Dr.WEB®
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

Услуга «Антивирус Dr.Web»

https://антивирус.рф
https://www.drweb.ru/saas

Центр управления защитой Dr.Web

- Гарантия соблюдения политик безопасности
- Снижение риска заражения компании
- Минимизация потерь от ВКИ

Оформите подписку на услугу «Антивирус Dr.Web» для бизнеса и получите для вашего системного администратора доступ к Центру управления Dr.Web (ЦУ Dr.Web). Это позволит вашему сотруднику эффективно управлять антивирусной защитой вашей организации в соответствии с принятыми в ней политиками информационной безопасности.

1. Управление возможно:

Из любой точки мира	Без физического доступа к защищаемым устройствам	Достаточно доступа через браузер	В том числе со смартфона Android/iOS

Управление защитой производится:

Для любого количества защищаемых объектов	Для рабочих станций, мобильных устройств и любых серверов

Широкие возможности ЦУ Dr.Web позволяют выполнить следующие группы задач.

- Настройка антивирусного ПО на защищаемых объектах.
- Группировка защищаемых объектов в пользовательские группы для применения на них единых политик безопасности.
- Настройка правил доступа к нерекомендуемым ресурсам — или только к определенному списку ресурсов.
- Настройка правил использования сменных носителей.
- Настройка правил работы используемых приложений.
- Создание заданий для защищаемых объектов, выполняемых по расписанию.
- Получение статистики по отдельным защищаемым объектам и пользовательским группам.
- Отправка оповещений на защищаемый объект или на группу объектов.
- Рассылка инсталляционных пакетов антивирусного ПО по электронной почте и возможности удаленной деинсталляции.
- Управление учетными записями администраторов Центра управления.
- Управление антивирусной защитой организации с мобильного устройства (iOS/Android).

Настройка на защищаемых объектах включает в себя следующие возможности.

1.1. КОНФИГУРИРОВАНИЯ АНТИВИРУСНЫХ КОМПОНЕНТОВ

- Настройка автоматического действия компонентов при обнаружении угроз.
- Настройка исключений объектов из антивирусной проверки.
- Настройка защиты от новейших угроз средствами Превентивной защиты.

1.2. НАСТРОЙКИ АНТИСПАМА И ПРАВИЛ ДОСТУПА К ВРЕДОНОСНЫМ РЕСУРСАМ

- Настройка антиспама.
- Настройка веб-фильтра по категориям, создание собственных черных/белых списков.

1.3. НАСТРОЙКИ ПРАВИЛ РАБОТЫ УСТАНОВЛЕННЫХ ПРИЛОЖЕНИЙ

- Контроль установленных приложений.
- Настройка контроля доступа к различным сервисам и системным файлам.

1.4. НАСТРОЙКИ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

- Настройка антивора.
- Настройки фильтра приложений.

1.5. НАСТРОЙКИ ОФИСНОГО КОНТРОЛЯ

- Управление доступом к ресурсам сети Интернет.
- Управление доступом к съемным носителям.
- Ограничение времени работы на компьютере.

1.6. НАСТРОЙКИ ДЛЯ РАБОТЫ НА СЛАБЫХ МАШИНАХ И В УСЛОВИЯХ НИЗКОГО КАЧЕСТВА СВЯЗИ

- Настройка потребления ресурсов компьютера.
- Настройки индивидуальных параметров получения обновлений антивирусного ПО.
  - Настройка ограничений по типам обновлений.
  - Настройка скорости передачи данных.
  - Настройка расписания и параметров получения обновлений.

1.7. ОПРЕДЕЛЕНИЯ ПРАВ ПОЛЬЗОВАТЕЛЕЙ ЗАЩИЩАЕМЫХ ОБЪЕКТОВ НА ИЗМЕНЕНИЕ НАСТРОЕК В ИНТЕРФЕЙСЕ АНТИВИРУСНОГО ПО

- Настройка прав доступа на запуск, изменения конфигурации компонентов антивирусного ПО пользователям компьютера.
- Настройки для мобильных пользователей

...и многое другое для различных ОС.

2. Группировка защищаемых объектов в пользовательские группы

Создание групп любой вложенности (иерархии)	Единые политики ИБ для объектов групп	Индивидуальные графики обновлений

3. Создание заданий для защищаемых объектов, выполняемых по расписанию

Функционал расписания заданий — списка действий, выполняемых автоматически в заданное время на защищаемых объектах, — позволяет создавать задания как для отдельного защищаемого объекта, так и для объектов, объединенных в пользовательскую группу.

4. Управление учетными записями администраторов

Системный администратор имеет возможность делегировать полномочия по централизованному управлению антивирусной защитой квалифицированному сотруднику своей организации. Для этого в ЦУ Dr.Web существует возможность создания групповых администраторов для управления политиками информационной безопасности выделенных групп.

5. Получение статистики по отдельным защищаемым объектам и пользовательским группам

- Данные об обнаруженных угрозах на защищаемых объектах.
- Статистка сканирования и ошибок, возникающих при работе компонентов.
- Просмотр списка компонентов, установленных и запущенных на защищаемых объектах.
- Сведения о необычном состоянии защищаемых объектов.
- Список заданий, назначенных защищаемому объекту в заданный период времени.
- Информация об установленных вирусных базах на защищаемом объекте.

А также

Текстовые оповещения пользователям — в виде всплывающего окна (на компьютерах) либо push-сообщений на мобильном устройстве.	Отправка ссылок на дистрибутивы ПО Dr.Web пользователям на электронную почту.	Возможность централизованной деинсталляции антивирусного ПО с защищаемых объектов.

Обучающий курс

Для администрирования ЦУ Dr.Web требуется достаточная квалификация (умение установки, удаления и настройки программ, базовые знания основ информационной безопасности, устройства локальных сетей). Поэтому мы рекомендуем изучить обучающий курс DWCERT-004-10 Интернет-сервис Dr.Web AV-Desk версия 10.

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. «Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Телефоны (многоканальные): +7 495 789-45-87, 8-800-333-7932 (бесплатно по России)

https://антивирус.рф | https://www.drweb.ru | https://www.drweb.ru/saas