движков:0]` – параметр задает количество загружаемых и используемых антивирусных движков, при значении "0" используется алгоритм, автоматически рассчитывающий это значение исходя из аппаратной конфигурации ПК и ОС (для рабочей станции формула: число ядер процессора+1).
- `Scan/CureLimit=dword:[число:500]` – параметр позволяет установить лимит на количество итераций (повторов) лечения файла. Данная функция помогает избавиться от багов, приводящих к закликиванию лечения. По умолчанию лимит 500 итераций.

Настройки временных файлов, используемых движком:

- `Scan/NoTempFiles=dword:0/1` – параметр разрешает/запрещает **Scanning Engine** создавать временные файлы по запросу антивирусного движка. Включать

данную опцию крайне не рекомендуется, поскольку проверка сложных объектов или распаковка архивов будет заканчиваться в большинстве случаев неудачей из-за больших объемов информации.

- `Scan/KeepTempFiles=dword:0/1` — параметр, будучи включенным, заставляет **Scanning Engine** сохранять на диске все временные файлы, которые создавал движок при сканировании и распаковке файлов. Параметр используется в процессе отладки, и включать его не рекомендуется, чтобы не замусорить жесткий диск временными файлами.

Системные настройки:

Важно! Эти настройки могут быть критичны как для работы сканера, так и для быстродействия компьютера.

- `Core/MapEnabled=dword:1/0` — параметр включает/отключает использование технологии проецирования файлов при сканировании. Если включено — ОС читает файлы из области памяти, а не с диска, что гораздо быстрее. Также опция позволяет обезвреживать вирусы, которые блокируют свои файлы на диске — без этой технологии прочитать и вылечить их невозможно. Отключать крайне не рекомендуется.
- `Core/CacheFiles=dword:1/0` — параметр позволяет включить/отключить технологию кеширования хендлов в **Scanning Engine**. При включенной опции **Scanning Engine** сам управляет всеми открытыми файлами, не полагаясь на движок, а также не открывает повторно хендлы на файлы по запросу движка, это повышает производительность и исключает ситуации, когда после проверки файла движком он остается заблокированным на диске для изменения. Отключать крайне не рекомендуется.
- `Core/UseMalloc=dword:0/1` — при включении опции для работы с памятью **Scanning Engine** будет использовать стандартные функции `malloc/free` вместо встроенного оптимизированного диспетчера памяти. Опция требуется в основном для отладки, включать ее крайне не рекомендуется.

Чтобы внесенные изменения вступили в силу, необходимо перезапустить **Scanning Engine**.

Примечание. Можно перезагрузить **Scanning Engine** без перезагрузки компьютера. Для этого необходимо завершить процесс `dwengine.exe` и запустить его вновь.

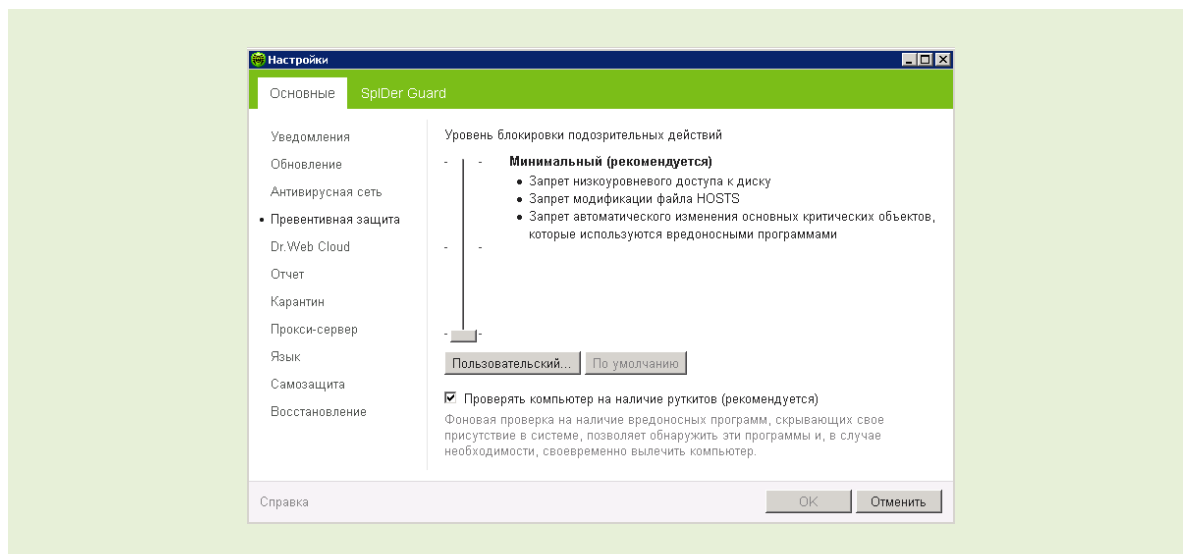
12.4. Антируткит Dr.Web

Антируткит Dr.Web — это специальный драйвер, который помогает компонентам антивируса Dr.Web для Windows обнаруживать вирусы, скрывающие свое присутствие в системе с помощью перехвата функций операционной системы (Windows API). Для его работы требуются права администратора.

Драйвер Антируткита позволяет антивирусу Dr.Web получать полный доступ к файлам, к которым обычно доступ запрещен системой, не только в безопасном режиме Windows, но и в обычном. Использование Антируткита позволяет гораздо эффективнее, чем прежде, противодействовать активным вредоносным программам, находящимся в системе. Так, **Антируткит Dr.Web**, например, позволяет антивирусу Dr.Web противодействовать так называемым буткитам — вредоносным программам, которые прописывают себя в загрузочный сектор жесткого диска и обеспечивают скрытую установку своего драйвера в памяти. Подобные руткит-драйверы записываются в последние сектора физического диска и, таким образом, не существуют в виде файла.

Драйвер **Антируткита Dr.Web** используется в **Сканере Dr.Web — Антируткит Dr.Web** внедрен в исполняемый файл GUI-сканера. Драйвер автоматически устанавливается в систему при запуске GUI-сканера и автоматически же из нее удаляется, когда в нем отпадает необходимость.

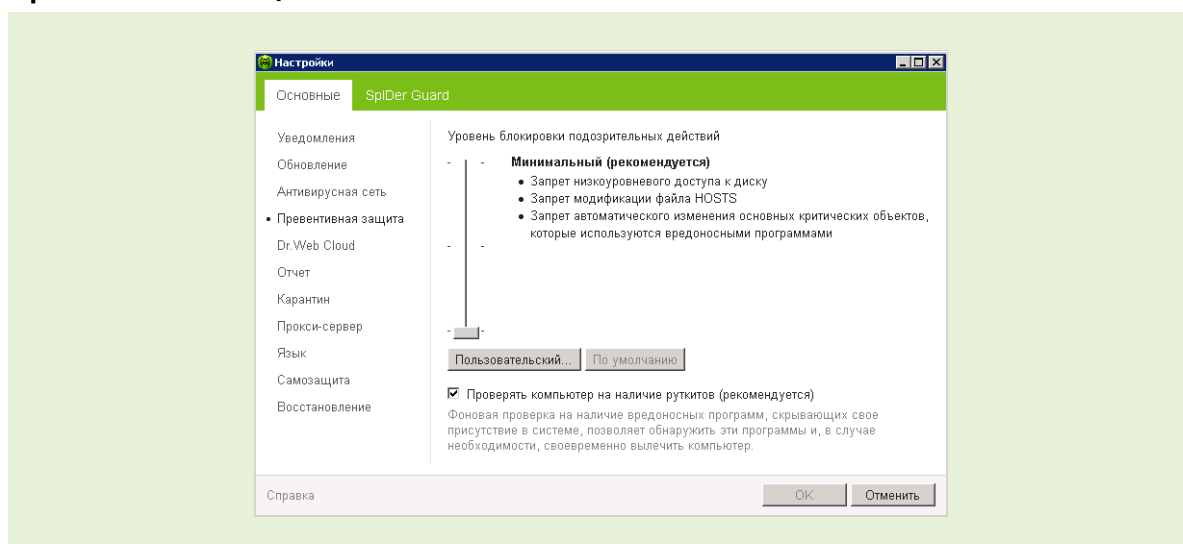
Провести фоновое сканирование операционной системы на заражение руткитами можно на странице **Превентивная защита**, доступном в окне **Настройки**.



12.5. Превентивная защита. Защита от неизвестных угроз

При подсоединении нового носителя информации (съёмного устройства) в современных операционных системах по умолчанию срабатывает система автозапуска. Она сканирует содержимое носителя и предлагает пользователю список возможных действий. Существует целый ряд вредоносных программ, загружающихся в память ПК при установке в привод инфицированного диска или флеш-накопителя. Чтобы предотвратить активацию таких вирусов, необходимо запретить автозапуск со всех съёмных носителей. Для этого можно использовать возможности Dr.Web для файловых серверов Windows.

Для того чтобы предотвратить изменение системных областей, необходимо настроить систему превентивной защиты. Для ее настройки (если функция контроля учетных записей Windows не включена) выберите пункт **Инструменты** в меню **SpiDer Агента** и в открывшемся списке выберите **Настройки**. В открывшемся окне выберите **Превентивная защита**. Если функция контроля учетных записей Windows включена – наведите курсор на пиктограмму Dr.Web, которая находится в нижнем правом углу экрана. Нажмите на правую клавишу мыши. В появившемся контекстном меню выберите пункт **Административный режим**. В появившемся окне **Контроль учетных записей пользователей** нажмите на кнопку **Да**, снова наведите курсор на пиктограмму Dr.Web, нажмите на правую клавишу мыши и в контекстном меню раскройте пункт **Инструменты**. Выберите пункт **Настройки** → **Превентивная защита**.



В данном разделе вы можете настроить реакцию антивируса на действия сторонних приложений, которые могут привести к заражению вашего компьютера — установив необходимый уровень блокировки подозрительных действий. Настройка параметров превентивной защиты позволяет держать под контролем все попытки изменения критических областей Windows.

Для изменения настроек превентивной защиты нажмите **Изменить**.

В режиме работы **Минимальный**, установленном по умолчанию, запрещается автоматическое изменение системных объектов, модификация которых однозначно свидетельствует о попытке вредоносного воздействия на операционную систему. Также запрещается низкоуровневый доступ к диску для защиты системы от заражения буткитами и троянками-блокировщиками, которые заражают главную загрузочную запись диска. Для предотвращения блокировки доступа к обновлениям антивируса через Интернет и блокировки доступа на сайты производителей антивирусов запрещается модификация файла HOSTS.

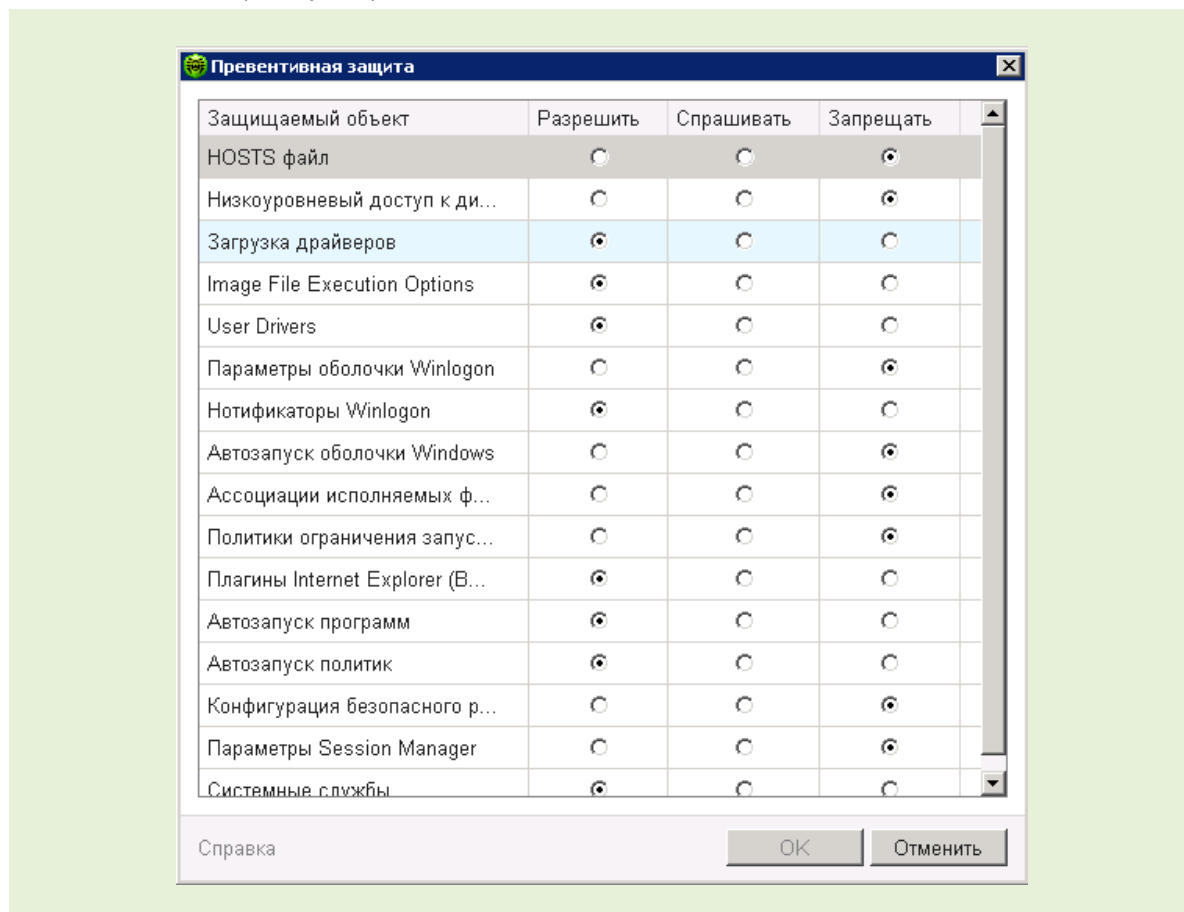
При повышенной опасности заражения необходимо увеличить уровень защиты до **Среднего**. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.

Внимание! В этом режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

При необходимости полного контроля за доступом к критическим объектам Windows можно поднять уровень защиты до **Параноидального**. В данном случае будет доступен интерактивный контроль за загрузкой драйверов и автоматическим запуском программ.

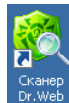
Пользовательский режим позволяет гибко настроить реакцию антивируса на определенные действия, которые могут привести к заражению вашего компьютера.

Для самостоятельного задания параметров защиты нажмите на кнопку **Пользовательский** и выполните настройку, определив действия для каждого элемента списка.



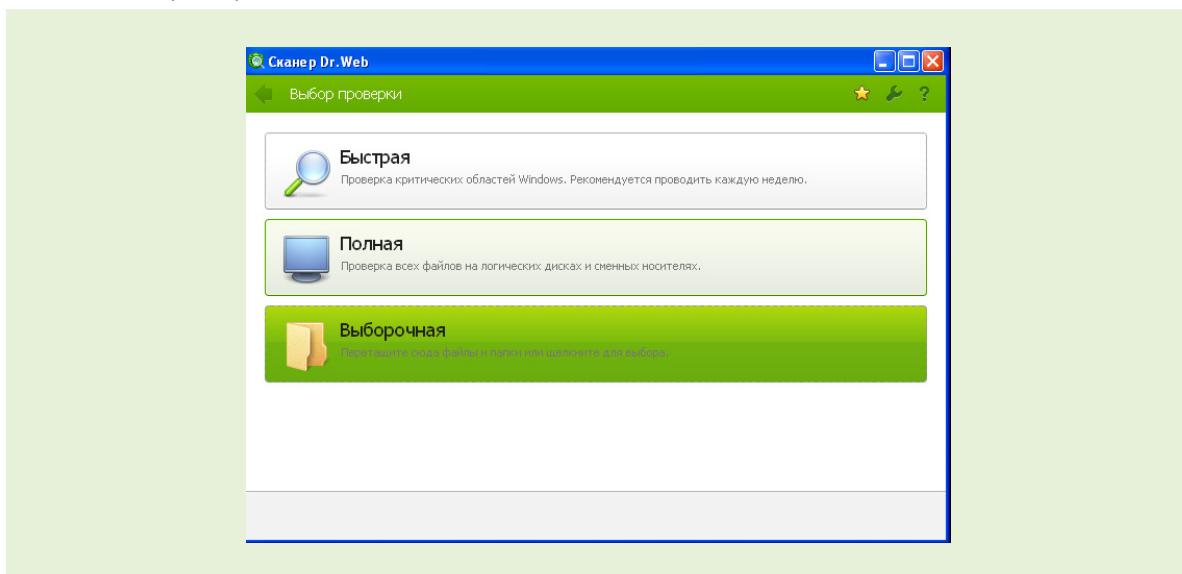
13. Антивирусная проверка

По умолчанию сразу после установки значок **Сканера** появляется на Рабочем столе.



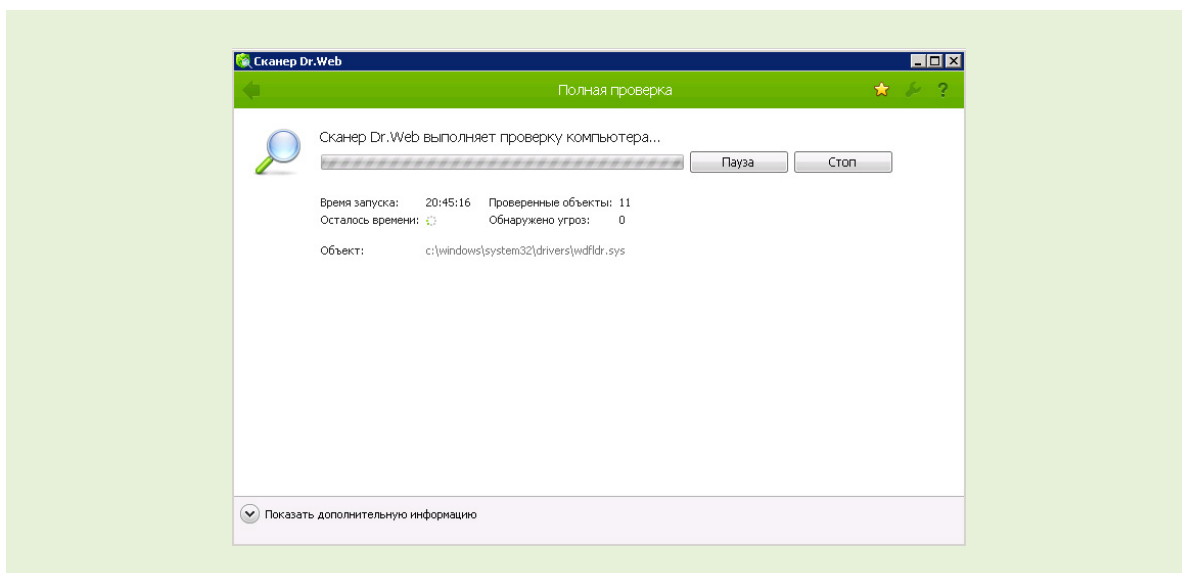
Соответственно, запустить сканирование или изменить его настройки вы можете как с Рабочего стола, так и из меню **Агента**. Помимо этого, Сканер можно запустить из командной строки или из папки Dr.Web главного меню Windows (по кнопке **Пуск**).

Рекомендуется сразу после инсталляции провести полную проверку системы. Рекомендуется проводить такую проверку регулярно — в частности, в связи с тем, что проверенные файловым монитором и записанные на диск файлы могут содержать вирусы, неизвестные на момент проверки.

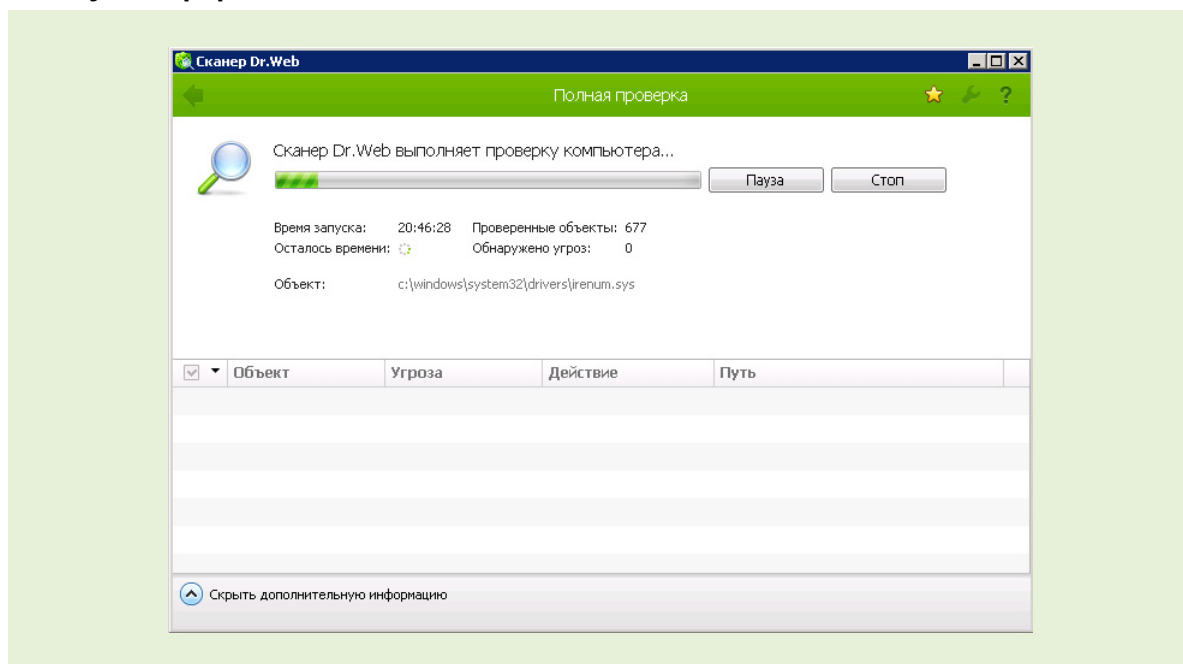


Существует три вида сканирования: быстрое, полное и выборочное. Чтобы начать проверку, выберите один из пунктов основного меню **Сканера** и задайте режим сканирования. Чтобы произвести тонкую настройку, воспользуйтесь кнопками в правом верхнем углу окна.

Выберите **Полную проверку**, чтобы сканировать все файлы, включая содержимое сменных носителей.



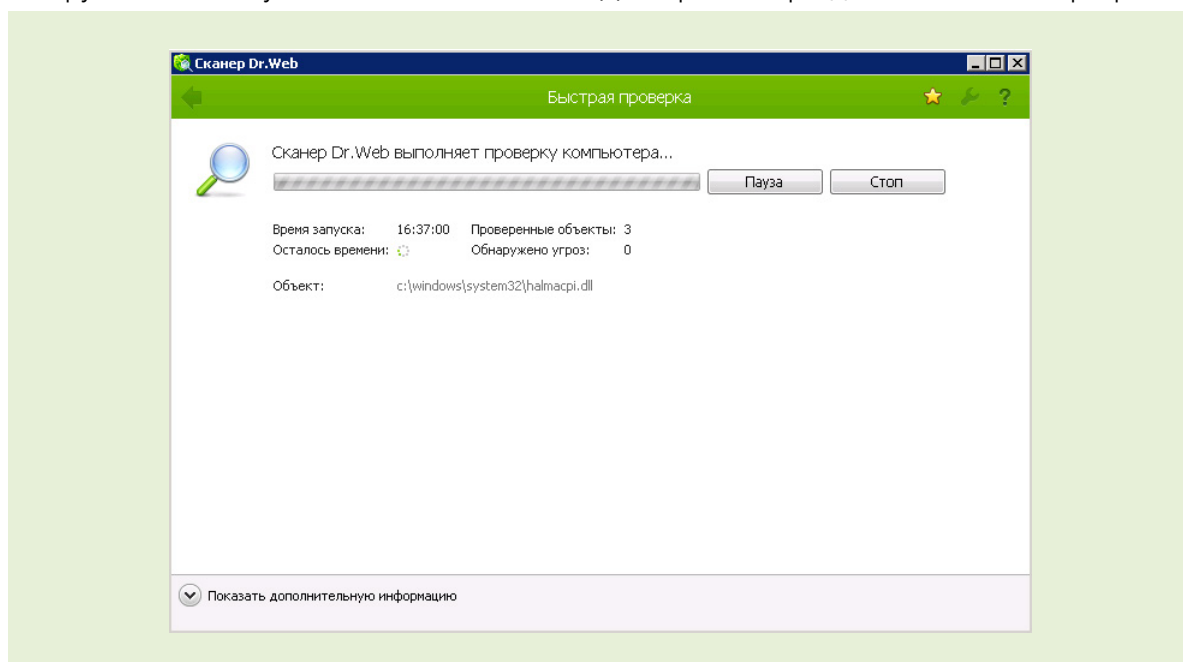
Для показа большего количества информации нажмите на кнопку **Показать дополнительную информацию**.



При старте компьютера или перед выполнением критических операций для сканирования важных областей памяти компьютера рекомендуется запускать **Быструю проверку**.

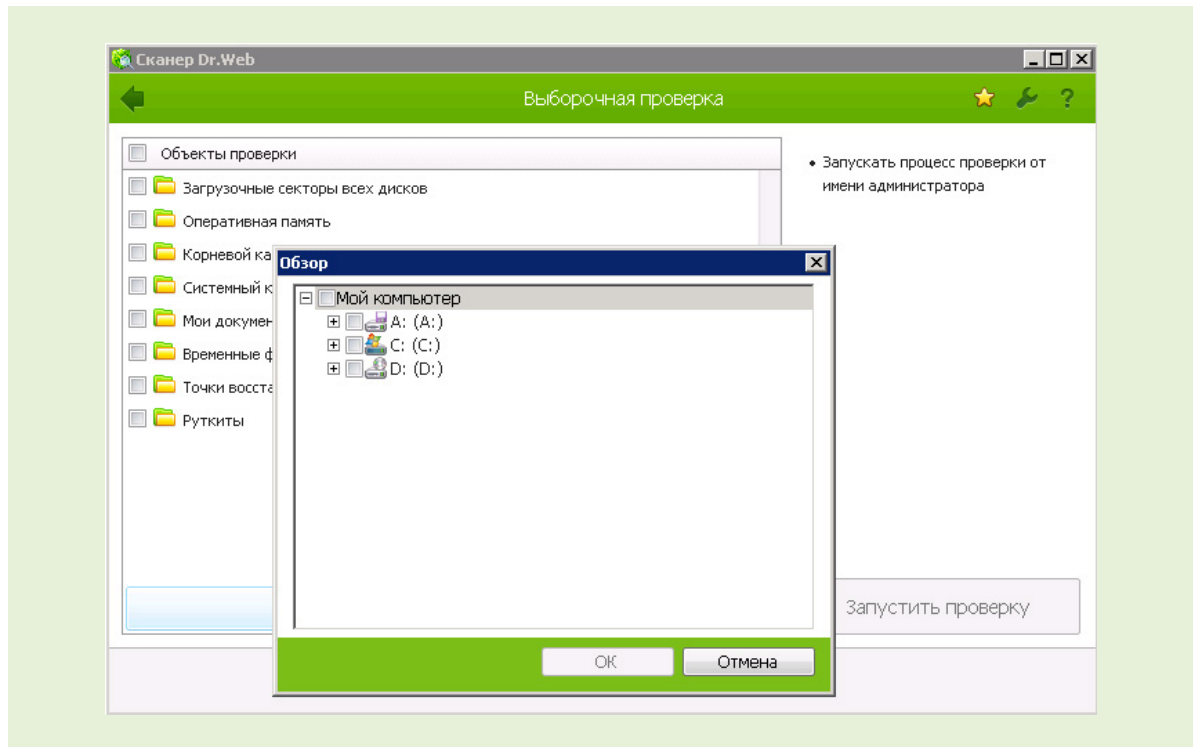
Быструю проверку рекомендуется производить не реже чем раз в неделю (но вы можете производить ее и чаще).



Внимание! Быстрая проверка сканером системы не гарантирует полной очистки вашего компьютера от вирусов — в частности, потому, что работающие вирусы могут заражать уже проверенные («чистые») файлы. В случае обнаружения вирусов мы рекомендуем проверить компьютер до начала установки с помощью бесплатной утилиты Dr.Web CureIt!, которую можно получить на сайте компании «Доктор Веб» в разделе бесплатных программ.



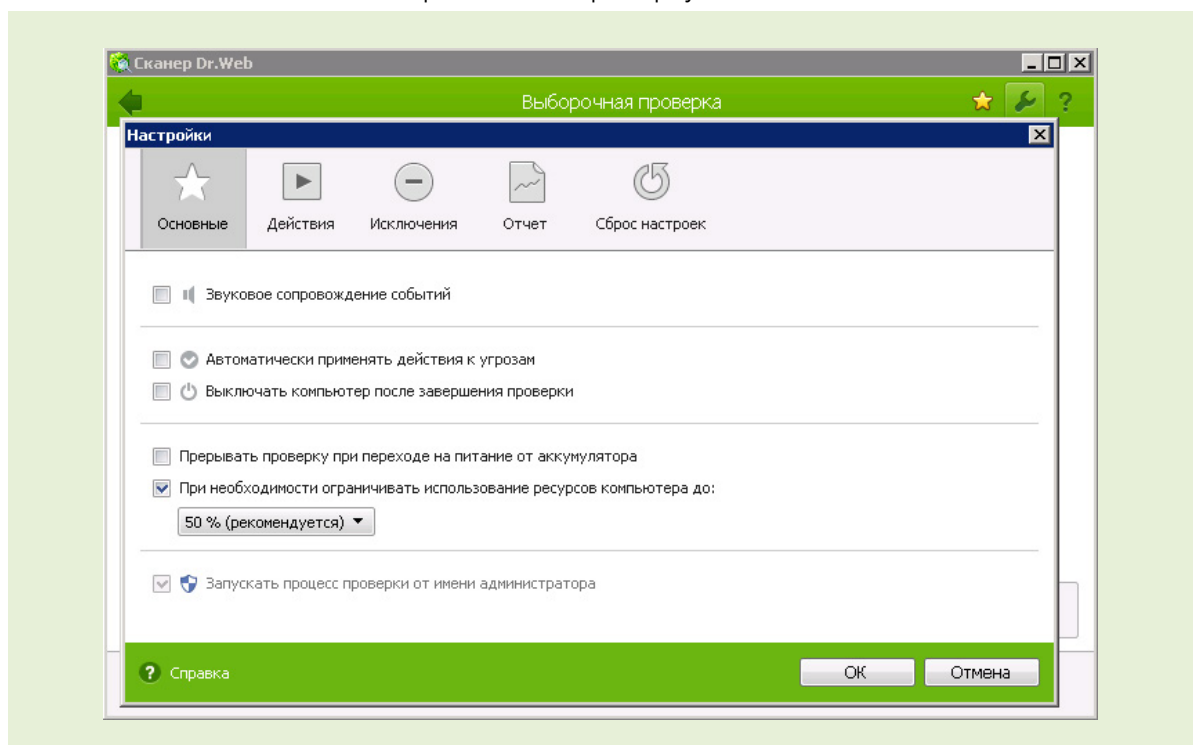
При выборочном сканировании вы можете сами указывать (или перетаскивать в окно **Сканера** мышкой) файлы и каталоги, которые необходимо проверить. Например, если вы хотите следить за состоянием важного для вас каталога с документами, просто добавьте

его в список проверяемых объектов и нажмите **Запустить проверку**. Если вы пометите в списке какой-либо каталог, проверяться будут все файлы и папки внутри каталога.



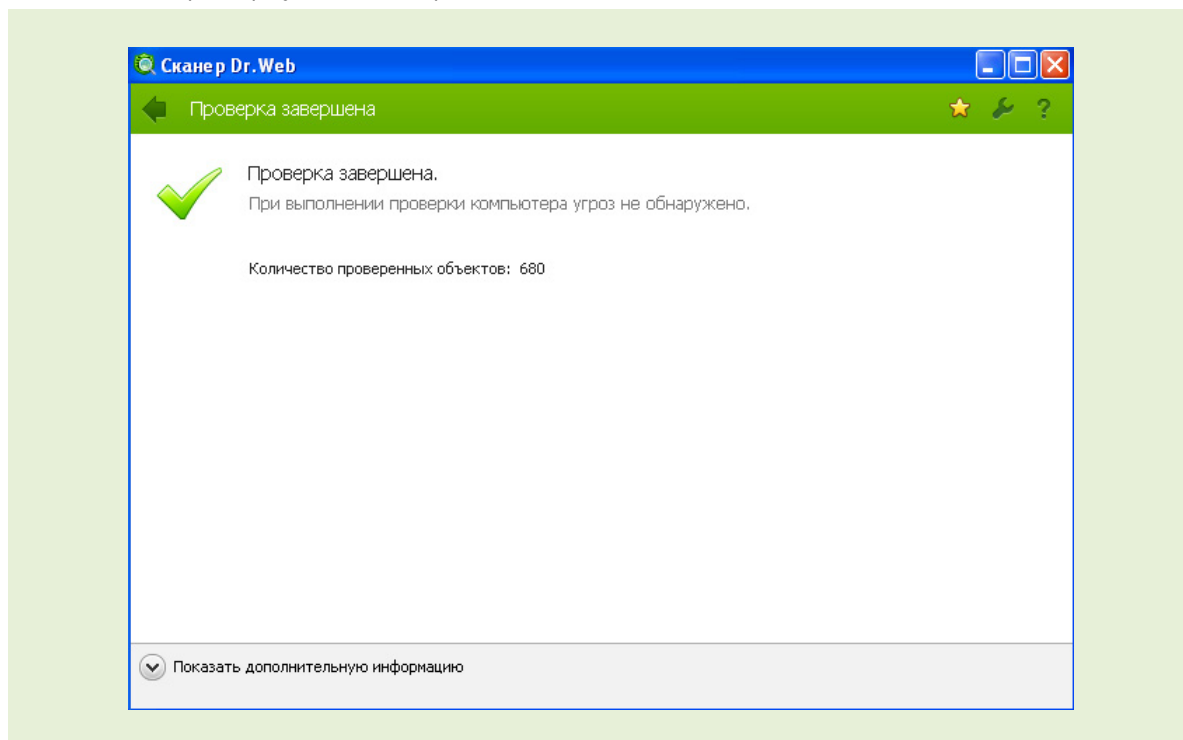
В правом верхнем углу окна **Сканера** имеются кнопки настроек и вызов **Справки** — . Символ «звезда» показывает основные настройки проверки, их рекомендуется оставить без изменений. Значок  ведет к расширенным настройкам **Сканера**. Рекомендуется оставить без изменений все, кроме следующих:

- **Основные** — **Автоматически применять действия к угрозам** — если вы не хотите тратить время на чтение уведомлений о найденных объектах.
- **Исключения** — добавить туда файлы медиа, занимающие большой объем памяти, если хотите сэкономить время на их проверку.



Если вы считаете, что выбранные настройки неправильны, выберите пункт **Сброс настроек – Восстановить значения по умолчанию**.

Остановить проверку компьютера можно, нажав **Стоп**.

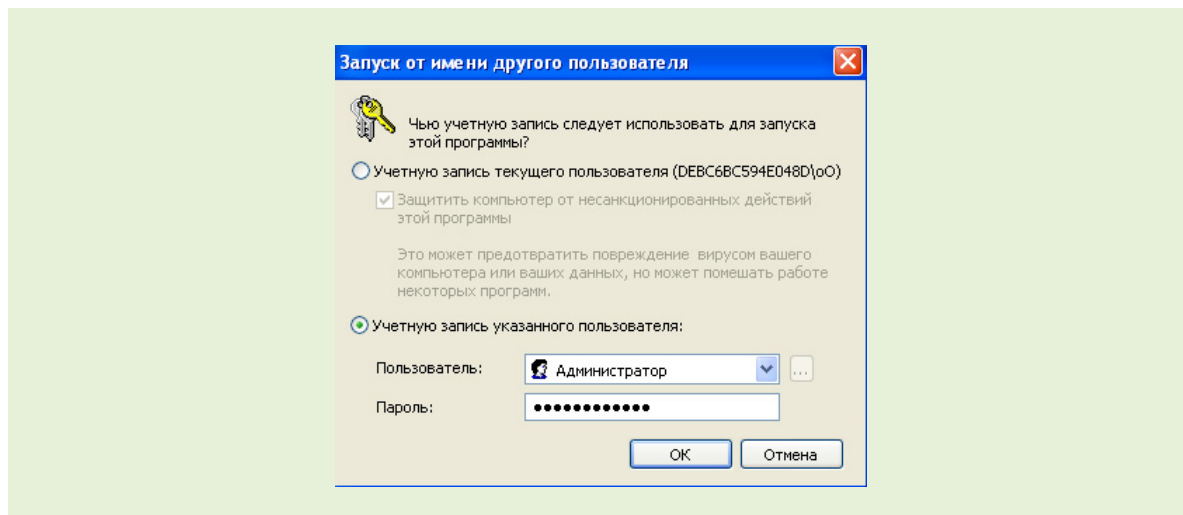


После завершения проверки в окне будет показан суммарный результат: число проверенных объектов. Дополнительную информацию о ходе проверки и сканируемых объектах можно посмотреть как в произвольный момент проверки, так и после ее завершения.

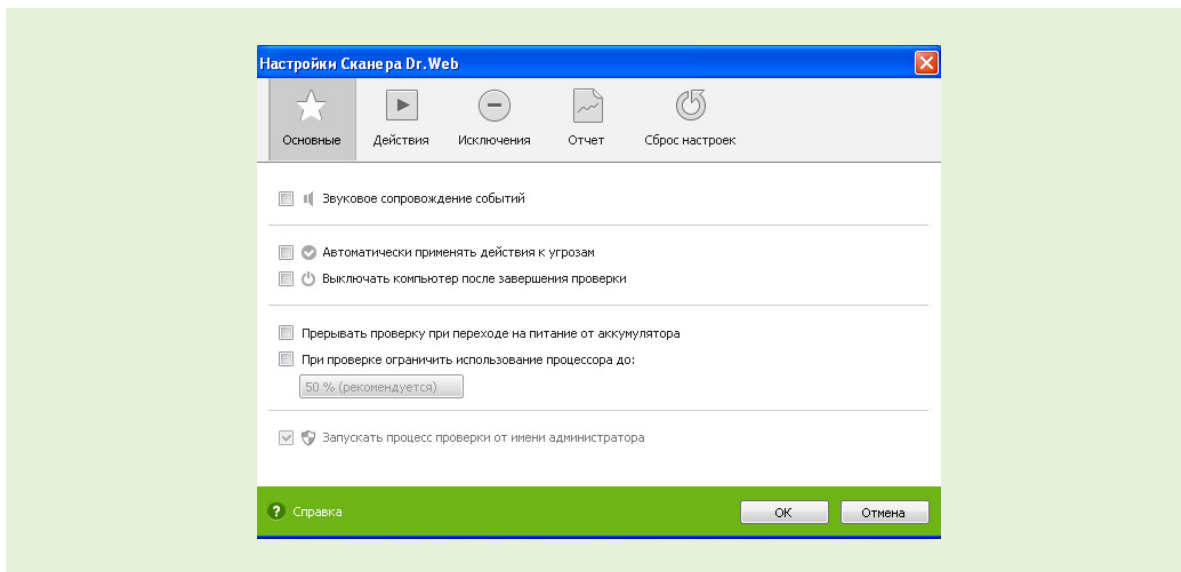
13.1. Проверка с правами другого пользователя

В некоторых случаях сканирование каталогов или файлов возможно только при наличии прав администратора. В частности, это относится к некоторым системным разделам, доступ к которым для обычного пользователя запрещен. Чтобы иметь возможность сканировать тот или иной каталог, выполните одно из двух действий:

- Запустите **Сканер** от имени другого пользователя. Для этого нажмите правой кнопкой на значок **Сканера**, в контекстном меню выберите пункт **Запуск от имени (Run as)...** Затем в появившемся окне выберите пользователя с правами администратора, если необходимо.

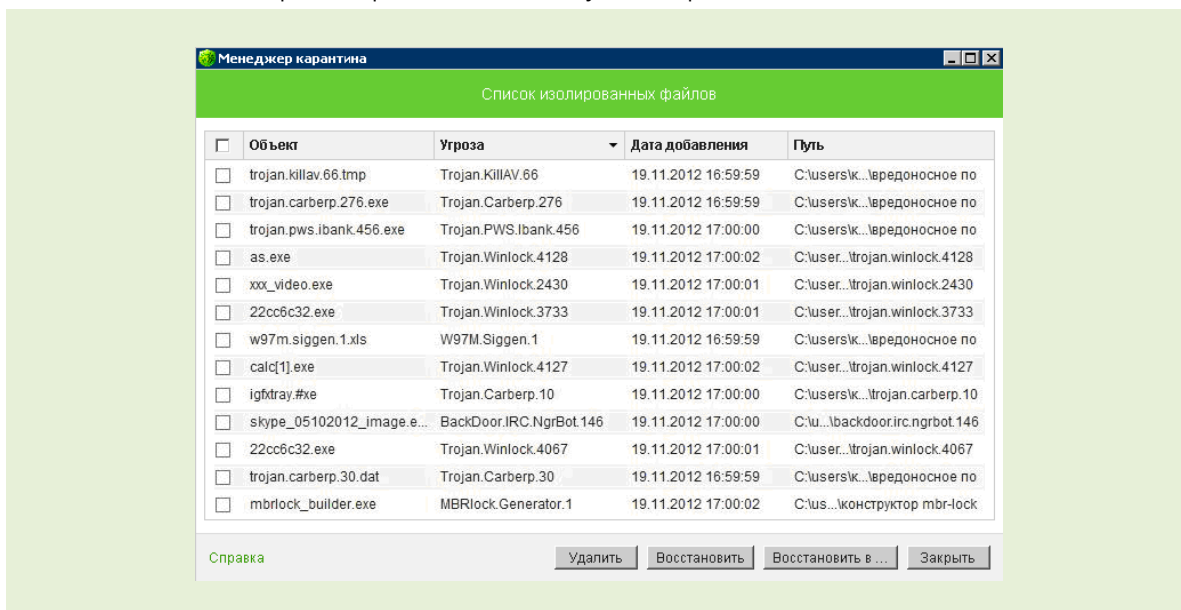


- В настройках **Сканера** (раздел **Основные**) отметьте флажок **Запускать процесс проверки от имени администратора**:



14. Управление Карантином

Окно **Менеджера карантина**, доступное из меню **Агента** (подменю **Инструменты**), содержит данные о содержимом **Карантина Dr.Web**, который служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Каталог **Карантина** создается отдельно на каждом логическом диске, где были обнаружены подозрительные файлы. При обнаружении зараженных объектов на съемном носителе папка **Карантина** создается только в том случае, если возможна запись на носитель. Зараженный объект переносится в соответствующую папку **Карантина** и, если файл находится не на съемном носителе, шифруется. Использование отдельных каталогов и отказ от шифрования на съемных носителях позволяют предотвратить возможную потерю данных.



В окне **Карантина** доступны следующие кнопки управления:

- **Восстановить** — нажмите, чтобы восстановить объект из **Карантина** в ту папку, откуда он был перемещен. Чтобы восстановить объект в другую папку, в выпадающем меню кнопки выберите вариант **Восстановить** в и укажите нужную папку.
- **Удалить** — нажмите, чтобы удалить выбранный объект насовсем.

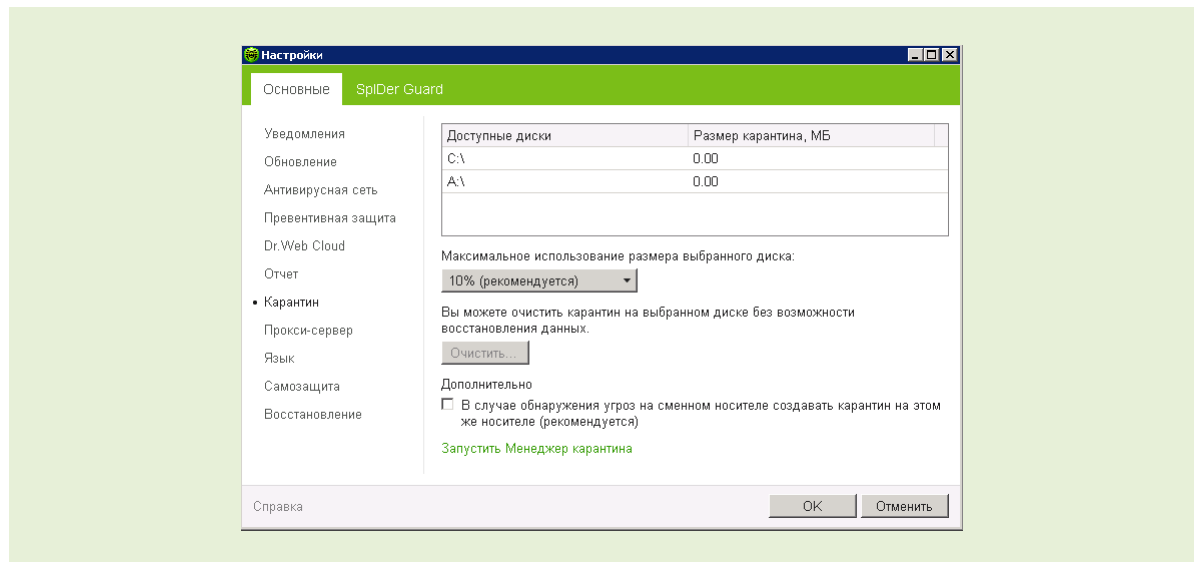
В центральной части окна отображается таблица с информацией о состоянии **Карантина**, включающая следующие поля:

- **Объект** — список имен объектов, находящихся в **Карантине**;
- **Угроза** — классификация вредоносной программы, определяемая **Dr.Web** при автоматическом перемещении объекта в **Карантин**;
- **Дата добавления** — дата, когда объект был перемещен в **Карантин**;
- **Путь** — полный путь, по которому находился объект до перемещения в **Карантин**.

В окне **Карантина** по умолчанию определенные файлы могут видеть только те пользователи, которые имеют к ним доступ. Чтобы отобразить скрытые объекты, запустите под административной учетной записью либо файл `dwgrui.exe`, расположенный в каталоге установки, либо сам **Dr.Web**.

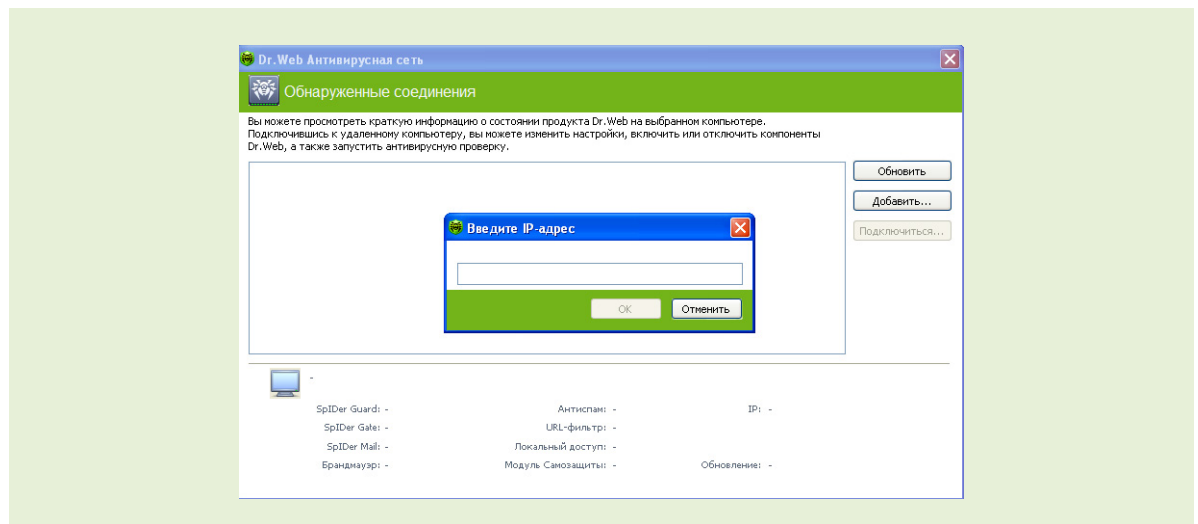
Для одновременной работы с несколькими файлами установите флажки рядом с названиями объектов, а затем выберите необходимое действие.

Настройки **Карантина** задаются на странице **Карантин**, меню **Основные**.



15. Управление антивирусной защитой удаленного компьютера

Удаленное управление позволяет осуществлять управление продуктами **Dr.Web** на других компьютерах в пределах одной локальной сети.



Чтобы запустить его, выберите пункт в меню Агента **Инструменты** → **Антивирусная сеть**. Этот компонент позволяет управлять программами Dr.Web на других компьютерах в пределах одной локальной сети.

Пункт **Антивирусная сеть** доступен только в **Административном режиме**.

Для доступа к удаленному антивирусу выберите компьютер в списке и нажмите кнопку **Подключиться**. Введите пароль, заданный в настройках удаленного антивируса. В области уведомлений Windows появится значок удаленного SplDer Agent. При работе с удаленным антивирусом вам доступны следующие пункты (внешне меню управления ничем не отличается от меню в обычном режиме, набор компонентов варьируется в зависимости от того, к какому продукту **Dr.Web** установлено подключение):

- О программе
- Зарегистрировать лицензию
- Мой Dr.Web
- Справка
- SplDer Guard
- SplDer Mail
- SplDer Gate
- Родительский контроль
- Брандмауэр
- Обновление
- Инструменты
- Отключить/Включить Самозащиту

Пункт **Инструменты** открывает меню, предоставляющее доступ к:

- Менеджеру лицензий
- Настройкам общих параметров работы Dr.Web Security Space
- Созданию отчета

Вы можете просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты **Антивирусная сеть**, **Карантин** и **Сканер** недоступны. Настройки и статистика **Брандмауэра Dr.Web** также недоступны, однако вы можете включить или отключить этот компонент (в случае подключения к продуктам **Антивирус Dr.Web** или **Dr.Web Security Space**). Также вам доступен пункт **Отсоединиться**, при выборе которого завершается установленное соединение с удаленным антивирусом.

Если необходимый компьютер не отображается в сети, попробуйте добавить его вручную. Для этого нажмите кнопку **Добавить** и введите IP-адрес.

Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте Dr.Web разрешено удаленное управление.

16. Включение и отключение самозащиты

Самозащита Dr.Web (Dr.Web SelfPROtect) применяется для защиты компонентов и каталогов самого антивируса как от несанкционированного воздействия извне (вирусные атаки), так и от случайных действий пользователя, которые могут навредить работе антивируса.

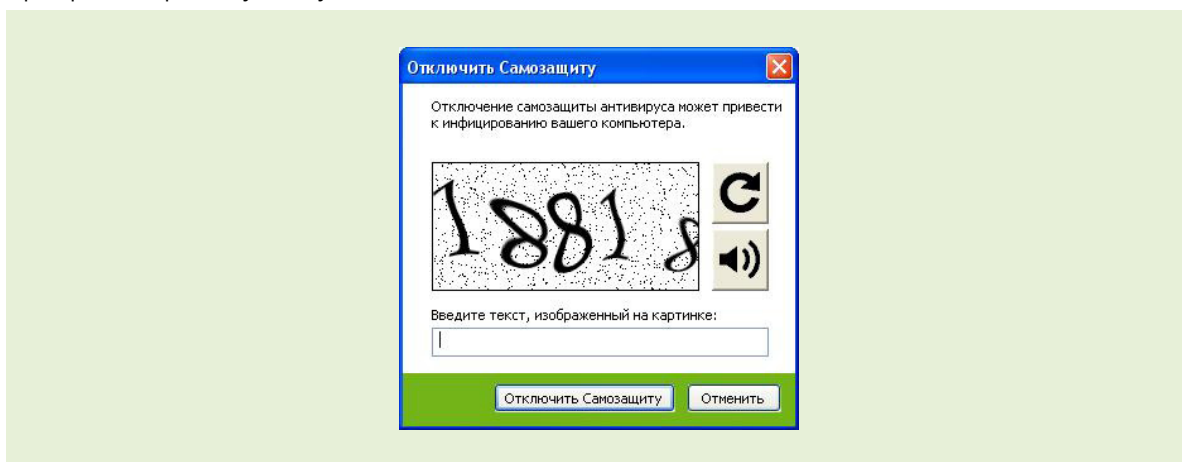
Dr.Web SelfPROtect служит для защиты модулей, процессов, а также веток реестра, которые использует Dr.Web для Windows в своей работе, от воздействия извне. Под внешним воздействием в данном случае могут пониматься как неосторожные действия пользователя, которые могут привести к неработоспособности или неправильной работе антивируса, так и деятельность анти-антивирусных вредоносных программ, в арсенал которых могут

входить такие действия, как завершение процессов антивируса, модификация или удаление файлов антивируса, а также модификация или удаление веток реестра Windows, которые использует Dr.Web.

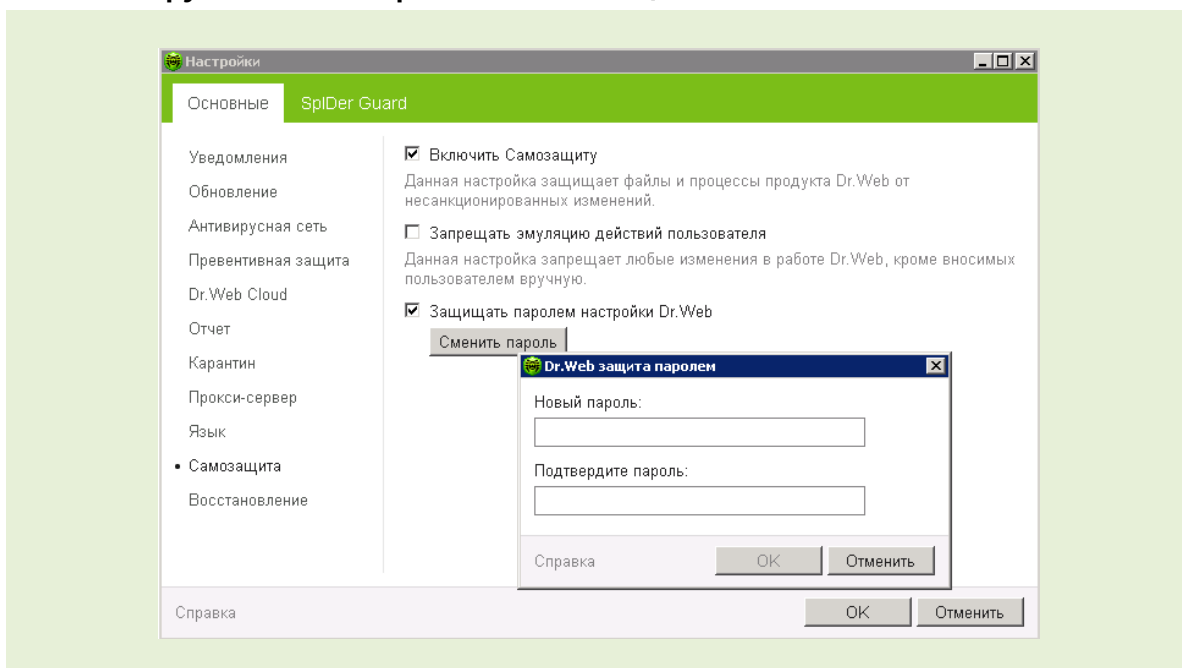
По умолчанию **Самозащита** всегда включена, и не рекомендуется отключать ее. Исключения составляют немногие ситуации. После завершения нужного действия не забудьте снова включить **Самозащиту**.

Модуль самозащиты **Dr.Web SelfPROtect** выполнен в виде драйвера уровня ядра системы `dwprot.sys`, и его невозможно выгрузить до перезагрузки системы.

Пользователь может временно приостановить работу модуля самозащиты, но для этого он должен ввести случайное число (либо пароль — в том случае, если он ранее был задан), которое показывается в специальном окне при попытке отключения **Dr.Web SelfPROtect**. Таким образом, вредоносная программа или пользователь без явного намерения не смогут прекратить работу модуля самозащиты.



Чтобы отключить самозащиту, выберите соответствующий пункт в меню **Агента**, а затем введите в появившемся окне пароль, который вы установили в настройках антивируса (меню **Инструменты** — **Настройки** — **Самозащита**):



Настройки **Dr.Web SelfPROtect** (как и настройки **Родительского контроля Dr.Web**, отвечающие за ограничение доступа к локальным объектам) содержатся в реестре в ветке `\\HKLM\\SYSTEM\\CurrentControlSet\\Services\\DwProt\\Parameters`.

Вся работа, которую администратору необходимо произвести с компонентами Dr.Web для Windows вручную, должна проводиться при отключенном модуле самозащиты Dr.Web SelfPROtect.

17. Создание отчета

При обращении в службу технической поддержки компании «Доктор Веб» вы можете сформировать отчет о вашей операционной системе и работе Dr.Web (необходимы права администратора).

Чтобы сформировать отчет, выберите пункт **Мастер отчетов** в подменю **Инструменты** меню **Агента**.



Для настройки параметров в открывшемся окне нажмите **Параметры отчета**. Отчет будет сохранен в виде архива в каталоге DoctorWeb, расположенном в папке профиля пользователя %USERPROFILE% (это путь сохранения по умолчанию, чтобы изменить его, укажите новый в строке **Путь** Параметров отчета).

Отчет может включать в себя следующие разделы (вы можете управлять составом разделов, добавляя и удаляя галочки в списке):

1. Техническая информация об ОС включает общие сведения о следующем:

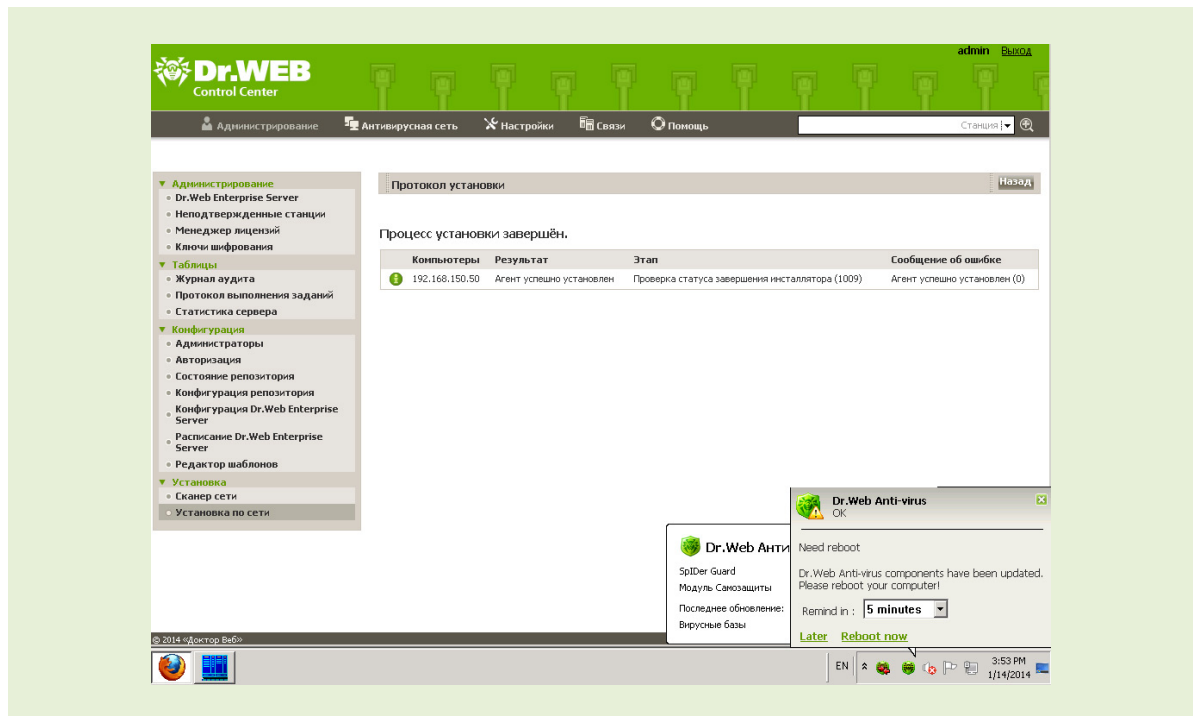
- компьютер;
- запущенные процессы;
- запланированные задания;
- службы, драйвера;
- браузер по умолчанию;
- установленные приложения;
- политики ограничений;
- файл HOSTS;
- серверы DNS;
- отчеты программы MSInfo;
- записи системного журнала событий;
- перечень системных каталогов;
- ветви реестра;
- провайдеры Winsock;
- сетевые соединения;
- отчеты отладчика Dr.Watson;
- индекс производительности.

2. Информация о продуктах Dr.Web:

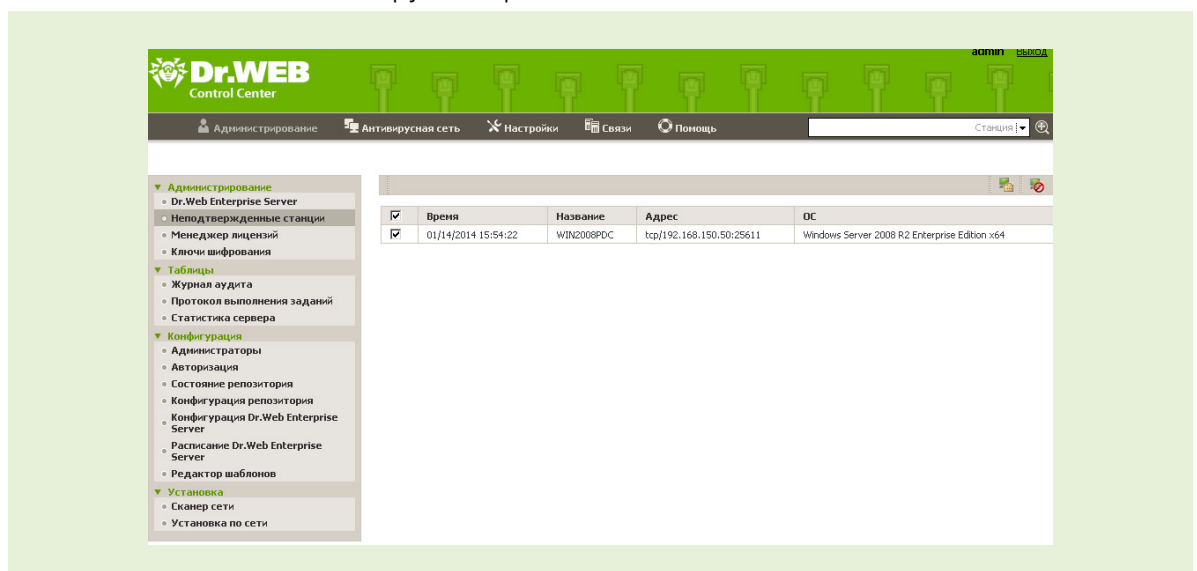
Информация о работе антивирусных решений Dr.Web всегда доступна в журнале событий операционной системы Windows, в разделе **Журналы приложений и служб – Doctor Web**. Чтобы создать отчет выбранной конфигурации, просто нажмите на кнопку **Сформировать отчет**.

18. Перевод антивирусного решения в режим централизованно управляемой защиты

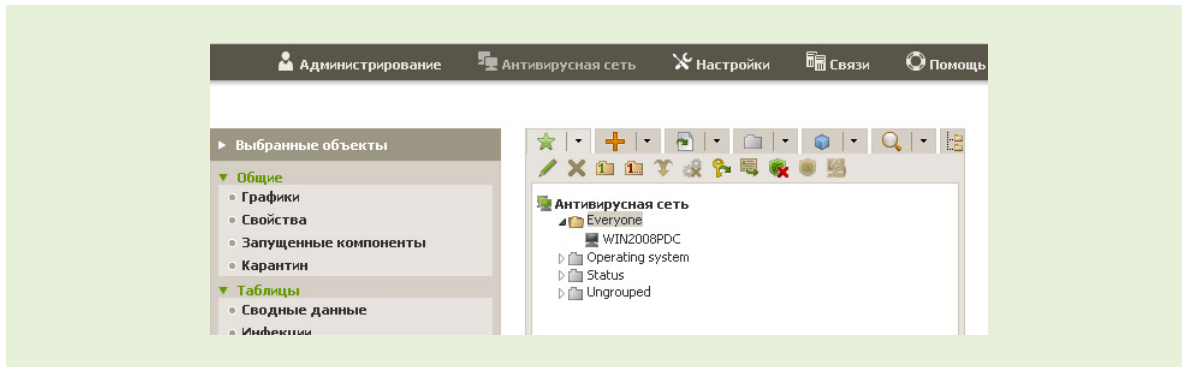
Для перевода Dr.Web для файловых серверов Windows в режим централизованно управляемой защиты необходимо воспользоваться возможностями, предоставляемыми **Центром управления** – например, **Сканером сети** Центра управления или **Установкой по сети** Центра управления.



После установки агента централизованной защиты необходимо подтвердить факт легитимности установки антивирусной защиты на файловый сервер – и перезапустить его для замены компонентов антивирусного решения.

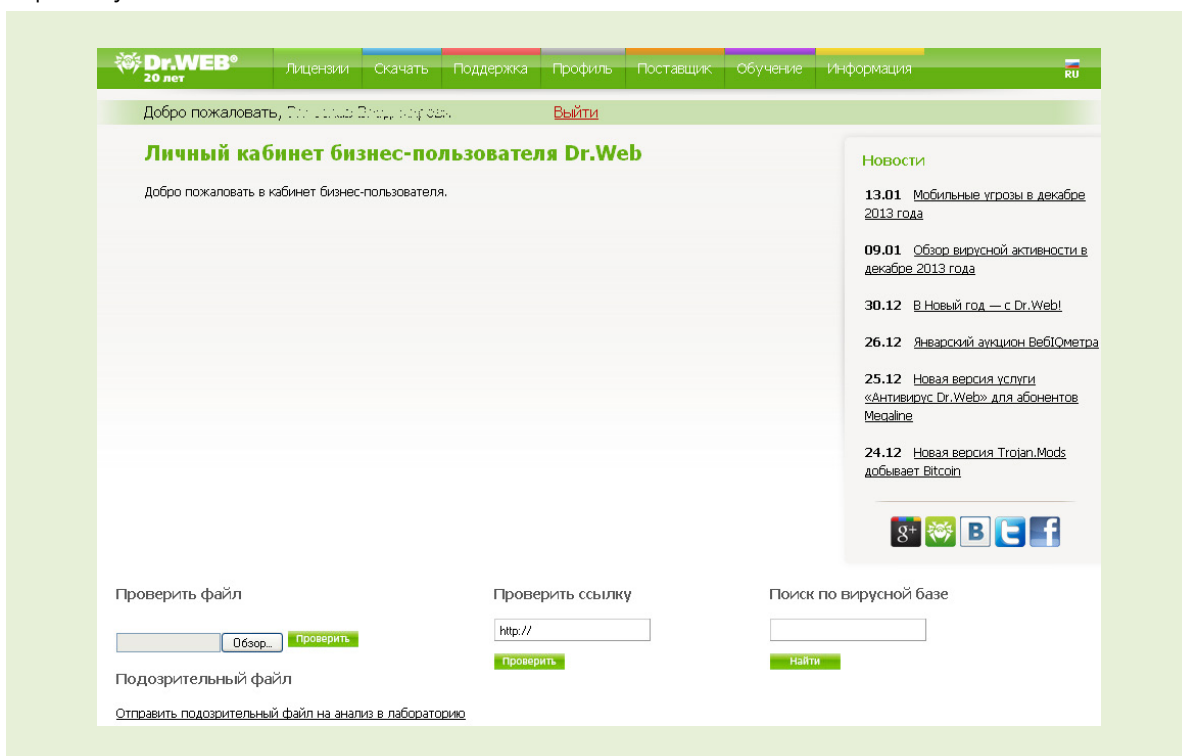


Перевод в режим централизованно управляемой защиты позволяет существенно расширить возможности антивирусной защиты, установив дополнительные компоненты или настроив систему автоматического реагирования на инциденты антивирусной безопасности.



19. Приложение 1. «Мой Dr.Web» — личный кабинет пользователя

Быть в курсе последних новостей вы можете, используя свой Личный Кабинет. Для того чтобы попасть в него из контекстного меню, выберите пункт Мой Dr.Web. Нажав на него, вы попадаете на домашнюю страницу сайта «Доктор Веб» (она откроется в вашем браузере по умолчанию):



Наиболее важными разделами сайта, с которыми рекомендуется ознакомиться, являются:

- **Скачать** — получение дистрибутивов продуктов Dr.Web, а также просмотр и скачивание документации.
- **Новости и Информация** — рекомендуется подписаться на новости компании, поскольку в ленте новостей периодически появляется важная информация об обновлении линейки продуктов Dr.Web, а также о вирусной активности.
- **Поддержка** — обращение в техническую поддержку и прочие полезные ресурсы и сервисы, которые помогут вам улучшить антивирусную защиту и узнать больше о вредоносных программах и средствах борьбы с ними.

- **Обучение** — важный раздел, посвященный обучению администрированию продуктов Dr.Web. На странице <https://training.drweb.com/external> вы можете зарегистрироваться в **Кабинете заочника**, записаться на понравившиеся курсы или вебинары, а по завершении этих курсов сдать экзамен и стать сертифицированным специалистом по антивирусной защите. Такой сертификат откроет для вас новые карьерные возможности и станет подтверждением полученных знаний.

20. Приложение 2. Получение услуг службы технической поддержки

В случае возникновения неразрешимой ситуации, какой-либо проблемы при работе антивируса или обнаружении недетектированного или ложно детектированного как вирус объекта, необходимо обратиться в службу технической поддержки компании «Доктор Веб».

20.1. Запрос в службу технической поддержки

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

- ознакомиться с последними версиями описаний и руководств по адресу <http://download.drweb.com/doc>,
- прочитать раздел часто задаваемых вопросов по адресу <http://support.drweb.com>,
- посетить форумы Dr.Web по адресу <http://forum.drweb.com>.

Чтобы отправить запрос в техподдержку, перейдите по ссылке **Поддержка** в верхнем меню официального сайта компании «Доктор Веб» (www.drweb.com). Попасть напрямую в данный раздел можно по ссылке <https://support.drweb.com>.

Dr.Web® Антивирус

Для дома Для бизнеса Скачать Магазин Поддержка Обучение Партнеры

Бесплатно в России 8-800-333-7932

Глобальная поддержка +7 (495) 789-45-86 круглосуточно

Казахстан +7 (727) 323-62-30 <http://www.drweb.kz>

Украина +380 (44) 238-24-35 <http://www.drweb.ua>

Языки поддержки: Русский, English, Deutsch, Français, 日本語

Вход на сайт
В чем преимущество?

E-mail:

Пароль:

Войти

Забыли пароль?

Услуги поддержки
[Задать вопрос](#)
Виртуальный инженер
[Форумы](#)

Услуги антивирусной лаборатории
[Расшифровка файлов \(Encoder\)](#)
[Отправить подозрительный файл](#)
[Сообщить о вредоносном сайте](#)

Бесплатно для пользователей Dr.Web
[Обновление до версии 9](#)
[Регистрация](#)
[Восстановление ключа «Мой Dr.Web»](#)
[Лицензионный сертификат](#)
[Разблокировка антивора](#)

Служба технической поддержки

Чтобы мы могли эффективно и максимально быстро ответить Вам, постарайтесь как можно более точно выбрать тему Вашего вопроса. После отправки запроса ему будет присвоен уникальный номер, а на указанный при заполнении формы запроса адрес электронной почты будет отправлена ссылка на страницу обработки Вашего запроса. На этой странице Вы можете производить различные действия с Вашим запросом: добавлять комментарии, просматривать историю запроса, закрыть запрос после разрешения проблемы.

Максимально допустимое время реакции на запрос — **48 часов**. Однако, как показывает практика, запросы начинают обрабатываться уже в течение первого часа с момента их поступления. Система обработки запросов пользователей находится под постоянным контролем руководства компании «Доктор Веб».

Прежде чем задать вопрос в поддержку, попытайтесь найти ответ самостоятельно в «Частых вопросах».

Я — владелец коммерческой лицензии Dr.Web

Я являюсь подписчиком на услугу «Антивирус Dr.Web»

Я не являюсь владельцем коммерческой лицензии Dr.Web

На начальной странице пользователю предлагается выбрать категорию, к которой он относится:

- **Я — владелец коммерческой лицензии Dr.Web.** К этой категории относятся пользователи всех антивирусных продуктов Dr.Web, владеющие лицензией на пользование антивирусом.

- **Я являюсь подписчиком на услугу «Антивирус Dr.Web».** Эту опцию необходимо выбрать пользователям, получающим антивирус как услугу от интернет-провайдера (Dr.Web AV-Desk).
- **Я не являюсь владельцем коммерческой лицензии Dr.Web.** Сюда можно отнести всех, кто пока не приобрел антивирус Dr.Web.

Рассмотрим создание запроса в техническую поддержку на примере первого варианта.

Когда пункт **Я — владелец коммерческой лицензии Dr.Web** будет отмечен, автоматически появятся два поля. Можно поступить двумя способами:


- В поле **Ключевой файл Dr.Web** с помощью кнопки **Обзор** указать размещение ключевого файла (по умолчанию располагается в папке установки антивируса).
- Указать **Серийный номер Dr.Web**, введя его в соответствующее поле.

Служба технической поддержки

Чтобы мы могли эффективно и максимально быстро ответить Вам, постарайтесь как можно более точно выбрать тему Вашего вопроса. После отправки запроса ему будет присвоен уникальный номер, а на указанный при заполнении формы запроса адрес электронной почты будет отправлена ссылка на страницу обработки Вашего запроса. На этой странице Вы можете производить различные действия с Вашим запросом: добавлять комментарии, просматривать историю запроса, закрыть запрос после разрешения проблемы.

Максимально допустимое время реакции на запрос — **48 часов**. Однако, как показывает практика, запросы начинают обрабатываться уже в течение первого часа с момента их поступления. Система обработки запросов пользователей находится под постоянным контролем руководства компании «Доктор Веб».

Прежде чем задать вопрос в поддержку, попытайтесь найти ответ самостоятельно в [«Частых вопросах»](#).

 *Я — владелец коммерческой лицензии Dr.Web*

Укажите ключевой файл Dr.Web или введите серийный номер Dr.Web

Ключевой файл Dr.Web	Серийный номер Dr.Web
<input type="text"/> <input type="button" value="Обзор..."/>	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>

Указав лицензионные данные, нажмите **Далее**.

Служба технической поддержки

Чтобы мы могли эффективно и максимально быстро ответить Вам, постарайтесь как можно более точно выбрать тему Вашего вопроса. После отправки запроса ему будет присвоен уникальный номер, а на указанный при заполнении формы запроса адрес электронной почты будет отправлена ссылка на страницу обработки Вашего запроса. На этой странице Вы можете производить различные действия с Вашим запросом: добавлять комментарии, просматривать историю запроса, закрыть запрос после разрешения проблемы.

Максимально допустимое время реакции на запрос — **48 часов**. Однако, как показывает практика, запросы начинают обрабатываться уже в течение первого часа с момента их поступления. Система обработки запросов пользователей находится под постоянным контролем руководства компании «Доктор Веб».

Прежде чем задать вопрос в поддержку, попытайтесь найти ответ самостоятельно в [«Частых вопросах»](#).

- [Работа антивируса: проблемы и вопросы](#)
- [Регистрация серийного номера/Получение ключевого файла](#)
- [Помощь в выборе антивируса, покупке/продление лицензии \(в том числе демо-лицензии\)](#)
- [Обнаружение или удаление вируса](#)
- **Новое!** [Заказать платную экспертизу вирусозависимого компьютерного инцидента](#)
- [Сообщить о ложном срабатывании Родительского контроля Dr.Web](#)
- [Бесплатная помощь пострадавшим от Trojan.Winlock](#)
- [Помощь пострадавшим от троянцев-шифровальщиков Trojan.Encoder](#)
- [Хочу работать в «Доктор Веб»!](#)
- [Предложения по улучшению функционала антивируса](#)
- [Отзыв о работе компании и ее партнеров](#)

На открывшейся странице необходимо выбрать нужную тему обращения. Это может быть:

- Технический вопрос о работе антивируса (кроме услуги «Антивирус Dr.Web»)
- Регистрация серийного номера / Получение ключевого файла
- Помощь в выборе антивируса, покупка/продление лицензии (в том числе демолицензии)
- Обнаружение или удаление вируса
- Сообщить о ложном срабатывании Родительского контроля Dr.Web

Сообщить о ложном срабатывании или пропуске вредных ссылок в модуле родительского контроля

Заполните, пожалуйста, форму:

Ваше имя/организация:


Ваш e-mail:

Категория запроса:

Фильтр:

Ссылка:

Комментарий:



Подтверждение:

- Бесплатная помощь пострадавшим от Trojan.Winlock
- Хочу работать в «Доктор Веб»!
- Предложения по улучшению функционала антивируса
- Отзыв о работе компании и ее партнеров

Нажмите левой кнопкой мыши на интересующий вас раздел. Например, [Работа антивируса: проблемы и вопросы](#). Теперь необходимо указать тип защищаемого оборудования (домашний или офисный ПК, сеть, сервер и т. д.). Начиная с этого момента, вы всегда сможете вернуться на предыдущий шаг, воспользовавшись кнопкой **Назад**. Для примера возьмем *Защита домашнего компьютера/ноутбука*.

Следующий этап — выбор используемой операционной системы. В качестве примера возьмем ОС *Windows*.

Теперь необходимо указать продукт, по поводу которого происходит обращение.

Откроется страница, на которой необходимо заполнить поля для непосредственного создания запроса.

В соответствующие поля требуется ввести следующие данные:

- **Ф. И. О.** Для обращения сотрудников службы поддержки к клиенту. Это поле может быть заполнено автоматически, при условии что на первом шаге указан серийный номер или ключевой файл.
- **Организация.** Название организации, владеющей лицензией (присутствует только в разделах для корпоративных клиентов).
- **Должность.** Можно указать должность сотрудника, обращающегося за поддержкой (присутствует только в разделах для корпоративных клиентов).

- **Провайдер.** Требуется указать провайдера, клиентом которого является пользователь (присутствует только при выборе варианта Вопрос об услуге «Антивирус Dr.Web»).
- **Контактный e-mail.** Для получения пользователем уведомлений о ходе рассмотрения запроса. Также заполняется автоматически при условиях, указанных в описании поля Ф. И. О.
- **Номер контактного телефона.** Как вариант контакта для быстрой связи при необходимости.
- **Число, отображенное на картинке.** Предназначено для противодействия отправлению запросов автоматическими средствами.
- **Вопрос.** В этом поле нужно предельно конкретно и подробно описать суть возникшей проблемы. Это и есть текст вашего обращения в службу поддержки.

Также есть возможность с помощью кнопки **Обзор** приложить к запросу какие-либо файлы. Это может быть отчет о работе антивируса, файлы, иллюстрирующие проблему (подозрительные объекты, скриншоты и т. д.).

Примечание. Во время ввода вопроса в левом верхнем углу окна может появиться зеленый прямоугольник **Похожие вопросы** — таким образом система предлагает вам поискать решение своей проблемы в FAQ. Нажмите левой кнопкой мыши на прямоугольник, и окно с похожими вопросами (отбор идет по ключевым словам) развернется в центр экрана.

Если проигнорировать предложение — после нажатия кнопки **Отправить** окно с похожими вопросами раскроется автоматически.

В окне похожих вопросов нажмите на подходящий, если он имеется в списке, или нажмите **Закреть**.

При нажатии на выбранный вопрос он раскрывается, и вы можете прочесть ответ. Отреагировать на полученные данные можно тремя способами:

- **Ответ помог** — если вы получили необходимую информацию и дальнейшая помощь не требуется.
- **Полезная информация** — если представленный текст был полезен или интересен, но не дал требуемого вам ответа.
- **Неподходящий вопрос** — если информация не имеет прямого отношения к интересующей вас проблеме.

При выборе любого из вариантов они исчезают, и окно похожих вопросов можно закрыть. Если ответ получен — запрос можно не отсылать, если неясные моменты еще остались — нажмите **Отправить**.

Если указанный серийный номер или ключевой файл заблокирован, пользователь будет автоматически перенаправлен на страницу http://support.drweb.com/key_blocked.

Примечание. Если вы выбрали раздел **Вопрос об услуге «Антивирус Dr.Web»**, то вам будет доступен только этот раздел, при этом не требуется указывать используемый продукт и операционную систему.

Незарегистрированные пользователи могут обратиться в службу поддержки со следующими запросами (без предоставления регистрационных данных):

- Вопрос об услуге «Антивирус Dr.Web»
- Помощь в выборе антивируса, покупка/продление лицензии (в том числе демолицензии)
- Сообщить о ложном срабатывании Родительского контроля Dr.Web
- Бесплатная помощь пострадавшим от Trojan.Winlock
- Хочу работать в «Доктор Веб»!
- Предложения по улучшению функционала антивируса
- Отзыв о работе компании и ее партнеров

Порядок действий с этими вариантами не отличается от описанных в примере. Для отправки запроса нажмите **Отправить**. Откроется окно с уведомлением об успешном создании запроса и ссылкой **Перейти к запросу**.

При взятии запроса в обработку и каждом изменении его статуса сотрудником, на указанный пользователем адрес электронной почты приходит информационное письмо с темой **your ticket KEYJ-0213** (где **KEYJ-0213** — уникальный номер запроса, присваиваемый автоматически) и следующим содержанием:

Уважаемый пользователь,

Это напоминание послано Вам о Вашем запросе в службу технической поддержки компании «Доктор Веб». В статусе Вашего запроса произошли изменения, возможно, от Вас требуется дополнительная информация. Чтобы посмотреть статус своего запроса, перейдите, пожалуйста, по ссылке:

<https://support.drweb.com/process/?ticket=KEYJ-0213>

Если проблема для Вас неактуальна или же Вы не хотите более получать уведомления по этому запросу, пожалуйста, нажмите на кнопку «Закреть запрос», после чего Ваш запрос не будет обрабатываться.

Спасибо за сотрудничество.

С уважением,

ООО «Доктор Веб»

Служба техподдержки

<http://www.drweb.com> <http://support.drweb.com>

Вы всегда можете открыть свой запрос, перейдя по указанной в письме ссылке.

После нажатия **Перейти к запросу**, откроется окно, содержимое которого является своеобразным диалогом между пользователем и сотрудником технической поддержки.

Рассмотрим страницу работы с запросом подробнее.

В верхней части указан номер запроса и его актуальный статус. Статус может быть следующим:

- **Новый** — запрос, не взятый в обработку никем из сотрудников.
- **Подтвержденный** — запрос, взятый в обработку сотрудником технической поддержки.
- **Ожидание ответа пользователя** — запрос, в котором ожидается реакция от пользователя. Если проблема решена, пользователь может закрыть запрос или предоставить дополнительную информацию (например, отчеты работы компонентов антивируса), если это требуется. Если пользователь никак не отреагировал в течение 10 рабочих дней, запрос будет автоматически закрыт.
- **Ожидание ответа разработчиков** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется помощь разработчиков. Например, требуется воспроизвести проблемную ситуацию на тестовом стенде или исправить ошибку в компоненте антивируса.
- **Ожидание ответа службы вирусного мониторинга** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется участие работников службы вирусного мониторинга. Например, при ложном срабатывании антивируса.
- **Ожидание ответа отдела по работе с партнерами** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется привлечь сотрудников отдела по работе с партнерами. Например, когда нужна консультация по вопросам, связанным с продажей или продлением лицензий, перевыдачей серийного номера.
- **Ожидание выпуска обновленного компонента** — данный статус присваивается запросу, если для решения описанной в нем проблемы требуется обновление

какого-либо компонента антивируса. Например, если в ходе обработки запроса выяснилось, что возникшая проблема исправлена в одном из обновлений и нужно дождаться его выхода.

- **Ожидание ответа техподдержки** — запрос, в котором требуется ответ сотрудника техподдержки. В это состояние запрос переключается после ответа пользователя.
- **Закрытый запрос** — статус присваивается, если пользователь самостоятельно закрывает запрос или автоматически после 10 рабочих дней отсутствия ответа от него. Также запрос может быть закрыт сотрудником при некорректном поведении пользователя. Закрытый запрос может быть вновь открыт сотрудником техподдержки с помощью добавления сообщения.

Ниже расположена таблица, первая колонка которой называется **Дата, время, статус**. Здесь указываются дата и время каждого нового сообщения (если только время — значит, сообщение написано в текущие сутки) и его статус. Статус отображает актуальное состояние запроса на момент размещения этого сообщения. Вторая колонка **Кто** показывает автора каждого из сообщений. Если ответ исходит от пользователя, здесь указано, что он ввел в поле **Ф. И. О.** при создании запроса, если сотрудник техподдержки — то имя сотрудника.

В колонке **Информация** отображаются сообщения участников диалога. Если текст слишком большой, видна только его часть. Чтобы прочитать такое сообщение, воспользуйтесь ссылкой **просмотр**.

Также при работе с запросом можно использовать кнопки:

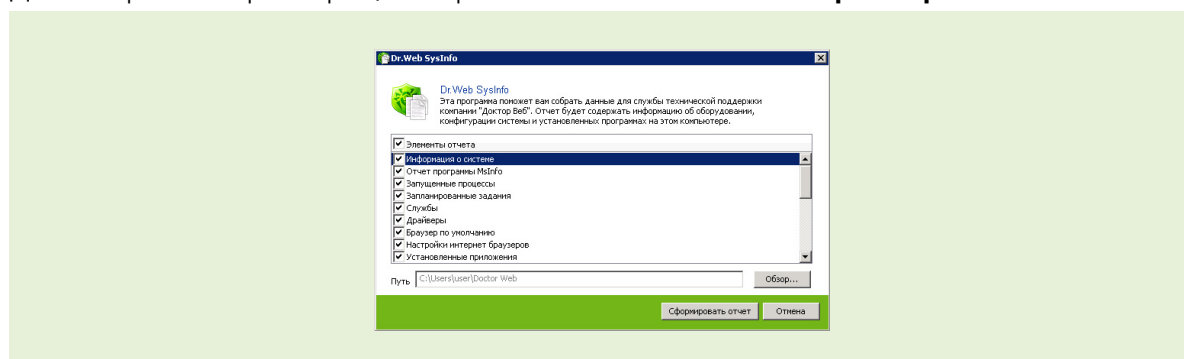
- **Добавить комментарий** — позволяет пользователю ответить на вопросы, заданные сотрудником техподдержки, или разъяснить какие-либо элементы проблемы (см. рис.). Также на странице добавления комментария к ответу можно приложить запрошенные сотрудником данные (например, log-файлы).
- **Обновить** — обновляет текущую страницу. Используется во время интенсивного диалога пользователя с сотрудником.
- **Закрыть запрос** — позволяет пользователю самостоятельно закрыть запрос, когда проблема решена. При этом предлагается оценить по пятибалльной шкале работу сотрудника и указать причину, по которой запрос закрывается.

Отметив флажком оценку работы сотрудника и указав причину закрытия запроса, необходимо нажать на кнопку **Отправить**. После этого откроется страница, информирующая об успешном закрытии запроса. Отсюда пользователь может либо вернуться на главную страницу трекера, либо еще раз просмотреть запрос, воспользовавшись одной из предложенных ссылок.

20.2. Сбор информации о системе

При обращении в службу технической поддержки компании «Доктор Веб» желательно сформировать отчет о вашей операционной системе и работе Dr.Web.

Чтобы это сделать, нажмите в меню **Агента** пункт **Инструменты**, затем **Мастер отчетов**. Для настройки параметров, в открывшемся окне нажмите **Параметры отчета**.



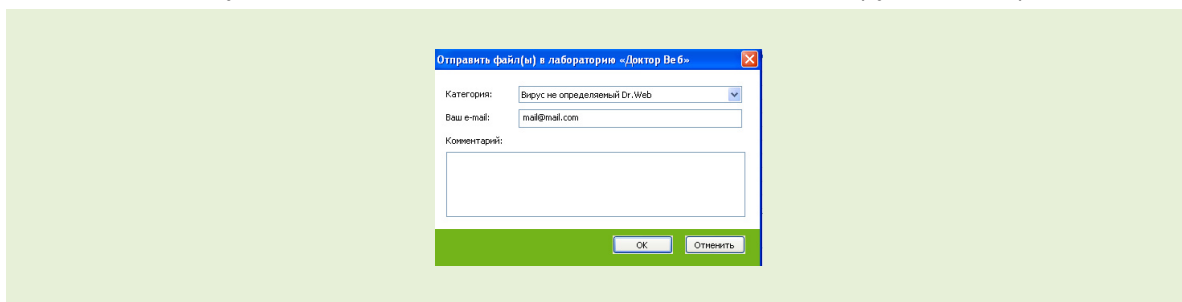
Отчет будет сохранен в виде архива в каталоге DoctorWeb, расположенном в папке профиля пользователя %USERPROFILE%.

20.3. Отсылка образцов на анализ

Если вы считаете, что Dr.Web не определил объект как вредоносный, или же произошло ложное срабатывание (не представляющий опасности объект был детектирован как вирус), необходимо:

- Поместить объект, на который произошло ложное срабатывание, в **Карантин**.
- Провести обновление вирусных баз.
- Выбрать объект в **Карантине** и произвести повторное сканирование.
- Если все еще наблюдается ложное срабатывание, отослать объект на анализ в **Анти-вирусную лабораторию «Доктор Веб»**. Это можно сделать двумя способами:
 - С главной страницы сайта «Доктор Веб» перейти на страницу **Послать вирус**: <https://vms.drweb.com/sendvirus>.
 - В **Менеджере Карантина** нажать правой кнопкой мыши на нужный объект. В контекстном меню в таблице доступна следующая опция: **Отправить файл(ы) в лабораторию «Доктор Веб»** — отправить в **Антивирусную лабораторию «Доктор Веб»** файл на проверку.

В обоих случаях необходимо заполнить сведения об обнаруженной проблеме.

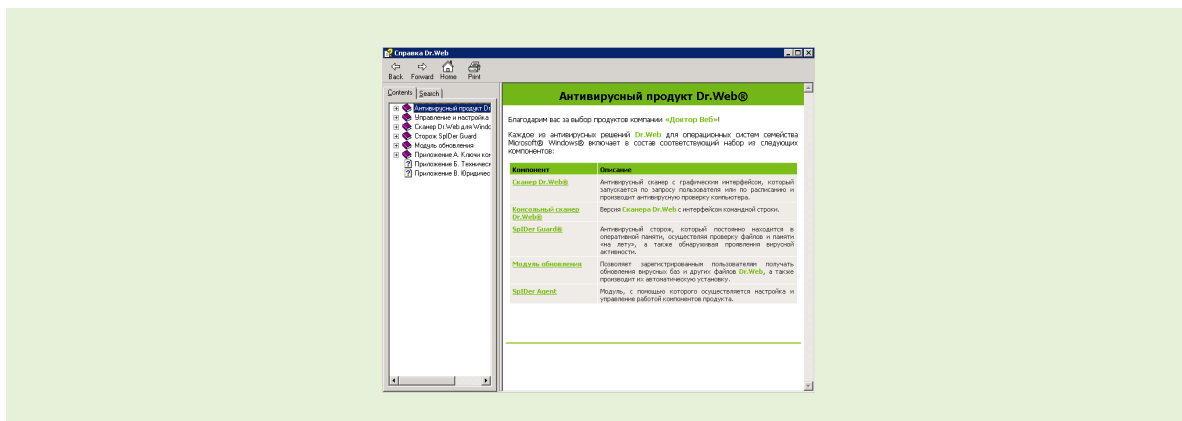


21. Приложение 3. Работа со справкой о программе

Справка о программе Dr.Web содержит достаточно подробную информацию о каждом компоненте, доступном в настройках программы. В случае возникновения затруднений при работе с программой, до того, как обратиться в службу технической поддержки, рекомендуется ознакомиться со справочными материалами.

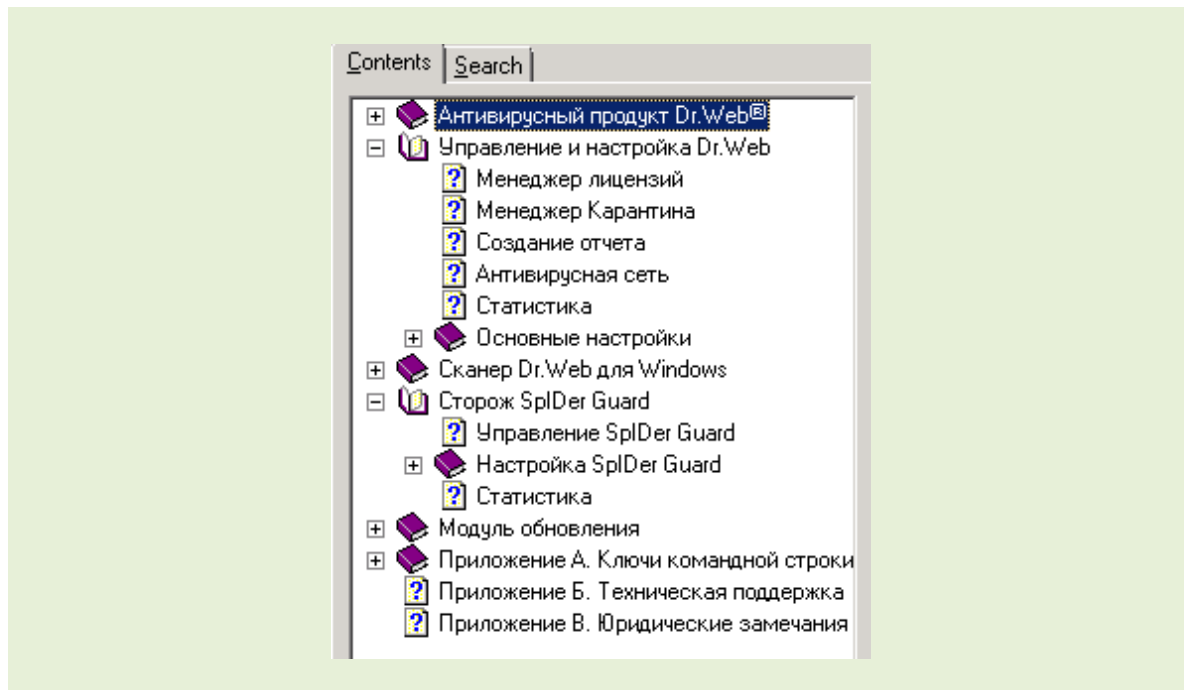
Справка запускается двумя способами:

1. Из контекстного меню **Агента** — щелчок по значку **Агента**, выбрать пункт **Справка**. Появится окно справки о программе:

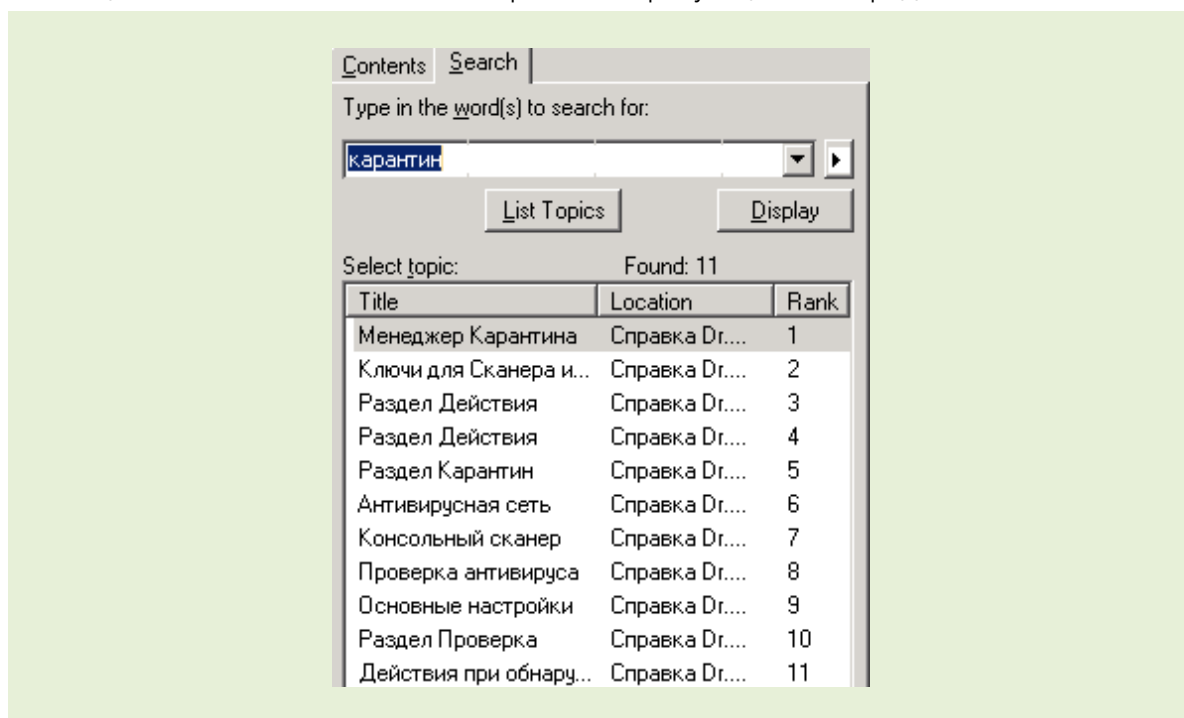


2. Нажатием на **Справка** в левом нижнем углу любого окна приложения – **Справка** откроется на нужном пункте, соответствующем разделу настроек.

В левой части окна **Справки** имеются две вкладки. Во вкладке **Содержание** расположен иерархический список компонентов справочного материала, каждый пункт раскрывается при нажатии на значок +:



Во вкладке **Поиск** вы можете найти интересующую вас информацию по ключевым словам или фразам. При этом вы можете использовать операторы **И**, **ИЛИ**, **ОКОЛО** (приблизительно) и **НЕ** для уточнения параметров поиска. Результатом станет список разделов **Справки**, касающихся в той или иной степени (ранг) интересующего вас предмета:



Кнопка **Домой** в левом верхнем углу открывает главную страницу «Доктор Веб» в окне **Справки**, кнопка **Печать** позволяет распечатать **Справку** на любом доступном вам принтере.

22. Приложение 4. Поисковый модуль Dr.Web

Поисковый модуль Dr.Web (файл `drweb32.dll`) является одним из основных модулей антивируса Dr.Web.

Этот компонент служит для обнаружения наличия в сканируемом объекте инфекции.

Поисковый модуль использует вирусные базы, расположенные в файлах с расширением `*.vdb`, которые автоматически обновляются в соответствии с текущими настройками компонентов антивируса. Вирусные базы являются неотъемлемой частью поискового модуля. Помимо записей для обнаружения инфекций, в вирусных базах Dr.Web могут содержаться процедуры, отвечающие за функции непосредственно поискового модуля, например некоторые функции эвристического анализатора.

Подробно о структуре и частоте выпуска обновлений вирусной базы Dr.Web можно прочитать в документации на антивирусный комплекс.

Поисковый модуль используют многие компоненты Dr.Web, а именно: сканеры, сторожи SpIDer Guard и SpIDer Mail. Это позволяет этим компонентам использовать одинаковые алгоритмы поиска вирусов. Более того, этот же самый поисковый модуль используется в версиях антивируса Dr.Web для операционных систем, отличных от Windows.

Взаимодействие компонентов антивируса Dr.Web с поисковым модулем происходит следующим образом.

1. Поисковый модуль производит первичное сканирование, при котором изучается общая структура сканируемого файла: упакован он или нет, является ли файловым контейнером или файловым архивом, производится сканирование контейнера или файлового архива как единого объекта. Если на этом этапе обнаруживается инфекция, то результаты сканирования возвращаются компоненту Dr.Web, и сканирование заканчивается.
2. Если инфекция не обнаружена, и если файл является контейнером или файловым архивом, то поисковый модуль возвращает компоненту название контейнера или файлового архива для записи их в файл отчета компонента.
3. Для составных объектов (файловых контейнеров и файловых архивов) последовательно распаковываются и сканируются вложенные объекты.
4. Если какой-то файл был вылечен, то процедура сканирования файла начинается сначала, т. к. существуют случаи многократного заражения файлов различными вирусами или одним и тем же вирусом.

Поисковый модуль может обновляться внутри одной и той же версии Dr.Web, таким образом возможно динамически добавлять проверку содержимого новых типов архивов и исполняемых файлов, сжатых новыми упаковщиками.

В поисковом модуле Dr.Web реализован эвристический анализатор для определения неизвестных вирусов по косвенным признакам. Так, в поисковом модуле реализованы алгоритмы для следующих типов неизвестных вирусов:

- COM – вирус, заражающий com-файлы (MS-DOS);
- EXE – вирус, заражающий exe-файлы (MS-DOS);
- TSR – резидентный вирус (MS-DOS);
- WIN.EXE – вирус, заражающий exe-файлы (Windows: NE, PE и т. д.);
- MACRO – вирус, заражающий документы Microsoft Office;
- BOOT – вирус, заражающий загрузочные секторы дисков;
- CRYPT – зашифрованный или полиморфный вирус;
- SCRIPT – вирус, содержащийся в скрипте;
- BATCH – вирус, содержащийся в командном файле;

- IRC – вирус, поражающий программы немедленного обмена сообщениями;
- DLOADER – неизвестная модификация вируса типа Trojan.DownLoader.xxx;
- MULDROP – неизвестная модификация вируса типа Trojan.MulDrop.xxx;
- STPAGE – неизвестная модификация вируса типа Trojan.StartPage.xxx;
- BACKDOOR – неизвестная модификация вируса типа BackDoor.xxx;
- PWS – неизвестная модификация вируса типа Trojan.PWS.xxx;
- WORM и MAIL.WORM – почтовые черви;
- прочее.

Данный список не претендует на полноту.

В большинстве случаев отключать эвристический анализатор не рекомендуется, т. к. часто с помощью эвристического анализа можно обнаружить новые вирусы или модификации уже известных вредоносных программ. Подозрительный файл можно отправить на анализ в антивирусную лабораторию ООО «Доктор Веб», после чего новый вирус будет в кратчайшие сроки добавлен в вирусную базу.

Отключение данной настройки можно рекомендовать лишь в том случае, когда было обнаружено ложное срабатывание на определенный тип файлов. После корректировки вирусной базы настройку рекомендуется включить и повторить сканирование.

Начиная с версии Dr.Web 4.44 в состав эвристического анализатора встроена новая технология Origins Tracing, которая основана на поиске вредоносных программ, некоторым образом похожих на программы, записи о которых уже имеются в вирусных базах Dr.Web. При обновлении вирусных баз Dr.Web технология Origins Tracing использует сразу же новые вирусные записи в качестве отправных точек для нахождения сходства. Данная технология практически не имеет ложных срабатываний. Все вредоносные файлы, найденные с помощью технологии Origins Tracing, считаются неизлечимыми, к ним применяются действия, соответствующие настройкам для неизлечимых объектов. В наименовании найденных с помощью данной технологии вирусов используется суффикс `.origin`. Хотя данная технология является частью несигнатурного анализа антивируса Dr.Web, файлы, обнаруженные с помощью этой технологии, не следует отправлять на анализ в вирусную лабораторию, т. к. в компонентах антивируса Dr.Web данная технология по весу приравнена к сигнатурному анализу. Исключения составляют файлы, обнаруженные с помощью этой технологии и являющиеся заведомо чистыми. Данные файлы следует отправлять на анализ в вирусную лабораторию с целью устранения ложного срабатывания.

Начиная с версии Dr.Web 5.0 в состав эвристического анализатора встроены универсальный распаковщик FLY-CODE. Данная технология позволяет распаковать файлы, упакованные неизвестными Dr.Web упаковщиками, и на основе специальных записей вирусной базы делать предположение о наличии опасного кода. Универсальный распаковщик FLY-CODE является эффективным средством против использования вирусописателями полиморфных (постоянно видоизменяющихся) упаковщиков.

В поисковом модуле Dr.Web реализована поддержка распаковки различных архивов. Это дает возможность проверять содержимое большинства архивов на наличие инфекций.

Следует помнить, что лечение, удаление, переименование и перемещение объектов, находящихся внутри архивов, невозможно. Если нужно проделать одну из этих операций, нужно предварительно распаковать соответствующие файлы из архива во временную папку, а после проведения необходимых действий – запаковать обратно.

Без специальной настройки в конфигурационном файле удаление архива целиком тоже невозможно.

В настоящее время поддерживаются следующие архиваторы: ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP.

Также поддерживаются следующие типы самораспаковывающихся архивов: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy.

Также поддерживаются следующие типы инсталляторов: Agentix Installer, Agency SFX, Commodore, FilePacker, File2Pack SFX, SFXFactory (ZIP-SFX), Stardust Setup Package и некоторые другие.

В поисковом модуле Dr.Web реализована проверка файлов почтовых форматов.

Поддерживается проверка писем, соответствующих формату ARPA Internet Text Messages (RFC822), в том числе с расширениями MIME, в кодировке форматов UUENCODE, BASE64, Quoted Printable.

Поддерживаются открытые форматы почтовых архивов, создаваемые почтовыми программами Mozilla, Netscape, The Bat! и др.

Не поддерживаются форматы почтовых архивов, созданных в программах Microsoft Outlook, Microsoft Outlook Express и других проприетарных форматов.

В поисковом модуле Dr.Web реализована поддержка файловых контейнеров следующих форматов: 1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM.

При настройке модулей антивируса Dr.Web следует различать файловые контейнеры и файловые архивы. Например, нельзя отключить проверку файловых контейнеров, но можно при необходимости отключить проверку файловых архивов.

В поисковом модуле Dr.Web реализована поддержка большинства известных программ сжатия исполняемых файлов, среди которых ASPACK, UPX, FSG, MORPHINE, YODA и многие другие.

Не все из этих программ служат только для уменьшения объема файлов. Некоторые из них созданы, например, для защиты программ от взлома, другие — для затруднения детектирования вирусов.

«Доктор Веб»

Dr.Web® – российский разработчик средств информационной безопасности.

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

Антивирусные продукты Dr.Web® разрабатываются с 1992 года, неизменно демонстрируют превосходные результаты детектирования вредоносных программ и 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®!

Dr.Web® Центральный офис в России

125124, Россия, Москва 3-я улица Ямского поля, вл. 2, корп. 12а

Телефон: +7 (495) 789-45-87 (многоканальный)

Факс: +7 (495) 789-45-97

www.drweb.com

www.freedrweb.com

www.av-desk.com

Информацию о региональных представительствах и офисах вы можете найти на официальном сайте компании.