Dr.WEB®
с 1992 года

Отключенные по умолчанию

Какие полезные возможности в Dr.Web ESS
не включены, почему так сделано,
и в каких случаях их надо включить

Отключенные по умолчанию

Какие полезные возможности в Dr.Web ESS не включены, почему так сделано, и в каких случаях их надо включить

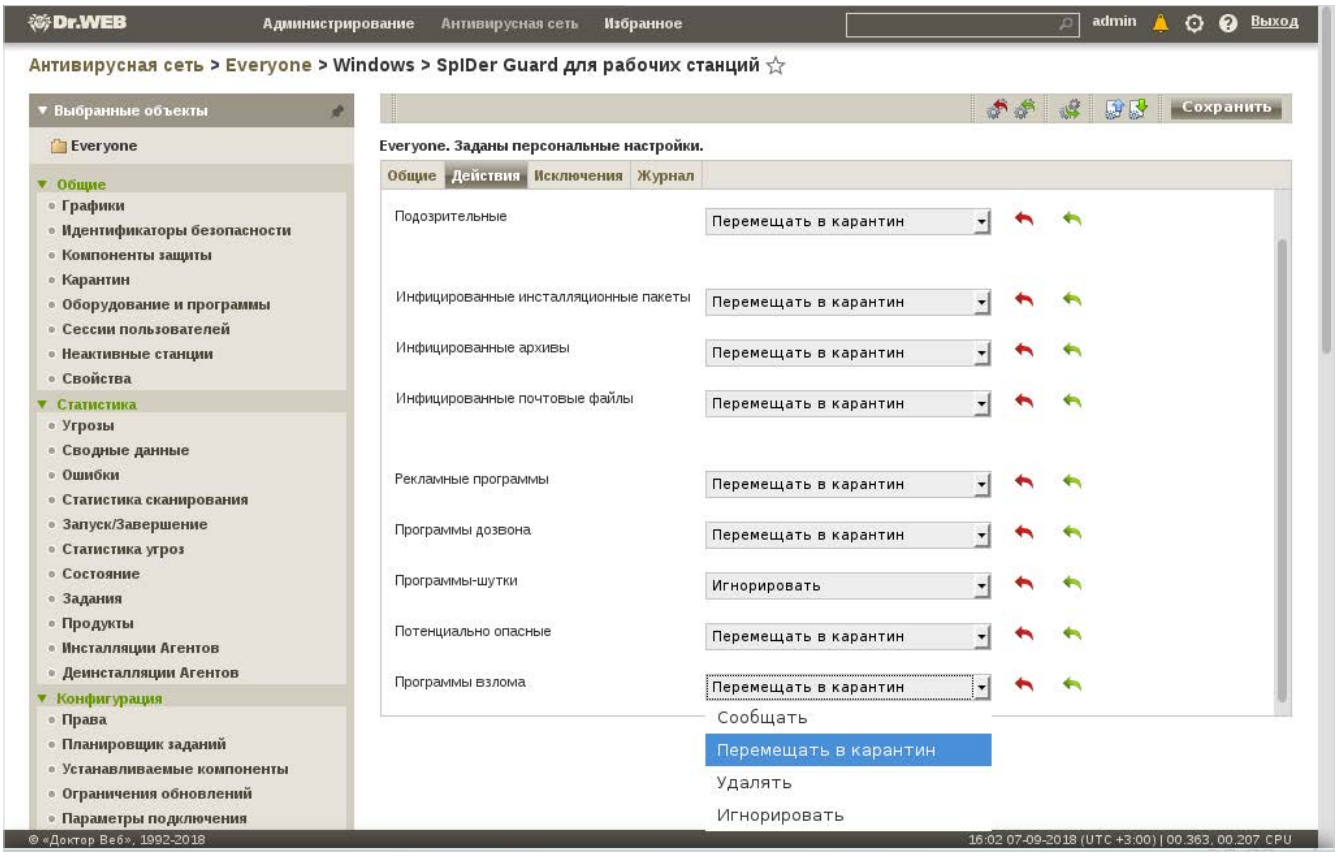
Dr.Web Enterprise Security Suite имеет по умолчанию оптимальные настройки компонентов антивирусных агентов и опций Центра управления, обеспечивающие эффективную защиту от всех типов современных и перспективных угроз.

1. Разрешите автоматическое перемещение потенциально опасного ПО и программ взлома в карантин

Потенциально опасное ПО и программы взлома представляют угрозу для безопасности корпоративной сети, могут обладать известными злоумышленникам уязвимостями и иметь недокументированные возможности, также известные злоумышленникам.
В связи с этим рекомендуем разрешить автоматическое перемещение потенциально опасного ПО и программ взлома в карантин.
Данная опция может быть включена для пользовательской группы или отдельной станции, после того как она будет выбрана в антивирусной сети.

Рекомендуемый порядок настройки

Для ОС Windows: в левом меню *Конфигурация* → *Windows* → *SpIDer Guard* для рабочих станций / серверов.
Во вкладке **Действие** установите режим **Перемещать в карантин** напротив пунктов **Потенциально опасные** и **Программы взлома**. Нажмите на кнопку **Сохранить** для применения настроек.
Обращаем внимание, что к категории потенциально опасных программ относятся программы удаленного управления, поэтому, в случае необходимости использования данного ПО, внесите их в исключения в соседней вкладке **Исключения**.



2. Настройте автоматическое применение действия при обнаружении вредоносного ПО антивирусным сканером

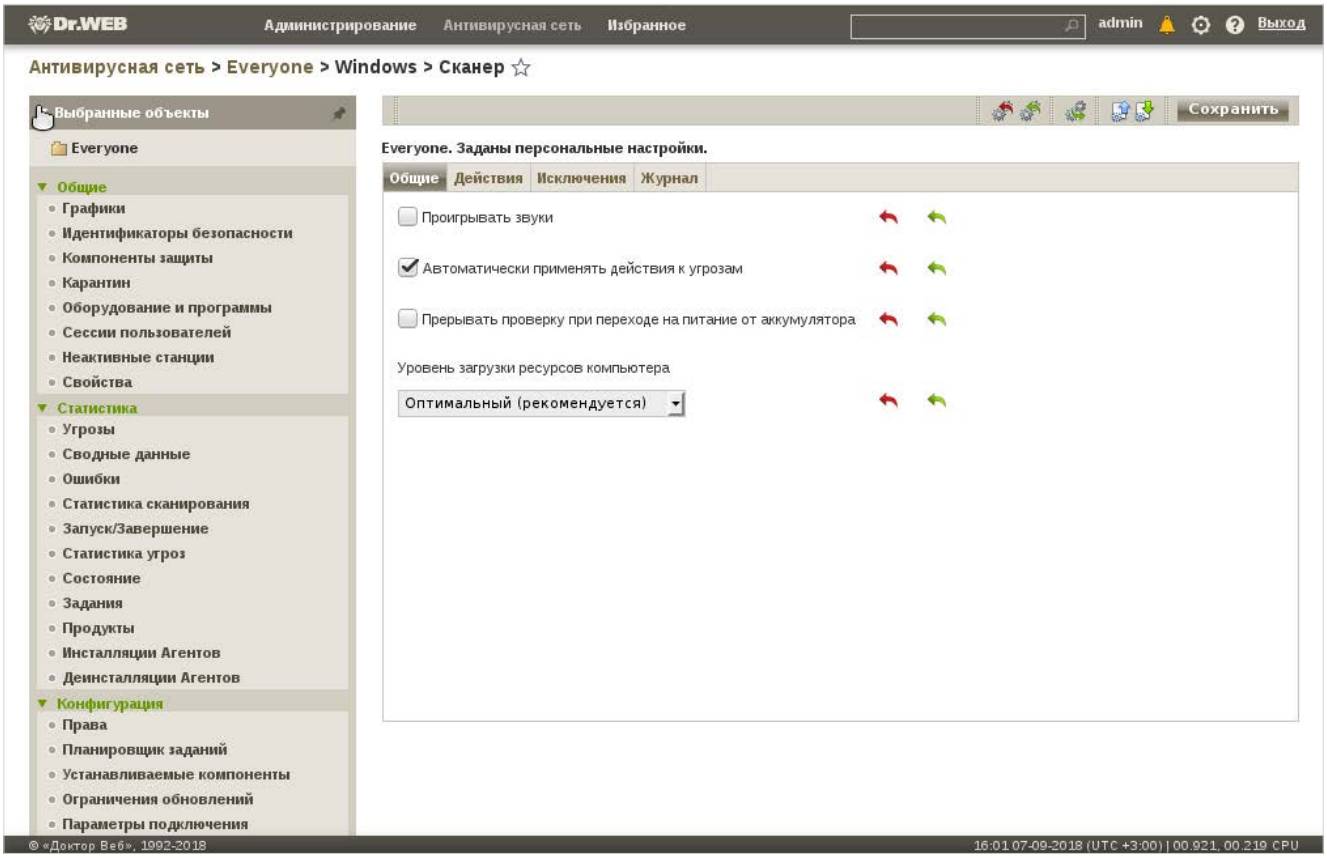
В случае обнаружения антивирусным сканером вредоносного или потенциально опасного ПО, по умолчанию пользователю предлагается выбрать действие, которое будет осуществлено с обнаруженным файлом. Файл может быть вылечен, перемещен в карантин, удален или проигнорирован.
Предполагается, что пользователь сможет принять квалифицированное решение по данному запросу. Однако при необходимости системный администратор может настроить автоматическое (предопределенное) действие сканера при обнаружении им угроз.

! Достаточно часто в случае заражения компьютеров локальной сети производится ее автоматическая проверка антивирусным сканером. При этом найденные вредоносные программы автоматически удаляются или лечатся. В связи с этим в случае возникновения необходимости анализа инцидента бывает невозможно воспроизвести пути заражения, найти использованные злоумышленниками инструменты. Для предотвращения подобных ситуаций рекомендуем перемещать найденные объекты в карантин.

Настроить опцию можно для пользовательской группы или отдельной станции, выбрав ее в антивирусной сети.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация* → *Windows* → *Сканер*. Во вкладке **Общие** установите галочку напротив пункта **Автоматически применять действие к угрозам**, а во вкладке **Действи**я выберите нужное поведение при обнаружении угроз. Нажмите на кнопку **Сохранить** для применения настроек.



3. Включите возможность использования Мобильного режима антивирусными агентами для macOS, Linux, Android

Мобильный режим используется для обновления антивирусных баз с Всемирной сети обновления Dr.Web при отсутствии подключения агентов к ES-серверу.

Мобильный режим может использоваться в случае, если защищаемые устройства используются сотрудниками вне локальной сети компании, краткосрочно могут не иметь доступа к сети организации (см. сценарий по защите «путешествующих» устройств) либо при плохом доступе к серверам компании и периодической недоступности ES-сервера.

! По умолчанию возможность использования Мобильного режима может быть разрешена только для антивирусных агентов для MS Windows.

Рекомендуемый порядок настройки

Для подключения возможности использования Мобильного режима для остальных типов агентов выберите в антивирусной сети группу Everyone.

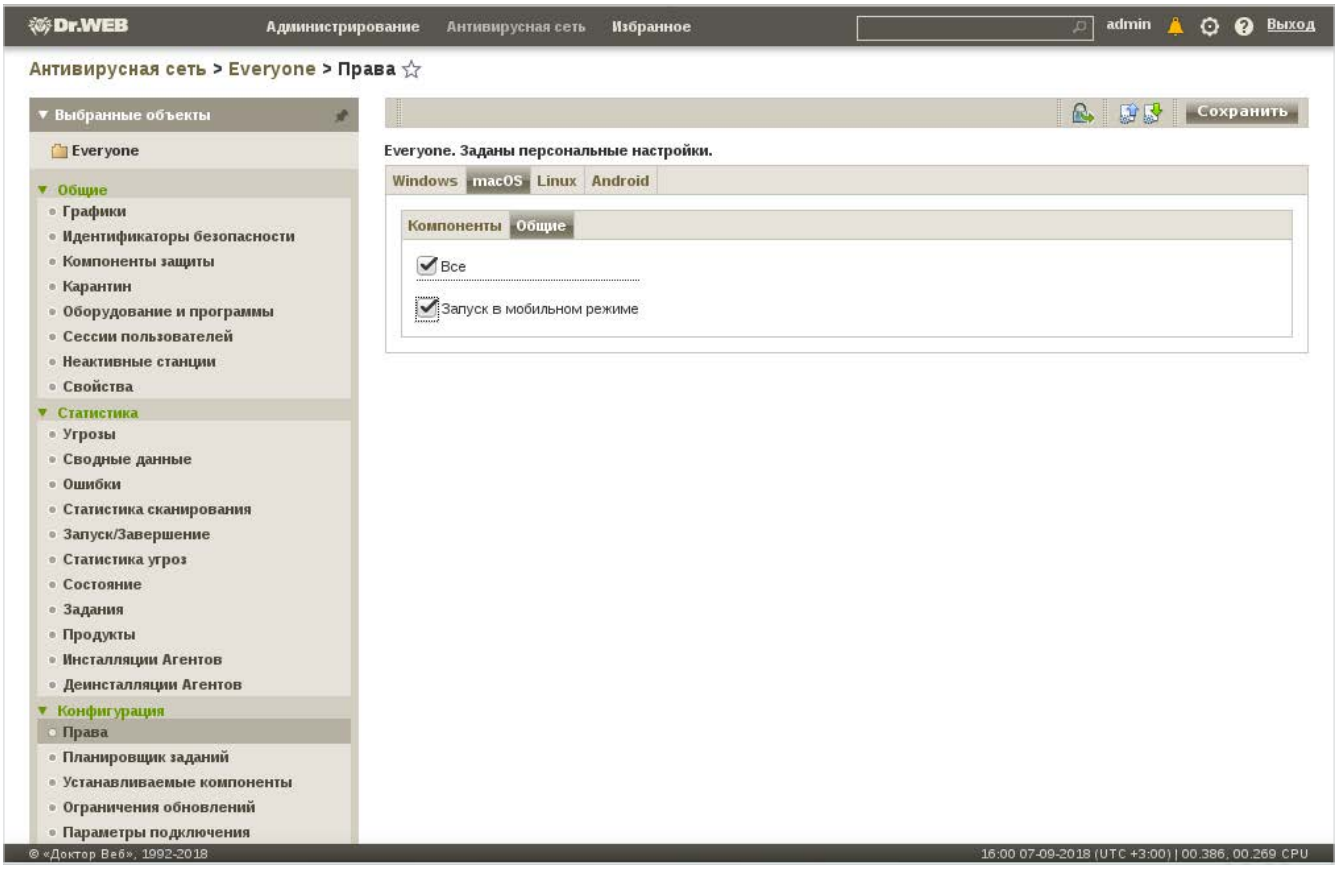
В левом меню выберите Конфигурация → Права. В окне выбора персональных настроек выберите вкладки:

macOS → *Общие* → установите галочку *Запуск в мобильном режиме* и нажмите на кнопку *Сохранить* для применения настроек.

Linux → *Общие* → установите галочку *Запуск в мобильном режиме* и нажмите на кнопку *Сохранить* для применения настроек.

Android → *Общие* → установите галочку *Запуск в мобильном режиме* и нажмите на кнопку *Сохранить* для применения настроек.

! Для станции, не имеющей доступа к антивирусному серверу компании производится обновление только вирусных баз но не компонентов антивирусной защиты в том числе влияющих на уровень защиты от угроз нулевого дня. В связи с этим:
1) не рекомендуется длительное время использовать станцию без ее подключения к серверу;
2) не рекомендуется использовать Мобильный режим без необходимости.



4. Настройте режим работы антивирусного сканера при работе устройства от батареи

Запуск антивирусного сканера на проверку дискового пространства на устройстве, работающем от АКБ/UPS (батареи), может значительно снизить время его автономной работы из-за повышенного расхода электроэнергии.

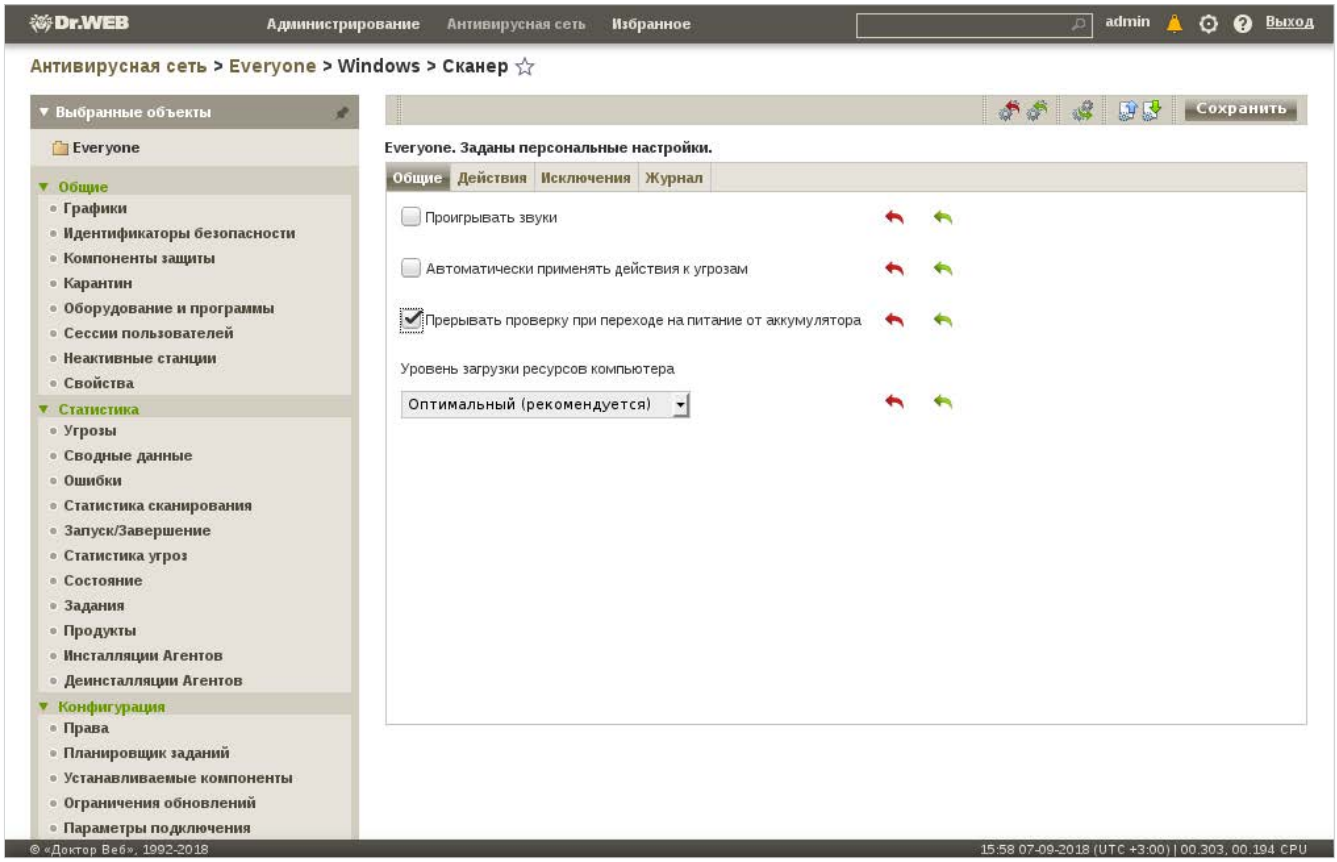
Для предотвращения времени автономной работы устройства настройте возможность прерывания антивирусной проверки в случае перехода на питание от батареи.

> **!** Прерывание антивирусной проверки может привести к необнаружению вредоносного ПО. Настроить опцию можно для пользовательской группы или отдельной станции выбрав ее в антивирусной сети.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация → Windows → Сканер*. Во вкладке **Общие** установите галочку **Прерывать проверку при переходе на питание от аккумулятора** и нажмите на кнопку **Сохранить** для применения настроек.

После восстановления стационарного электропитания станции рекомендуем продолжить проверку сканером дискового пространства устройства.



5. Разрешите возможность автозапуска со съемных носителей (не рекомендуется)

По соображениям безопасности в настройках антивирусных агентов по умолчанию отключена возможность автозапуска приложений со съемных носителей в связи с тем, что заражение вредоносным ПО со сменных носителей — один из основных путей проникновения злоумышленников в сети компаний.

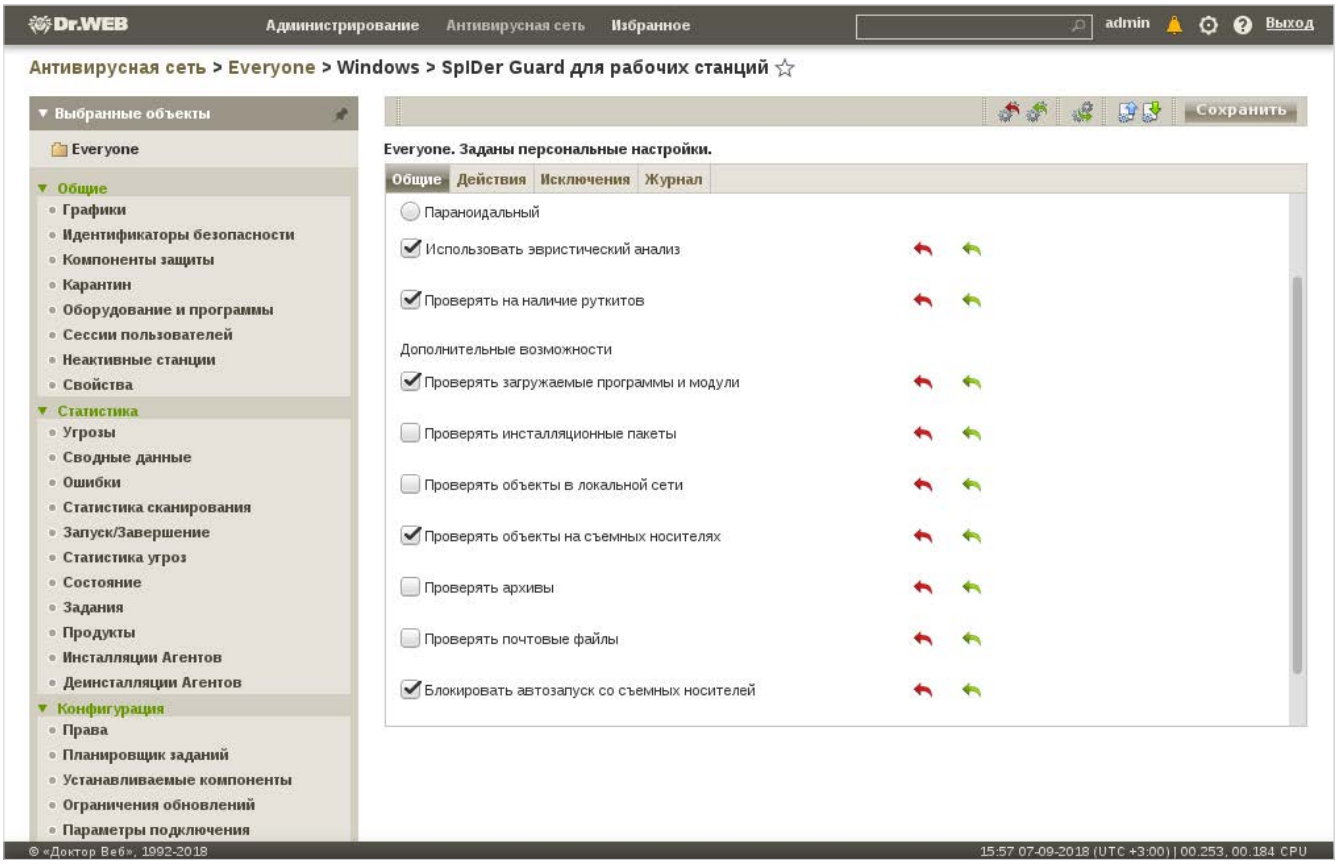
В случае если такая необходимость потребуется, временно отключите блокировку на станции, выбрав ее в антивирусной сети.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация → Windows → SpIDer Guard для рабочих станций / серверов.*

Во вкладке **Общие** уберите галочку напротив пункта Блокировать автозапуск со съемных носителей и нажмите на кнопку **Сохранить** для применения настроек.

Верните блокировку автозапуска со съемных носителей, после того как отпадет необходимость в использовании данной опции.



6. Подключите проверку USB-устройств на наличие BadUSB-уязвимости

BadUSB — это класс хакерских атак, основанный на уязвимости USB-устройств, возможности их маскировки под иные типы устройств, например добавление функционала передачи данных в клавиатуру или мышь.

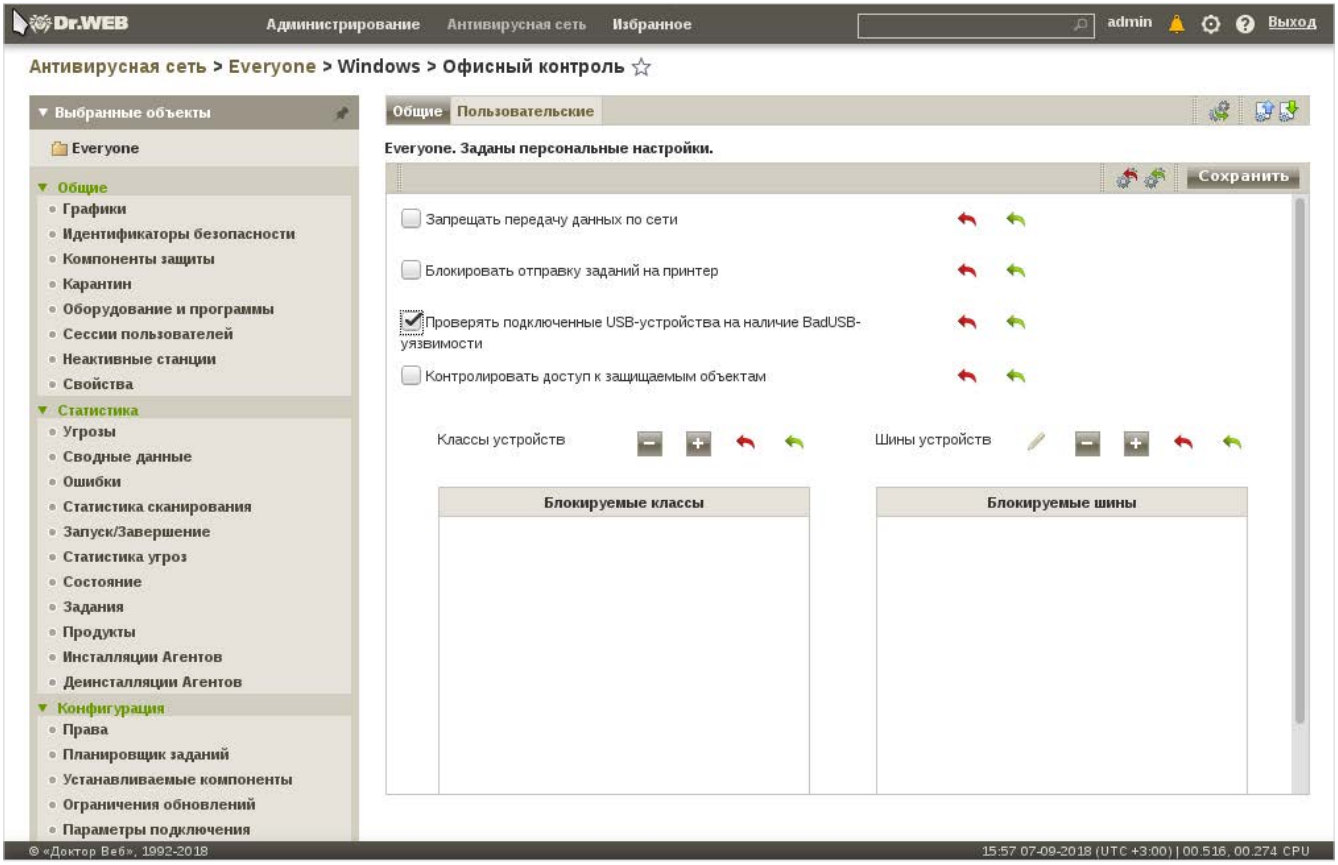
Благодаря отсутствию защиты от перепрошивки в некоторых USB-устройствах, злоумышленник может видоизменить оригинальную прошивку и имитировать работу неоригинального устройства.

Dr.Web ESS защищает от всех типов современных и перспективных угроз, в том числе от BadUSB. Во избежание сбоев в работе некоторых типов устройств, связанных с возможными ошибками в их прошивках, данная опция по умолчанию отключена.

Для подключения опции выберите в антивирусной сети пользовательскую группу или отдельную станцию.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация → Windows → Офисный контроль*. Во вкладке **Общие** установите галочку напротив пункта **Проверять подключенные USB-устройства на наличие BadUSB-уязвимости** и нажмите на кнопку **Сохранить** для применения настроек. Убедитесь в работоспособности всех USB-устройств, подключаемых к станции.



7. Настройте блокировку веб-ресурсов по категориям и запретите использование рабочих станций / интернет-соединений в нерабочее время

По умолчанию в Офисном контроле отключена возможность блокировки на рабочих станциях веб-ресурсов в сети Интернет по категориям.

Рекомендуем настроить блокировку нежелательных ресурсов по предложенным категориям, как возможных источников ВПО и нежелательного контента / трафика, а также задать белый и черный списки веб-ресурсов.

Для подключения опции выберите в антивирусной сети пользовательскую группу или отдельную станцию.

Рекомендуемый порядок настройки

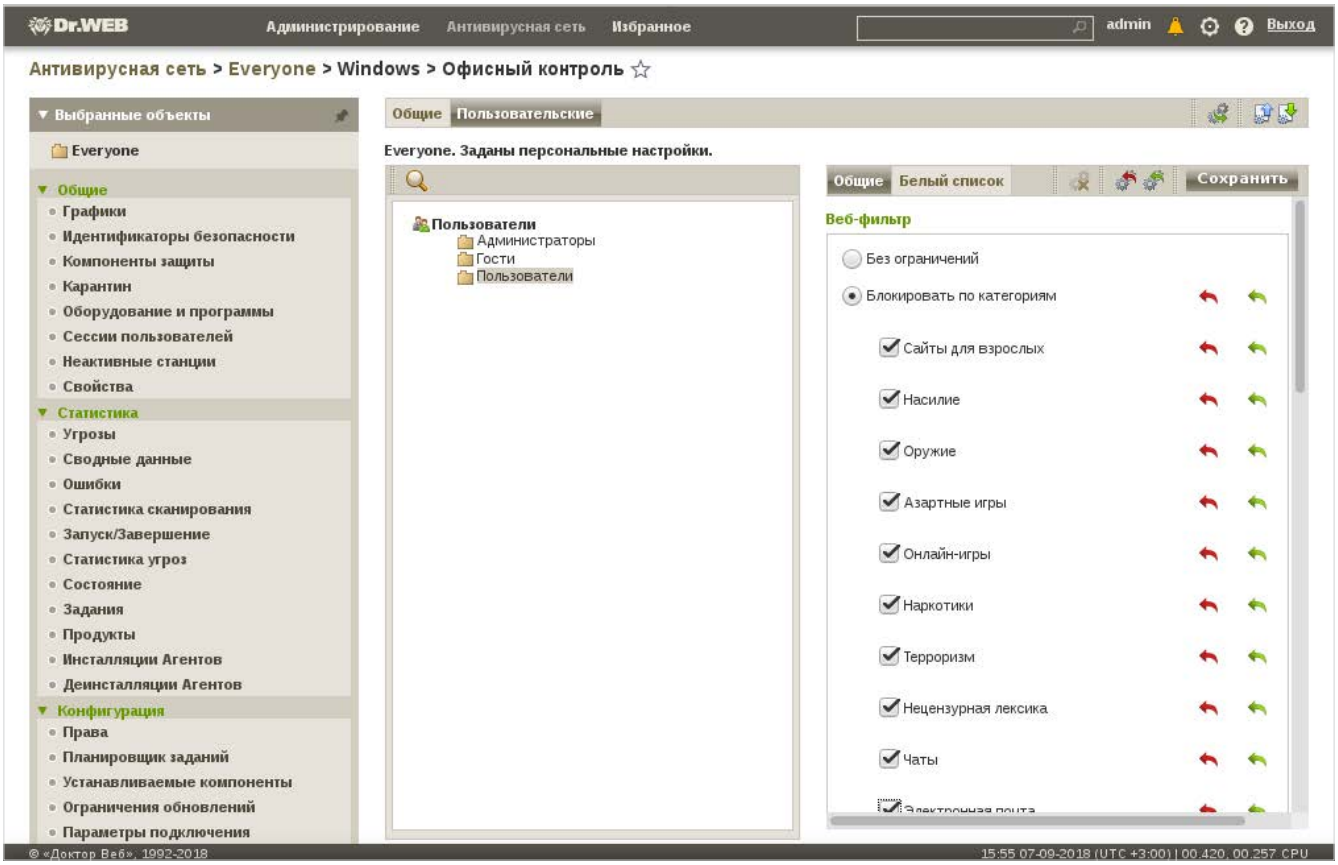
Для Windows: в левом меню выберите *Конфигурация → Windows → Офисный контроль*. Во вкладке **Пользовательские** выберите тип локального пользователя, включите для него блокировку требуемых категорий и нажмите на кнопку **Сохранить** для применения настроек.

При необходимости рекомендуем также запретить использование ПК / интернет-соединения в нерабочее время. Сделать это можно в той же вкладке **Пользовательские**, выбрав пользователя и задав ограничение по времени в правом окне.

Нажмите на кнопку **Сохранить** для применения настроек.

Для Linux/macOS: в левом меню выберите *Конфигурация → Linux/MacOS → SpIDer Gate для рабочих станций/серверов*. Во вкладке Веб-фильтр выберите требуемые категории для блокировки и нажмите на кнопку **Сохранить** для применения настроек.

Для Android: в левом меню *Конфигурация → Android → Cloud Checker*. Выберите требуемые категории для блокировки и нажмите на кнопку **Сохранить** для применения настроек.



8. Запретите эмуляцию действий пользователя

Программы для удаленного администрирования (Radmin, Teamviewer и пр.) являются удобным средством доступа на рабочие станциях пользователей.

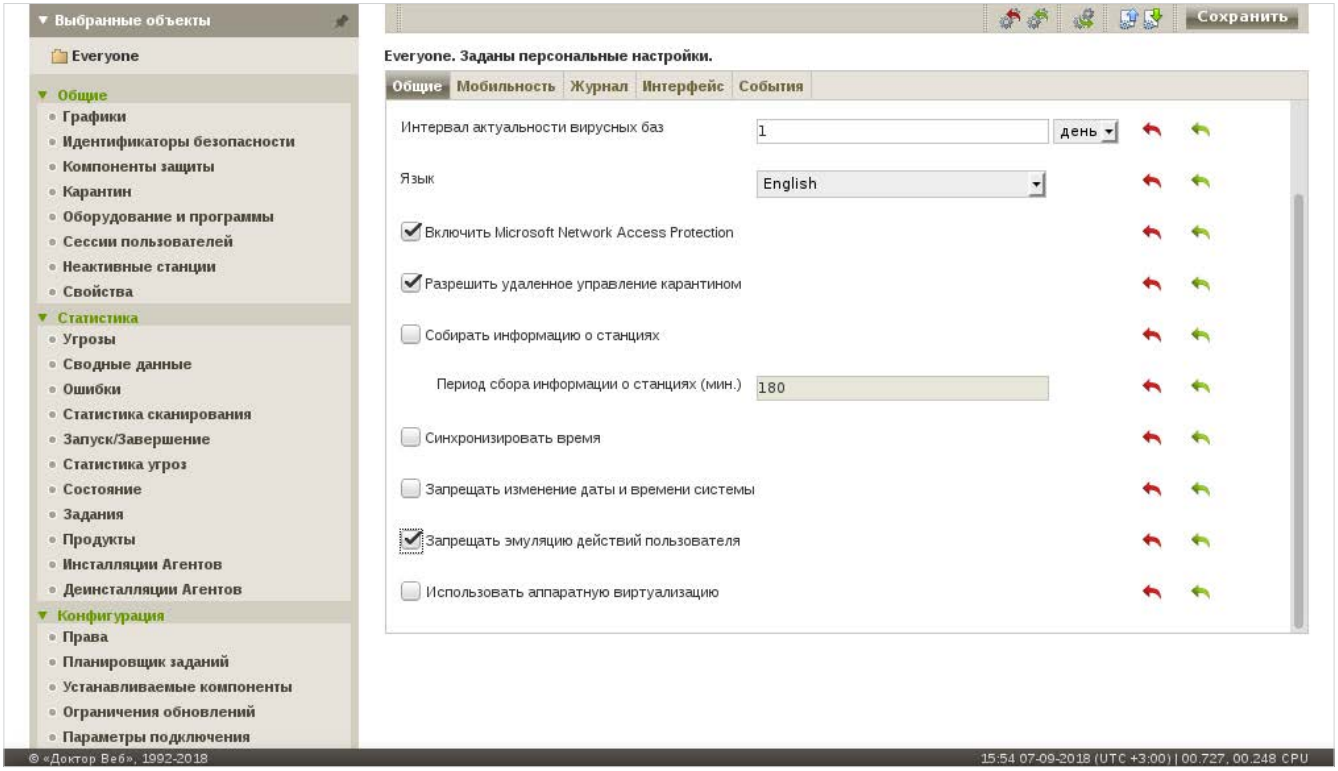
Однако использование средств удаленного доступа, особенно в публичных сетях, — это потенциальная уязвимость, в частности, позволяющая злоумышленнику изменить настройки системы защиты.

Рекомендуем запретить эмуляцию действий пользователя на рабочих станциях, когда не требуется использования средств удаленного администрирования.

Для подключения опции выберите в антивирусной сети пользовательскую группу или отдельную станцию.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация* → *Windows* → *Агент Dr.Web*. Во вкладке **Общие** установите галочку напротив пункта **Запрещать эмуляцию действий пользователя** и нажмите на кнопку **Сохранить** для применения настроек.



9. Настройте сбор информации об оборудовании и ПО на рабочей станции (опционально)

В случае необходимости антивирусный агент под управлением MS Windows может собирать информацию об оборудовании и ПО, установленном на станции.

По умолчанию эта опция отключена в целях снижения ресурсозатрат. Для подключения опции выберите в антивирусной сети пользовательскую группу или отдельную станцию.

Рекомендуемый порядок настройки

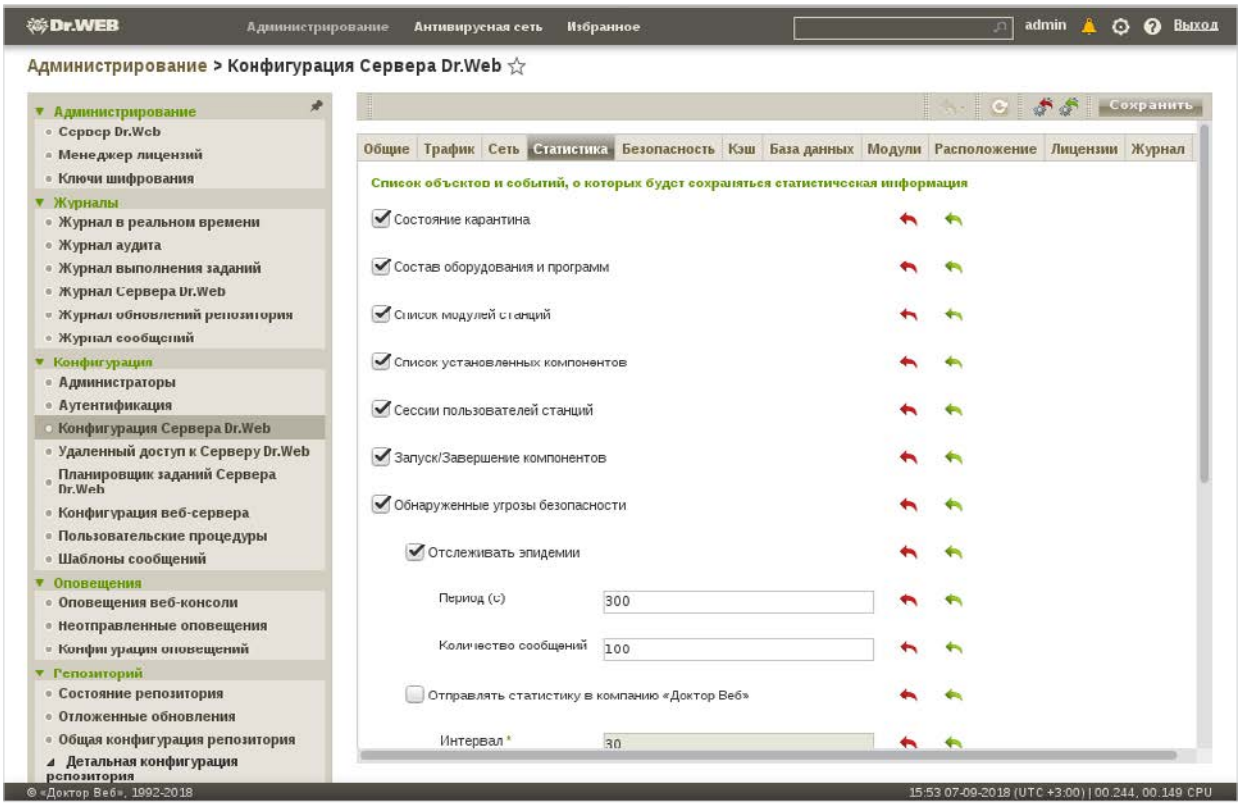
Проверьте, включен ли сбор статистики на Сервере:

а) выберите пункт **Администрирование главного меню** Центра управления;

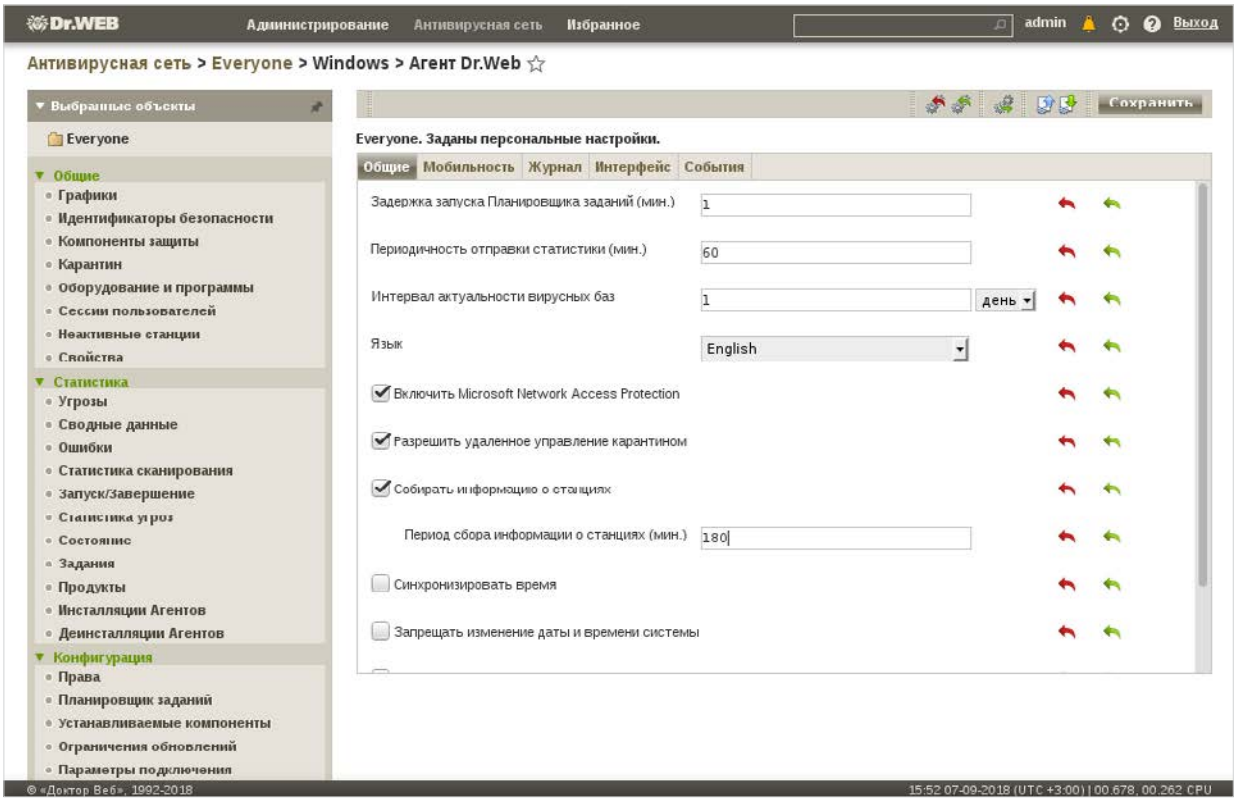
б) выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**;

в) в настройках Сервера откройте вкладку **Статистика** и убедитесь, что установлен флаг **Состав оборудования и программ**.

Если флаг не установлен, то установите его, нажмите на кнопку **Сохранить** для применения внесенных изменений и перезапустите Сервер.



В левом меню выберите *Конфигурация → Windows → Агент Dr.Web*. Во вкладке **Общие** установите галочку напротив пункта **Собирать информацию о станциях**.
При необходимости можно изменить период сбора информации, но не рекомендуется устанавливать слишком короткие тайм-ауты.
Нажмите на кнопку **Сохранить** для применения настроек.
Просмотреть конфигурацию станции можно в разделе меню *Общие → Оборудование и программы.*



10. Настройте периодическую проверку дисков антивирусным сканером

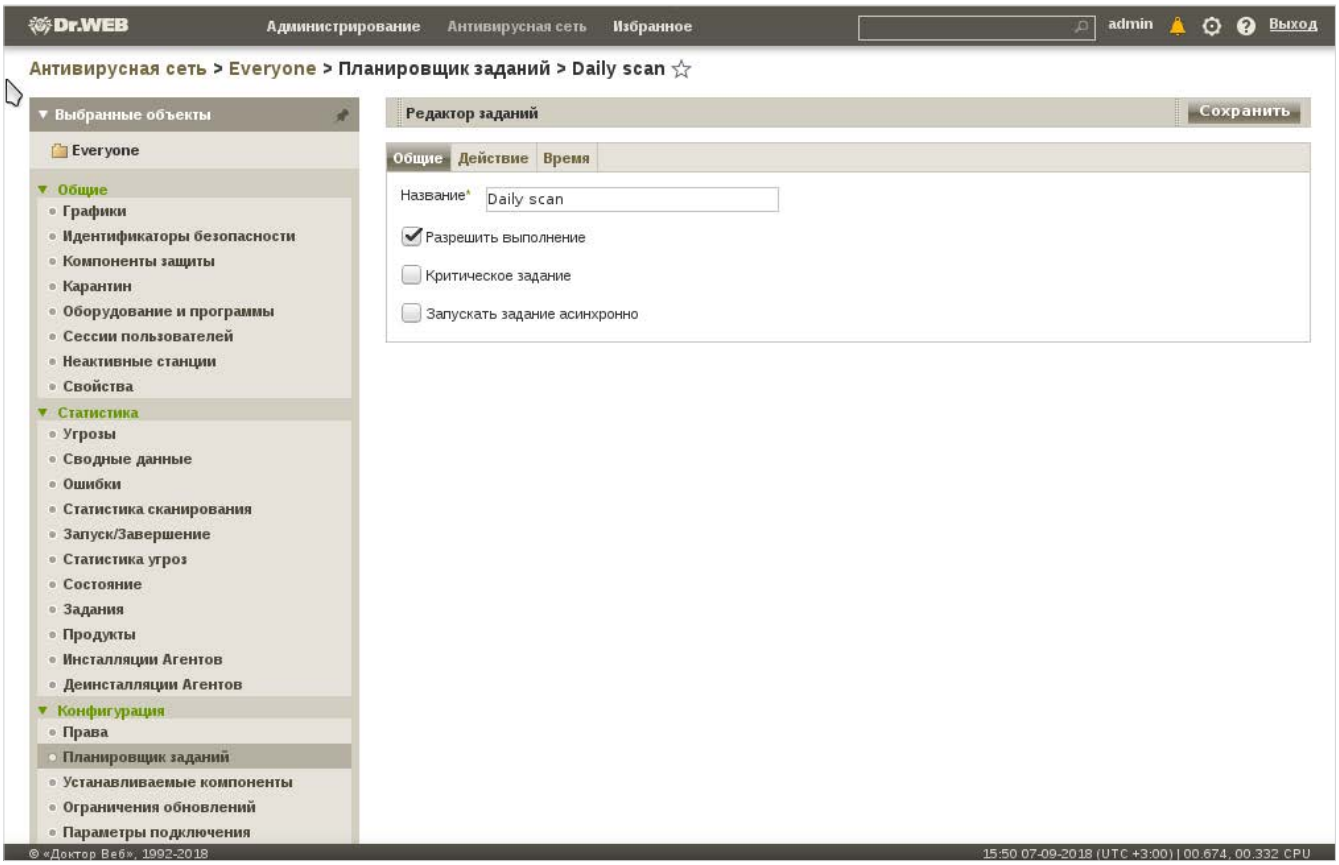
Рекомендуем настроить периодическую проверку рабочих станций и файловых серверов антивирусным сканером в нерабочее время не реже одного раза в неделю. Такая проверка позволит детектировать вредоносное ПО актуальными антивирусными базами.

Настроить расписание можно для пользовательской группы или отдельной станции, выбрав ее в антивирусной сети.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация → Планировщик задания*. В открывшемся окне планировщика выберите предустановленное задание Daily scan. Во вкладке **Общие** установите галочку напротив пункта **Разрешить выполнение**, во вкладке **Действия** настройте опции сканирования и возможные ограничения, а также выставите время сканирования во вкладке Время. Нажмите на кнопку **Сохранить** для применения настроек.

Убедитесь, что задание в планировщике имеет статус **Разрешено**.



11. Заблокируйте возможность использования WSL на рабочих станциях / файловых серверах под управлением MS Windows 10

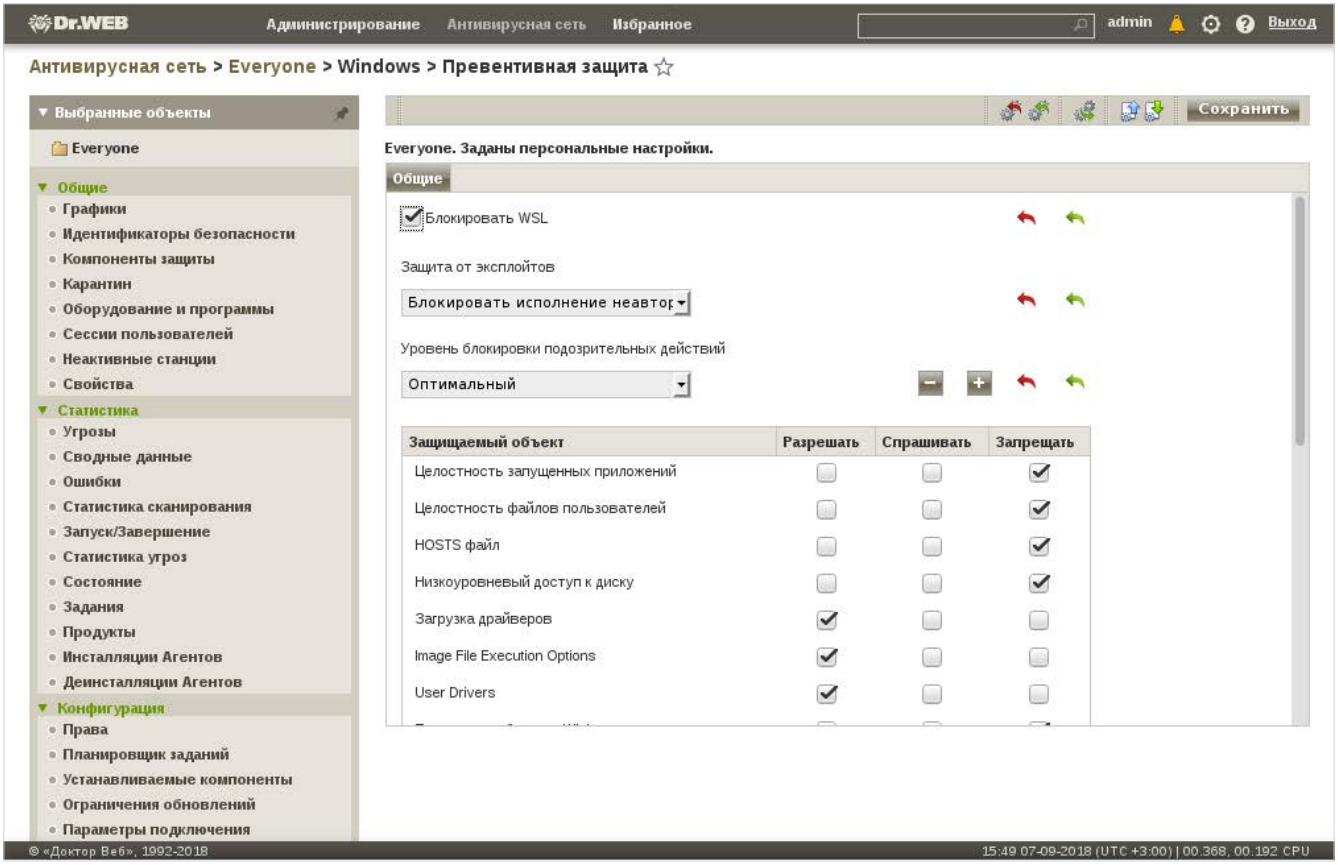
В ОС MS Windows 10 реализована возможность запуска Linux-приложений при помощи встроенной подсистемы Windows Subsystem for Linux (WSL).

В настоящее время WSL отключена по умолчанию, и для ее активации необходимо включить в системе «режим разработчика». Тем не менее существует потенциальная опасность тихой активации режима WSL на рабочей станции и его использования вредоносным ПО для сокрытия себя в системе и деструктивных действий.

Рекомендуемый порядок настройки

Для отключения возможности использования WSL выберите в антивирусной сети группу **Everyone**. В левом меню выберите *Конфигурация → Windows → Превентивная защита*.

Во вкладке **Общие** установите галочку напротив пункта **Блокировать WSL**. Нажмите на кнопку **Сохранить** для применения настроек.



12. Настройте брандмауэр на рабочих стациях

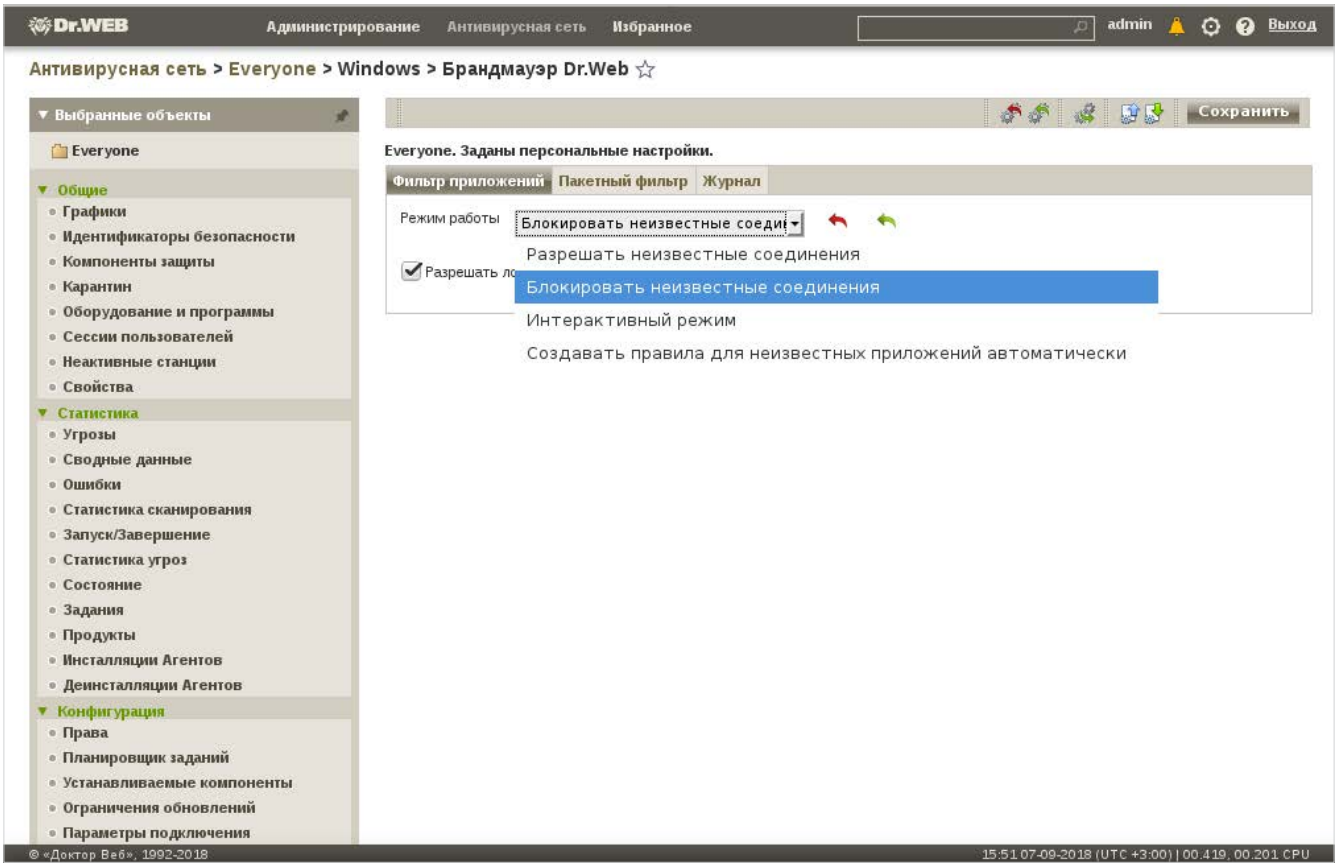
Для противодействия сетевым атакам рекомендуем настроить компонент Брандмауэр (Firewall) для рабочих станций, которые используются для обработки персональных данных, конфиденциальной информации, а также работы с системами дистанционного банковского обслуживания.

Для этого выберите в антивирусной сети пользовательскую группу или отдельную станцию.

Рекомендуемый порядок настройки

В левом меню выберите *Конфигурация → Windows → Брандмауэр Dr.Web*. Во вкладке **Фильтр приложений** установите режим работы **Блокировать неизвестные соединения**, во вкладке **Пакетный фильтр** установите галочку напротив пункта **Включить пакетный фильтр** и настройте правила его работы. Во вкладке **Журнал** установите галочку напротив пункта Вести подробный журнал и нажмите на кнопку **Сохранить** для применения настроек.

Убедитесь в работоспособности программ, использующих доступ к сети, на рабочей станции.



О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.
Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  - информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  - отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97
антивирус.рф | www.drweb.ru