Dr.WEB

KATANA Business Edition

Руководство администратора

Dr.Web KATANA Business Edition
Версия 1.0
Руководство администратора
26.11.2021

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. Введение

Эта документация представляет собой руководство администратора Dr.Web KATANA Business Edition и содержит необходимые сведения по установке и эффективному использованию программы Dr.Web KATANA Business Edition. Порядок глав соответствует порядку работы с программой. Первые главы описывают установку Dr.Web KATANA Business Edition, начало работы, поиск станций, установку Dr.Web KATANA на станции; последние главы — управление настройками по защите станций и настройками самой программы Dr.Web KATANA Business Edition.

Это руководство не описывает антивирусное решение Dr.Web KATANA. За соответствующими сведениями обратитесь к руководству **Dr.Web KATANA. Руководство пользователя** или посетите официальный сайт компании «Доктор Веб».

1.1. Используемые 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. Основные функции Dr.Web KATANA Business Edition

С помощью Dr.Web KATANA Business Edition вы можете централизованно устанавливать Dr.Web KATANA на станции сети. Dr.Web KATANA защищает станции от компьютерных угроз с помощью несигнатурных методов: анализирует поведение процессов, использует облачные технологии поиска угроз и предустановленные правила.

Используя Dr.Web KATANA Business Edition, вы сможете контролировать уровень безопасности станций и их состояние.

Основные функции Dr.Web KATANA Business Edition:

- централизованная установка Dr.Web KATANA на защищаемые станции сети;
- централизованная настройка Dr.Web KATANA;
- мониторинг вирусных событий, а также состояния Dr.Web KATANA на защищаемых станциях.

1.3. Системные требования

Для работы Dr.Web KATANA Business Edition (консоли управления) компьютер должен соответствовать следующим требованиям:

Параметр	Требование
Процессор	С поддержкой системы команд i686 и набором инструкций SSE2.
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 SP3 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 с пакетом обновлений SP2 или более поздними.

Параметр	Требование
	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 KATANA Business Edition 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 установки Dr.Web KATANA станции (непосредственно защищаемые клиенты) должны соответствовать 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 KATANA 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

Назначение	Направление	Номера портов
Для соединения с облачным сервисом Dr.Web Cloud	исходящие	2075 (в том числе для UDP)

2. Лицензирование

Для использования Dr.Web KATANA Business Edition требуется лицензия. Ее можно приобрести вместе с продуктом, на официальном сайте компании «Доктор Веб» или у партнеров.

Активация лицензии

Для использования Dr.Web KATANA Business Edition необходимо активировать лицензию. Для этого зарегистрируйте лицензию на официальном сайте компании «Доктор Веб» и получите ключевой файл. Рекомендуется активировать лицензию до начала процесса установки Dr.Web KATANA Business Edition. В этом случае вы сможете указать ключевой файл в процессе установки и по ее окончании сразу же приступить к работе с программой. В противном случае использование Dr.Web KATANA Business Edition будет невозможно, пока вы не укажете действительный ключевой файл.

Стоимость лицензии

Стоимость лицензии на использование Dr.Web KATANA Business Edition зависит от количества станций в сети, на которые необходимо установить Dr.Web KATANA. Компьютер администратора сети учитывается в том случае, если на него устанавливается не только Dr.Web KATANA Business Edition, но и Dr.Web KATANA. Установка Dr.Web KATANA на компьютер администратора происходит при помощи Dr.Web KATANA Business Edition в разделе **Установка**.

Покупка новой лицензии

Если во время работы с Dr.Web KATANA Business Edition вам понадобится установить Dr.Web KATANA на большее количество станций, вы сможете купить новую лицензию на официальном сайте компании «Доктор Веб» или у партнеров. Используя новую лицензию, вы сможете установить Dr.Web KATANA на новые станции и продолжить управление теми станциями, на которые Dr.Web KATANA уже был установлен. Предыдущая лицензия при этом будет заблокирована.

Установка Dr.Web KATANA возможна только на то количество станций, которое указано в действующей лицензии.

2.1. Повторная активация лицензии

Повторная активация лицензии может потребоваться в случае утраты ключевого файла.

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

При переустановке продукта 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 программы). Ключевой файл будет выслан вам службой технической поддержки по электронной почте.

2.2. Ключевой файл

Права пользователя на использование Dr.Web хранятся в специальном файле, называемом *ключевым файлом*. Ключевой файл имеет расширение `.key` и содержит следующую информацию:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использовать программу;
- 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, не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла Dr.Web KATANA Business Edition не будет работать.

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.

3. Установка, восстановление и удаление Dr.Web KATANA Business Edition

Перед установкой Dr.Web KATANA Business Edition настоятельно рекомендуется ознакомиться с системными требованиями, а также:

- установить все критические обновления, выпущенные компанией Microsoft для вашей операционной системы (подробнее об обновлении ОС Windows и ОС Windows Server); если поддержка операционной системы производителем прекращена, рекомендуется перейти на более современную версию операционной системы;
- проверить файловую систему и устранить обнаруженные дефекты;
- закрыть активные приложения.

3.1. Установка Dr.Web KATANA Business Edition

Чтобы установить Dr.Web KATANA Business Edition

1. Запустите установочный файл, который вы получили при покупке лицензии.
2. Ознакомьтесь с лицензионным соглашением. Для этого нажмите соответствующую ссылку в первом окне.
3. Для того чтобы самостоятельно указать путь установки и некоторые дополнительные параметры, нажмите **Параметры установки**. Если вы хотите произвести установку с параметрами по умолчанию, перейдите к пункту 4.
   - На первой вкладке вы можете выбрать путь установки.
   - На вкладке **Дополнительные опции** вы можете настроить создание ярлыков для запуска программы.

   Чтобы сохранить изменения, нажмите **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите **Отменить**.
4. Нажмите кнопку **Далее**. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.
5. В открывшемся окне **Лицензия**:
   - выберите **Указать путь к действительному ключевому файлу**, если у вас есть ключевой файл и он находится на жестком диске или съемном носителе. Нажмите кнопку **Обзор** и выберите ключевой файл в окне открытия файла;
   - выберите **Получить лицензию позднее** для продолжения установки без ключевого файла. В этом случае использование программы будет невозможно, пока вы не укажете действительный ключевой файл.

   Нажмите кнопку **Установить**, чтобы запустить процесс установки.
6. После завершения установки включите опцию **Запустить Dr.Web KATANA Business Edition**, чтобы запустить KATANA Business Edition.

Действия после установки Dr.Web KATANA Business Edition

Если на компьютере администратора сети установлен сторонний брандмауэр:

- добавьте файл `dwservice.exe` в исключения брандмауэра. Номер используемого UDP-порта должен быть 55567, номер TCP-порта — произвольный.

Если на компьютерах сети установлен сторонний брандмауэр:

- добавьте файл `katana-console.exe` в исключения брандмауэра на каждом компьютере с установленной Dr.Web KATANA. Номера используемых UDP- и TCP-порта — произвольные.

Установка Dr.Web KATANA на компьютер администратора сети

Помимо Dr.Web KATANA Business Edition вы также можете установить Dr.Web KATANA на ваш компьютер. Для этого после запуска Dr.Web KATANA Business Edition перейдите в раздел **Установка** и продолжите установку Dr.Web KATANA на ваш компьютер вместе с установкой Dr.Web KATANA на другие станции.

Подробную информацию об установке Dr.Web KATANA на станции вы можете узнать в главе Установка Dr.Web KATANA на станции.

3.2. Восстановление и удаление Dr.Web KATANA Business Edition

1. Для удаления или восстановления Dr.Web KATANA Business Edition выберите (в зависимости от операционной системы):
   - для Windows XP (в зависимости от вида меню «Пуск»):
     - Меню «Пуск»: Пуск → Панель управления → Установка и удаление программ.
     - Классическое меню «Пуск»: Пуск → Настройка → Панель управления → Установка и удаление программ.
   - для Windows Vista (в зависимости от вида меню «Пуск»):
     - Меню «Пуск»: Пуск → Панель управления, далее в зависимости от вида Панели управления:
     - Классический вид: Программы и компоненты.
     - Домашняя страница: Программы → Программы и компоненты.
     - Классическое меню «Пуск»: Пуск → Настройка → Панель управления → Программы и компоненты.
   - для Windows 7 выберите Пуск → Панель управления, далее в зависимости от вида Панели управления:
     - Мелкие/крупные значки: Программы и компоненты.
     - Категория: Программы → Удаление программ.

- для Windows 8, Windows 8.1 и Windows 10 откройте Панель управления любым удобным способом, например через пункт Панель управления в контекстном меню, вызываемом правым щелчком мыши по левому нижнему углу экрана. Далее в зависимости от типа настройки Просмотр для Панели управления:
  - Мелкие/крупные значки: Программы и компоненты.
  - Категория: Программы → Удаление программ.

2. В открывшемся списке выберите строку с названием программы. Далее для восстановления или удаления программы нажмите необходимую кнопку.
3. В окне **Сохраняемые параметры** вам будет предложено сохранить настройки профилей, которые могут использоваться программой при повторной установке. Эта опция выбрана по умолчанию.

4. Начало работы

Если во время установки Dr.Web KATANA Business Edition вы указали действительный ключевой файл, после запуска программы вы сможете сразу же приступить к работе. Если ключевой файл не был указан, при запуске программы укажите действительный ключевой файл для продолжения работы с Dr.Web KATANA Business Edition.

Чтобы приступить к управлению станциями

1. Создайте профиль.
2. Подготовьте станции к установке Dr.Web KATANA.
3. Добавьте станции.
4. Установите Dr.Web KATANA на станции.

По мере завершения установки Dr.Web KATANA станции появляются в списке раздела **Управление**. Перейдя в этот раздел программы, вы можете начать управление станциями из списка, даже если установка Dr.Web KATANA завершена не на всех станциях. Остальные станции появятся в разделе **Управление** автоматически по завершении установки на них Dr.Web KATANA.

5. Работа с профилями

Работа с Dr.Web KATANA Business Edition возможна только при наличии профиля, в котором хранятся ключи, учетные данные для доступа к сети и настройки Dr.Web KATANA Business Edition. При последующих запусках программы вы сможете войти в уже существующий профиль или создать новый.

Чтобы создать новый профиль при запуске программы

1. Нажмите кнопку **Начать работу** в окне приветствия.
2. В открывшемся окне задайте имя профиля и пароль.
3. Создайте для своего профиля ключи шифрования. Вы можете сгенерировать ключи автоматически или загрузить уже существующий закрытый ключ. В последнем случае открытый ключ будет сгенерирован автоматически.
4. После создания нового профиля откроется раздел **Установка**, в котором вы можете найти станции и установить на них Dr.Web KATANA.

Создание ключей шифрования для каждого профиля является обязательным. В профиле может быть сохранена только одна пара ключей. Впоследствии вы сможете создать новые ключи шифрования и распространить их на станции, если это будет необходимо.

Чтобы войти в существующий профиль

1. Выберите имя необходимого профиля в списке **Имя пользователя**.
2. Введите пароль. Чтобы просмотреть пароль, нажмите .
3. Нажмите кнопку **Войти**.

Чтобы создать новый профиль из главного окна программы

Если вам нужно создать профиль во время работы в программе

1. Нажмите рядом с пунктом меню **Профили**.
2. В открывшемся окне задайте имя профиля и пароль.
3. Создайте для своего профиля ключи шифрования, сгенерировав их при помощи Dr.Web KATANA Business Edition или загрузив уже существующий закрытый ключ. В последнем случае открытый ключ будет сгенерирован автоматически.

   Опция **Импортировать текущие настройки в новый профиль** позволяет импортировать настройки и ключи шифрования из профиля, из-под которого в настоящий момент осуществляется работа. В новый профиль импортируются все настройки, включая те, которые вы еще не сохранили. Опция включена по умолчанию.

Во время работы вы можете переключать существующие профили в боковом меню.

Вы также можете удалять профили. Для этого наведите курсор на имя профиля в боковом меню и нажмите . При удалении профиля, из-под которого осуществляется работа со станциями, вы можете войти в один из существующих профилей или создать новый.

6. Подготовка станций

Для установки Dr.Web KATANA на станции требуется одновременное выполнение следующих условий:

- опция **Сетевое обнаружение** должна быть включена на компьютере, на котором запущен Dr.Web KATANA Business Edition, если вы планируете искать станции в сети этим методом;
- станция должна быть доступна по сети;
- используемая для подключения учетная запись должна существовать и обладать необходимыми правами;
- если для защиты удаленного компьютера используется брандмауэр, необходимо провести дополнительные настройки.

  При использовании брандмауэра Windows в его настройках перейдите на вкладку **Дополнительные параметры**, выберите **Правила для входящих подключений** и включите следующие исключения: **Служба входа в сеть (NP-In)** и **Общий доступ к файлам и принтерам (SMB-In)**. Исключения должны быть включены для профиля брандмауэра **Private**. Если станция находится в домене, исключения должны быть включены для профиля **Domain**.

  При использовании других брандмауэров необходимо открыть 445 порт;
- должна быть выполнена дополнительная настройка (см. ниже).

Перед началом установки убедитесь, что у вас имеется информация об учетных данных администраторов на всех станциях.

Все действия по подготовке операционной системы станции необходимо проводить под учетной записью с правами администратора.

Дополнительная настройка

Для установки Dr.Web KATANA на станции требуется одновременное выполнение следующих дополнительных условий:

- Ограничения системы контроля учетных записей (UAC) должны быть отключены, если станция работает под управлением Windows Vista или более поздней операционной системы. Если вы работаете под встроенной учетной записью администратора, то данную настройку проводить не нужно. Перейдите к следующему пункту.

  Откройте редактор реестра операционной системы.

  1. Найдите и выберите ветку HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM.
  2. Если в данной ветке отсутствует ключ **LocalAccountTokenFilterPolicy**, создайте его:

a. В меню **Правка** выберите команду **Создать**, а затем выберите **Параметр DWORD**.

b. Введите в качестве имени ключа **LocalAccountTokenFilterPolicy**.

3. В контекстном меню ключа **LocalAccountTokenFilterPolicy** выберите **Изменить**.
4. В поле **Значение** введите **1**.
5. Нажмите кнопку **OK** и выйдите из редактора реестра.
6. Перезагрузите станцию.
7. Повторите операцию для всех станциях, подлежащих проверке.

Данную операцию рекомендуется выполнять только администратору или опытному пользователю системы. Неверные действия при изменении реестра могут серьезно повредить систему. Специалисты компании Microsoft рекомендуют перед изменением реестра создать резервную копию всех важных данных, имеющихся на компьютере.

- Все необходимые для работы сети службы должны быть установлены и настроены.

Чтобы проверить сетевые настройки

1. Запустите Панель управления на станции.
   - При настройке поддерживаемых систем более ранних, чем Windows Vista, выберите раздел **Сетевые подключения** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**).
   - При настройке Windows Vista выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Просмотр состояния сети и задач** → **Управление сетевыми подключениями**.
   - При настройке Windows 7 или Windows Server 2008 выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Просмотр состояния сети и задач** → **Изменение параметров адаптера**.
   - При настройке Windows 8, Windows 10 или Windows Server 2012 в категории **Сеть и Интернет** выберите **Центр управления сетями и общим доступом** → **Изменение параметров адаптера**.
2. Щелкните правой кнопкой мыши по необходимому подключению и выберите пункт **Свойства**.
3. Проверьте, что для выбранного подключения установлены и настроены следующие службы:
   - клиент для сетей Microsoft;
   - служба доступа к файлам и принтерам сетей Microsoft;
   - протокол Интернета версии 4 (TCP/IPv4) или версии 6 (TCP/IPv6).
4. Сохраните изменения и закройте окно настроек.

- Параметры общего доступа должны допускать расширенную настройку.

Чтобы настроить общий доступ

1. Запустите Панель управления на станции.
   - При настройке Windows XP или Windows Server 2003 выберите пункт **Брандмауэр Windows** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**).
   - При настройке Windows Vista выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Настройка общего доступа к файлам**.
   - При настройке Windows 7 или Windows Server 2008 выберите режим просмотра по категории. В категории **Сеть и Интернет** выберите **Центр управления сетями и общим доступом** и затем выберите **Изменить дополнительные параметры общего доступа**.
   - При настройке Windows 8, Windows 10 или Windows Server 2012 в категории **Сеть и Интернет** выберите **Центр управления сетями и общим доступом** и затем выберите **Изменить дополнительные параметры общего доступа**.
2. В открывшемся окне выполните одно из следующих действий:
   - При настройке Windows XP или Microsoft Windows Server 2003 перейдите на вкладку **Исключения** и включите настройку **Общий доступ к файлам и принтерам**.
   - При настройке Windows Vista установите **Сетевое обнаружение** и выберите **Общий доступ к файлам**.
   - При настройке Windows 7 выберите **Включить сетевое обнаружение** и **Включить общий доступ к файлам и принтерам**.
   - При настройке Microsoft Windows Server 2008, Windows 8, Windows 10 или Microsoft Windows Server 2012 выберите **Включить общий доступ к файлам и принтерам**.
3. Сохраните изменения и закройте окно настроек.

- Для локальных учетных записей должна использоваться обычная модель совместного доступа и безопасности.

Чтобы настроить модель совместного доступа и безопасности

1. Запустите Панель управления на станции.
   - При настройке поддерживаемых систем более ранних, чем Windows Vista выберите пункт **Администрирование** (если раздел отсутствует, нажмите кнопку **Переключиться к стандартному виду**) и запустите утилиту **Локальная политика безопасности**.
   - При настройке Windows Vista и более поздних систем выберите режим просмотра по категории. В категории **Система и безопасность** выберите группу **Администрирование** и запустите утилиту **Локальная политика безопасности**.

Для запуска утилиты по настройке локальных политик безопасности вы также можете набрать в поле поиска Windows команду `secpol.msc` и нажать клавишу ENTER.

2. В дереве консоли выберите группу **Локальные политики**, а затем — группу **Параметры безопасности**.
3. Щелкните правой кнопкой мыши по параметру **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей**, выберите пункт **Свойства** и задайте значение **Обычная — локальные пользователи удостоверяются как они сами**.

По умолчанию подключение к удаленному компьютеру не может быть установлено, если используемая учетная запись содержит пустой пароль. Чтобы подключиться, задайте непустой пароль.

4. Закройте консоль.

7. Настройка контроллера домена Active Directory

Если в организации используется контроллер домена Active Directory, следует настроить:

- параметры общего доступа к файлам и принтерам;
- параметры безопасности.

Вы можете создать новый объект групповой политики (GPO) для применения данных настроек или же изменить параметры уже существующего объекта.

Чтобы создать новый объект групповой политики

1. В окне командной строки введите в текстовое поле `gpmc.msc` и запустите консоль управления групповыми политиками **GPMC**.
2. Создайте новый объект групповой политики, например **GPO-KATANABUSINESSEDITION**. Для этого в дереве консоли **GPMC** правой кнопкой мыши щелкните **Объекты групповой политики** в соответствующем лесу и домене. Нажмите **Создать**. В открывшемся диалоговом окне укажите имя нового объекта и нажмите **ОК**.
3. Привяжите созданный объект к нужному домену.
4. Правой кнопкой мыши нажмите на созданный объект, выберите **Изменить** и скорректируйте необходимые настройки в соответствие с описанием, приведенным ниже.

Если вы решили не создавать новый объект, а изменить параметры уже существующего объекта, то откройте окно с соответствующими настройками.

1. На компьютере, где установлена консоль управления групповыми политиками GPMC, нажмите **Пуск** → **Администрирование** → **Управление групповой политикой**.
2. Если появится диалоговое окно контроля учетных записей, поверьте данные и нажмите кнопку **Продолжить**.
3. В области навигации найдите и разверните узел **Лес: Имя леса**, затем разверните узел **Объекты групповой политики** и щелкните правой кнопкой мыши имя того объекта, для которого вы хотите задать разрешение.
4. В открывшемся меню выберите **Изменить**.

Настройка общего доступа к файлам и принтерам

Разрешите входящие запросы на доступ к файлам от клиентских компьютеров. Включение данного исключения брандмауэра открывает для IP-адресов, указанных в данном правиле, UDP-порты 137 и 138, а также TCP-порт 445.

Чтобы разрешить общий доступ к файлам и принтерам

1. В области навигации открывшегося окна разверните следующие узлы: **Конфигурация компьютера → Политики → Административные шаблоны → Сеть → Сетевые подключения → Брандмауэр Windows → Профиль домена**.
2. В области сведений дважды щелкните по настройке **Брандмауэр Windows: Разрешает исключение для входящего общего доступа к файлам и принтерам** и включите данное правило на вкладке настроек.
3. В текстовом поле **Разрешить незапрошенные входящие сообщения с этих IP-адресов** укажите нужный диапазон.
4. Нажмите **ОК**, чтобы сохранить изменения.

Настройка параметров безопасности

Настройте политику **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** так, чтобы при входе в сеть с учетными данными локальной учетной записи проверка подлинности производилась по этим данным.

Разрешение сетевого доступа по учетным записям пользователей

1. В области навигации открывшегося окна разверните следующие пункты: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Параметры безопасности**.
2. Для политики **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** установите режим **Обычная — локальные пользователи удостоверяются как они сами**.

Применение изменений в домене

Для того, чтобы применить изменения групповых политик в домене, в обоих случаях (и при создании нового объекта, и при изменении политик уже существующего объекта) в окне командной строки укажите команду `gpupdate/force`.

8. Поиск станций и установка Dr.Web KATANA

Чтобы приступить к управлению станциями и регулированию уровня их защиты, вам необходимо найти станции и установить на них Dr.Web KATANA.

Подключаемые станции должны быть расположены в том же сегменте сети, в котором установлен Dr.Web KATANA Business Edition

Если у вас не хватает прав для доступа к сети, вы увидите соответствующее предупреждение. Чтобы установка Dr.Web KATANA на станции завершилась успешно, укажите имя пользователя и пароль для доступа к сети в разделе Настройки или перезапустите Dr.Web KATANA Business Edition с правами администратора. В противном случае установка Dr.Web KATANA на станции может закончиться ошибкой.

Чтобы найти станцию и установить Dr.Web KATANA

1. В разделе программы **Установка** нажмите кнопку **Добавить станции**.
2. В окне добавления станций выберите способ поиска станций:
   - обнаружение сети;
   - поиск в Active Directory;
   - добавление станций вручную (вы можете ввести IP-адрес станции или ее сетевое имя, а также диапазон IP-адресов станций через дефис («-») или с использованием маски).
3. Нажмите кнопку **Найти станции**, чтобы начать поиск станций. Когда все доступные станции будут найдены, поиск автоматически прекратится. Вы можете остановить поиск, нажав кнопку **Остановить поиск**. При этом все найденные на этот момент станции сохранятся в списке.
4. После того как поиск будет завершен, выберите необходимые станции из списка и нажмите кнопку **Установить KATANA**.
5. Откроется окно установки Dr.Web KATANA со списком станций. Этот список сохраняется в разделе **Установка** до перезапуска Dr.Web KATANA Business Edition.

Установка Dr.Web KATANA возможна только на то количество станций, которое разрешено действующей лицензией.

Установка Dr.Web KATANA происходит автоматически. По мере завершения установки станции появляются в списке раздела **Управление**. Перейдя в этот раздел, вы можете начать управление станциями из списка, даже если установка Dr.Web KATANA завершена не на всех станциях. Остальные станции появятся в разделе **Управление** автоматически.

Если среди выбранных станций есть те, на которых уже установлена автономная версия Dr.Web KATANA, повторная установка выполнена не будет. Эти станции автоматически появятся в списке раздела **Управление**. Чтобы приступить к управлению этими станциями, распространите на них используемый открытый ключ.

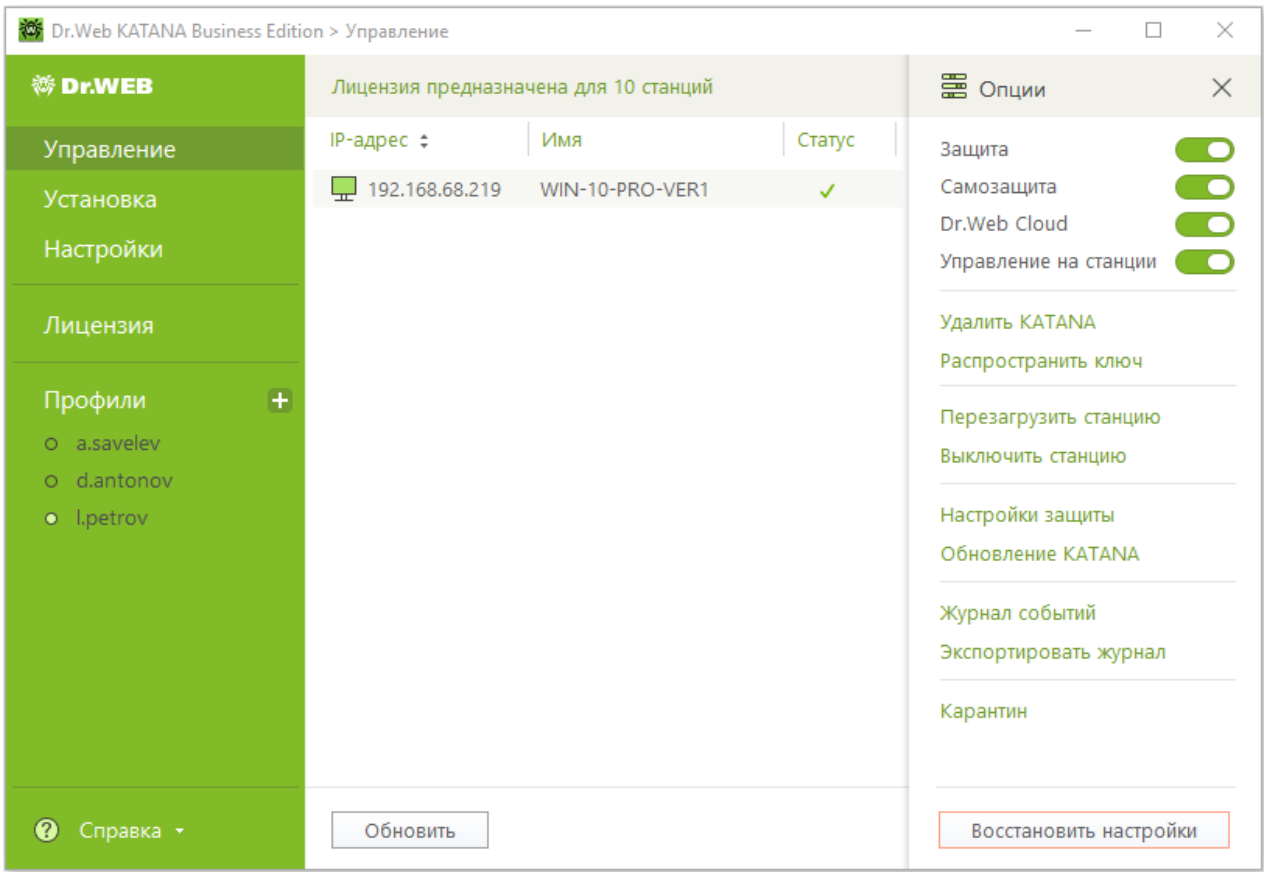

Рисунок 1. Управление станциями

Список станций

Список раздела **Установка** содержит три столбца: **IP-адрес**, **Имя** и **Статус**. При необходимости вы можете отсортировать список по любому из столбцов. Значок станции в столбце **IP-адрес** отображает следующие состояния установки:

- — установка завершена успешно;
- — установка Dr.Web KATANA происходит в штатном режиме;
- — установка завершена ошибкой. Чтобы узнать подробную информацию об ошибке, дважды нажмите .

Чтобы настроить отображение станций в списке, выберите необходимый параметр фильтрации в выпадающем меню внизу окна.

Переустановить. Нажмите эту кнопку, чтобы повторить попытку установки Dr.Web KATANA на одной или нескольких выбранных станция, если установка на них закончилась ошибкой.

Добавить станции. Нажмите эту кнопку, чтобы добавить новые станции к уже имеющимся в списке.

Если в процессе установки Dr.Web KATANA на станции у вас возникли трудности, вы всегда можете обратиться к Справке программы, перейдя в раздел **Справка**. Этот раздел находится в боковом меню программы.

9. Управление станциями

В разделе программы **Управление** вы можете управлять настройками станций, на которые установлен Dr.Web KATANA, регулировать уровень защиты, а также просматривать состояние компонентов Dr.Web KATANA на выбранных станциях. Вы можете начать управление станциями, даже если процесс установки Dr.Web KATANA завершился не на всех станциях. Остальные станции будут автоматически появляться в списке раздела **Управление**. Чтобы настроить отображение станций в списке, нажмите . Чтобы перейти к настройкам станции, нажмите .

Список станций

Список содержит три столбца: **IP-адрес**, **Имя** и **Статус**. При необходимости вы можете отсортировать список по любому из столбцов. В столбце **IP-адрес** отображается состояние станции, в столбце **Статус** — информация о работе Dr.Web KATANA на станции. В этих столбцах может быть указана следующая информация:

IP-адрес	Статус
— станция доступна для управления.	Возможные статусы 1. — станция надежно защищена; 2. — станция защищена не полностью по одной из следующих причин: • выключена самозащита; • выключена превентивная защита; • отключены автоматические обновления; • истек срок действия лицензии; • станции требуется перезагрузка. Нажмите , чтобы узнать статус работы Dr.Web KATANA на выбранной станции. Для обеспечения оптимальной защиты станции, рекомендуется включить необходимые компоненты или перезагрузить станцию, если это необходимо.
— станция недоступна для управления.	— станция не защищена, поскольку на нее не был распространен новый открытый ключ (подробнее см. Управление ключами). **Чтобы распространить новый ключ** 1. Проверьте, что соблюдены все требования из раздела Подготовка станций. 2. Выберите одну или несколько станций. 3. Откройте панель **Опции** и нажмите кнопку **Распространить ключ**.

В списке отображаются только станции, находящиеся в сети. Станции, которые находятся не в сети или перезагружаются, не отображаются в списке.

Dr.Web KATANA Business Edition автоматически обновляет список станций. При необходимости, вы можете принудительно обновить список станций, нажав кнопку **Обновить**.

9.1. Фильтр

Чтобы настроить параметры фильтрации для списка станций, нажмите . Список станций меняется автоматически в зависимости от выбранных параметров. При закрытии боковой панели заданные параметры фильтрации сохраняются до выхода из программы.

9.2. Опции

Чтобы изменить настройки для выбранных станций, нажмите . При закрытии боковой панели заданные настройки сохраняются. Некоторые настройки могут быть применены сразу к нескольким станциям.

Настройки защиты станций

- **Защита**. Включить или выключить защиту Dr.Web KATANA на станции. Настройка может быть применена только к одной станции.
- **Самозащита**. Включить или выключить защиту файлов и процессов Dr.Web KATANA на выбранной станции от несанкционированного воздействия, а также от случайного повреждения. Настройка может быть применена только к одной станции.
- **Dr.Web Cloud**. Разрешить или запретить подключение к облачному сервису компании «Доктор Веб» и к программе улучшения качества работы продуктов Dr.Web. Dr.Web Cloud позволяет антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени. Настройка может быть применены только к одной станции.
- **Управление на станции**. Разрешить или запретить локальное управление Dr.Web KATANA. Если опция отключена, пользователь станции не сможет управлять настройками Dr.Web KATANA, поскольку они будут неактивны. Настройка может быть применены только к одной станции.

Дополнительные настройки защиты станций

- **Удалить KATANA**. Удалить Dr.Web KATANA на одной или нескольких выбранных станциях.
- **Распространить ключ**. Распространить новый открытый ключ на одну или несколько выбранных станций.
- **Настройки защиты**. Настроить реакцию Dr.Web KATANA на действия сторонних приложений, которые могут привести к заражению выбранной станции и выбрать

уровень защиты от эксплойтов. Настройка может быть применены только к одной станции.

- **Обновление KATANA**. Задать параметры обновления Dr.Web KATANA на выбранной станции. Настройка может быть применены только к одной станции.
- **Карантин**. Просмотреть содержимое карантина выбранной станции, который служит для изоляции файлов, подозрительных на наличие вредоносных объектов. Настройка может быть применены только к одной станции.

Настройки работы станций

- **Перезагрузить станцию**. Перезагрузить одну или несколько выбранных станций.
- **Выключить станцию**. Выключить одну или несколько выбранных станций.

Настройки журнала событий

- **Журнал событий**. Открыть окно, содержащее подробную информацию о работе Dr.Web KATANA на выбранной станции. Настройка может быть применены только к одной станции.
- **Экспортировать журнал**. Сохранить журналы событий с одной или нескольких выбранных станций.

9.2.1. Распространение ключей

После создания или загрузки новых ключей шифрования в разделе Настройки необходимо распространить их на станции. В противном случае вы не сможете продолжить управление станциями.

При работе в профилях, использующих старый ключ, вы не сможете управлять станциями, на которые был отправлен новый открытый ключ шифрования.

Чтобы распространить ключи шифрования

1. Проверьте, что соблюдены все требования из раздела Подготовка станций.
2. Выберите одну или несколько станций с действующей лицензией.
3. Нажмите кнопку **Распространить ключ**.

9.2.2. Перезагрузка и выключение станций

Чтобы перезагрузить или выключить станции

1. Выберите одну или несколько станций с действующей лицензией.
2. Нажмите кнопку **Перезагрузить станцию** или **Выключить станцию**.

3. В открывшемся окне выберите время, через которое станции будут перезагружены или выключены.
4. При необходимости в поле **Сообщение** введите текст, который будет показан пользователю станции перед выполнением выбранного действия.

9.2.3. Обновление Dr.Web KATANA

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

Использовать прокси-сервер. Включите эту опцию, если вы хотите использовать прокси-сервер при обновлении, и задайте настройки подключения к нему.

Настройка	Описание
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.
Имя пользователя	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.

9.2.4. Журнал событий

В этом окне вы можете посмотреть подробную информацию о работе Dr.Web KATANA на выбранной станции. Журнал событий содержит сведения о состоянии компонентов Dr.Web KATANA. При появлении каких-либо ошибок или предупреждений о работе Dr.Web KATANA они также отображаются в журнале событий.

Фильтр

Чтобы настроить параметры фильтрации событий, нажмите . Список событий меняется автоматически в зависимости от выбранных параметров фильтрации. При закрытии боковой панели заданные параметры фильтрации сохраняются до выхода из программы.

Опции

При нажатии  откроется боковая панель, в которой доступны дополнительные настройки журнала событий. Данная панель предоставляет вам следующие возможности:

- **Показывать подробности**. При включении этой опции для выбранного события будет отображаться подробная информация в дополнительном окне. Опция включена по умолчанию.
- **Экспортировать журнал**. При нажатии этой кнопки вы можете сохранить журнал событий для выбранной станции. В открывшемся окне выберите формат файла, параметры фильтрации событий, а также путь, по которому файл должен быть сохранен.
- **Очистить журнал**. При нажатии этой кнопки удаляются все записи о событиях на выбранной станции.

9.2.5. Экспорт журнала

Чтобы экспортировать журнал событий

1. Выберите станции, для которых необходимо сохранить журнал событий, и нажмите **Экспортировать журнал**.
2. В открывшемся окне выберите формат файла, тип и период событий, а также путь, по которому файл журнала должен быть сохранен.

Если вы хотите сохранить файл журнала только для одной станции и уже ранее задавали для нее параметры фильтрации событий в окне настроек журнала событий, эти параметры сохраняются.

9.2.6. Настройки защиты

В этом окне вы можете настроить реакцию Dr.Web KATANA на действия сторонних приложений, которые могут привести к заражению станции, и выбрать уровень защиты от эксплойтов.

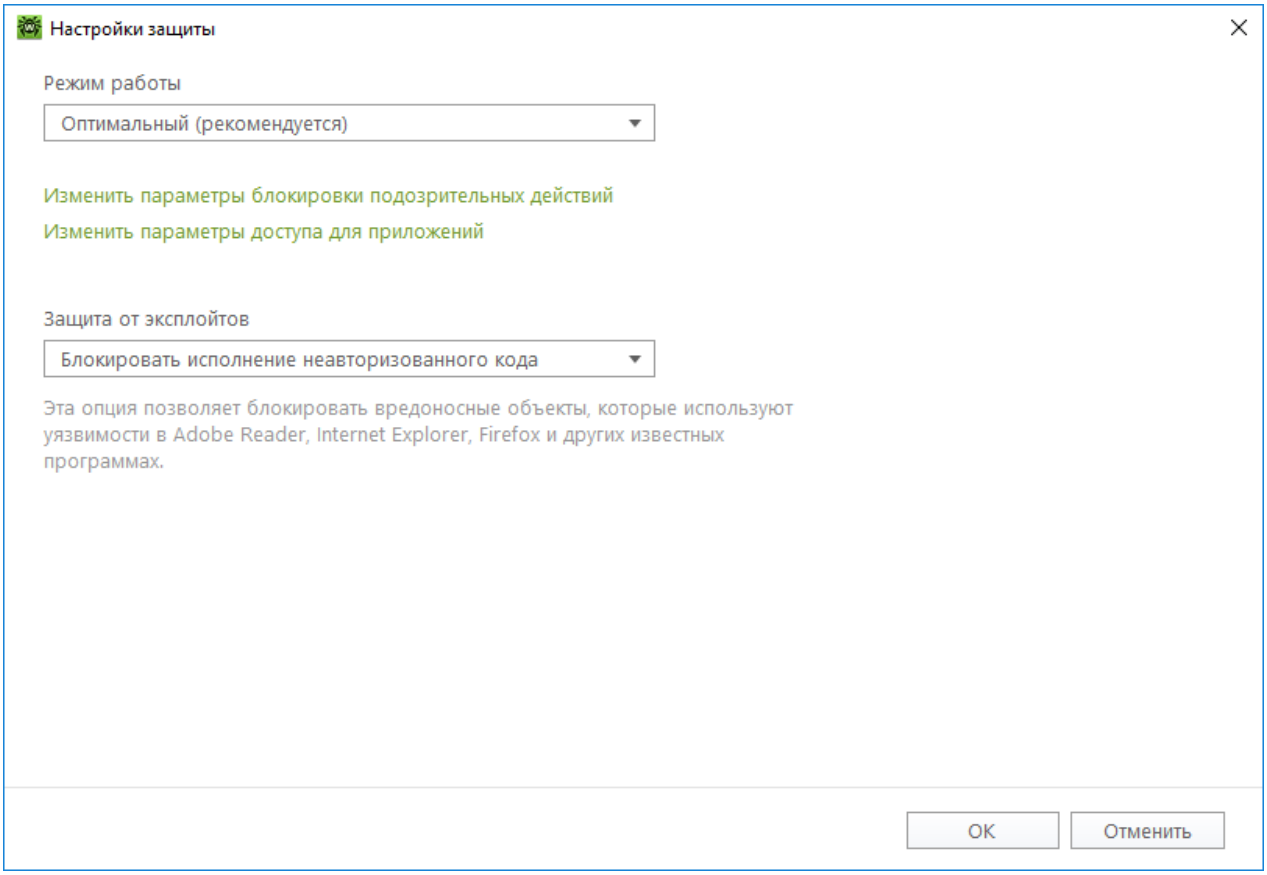

Рисунок 2. Настройки защиты

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 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 режиме работы **Пользовательский**. В этом окне вы также можете создать новый профиль для сохранения нужных настроек.

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 повысить уровень защиты, выбрав режим работы **Средний**. В этом 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, выбрав **Параноидальный** режим. 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	Эта настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера.
Целостность файлов пользователей	Эта настройка позволяет отслеживать процессы, которые модифицируют пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера.
Файл HOSTS	Файл HOSTS используется операционной системой для упрощения доступа к сети Интернет. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
Низкоуровневый доступ к диску	Эта настройка позволяет запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
Загрузка драйверов	Эта 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.

9.2.7. Карантин

В этом окне приводятся данные о содержимом карантина, который служит для изоляции файлов. 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.

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

- **Объект** — имя объекта, находящегося 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:

- **Скачать** — загрузить выбранный объект со станций на компьютер администратора сети;

- **Восстановить** — переместить выбранный объект в исходную папку на станции;

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

- **Удалить** — удалить выбранный объект из карантина и из системы;
- **Очистить карантин** — удалить все объекты из карантина.

10. Настройки

В разделе программы **Настройки** вы можете регулировать настройки Dr.Web KATANA Business Edition и настройки взаимодействия компьютера администратора и станций, на которые Dr.Web KATANA была установлена. Вам доступны следующие настройки:

- язык программы;
- управление ключами;
- сетевое взаимодействие;
- параметры доступа в сеть;
- обновление Dr.Web KATANA Business Edition.

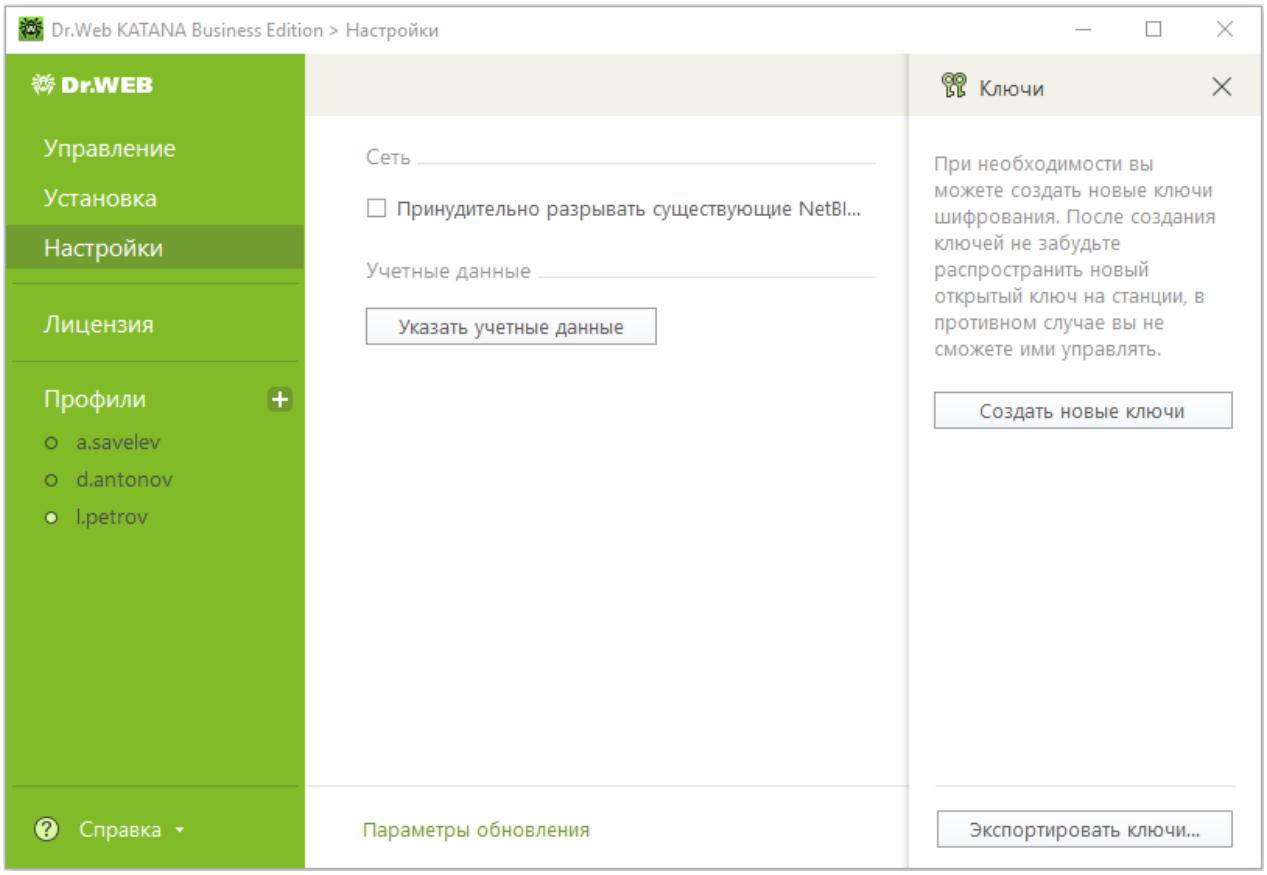

Рисунок 3. Настройки

Все измененные настройки будут применены к текущей сессии. Вы сможете сохранить их в профиль при закрытии программы или смене профиля.

Если у вас возникли трудности при работе с настройками Dr.Web KATANA Business Edition, вы всегда можете обратиться к Справке программы, перейдя в раздел **Справка**. Этот раздел находится в боковом меню программы.

10.1. Язык программы

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

10.2. Управление ключами

При необходимости, вы можете экспортировать используемые ключи шифрования или создать новые.

Чтобы создать новые ключи

1. В разделе **Настройки** нажмите .
2. В открывшейся боковой панели нажмите кнопку **Создать новые ключи**.
3. После создания новых ключей распространите их на станции в разделе **Управление**, используя панель **Опции**.

> Вы не сможете продолжить управление станциями, пока не распространите на них новый открытый ключ. Для таких станций в разделе **Управление** будет указан статус .

Чтобы экспортировать используемые ключи

1. В разделе **Настройки** нажмите .
2. В открывшейся боковой панели нажмите кнопку **Экспортировать ключи**.
3. Выберите папку, в которую будут сохранены ключи шифрования.

10.3. Настройки сетевого взаимодействия

При необходимости вы можете настроить сетевое взаимодействие компьютера администратора и станций. Выберите режим **Принудительно разрывать существующие NetBIOS-соединения**, чтобы перед началом установки прерывать все существующие NetBIOS-соединения со станцией, включая те, в рамках которых имеются открытые файлы или выполняемые задания (необходимо для копирования файлов и запуска Dr.Web KATANA).

10.4. Настройка параметров доступа в сеть

Если у вас отсутствуют права для доступа к сети, перед добавлением станций в разделе **Установка** вы увидите соответствующее предупреждение. Чтобы установка

Dr.Web KATANA на станции завершилась успешно, укажите имя пользователя и пароль, нажав кнопку **Указать учетные данные** в разделе **Настройки**. Вы можете создать новую учетную запись или удалить уже существующую.

- Чтобы создать новую учетную запись, введите имя пользователя и пароль. Нажмите кнопку **Добавить**. Созданная учетная запись появится в списке.
- Чтобы удалить существующую учетную запись, наведите курсор на нее в списке и нажмите .

Обратите внимание, что у администратора нет возможности просматривать пароли учетных записей.

10.5. Обновление Dr.Web KATANA Business Edition

Чтобы изменить параметры обновления Dr.Web KATANA Business Edition, перейдите в раздел **Настройки** и нажмите ссылку **Параметры обновления**.

Автоматическое обновление программы

Если у вас включена опция **Проверять наличие обновлений автоматически** Dr.Web KATANA Business Edition проверяет имеются ли доступные обновления и скачивает их, при этом в боковом меню рядом с названием раздела **Справка** появляется значок . Для полного обновления программы, перезапустите Dr.Web KATANA Business Edition. Для этого сделайте следующее:

1. В выпадающем меню раздела **Справка** выберите пункт **О программе**.
2. В открывшемся окне нажмите кнопку **Перезапустить для обновления**.

Обновление программы вручную

Если у вас отключена опция **Проверять наличие обновлений автоматически**, обновление Dr.Web KATANA Business Edition происходит вручную. Чтобы обновить программу, сделайте следующее:

1. Нажмите в выпадающем меню раздела **Справка** пункт **О программе**, затем кнопку **Проверить наличие обновлений**. При наличии обновлений начнется их скачивание.
2. Перезапустите Dr.Web KATANA Business Edition для полного обновления программы. Для этого сделайте следующее:
   a) В выпадающем меню раздела **Справка** выберите пункт **О программе**.
   b) В открывшемся окне нажмите кнопку **Перезапустить для обновления**.

Параметры обновления

При необходимости вы можете выбрать следующие режимы обновления Dr.Web KATANA Business Edition:

- **Использовать HTTPS-соединения** — включите эту опцию, если вы хотите загружать обновления по безопасному протоколу;
- **Использовать прокси-сервер** — включите эту опцию, если вы хотите использовать прокси-сервер, и задайте настройки подключений к нему:

Настройка	Описание
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.
Имя пользователя	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.

11. Управление лицензиями

В разделе программы **Лицензия** отображается информация об имеющейся у вас лицензии на Dr.Web KATANA Business Edition.

В некоторых случаях, например при окончании срока действия лицензии или при необходимости увеличить количество станций для установки Dr.Web KATANA, вы можете принять решение о приобретении новой лицензии на Dr.Web. В этом разделе вы сможете заменить лицензию на новую.

Чтобы заменить лицензию

1. Нажмите кнопку **Заменить лицензию**.
2. В открывшемся окне укажите путь к действительному новому ключевому файлу.

После добавления новой лицензии она автоматически распространится на станции, на которых установлен Dr.Web KATANA, при этом не требуется переустанавливать или прерывать работу Dr.Web KATANA Business Edition и Dr.Web KATANA на станциях.

Ссылка Мой Dr.Web открывает вашу персональную страницу на сайте компании «Доктор Веб». На данной странице вы сможете получить информацию о вашей лицензии (срок действия, серийный номер и т. д.), продлить срок ее действия, задать вопрос службе поддержки и многое другое.

Ссылка Лицензионное соглашение открывает текст соглашения на сайте компании «Доктор Веб».

12. Приложение А. Методы обнаружения

Dr.Web KATANA использует технологии блокировки вредоносных процессов на основе поведенческого анализа.

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.

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.

Облачная система обновления алгоритмов несигнатурной блокировки Dr.Web ShellGuard

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.