Dr.WEB®
с 1992 года

Возможности модуля Контроль приложений. Функциональный анализ в Dr.Web Enterprise Security Suite 12.0

Dr.Web Enterprise Security Suite 12.0

Возможности модуля Контроль приложений

Функциональный анализ

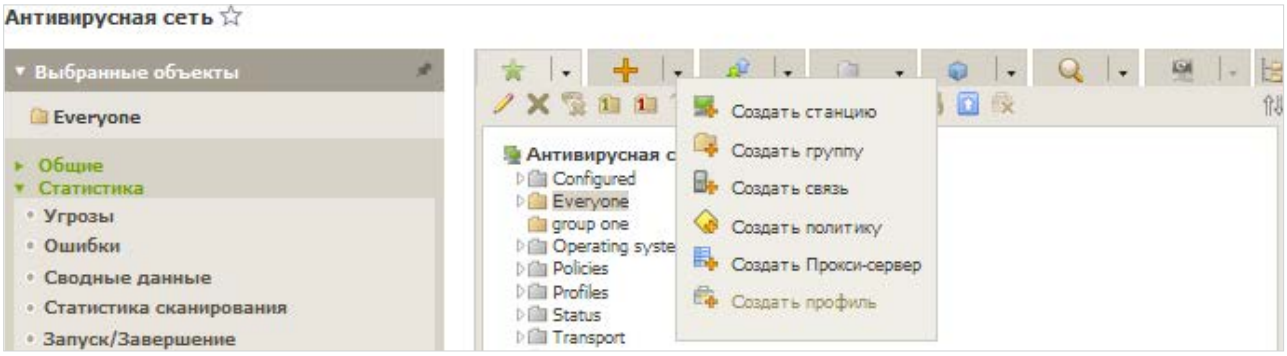
Никто не знает, что запущено на подконтрольном компьютере. Список загруженных программ вполне возможно посмотреть с помощью спецутилит (если не знать, конечно, что вредоносные программы отслеживают запуск таких утилит и прекращают свою работу). Но если получить список запущенного более-менее осуществимо, то узнать, что делает та или иная программа или скрипт, уже не всегда возможно.

Контроль приложений Центра управления Dr.Web Enterprise Suite позволяет сформировать правила, запрещающие запуск определенных категорий программного обеспечения, убрав возможность запуска подозрительных программ из зоны риска, — кто если не разработчики антивирусных программ знают, какие признаки, как правило, встречаются именно у вредоносных программ!

Настройки системы контроля приложений осуществляются с помощью профилей, в соответствии с настройками которых приложения на станциях (или для определенных пользователей) будут запускаться или блокироваться.

Чтобы создать профиль

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне на панели инструментов выберите пункт **Добавить объект сети** ⇒ **Создать профиль**.



3. На открывшейся панели задайте **Название профиля**.

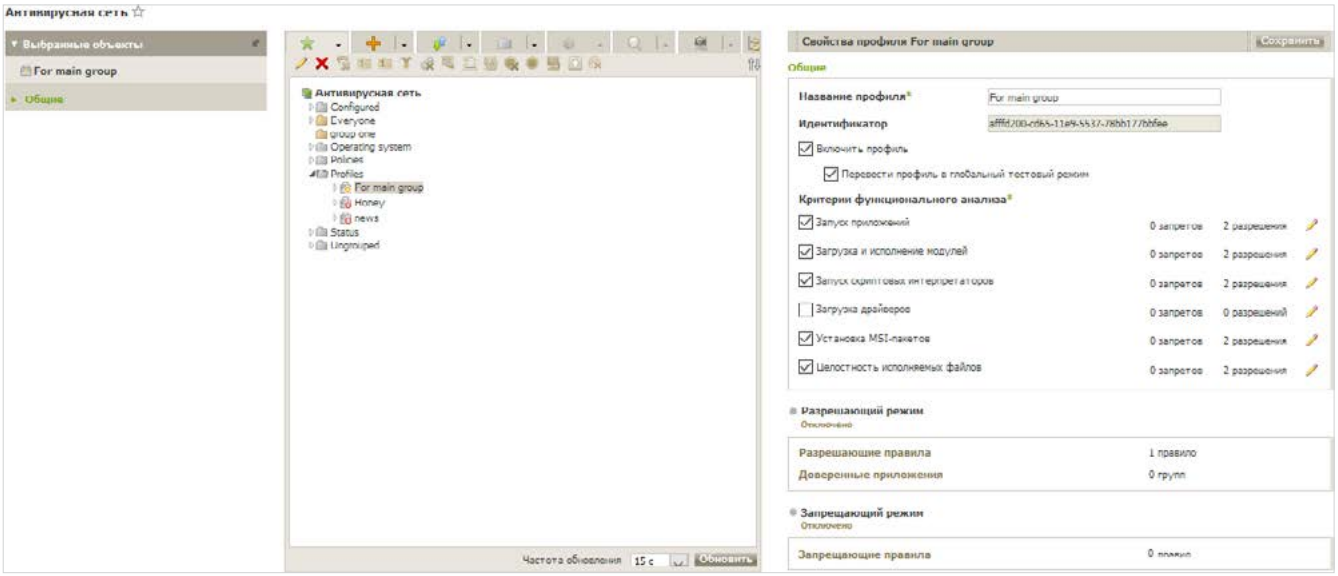
4. Нажмите кнопку **Сохранить**.

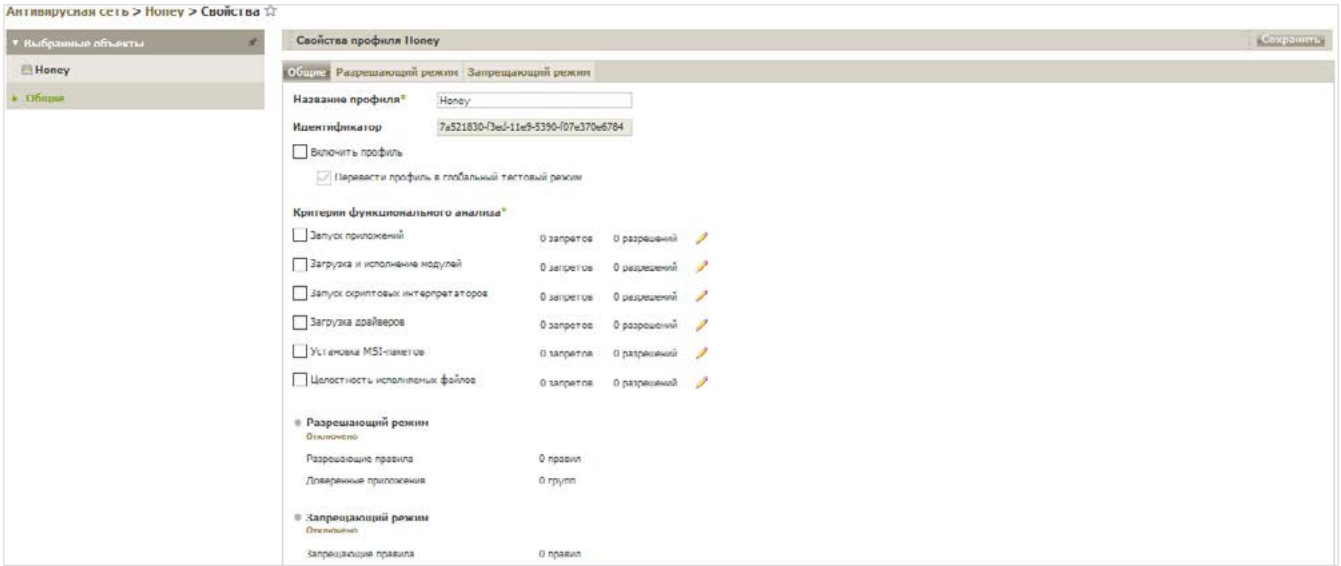
5. Новый профиль будет создан и помещен в группу **Profiles** дерева Антивирусной сети.

После создания профиля его нужно настроить (установить нужные ограничения, правила работы), а также назначить станциям и пользователям антивирусной сети.

Внимание! Настройку работы профилей рекомендуется производить в тестовом режиме. Тестовый режим имитирует работу Контроля приложений с полным ведением журнала статистики активности на защищаемых станциях, однако фактическая блокировка приложений не производится.

1. В дереве **Антивирусная сеть** в главном меню Центра управления нажмите на название профиля в иерархическом списке антивирусной сети (в правой части окна Центра управления автоматически откроется панель со свойствами профиля), или нажмите на иконку профиля в дереве антивирусной сети, или выберите профиль и затем выберите пункт **Свойства** управляющего меню (откроется окно со свойствами профиля).





2. Установите флаг **Включить профиль**, чтобы начать использовать этот профиль. Если установлен флаг **Перевести профиль в глобальный тестовый режим**, все настройки профиля не будут применяться к станциям, однако будет осуществляться запись журнала активности как при включенных настройках.
3. В разделе **Критерии функционального анализа** установите флаги для событий, которые вы хотите отслеживать.

   Именно в этом разделе мы можем задать признаки, нежелательные или желательные у программ, запускаемых на защищаемых компьютерах. Для задания расширенных настроек по каждому выбранному типу событий критерию нажмите ✎ (**Редактировать**) напротив соответствующего типа событий. Откроется окно со списком настроек.

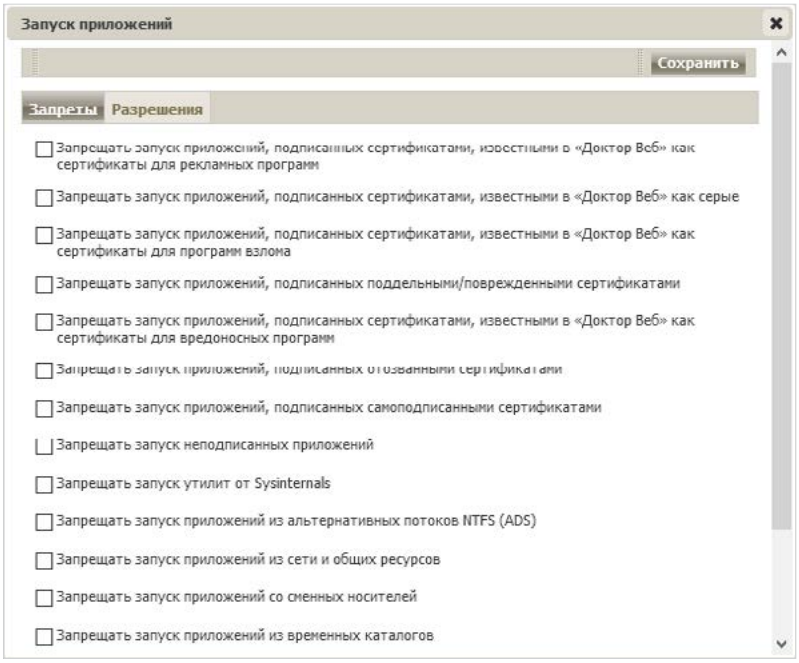
   Рассмотрим расширенные настройки более подробно.

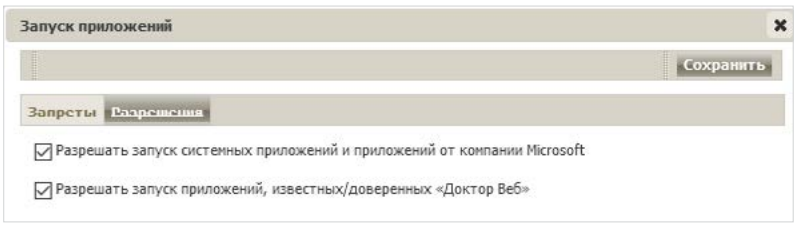
Имеется 6 групп критериев функционального анализа:

- Запуск приложений
- Загрузка и исполнение модулей
- Запуск скриптовых интерпретаторов
- Загрузка драйверов
- Установка MSI-пакетов
- Целостность исполняемых файлов

Для каждой из групп есть своя группа критериев, рассмотрим их подробнее.

Запуск приложений





С разрешениями все понятно, перейдем к запретам. Большинство пунктов даже не нужно комментировать — вполне понятно, какого рода программы под них попадают и нужен ли их запуск:

- Запрещать запуск приложений, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для рекламных программ
- Запрещать запуск приложений, подписанных сертификатами, известными в «Доктор Веб» как серые
- Запрещать запуск приложений, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для программ взлома
- Запрещать запуск приложений, подписанных поддельными/поврежденными сертификатами
- Запрещать запуск приложений, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для вредоносных программ

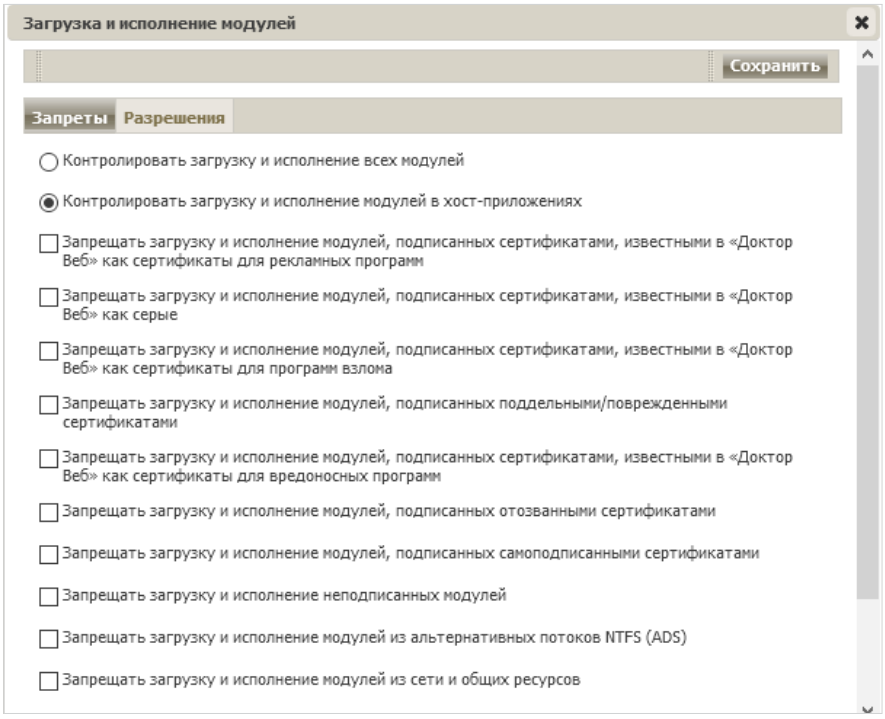
- Запрещать запуск приложений, подписанных отозванными сертификатами
- Запрещать запуск утилит от Sysinternals
- Запрещать запуск приложений из альтернативных потоков NTFS (ADS)
- Запрещать запуск Windows/Microsoft Store приложений (только для Windows 8 и выше)
- Запрещать запуск приложений с двойным/нетипичным расширением

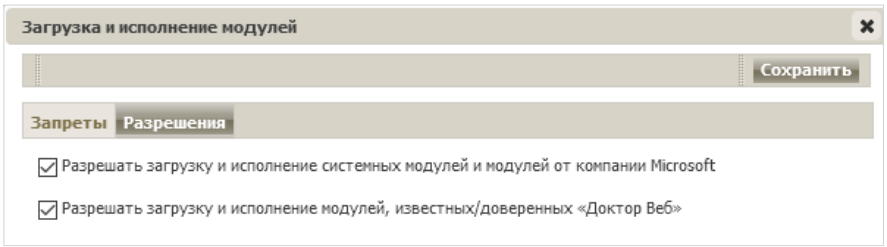
Вполне понятно, что в большинстве систем не используются запускаемые в среде Windows программы Linux, поэтому мы также можем отметить пункт **Запрещать запуск bash-оболочек и WSL-приложений (только для Windows 10 и выше)**

Запуск приложений со сменных носителей (**Запрещать запуск приложений со сменных носителей**) и по сети (**Запрещать запуск приложений из сети и общих ресурсов**), если у вас не используются данные возможности, тоже не вредно запретить. Те де флешки — известный источник вирусов.

Достаточно часто вредоносные программы используют для запуска каталоги для временных файлов. Если вы не планируете разворачивать новое ПО, которое также может использовать данные папки, — отметьте опцию **Запрещать запуск приложений из временных каталогов**.

Загрузка и исполнение модулей



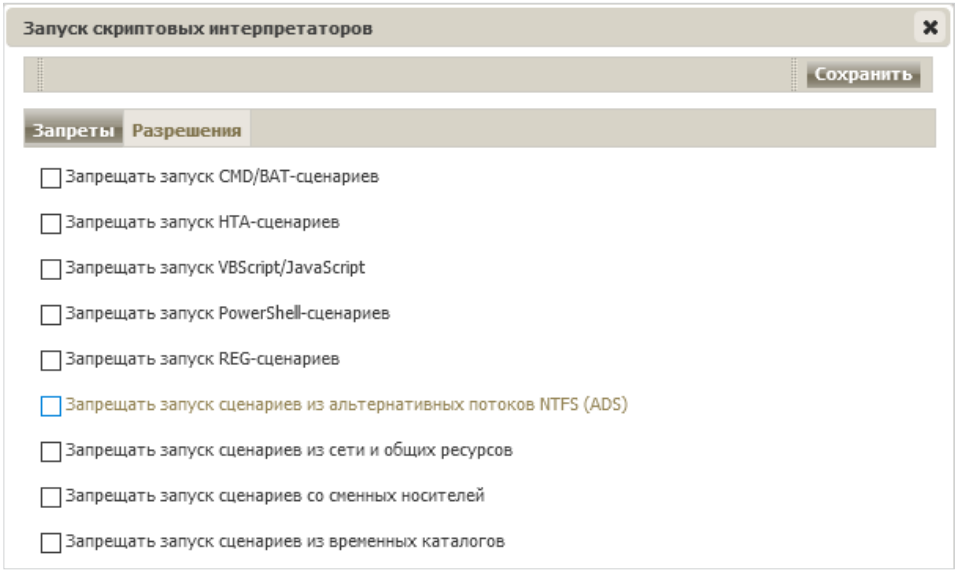


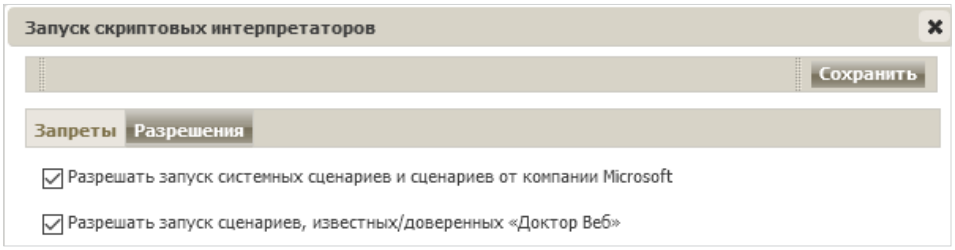
Контролировать загрузку и исполнение всех модулей

Контролировать загрузку и исполнение модулей в хост-приложениях

С разрешениями так же всё ясно, запреты аналогичны предыдущему разделу.

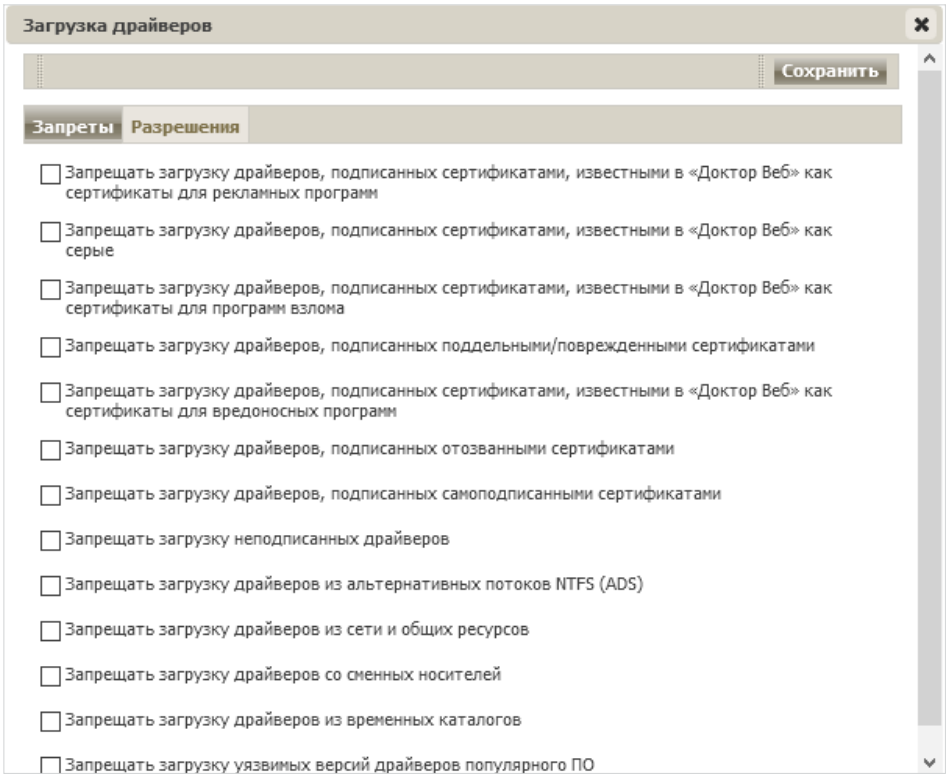
Запуск скриптовых интерпретаторов

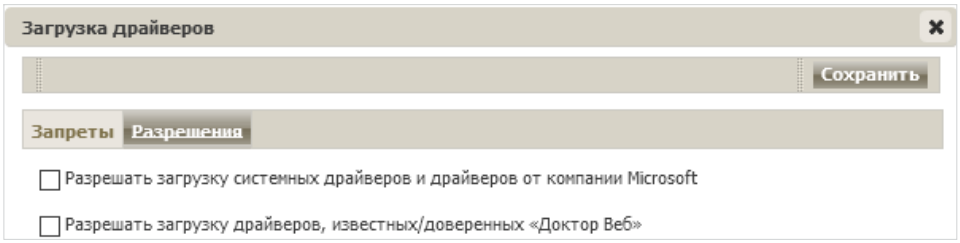




В данном разделе вы можете запретить те типы скриптов (а также модификацию реестра), которые точно не используются в вашей системе, а также их запуск со сменных носителей или из временных каталогов.

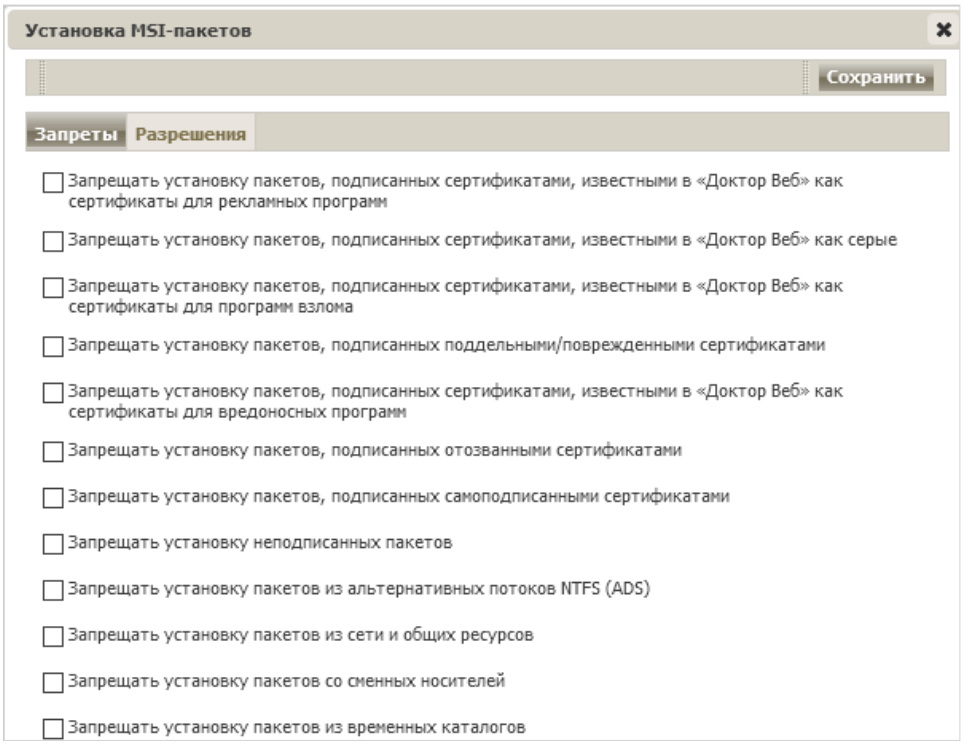
Загрузка драйверов

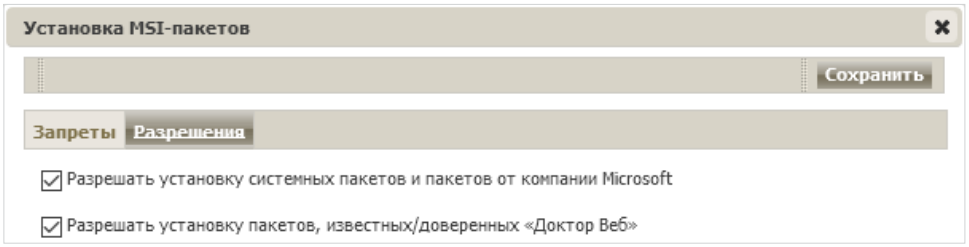




Кроме описанных выше запретов в данном разделе имеется уникальный — **Запрещать загрузку уязвимых версий драйверов популярного ПО**. Думаем, его важность понятна.

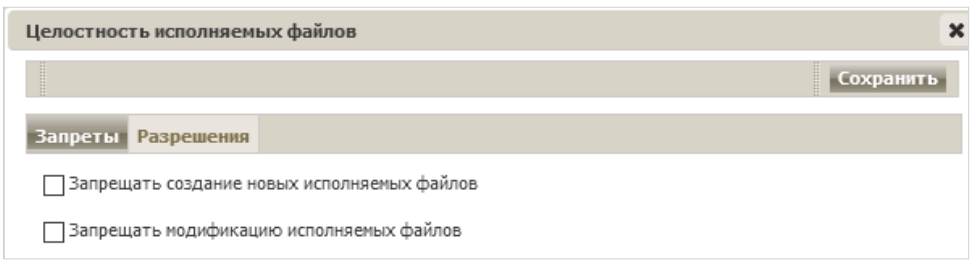
Установка MSI-пакетов

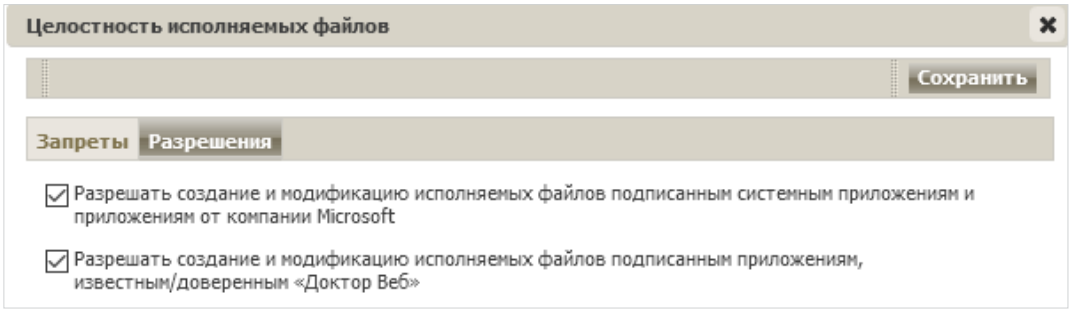




Вредоносные пакеты часто используются вредоносными программами, вы смело можете запретить запуск инсталляционных пакетов, используя опции данного раздела.

Целостность исполняемых файлов





Пожалуй, самый простой и заманчивый пункт. Антивирус должен лечить, поэтому право на модификацию для него логично. Но модифицировать может и система обновлений. Поэтому если у вас используется только система обновлений от компании Microsoft, вы можете запретить модификацию исполняемых файлов для всех иных источников, отметив галочкой пункты на странице **Запреты**.

Установите флаги для тех настроек, которые должны выполняться, и не забывайте, что перед использованием на станциях новый режим работы должен быть протестирован.

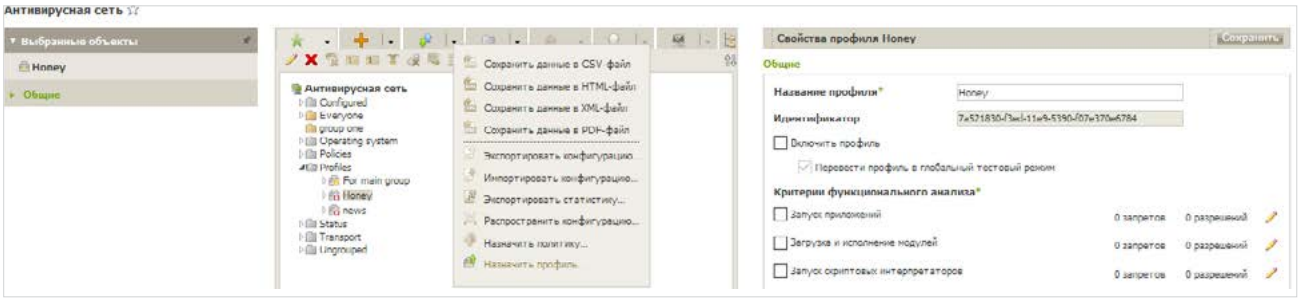
Если вы включите использование какого-либо из типов событий, но не зададите его расширенные настройки, то контроль запуска будет производиться для всех объектов по этому критерию в соответствии с настройками разрешающего или запрещающего режимов. Если вы зададите расширенные настройки, но не включите использование самого типа события, то ни расширенные настройки, ни сам критерий выполняться не будут.

Для сохранения расширенных настроек нажмите **Сохранить** в окне со списком расширенных настроек.

4. Чтобы применить настройки, заданные в разделе **Общие**, нажмите **Сохранить** в настройках профиля.

Вторым этапом настройки системы контроля запуска приложений является назначение созданного и настроенного профиля станциям или пользователям антивирусной сети.

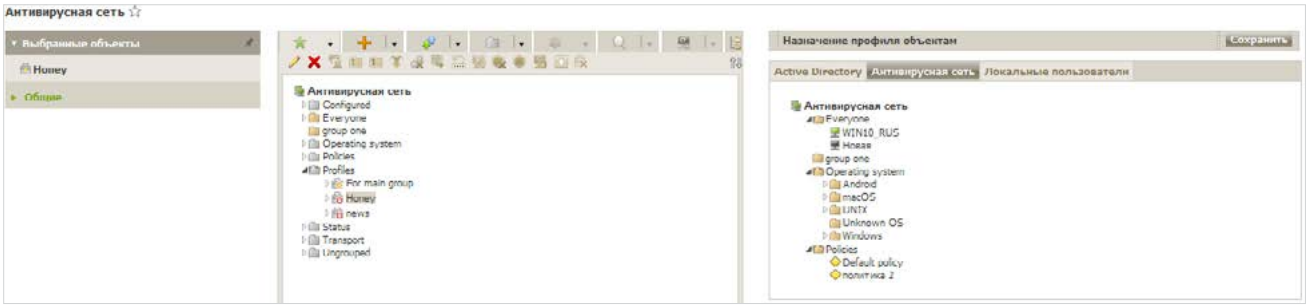
1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в иерархическом списке выберите профиль, который вы хотите назначить.
3. На панели инструментов нажмите **Экспортировать данные → Назначить профиль**.



4. Выберите объект распространения настроек в открывшемся окне. Если мы рассматриваем случай глобального запрета на исполнение вредоносного кода, то наиболее логично назначить данное ограничение на все станции антивирусной сети.

   На вкладке **Антивирусная сеть** вы можете выбрать группы станций (настройки будут распространяться на учетные записи всех пользователей всех станций, входящих

в данные группы) или отдельные станции в группах (настройки будут распространяться на учетные записи всех пользователей выбранных станций):



5. Нажмите кнопку **Сохранить**. Все выбранные объекты будут добавлены в список, на который распространяется настраиваемый профиль, и будут отображены в дереве как вложенные объекты настраиваемого профиля.

Проблема решена.

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.).
- Его использование 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
https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru