



Запрет запуска устаревшего ПО с помощью Контроля приложений в Dr.Web Enterprise Security Suite 12.0



Dr.Web Enterprise Security Suite 12.0

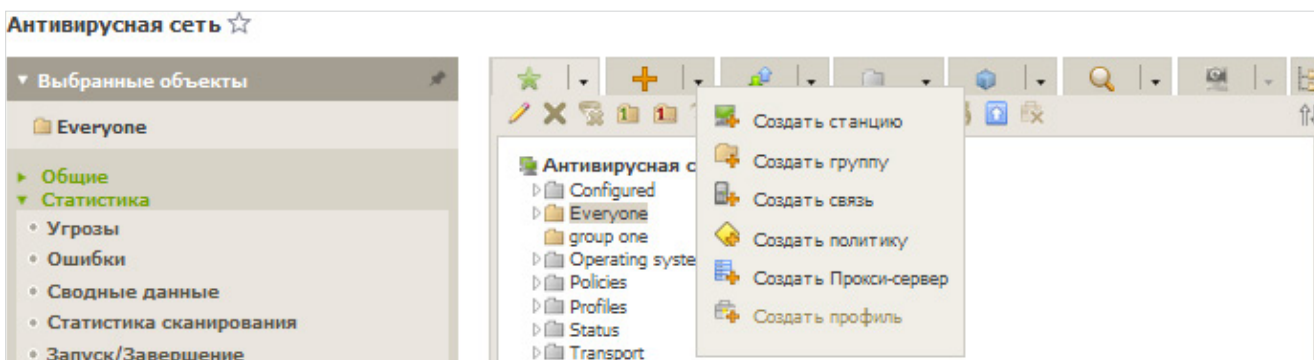
Запрет запуска устаревшего ПО с помощью Контроля приложений

Устаревшее ПО — одна из проблем безопасности. Пользователи не желают обновляться, а через незакрытые уязвимости проникают вредоносные программы. К счастью, выход есть. **Контроль приложений** Центра управления Dr.Web Enterprise Suite способен запретить запуск устаревшего ПО.

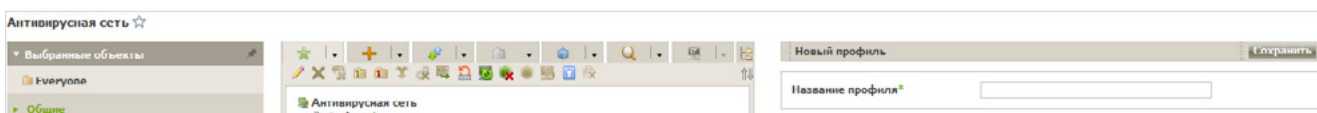
Настройки системы контроля приложений осуществляются с помощью профилей, в соответствии с настройками которых приложения на станциях (или для определенных пользователей) будут запускаться или блокироваться.

Чтобы создать профиль

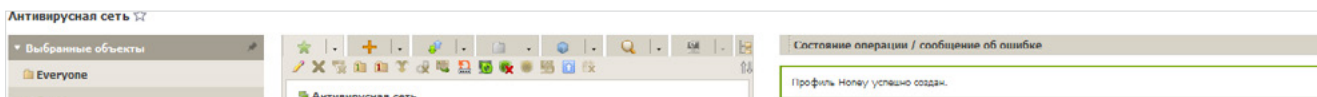
1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне на панели инструментов выберите пункт **Добавить объект сети** → **Создать профиль**.



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



4. Нажмите кнопку **Сохранить**.

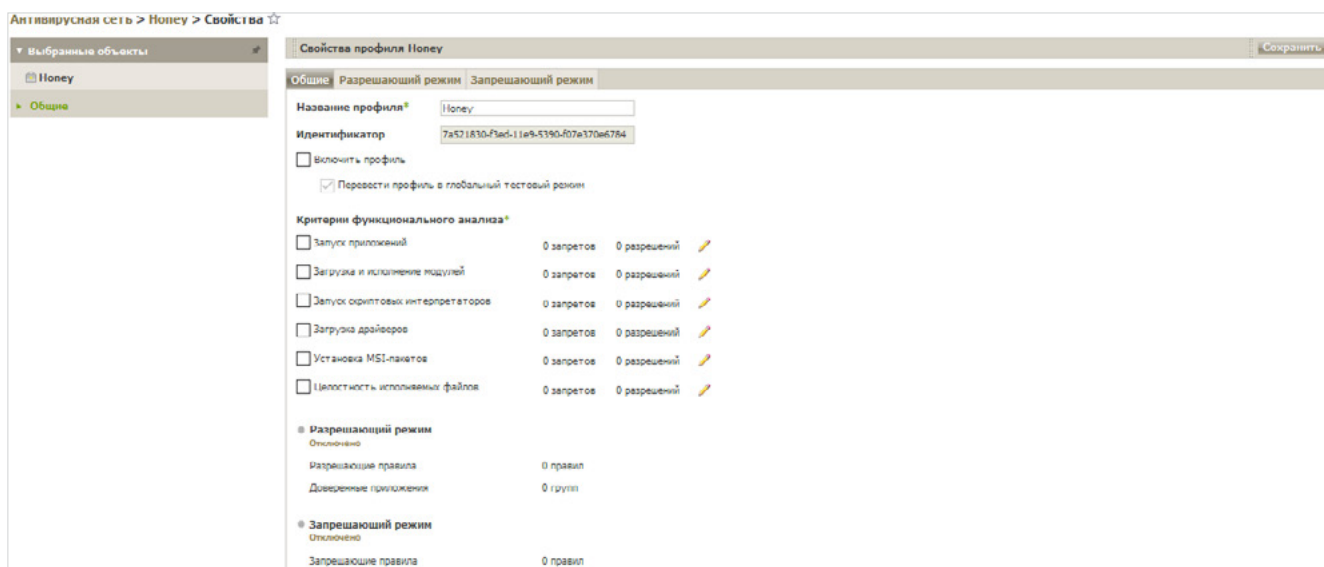
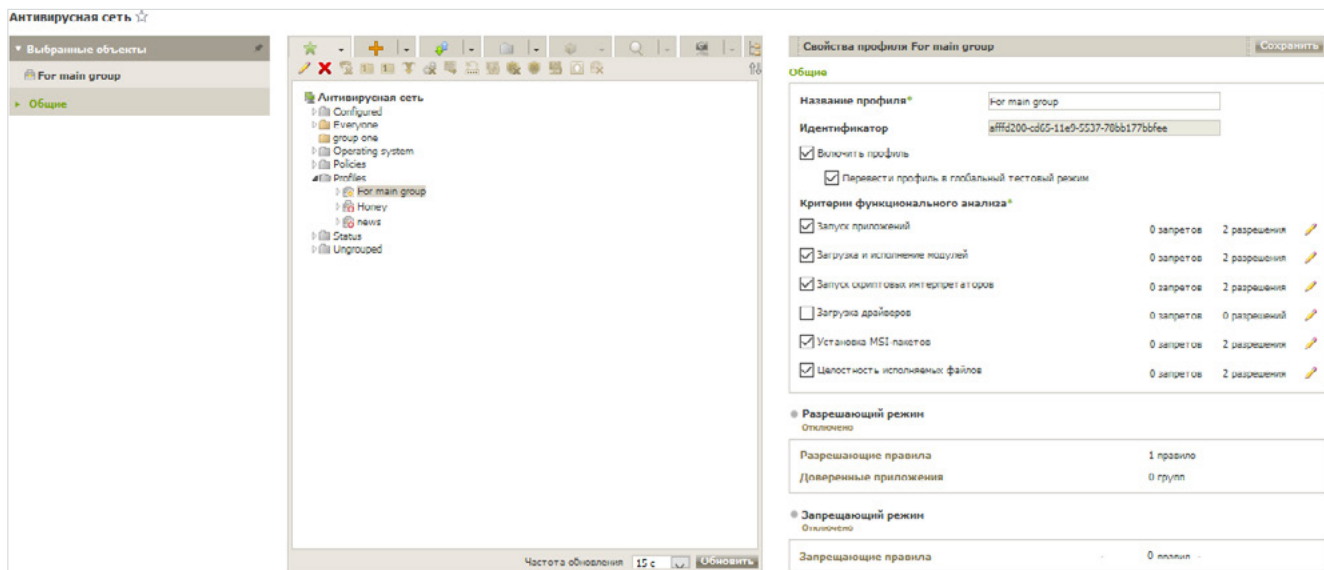


5. Новый профиль будет создан и помещен в группу **Profiles** дерева Антивирусной сети. После создания профиля его нужно настроить (становить нужные ограничения, правила работы), а также назначить станциям и пользователям антивирусной сети.

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

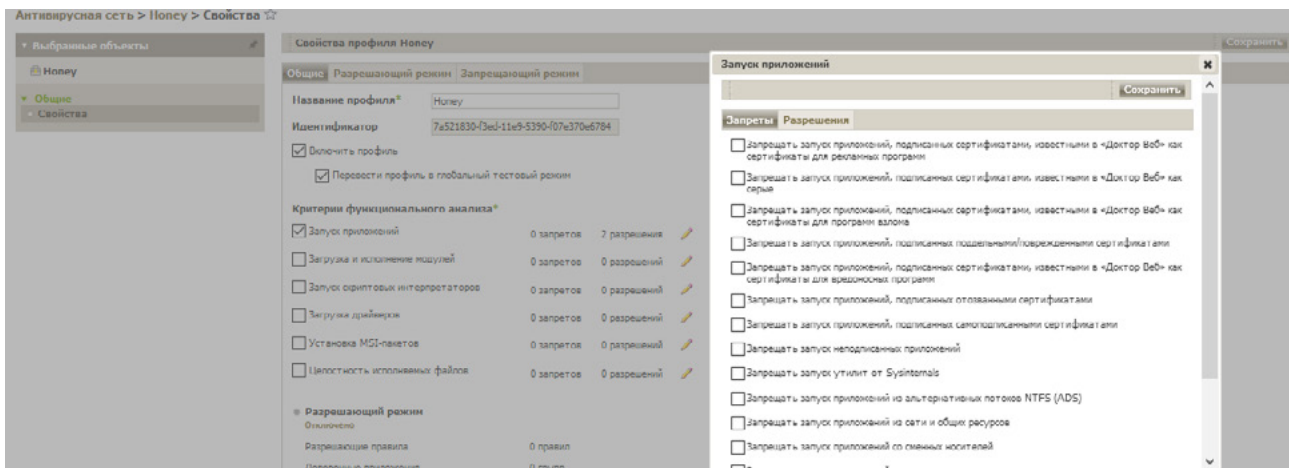
иконку профиля в дереве антивирусной сети, или выберите профиль и затем выберите пункт **Свойства** управляющего меню (откроется окно со свойствами профиля).



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.

Для задания расширенных настроек по каждому выбранному типу событий критерию нажмите  (**Редактировать**) напротив соответствующего типа событий. Откроется окно со списком настроек.



Установите флаги для тех настроек, которые должны выполняться.

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.

5. **Запрещающий режим** подразумевает, что на всех контролируемых станциях запрещается запуск только тех приложений, которые соответствуют запрещающим правилам. Все остальные приложения разрешаются.

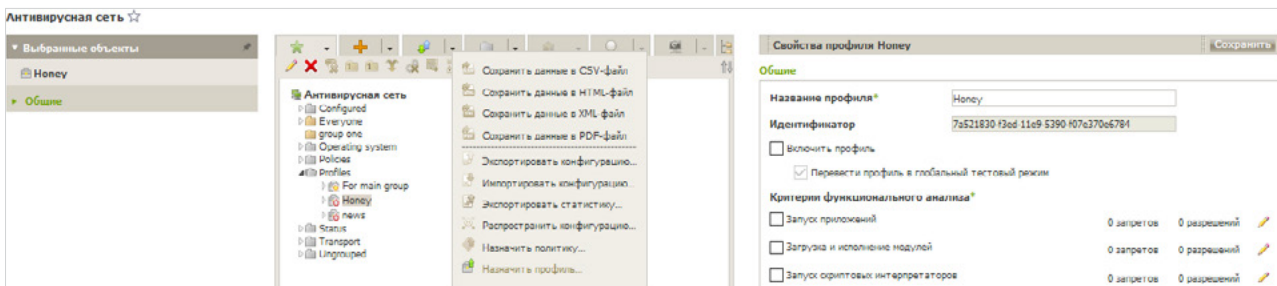
Чтобы включить или отключить режим, а также настроить правила, перейдите в раздел **Запрещающий режим** для перехода в соответствующий раздел.

1. Чтобы использовать запрещающий режим, установите флаг **Использовать запрещающий режим** на вкладке **Запрещающий режим**.

2. Нажмите **Сохранить**.

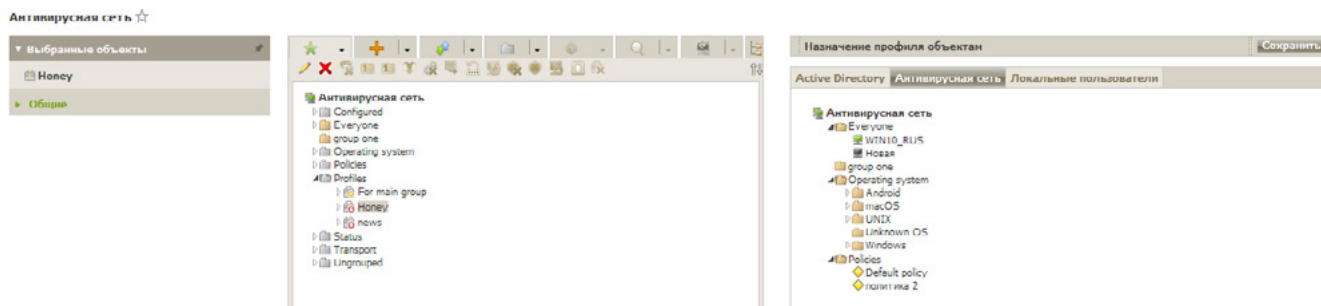
Вторым этапом настройки системы контроля запуска приложений является назначение созданного и настроенного профиля станциям или пользователям антивирусной сети.

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.

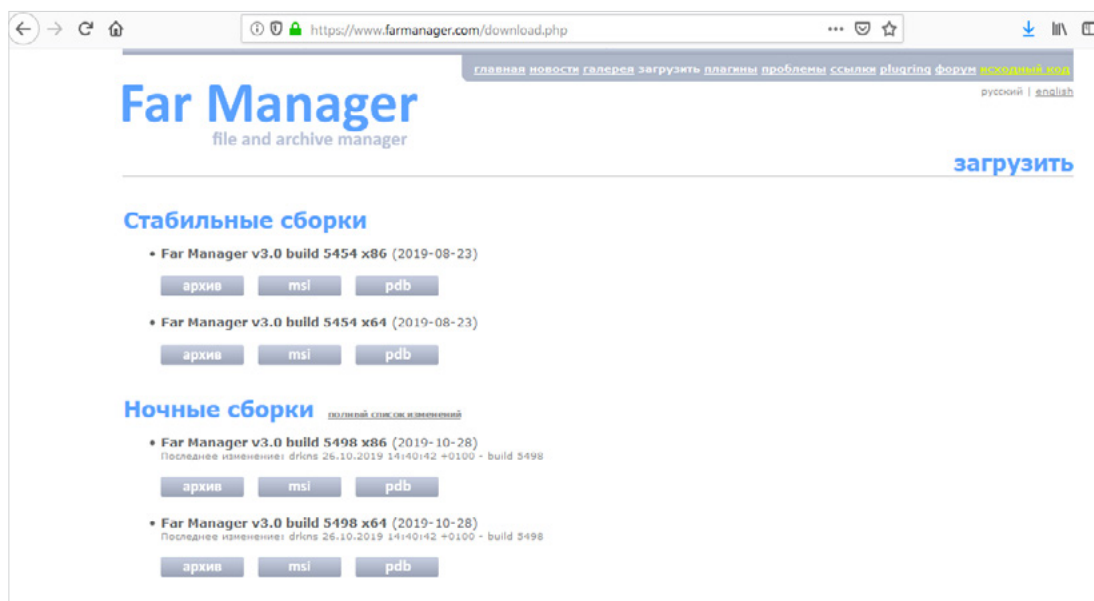
На вкладке **Антивирусная сеть** вы можете выбрать группы станций (настройки будут распространяться на учетные записи всех пользователей всех станций, входящих в данные группы) или отдельные станции в группах (настройки будут распространяться на учетные записи всех пользователей выбранных станций):



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.

Теперь можно приступить к созданию запрещающих правил.

В качестве примера возьмем одну из популярных утилит — Far Manager и скачаем две его версии.

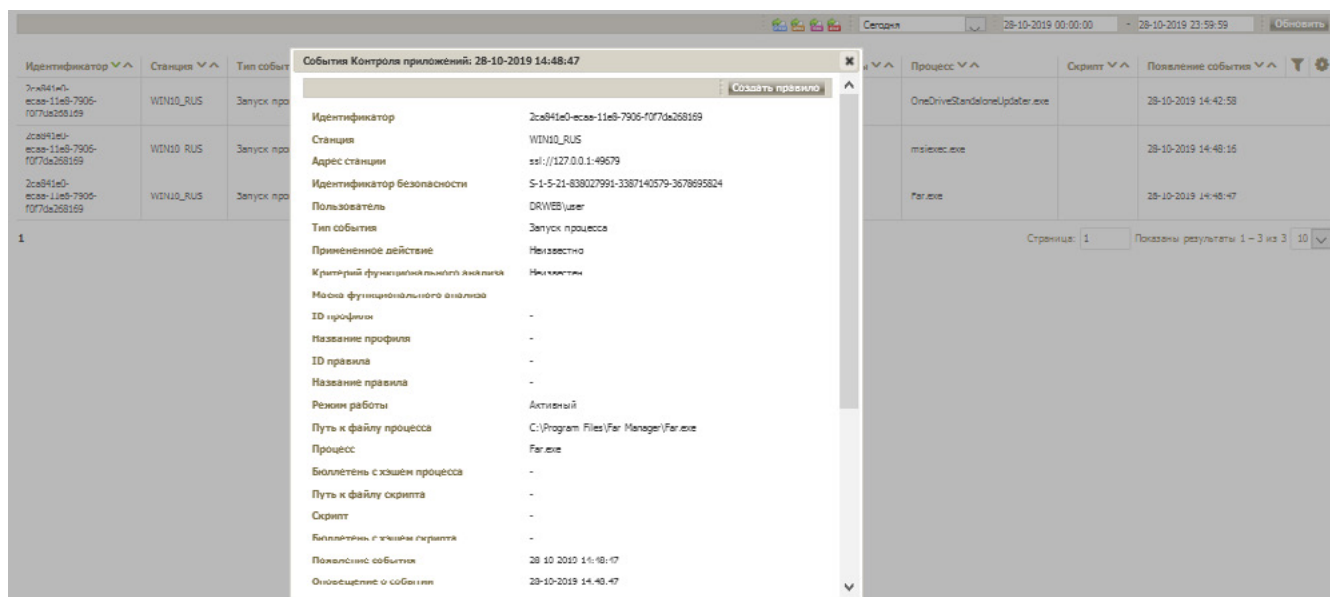


Установим более старую версию. Запустим ее.

Переходим в раздел **Статистика** → **События Контроля приложений**.

Идентификатор	Станция	Тип события	Применённое действие	Название профиля	Название правила	Режим работы	Процесс	Скрипт	Появление события
2c6941e0- e5aa-11e8-7906- f0770a268169	WIN10_RUS	Запуск процесса	Неизвестно			Активный	OneDriveStandaloneUpdater.exe		28-10-2019 14:42:58
2c6941e0- e5aa-11e8-7906- f0770a268169	WIN10_RUS	Запуск процесса	Неизвестно			Активный	msiexec.exe		28-10-2019 14:48:16
2c6941e0- e5aa-11e8-7906- f0770a268169	WIN10_RUS	Запуск процесса	Неизвестно			Активный	Far.exe		28-10-2019 14:48:47

Кликните по строке с информацией о запущенной программе.



Если мы прокрутим открывшееся окно, то увидим нужную нам информацию о версии программы.



Прокрутите обратно и кликните **Создать правило**.

События Контроля приложений: 28-10-2019 14:48:47

Сохранить Отменить

Название профиля

For main group

news

Money

For main group

Тип правила

Разрешающее

Запрещающее

Режим работы

Активный

Тестовый

Разрешать запуск приложений по следующим критериям:

Совпадение по хэшу исполняемого файла (SHA-256)

Совпадение по следующим параметрам:

Хэш сертификата приложения (SHA-1)

Метаданные исполняемого файла

Имя файла

Размер файла (байты)

В выпадающем списке профилей выберите тот, где будете создавать запрещающее правило.

События Контроля приложений: 28-10-2019 14:48:47

Запрещающее

Режим работы

Активный

Тестовый

Запрещать запуск приложений по следующим критериям:

Совпадение по хэшу исполняемого файла (SHA-256)

Совпадение по следующим параметрам:

Хэш сертификата приложения (SHA-1)

Метаданные исполняемого файла

Имя файла

Размер файла (байты)

Версия файла

= 3.0.5454.0

Описание файла

Исходное имя файла

Название продукта

Версия продукта

= 3.0.5454.0

Отметьте переключатели типа правила (**Запрещающее**) и режима работы (для простоты выберем **Активный**). Завершите создание правила.

Запрещающее правило oldfar в профиле For main group успешно создано.

Идентификатор	Станция	Тип события	Примененное действие	Название профиля	Название правила	Режим работы	Процесс	Скринт	Появление события
2ca941e0- e5ae-11e9-7906- f073a268169	WIN10_RUS	Запуск процесса	Неизвестно			Активный	OneDriveBandoneUpdater.exe		28-10-2019 14:42:58
2ca941e0- e5ae-11e9-7906- f073a268169	WIN10_RUS	Запуск процесса	Неизвестно			Активный	oldfar.exe		28-10-2019 14:48:16
2ca941e0- e5ae-11e9-7906- f073a268169	WIN10_RUS	Запуск процесса	Неизвестно			Активный	Far.exe		28-10-2019 14:48:47

Не забудьте, что для работы запрещающих правил в профиле должен быть отключен тестовый режим для профиля в целом и включена работа запрещающих правил.

Антивирусная сеть > For main group > Свойства

Свойства профиля For main group

Общие | Разрешающий режим | Запрещающий режим

Название профиля: for main group
Идентификатор: 2f1f0200-e985-11e9-8537-78a61776afec

Включить профиль
 Переместить профиль в глобальный тестовый режим

Антивирусная сеть > For main group > Свойства

Свойства профиля For main group

Общие | Разрешающий режим | Запрещающий режим

Использовать запрещающий режим

Название	Режим работы
oldfar	Активный

Если эти свойства не установлены, установите их и нажмите **Сохранить**.

Антивирусная сеть > For main group > Свойства

Свойств профиля For main group

Общие | Разрешающий режим | Запрещающий режим

Операция успешно завершена

Запускаем утилиту. Точнее, пытаемся запустить. Запуска не происходит, а в статистике появляется запись:

2ca941e0- e5ae-11e9-7906- f073a268169	WIN10_RUS	Запуск процесса	Заблокирован запрещающими правилами	For main group	oldfar	Активный	Far.exe		28-10-2019 15:06:22
---	-----------	-----------------	-------------------------------------	----------------	--------	----------	---------	--	---------------------

Однако если мы обновим утилиту, то она запустится корректно. 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.

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

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

