Dr.WEB

KATANA

Руководство пользователя

Dr.Web KATANA
Версия 1.0
Руководство пользователя
04.08.2022

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

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

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. О продукте

Dr.Web KATANA защищает систему от компьютерных угроз с помощью несигнатурных методов: анализирует поведение процессов, использует облачные технологии обнаружения угроз и предустановленные правила. Программа не конфликтует с антивирусами других разработчиков и может работать в паре с ними, чтобы усилить защиту компьютера.

1.1. Условные обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

1.2. Методы обнаружения угроз

Поведенческий анализ

Технология поведенческого анализа Dr.Web Process Heuristic защищает от новейших, наиболее опасных вредоносных программ, которые способны избежать обнаружения традиционными сигнатурными и эвристическими механизмами.

Dr.Web Process Heuristic анализирует поведение каждой запущенной программы, сверяясь с постоянно обновляемыми облачным сервисом Dr.Web, и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности, после чего принимаются необходимые меры по нейтрализации угрозы.

Данная технология защиты данных позволяет свести к минимуму потери от действий неизвестного вируса — при минимальном потреблении ресурсов защищаемой системы.

Dr.Web Process Heuristic контролирует любые попытки изменения системы:

- распознает процессы вредоносных программ, изменяющих нежелательным образом пользовательские файлы (например действия троянских программ-шифровальщиков);
- препятствует попыткам вредоносных программ внедриться в процессы других приложений;
- защищает от модификаций вредоносными программами критических участков системы;
- выявляет и прекращает вредоносные, подозрительные или ненадежные сценарии и процессы;
- блокирует возможность изменения вредоносными программами загрузочных областей диска с целью невозможности запуска (например буткитов) на компьютере;
- предотвращает отключение безопасного режима Windows, блокируя изменения реестра;
- не позволяет вредоносным программам изменить правила запуска программ;
- пресекает загрузки новых или неизвестных драйверов без ведома пользователя;
- блокирует автозапуск вредоносных программ, а также определенных приложений, например анти-антивирусов, не давая им зарегистрироваться в реестре для последующего запуска;
- блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможной установку троянских программ под видом нового виртуального устройства;
- не позволяет вредоносному программному обеспечению нарушить нормальную работу системных служб.

Защита от эксплойтов

Технология Dr.Web ShellGuard, входящая в состав Dr.Web Process Heuristics, защищает компьютер от эксплойтов — вредоносных объектов, пытающихся использовать уязвимости с целью получения контроля над атакуемыми приложениями или операционной системой в целом.

Dr.Web ShellGuard защищает распространенные приложения, устанавливаемые на компьютеры под управлением Windows:

- интернет-браузеры (Internet Explorer, Mozilla Firefox, Яндекс.Браузер, Google Chrome, Vivaldi Browser);
- приложения MS Office, включая MS Office 2016;
- системные приложения;
- приложения, использующие java-, flash- и pdf-технологии;

- медиапроигрыватели.

Анализируя потенциально опасные действия, система защиты, благодаря технологии Dr.Web ShellGuard, опирается не только на прописанные правила, хранящиеся на компьютере, но и на знания облачного сервиса Dr.Web, в котором собираются:

- данные об алгоритмах программ с вредоносными намерениями,
- информация о заведомо чистых файлах,
- информация о скомпрометированных цифровых подписях известных разработчиков программного обеспечения,
- информация о цифровых подписях рекламных или потенциально опасных программ,
- алгоритмы защиты тех или иных приложений.

1.3. Системные требования

Использование Dr.Web возможно на компьютерах, удовлетворяющих следующим требованиям:

Параметр	**Требование**
Процессор	С поддержкой системы команд i686.
Свободная оперативная память	Не менее 100 МБ.
Место на жестком диске	150 МБ для размещения компонентов продукта. Файлы, создаваемые в ходе установки, потребуют дополнительного места.
Операционная система	Для 32-разрядных операционных систем: • Windows XP с пакетом обновлений SP2 или более поздними; • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10 21H2 или более ранняя; • Windows Server 2003 с пакетом обновлений SP1 или более поздними; • Windows Server 2008. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1;

	• Windows 10 21H2 или более ранняя; • Windows 11; • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022.
Разрешение экрана	Не менее 1024x768.

Для обеспечения правильной работы Dr.Web должны быть открыты следующие порты:

Назначение	**Направление**	**Номера портов**
Для активации и продления лицензии	исходящий	443
Для обновления (если включена опция обновления по https)	исходящий	443
Для обновления	исходящий	80
Для соединения с облачным сервисом Dr.Web Cloud	исходящие	2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

Опущенные требования к конфигурации совпадают с таковыми для соответствующих операционных систем.

2. Установка, восстановление и удаление Dr.Web KATANA

Перед началом установки Dr.Web KATANA ознакомьтесь с системными требованиями. Также рекомендуется выполнить следующие действия:

- установить все критические обновления, выпущенные компанией Microsoft для вашей версии операционной системы (их можно загрузить и установить с сайта обновлений компании: https://support.microsoft.com/help/12373/windows-update-faq); если поддержка операционной системы производителем прекращена, рекомендуется перейти на более современную версию операционной системы;
- проверить при помощи системных средств файловую систему и устранить обнаруженные проблемы;
- закрыть активные приложения.

2.1. Первая установка

Установка Dr.Web возможна в любом из следующих режимов:

- в фоновом режиме,
- в обычном режиме.

Установка в обычном режиме

Чтобы запустить установку в обычном режиме, воспользуйтесь одним из следующих методов:

- если у вас имеется установочный файл (`drweb-1.0-katana.exe`), запустите его;
- если у вас имеется фирменный диск с установочным комплектом, вставьте диск в привод. Если для привода включен режим автозапуска диска, процедура установки запустится автоматически. Если режим автозапуска отключен, запустите на выполнение файл `autorun.exe`, расположенный на диске. Откроется окно, содержащее меню автозапуска. Нажмите кнопку **Установить**.

Следуйте указаниям программы установки. На любом шаге до начала копирования файлов на компьютер вы можете выполнить следующее:

- чтобы вернуться к предыдущему шагу программы установки, нажмите кнопку **Назад**;
- чтобы перейти на следующий шаг программы, нажмите **Далее**;
- чтобы прервать установку, нажмите кнопку **Отмена**.

Чтобы установить программу

1. Если на вашем компьютере уже установлен антивирус компании «Доктор Веб», Мастер установки предупредит вас о несовместимости программы Dr.Web и иных антивирусных решений и предложит удалить их.

Перед началом установки проверяется актуальность установочного файла. В случае если существует более новый установочный файл, вам будет предложено его скачать.

2. На этом шаге вы можете подключиться к облачным сервисам Dr.Web, которые позволят осуществлять проверку данных, используя наиболее свежую информацию об угрозах, которая обновляется на серверах компании «Доктор Веб» в режиме реального времени. Опция включена по умолчанию.

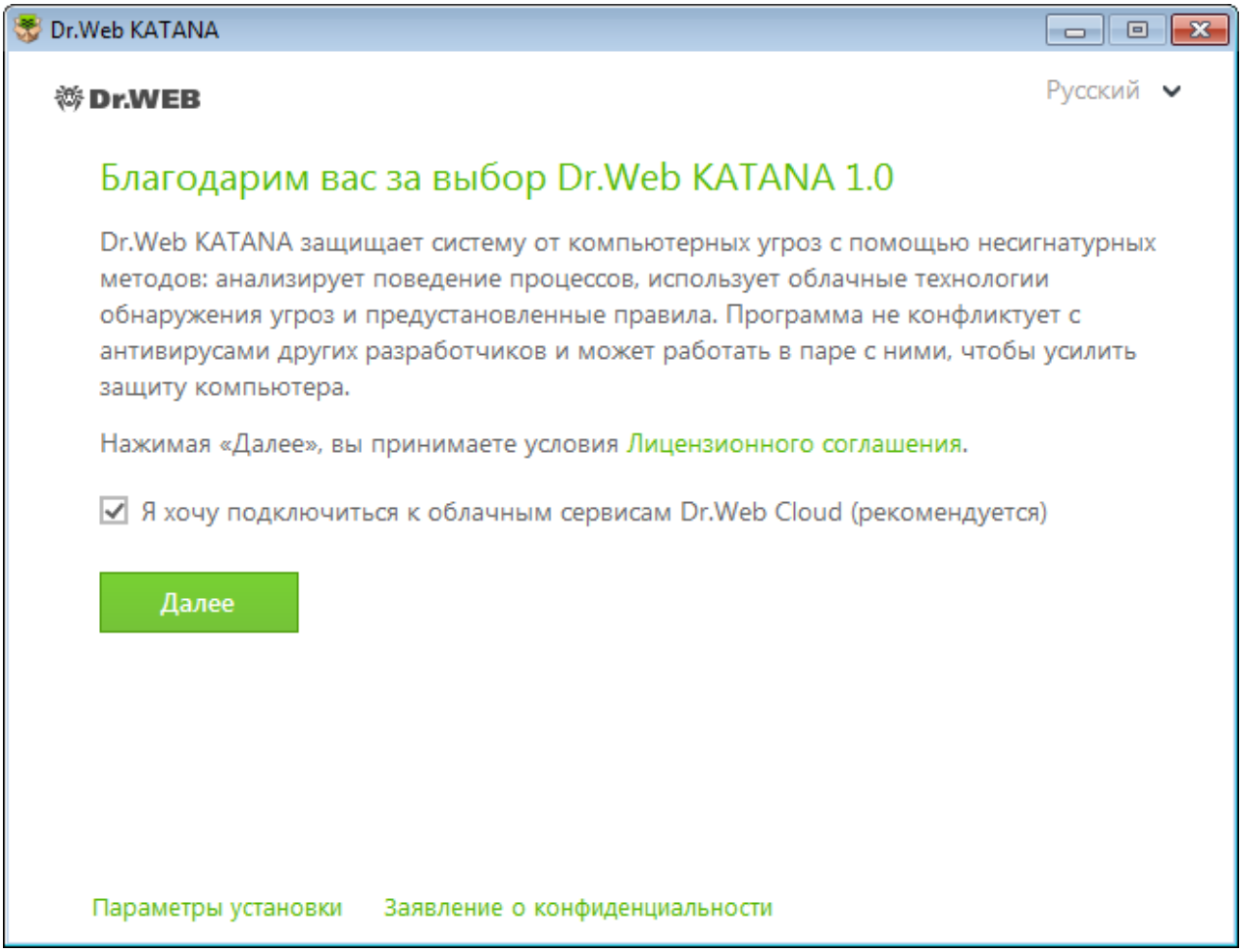

Рисунок 1. Мастер установки

3. Если вы хотите произвести установку с параметрами по умолчанию, перейдите к пункту 4. Чтобы выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры, нажмите ссылку **Параметры установки**. Данная опция предназначена для опытных пользователей.
   - На первой вкладке вы можете изменить путь установки.
   - На второй вкладке при необходимости вы можете указать параметры прокси-сервера.

   Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**.
4. Нажмите **Далее**. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.

5. В окне **Мастер регистрации** необходимо выбрать одну из следующих опций:
   - Если у вас есть ключевой файл и он находится на жестком диске или сменном носителе, выберите **Указать путь к действующему ключевому файлу**. Нажмите кнопку **Обзор** и выберите нужный ключевой файл в открывшемся окне.
   - Если у вас нет ключевого файла, но вы готовы его получить в процессе установки, выберите **Получить лицензию в процессе установки** и нажмите **Установить**.

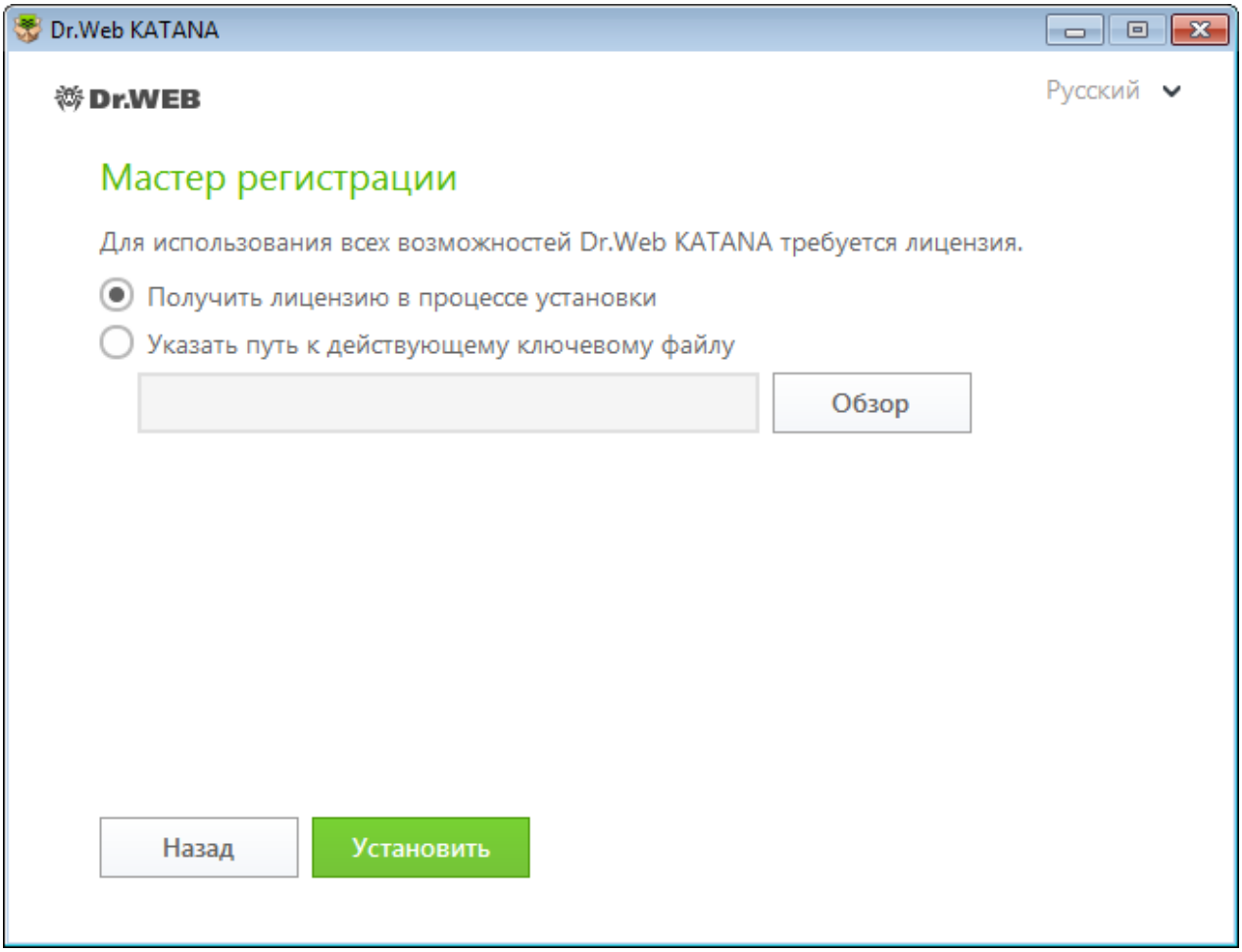

Рисунок 2. Мастер регистрации

Установка с параметрами командной строки

Чтобы запустить установку Dr.Web с параметрами командной строки, в командной строке введите имя исполняемого файла с необходимыми параметрами (параметры влияют на установку в фоновом режиме, язык установки, перезагрузку после окончания установки):

Параметр	Значение
`lang`	Язык продукта. Значение параметра — код языка в формате ISO 639-1, например, `/lang ru`.

Параметр	Значение
`reboot`	Автоматическая перезагрузка компьютера после завершения установки.
`silent`	Установка в фоновом режиме.

Например, при запуске следующей команды будет проведена установка Dr.Web в фоновом режиме:

```
drweb-1.0-katana.exe /silent yes
```

2.2. Восстановление и удаление Dr.Web KATANA

Восстановление или удаление Dr.Web KATANA штатными средствами операционной системы Windows

1. Для удаления или восстановления Dr.Web KATANA запустите утилиту удаления программ операционной системы Windows.
2. В открывшемся списке выберите строку с названием программы.
   - Для удаления программы полностью нажмите кнопку **Удалить** и перейдите к шагу 5.
   - Для восстановления Dr.Web нажмите кнопку **Изменить**. Откроется окно Мастера восстановления/удаления программы.

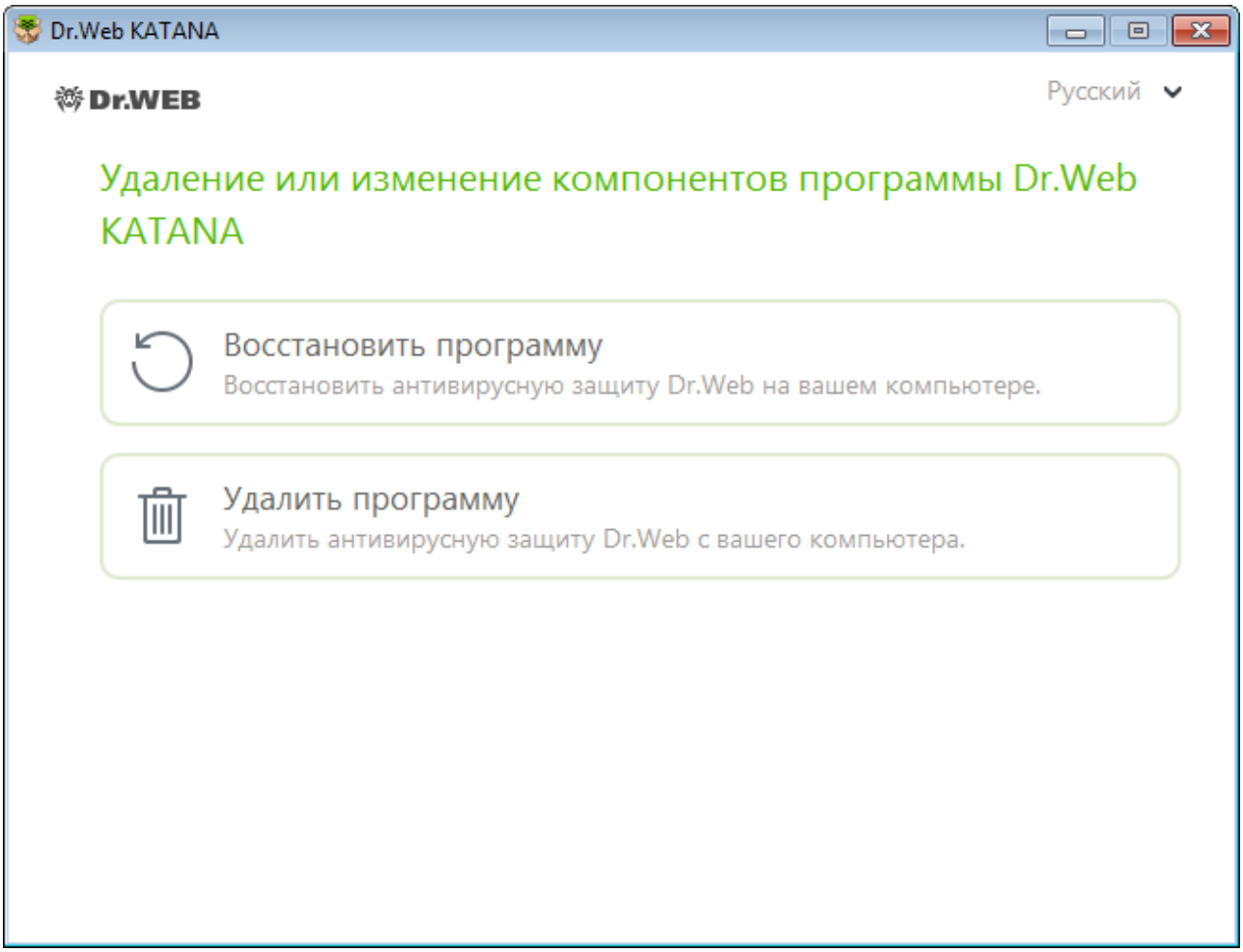

Рисунок 3. Мастер восстановления/удаления программы

3. Если необходимо восстановить антивирусную защиту на вашем компьютере, в открывшемся окне выберите пункт **Восстановить программу**. Эта функция применяется в том случае, когда некоторые из компонентов программы Dr.Web были повреждены.
4. Чтобы удалить все установленные компоненты, выберите пункт **Удалить программу**.
5. В окне **Сохраняемые параметры** установите флажки напротив того, что следует сохранить после удаления программы. Сохраненные объекты и настройки могут использоваться программой при повторной установке. Нажмите **Далее**.
6. В следующем окне для подтверждения удаления Dr.Web введите изображенный код, после чего нажмите кнопку **Удалить программу**.
7. Перезагрузите компьютер для завершения процедуры удаления.

3. Лицензирование

Для работы Dr.Web в течение продолжительного времени требуется лицензия. Приобретение лицензии возможно вместе с продуктом, а также на сайте компании «Доктор Веб» и у партнеров. Лицензия позволяет полноценно использовать все возможности продукта на протяжении всего срока действия. Лицензия регулирует права пользователя, установленные в соответствии с пользовательским договором.

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете активировать пробную версию. Она обеспечивает полную функциональность основных компонентов, но срок действия существенно ограничен.

Активация пробной версии на одном и том же компьютере возможна не чаще, чем один раз в год.

Пробная версия может быть активирована сроком на 1 месяц, при этом серийный номер не требуется, регистрационные данные не запрашиваются.

Ключевой файл

Права пользователя на использование Dr.Web хранятся в специальном файле, называемом ключевым файлом. При получении ключевого файла в процессе установки или в комплекте дистрибутива продукта установка ключевого файла производится автоматически и никаких дополнительных действий не требует.

Ключевой файл имеет расширение `.key` и содержит, в частности, следующую информацию:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование программы;
- наличие или отсутствие технической поддержки;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать программу).

При работе программы ключевой файл по умолчанию должен находиться в папке установки Dr.Web. Программа регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа, не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла активность всех компонентов Dr.Web блокируется.

Ключевой файл Dr.Web является действительным при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится недействительным.

Рекомендуется сохранять ключевой файл до истечения срока действия лицензии или пробной версии.

Ключевой файл, полученный для активации пробной версии, может использоваться только на том компьютере, на котором вы проходили регистрацию.

3.1. Способы активации

Активировать лицензию вы можете одним из следующих способов:

- с помощью Мастера регистрации в процессе установки или любой другой момент;
- получив ключевой файл во время регистрации лицензии на официальном сайте «Доктор Веб»;
- указав путь к имеющемуся у вас действительному ключевому файлу в процессе установки либо в Мастере регистрации.

Повторная активация

Повторная активация лицензии или пробной версии может потребоваться в случае утраты ключевого файла.

В случае повторной активации лицензии или пробной версии выдается тот же ключевой файл, который был выдан ранее, при условии, что срок его действия не истек.

При переустановке продукта или в случае, когда лицензия предоставляет право установки продукта на несколько компьютеров, повторная активация серийного номера не требуется. Вы можете использовать ключевой файл, полученный при первой регистрации.

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

3.2. Продление лицензии

В некоторых случаях, например при окончании срока действия лицензии, вы можете принять решение о приобретении новой лицензии на Dr.Web. В таком случае вам потребуется заменить текущий ключевой файл. Dr.Web поддерживает обновление лицензии «на лету», при котором не требуется переустанавливать Dr.Web или прерывать его работу.

Чтобы заменить ключевой файл

1. Чтобы заменить текущую лицензию, используйте Мастер регистрации.
2. Если текущий ключевой файл недействителен, Dr.Web переключится на использование нового ключевого файла.

3.3. Мастер регистрации

Модуль управления SplDer Agent после старта проверяет наличие ключевого файла. При его отсутствии модуль предлагает получить ключевой файл через интернет.

Ключевой файл может быть получен в процессе установки. Для этого на 5 шаге установки выберите пункт **Получить лицензию в процессе установки**, при этом будет запущена процедура активации лицензии или демонстрационного периода.

Вы также можете получить ключевой файл, запустив процедуру активации лицензии или демонстрационного периода после установки продукта. Для этого воспользуйтесь одной из следующих опций:

- в меню SplDer Agent  в области уведомлений Windows выберите пункт **Лицензия**;
- в окне Менеджера лицензий нажмите кнопку **Получить новую лицензию** и в выпадающем списке выберите **через сеть Интернет**.

После запуска процедуры активации откроется окно Мастера регистрации.

Для активации лицензии вам потребуется серийный номер, выданный вам при приобретении Dr.Web.

Для ознакомления с работой программы вы можете активировать пробную версию на 1 месяц, при этом серийный номер не требуется, регистрационные данные не запрашиваются.

В первом окне вам будет предложено выбрать один из следующих вариантов активации:

- активировать лицензию;
- получить демо;
- приобрести лицензию.

Если у вас имеется серийный номер для активации лицензии, выберите **Активировать лицензию**. Введите серийный номер и нажмите **Далее**. Откроется окно ввода регистрационных данных.

Если серийного номера у вас нет, но вы хотите ознакомиться с продуктом, активируйте демонстрационный период на 1 месяц, выбрав **Получить демо**. Нажмите **Далее**, при этом откроется окно с результатом активации.

Чтобы приобрести лицензию в онлайн-магазине компании «Доктор Веб», выберите **Приобрести лицензию**.

Если у вас уже есть действительный ключевой файл, выберите **Другие типы активации**. В открывшемся окне укажите путь к файлу.

Ввод регистрационных данных

Для регистрации лицензии введите персональные сведения (имя, фамилию, в раскрывающемся списке выберите страну и введите адрес электронной почты). Все перечисленные поля являются обязательными для заполнения.

Нажмите **Далее**.

Результат активации

Если активация закончилась успешно, выводится соответствующее сообщение. Нажмите кнопку **Готово**, чтобы перейти к обновлению вирусных баз и других файлов пакета. Данная процедура, как правило, не требует вмешательства пользователя.

Если активация завершилась неудачно, выводится сообщение об ошибке. Нажмите кнопку **Параметры соединения**, чтобы изменить настройки подключения к интернету, либо кнопку **Повторить** для исправления неверно введенных данных.

4. Начало работы

После установки Dr.Web в область уведомлений Windows добавляется значок модуля управления SpIDer Agent :

> Если SpIDer Agent не запущен, в меню Пуск раскройте группу Dr.Web и выберите пункт SpIDer Agent.

Значок SpIDer Agent отражает текущее состояние Dr.Web:

- — все компоненты, необходимые для защиты компьютера, запущены и работают правильно;
- — самозащита Dr.Web или защита компьютера отключены;
- — ожидается запуск компонентов после старта операционной системы, дождитесь запуска компонентов программы; либо в процессе запуска одного из ключевых компонентов Dr.Web возникла ошибка, компьютер находится под угрозой заражения. Проверьте наличие действительного ключевого файла и при необходимости установите его.

В меню SpIDer Agent сосредоточены основные средства управления и настройки Dr.Web. Для доступа к меню SpIDer Agent щелкните по значку SpIDer Agent в области уведомлений Windows.

Лицензия. Открывает Менеджер лицензий.

Обновление. Информация об актуальности компонентов. Запускает обновление.

Защита. Быстрый доступ к отключению или включению превентивной защиты. Каждое включение и отключение превентивной защиты записывается в Журнал событий операционной системы Windows, в разделе **Журналы приложений и служб → Doctor Web**.

Настройки . Открывает окно настроек.

Инструменты . Открывает доступ к следующим инструментам:

- Менеджер лицензий;
- Менеджер карантина;
- Поддержка.

Справка . Открывает эту справку.

5. Инструменты

Для того чтобы просмотреть список изолированных файлов и восстановить файлы из карантина, выберите Менеджер карантина.

Если у вас возникли вопросы или неполадки в процессе работы Dr.Web, выберите раздел Поддержка.

5.1. Менеджер лицензий

В данном окне отображается информация об имеющихся у вас лицензиях Dr.Web.

В верхней части окна приводится информация о выбранной лицензии.

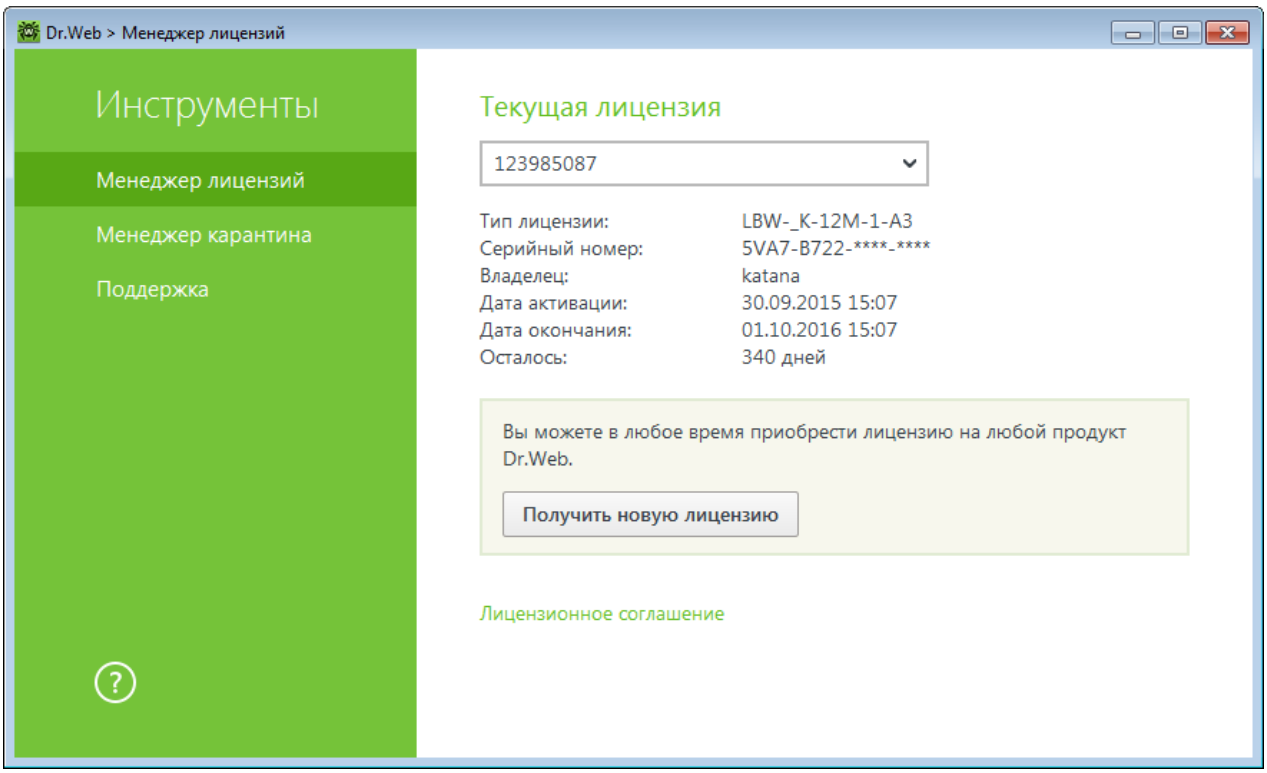

Рисунок 4. Данные о текущей лицензии

Кнопка **Получить новую лицензию** открывает Мастер регистрации, в котором вы можете активировать новую лицензию, указать путь к ключевому файлу другой лицензии или приобрести лицензию на любой продукт Dr.Web.

Кнопка позволяет удалить лицензию, выбранную в списке.

Для работы Dr.Web требуется установить в защищаемой системе ключевой файл Dr.Web. При получении ключевого файла в процессе установки или в комплекте дистрибутива продукта установка ключевого файла производится автоматически и никаких дополнительных действий не требует.

При работе программы ключевой файл по умолчанию должен находиться в папке установки Dr.Web. Программа регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа, не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла активность всех компонентов Dr.Web блокируется.

5.2. Менеджер карантина

Менеджер карантина — инструмент, позволяющий управлять изолированными файлами. В карантине содержатся резервные копии объектов, созданные перед их удалением Dr.Web. В карантин помещаются вредоносные программы, которые определены Dr.Web Process Heuristic как программы, изменяющие нежелательным образом пользовательские файлы (например, троянские программы-шифровальщики), и программы, внедряющиеся в процессы других приложений.

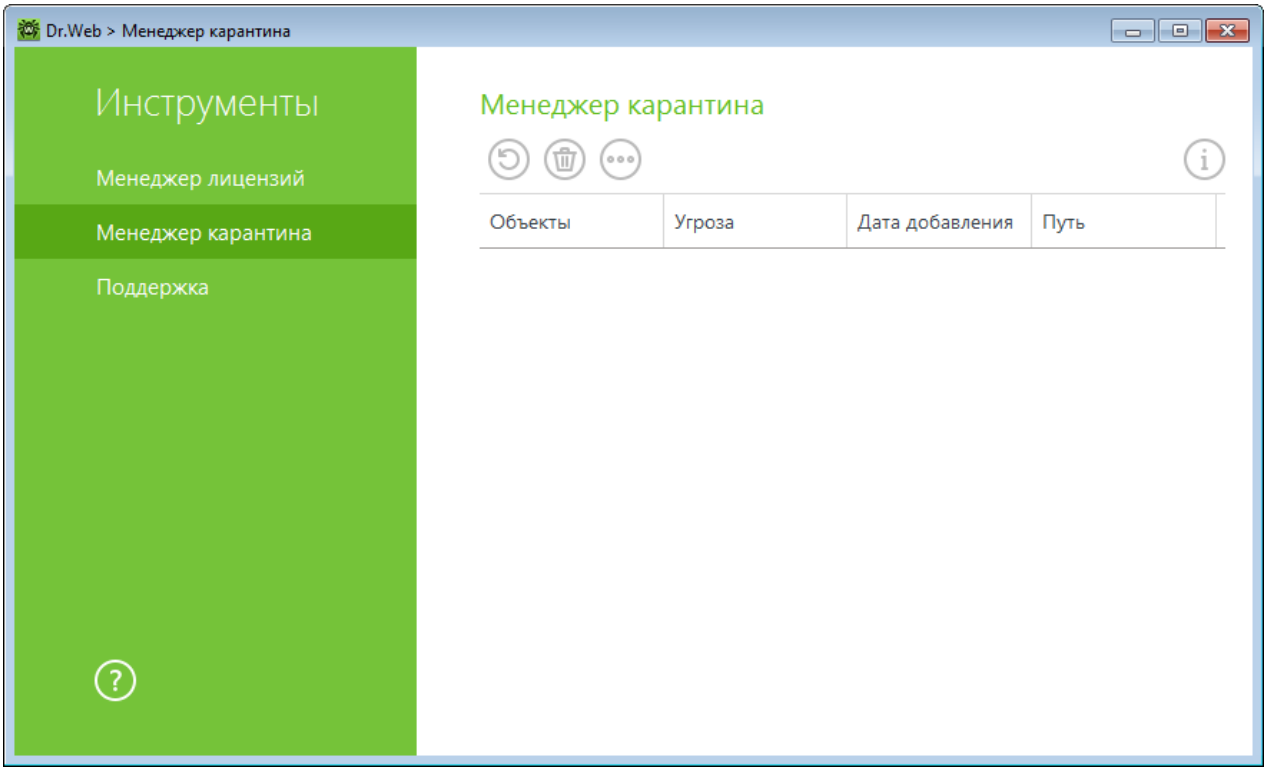

Рисунок 5. Объекты в карантине

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

- **Объекты** — 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.

Работа с объектами в карантине

Для каждого объекта доступны следующие кнопки управления:

- **Восстановить** — переместить один или несколько выбранных объектов под заданным именем в нужную папку;

  

  Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

- **Удалить** — удалить один или несколько выбранных объектов из карантина и из системы.

Эти действия доступны также в контекстом меню при нажатии правой кнопкой мыши на один или несколько выбранных объектов.

Для того чтобы удалить сразу все объекты из карантина, нажмите кнопку  и в выпадающем списке выберите пункт **Удалить все**.

5.3. Поддержка

Этот раздел содержит информацию о версии продукта, составе компонентов и дате последнего обновления, а также полезные ссылки, которые могут помочь вам ответить на вопросы или исправить неполадки, возникшие в процессе работы Dr.Web.

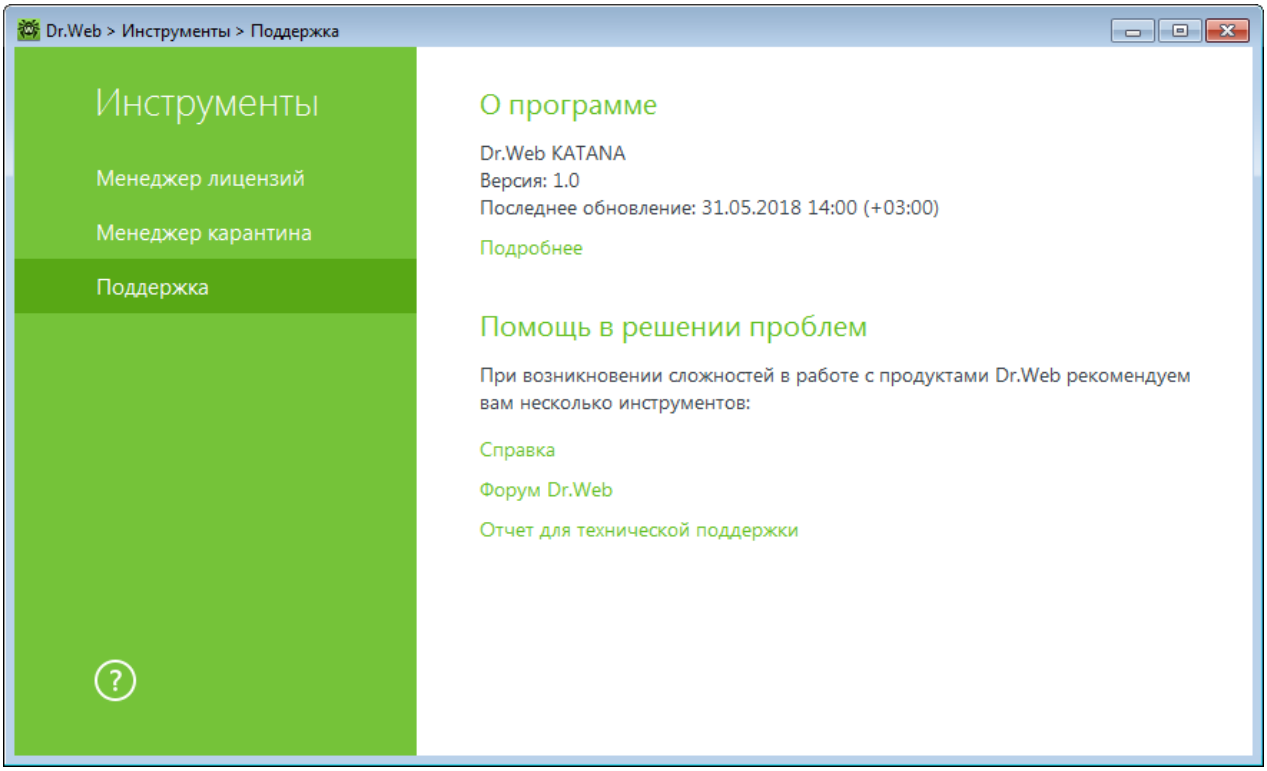

Рисунок 6. Сведения о версии продукта и поддержка

Воспользуйтесь одним из следующих инструментов в том случае, если у вас возникли вопросы:

Справка. Открывает справку.

Форум Dr.Web. Открывает форум Dr.Web по адресу https://forum.drweb.com/.

Отчет для технической поддержки. Запускает мастер, который позволит вам создать отчет, содержащий важную информацию о системе и работе компьютера.

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

Найти ближайшее к вам представительство «Доктор Веб» и всю контактную информацию, необходимую пользователю, вы можете на сайте компании https://company.drweb.com/contacts/moscow/.

5.3.1. Создание отчета

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

Отчет будет сохранен в виде архива в папке Doctor Web, расположенном в папке профиля пользователя %USERPROFILE%.

Чтобы сформировать отчет, нажмите соответствующую кнопку. В отчет будет включаться:

1. Техническая информация об операционной системе:
   - общие сведения о компьютере,
   - информация о запущенных процессах,
   - информация о запланированных заданиях,
   - информация о службах, драйверах,
   - информация о браузере по умолчанию,
   - информация об установленных приложениях,
   - информация о политиках ограничений,
   - информация о файле HOSTS,
   - информация о серверах DNS,
   - записи системного журнала событий,
   - перечень системных каталогов,
   - ветви реестра,
   - провайдеры Winsock,
   - сетевые соединения,
   - отчеты отладчика Dr.Watson,
   - индекс производительности.
2. Информация об установленном продукте Dr.Web:
   - тип и версия установленного продукта Dr.Web;
   - информация о составе установленных компонентов; сведения о модулях Dr.Web;
   - настройки и параметры конфигурации продукта Dr.Web;
   - информация о лицензии;
   - журналы работы Dr.Web.

Информация о работе антивирусных продуктов Dr.Web находится в Журнале событий операционной системы Windows, в разделе **Журналы приложений и служб** → **Doctor Web**.

6. Обновление

Для поддержания актуальности программных алгоритмов компанией «Доктор Веб» реализована система распространения обновлений через интернет.

Запуск обновления

При обновлении Dr.Web загрузит все обновленные файлы, соответствующие вашей версии Dr.Web, а также новую версию Dr.Web в случае ее выхода.

Для обновления Dr.Web необходимо иметь доступ к интернету.

Настройка необходимых параметров производится в разделе **Обновление** основных настроек Dr.Web.

Запуск обновления с помощью модуля управления SpIDer Agent

В меню SpIDer Agent  выберите пункт **Обновление**. Откроется информация о необходимости обновления, а также дата последнего обновления. Чтобы запустить процесс обновления, нажмите кнопку **Обновить**.

Запуск обновления из командной строки

Перейдите в папку установки Dr.Web и запустите `drwupsrv.exe`. Список параметров вы можете найти в Приложении А.

Автоматический запуск обновления

При автоматическом запуске обновление проводится в фоновом режиме, при этом отчеты записываются в файл `dwupdater.log` в папке `%allusersprofile%\Doctor Web\Logs\`.

При обновлении исполняемых файлов, драйверов и библиотек может потребоваться перезагрузка компьютера. В этом случае будет показано соответствующее предупреждение.

7. Настройки

Для доступа к настройкам откройте меню SpIDer Agent и запустите **Настройки**.

7.1. Основные

В этом разделе вы можете задать язык программы, а также импортировать и экспортировать настройки Dr.Web.

Язык

Вы можете выбрать из выпадающего списка язык программы. Список языков пополняется автоматически и содержит все доступные на текущий момент локализации графического интерфейса Dr.Web.

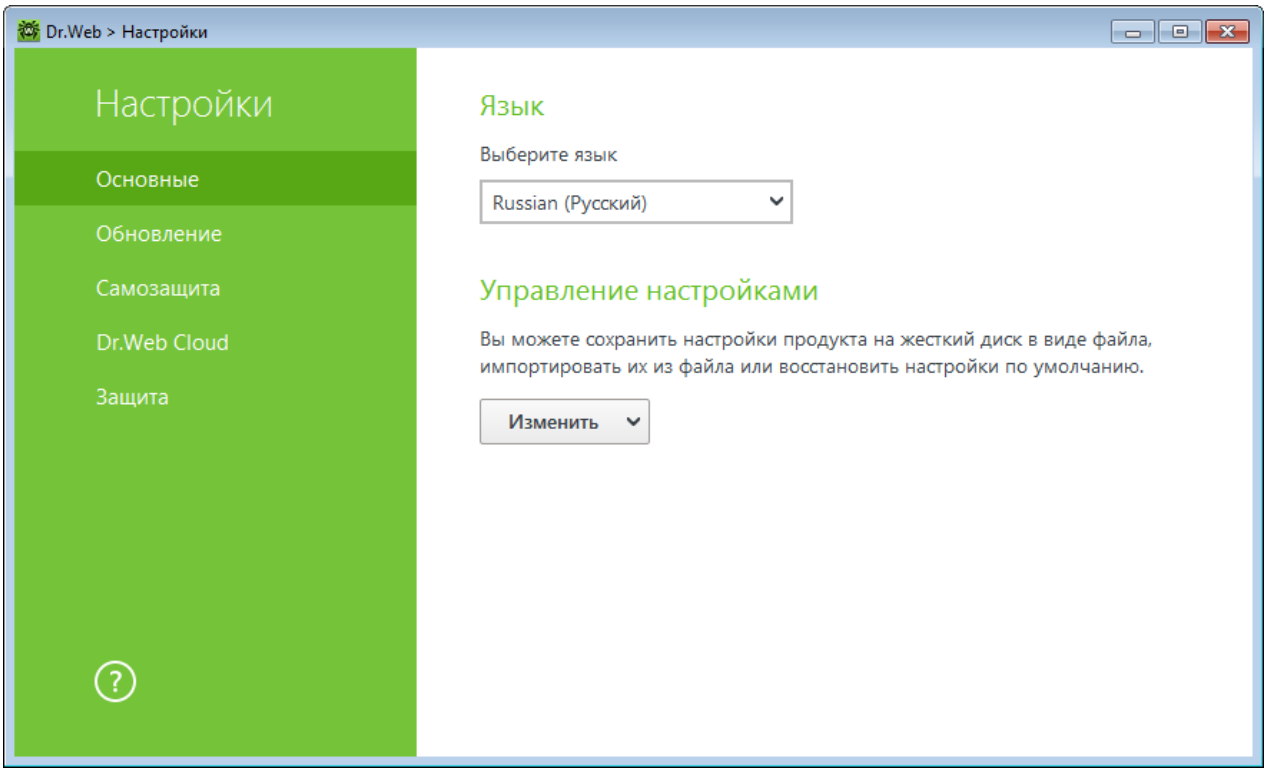

Рисунок 7. Основные настройки

Управление настройками

Чтобы восстановить настройки по умолчанию, в выпадающем списке выберите пункт **Сбросить настройки**.

Если вы уже настроили работу программы на другом компьютере и хотите использовать те же настройки, в выпадающем списке выберите пункт **Импорт**.

Если вы хотите использовать свои настройки на других компьютерах, в выпадающем списке выберите пункт **Экспорт**, а затем воспользуйтесь аналогичной вкладкой на другом компьютере.

7.2. Обновление

Основные настройки обновления

Периодичность обновлений. Задайте необходимую периодичность, с которой будет производиться проверка на наличие обновлений. По умолчанию установлено оптимальное значение (30 минут), которое позволяет поддерживать информацию об угрозах в актуальном состоянии.

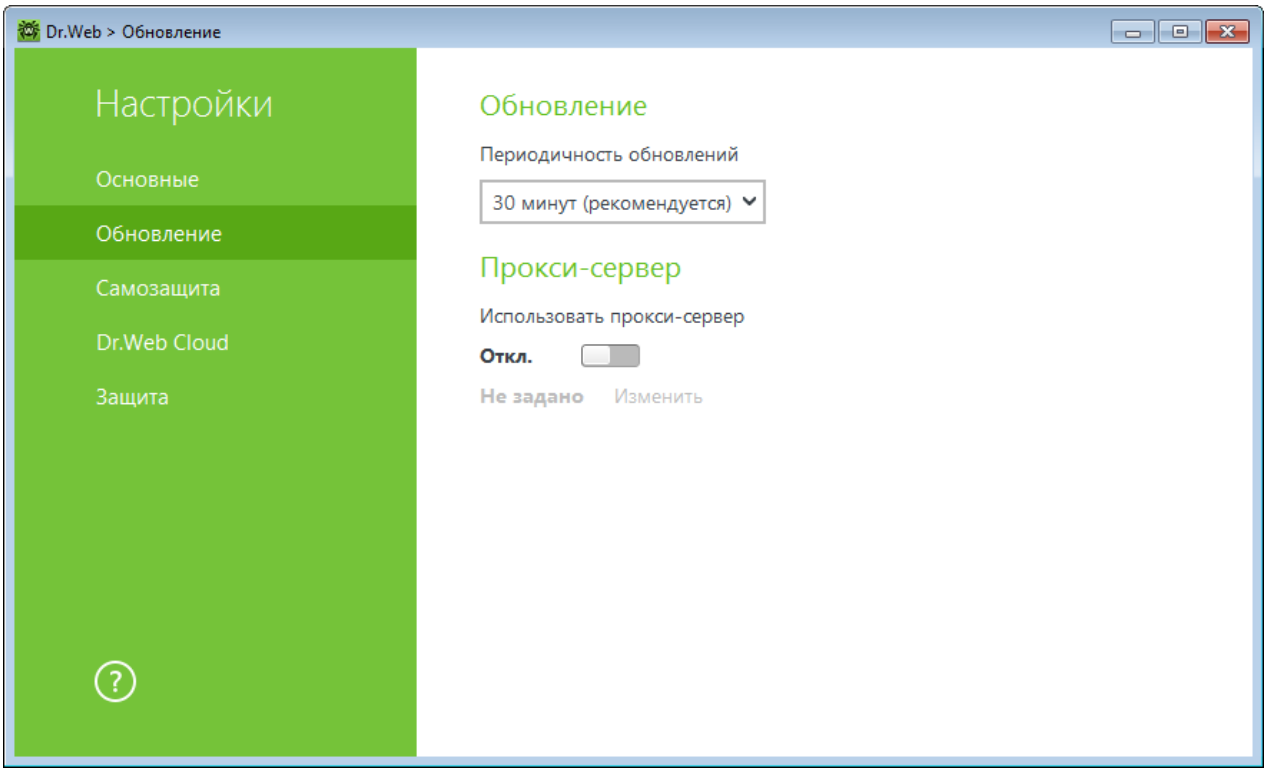

Рисунок 8. Настройки обновления

Использование прокси-сервера

При необходимости вы можете включить использование прокси-сервера и задать настройки подключения к нему. Нажмите **Изменить**, чтобы задать настройки подключения к прокси-серверу:

Настройка	Описание
Адрес	Укажите адрес прокси-сервера.

Настройка	Описание
Порт	Укажите порт прокси-сервера.
Пользователь	Укажите имя учетной записи для подключения к прокси-серверу.
Пароль	Укажите пароль учетной записи, используемой для подключения к прокси-серверу.
Тип авторизации	Выберите тип авторизации, требуемый для подключения к прокси-серверу.

7.3. Самозащита

Настройки самозащиты

В данном разделе вы можете настроить параметры защиты самого Dr.Web от несанкционированного воздействия, например анти-антивирусных программ, а также от случайного повреждения. Настройка **Включить Самозащиту** позволяет защитить файлы и процессы Dr.Web от несанкционированного доступа. Отключать Самозащиту не рекомендуется.

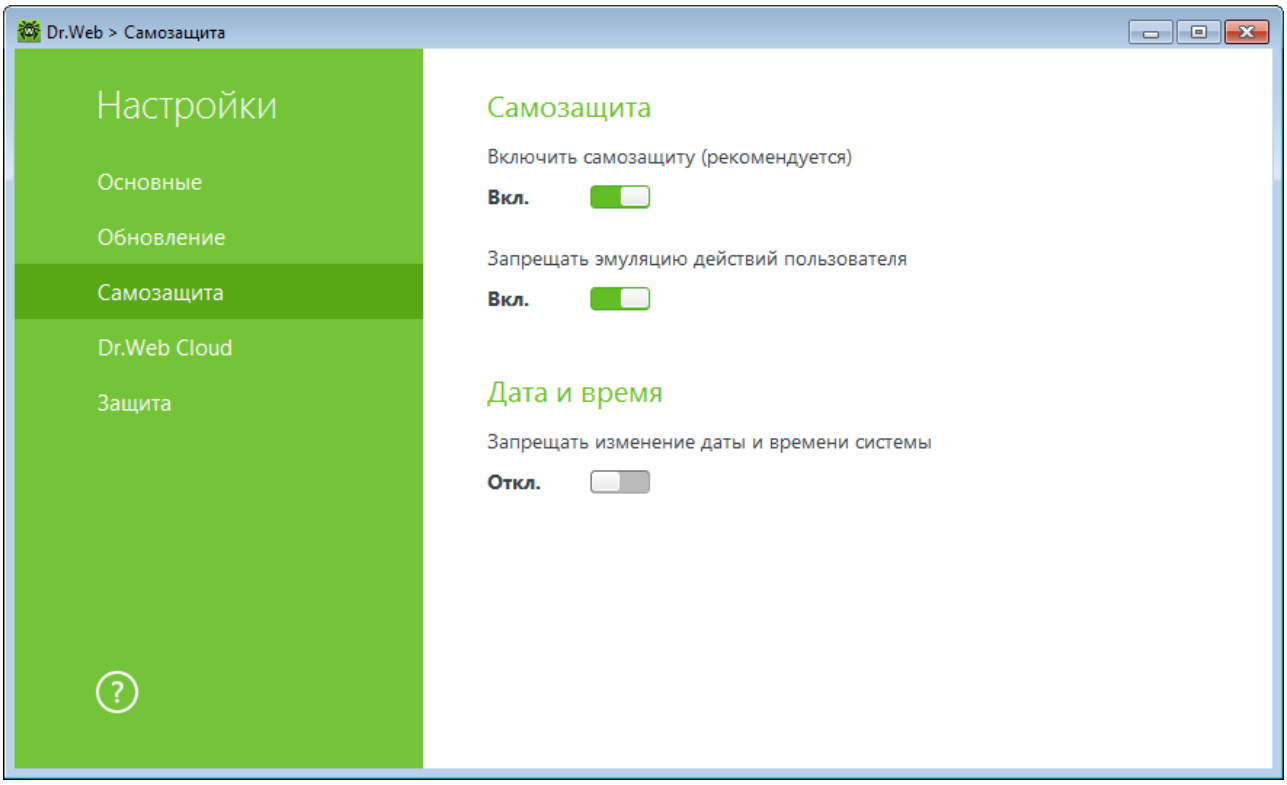

Рисунок 9. Настройки Самозащиты Dr.Web

В случае возникновения проблем при использовании программ дефрагментации, рекомендуется временно отключить модуль Самозащиты.

Для того чтобы произвести возврат к точке восстановления системы, необходимо отключить модуль Самозащиты.

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.

Дата и время

Настройка **Запрещать изменение даты и времени системы** позволяет заблокировать ручное и автоматическое изменение системных даты и времени, а также часового пояса. Это ограничение устанавливается для всех пользователей системы.

7.4. Dr.Web Cloud

В данном разделе вы можете подключиться к облачному сервису компании «Доктор Веб» и программе улучшения качества работы продуктов Dr.Web.

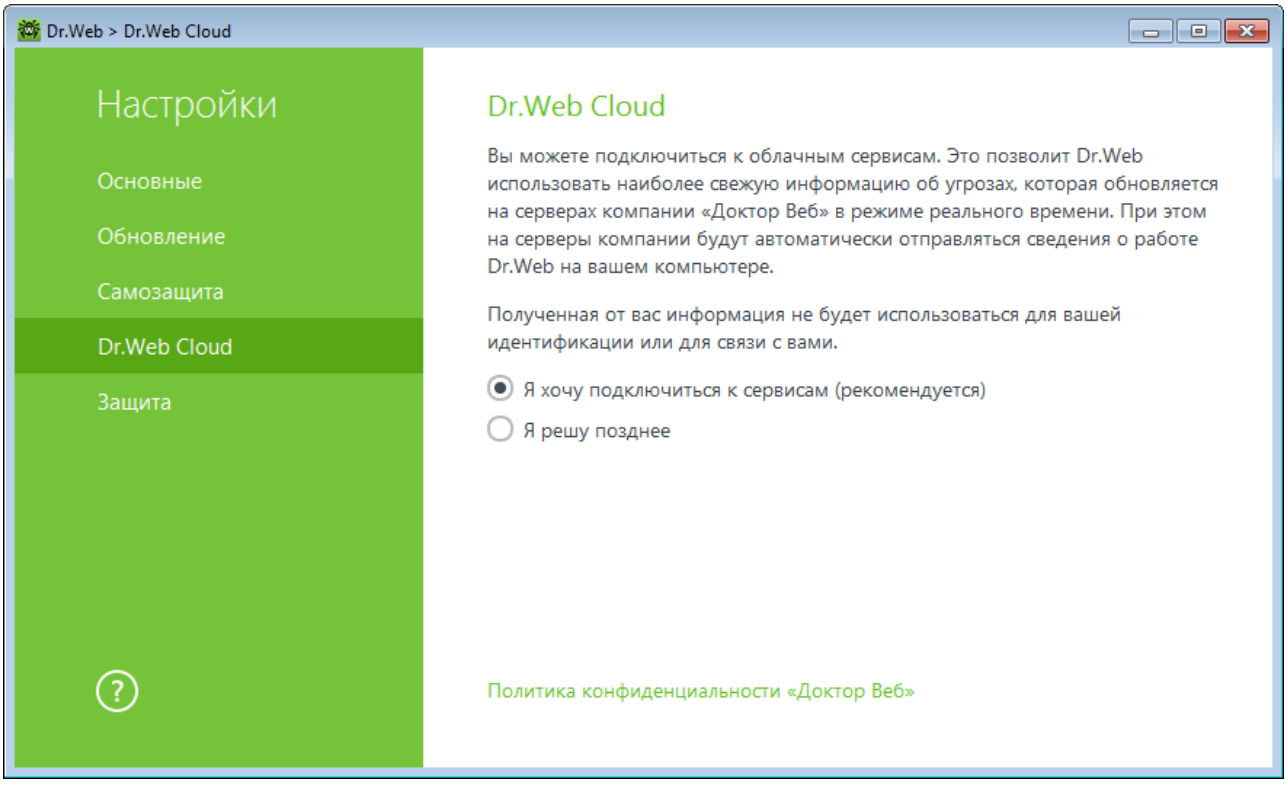

Рисунок 10. Подключение к Dr.Web Cloud

Облачный сервис

Dr.Web Cloud позволяет антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени.

Программа улучшения качества ПО

При участии в программе на сервера компании «Доктор Веб» будут автоматически отправляться обезличенные сведения о работе Dr.Web на вашем компьютере. Полученная информация не будет использоваться для идентификации пользователя или связи с ним.

Нажмите на ссылку **Политика конфиденциальности «Доктор Веб»**, чтобы ознакомиться с политикой конфиденциальности на официальном сайте компании «Доктор Веб».

7.5. Защита

В данном разделе вы можете настроить реакцию Dr.Web на действия сторонних приложений, которые могут привести к заражению вашего компьютера и выбрать уровень защиты от эксплойтов.

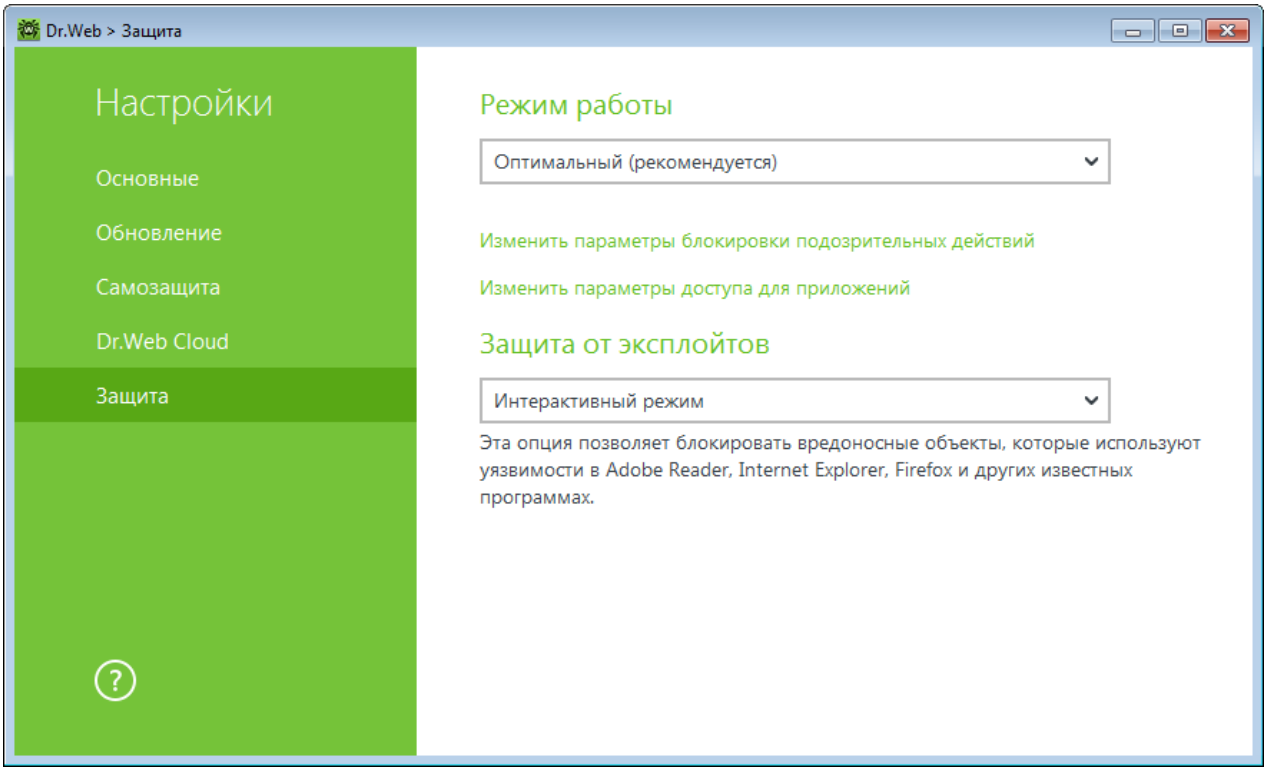

Рисунок 11. Выбор режима работы Защиты

При этом вы можете задать отдельный режим защиты для конкретных приложений и общий режим, настройки которого будут применяться ко всем остальным процессам.

Для задания общего режима превентивной защиты, выберите его в списке **Режим работы** или нажмите на опцию **Изменить параметры блокировки подозрительных действий**. В последнем случае откроется окно, где вы сможете подробнее ознакомиться с настройками для каждого из режимов или изменить их. Все изменения в настройках сохраняются в **Пользовательском** режиме работы. В этом окне вы также можете создать новый профиль для сохранения нужных настроек.

Чтобы создать новый профиль

1. Нажмите кнопку  .
2. В открывшемся окне укажите название для нового профиля.
3. Просмотрите настройки защиты, заданные по умолчанию, и при необходимости отредактируйте их.

Для задания настроек превентивной защиты для конкретных приложений нажмите на опцию **Изменить параметры доступа для приложений**. В открывшемся окне вы можете добавить новое правило для приложения, отредактировать уже созданное правило или удалить ненужное.

Чтобы добавить правило

1. Нажмите кнопку  .
2. В открывшемся окне нажмите кнопку **Обзор** и укажите путь к исполняемому файлу приложения.
3. Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.

Чтобы отредактировать уже созданное правило, выберите его из списка и нажмите кнопку  .

Чтобы удалить уже созданное правило, выберите его из списка и нажмите кнопку  .

Уровень превентивной защиты

В режиме работы **Оптимальный**, установленном по умолчанию, Dr.Web запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещается низкоуровневый доступ к диску и модификация файла HOSTS.

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

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

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

В режиме работы **Пользовательский** вы можете выбрать уровни защиты для каждого объекта по своему усмотрению.

Защищаемый объект	**Описание**
Целостность запущенных приложений	Данная настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера.
Целостность файлов пользователей	Данная настройка позволяет отслеживать процессы, которые модифицируют пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера.
HOSTS файл	Файл HOSTS используется операционной системой для упрощения доступа к интернету. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
Низкоуровневый доступ к диску	Данная настройка позволяет запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
Загрузка драйверов	Данная настройка позволяет запрещать приложениям загрузку новых или неизвестных драйверов.
Критические области Windows	Прочие настройки позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей). Доступ к Image File Execution Options: • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Доступ к User Drivers: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Параметры оболочки Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Нотификаторы Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

Защищаемый объект	Описание
	Автозапуск оболочки Windows: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Ассоциации исполняемых файлов: • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи) Политики ограничения запуска программ (SRP): • Software\Policies\Microsoft\Windows\Safer Плагины Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Автозапуск программ: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Автозапуск политик: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Конфигурация безопасного режима: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Параметры Session Manager: • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows Системные службы: • System\CurrentControlXXX\Services

Если при установке важных обновлений от Microsoft или при установке и работе программ (в том числе программ дефрагментации) возникают проблемы, временно отключите превентивную защиту.

Защита от эксплойтов

Эта опция позволяет блокировать вредоносные объекты, которые используют уязвимости в популярных приложениях. В соответствующем выпадающем списке выберите подходящий уровень защиты от эксплойтов.

Уровень защиты	Описание
Блокировать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически заблокирована.
Интерактивный режим	При попытке вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы Dr.Web выведет соответствующее сообщение. Ознакомьтесь с информацией и выберите нужное действие.
Разрешать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически разрешена.

8. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/index.php.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.

9. Приложение А. Параметры командной строки для Модуля обновления

Общие параметры:

Параметр	Описание
-h [--help]	Вывести на экран краткую справку о работе с программой.
-v [--verbosity] arg	Уровень детализации журнала: `error` (стандартный), `info` (расширенный), `debug` (отладочный).
-d [--data-dir] arg	Папка, в которой размещены репозиторий и настройки.
--log-dir arg	Папка, в которой будет сохранен журнал.
--log-file arg (=dwupdater.log)	Имя файла журнала.
-r [--repo-dir] arg	Папка репозитория, (по умолчанию <*data_dir*>`/repo`).
-t [--trace]	Включить трассировку.
-c [--command] arg (=update)	Выполняемая команда: `getversions` — получить версии, `getcomponents` — получить компоненты, `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 обновления (update):

Параметр	Описание
-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.

Параметр	Описание
--geo-update	Получить список IP-адресов `update.drweb.com` перед обновлением.
--type arg (=normal)	Может быть одним из следующих: • `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):

Параметр	Описание
-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):

Параметр	Описание
-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):

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

Параметры команды удаления (uninstall):

Параметр	Описание
-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):

Параметр	Описание
-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):

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Папка, в которой находится ключевой файл.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.

Параметр	Описание
-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	Номер версии.
-p [--product] arg	Название продукта, который необходимо скачать.