



Запрет запуска новейших вредоносных приложений с помощью Контроля приложений в Dr.Web Enterprise Security Suite 12.0



Dr.Web Enterprise Security Suite 12.0

Запрет запуска новейших вредоносных приложений с помощью Контроля приложений

Среднее время между обновлениями средств антивирусной защиты может достигать почти двух часов. Достаточно большой промежуток времени, за который шифровальщик вполне может вывести компьютеры сети из строя, а банковский троянец — перевести некую сумму на счет злоумышленника. Заблокировать запуск вредоносных программ, сведения о которых еще не получены с ходе обновлений, можно различными способами — например, с помощью модулей Офисного контроля или Превентивной защиты. Можно сделать это и с использованием возможностей Контроля приложений.

Чтобы настроить **Контроль приложений**, необходимо выполнить следующую последовательность действий.

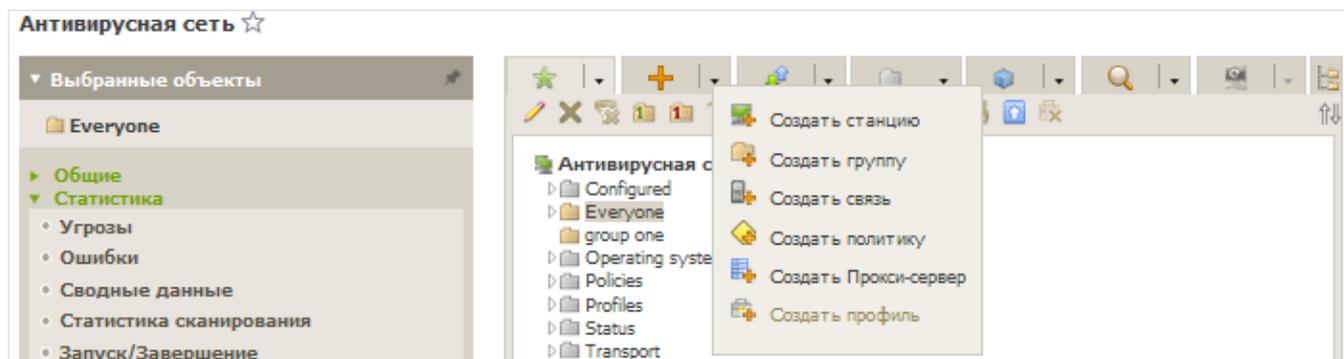
1. Разрешите сбор и отправку информации со станций для раздела **События Контроля приложений**, установив флаг **Отслеживать события Контроля приложений** на вкладке **Общие** компонента **Агент Dr.Web** для станций или группы станций с установленным Контролем приложений, с которых вы хотите получать информацию о запуске приложений.
2. Разрешите сбор информации антивирусным сервером для раздела **События Контроля приложений**, установив флаги **Статистика Контроля приложений по активности процессов** и **Статистика Контроля приложений по блокировке процессов** в разделе **Администрирование Конфигурация Сервера Dr.Web** на вкладке **Статистика**.
3. Перезапустите антивирусный сервер.
4. Создайте профиль. Настройки системы контроля приложений осуществляются с помощью профилей, в соответствии с настройками которых приложения на станциях (или для определенных пользователей) будут запускаться или блокироваться. До создания профилей и назначения их на станции антивирусной сети запуск всех приложений разрешается.
5. Назначьте станции, пользователей и/или их группы, на которые будут распространяться настройки созданного профиля.
6. Задайте настройки профиля.

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.

Чтобы создать профиль

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.

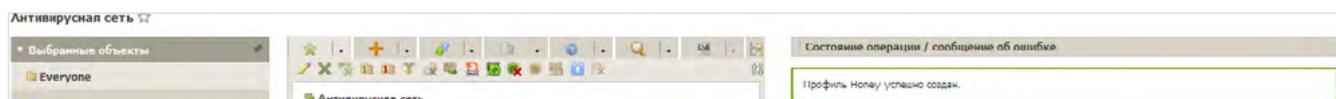
2. В открывшемся окне на панели инструментов выберите пункт **Добавить объект сети** → **Создать профиль**.



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



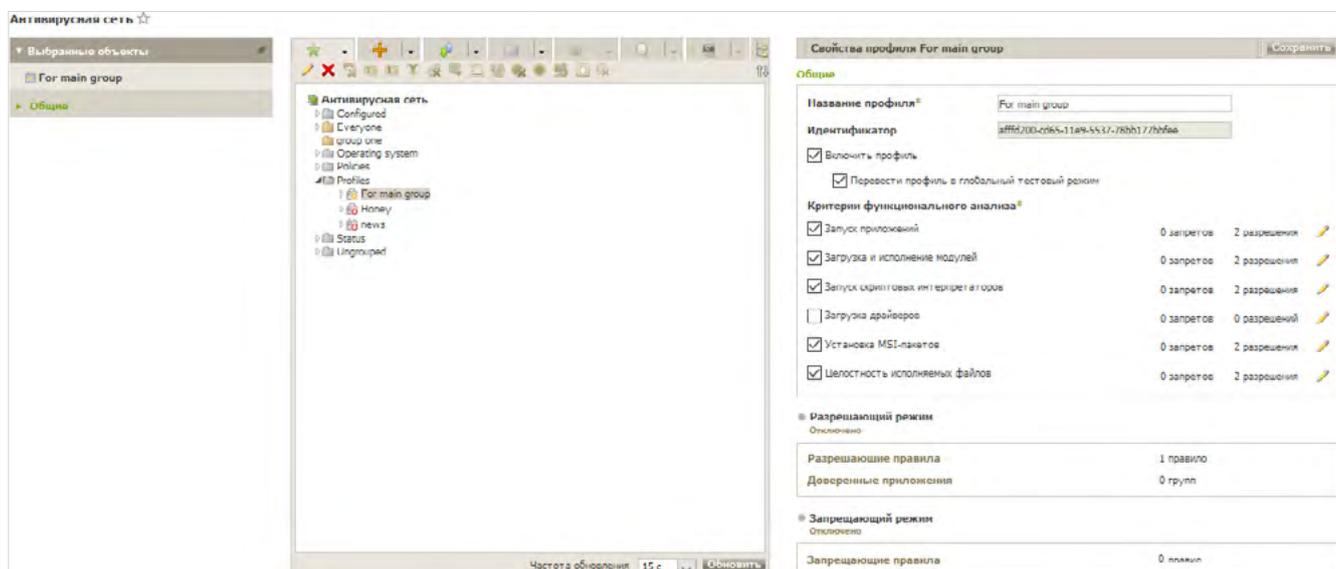
4. Нажмите кнопку **Сохранить**.

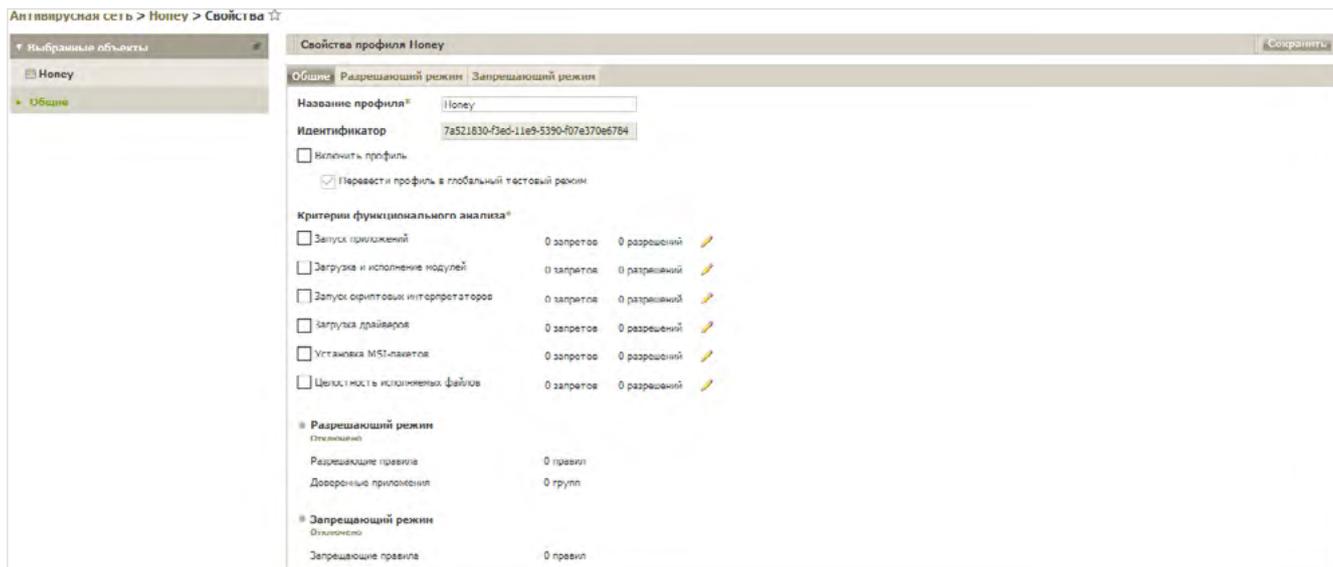


5. Новый профиль будет создан и помещен в группу **Profiles** дерева Антивирусной сети. После создания профиля его нужно настроить (установить нужные ограничения, правила работы), а также назначить станциям и пользователям антивирусной сети.

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).





- 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.
- В разделе **Критерии функционального анализа** установите флаги для событий, которые будут контролироваться.

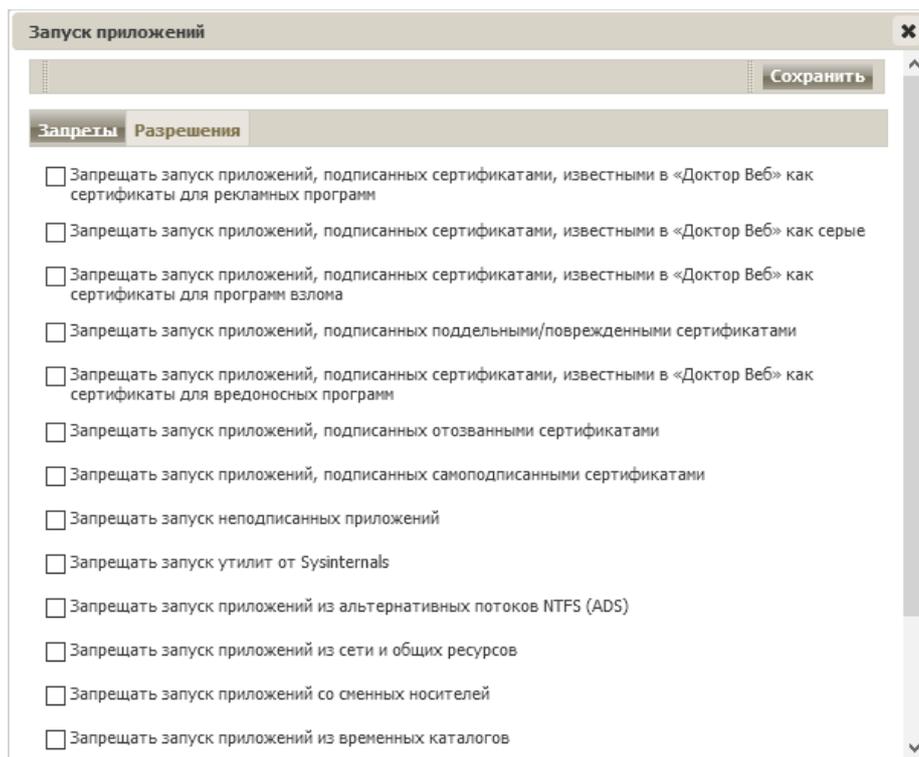
Имеется 6 групп критериев функционального анализа:

- 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, с помощью которых мы можем отметить правила, по которым будут выявляться подозрительные программы. Для задания расширенных настроек по каждому выбранному типу событий критерию нажмите  (**Редактировать**) напротив соответствующего типа событий. Откроется окно со списком настроек.

Рассмотрим группы критериев подробнее.

Запуск приложений



Запуск приложений

Сохранить

Запреты | Разрешения

- 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 приложений, подписанных самоподписанными сертификатами
- Запрещать запуск неподписанных приложений
- Запрещать запуск утилит от Sysinternals
- Запрещать запуск приложений из альтернативных потоков NTFS (ADS)
- Запрещать запуск приложений из сети и общих ресурсов
- Запрещать запуск приложений со сменных носителей
- Запрещать запуск приложений из временных каталогов



Запуск приложений

Сохранить

Запреты | Разрешения

- Разрешать запуск системных приложений и приложений от компании Microsoft
- Разрешать запуск приложений, известных/доверенных «Доктор Веб»

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 приложений Windows / Microsoft Store (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.

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

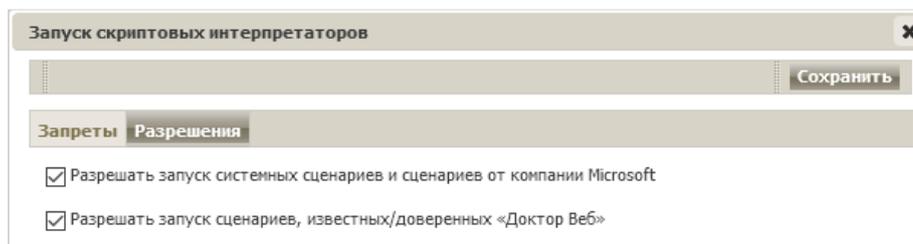


Запуск скриптовых интерпретаторов

Сохранить

Запреты Разрешения

- Запрещать запуск CMD/BAT-сценариев
- Запрещать запуск HTA-сценариев
- Запрещать запуск VBScript/JavaScript
- Запрещать запуск PowerShell-сценариев
- Запрещать запуск REG-сценариев
- Запрещать запуск сценариев из альтернативных потоков NTFS (ADS)
- Запрещать запуск сценариев из сети и общих ресурсов
- Запрещать запуск сценариев со сменных носителей
- Запрещать запуск сценариев из временных каталогов



Запуск скриптовых интерпретаторов

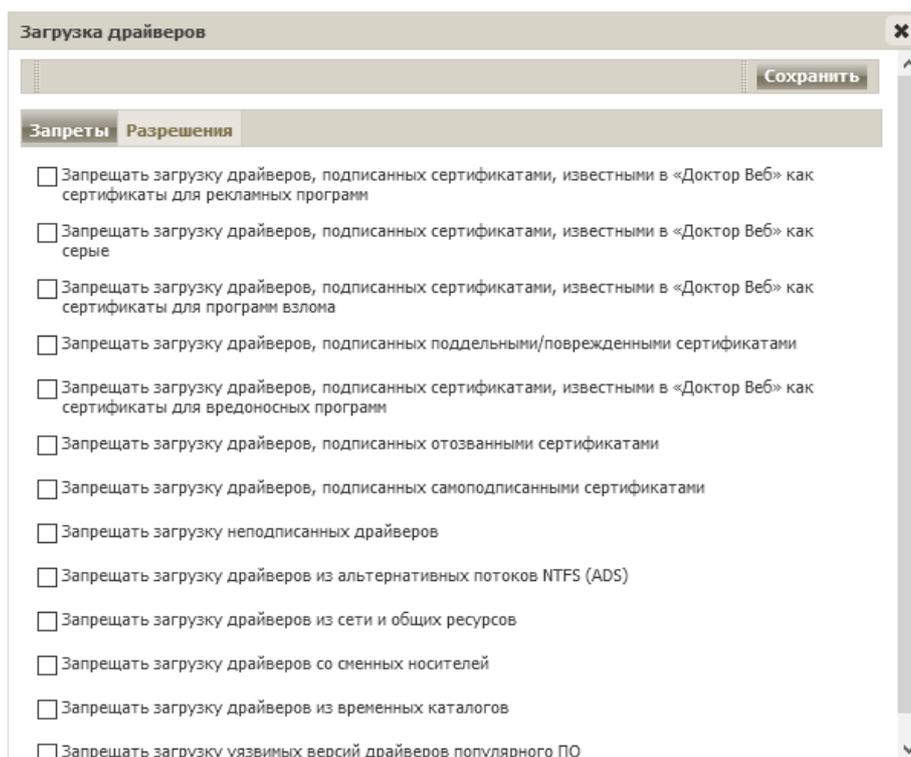
Сохранить

Запреты **Разрешения**

- Разрешать запуск системных сценариев и сценариев от компании Microsoft
- Разрешать запуск сценариев, известных/доверенных «Доктор Веб»

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

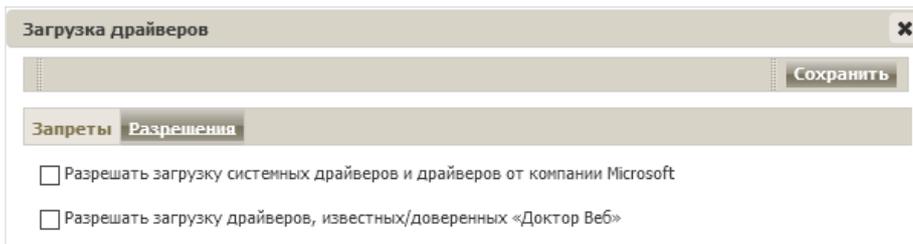


Загрузка драйверов

Сохранить

Запреты Разрешения

- Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для рекламных программ
- Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как серые
- Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для программ взлома
- Запрещать загрузку драйверов, подписанных поддельными/поврежденными сертификатами
- Запрещать загрузку драйверов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для вредоносных программ
- Запрещать загрузку драйверов, подписанных отозванными сертификатами
- Запрещать загрузку драйверов, подписанных самоподписанными сертификатами
- Запрещать загрузку неподписанных драйверов
- Запрещать загрузку драйверов из альтернативных потоков NTFS (ADS)
- Запрещать загрузку драйверов из сети и общих ресурсов
- Запрещать загрузку драйверов со сменных носителей
- Запрещать загрузку драйверов из временных каталогов
- Запрещать загрузку уязвимых версий драйверов популярного ПО



Загрузка драйверов [X]

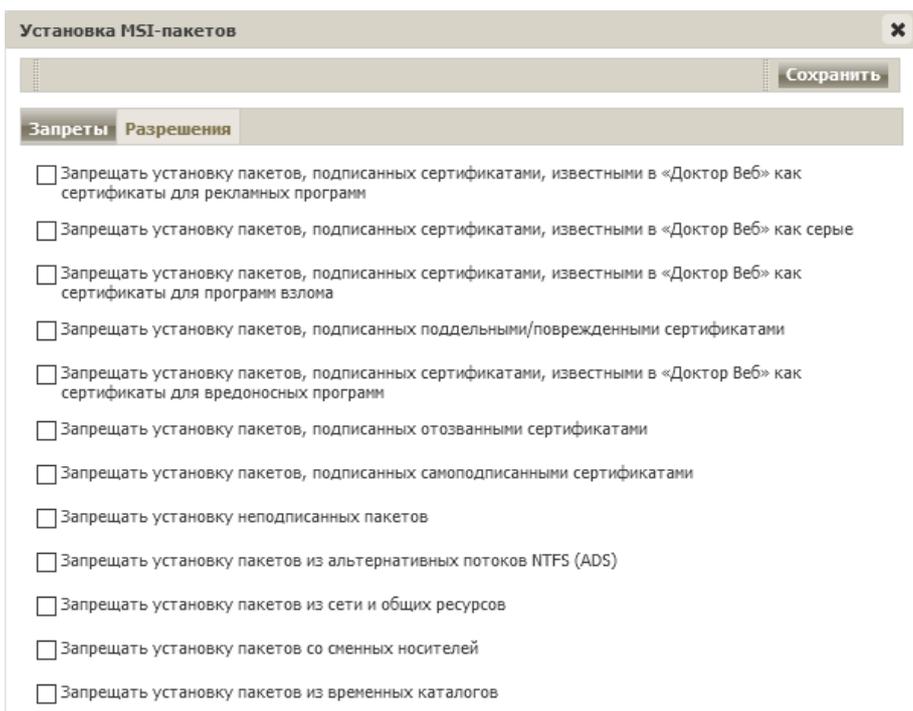
Сохранить

Запреты | **Разрешения**

- Разрешать загрузку системных драйверов и драйверов от компании Microsoft
- Разрешать загрузку драйверов, известных/доверенных «Доктор Веб»

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

Установка MSI-пакетов

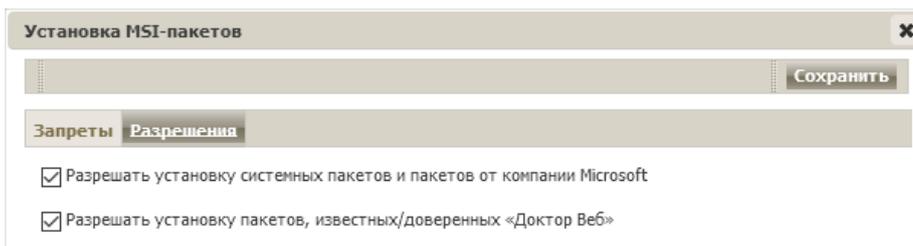


Установка MSI-пакетов [X]

Сохранить

Запреты | **Разрешения**

- Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для рекламных программ
- Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как серые
- Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для программ взлома
- Запрещать установку пакетов, подписанных поддельными/поврежденными сертификатами
- Запрещать установку пакетов, подписанных сертификатами, известными в «Доктор Веб» как сертификаты для вредоносных программ
- Запрещать установку пакетов, подписанных отозванными сертификатами
- Запрещать установку пакетов, подписанных самоподписанными сертификатами
- Запрещать установку неподписанных пакетов
- Запрещать установку пакетов из альтернативных потоков NTFS (ADS)
- Запрещать установку пакетов из сети и общих ресурсов
- Запрещать установку пакетов со сменных носителей
- Запрещать установку пакетов из временных каталогов



Установка MSI-пакетов [X]

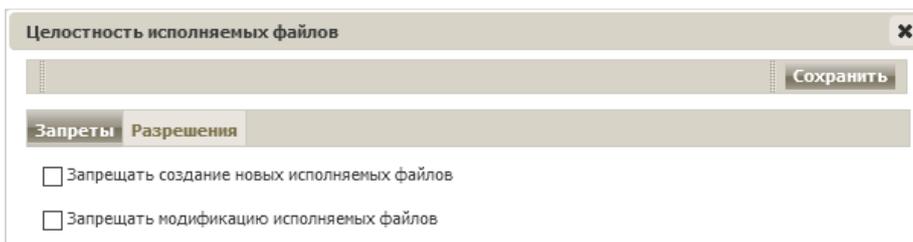
Сохранить

Запреты | **Разрешения**

- Разрешать установку системных пакетов и пакетов от компании Microsoft
- Разрешать установку пакетов, известных/доверенных «Доктор Веб»

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

Целостность исполняемых файлов



Целостность исполняемых файлов [X]

Сохранить

Запреты | **Разрешения**

- Запрещать создание новых исполняемых файлов
- Запрещать модификацию 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.

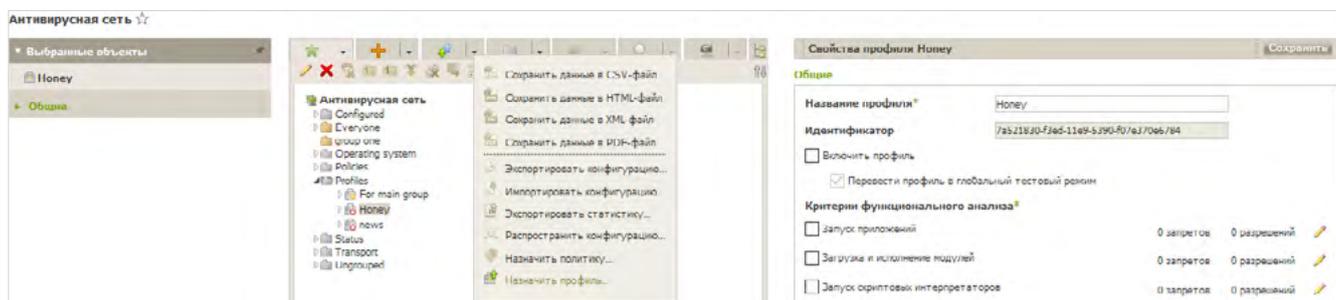
Если вы включите использование какого-либо из типов событий, но не зададите его расширенные настройки, то контроль запуска будет производиться для всех объектов по этому критерию в соответствии с настройками разрешающего или запрещающего режимов. Если вы зададите расширенные настройки, но не включите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

Следующим 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 дан-

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

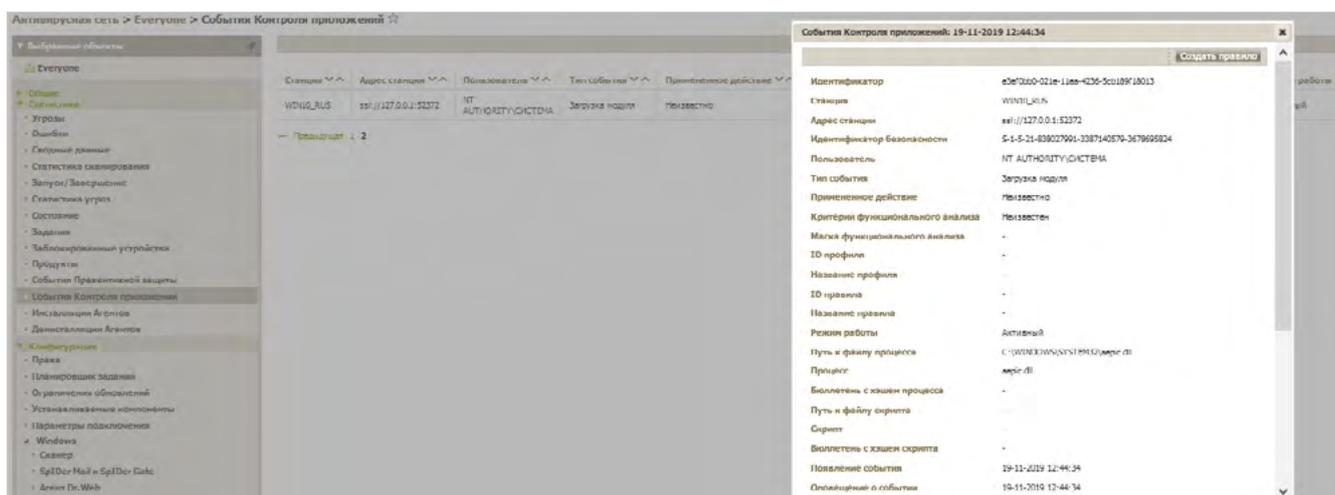


5. Нажмите кнопку **Сохранить**. Все выбранные объекты будут добавлены в список, на который распространяется настраиваемый профиль, и будут отображены в дереве как вложенные объекты настраиваемого профиля.

Если все настройки были проведены корректно, сведения о запускаемых программах будут отображаться в разделе **Статистика → События Контроля приложений**.



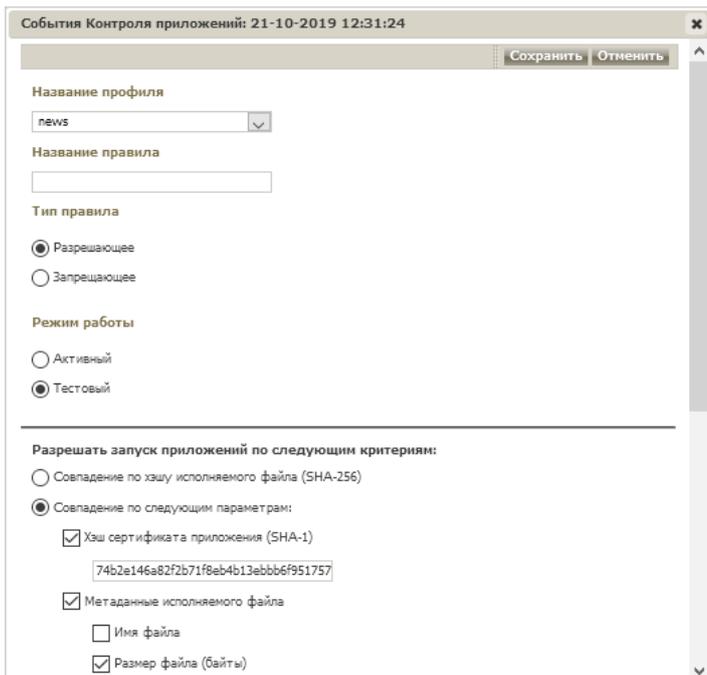
Обнаружив запуск некой программы или модуля, кликните по соответствующей строке таблицы.



1. В открывшемся окне с информацией о выбранном событии нажмите кнопку **Создать правило**.

2. В открывшемся окне задайте:

- а. В выпадающем списке **Название профиля** выберите профиль Контроля приложений, в котором будет создано правило.



- b. В поле **Название правила** задайте название для создаваемого правила.
- c. В разделе **Тип правила** выберите тип создаваемого правила: запрещающее или разрешающее.
- d. Для опции **Режим работы** выберите, в каком режиме будет работать созданное правило.

В режиме **Тестовый** приложения не будут блокироваться на станциях, однако будет осуществляться запись журнала активности, как при включенных настройках. Результаты потенциальных блокировок приложений по созданному правилу будут отображаться в разделе **События Контроля приложений**.

- e. В разделе **Запрещать запуск приложений по следующим критериям / Разрешать запуск приложений по следующим критериям** поля заполняются автоматически в соответствии с данными приложения, на основе которого создается правило. При необходимости данные можно отредактировать.

3. Нажмите **Сохранить**. Правило будет создано в заданном профиле Контроля приложений. Кроме того, что правила Контроля приложений могут создаваться исходя из статистики запуска приложений, правила могут быть созданы и вручную.

Предположим, вы хотите запретить несанкционированный запуск пользователями утилиты **drw_remover.exe**.

Вычислить хеш-сумму данного файла можно с помощью утилиты **CertUtil**, по умолчанию входящей в комплект OS Windows.

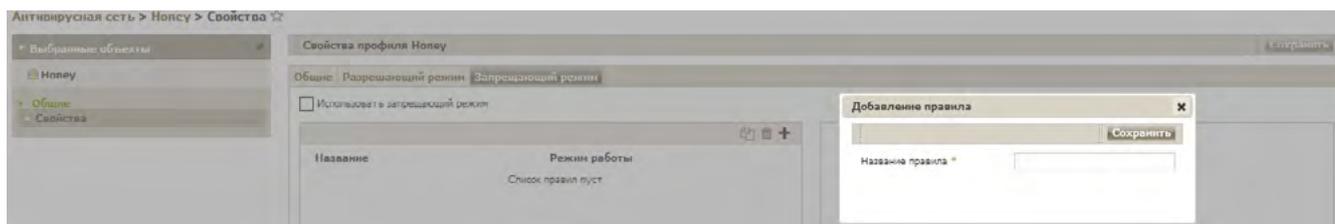
Чтобы узнать хеш-сумму файла, необходимо запустить командную строку (например, последовательно вызвав **Пуск** → **Все программы** → **Стандартные** → **Командная строка**) и выполнить команду `certutil -hashfile c:file SHA256`, где `c:file` — путь до файла.

```
C:\temp>certutil -hashfile drw_remover.exe SHA256
SHA256 hash of drw_remover.exe:
14f9a93a690f5c607cef6b5d36b122e31d7f164e2d64dd51e5d0d7ee9872b3c8
CertUtil: -hashfile command completed successfully.
```

Данную задачу можно выполнить также и с помощью иных утилит, например команды PowerShell `Get-FileHash _путь_к_файлу| Format-List`. При использовании команды в таком виде, хеш вычисляется по алгоритму SHA256.

Для добавления запрета используем **Запрещающий режим** ранее созданного правила.

1. Откроем ранее созданное правило и перейдем на закладку **Запрещающий режим**. По умолчанию режим выключен. Для его использования установите флаг **Использовать запрещающий режим**.
2. Для создания правила нажмите кнопку **+** (**Создать правило**) и в окне **Добавление правила** задайте **Название правила**.



Нажмите **Сохранить**.

3. В списке правил выберите созданное правило и задайте его настройки на открывшейся панели свойств — в данном примере укажите контрольную сумму вредоносного файла.
 - a. Установите флаг **Включить правило**, чтобы начать использовать правило.
 - b. Если вы хотите проверить работу правила без применения его на станциях, установите флаг **Перевести правило в тестовый режим**. В противном случае правило будет работать в активном режиме с блокировкой приложений на станциях по заданным настройкам правила.
 - c. В разделе **Запрещать запуск приложений по следующим критериям** укажите контрольную сумму вредоносного файла.

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

- «ДокторВеб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недеklarированных 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.

<u>Сертификаты ФСТЭК России</u>	<u>Сертификаты Минобороны России</u>	<u>Сертификаты ФСБ России</u>	<u>Все сертификаты и товарные знаки</u>
---	--	---	---

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



© ООО «Доктор Веб»,
2003–2019

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>