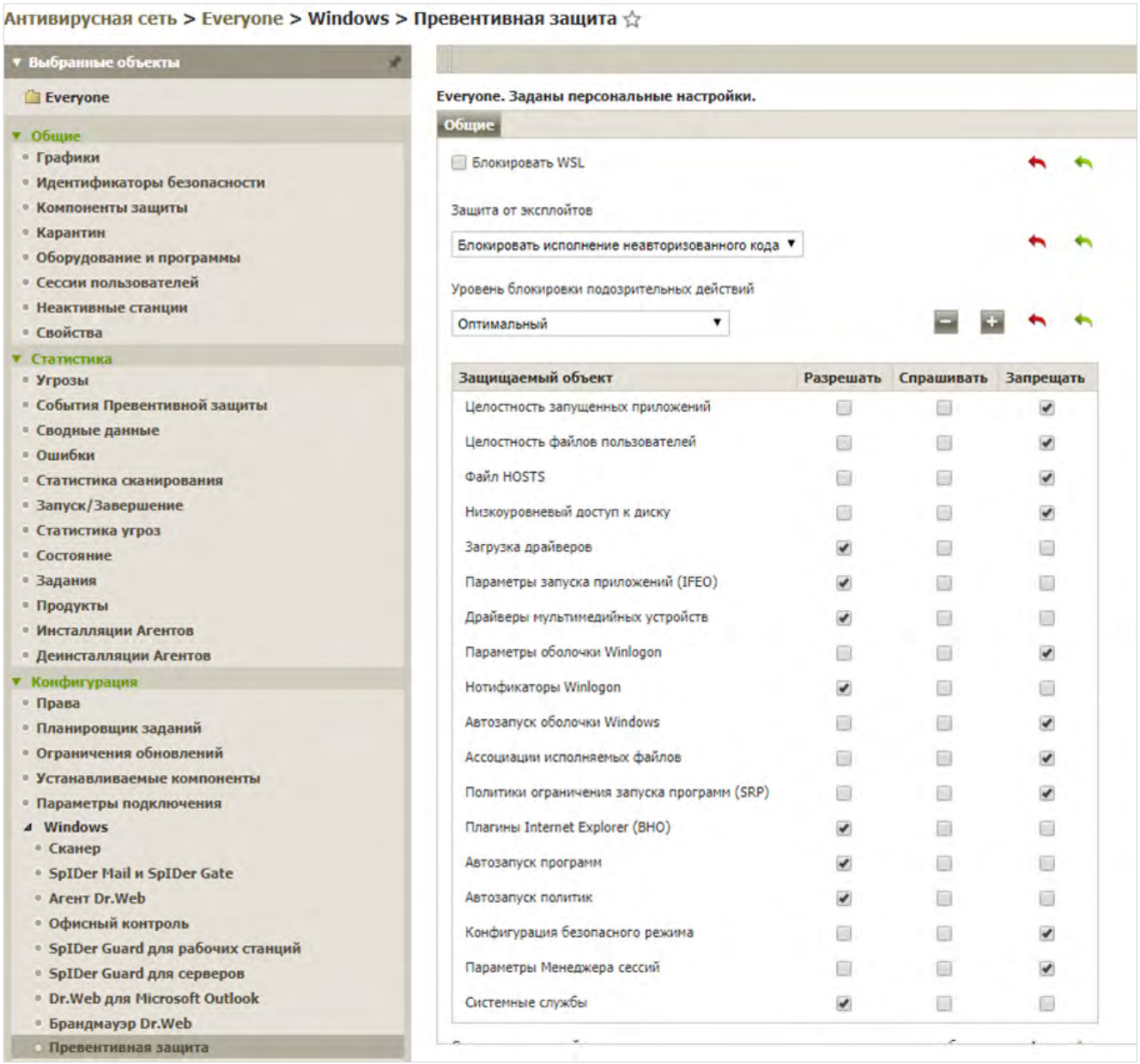
Dr.WEB®
с 1992 года

Мониторинг эффективности защиты от неизвестных угроз

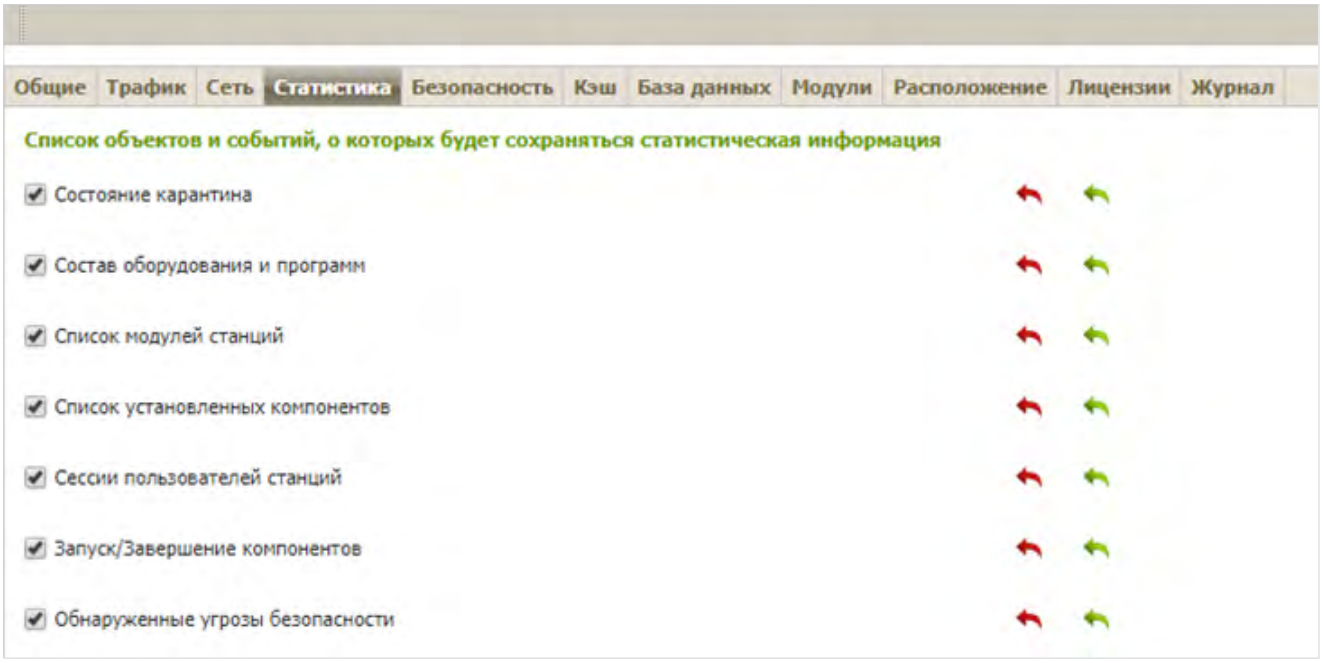
Мониторинг эффективности защиты от неизвестных угроз

Превентивная защита — ключевой компонент антивирусной системы защиты, предотвращающий действие в системе еще не известных угроз — вирусов, сигнатуры которых еще не были добавлены в антивирусные базы, а также любого другого вредоносного ПО за счет контроля запущенных приложений и защиты ключевых точек системы.

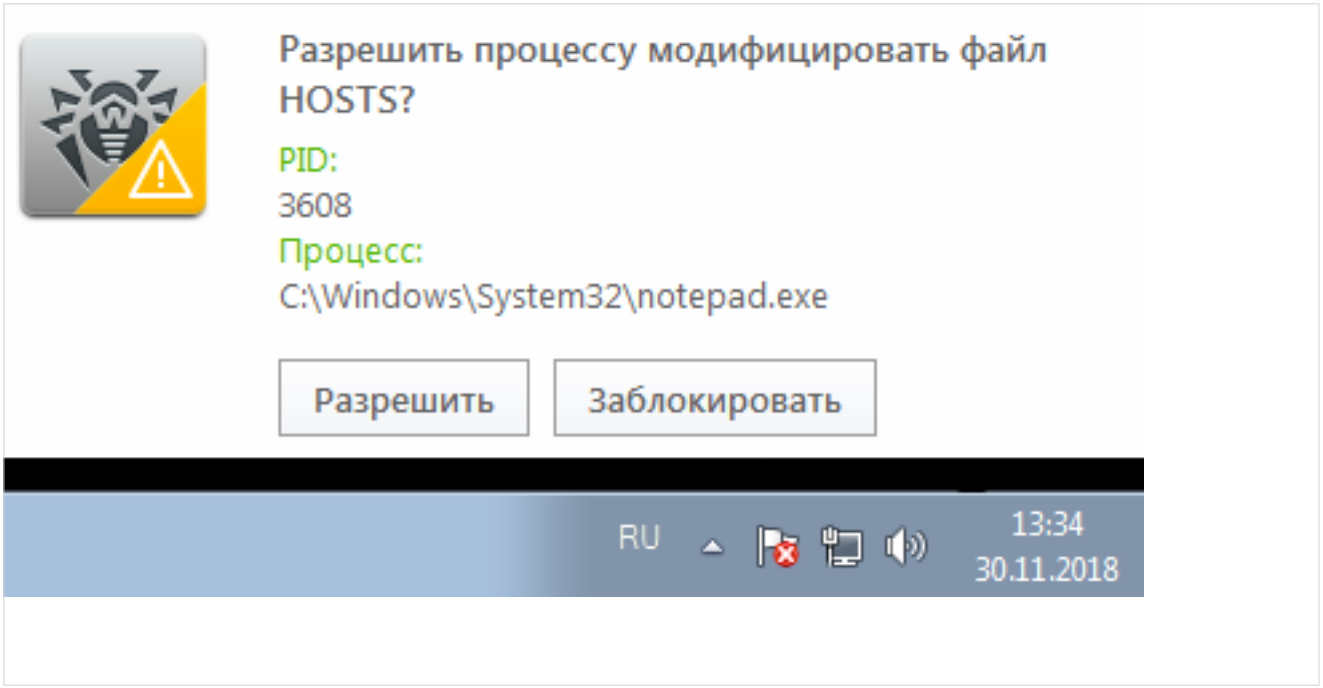
Централизованная настройка **Превентивной защиты** для Агентов осуществляется через Центр управления Сервера Dr.Web в разделе *Антивирусная сеть — Конфигурация — Windows — Превентивная защита*. По умолчанию установлен оптимальный уровень защиты, чтобы Dr.Web отражал большинство возможных атак, работая незаметно для пользователя.



После настройки параметров **Превентивной защиты** можно включить ее в отображаемую на Сервере статистику (*Администрирование — Конфигурация — Конфигурация Сервера Dr.Web — Статистика*). Для этого нужно установить флажок *Обнаруженные угрозы безопасности*.



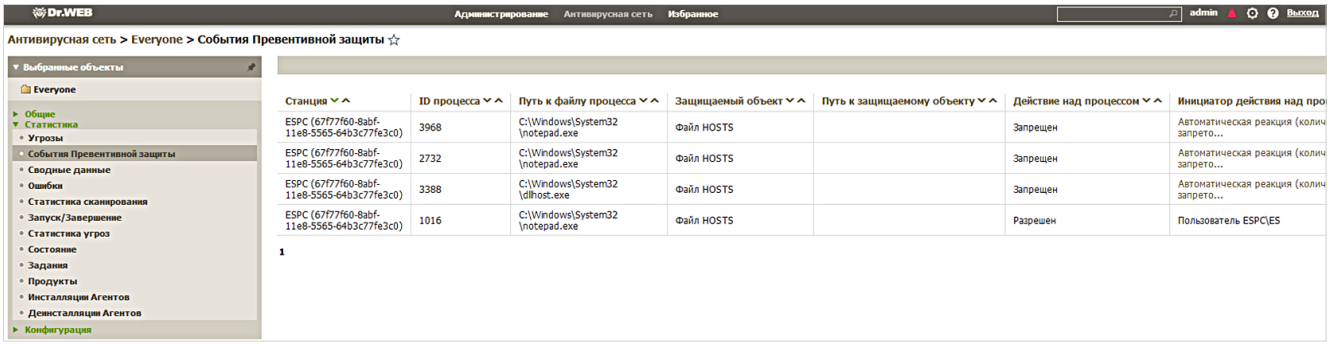
Если **Превентивная защита активна**, а вредоносное ПО пытается внедриться в защищаемый процесс или совершить какие-то запрещенные действия в системе, то пользователь рабочей станции получит уведомление о блокировке или запрос на подтверждение действия.



Администратор антивирусной сети видит все подробности атаки в разделе *Антивирусная сеть — Статистика — События Превентивной защиты* и может предпринять действия по недопущению повторения таких инцидентов в будущем. Это возможно за счет наличия в статистическом отчете исчерпывающих данных о событии (инциденте):

- Станция — имя станции, где произошло событие
- ID процесса — ID процесса, чье действие спровоцировало реакцию Превентивной защиты

- Путь к файлу процесса — путь к файлу, связанному с процессом
- Защищаемый объект — объект, который стал целью атаки
- Путь к защищаемому объекту — путь к объекту, который стал целью атаки
- Действие над процессом — какая была реакция на действия процесса (например, автоматическая блокировка или разрешение)
- Инициатор действия над процессом — кто принял решение о совершении действия (пользователь или автоматически)
- Инициатор процесса — пользователь или приложение, инициировавшее заблокированный процесс
- Появление события — время возникновения события
- Оповещение о событии (от станции) — время, когда станция отправила на Сервер информацию о событии



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
https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru