



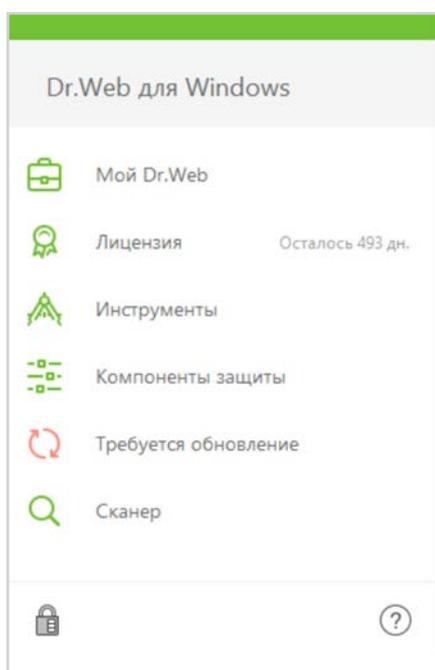
# Настрой-ка Dr.Web от майнеров

В целях максимальной защиты от современных программ — в том числе вредоносных программ-майнеров — сразу после установки необходимо произвести следующие настройки антивирусной защиты.

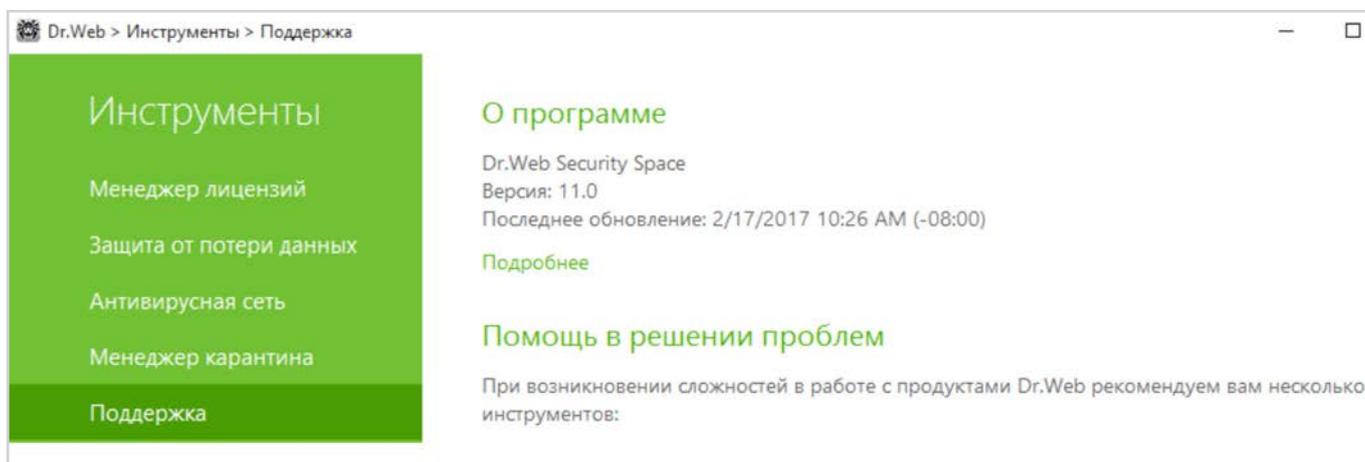
## 1. Проверьте, чтобы используемая вами версия антивируса была актуальной, а лицензия — действующей

**Внимание!** Статистика работы службы технической поддержки компании «Доктор Веб» показывает, что значительное число заражений происходит вследствие того, что антивирус был отключен или длительное время не обновлялся.

Для того чтобы проверить актуальность лицензии, щелкните на значок . Напротив пункта **Лицензия** будет показано количество дней до истечения текущей лицензии.



Для того чтобы узнать используемую версию продукта, щелкните на значок , выберите пункт **Инструменты** и в открывшемся окне — **Поддержка**.



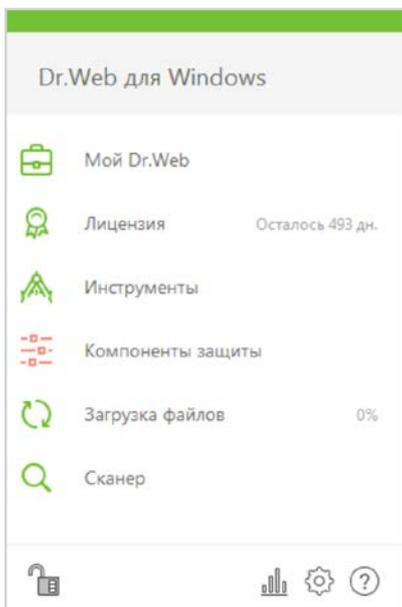
**Внимание!** Текущая версия антивируса Dr.Web Security Suite — 11.5. Использование неактуальных версий антивирусных программ увеличивает риск заражения в связи с отсутствием в них [новейших технологий детектирования](#).

## 2. Все компоненты антивирусной защиты на момент заражения должны быть включены

В том числе модули Превентивной защиты, Dr.Web SplDer Gate, Антиспам Dr.Web и Брандмауэр Dr.Web.

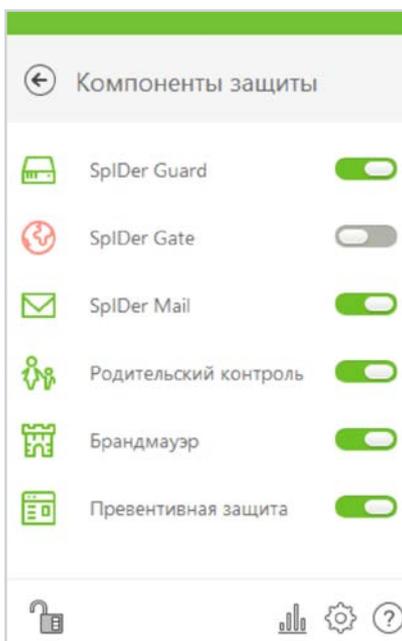
Лишних компонентов в антивирусе Dr.Web нет! В качестве примера можно привести Антиспам Dr.Web. Тестирование данного модуля показало, что он отфильтровывает более 90% неизвестных вредоносных программ, рассылаемых злоумышленниками, по признакам распространения мошеннических писем. И это без использования технологий антивирусного ядра.

Об отключении одного или нескольких компонентов свидетельствует вид значка **SplDer Agent'a** в системном трее: 🕸, а само меню агента будет выглядеть так:



Отсутствие значка агента может означать, что антивирус выгружен и компьютер остался без антивирусной защиты.

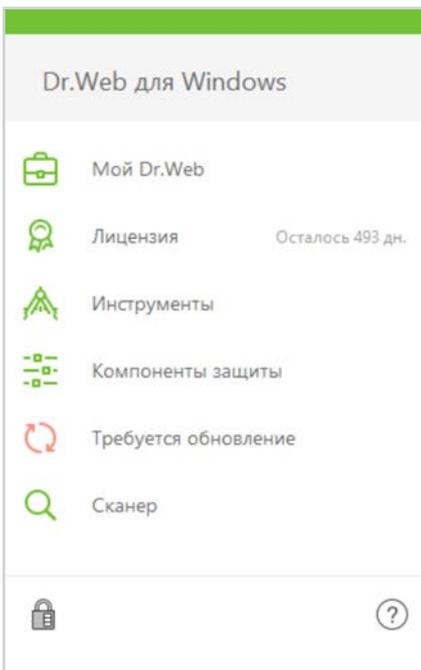
Узнать, какие компоненты отключены, можно, кликнув на значок агента и далее на пункт **Компоненты защиты**.



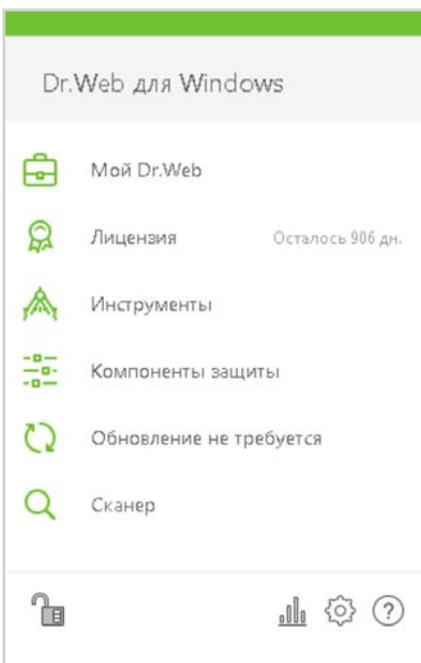
**3. Все обновления антивируса должны быть установлены,** включая обновления, требующие перезагрузки в целях установки новых драйверов перехвата и исправления потенциальных уязвимостей защиты.

Ежедневно злоумышленниками создаются сотни новых майнеров (не считая других вредоносных программ). Если антивирус отключен или долго не обновлялся — каждый из этих майнеров может беспрепятственно установиться на вашем компьютере или устройстве.

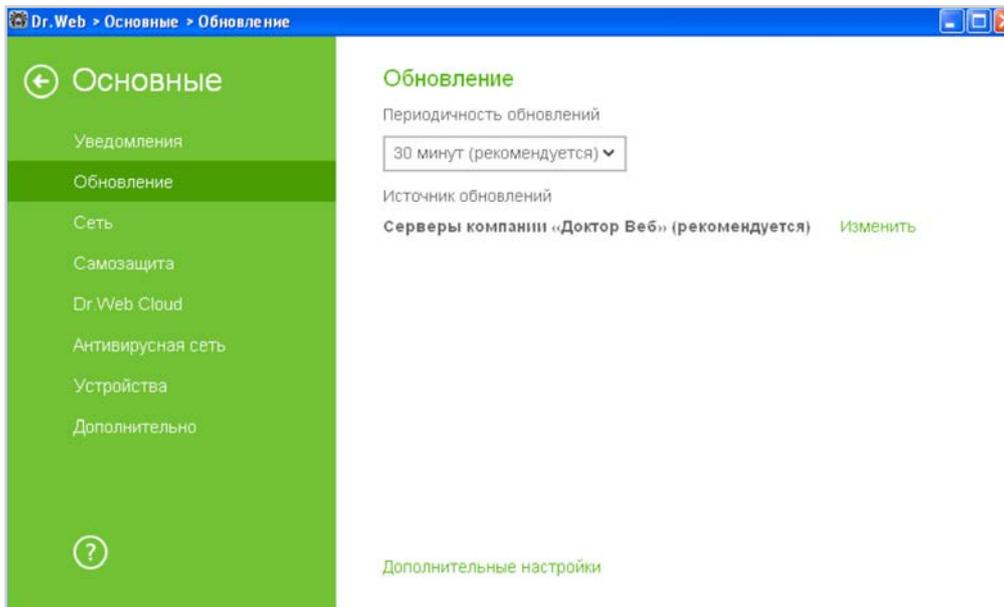
Чтобы проверить статус обновлений, кликните на значок . Статус обновлений будет показан в открывшемся меню.



Чтобы проверить периодичность получения обновлений, кликните на значок  в системном меню, затем в открывшемся меню последовательно нажмите на  и появившийся значок .



В открывшемся окне **Настройки** выберите **Основные** → **Обновление**.



Не рекомендуется увеличивать период между обновлениями более 1 часа.

- 4. Должен быть включен компонент Dr.Web Cloud**, обеспечивающий мгновенную реакцию на появление новых угроз — до получения обновления.

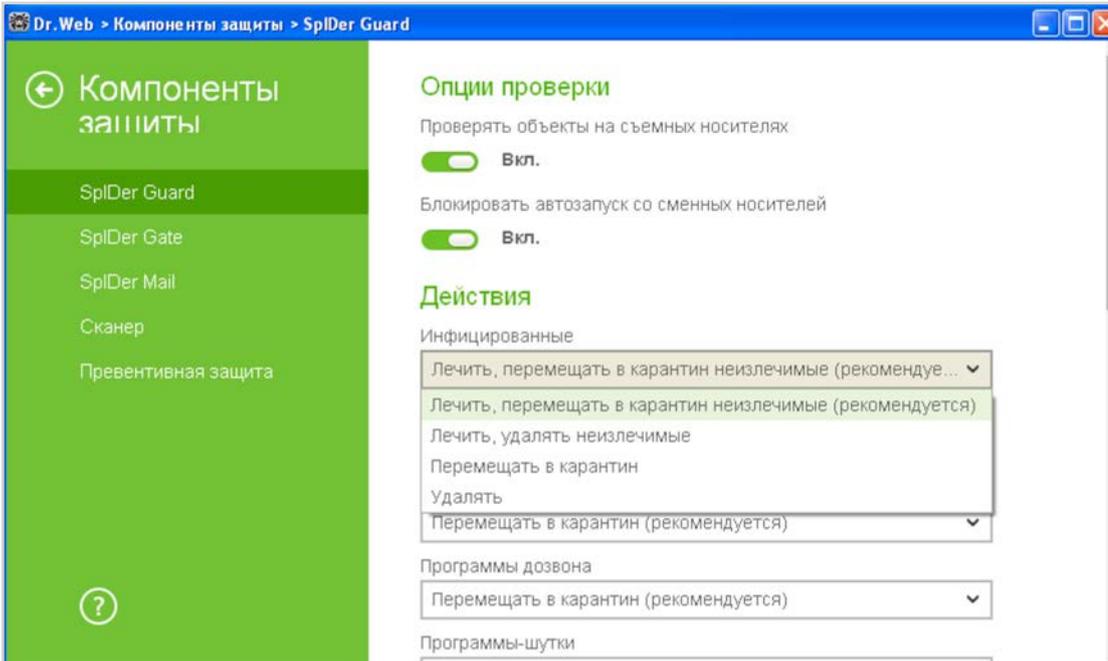
Проверить использование облачного контроля можно, нажав значок  (значок изменит вид на ) , нажав на появившийся значок  и выбрав в меню **Настройки** пункт **Основные**.



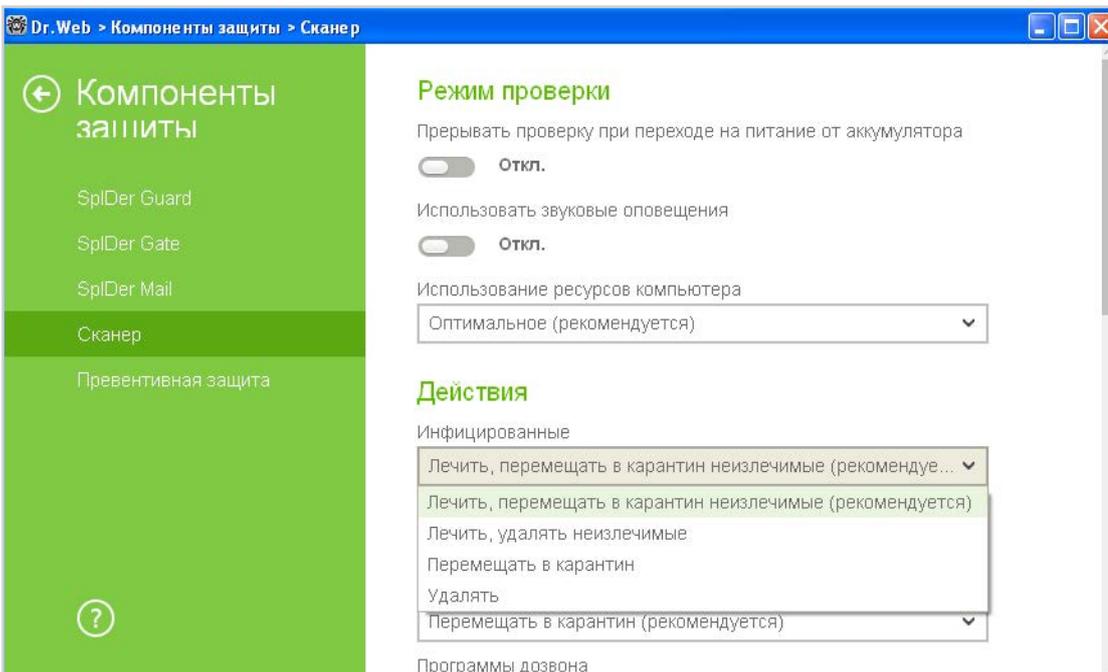
- 5. Действия антивируса Dr.Web Security Space по отношению к вредоносным программам-майнерам должны включать перемещение их в карантин**

В случае повторных заражений, целевых атак, а также в случаях, когда нужно выявить путь заражения, наличие тела вредоносной программы может быть критически важным. Поэтому по отношению к вредоносным программам рекомендуется использовать действие **Перемещать в карантин**.

Кликните на значок  в системном меню, затем в открывшемся меню последовательно нажмите на (Режим администратора) и появившийся значок  (Настройки). В открывшемся окне **Настройки** выберите пункт **Компоненты защиты** и далее **SpIDer Guard**. Настройте действия для групп **Инфицированные** и **Потенциально опасные**.



Аналогичные настройки необходимо использовать и для иных модулей антивируса — в частности, Антивирусного модуля, модуля Dr.Web SpiDer Gate.



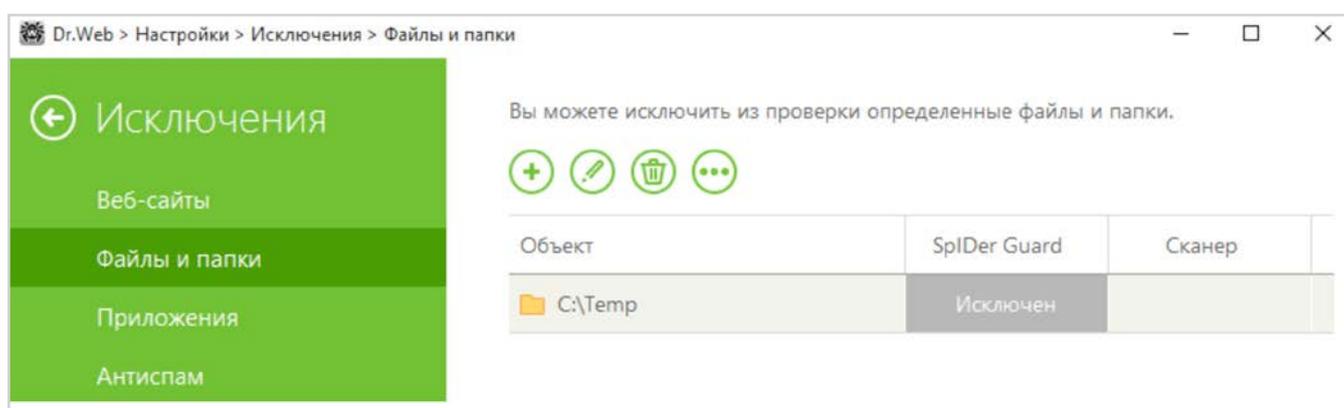
**Внимание!** Майнеры — это общее название вредоносных программ. В частности, они могут распознаваться как троянские программы (Trojan.BtcMine), Java-скрипты (JS.BtcMine), утилиты (Tool.BtcMine). Настройки Dr.Web Security Space позволяют выбрать действия по умолчанию применительно ко всем этим типам майнеров.

Так, для обнаружения вредоносных программ-майнеров, относящихся к типу Tool, рекомендуется установить действие **Потенциально опасные** в **Перемещать в карантин**.

**6. Правила исключения из антивирусной проверки должны использоваться крайне осторожно.** В случае необходимости использования исключений необходимо указывать конкретные файлы.

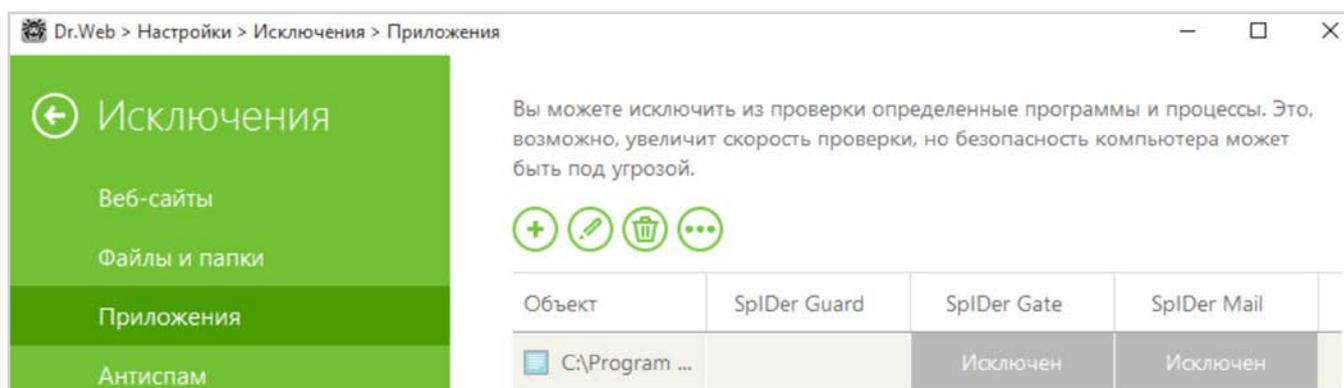
Зачастую вредоносные программы используют для майнинга легальные программы. Такие программы распознаются средствами защиты как потенциально опасные. Если вы уверены, что установленный вами майнер не является вредоносным, вы можете разрешить его использование, используя **Исключения**.

Для того чтобы добавить используемый вами майнер в исключения антивирусной проверки, нажмите значок  (значок изменит вид на ) и, нажав на появившийся значок , войдите в меню **Настройки** в пункт **Исключения**.



**Внимание!** Исключения по маскам типа \*.exe или \*.dll будут служить причиной того, что никакие объекты, подходящие под такую маску, не будут и будут пропущены. В случае маски \*.exe будут пропущены все исполняемые файлы.

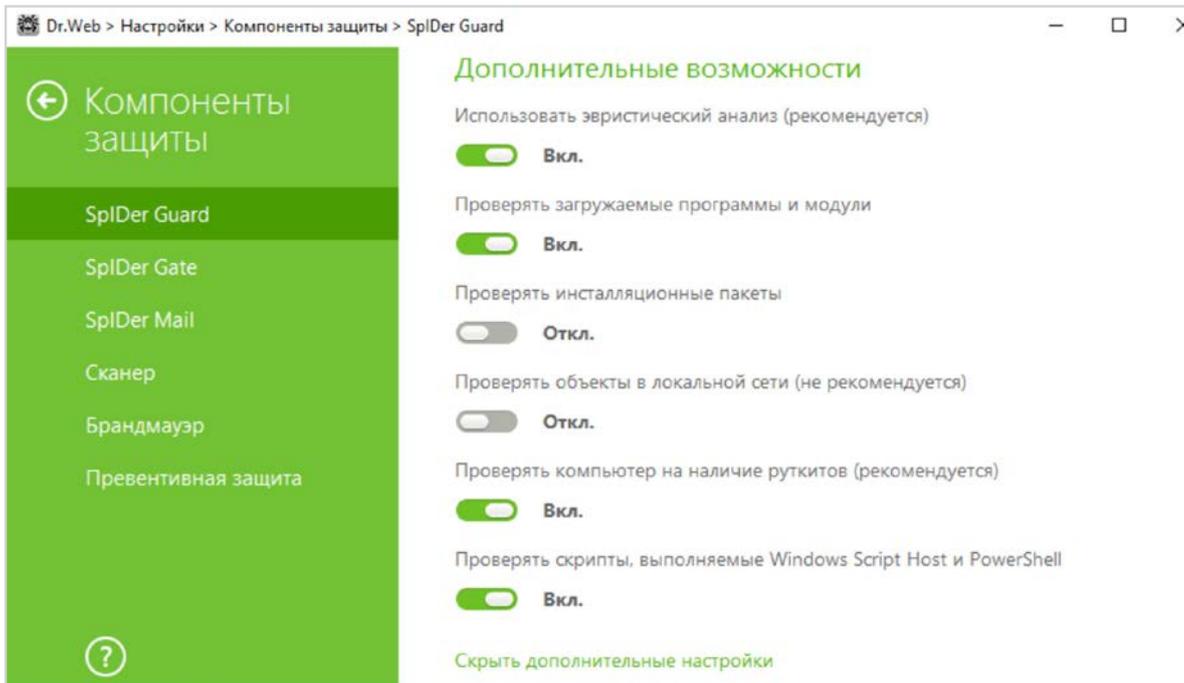
**Внимание!** Не рекомендуется исключать проверку трафика для используемых программ — в таком случае никакое вредоносное ПО, загруженное данными программами, проверяться не будет.



**7. Должна использоваться система обнаружения вредоносных скриптов**

Используемая в Dr.Web технология ScriptHeuristic предотвращает исполнение вредоносных скриптов (в том числе майнеров) в браузере, не нарушая при этом функциональности легитимных скриптов. Дополнительно к данной технологии для противодействия использованию вирусомисателями скриптовых языков JScript, JavaScript, VBScript и PowerShell используется модуль защиты Dr.Web Amsi-client, обеспечивающий проверку выполняемых скриптов, написанных на данных языках.

Включение антивирусной проверки модуля Dr.Web Amsi-client производится в разделе настроек **SpIDer Guard**. По умолчанию проверка включена. Для того чтобы проверить состояние модуля, кликните на значок  в системном меню, затем в открывшемся меню последовательно нажмите на  (**Режим администратора**) и появившийся значок  (**Настройки**). В открывшемся окне **Настройки** выберите пункт **Компоненты защиты** → **SpIDer Guard** и кликните на пункт **Дополнительные настройки**. Пункт **Проверять скрипты...** должен быть включен.

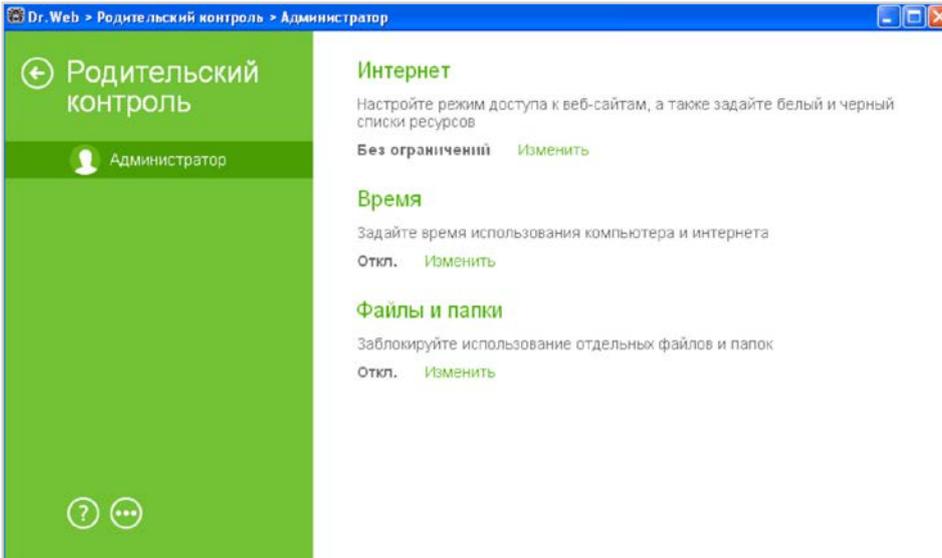


**Внимание!** Установка и удаление модуля Dr.Web Amsi-client производится совместно с модулем Dr.Web SpIDer Guard. Модуль доступен при использовании Антивируса Dr.Web и Dr.Web Security Suite в операционных системах начиная с Windows 10 (x86, x64), а также Windows Server 2016.

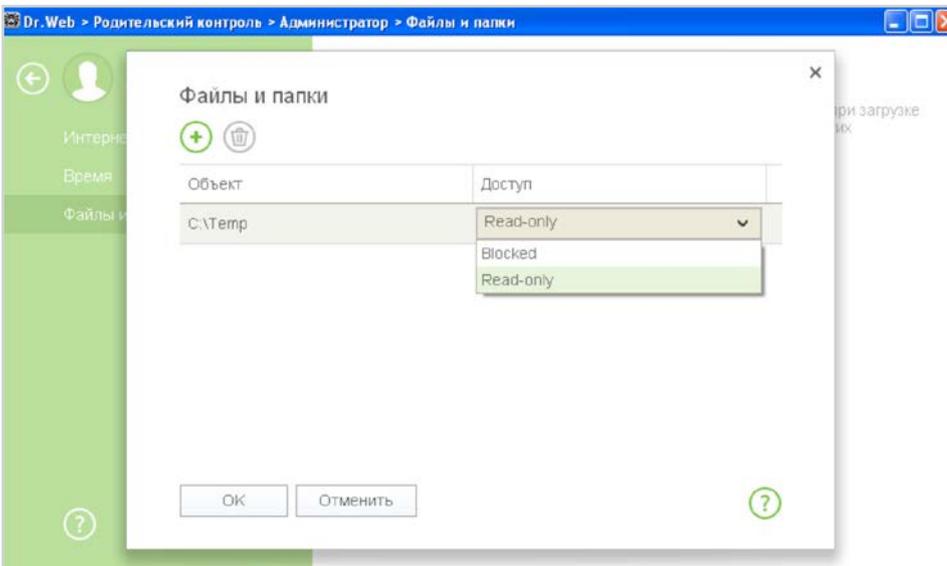
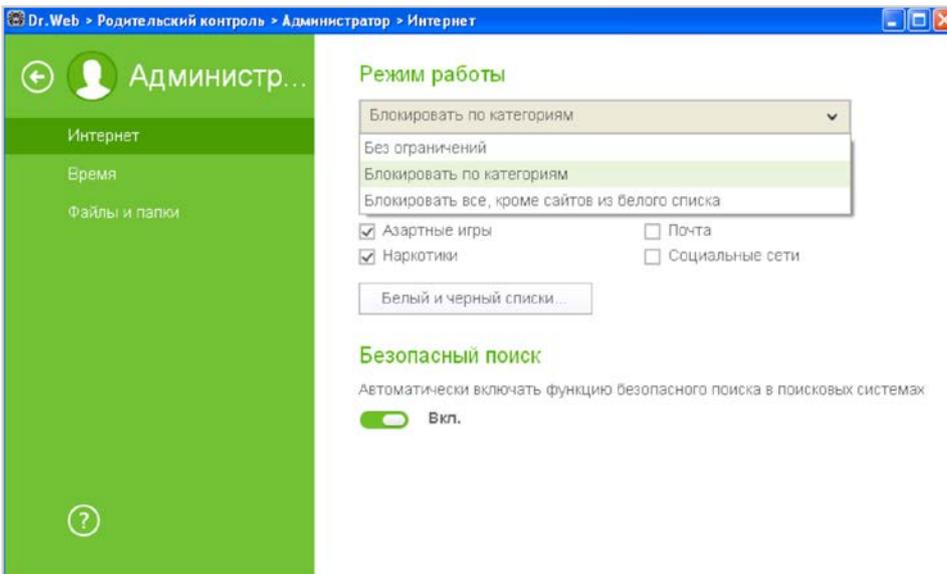
## 8. Должен быть настроен Офисный/Родительский контроль

Троянец-майнер может проникнуть в локальную сеть или на отдельный компьютер через спам (как правило, сообщение содержит вредоносное вложение или специально сформированную ссылку), с помощью сообщения мессенджера (также содержащего ссылку), путем загрузки файла (например, Java-скрипта) пользователем с зараженного сайта или на зараженной флешке.

Для настройки режима доступа к ресурсам сети Интернет, а также ограничения доступа к файлам и папкам, последовательно кликните на значки  и . Затем нажмите на появившийся значок  и в окне **Настройки** перейдите к пункту меню **Родительский контроль**.

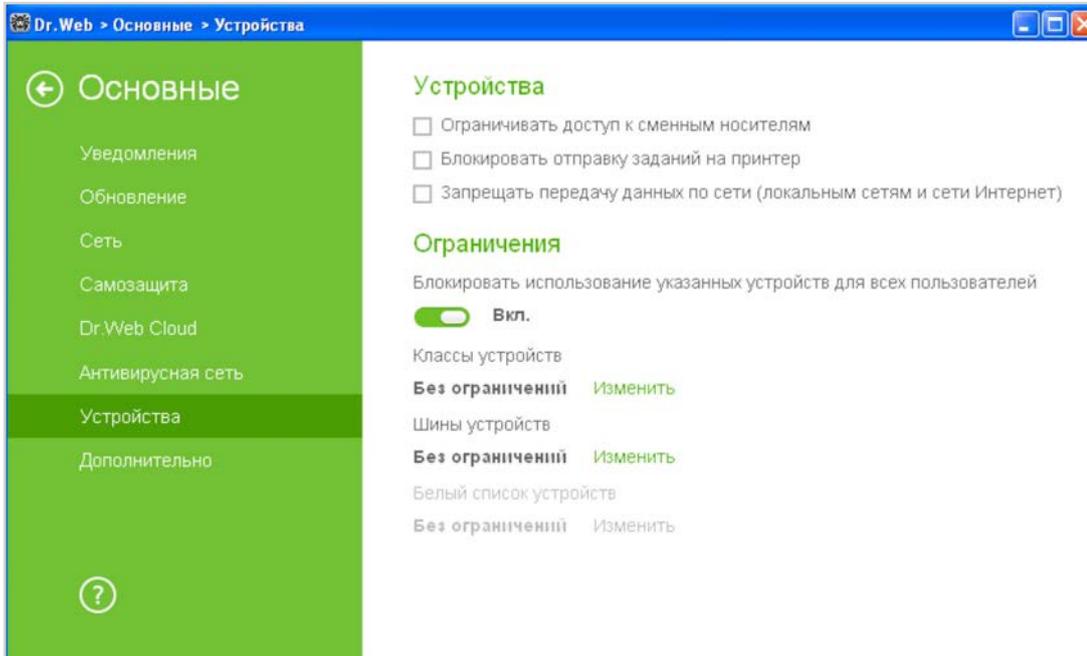


В открывшемся окне выберите пользователя, для которого необходимо настроить ограничения и сделать необходимые настройки.

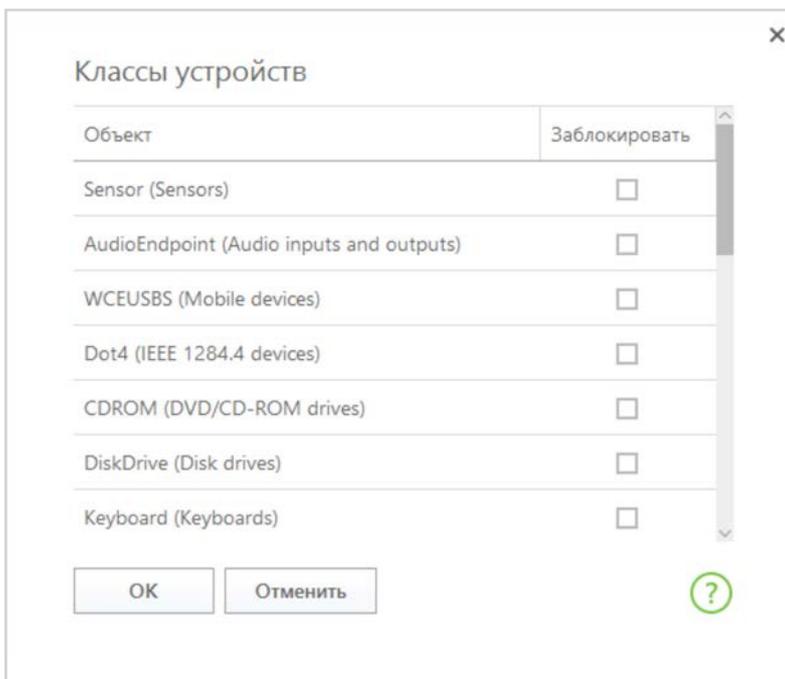


По умолчанию ограничения отключены.

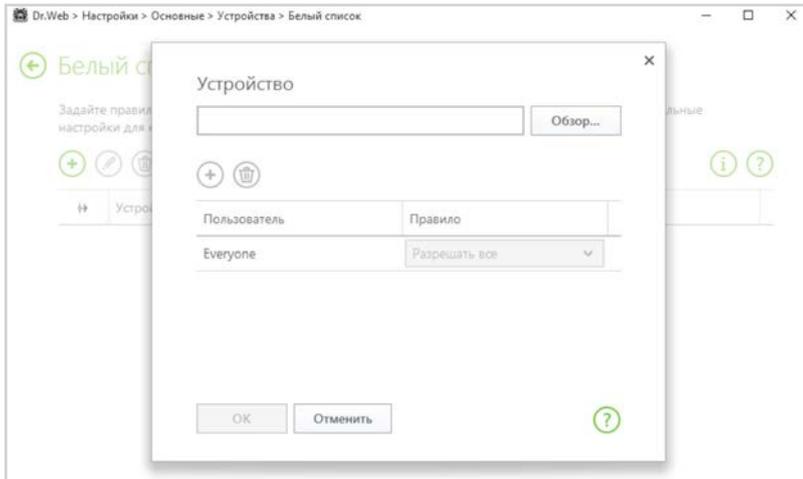
Для настройки ограничений к сменным носителям в окне **Настройки** выберите **Основные** → **Устройства**.



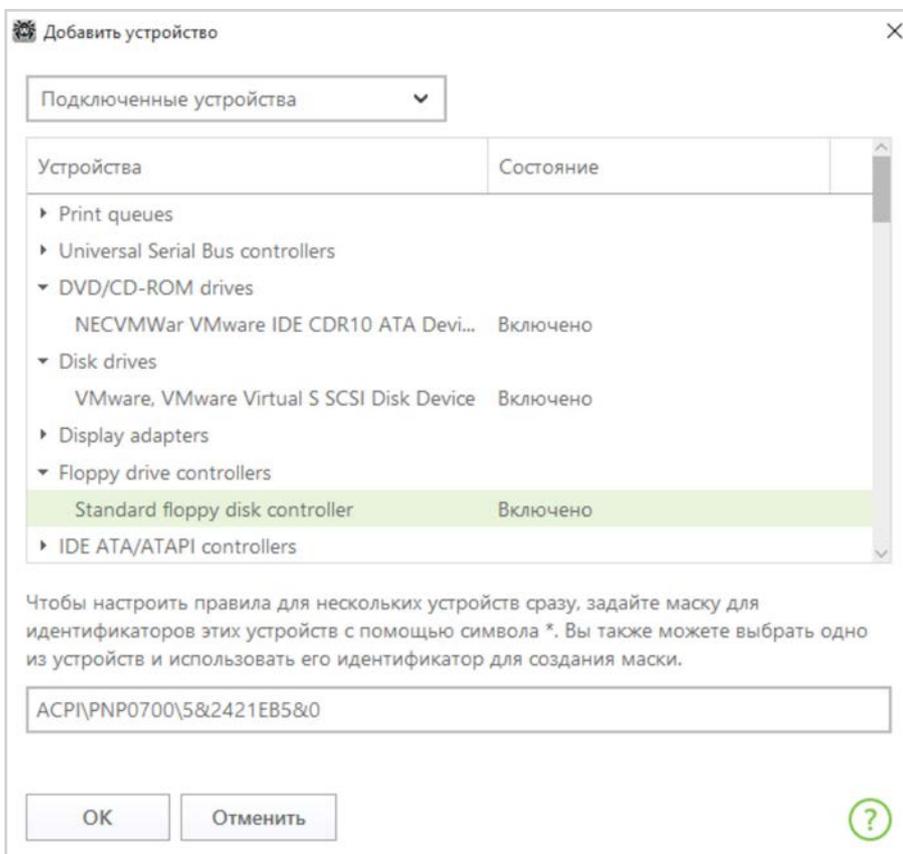
В данном окне выберите **Ограничивать доступ к сменным носителям**. Далее нажмите на **Изменить** для классов устройств и выберите необходимые классы устройств.



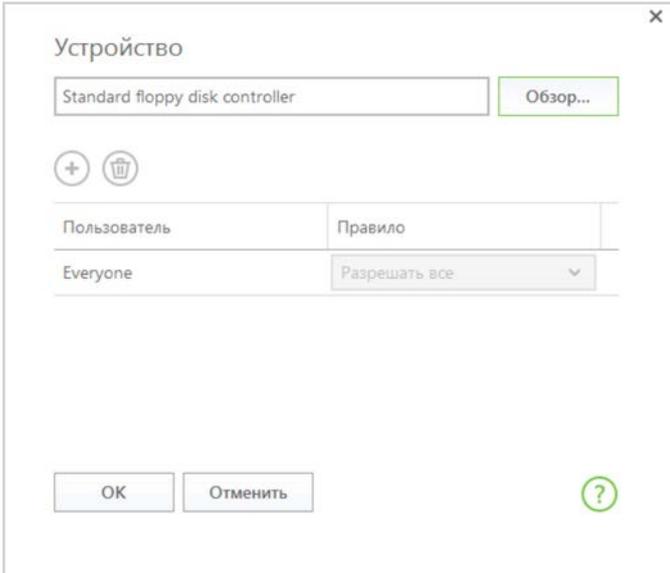
После этого появится возможность настройки для раздела **Белый список устройств**. Если необходимо использовать только разрешенные сменные носители, нажмите на **Изменить** → .



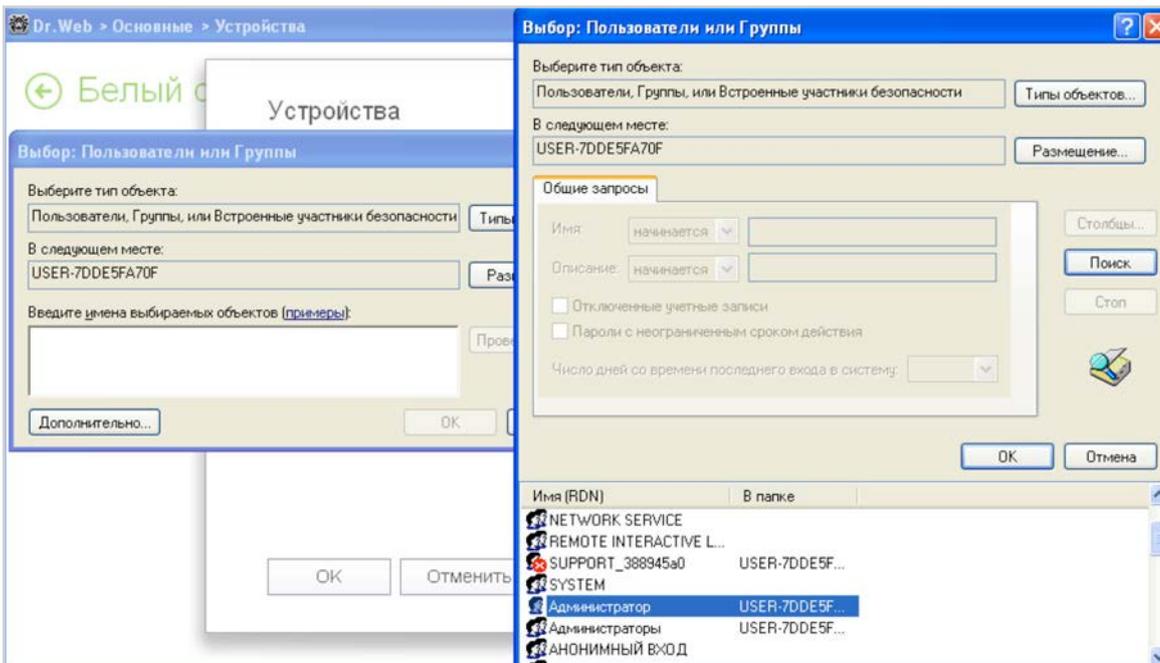
В открывшемся окне нажмите **Обзор** и выберите необходимое устройство.



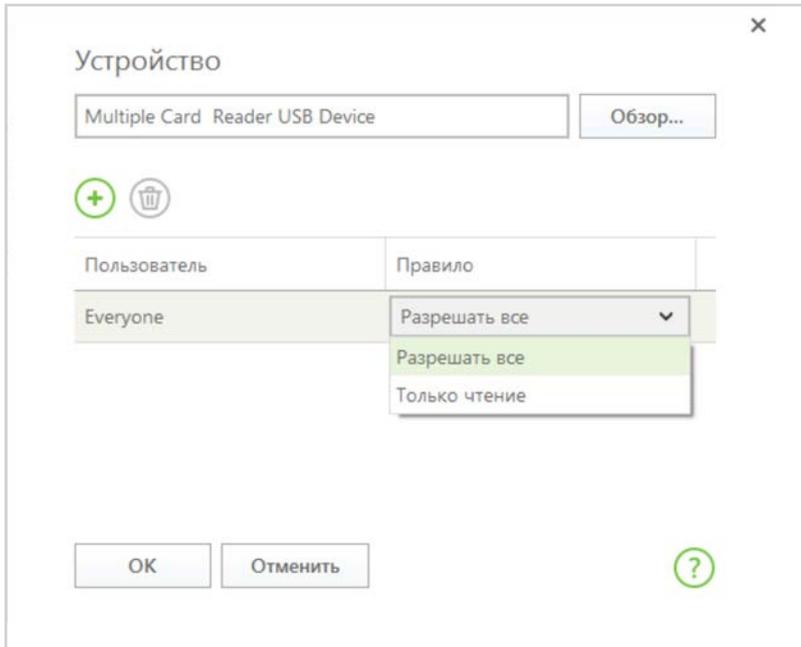
Подтвердите выбор, нажав **ОК**.



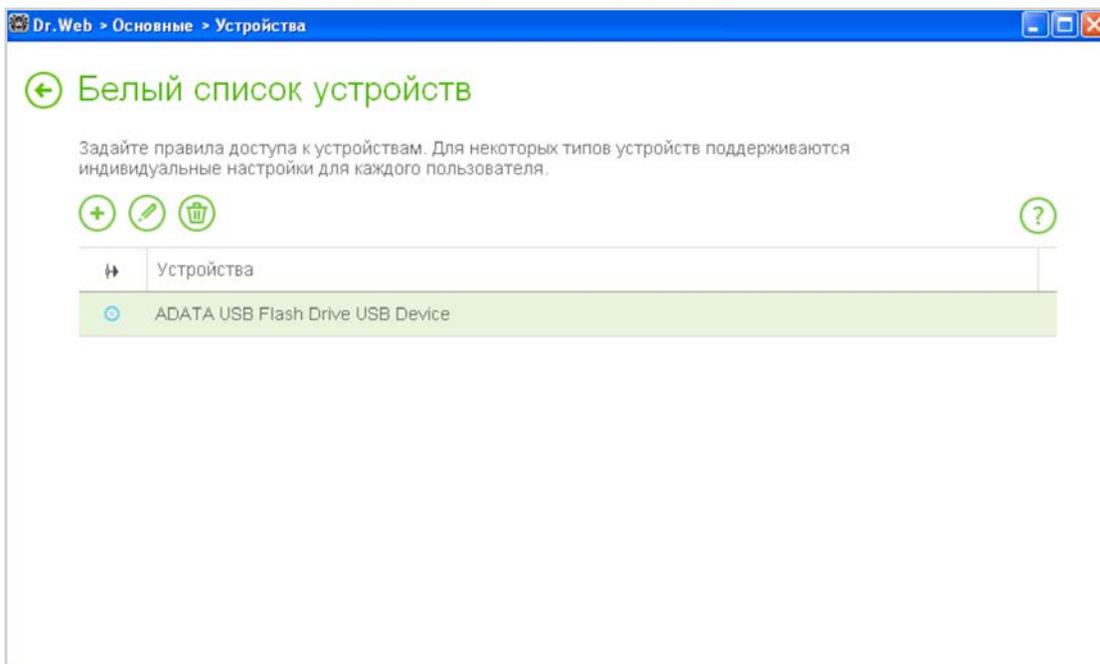
Если необходимо разрешить использование данного носителя только для определенных пользователей компьютера, нажмите  и выберите необходимого пользователя.



Укажите права по использованию данного устройства.

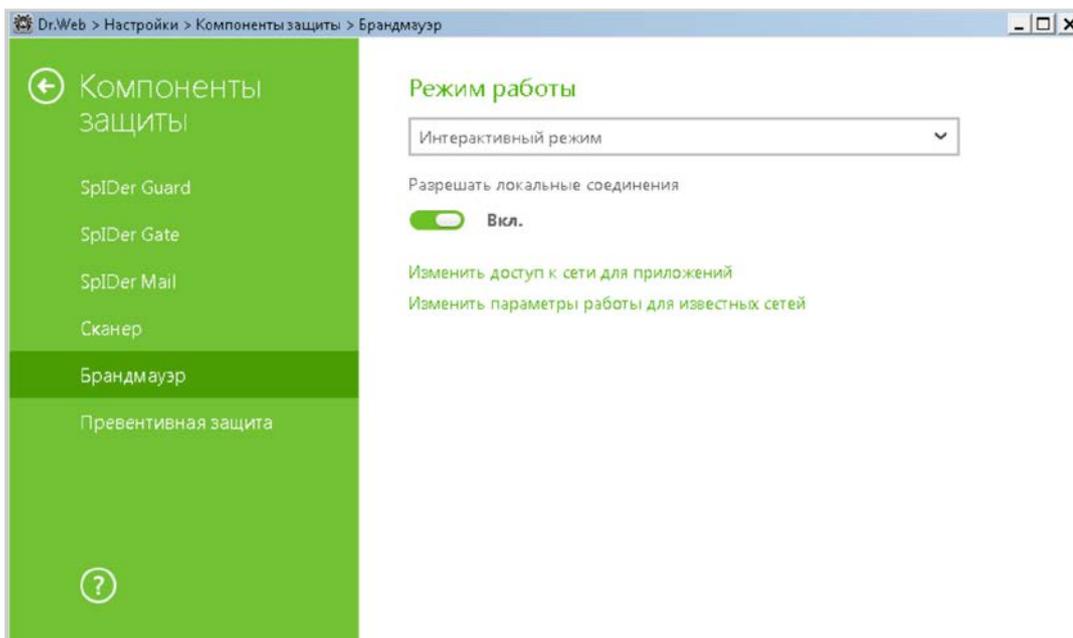


Подтвердите выбор.



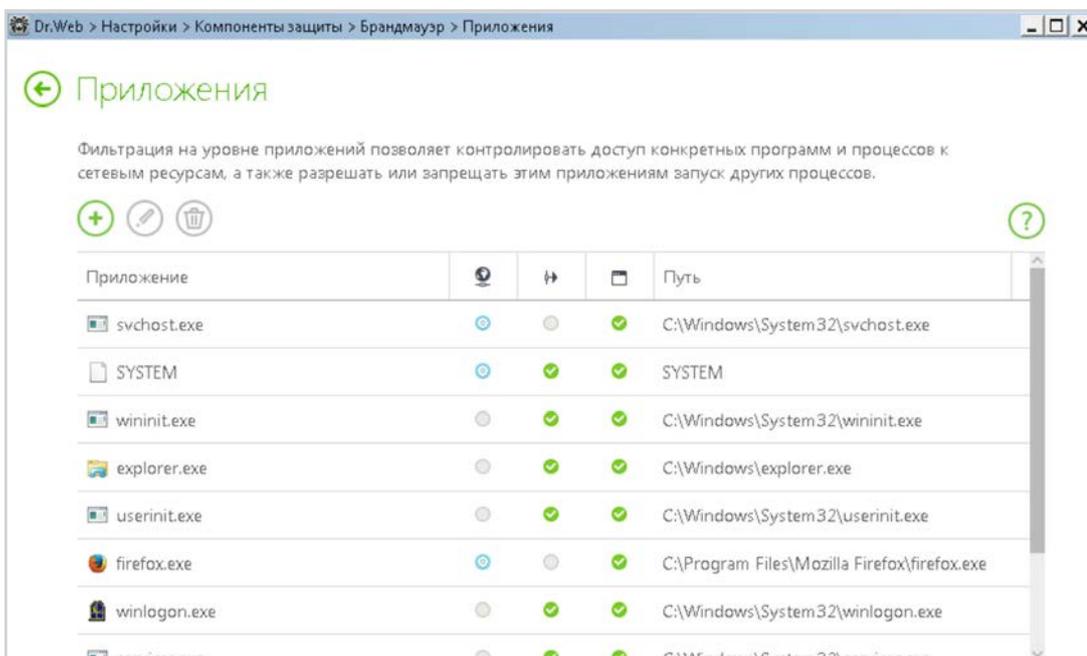
**9. Доступ используемых программ в сеть Интернет должен быть ограничен** — это можно сделать с помощью компонента **Брандмауэр**.

Для настройки параметров работы **Брандмауэра** щелкните кнопкой мыши значок  в системном трее, разблокируйте возможность изменения настроек путем нажатия значка  (значок изменит вид на ) и, нажав на появившийся значок , выберите в меню **Компоненты защиты** пункт **Брандмауэр**.



Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам.

Для каждой программы может быть не более одного набора правил фильтрации.

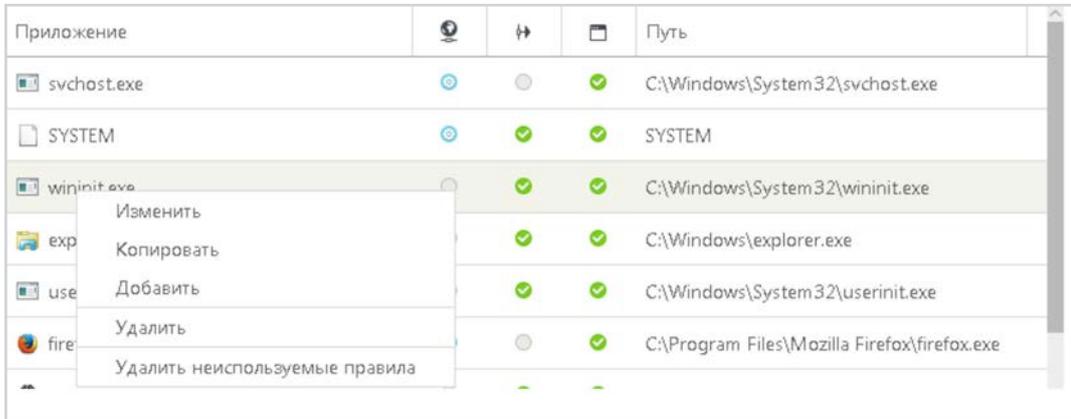


Для доступа к этому окну в настройках **Брандмауэра** нажмите **Изменить доступ к сети для приложений** и нажмите кнопку  или выберите приложение и нажмите кнопку .

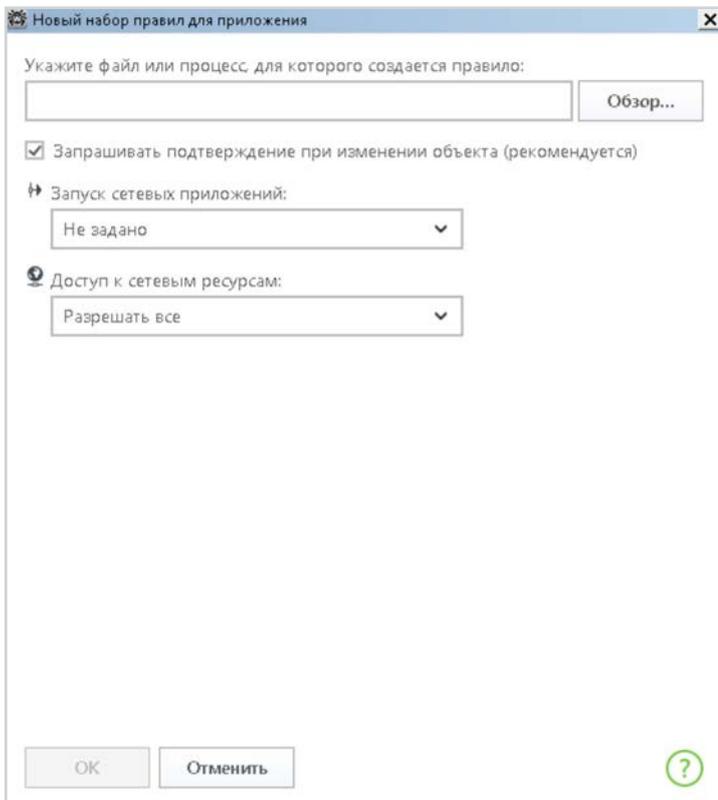
Для формирования набора правил выполните одно из следующих действий.

- Чтобы создать набор правил для новой программы, нажмите кнопку  (**Создать**).
- Чтобы отредактировать существующий набор правил, выберите его в списке и нажмите кнопку  (**Изменить**).

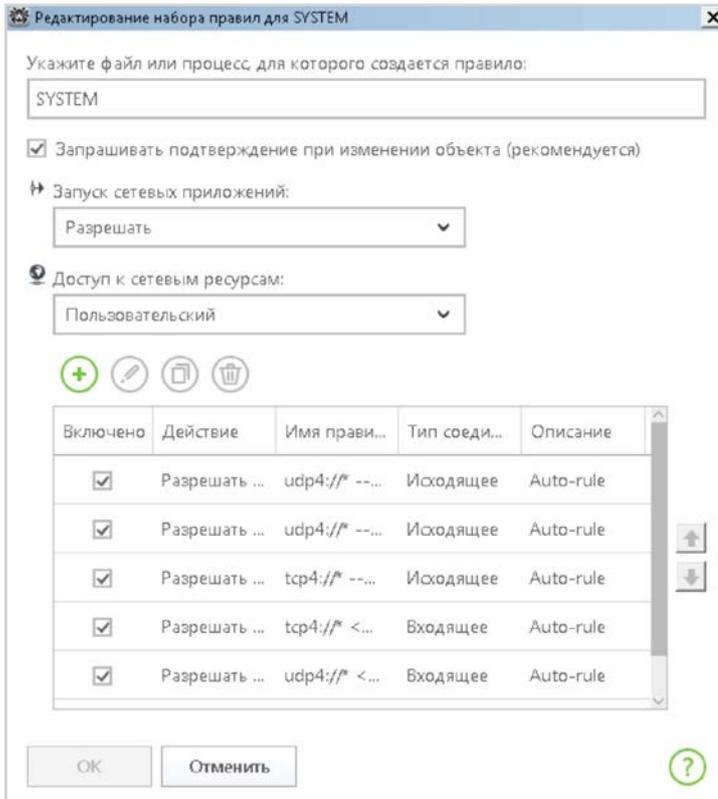
- Чтобы добавить копию существующего набора правил, выберите **Копировать** в контекстном меню. Копия добавляется под выбранным набором.
- Чтобы удалить все правила для программы, выберите соответствующий набор в списке и нажмите кнопку **Удалить**.



В окне **Новый набор правил для приложения** (или **Редактирование набора правил**) отображается тип правила для конкретного приложения или процесса, а также список правил. Вы можете изменять тип правила, формировать список, добавляя новые или редактируя существующие правила фильтрации, а также изменяя порядок их выполнения. Правила применяются последовательно, согласно очередности в списке.



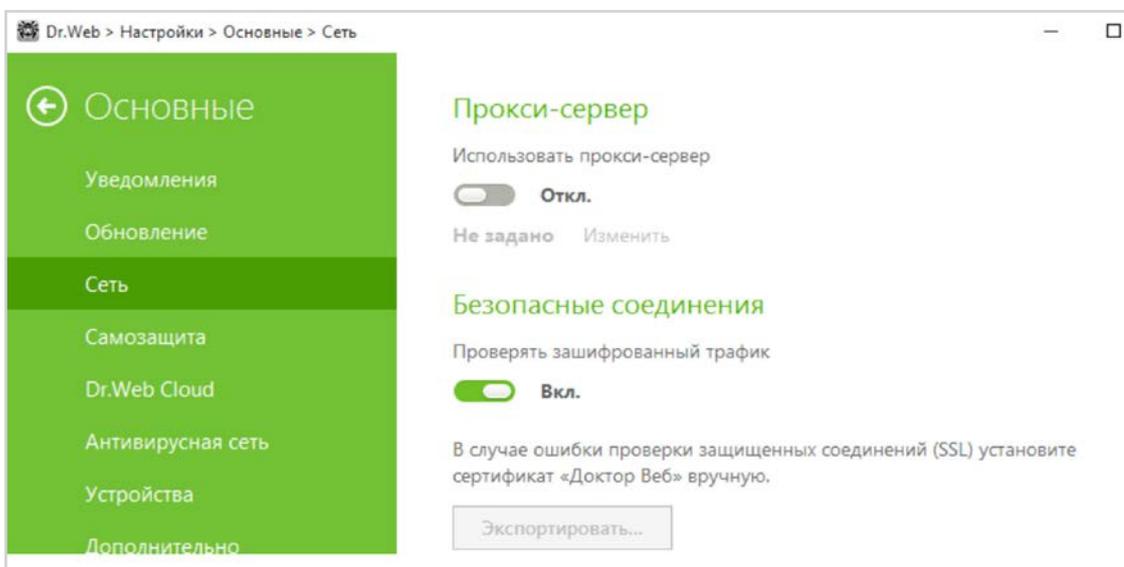
Вы можете создать правило при помощи окна настроек **Брандмауэра**. При работе в режиме обучения вы можете инициировать создание правила непосредственно из окна оповещения о попытке несанкционированного подключения.



**10. Должна быть включена проверка зашифрованного трафика.** На данный момент до половины трафика сети Интернет зашифровано, чем могут воспользоваться злоумышленники.

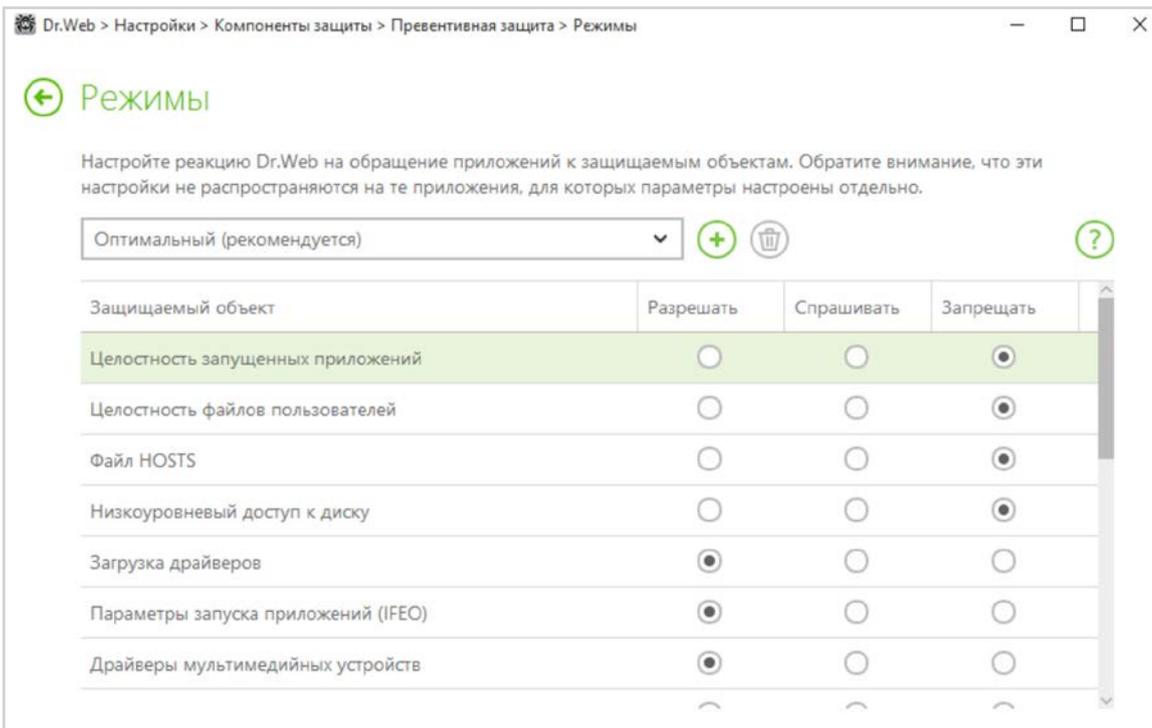
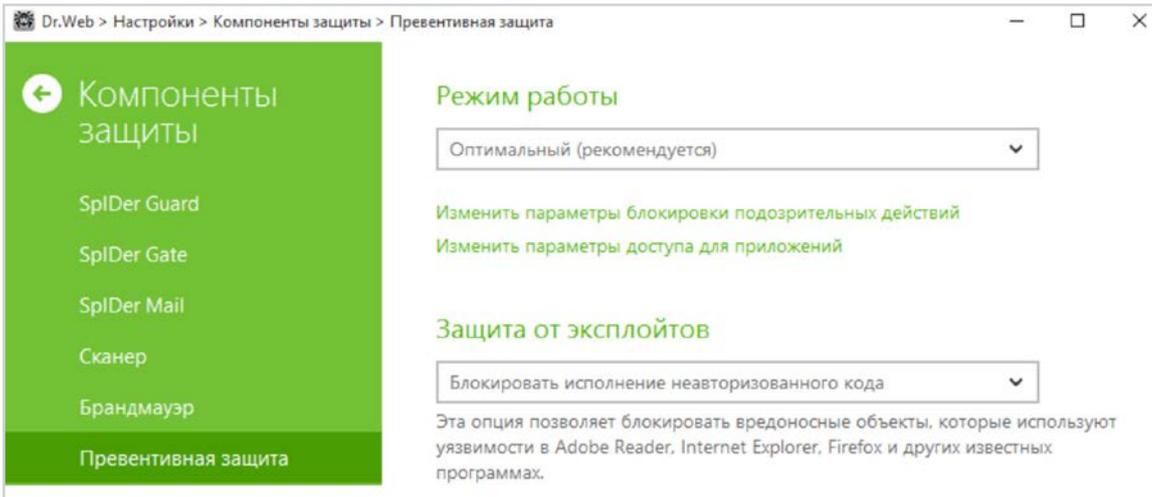
Как правило, майнеры действуют в составе ботнетов — групп зараженных компьютеров. Это позволяет им существенно увеличить вероятность заработка на криптовалютах. Кроме того, сами по себе майнеры бесполезны для злоумышленников без наличия связи с сетью Интернет.

Включите проверку зашифрованного трафика (функционал доступен для Dr.Web Security Space) — кликните на значок  в системном меню, затем в открывшемся меню последовательно нажмите на  (**Режим администратора**) и появившийся значок  (**Настройки**). В открывшемся окне **Настройки** выберите пункт **Основные** и далее **Сеть**. Переключатель **Безопасные соединения** должен быть включен.



## 11. Настройки Dr.Web Process Heuristic не должны позволять внедрение майнерами эксплоитов в работающие приложения

Проверить настройки можно, нажав значок  (значок изменит вид на ) , нажав на появившийся значок  и выбрав в меню **Настройки** пункт **Компоненты защиты** и далее **Изменить параметры блокировки подозрительных действий**.

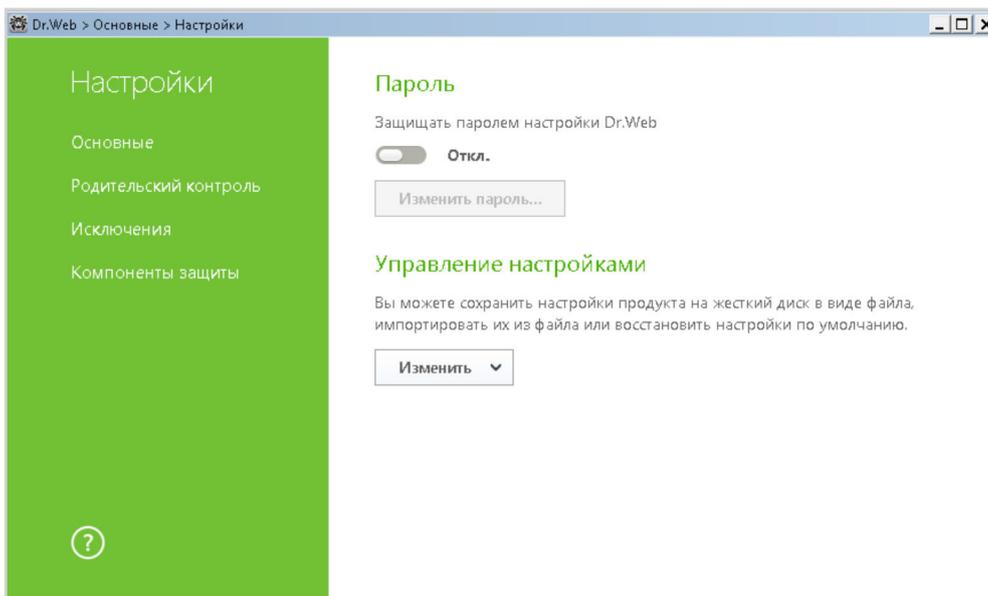


Статус **Разрешить** разрешает внесение изменений в соответствующие ресурсы пользователям и злоумышленникам.

## 12. Установка пароля позволит гарантировать невозможность отключения защиты злоумышленниками — в том числе в случае взлома вашего компьютера.

Вредоносные программы, в том числе майнеры, стремятся отключить антивирус. Не стоит способствовать им в этом желании.

Для установки пароля доступа нажмите значок  (значок изменит вид на ) и, нажав на появившийся значок , выберите в меню **Настройки** пункт **Основные**. Нажмите на переключатель и далее на кнопку **Изменить пароль**.



**Внимание!** Не рекомендуется устанавливать пароль, совпадающий с паролем доступа к компьютеру или устройству.

### Мы также рекомендуем:

1. Включите и настройте компонент **Защита от потери данных**.

Далеко не все майнеры безобидны. В качестве примера можно привести [Trojan.BtcMine.1978](#). При попытке завершить его вручную Windows аварийно прекращает работу и демонстрирует «синий экран смерти» (BSOD).

Не нужно забывать также о том, что далеко не все вирусописатели являются профессионалами в программировании и их «творения» могут повредить данные, находящиеся на вашем компьютере.

Для настройки параметров **Защиты от потери данных** кликните на значок  в системном меню, затем в открывшемся меню нажмите на  и выберите пункт **Инструменты**.

## Dr.Web — российский антивирус

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Это один из первых антивирусов в мире. «Доктор Веб» — один из немногих антивирусных вендоров, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ.

[Технологии Dr.Web](#) | [История разработки](#) | [Наши клиенты](#)

## Продукты Dr.Web внесены в Реестр отечественного ПО

### Лицензии и сертификаты

- [Сертификаты ФСТЭК России](#)
- [Сертификаты МО России](#)
- [Сертификаты ФСБ России](#)
- [Все сертификаты и товарные знаки](#)

### Демо бесплатно

На 30 дней на все продукты комплекса Dr.Web Enterprise Security Suite:

<https://download.drweb.ru/demoreq/biz/v2>

Проверить качество работы наших решений вы также можете как с помощью бесплатных лечащих утилит [Dr.Web CureNet!](#) и [Dr.Web CureIt!](#), так и с помощью сервиса тестирования наших решений — [Dr.Web LiveDemo](#).

### Контакты

Центральный офис ООО «Доктор Веб»  
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а

[Телефоны](#)

[Схема проезда](#)

[Контакты для прессы](#)

[Офисы за пределами России](#)

[антивирус.пф](#) | [www.drweb.ru](#) | [free.drweb.ru](#) | [www.av-desk.ru](#) | [curenet.drweb.ru](#)



© ООО «Доктор Веб»,  
2003-2018