Dr.WEB®

с 1992 года

Майнеры

Информационный бюллетень

Майнеры

Дата составления	**07.03.18**
Текущий уровень опасности	**Средний**

Краткое описание угрозы*

Вредоносные программы, предназначенные для скрытого заработка криптовалют или их кражи

Основные представители угроз

Семейства Trojan.BtcMine, Tool.BtcMine, Tool.Mac.BtcMine, Tool.Linux.BtcMine

* Актуальность угроз определяется не только количеством и разнообразием вредоносных программ, но и уровнем защиты от них в компаниях и организациях различного типа.

Dr.WEB®
с 1992 года

Тема выпуска:

Защита локальных сетей

Причина выпуска бюллетеня

Майнинг (от англ. Mining — «добыча») — способ заработка современных цифровых валют, самой известной (но не единственной) из которых является биткойн. Для гарантированного получения новых единиц цифровых валют требуются серьезные вычислительные мощности — и, по мнению злоумышленников, их можно «позаимствовать» у простых пользователей.

Вредоносные программы для майнинга существуют достаточно давно (Trojan.BtcMine.1 появился в 2011 году), но их стремительное развитие и распространение началось с началом бурного роста стоимости криптовалют.

Особую опасность данные программы представляют как для частных пользователей — в связи с тем, что майнеры часто встраиваются в популярные сайты, — так и для компаний, в частности в связи с тем, что эти программы самостоятельно устанавливаются сотрудниками компаний.

Первые представители вредоносных программ-майнеров были достаточно примитивны, отражали свои процессы в списке процессов, и удалить их можно было самостоятельно. Это породило миф о том, что для защиты от майнеров антивирус не нужен. Однако со временем майнеры стали использовать средства маскировки, противодействия антивирусам, и более того — могут иметь деструктивный функционал.

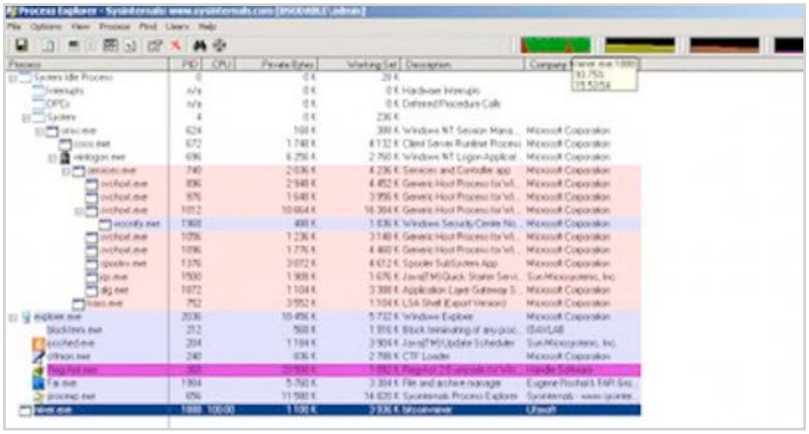
Внимание! Самостоятельное удаление майнера может быть опасно, так как майнеры могут ему противодействовать. Так, Trojan.BtcMine.1978 запускается в качестве критически важного системного процесса, при попытке завершить который Windows аварийно прекращает работу и демонстрирует «синий экран смерти» (BSOD).

Типичные представители вредоносных программ

Вредоносные программы, функционал которых включает заработок (или кражу) криптовалют, имеются для всех основных операционных систем. Как правило, майнеры относятся к семействам Trojan.BtcMine, Tool.BtcMine, JS.BtcMine, Tool.Mac.BtcMine, Tool.Linux.BtcMine.

Несмотря на схожее назначение, майнеры могут относиться к самым разным типам и семействам вредоносных программ, в том числе распознаваться средствами защиты как Java-скрипты или потенциально опасные утилиты.

Так, **Trojan.BtcMine.1** сам по себе майнером не являлся. Для майнинга он использовал две легитимные программы. При этом майнер был очень «жадным» — вторая программа майнинга загружалась им именно для того, чтобы максимально загрузить компьютер расчетами. На иллюстрации можно увидеть нагрузку на процессор, которую создавала программа-майнер, запущенная троянцем **Trojan.BtcMine.1.**



Использование легитимных программ в целях майнинга оказалось невыгодно. Данные программы, естественно, не скрываются от пользователя — их видно в списке запущенных программ. И, соответственно, их легко обнаружить и удалить (или перенастроить для себя).

Еще одна особенность легитимных программ — потребление максимального количества доступных ресурсов. Это вполне логично, так как только в таком случае вероятность получения новой единицы криптовалюты максимальна. Но одновременно это приводит еще и к тому, что компьютер начинает тормозить, а значит, пользователь ищет причину — и в итоге удаляет вредоносную программу.

В результате наряду с майнерами, использующими легитимные программы, появились специально написанные, уже полностью учитывающие специфику преступного бизнеса. Они могут не показывать себя в списке процессов и/или ограничивать потребление ресурсов.

На данный момент майнеры существуют для всех популярных операционных систем. Для Windows, macOS, Linux, Android.

Первые майнеры для Linux — Linux.BtcMine и Linux.CpuMiner — были обнаружены в 2014 году. Тогда же были найдены и первые варианты майнеров для Android OS (Android.CoinMine).

Внимание! эти троянцы влияют не только на время работы аккумулятора и повышают температуру интенсивно работающих компонентов устройства. Сообщалось о взрывах перегретых аккумуляторов мобильных устройств.

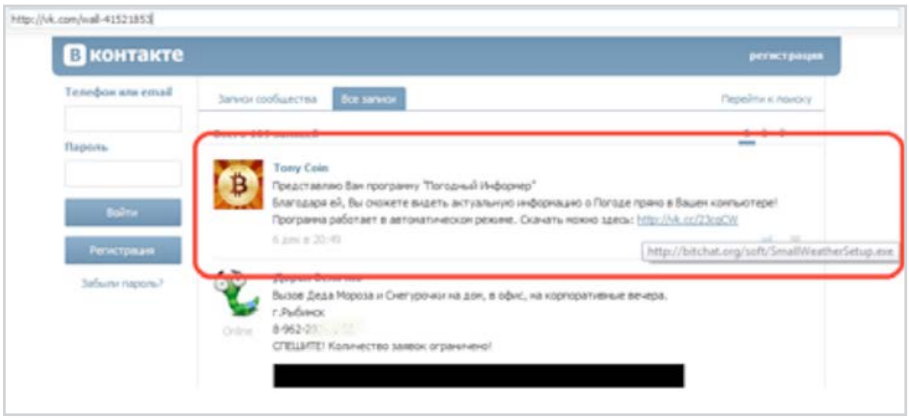
Пути и методы проникновения

В целях майнинга криптовалют злоумышленники используют как специально разработанные вредоносные программы, так и легальное ПО, предназначенное для майнинга. При этом легальное и вредоносное ПО может собираться из одних и тех же исходных текстов, свободно доступных в сети Интернет.

Типичные программы-майнеры являются троянцами — вредоносными программами, не умеющими самостоятельно распространяться. Для проникновения на компьютер, а иногда и для запуска им нужна помощь пользователя.

Наиболее часто встречаются следующие методы распространения вредоносного ПО.

1. Распространение под видом полезных приложений или в составе приложений в качестве дополнительного ПО. В последнем случае майнер может даже иметь собственную галочку в инсталляторе — и даже быть упомянут в лицензионном соглашении. Так, Trojan.BtcMine.218 распространялся под видом «погодного тулбара» — и действительно устанавливал безобидный «погодный информатор» SmallWeatherSetup.exe. А наряду с ним еще и вредоносную программу Tool.BtcMine.130.



2. Плагины для браузеров. В данном случае используется известный плагин, в который так или иначе встраивается вредоносный код. Как вариант создается и раскручивается вредоносное приложение с именем, похожим на уже существующее. В качестве примера можно привести Tool.BtcMine.1046 — плагин SafeBrowse для браузера Google Chrome был предназначен для заработка широкого спектра криптовалют — Monero, Dashcoin, DarkNetCoin и пр. А Trojan.BtcMine.221 распространялся с нескольких принадлежащих злоумышленникам веб-сайтов под видом различных приложений — например, надстройки к браузеру, якобы помогающей пользователю в подборе товара при совершении покупок в интернет-магазинах. Создатели приложения утверждали, что этот плагин автоматически распознает просматриваемые пользователем на различных торговых площадках товары и отыскивает в сети аналогичные предложения по более выгодным ценам. Также этот троянец мог маскироваться под иные приложения, такие как VLC-плеер или программу для анонимного серфинга в Интернете.
3. Установка иными вредоносными приложениями. Так, основное предназначение троянца Trojan.Mods.10 — подмена просматриваемых пользователем сайтов принадлежащими злоумышленникам веб-страницами, а для Trojan.Tofsee основное назначение — рассылка спама.
4. Установка с использованием уязвимостей, эксплуатирующих ошибки и недокументированные возможности современного ПО, в частности браузеров и операционных систем.
5. Самый модный вариант — скрипты на сайте. Неоднократно отмечалось, что

выгодность подобного заработка крайне мала — но тем не менее все больше и больше сайтов — с помощью собственных администраторов или в результате взлома — включаются в гонку за криптовалютами. В качестве интересных примеров можно привести майнер, создававший невидимое всплывающее окошко, прятавшееся за треем на десктопе, или вредоносные программы, подменявшие содержимое неактивных закладок браузера.

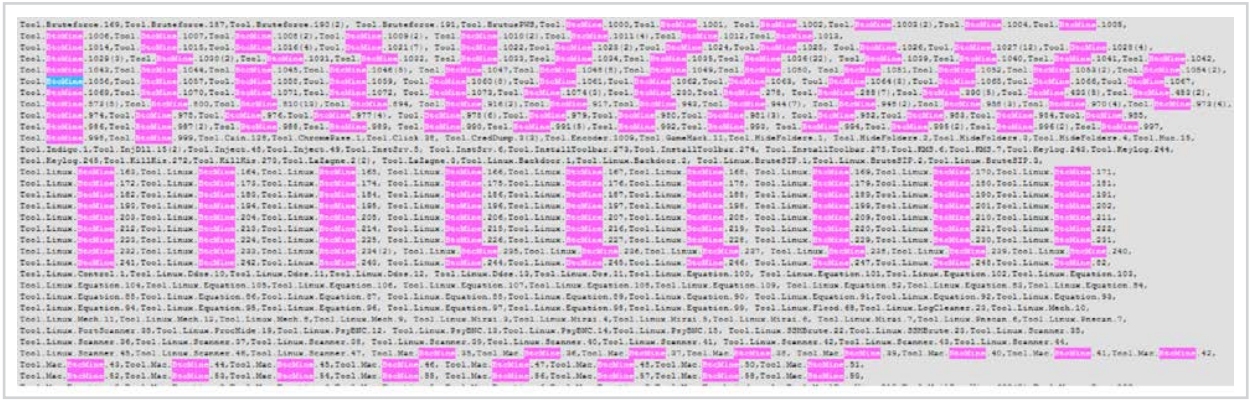
Данный вариант представляет достаточно серьезную опасность, так как, согласно статистике, более 80% сайтов так или иначе уязвимы. В распространении скриптовых майнеров были замечены крупнейшие сайты сети Интернет.

Майнеры для мобильных устройств также могут распространяться и через официальные магазины приложений.

Еще один миф утверждает, что манеры предназначены только для заражения рабочих станций. Это не так. Заражение серверов дает злоумышленникам гораздо больше возможностей заработка. В качестве примера майнеров для серверов Windows можно привести Trojan.BtcMine.1324, Trojan.BtcMine.1369 и Trojan.BtcMine.1404. Эти майнеры используют незакрытую уязвимость на серверах. Серверы Linux особо интересны злоумышленникам, ведь традиционно считается, что эта операционная система неуязвима для вредоносных программ, и зараженные машины могут долго оставаться необнаруженными.

Причина актуальности угрозы

На данный момент майнеры — одна из самых распространенных вредоносных программ. Для того чтобы оценить количество угроз, можно открыть список записей, внесенных в вирусные базы на интересующую дату, и выделить все записи, имеющие в названии слово mine.



Отметим, что данный скриншот содержит лишь часть майнеров, попавших в вирусную базу за один день. На самом деле их в несколько раз больше.

Только представителей семейства Trojan.BtcMine известно более двух тысяч (если говорить точно — 2025 на 24 января 2018 года).

Поскольку вероятность заработка криптовалюты при заражении одиночной машины кране мала, злоумышленники стремятся формировать ботнеты, размеры которых достигают сотен тысяч машин.

Методы маскировки от средств контроля и наблюдения

Вредоносные программы-майнеры используют достаточно продвинутые методы для того, чтобы избежать обнаружения (в том числе средствами защиты).

1. Упаковка и шифрование. Ранее созданная и уже известная антивирусу вредоносная программа пакуется специальной программой так, чтобы известные признаки вредоносной программы изменились.
2. Подпись вредоносного приложения. Так поступает, например, уже упомянутый Trojan.BtcMine.218.
3. Удаление средств защиты. Как пример можно привести Trojan.BtcMine.1978, который пытается удалить службы антивирусов Dr.Web, Windows Live OneCare, «Антивируса Касперского», ESET Nod32, Emsisoft Anti-Malware, Avira, 360 Total Security и Windows Defender.
4. Блокировка доступа к различным ресурсам сети Интернет, в том числе серверам обновлений систем безопасности.

Майнеры для мобильных устройств могут активизироваться в те моменты, когда зараженное мобильное устройство находится в режиме ожидания.

Подавляющее количество манеров относится к троянцам — и не может заражать файлы. Но работающие процессы заражаться майнерами могут. Причем могут заражаться все запущенные процессы, но использоваться для майнинга будет первый процесс, в котором этот троянец начинает работу.

Обязательные средства защиты

Средство защиты	Необходимость применения
Система ограничения доступа	■ Позволяет ограничить доступ на запись к общим сетевым ресурсам, предотвратив распространение вредоносных программ. ■ Позволяет ограничить количество посещаемых ресурсов Интернета до необходимого минимума, что минимизирует риск заражения с сайтов, содержащих вредоносные объекты. ■ Позволяет исключить возможность отключения пользователями программных средств защиты.
Система проверки интернет-трафика	■ Обеспечивает проверку загружаемых файлов до момента их поступления/запуска в клиентских приложениях, в том числе браузерах. ■ Позволяет исключить использование уязвимостей клиентского ПО за счет проверки трафика до его поступления в приложения.
Система проверки интернет-ссылок	Позволяет исключить возможность перехода на зараженные и мошеннические ресурсы.
Антивирусный монитор	Позволяет исключить запуск вредоносных программ, проникших на машину пользователя без проверки, в том числе в запароленных архивах.
Технология ScriptHeuristic	Предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов.

Средство защиты	Необходимость применения
Превентивная защита	Позволяет исключить заражение работающих процессов.
Антивирусный сканер	Периодическая проверка дает возможность обнаружения ранее неизвестных вирусов, находящихся в неактивированном виде.
Персональный брандмауэр	■ Ограничение возможности доступа запущенных программ к ресурсам сети Интернет. ■ Исключение возможности проникновения через открытые порты с помощью эксплойтов.

Кроме установки и настройки Антивируса Dr.Web, рекомендуется:

1) своевременно устанавливать все обновления системы безопасности и операционной системы;

2) ограничить права пользователей и запретить для них вход в систему под учетной записью администратора сети или локального компьютера;

3) использовать стойкие пароли.

Перечисленные меры защиты позволяют уменьшить риск заражения вредоносными программами через взломанные и фишинговые сайты, системы показа рекламной информации, заражение компьютеров самими пользователями, а также снизить риск взлома машин пользователей.

Рекомендуемые средства защиты

Средство защиты	Необходимость применения
Система централизованного управления	■ Позволяет исключить возможность отключения пользователями систем защиты. ■ Позволяет устанавливать единые для всей компании или групп пользователей правила информационной безопасности. ■ Позволяет в случае возникновения той или иной угрозы мгновенно менять настройки системы безопасности.
Система сбора и анализа статистики	Дает возможность контролировать уровень защищенности компании в режиме реального времени, определять источники заражения
Система сбора информации для служб технической поддержки	Позволяет исключить запуск вредоносных программ, проникших на машину пользователя без проверки, в том числе в запароленных архивах.
Система установки обновлений безопасности	Позволяет минимизировать возможность проникновения через известные уязвимости.

Скомпрометированные средства защиты

Средство защиты	Методы обхода системы защиты
Составление черных списков доменов, используемых майнерами	Использование вредоносными программами незарегистрированных доменов
Ручное удаление майнеров из зараженной системы	Использование майнерами средств маскировки, использование части ресурсов компьютера, деструктивные действия майнеров при попытке их удаления

Пример настройки средств защиты

В качестве примера рассмотрим настройку системы ограничения доступа для операционной системы Windows.

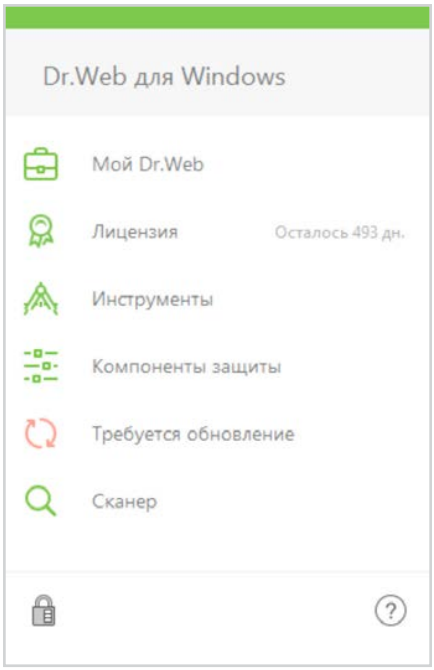
Внимание! В связи с тем, что майнеры существуют для всех операционных систем — защищена должна быть любая — в том числе операционные системы семейств Windows, Linux, Android.

Защита системы ограничения доступа на уровне отдельной рабочей станции

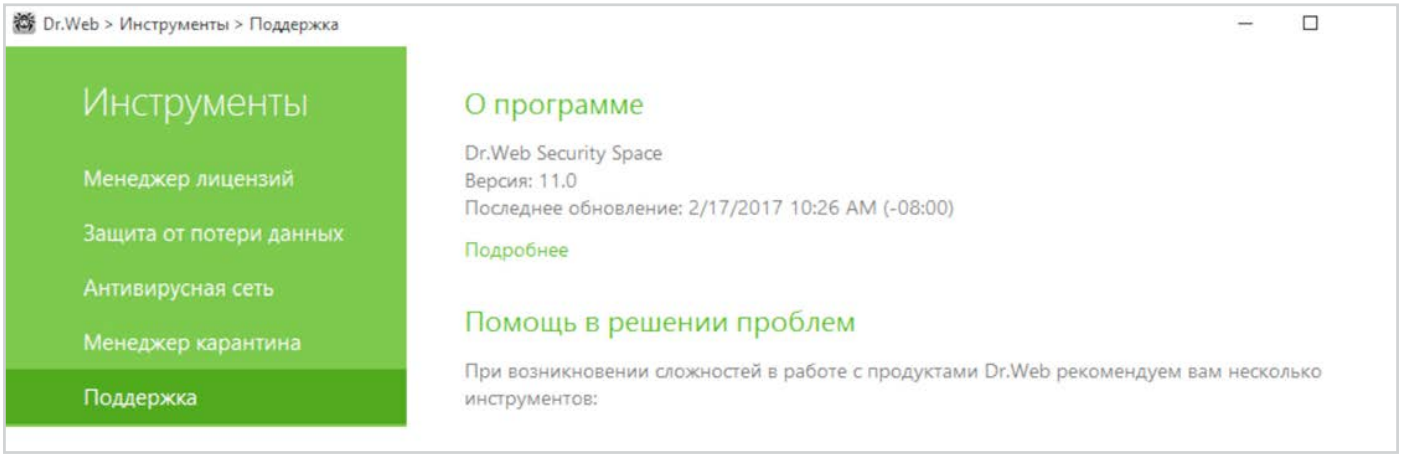
1. Убедитесь, что используемая вами версия антивируса является актуальной, а лицензия — действующей

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.**



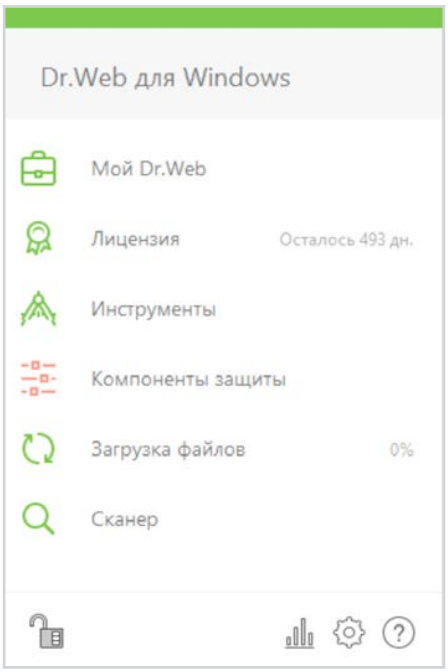
Внимание! Текущая версия антивируса Dr.Web Security Suite — 11. Использование неактуальных версий антивирусных программ увеличивает риск заражения в связи с отсутствием в них новейших технологий детектирования.

2. **Убедитесь, что все компоненты антивирусной защиты** (в том числе модули Превентивной защиты, Dr.Web SpIDer Gate, Антиспам Dr.Web и Брандмауэр Dr.Web) **установлены и не отключены.**

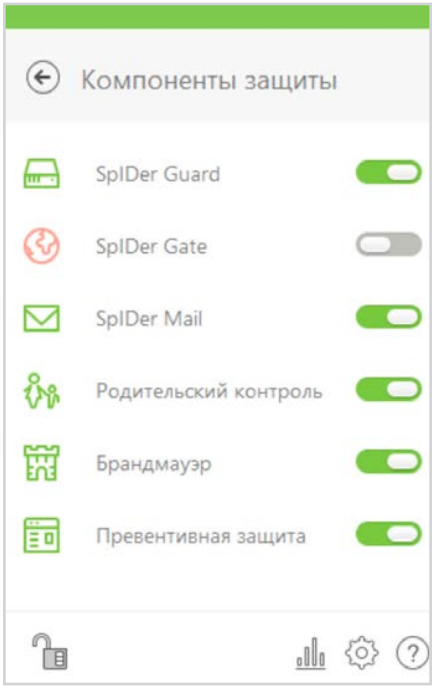
Лишних компонентов в антивирусе Dr.Web нет! В качестве примера можно привести Антиспам Dr.Web. Тестирование данного модуля показало, что он отфильтровывает более 90% неизвестных вредоносных программ, рассылаемых злоумышленниками, по признакам распространения мошеннических писем. И это без использования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

Отключение модуля Dr.Web SpIDer Gate может привести к тому, что вредоносные скрипты будут запускаться браузером без помех.

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



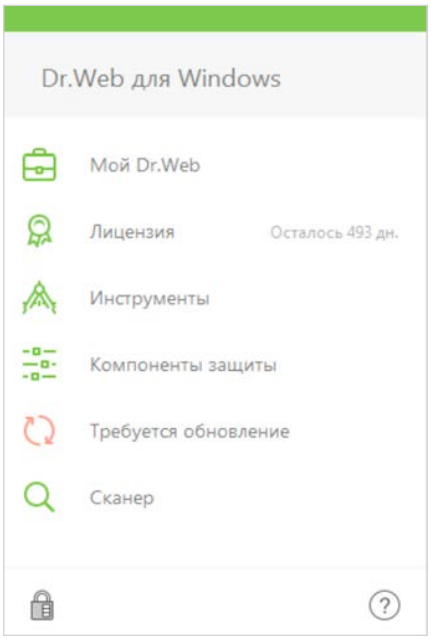
Отсутствие значка агента может означать, что антивирус выгружен и компьютер остался без антивирусной защиты.
Узнать, какие компоненты отключены, можно, кликнув на значок агента и далее на пункт **Компоненты защиты.**



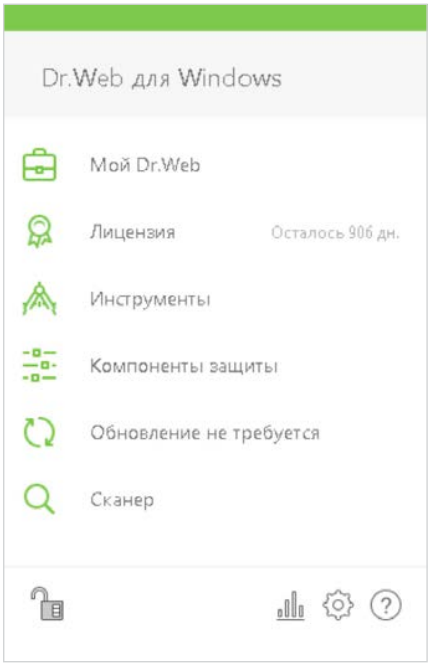
3. **Убедитесь, что все обновления антивируса установлены,** включая обновления, требующие перезагрузки в целях установки новых драйверов перехвата и исправления потенциальных уязвимостей защиты.

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.

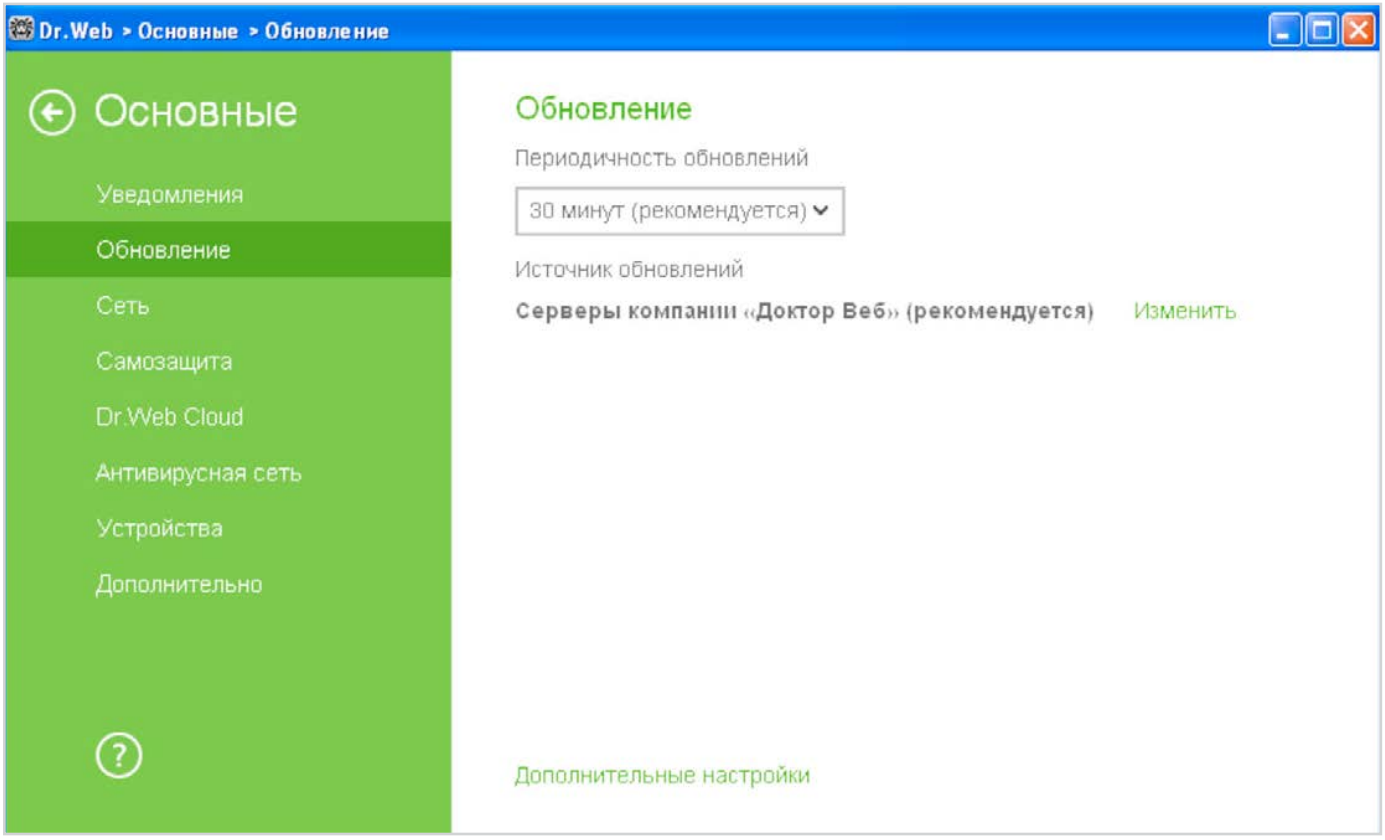
Для того чтобы проверить статус обновлений, кликните на значок  . Статус обновлений будет показан в открывшемся меню.



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



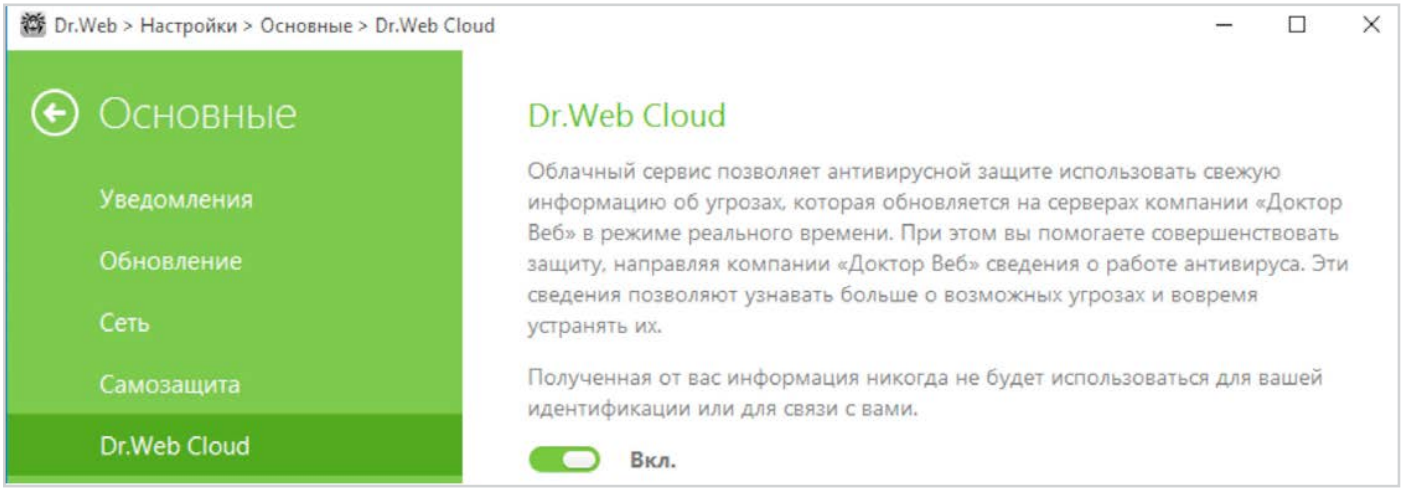
В открывшемся окне **Настройки** выберите **Основные** → **Обновление**.



Не рекомендуется увеличивать период между обновлениями более 1 часа.

4. **Включите 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**.



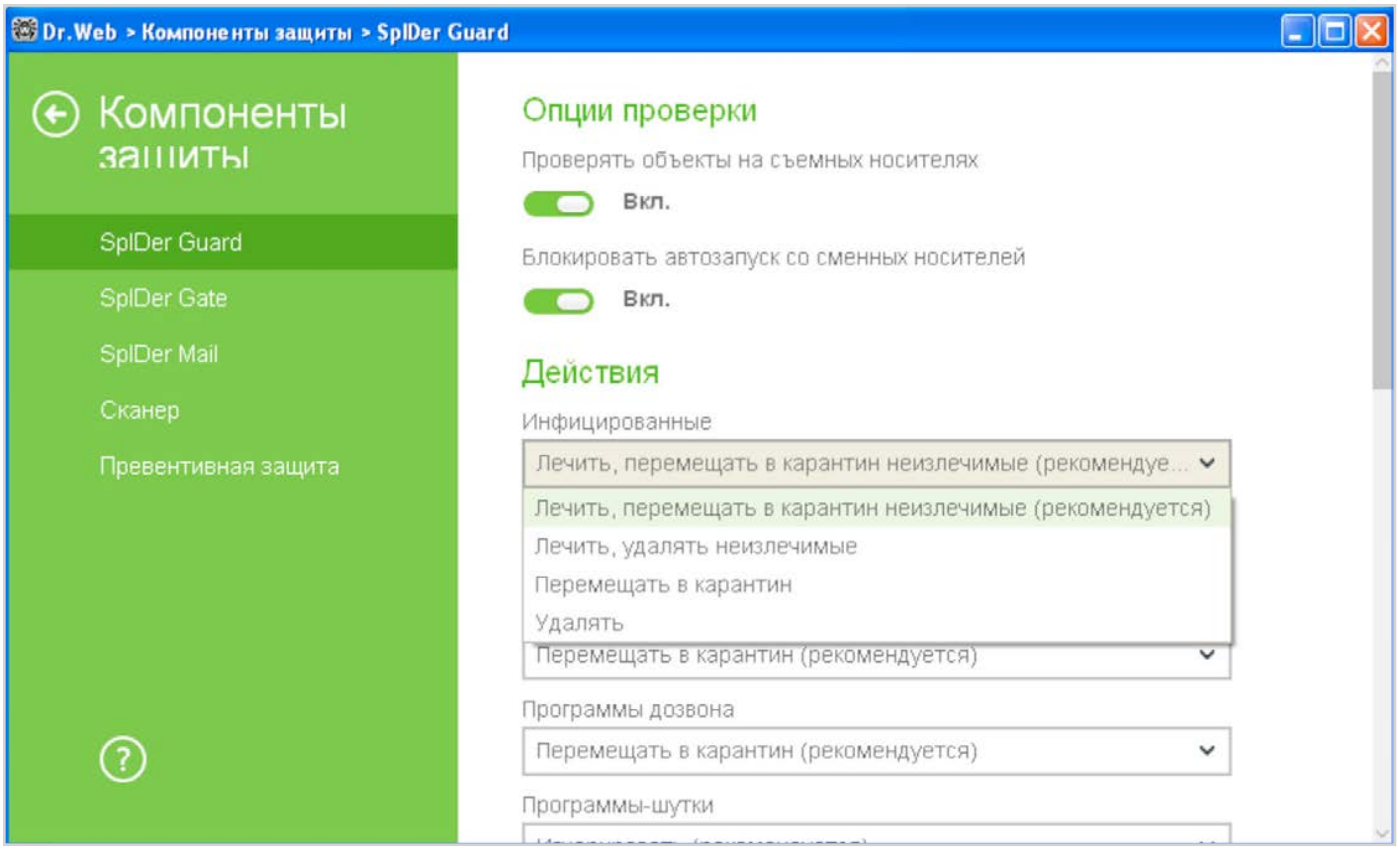
5. **Настройте действия антивируса Dr.Web по отношению к вредоносным программам-майнерам**

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**.

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**.

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 **SplDer 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 SplDer Gate.

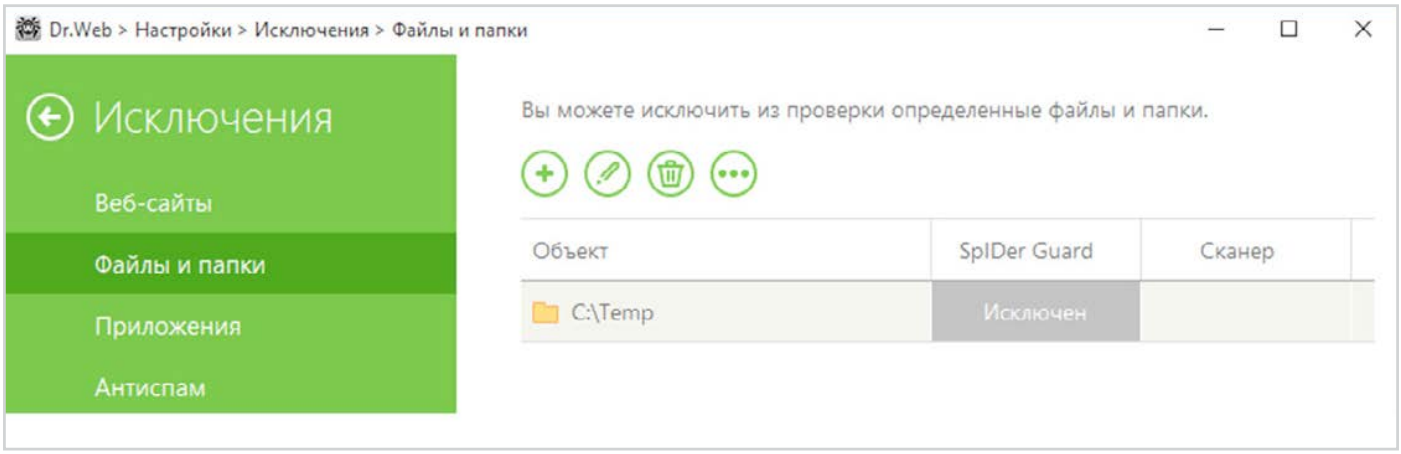
6. В случае необходимости настройте исключения из антивирусной проверки

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.

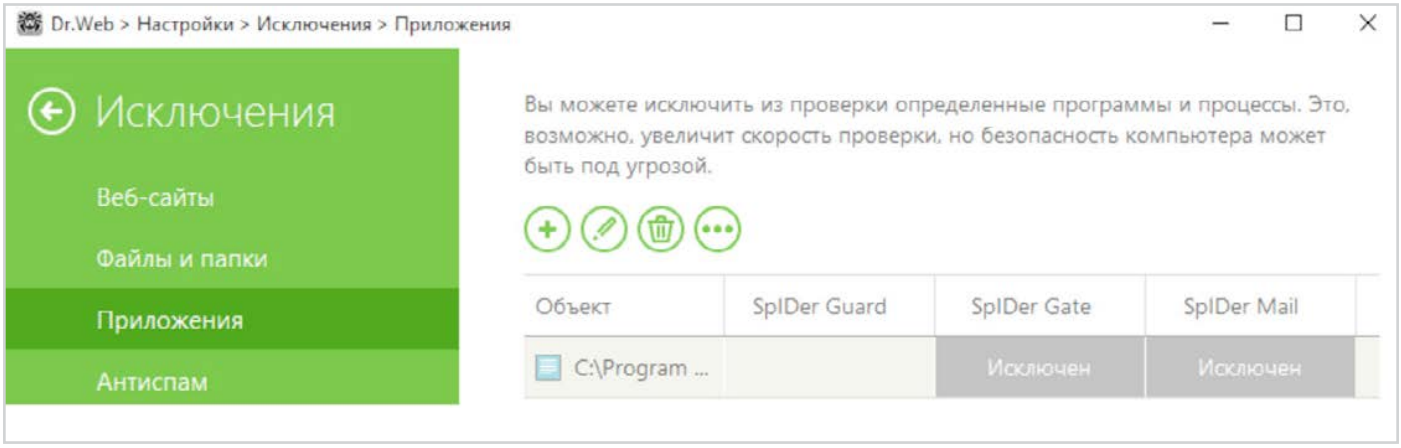
Если вы уверены, что установленный вами майнер не является вредоносным, вы можете разрешить его использование, используя **Исключения.**

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 проверяется и будут пропущены. В случае маски *.exe будут пропущены все исполняемые файлы.

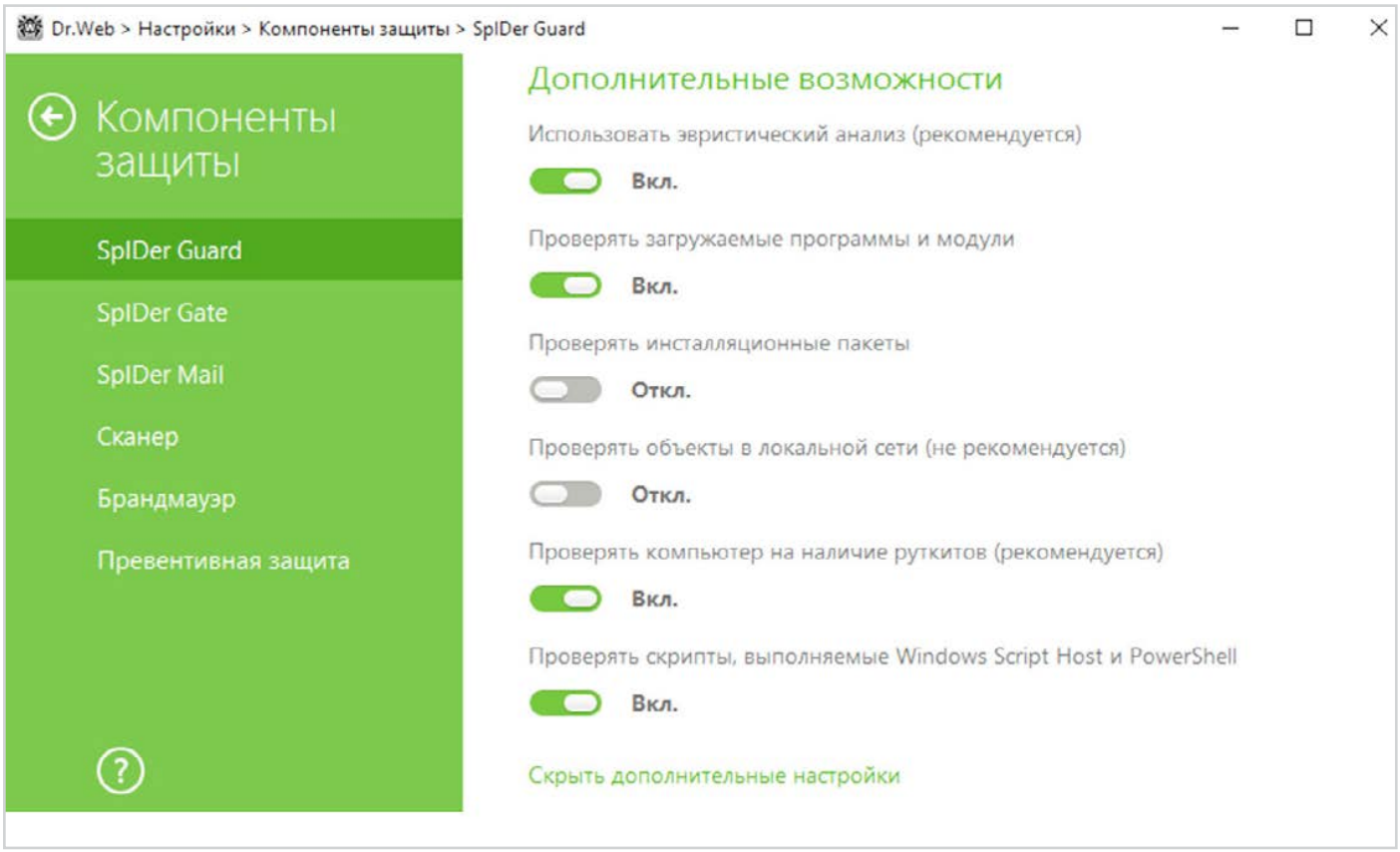
Внимание! Не рекомендуется исключать проверку трафика для используемых программ — в таком случае никакое вредоносное ПО, загруженное данными программами, проверяться не будет.



7. Убедитесь, что ваша антивирусная защита использует систему обнаружения вредоносных скриптов

Используемая в Dr.Web Security Space 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 вирусописателями 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.

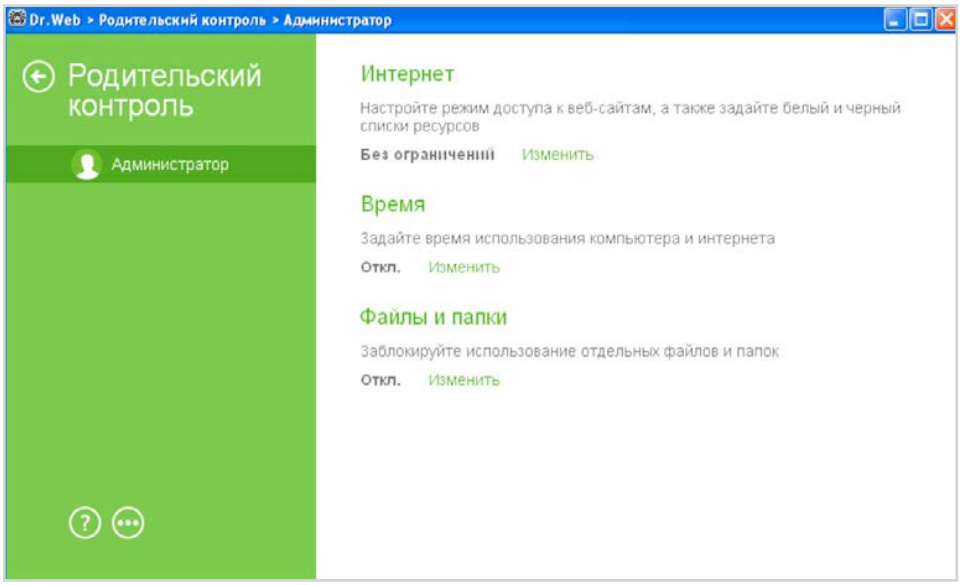


Внимание! Установка и удаление модуля Dr.Web Amsi-client производится совместно с модулем Dr.Web SpIDer Guard. Модуль доступен при использовании Антивируса Dr.Web и Dr.Web Security Suite в операционных системах начиная с Windows 10 (x86, x64), а также Windows Server 2016.

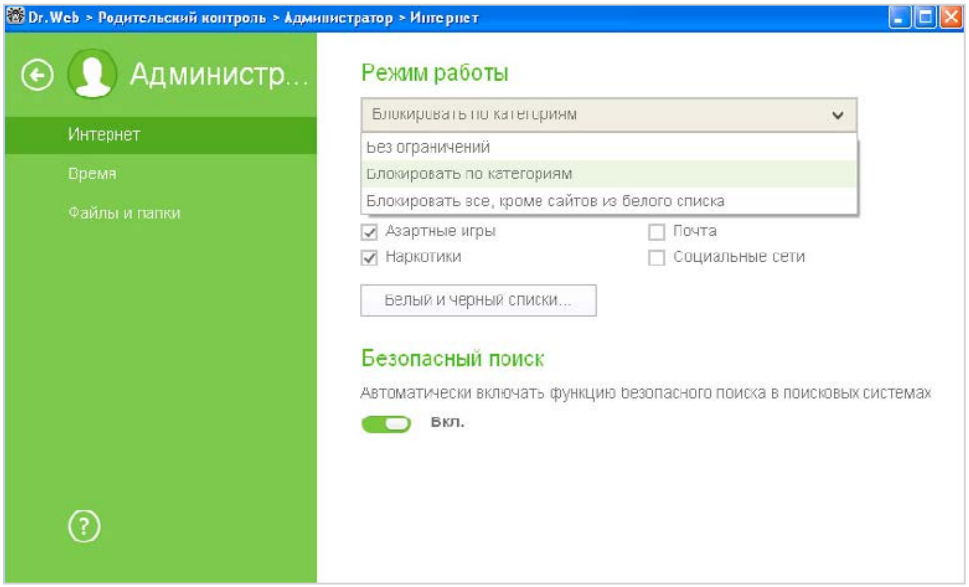
8. Ограничьте доступ к заведомо вредоносным сайтам с помощью настроек Офисного/Родительского контроля

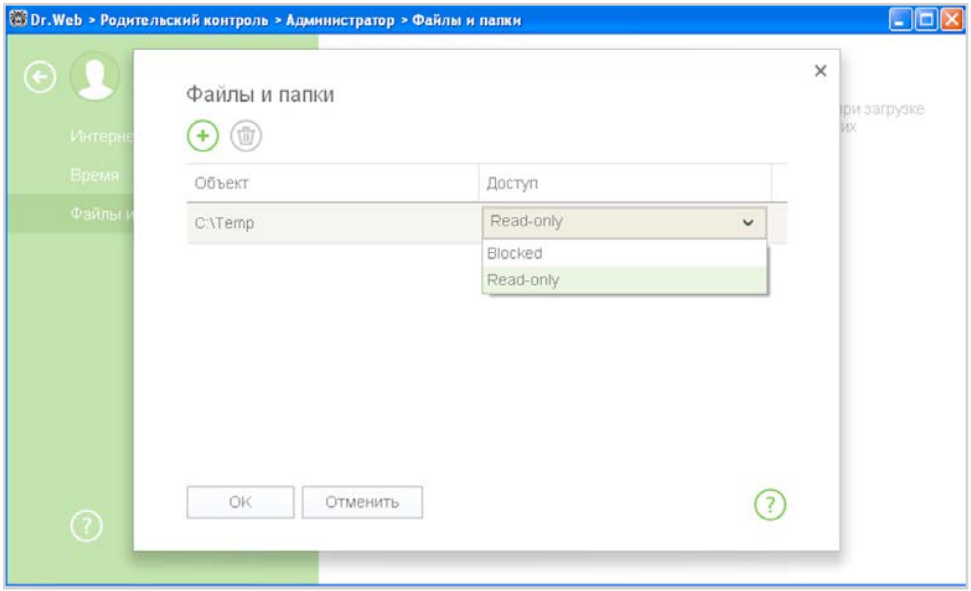
Троянец-майнер может проникнуть в локальную сеть или на отдельный компьютер через спам (как правило, сообщение содержит вредоносное вложение или специально сформированную ссылку), с помощью сообщения мессенджера (также содержащего ссылку), путем загрузки файла (например, Java-скрипта) пользователем с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



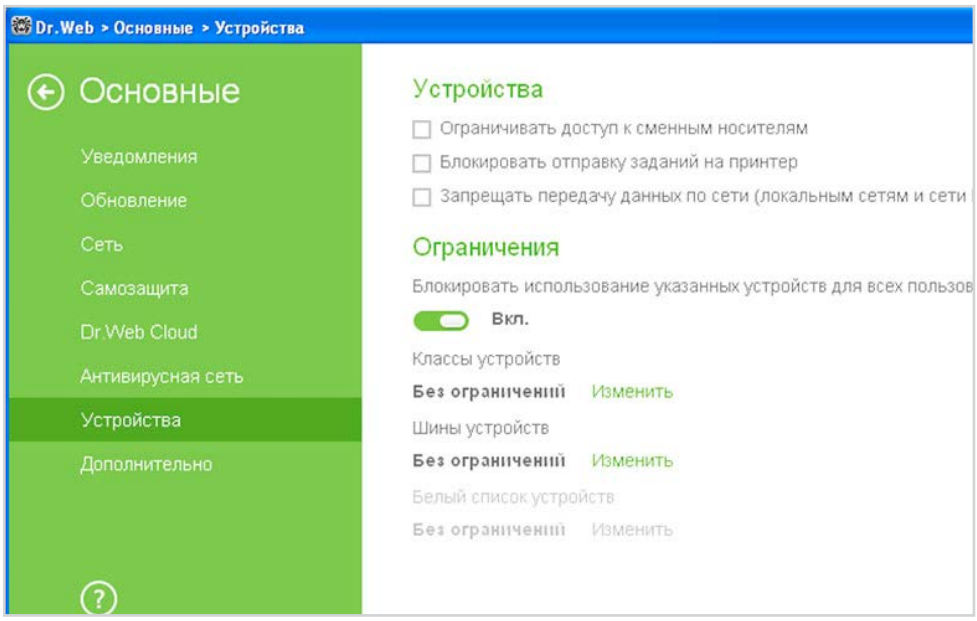
В открывшемся окне выберите пользователя, для которого необходимо настроить ограничения и сделать необходимые настройки.



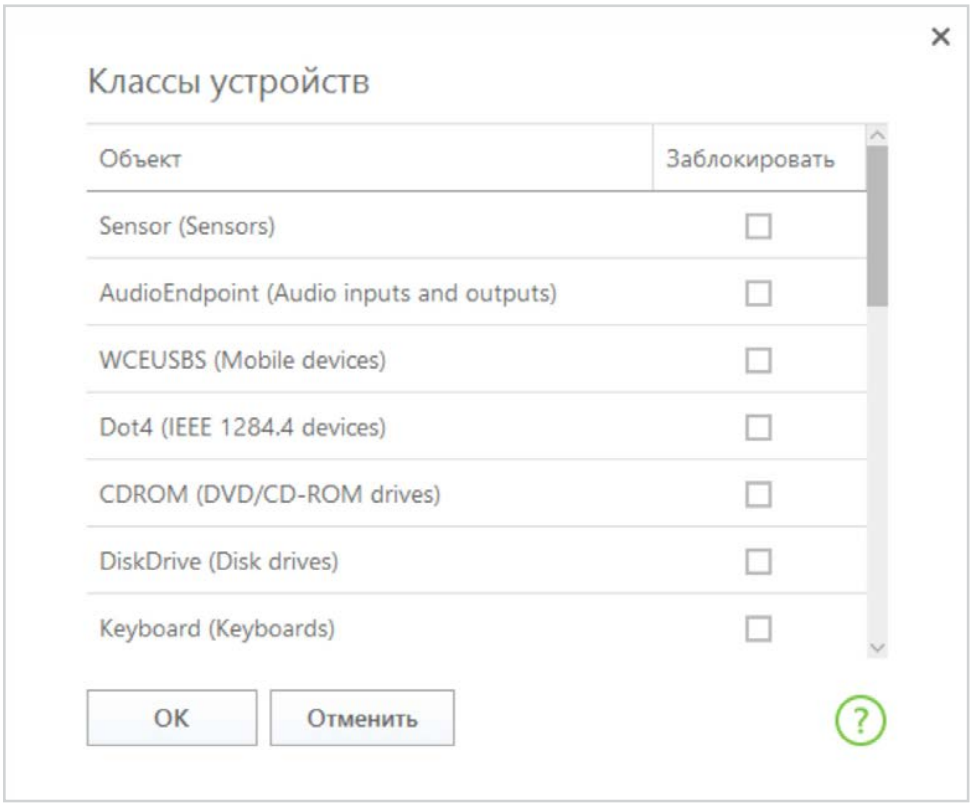


По умолчанию ограничения отключены.

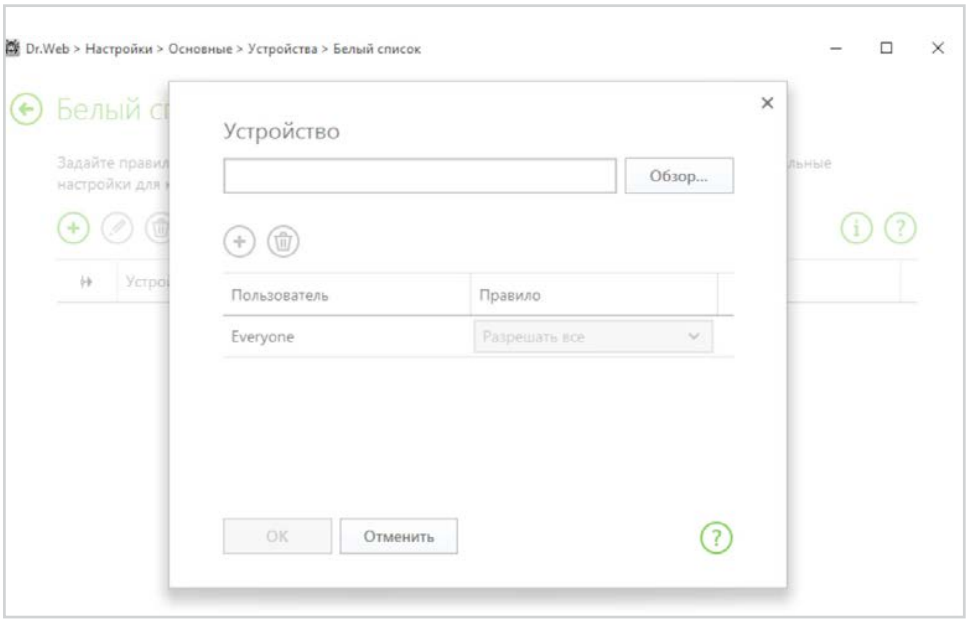
Для настройки ограничений к сменным носителям в окне **Настройки** выберите **Основные** → **Устройства.**



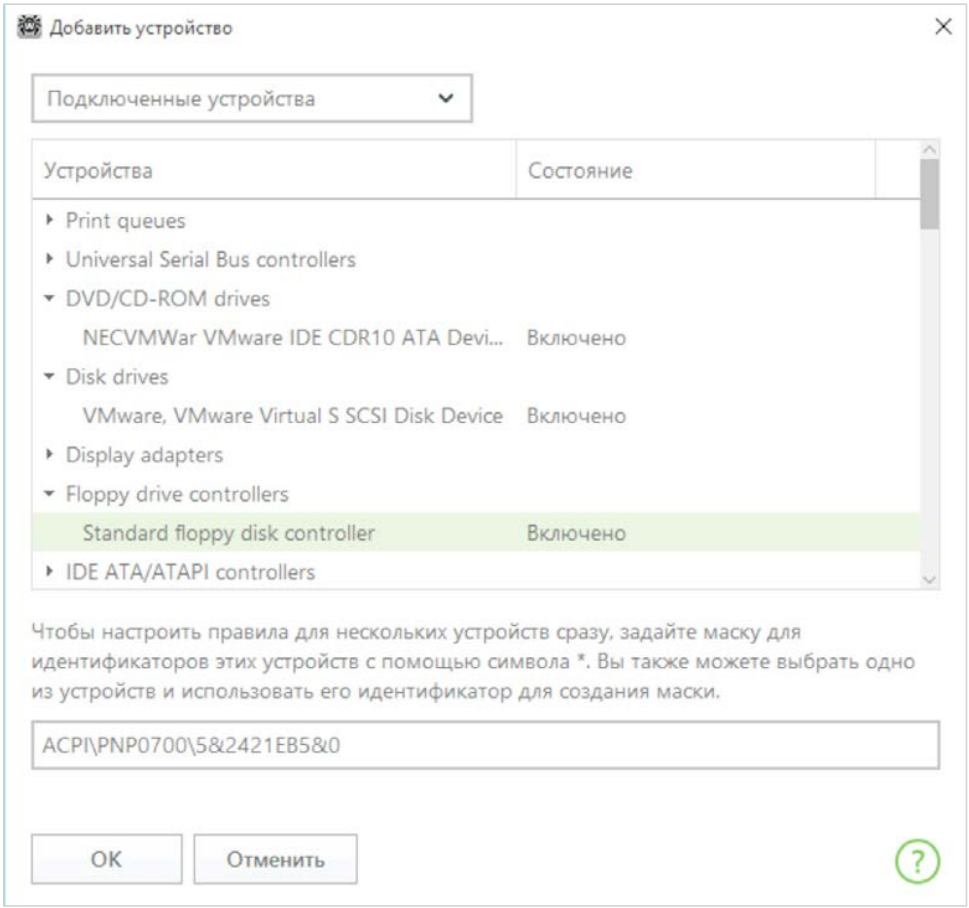
В данном окне выберите **Ограничивать доступ к сменным носителям.** Далее нажмите на **Изменить** для классов устройств и выберите необходимые классы устройств.



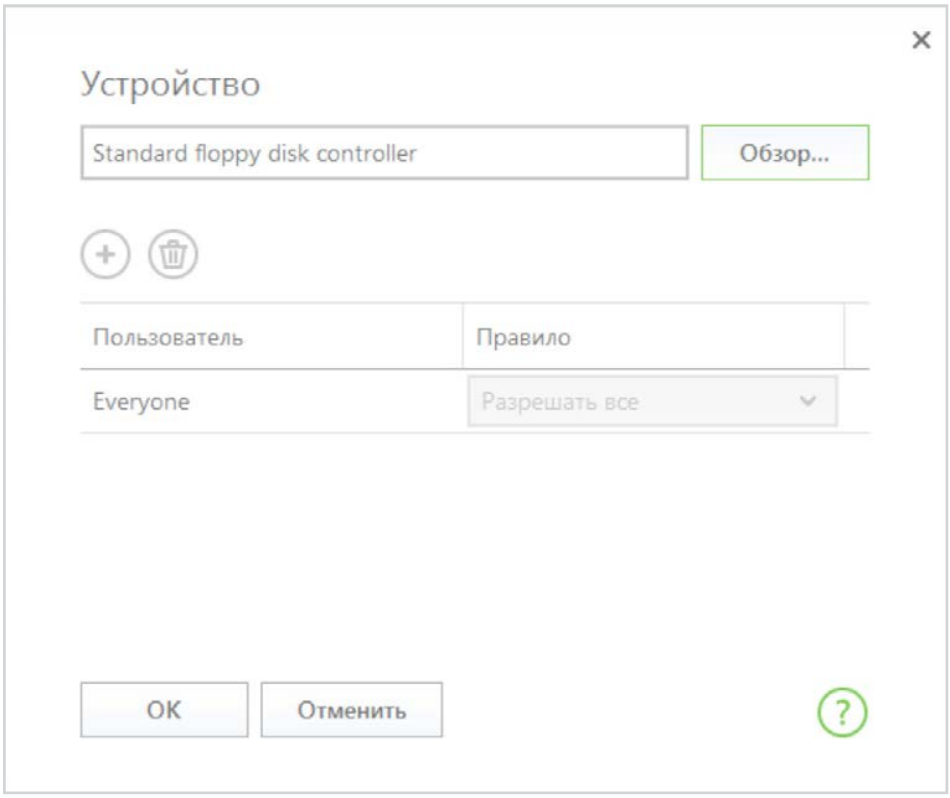
После этого появится возможность настройки для раздела **Белый список устройств.** Если необходимо использовать только разрешенные сменные носители, нажмите на **Изменить** → **.** →



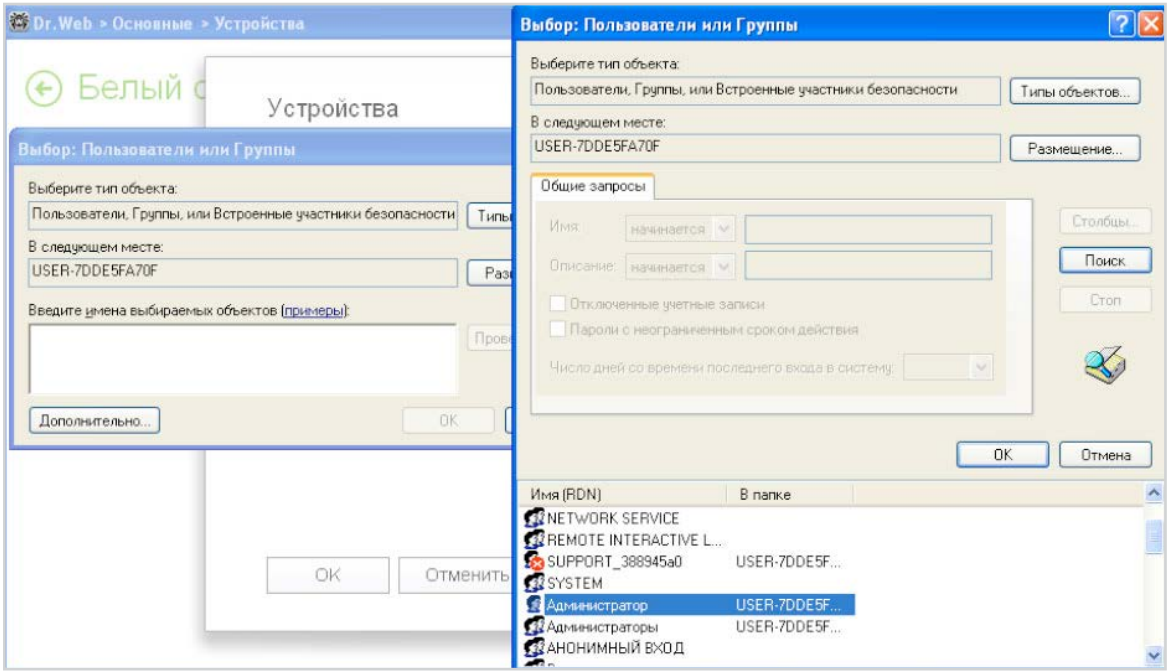
В открывшемся окне нажмите **Обзор** и выберите необходимое устройство.



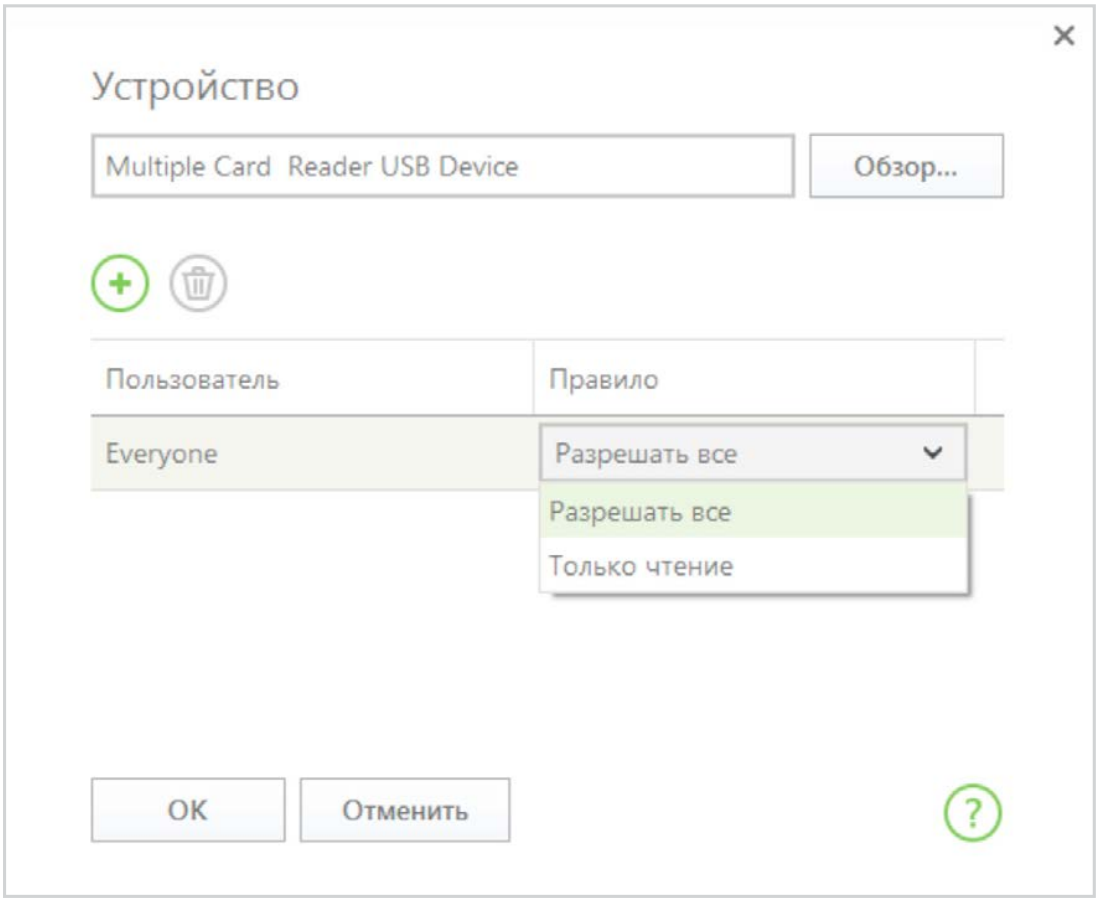
Подтвердите выбор, нажав **OK.**



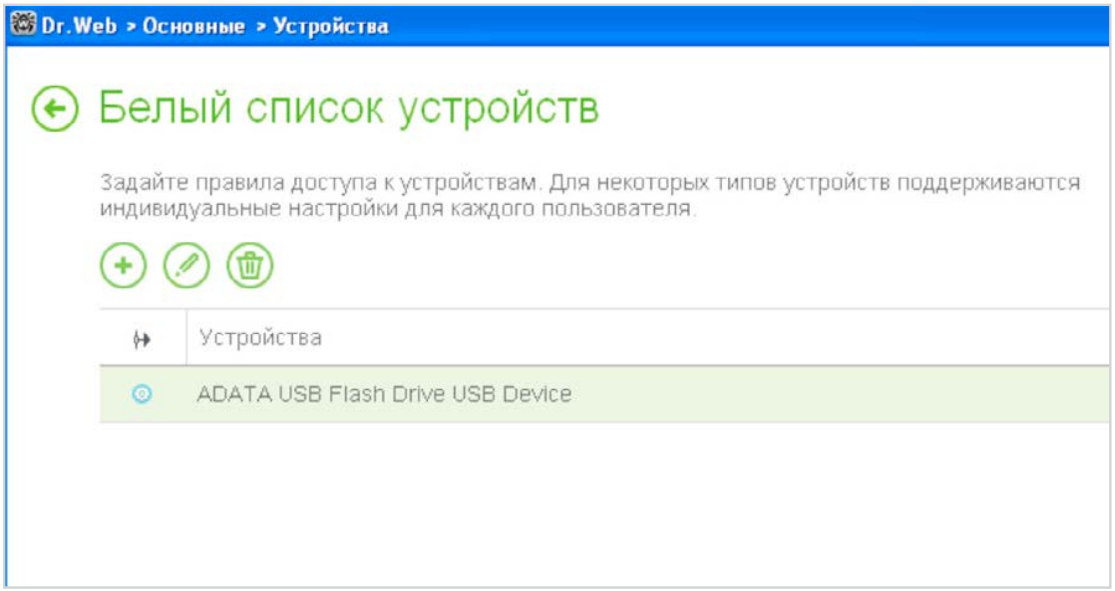
Если необходимо разрешить использование данного носителя только для определенных пользователей компьютера, нажмите ⊕ и выберите необходимого пользователя.



Укажите права по использованию данного устройства.

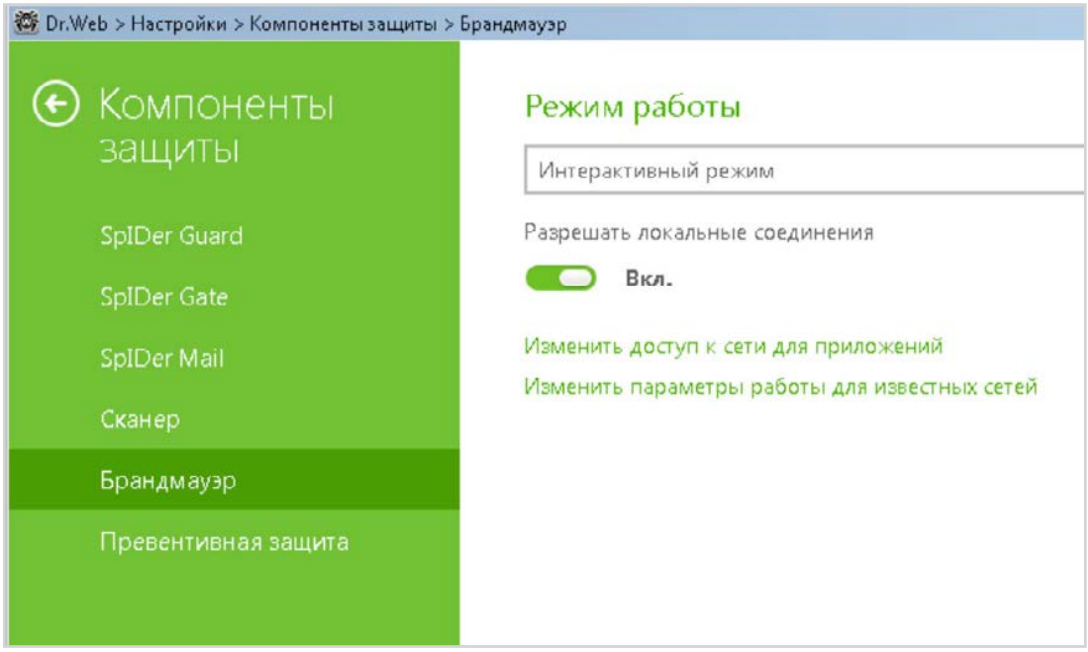


Подтвердите выбор.



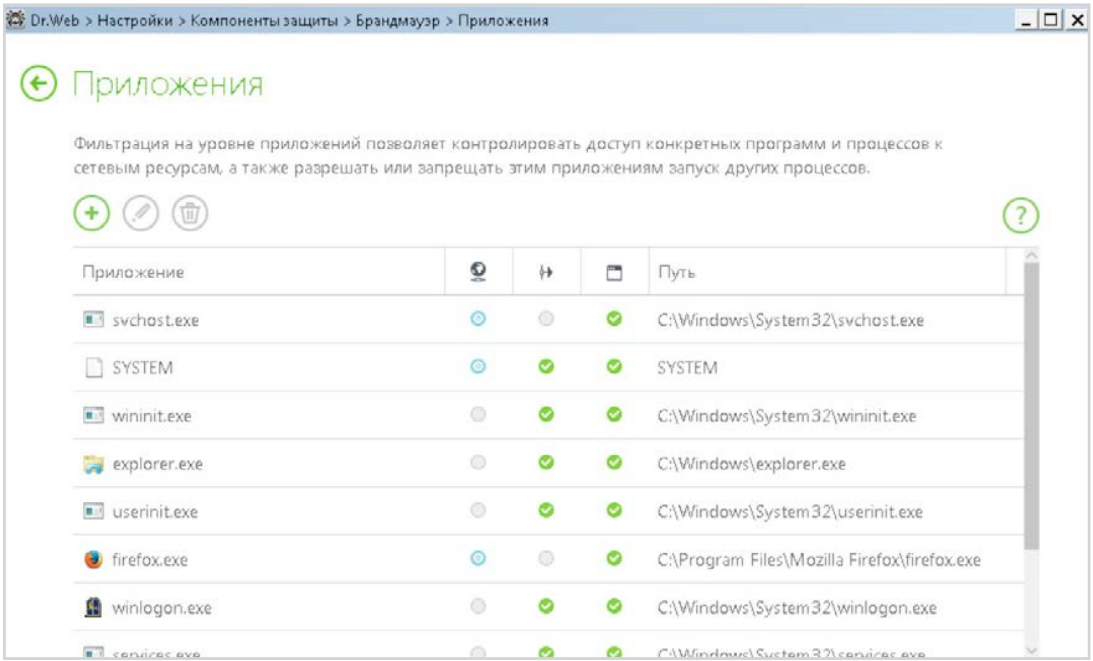
9. **Доступ используемых программ в сеть Интернет должен быть ограничен** — это можно сделать с помощью компонента Брандмауэр.

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.

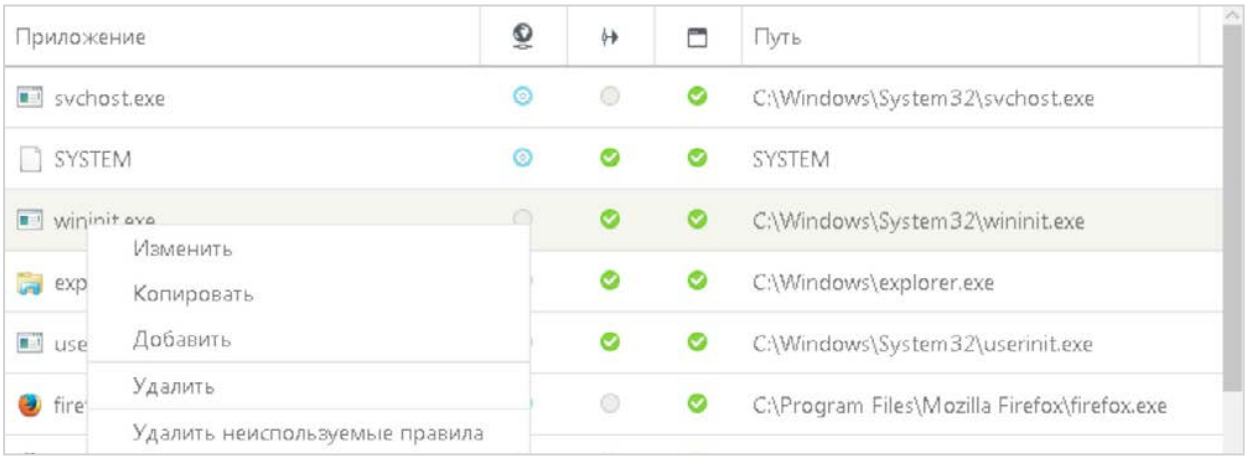
Для каждой программы может быть не более одного набора правил фильтрации.



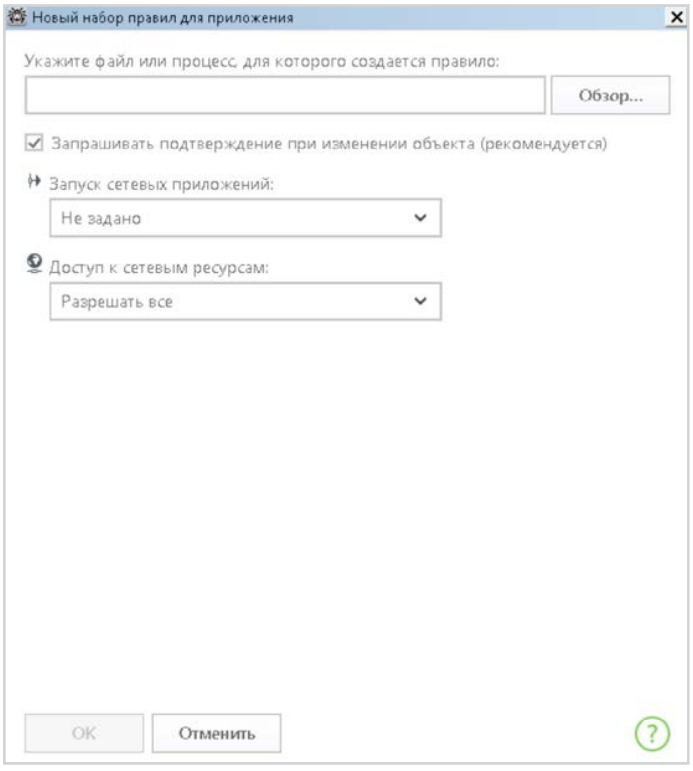
Для доступа к этому окну в настройках **Брандмауэра** нажмите **Изменить доступ к сети для приложений** и нажмите кнопку или выберите приложение и нажмите кнопку .

Для формирования набора правил выполните одно из следующий действий.

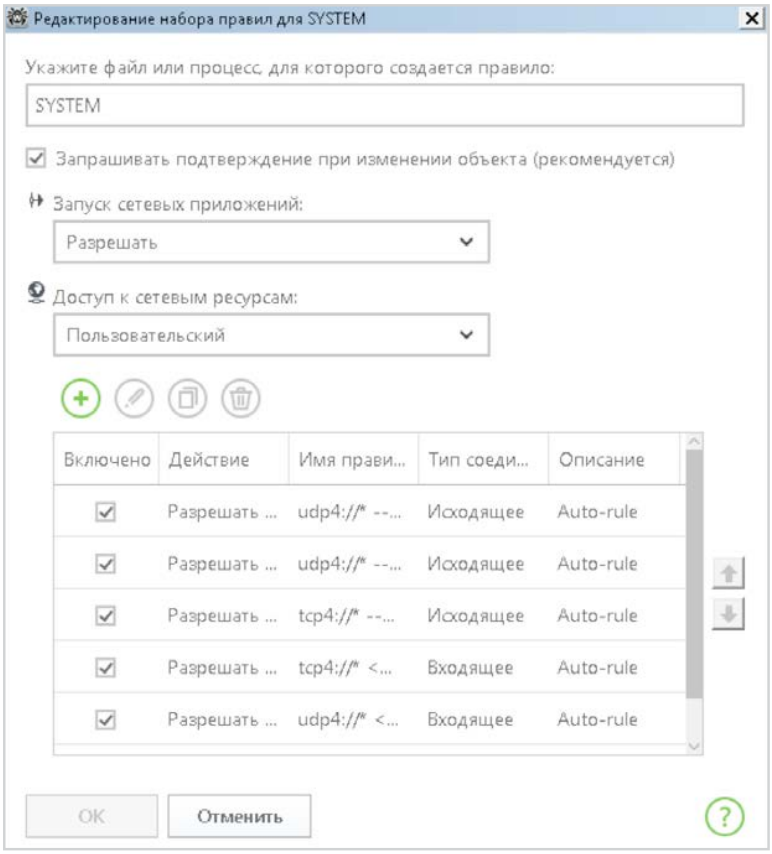
- Чтобы создать набор правил для новой программы, нажмите кнопку **(Создать).**
- Чтобы отредактировать существующий набор правил, выберите его в списке и нажмите кнопку **(Изменить).**
- Чтобы добавить копию существующего набора правил, выберите **Копировать** в контекстном меню. Копия добавляется под 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.

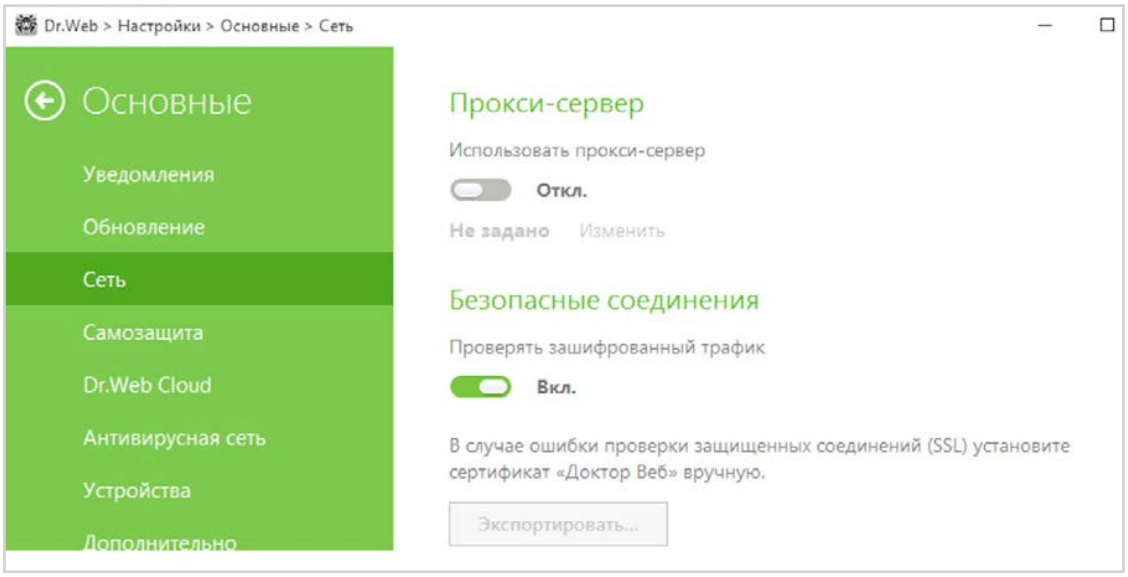


Вы можете создать правило при помощи окна настроек **Брандмауэра.** При работе в режиме обучения вы можете инициировать создание правила непосредственно из окна оповещения о попытке несанкционированного подключения.



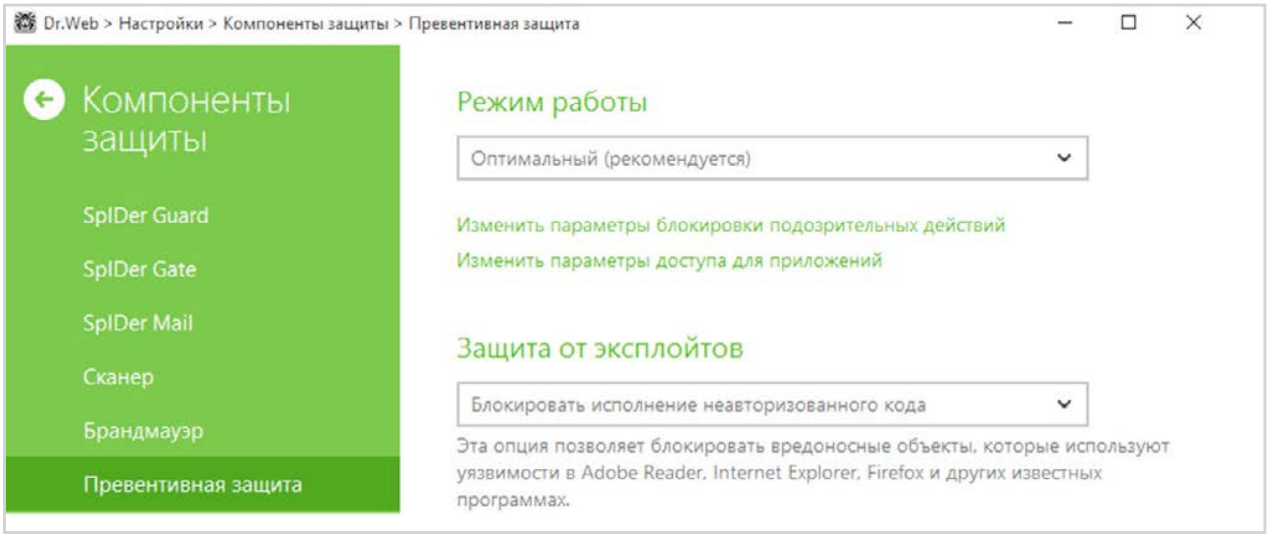
10. На данный момент до половины трафика сети Интернет зашифровано, чем могут воспользоваться злоумышленники.

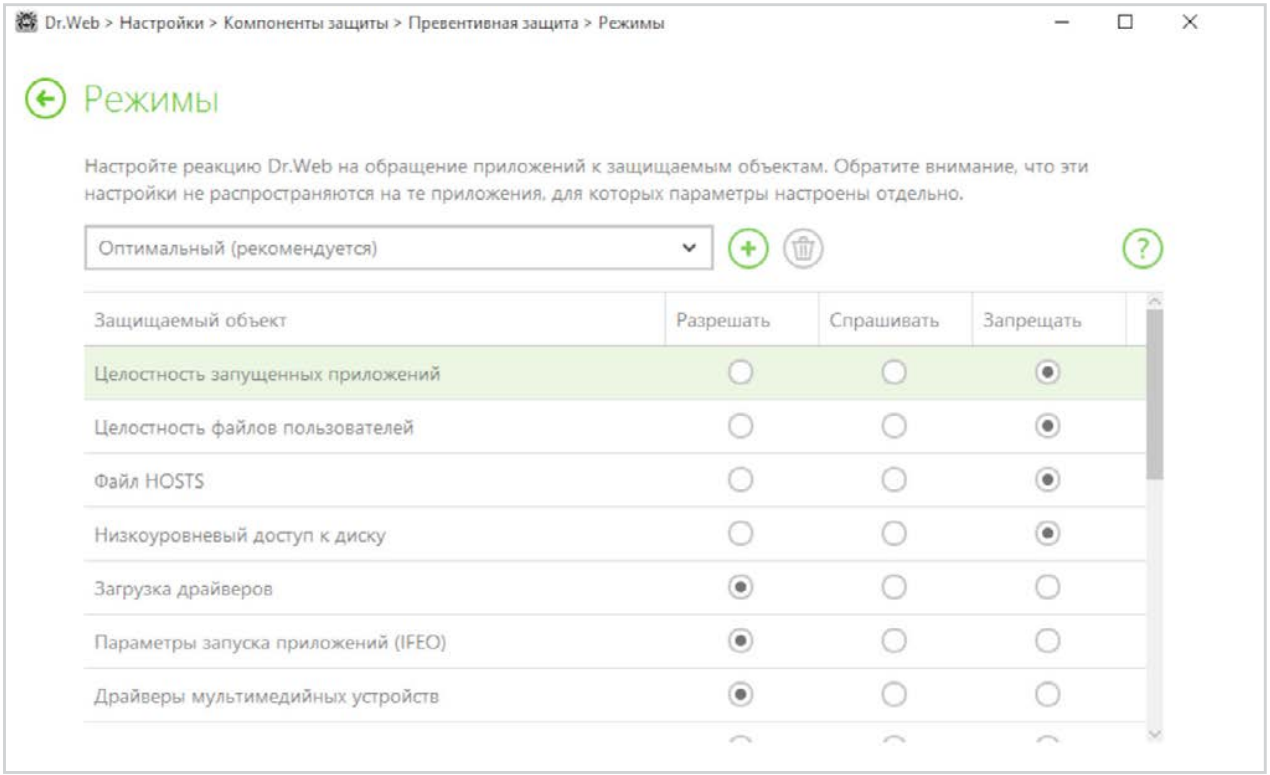
Включите проверку зашифрованного трафика (функционал доступен для Dr.Web Security Space): кликните на значок в системном меню, затем в открывшемся меню последовательно нажмите на **(Режим администратора)** и появившийся значок **(Настройки)**. В открывшемся окне **Настройки** выберите пункт **Основные**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



11. Настройки Dr.Web Process Heuristic не должны позволять внедрение майнерами эксплойтов 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.**



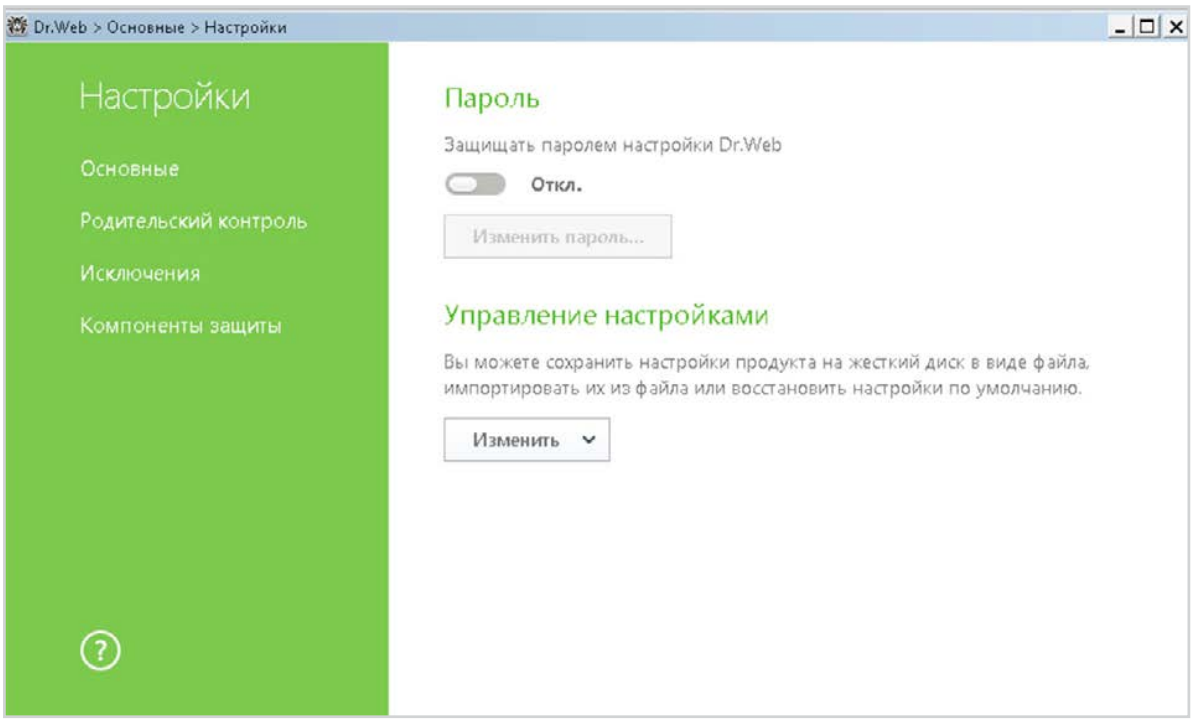


Статус **Разрешить** разрешает внесение изменений в соответствующие ресурсы пользователям и злоумышленникам.

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.

Защита системы ограничения доступа с помощью централизованной системы управления

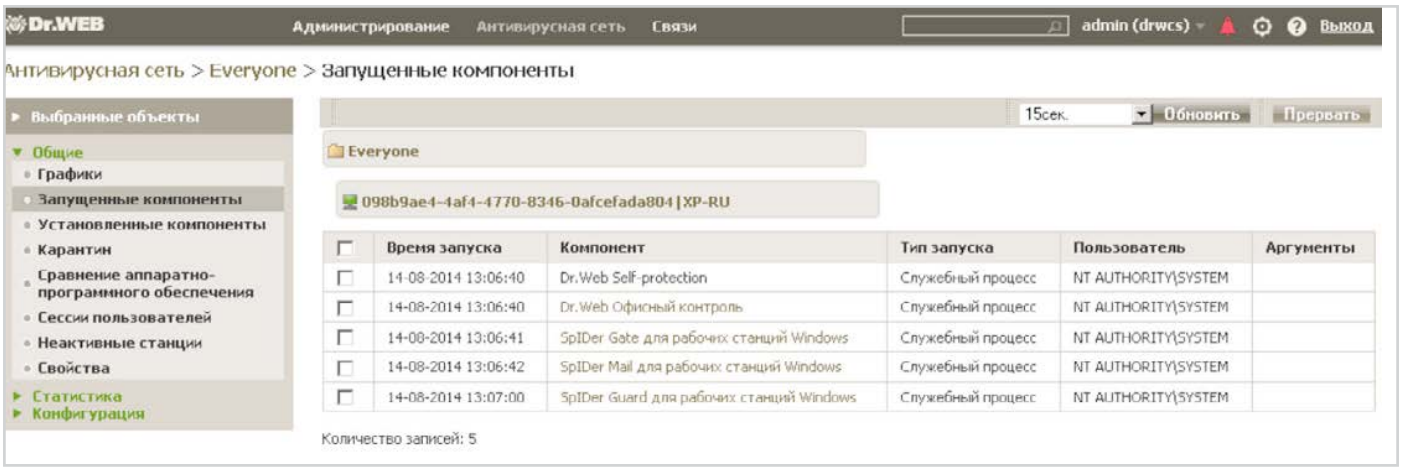
1. Убедитесь, что используемая вами версия антивируса является актуальной, а лицензия — действующей

Для того чтобы проверить актуальность лицензии, перейдите на страницу **Менеджер лицензий** раздела **Администрирование.**

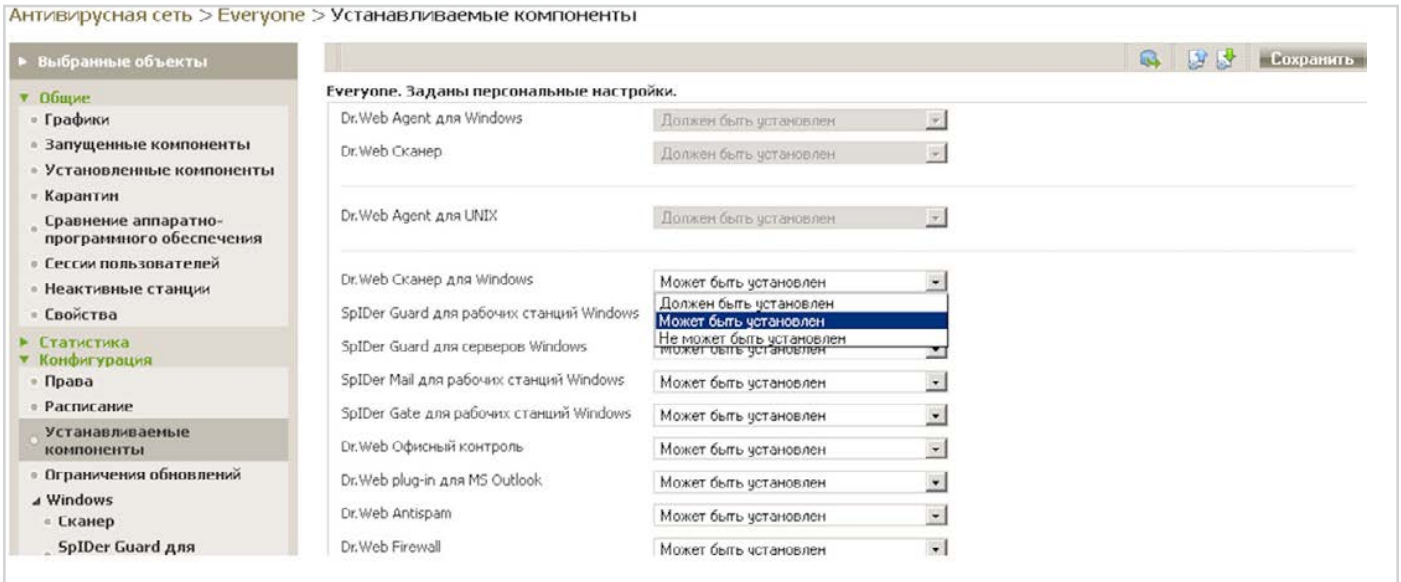
На этой же странице можно проверить актуальную версию антивирусного сервера.
Проверить наличие обновлений компонентов антивируса можно на странице **Состояние репозитория.**

2. **Убедитесь, что все компоненты антивирусной защиты** (в том числе модули Превентивной защиты, Dr.Web SpIDerGate, Антиспам Dr.Web и Брандмауэр Dr.Web) **установлены и не отключены.**

Администратор может контролировать все запущенные процессы. Для этого необходимо выбрать станцию, а затем пункт **Запущенные компоненты.**



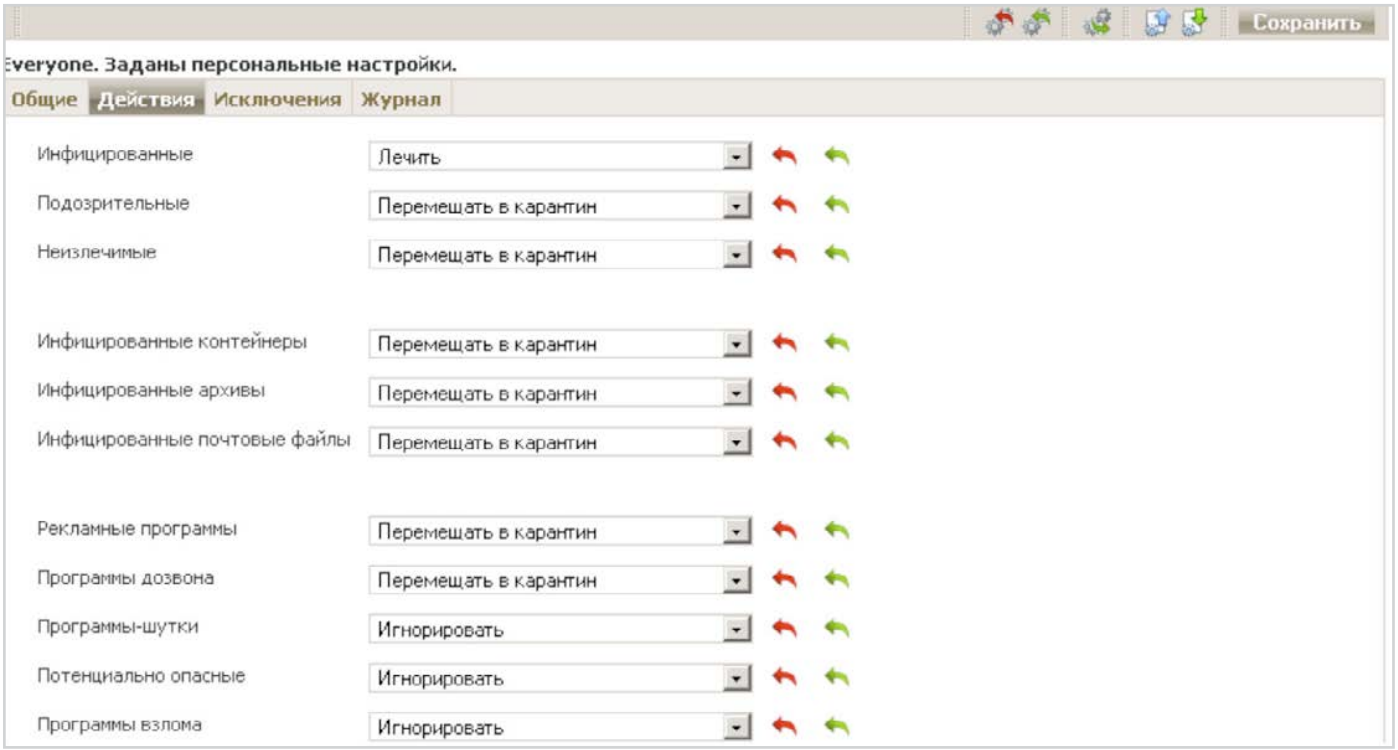
Проверить список устанавливаемых компонентов можно, выбрав пункт



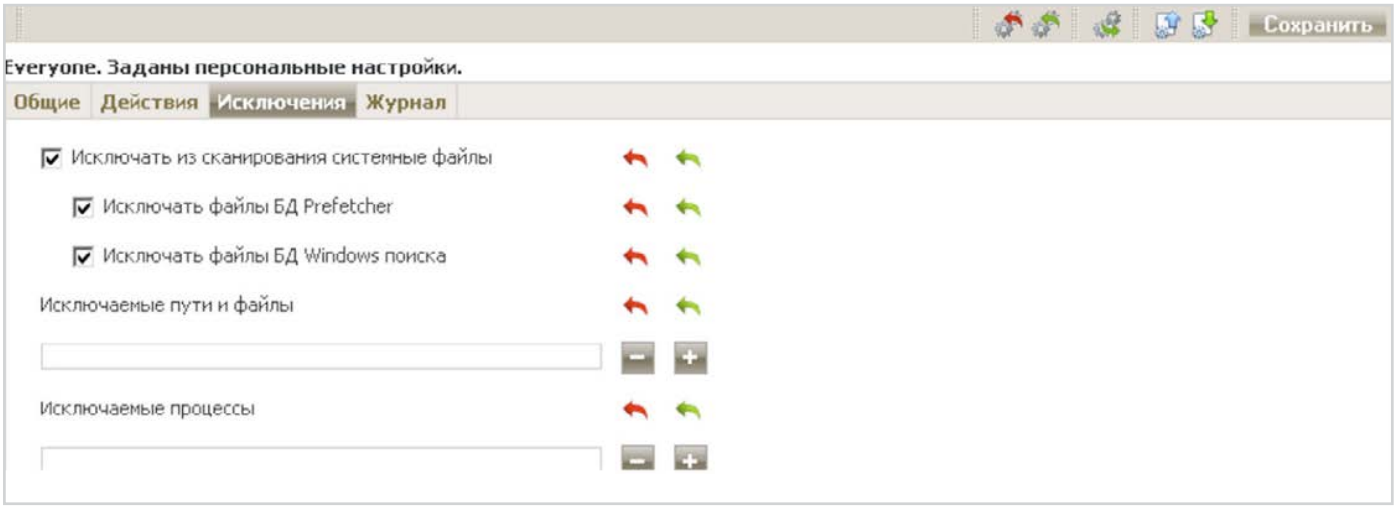
3. Настройте действия антивируса по отношению к вредоносным программам-майнерам

Настроить параметры защиты рабочих станций и серверов, а также групп станций можно, выделив соответствующий объект в дереве антивирусной сети, выбрав соответствующий пункт в группе настроек **Конфигурация** и далее перейдя на закладку **Действия.**

Действия программы для различных типов вредоносных объектов:

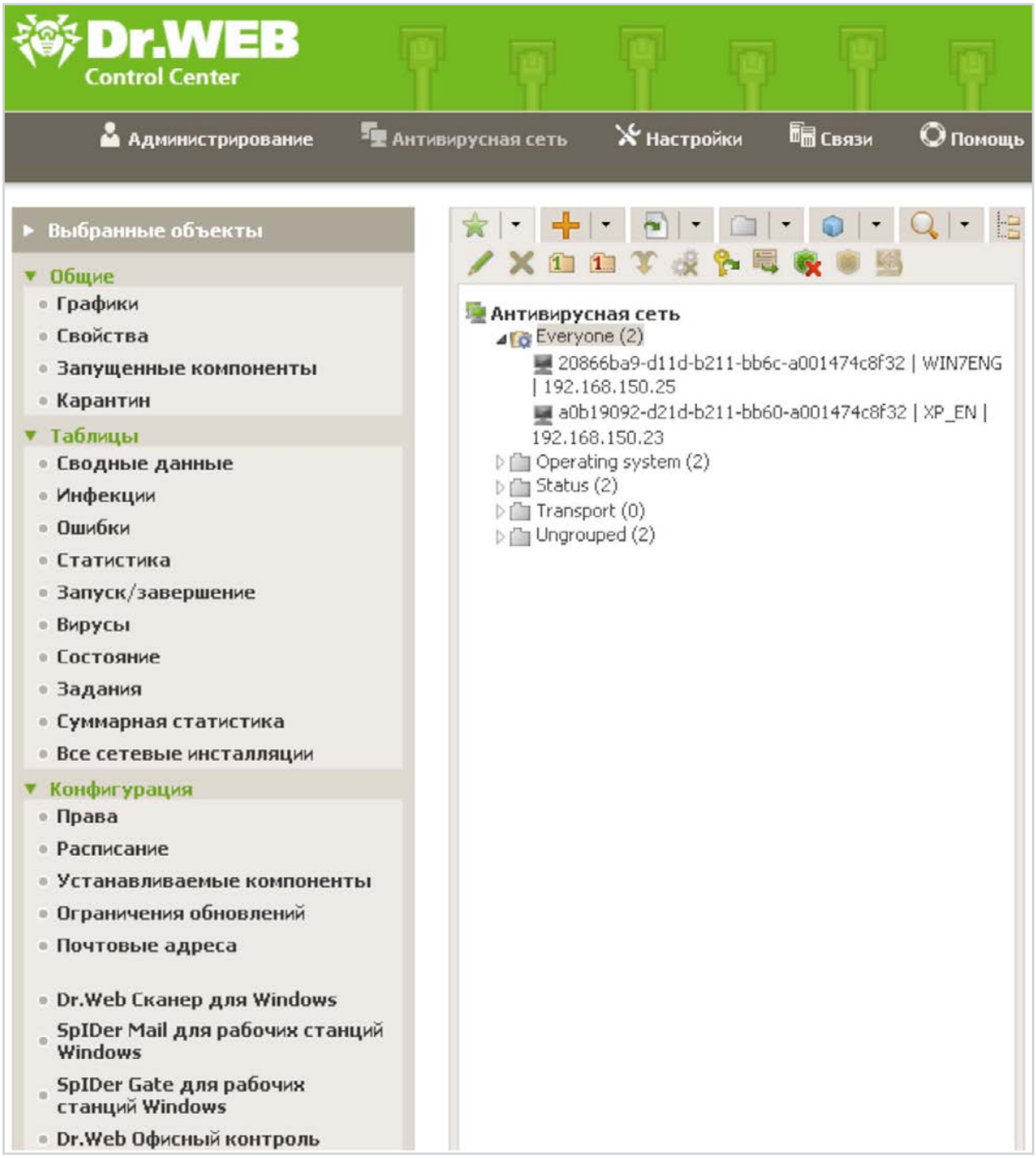


В случае необходимости исключаемые из проверки пути и маски файлов указываются на закладке **Исключения:**

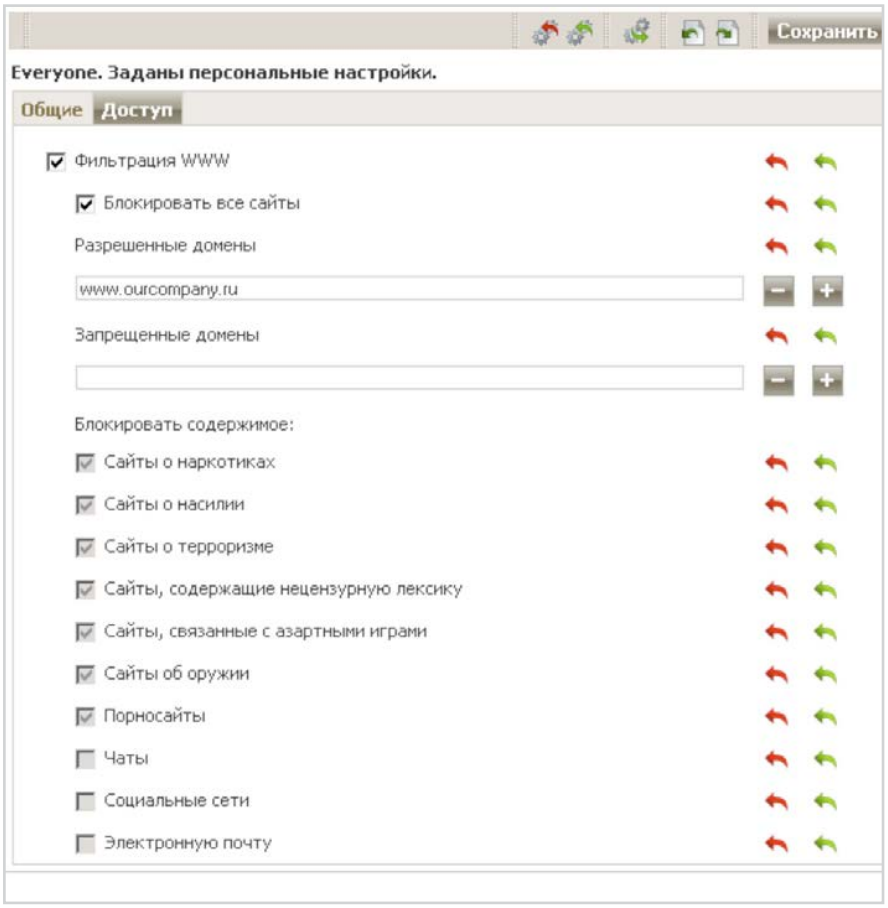


4. Ограничьте доступ к заведомо вредоносным сайтам с помощью настроек Офисного/Родительского контроля

Для настройки параметров доступа необходимо в окне системы управления выбрать предустановленную группу Everyone или (в случае необходимости задания индивидуальных правил безопасности) любую иную группу либо отдельную станцию, а затем выбрать пункт **Офисный контроль.**

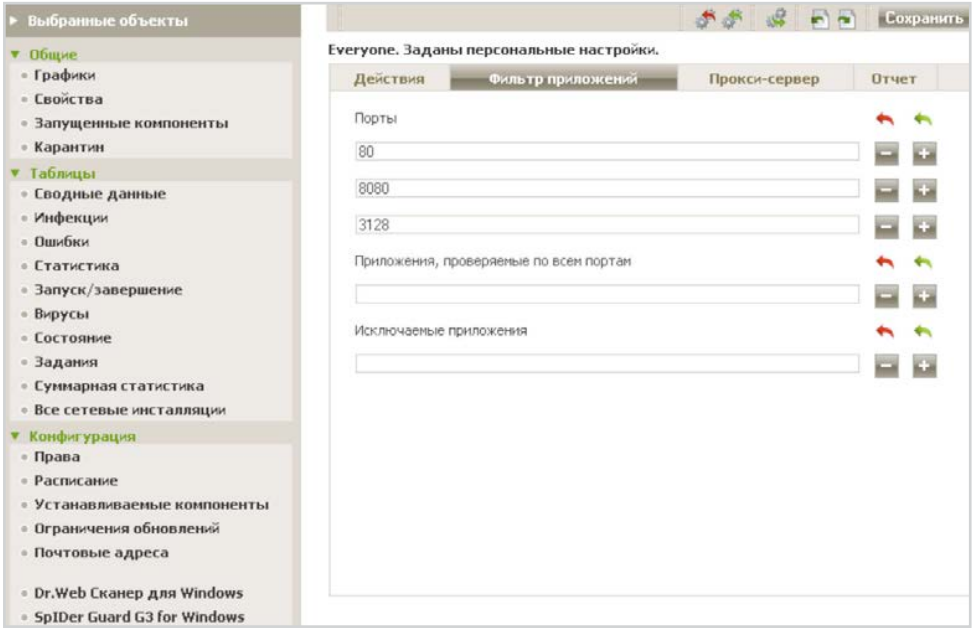


На странице **Офисный контроль** необходимо, выбрав закладку **Доступ**, отметить **Фильтрация WWW**, определить режим блокировки **Блокировать все сайты** и задать список разрешенных сайтов.

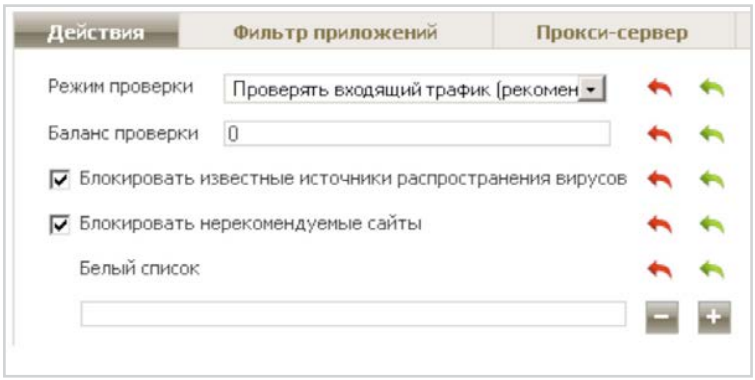


Для сохранения настроек необходимо нажать кнопку **Сохранить.**

После этого рекомендуется с помощью настроек модулей **SpIDer Gate для рабочих станций Windows** (закладка **Фильтр приложений**) и **Firewall** определить список приложений, которым запрещен выход в Интернет.

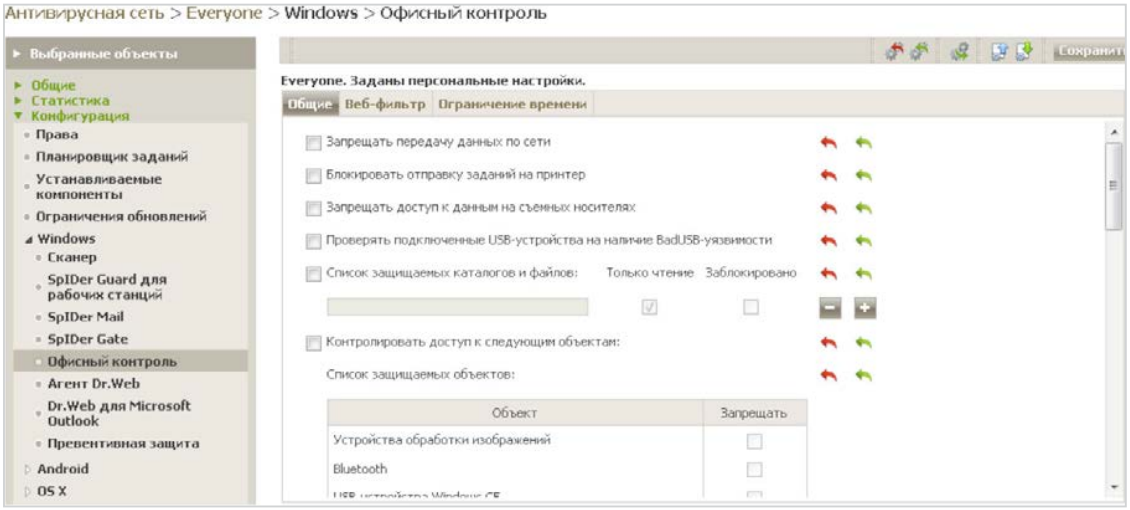


В соседней закладке **Действия** необходимо проверить наличие отметок у пунктов **Блокировать известные источники распространения вирусов** и **Блокировать нерекомендуемые сайты.**

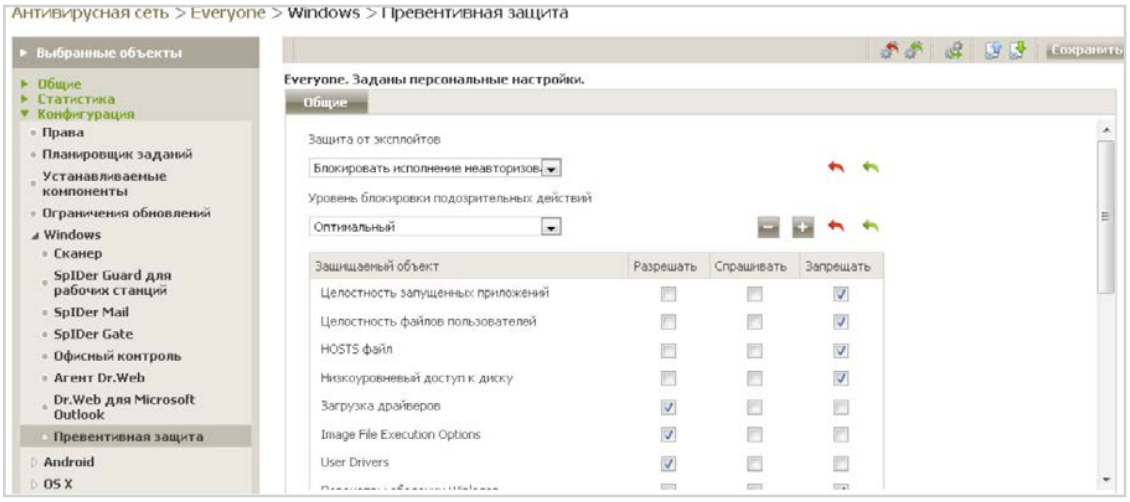


Для сохранения настроек необходимо нажать кнопку **Сохранить.**

Настройки по отношению к сменным носителям производятся на странице **Офисный контроль**, закладка **Общие.**



5. Настройки Dr.Web Process Heuristic не должны позволять внедрение майнерами эксплойтов в работающие приложения. Проверить данные настройки можно на странице Превентивная защита.



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

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.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru | curenet.drweb.ru