Dr.WEB®
с 1992 года

Защита критической инфраструктуры в государственных и бизнес-структурах на свежем примере

www.антивирус.рф
www.drweb.ru

Dr.WEB®
с 1992 года

Необходимость защиты
критической инфраструктуры
не вызывает сомнений:
существуют требования государства, прописана ответственность за их нарушение…

И, в принципе, от чего защищаться – известно.

Например (но не только) – от внедрения вредоносных программ.
Но несмотря на то, что защита от вредоносных программ в той или иной мере есть почти у всех, результаты противостояния вирусописателям разнятся.

Почему? Разберем на примере.

Dr.WEB®
с 1992 года

В марте 2019 года в компанию «Доктор Веб»
обратился клиент из государственного учреждения Республики Казахстан
по вопросу наличия вредоносного ПО
на одном из компьютеров корпоративной сети.

Dr.WEB®
с 1992 года

В ходе расследования было установлено,
что сетевая инфраструктура учреждения
была скомпрометирована
как минимум с декабря 2017 года.

Несанкционированное присутствие продолжалось как минимум три года

Dr.WEB®
с 1992 года

И это –
не самое поразительное

Были выявлены совершенно разные семейства троянских программ,
а это позволяет предположить,
что за заражениями могут стоять
сразу несколько хакерских групп.

И да – часть заражений имела зарубежное происхождение:
некоторые найденные трояны используются различными APT-группами Китая.

Dr.WEB®
с 1992 года

Как происходило заражение?

Dr.WEB®
с 1992 года

С использованием уязвимости злоумышленники загружали на компьютер одну из модификаций трояна семейства **BackDoor.PlugX**. Модули полезной нагрузки трояна позволяли удаленно управлять инфицированным компьютером и использовать его для дальнейшего продвижения по сети… После установления присутствия в сети хакерская группа использовала специализированное вредоносное ПО для решения поставленных задач.

Dr.WEB®
с 1992 года

Из интересного

Dr.WEB®
с 1992 года

Семейство обладает руткитом для сокрытия сетевой активности и следов присутствия
в скомпрометированной системе,
обнаружить который удалось при помощи антируткита Dr.Web,
установленного на атакованном сервере.
…В основе программ лежат проекты
с открытым исходным кодом…

Dr.WEB®
с 1992 года

Подведем итог

Dr.WEB®
с 1992 года

- Незакрытые уязвимости
- Возможность установки ПО на компьютеры, интересующие злоумышленников
- Использование вредоносного ПО, частично уже известного
- Использование для создания вредоносного ПО открытого кода
- Методы маскировки, не способные скрыть присутствие трояна от Антируткита Dr.Web

Dr.WEB®
с 1992 года

В августе 2019 года представитель Совбеза сообщил, что в 2018 г. было зафиксировано порядка 17 тыс. кибератак на КИИ в России. Еще на 7 тыс. объектов злоумышленники пытались установить вредоносное ПО.
https://www.tadviser.ru/index.php/Статья:Закон_О_безопасности_критической_информационной_инфраструктуры_Российской_Федерации

Просто установить антивирус (любой) для защиты от вредоносного ПО – недостаточно

Dr.WEB®
с 1992 года

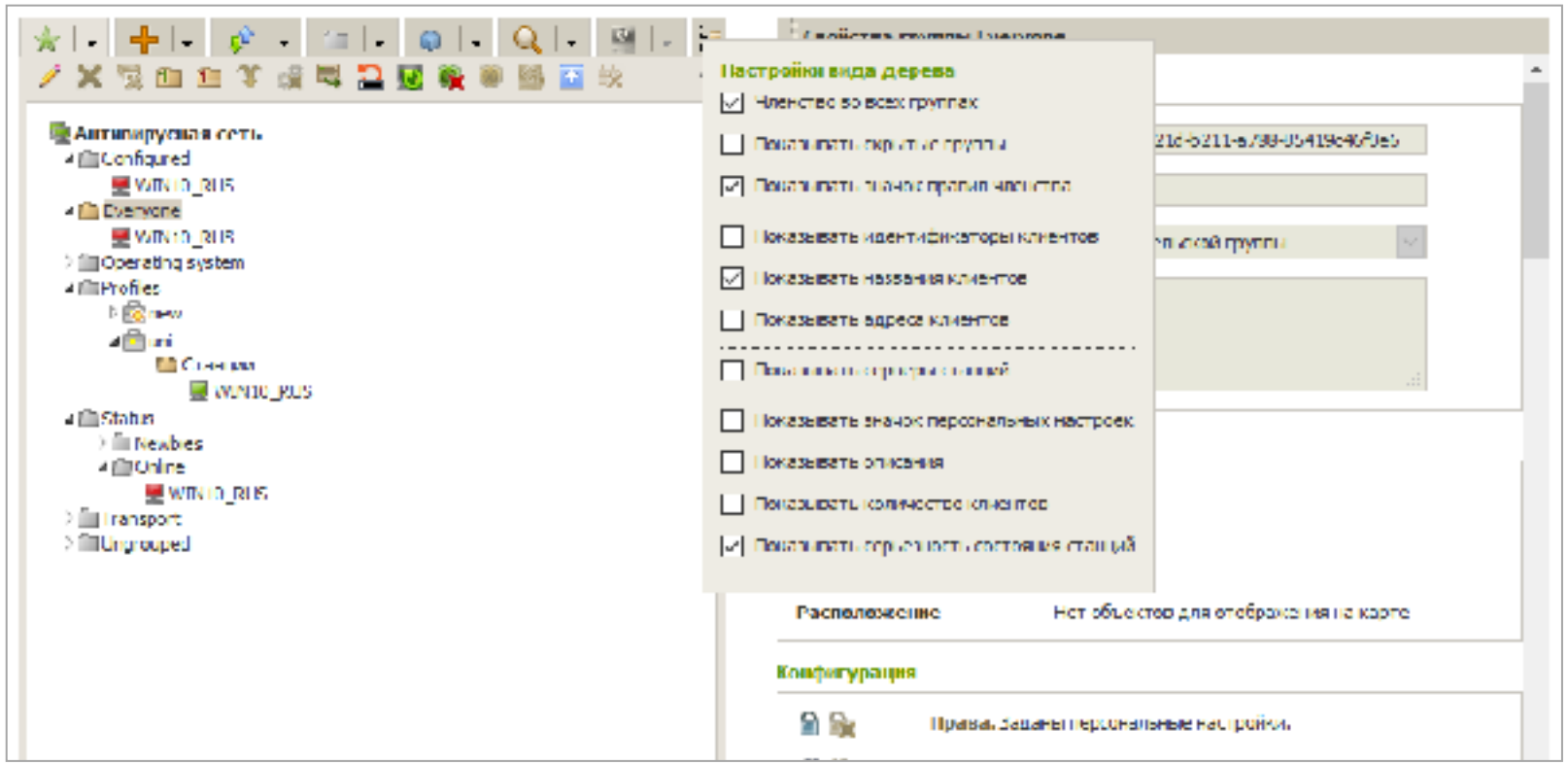
Необходимо:

- Своевременно закрывать уязвимости
- Ограничить возможность несанкционированной установки ПО
- Запретить работу под административными учетными записями
- Использовать надежные пароли и периодически их менять

Dr.WEB®
с 1992 года

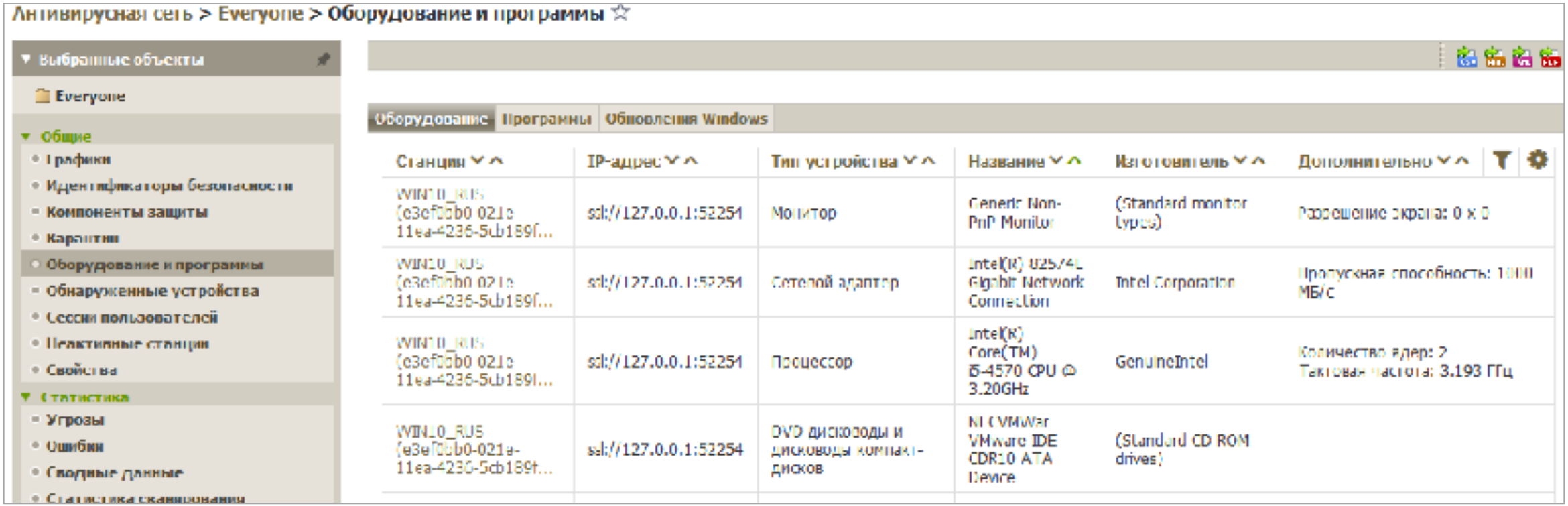
Центр управления Dr.Web:

система комплексной настройки станций на основе политик и правил



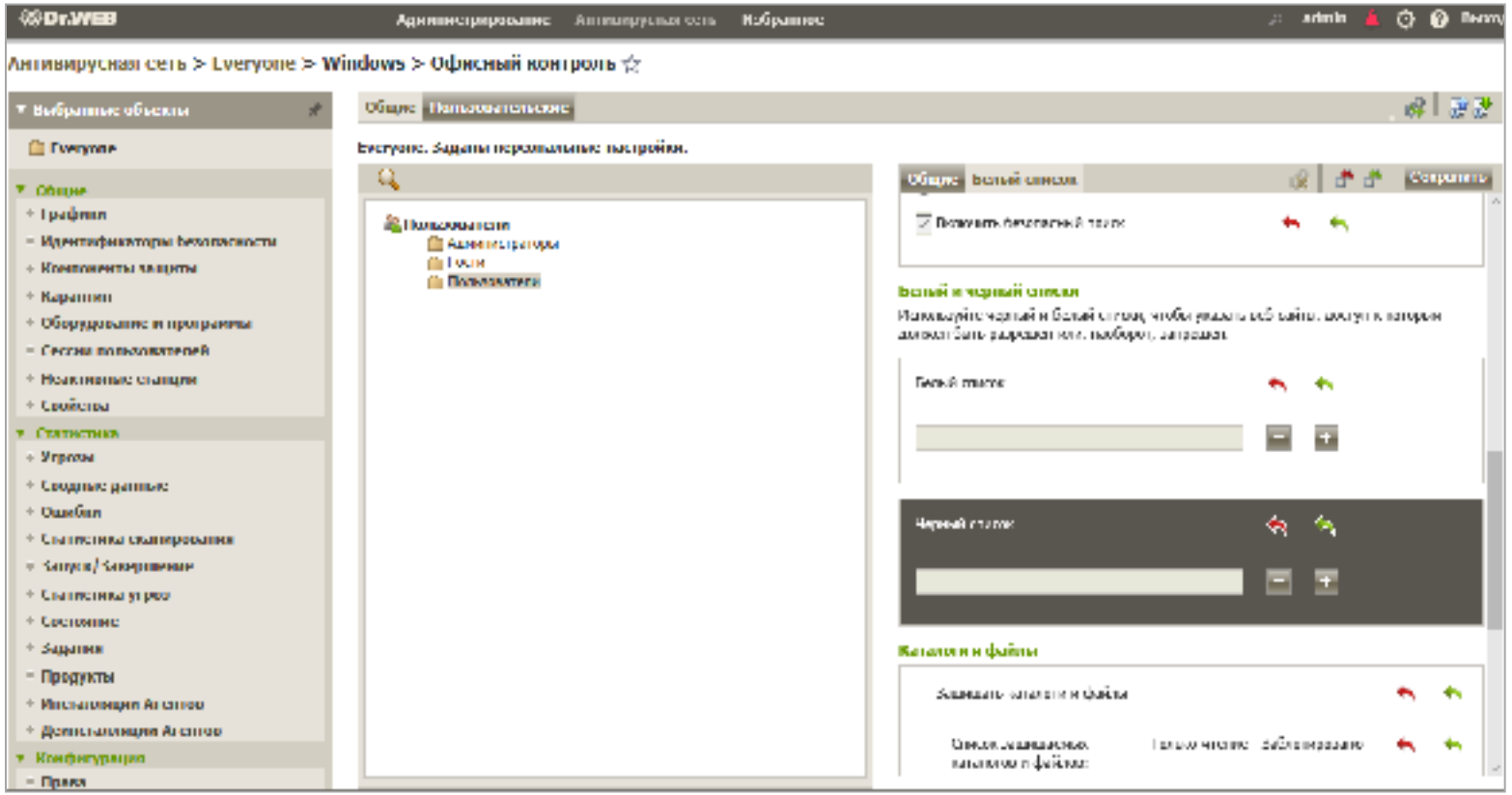
Dr.WEB®
с 1992 года

Оборудование, программы и сменные носители, обнаруженные в сети



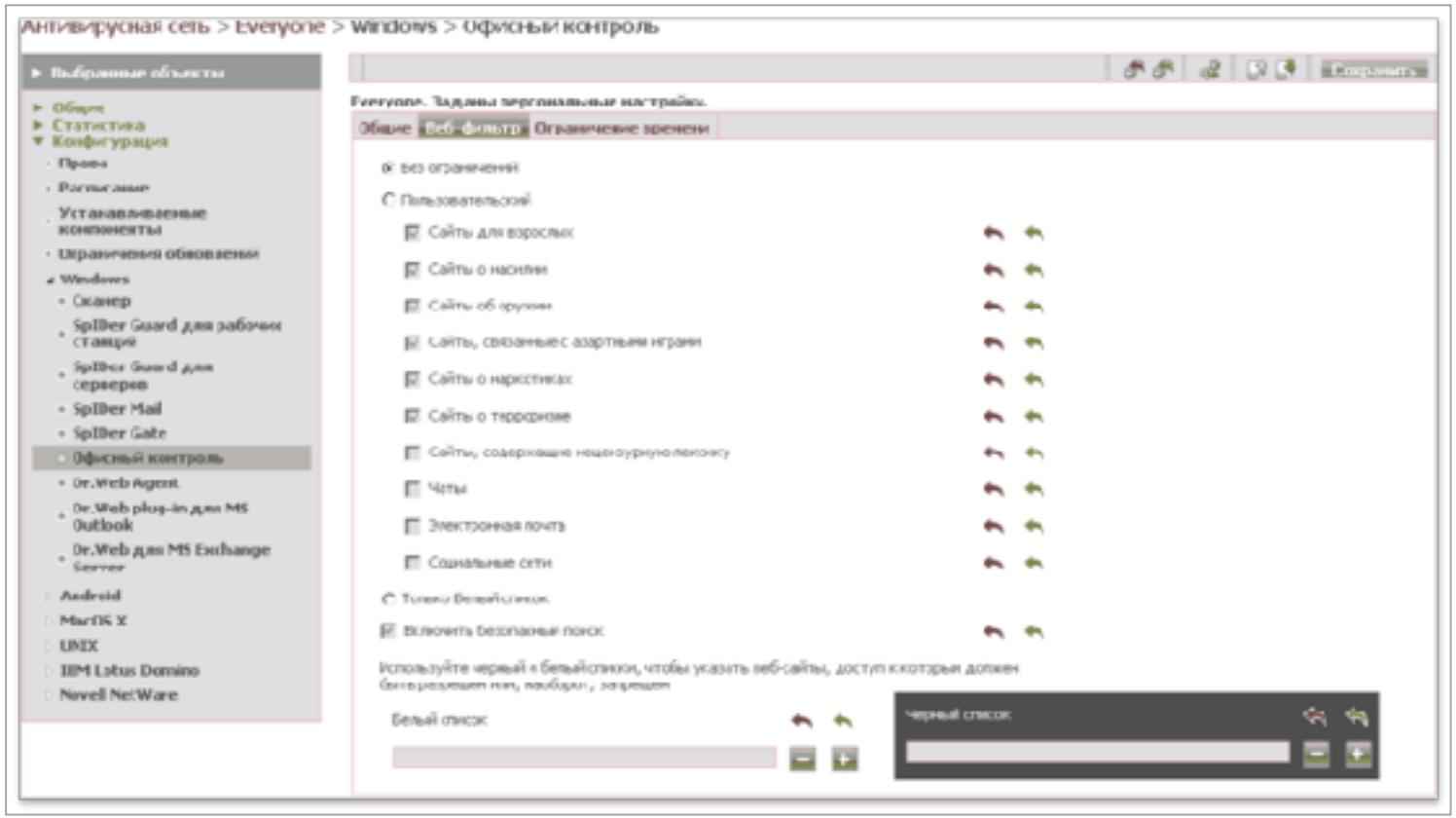
Dr.WEB®
с 1992 года

Офисный контроль



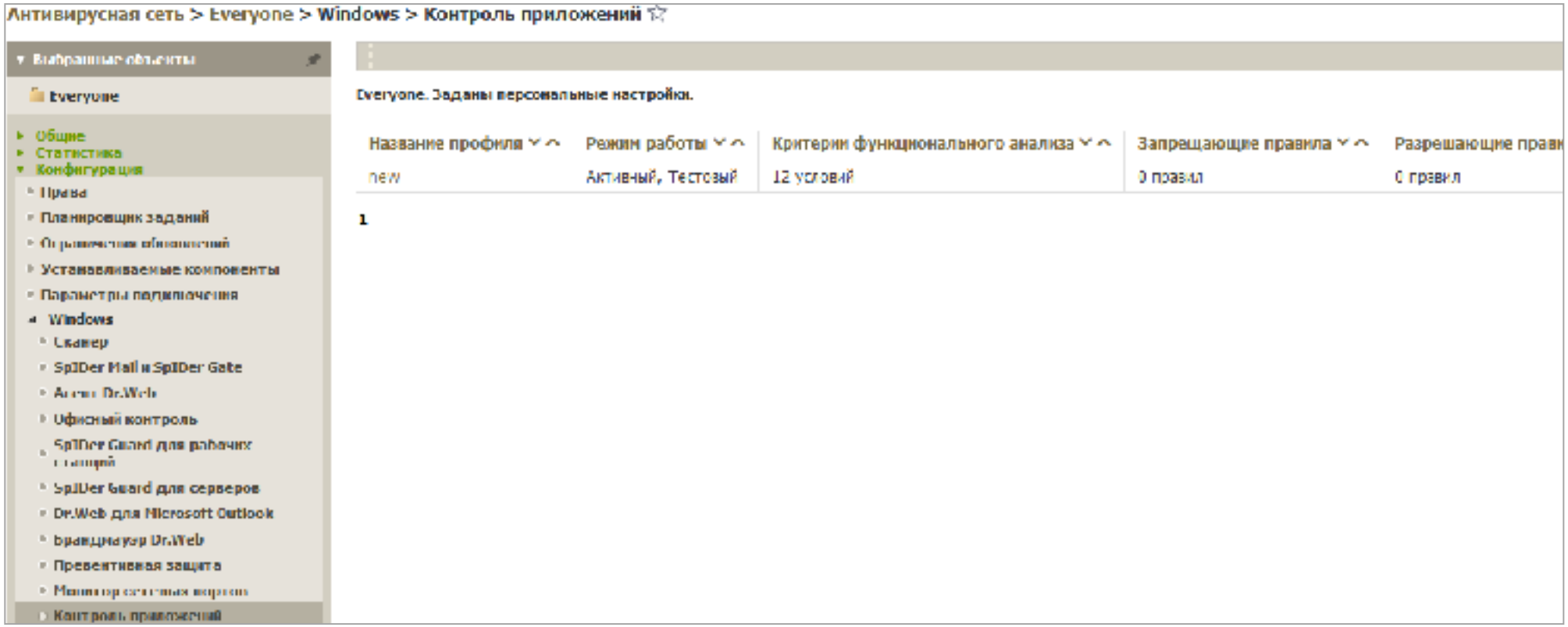
Dr.WEB®
с 1992 года

Ограничение доступа сотрудников к сайтам



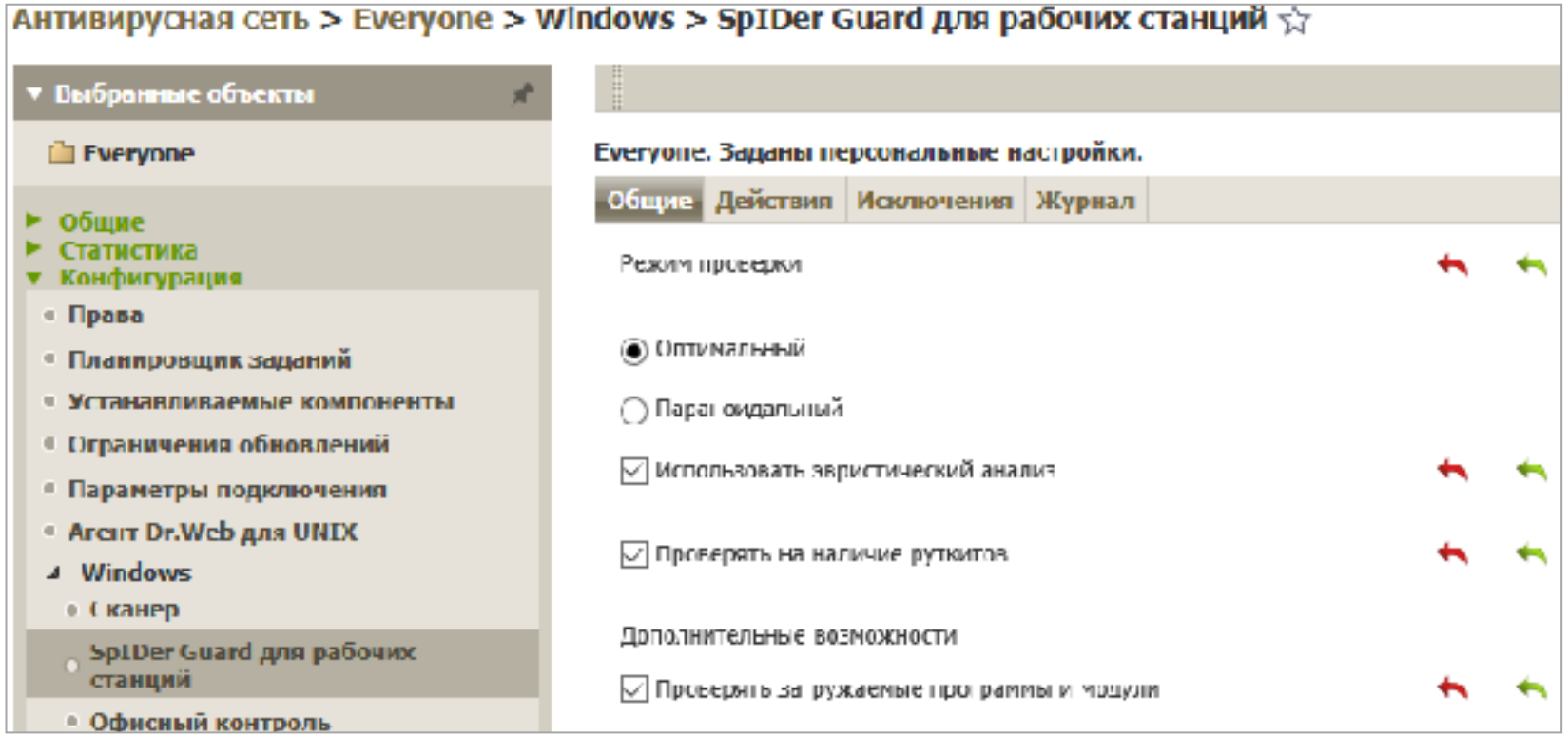
Dr.WEB®
с 1992 года

Контроль запуска программ пользователем



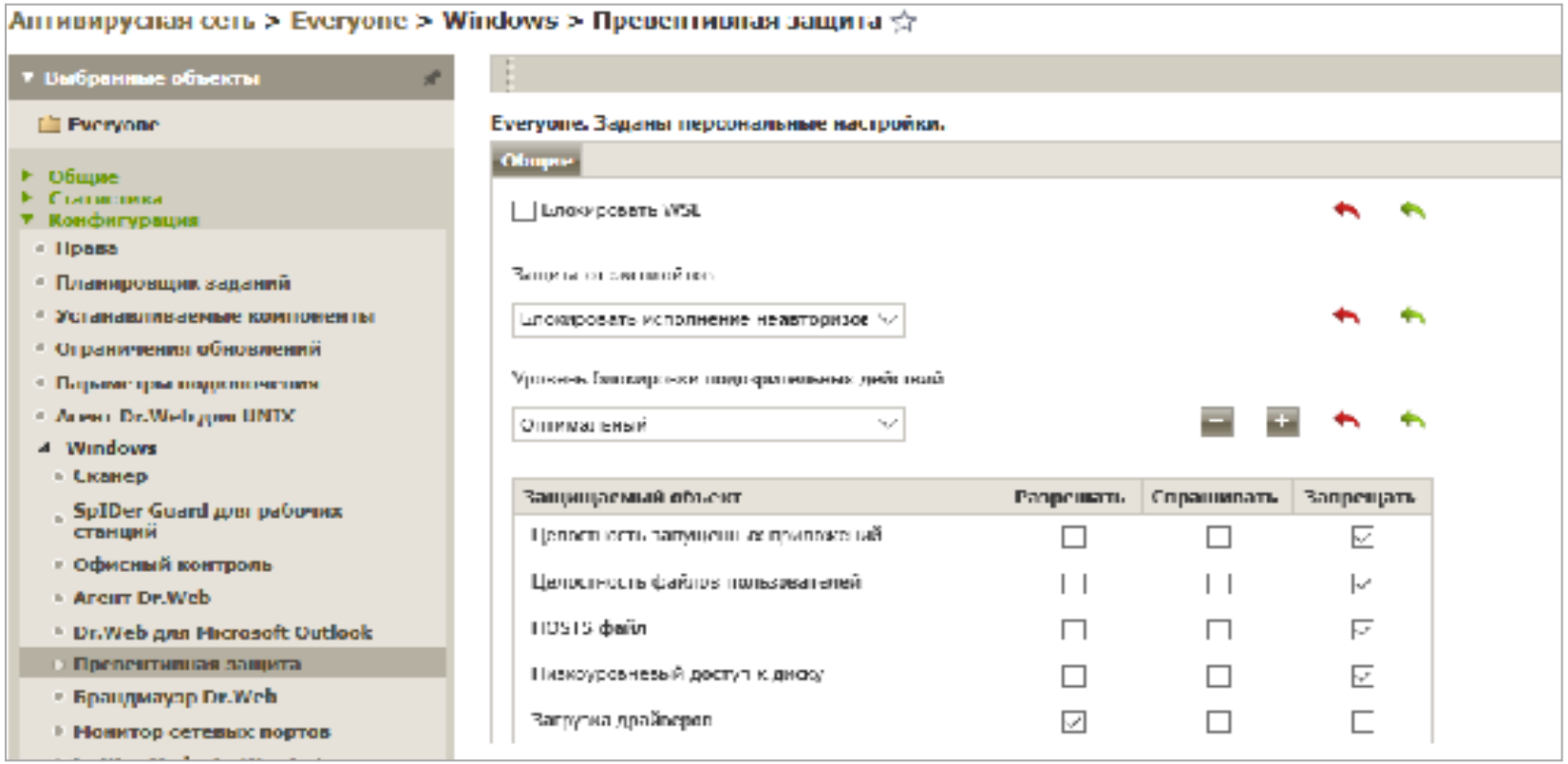
Dr.WEB®
с 1992 года

Лечение активных заражений



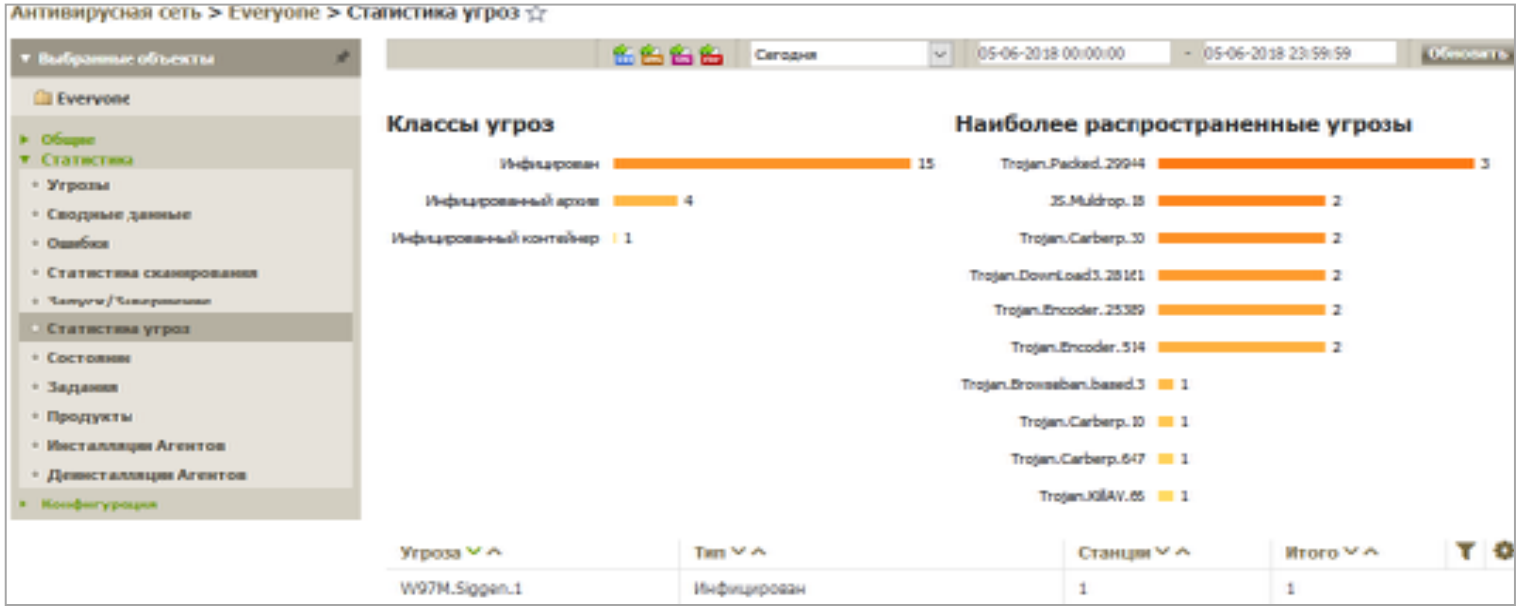
Dr.WEB®
с 1992 года

Превентивная защита



Dr.WEB®
с 1992 года

Удобная статистика



- Интуитивно понятное отображение нужных сведений.
- Возможность экспорта статистических отчетов сразу для нескольких объектов антивирусной сети.

Dr.WEB®
с 1992 года

С радостью ответим
на ваши вопросы!

И благодарим за внимание.