



КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ  
ОНЛАЙН

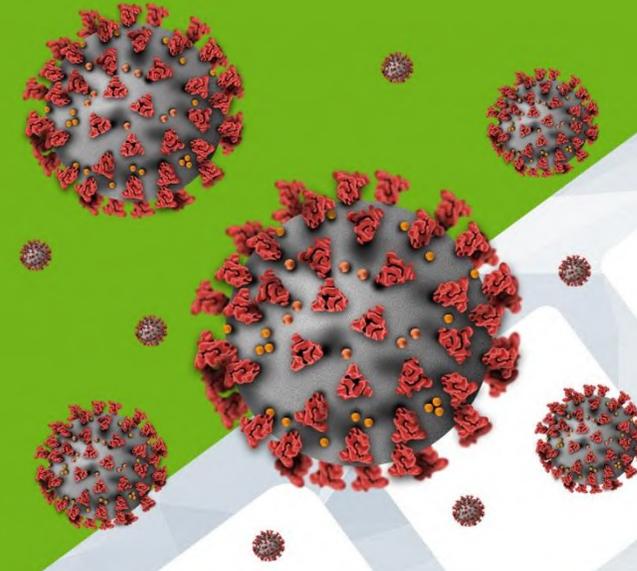
# Защита устройств удаленных сотрудников

Кирилл Тезиков  
*Компания «Доктор Веб»*



Перевод сотрудников  
на удаленную работу  
не должен вызвать  
проблем для бизнеса.

 **Dr.WEB®**  
iТ-краткое



**Это очень  
актуальный вопрос  
для руководителей  
во время эпидемии  
коронавируса**

 © ООО «Доктор Веб»,  
2003–2020



# Какие риски ИБ несет для компании работа сотрудников вне офиса?

Работая удаленно сотрудник может:

- получать удаленный доступ к своему рабочему месту;
- пользоваться почтой и иными корпоративными сервисами;
- пользоваться внешними сервисами.



А если компьютер или устройство сотрудника принадлежит ему и не контролируются системным администратором компании, то сотрудник:

- как правило, не ограничивает доступ с устройства к каким-либо сетевым ресурсам;
- не использует антиспам и защиту от фишинга;
- устанавливает самые разные программы – не всегда безопасные.



А еще к устройству сотрудника имеет доступ, как правило, не только он. Дети, родители, гости — далеко не полный список. Так что:

- в устройство может быть вставлена флешка, принесенная из школы или найденная на улице;
- на компьютере могут быть открыты небезопасные ресурсы;
- дети, родители или гости могут попробовать отключить защиту, «чтобы установить нужную программу».



Таким образом, повышаются риски, связанные с:

- Инфицированием устройств вредоносным ПО;
- Утечкой паролей к служебным ресурсам;
- Репутацией компании;
- Утечкой документов.



Для снижения ИБ-рисков антивирус должен решать следующие задачи:

- Обнаруживать вредоносное ПО любого типа и любой сложности;
- Корректно лечить ОС;
- Применять политики безопасности, принятые в компании, для защиты, в том числе, устройств удаленных сотрудников;
- Поддерживать контроль состояния защиты.



Давайте рассмотрим, как реализовать  
эти задачи с помощью

# Dr.Web Enterprise Security Suite

- Разрешить безопасный доступ к серверу Dr.Web через Интернет
- Создать отдельную группу для удаленных станций
- Распространить лицензию на эту группу
- Применить групповые политики к новой группе (или скопировать готовые из другой группы)
- Установить агенты на удаленные ПК
- Выполнить полную проверку ОС и вылечить их, если будут найдены угрозы



Разрешить безопасный доступ к серверу Dr.Web через Интернет с помощью Dr.Web Proxy Server:

1. Выделите одну (несколько) машину, которая будет иметь внешний статический IP-адрес;
2. Установите на нее Dr.Web Proxy Server;
3. Задайте адрес перенаправления прокси-сервера на адрес Dr.Web-сервера

Через прокси-сервер агенты, установленные на удаленных станциях, будут получать БЕЗОПАСНЫЙ доступ к Dr.Web-серверу.



## Антивирусная сеть ☆

## ▼ Выбранные объекты

📁 Everyone

▶ **Общие**  
▶ **Статистика**  
▶ **Конфигурация**

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты
- Параметры подключения
- ▶ **Windows**
  - Сканер
  - Агент Dr.Web
  - Офисный контроль
  - SpIDer Mail и SpIDer Gate
  - SpIDer Guard для рабочих станций
  - Dr.Web для Microsoft Outlook
  - Брандмауэр Dr.Web
  - Превентивная защита
  - Монитор сетевых портов
  - Контроль приложений

▶ macOS

▶ UNIX

Антивирусная сеть

Антивирусная сеть

СAB1

Installing system

Status

Uninstalling system

Частота обновления 15 c Обновить

## Свойства группы Everyone

## Общие

Идентификатор\* 20e27d73-d21d-b211-a788-85419c46f0e6

Название\* Everyone

Родительская группа Нет родительской группы

Описание All stations

## Сведения о станциях

Всего станций 1

Первичная группа для 1

Станций в сети 0

Расположение Нет объектов для отображения на карте

## Конфигурация

- 🔒 Права. Заданы персональные настройки.
- 📅 Планировщик заданий. Заданы персональные настройки.
- 🔑 Лицензионные ключи. Заданы персональные настройки.
- 🔄 Ограничения обновлений. Заданы персональные настройки.
- 📦 Устанавливаемые компоненты. Заданы персональные настройки.
- ⚙️ Параметры подключения. Заданы персональные настройки.

Windows

1

## Администрирование

- Сервер Dr.Web
- Ключи шифрования

## Лицензии

- Менеджер лицензий
- Отчет об использовании лицензий

## Журналы

- Журнал в реальном времени
- Журнал аудита
- Журнал выполнения заданий
- Журнал Сервера Dr.Web
- Журнал обновлений репозитория
- Журнал сообщений
- Журнал аварийно завершенных соединений

## Конфигурация

- Администраторы
- Аутентификация
- Конфигурация Сервера Dr.Web
- Удаленный доступ к Серверу Dr.Web
- Конфигурация SNMP-агента Dr.Web
- Планировщик заданий Сервера Dr.Web
- Конфигурация 5-сервера
- Пользователи и процедуры

## Оповещения

- Оповещения веб-консоли
- Неотправленные оповещения
- Конфигурация оповещений
- Шаблоны сообщений

## Репозиторий

- Состояние репозитория

Состояние ▾

Серьезность ▾



Выполнить задание

## Планировщик заданий Сервера Dr.Web

<input type="checkbox"/>	Название ▾ ▲	Состояние ▾ ▲	Серьезность ▾ ▲	Тип запуска ▾ ▲	Периодичность ▾ ▲	Действие ▾ ▲	🔍 ⚙️
<input type="checkbox"/>	Backup repository	Запрещено	Не критическое	Синхронно	Еженедельно в субботу, 01:45	Резервное копирование репозитория, Только важные ревизии	
<input type="checkbox"/>	Backup sensitive data	Разрешено	Не критическое	Асинхронно	Через 2 минуты после задания "Purge old data"	Резервное копирование критичных данных Сервера	
<input type="checkbox"/>	Key expiration reminder	Разрешено	Не критическое	Синхронно	Ежедневно в 07:30	Окончание срока действия лицензионного ключа	
<input type="checkbox"/>	Long time unseen servers	Разрешено	Не критическое	Синхронно	Ежечасно в 30 минут	Соседний Сервер давно не подключался	
<input type="checkbox"/>	Long time unseen stations	Разрешено	Не критическое	Синхронно	Ежедневно в 07:30	Станция давно не подключалась	
<input type="checkbox"/>	Purge old data	Разрешено	Не критическое	Асинхронно	Через 2 минуты после задания "Remove outdated messages"	Очистка старых записей	
<input type="checkbox"/>	Purge old stations	Разрешено	Не критическое	Асинхронно	Ежедневно в 00:13	Очистка старых станций	
<input type="checkbox"/>	Purge unsend IS events	Разрешено	Не критическое	Синхронно	Ежечасно в 17 минут	Очистка неотправленных событий	
<input type="checkbox"/>	Remove outdated messages	Разрешено	Не критическое	Асинхронно	Через 2 минуты после задания "Purge old stations"	Очистка устаревших сообщений	
<input type="checkbox"/>	Update all Dr.Web products	Разрешено	Не критическое	Синхронно	Ежечасно в 56 минут	Обновление репозитория, Все продукты Dr.Web	
<input type="checkbox"/>	Update all Dr.Web products	Разрешено	Критическое	Синхронно	Ежечасно в 26 минут	Обновление репозитория, Все продукты Dr.Web	
<input type="checkbox"/>	Vacuum database	Разрешено	Не критическое	Асинхронно	Еженедельно в воскресенье, 01:17	Очистка базы данных	

3

1

Страница: 1

Результаты 1 – 12 из 12

20 ▾

## Антивирусная сеть ☆

## Выбранные объекты

Бухгалтерия

## Общие

- Графики
- Идентификаторы безопасности
- Компоненты защиты
- Карантин
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Неактивные станции
- Свойства
- Правила членства в группе

## Статистика

- Угрозы
- Ошибки
- Сводные данные
- Статистика сканирования
- Запуск/Завершение
- Статистика угроз
- Состояние
- Задания
- Заблокированные устройства
- Продукты
- События Превентивной защиты
- События Контроля приложений
- Инсталляции Агентов
- Деинсталляции Агентов

## Конфигурация

- Права
- Планировщик заданий

Антивирусная сеть

- Everyone
- Отдел продаж
- Удаленка
- Бухгалтерия
- Отдел продаж

Частота обновления 15 с Обновить

## Свойства группы Бухгалтерия

Сохранить

## Общие

Идентификатор\* 7c0efd31-fd09-460c-8e65-c226e58b8b68

Название\* Бухгалтерия

Родительская группа Удаленка

Описание

Инсталляционный файл Windows

## Сведения о станциях

Всего станций	0
Первичная группа для	0
Станций в сети	0
Расположение	Нет объектов для отображения на карте

## Конфигурация

- Права.** Настройки унаследованы от группы **Everyone**.
- Планировщик заданий.** Настройки унаследованы от группы **Everyone**.
- Лицензионные ключи.** Настройки унаследованы от группы **Everyone**.
- Ограничения обновлений.** Настройки унаследованы от группы **Everyone**.
- Устанавливаемые компоненты.** Настройки унаследованы от группы

## Администрирование &gt; Менеджер лицензий ☆

## Администрирование

- Сервер Dr.Web
- Ключи шифрования

## Лицензии

- Менеджер лицензий
  - Отчет об использовании лицензий
- 
- Журналы
  - Журнал в реальном времени
  - Журнал аудита
  - Журнал выполнения заданий
  - Журнал Сервера Dr.Web
  - Журнал обновлений репозитория
  - Журнал сообщений
  - Журнал аварийно завершенных соединений

## Конфигурация

- Администраторы
- Аутентификация
- Конфигурация Сервера Dr.Web
- Удаленный доступ к Серверу Dr.Web
- Конфигурация SNMP-агента Dr.Web
- Планировщик заданий Сервера Dr.Web
- Конфигурация веб-сервера
- Пользовательские процедуры

## Оповещения

- Оповещения веб-консоли
- Неотправленные оповещения
- Конфигурация оповещений
- Шаблоны сообщений

## Репозиторий

- Состояние репозитория



Лицензии и ключи

- OOO "Доктор Веб" - 21-02-2021 01:58:16
  - Everyone
  - Удаленка

Редактировать

Сохранить

## Выбор файла

## Информация о количестве лицензий

Всего	5
Доступно	4
Используется станциями	1
Распространено по	0

## Распространение ключа на группы, станции и политики

Добавить лицензионный ключ

Заменить лицензионный ключ

- Антивирусная сеть
  - Everyone
  - Operating system
  - Удаленка

Серийный номер	766C-162T-FC55-RBR4
Дата окончания лицензии	21-02-2021 01:58:16
Антиспам	лицензирован
MD5-хеш ключа	424c3a67421816c203d7a706e39a0ec5
Конфигурация	Общие параметры

## Windows

- Сканер Dr.Web для Windows
- SpIDer Guard для рабочих станций Windows
- SpIDer Mail для Windows
- SpIDer Gate для рабочих станций Windows
- Общий журнал Dr.Web

## Выбранные объекты

## Удаленка

Общие  
Статистика  
Конфигурация

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты

## Параметры подключения

## Windows

- Сканер
- Агент Dr.Web
- Офисный контроль
- SpIDer Mail и SpIDer Gate
- SpIDer Guard для рабочих станций
- Dr.Web для Microsoft Outlook
- Брандмауэр Dr.Web
- Превентивная защита
- Монитор сетевых портов
- Контроль приложений

## macOS

## UNIX

## Удаленка. Заданы персональные настройки.

## Общие

Сертификат

5aa33821-2ffd-466a-b85f-cc5ad0e652fe

Сервер

192.168.200.200

yourdoman.zone

Количество повторений поиска

3

Тайм-аут поиска (с)

5

Режим скатия

Возможно

Режим шифрования

Да

Параметры прослушивания сети

udp/:2193

Сохранить

## Антивирусная сеть ☆

## Выбранные объекты

Бухгалтерия

## Общие

- Графики
- Идентификаторы безопасности
- Компоненты защиты
- Карантин
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Неактивные станции
- Свойства
- Правила членства в группе

## Статистика

- Угрозы
- Ошибки
- Сводные данные
- Статистика сканирования
- Запуск/Завершение
- Статистика угроз
- Состояние
- Задания
- Заблокированные устройства
- Продукты
- События Превентивной защиты
- События Контроля приложений
- Инсталляции Агентов
- Деинсталляции Агентов

## Конфигурация

- Права
- Планировщик заданий

1

2

3

Частота обновления 15 с Обновить

## Новая станция

Сохранить

## Общие

Количество\*

5

Идентификатор\*

40a...-8d6c-404f-84d7-d236b94aab28

Название\*

Новая станция

Пароль

•

Подтвердите пароль

•

Описание

## Группы

Членство

- Everyone
- Отдел продаж
- Удаленка
  - Бухгалтерия
  - Отдел продаж

## Безопасность

 Использовать этот список доступа Приоритетность запрета

TCP: Разрешено

TCP: Запрещено

 - + - +

TCPv6: Разрешено

TCPv6: Запрещено

Выбранные объекты

Удаленка

- Общие
- Статистика
- Конфигурация

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты

Параметры подключения

Windows

- Сканер
- Агент Dr.Web
- Офисный контроль
- SpIDer Mail и SpIDer Gate
- SpIDer Guard для рабочих станций
- Dr.Web для Microsoft Outlook
- Брандмауэр Dr.Web
- Превентивная защита
- Монитор сетевых портов
- Контроль приложений

macOS

- Сканер для рабочих станций
- SpIDer Guard для рабочих станций
- SpIDer Gate для рабочих станций

UNIX

- Сканер для рабочих станций
- Агент Dr.Web
- SpIDer Guard

Сохранить

Удаленка. Заданы персональные настройки.

Общие

Сертификат

5aa33821-2ffd-466a-b85f-cc5ad0e652fe

Сервер

Количество повторений поиска

3

Тайм-аут поиска (с)

5

Режим скатия

Возможно

Режим шифрования

Да

Параметры прослушивания сети

udp/2

Установить агенты на удаленные ПК можно с помощью:

- Полного инсталляционного пакета;
- Группового инсталляционного пакета;
- Индивидуального инсталляционного пакета.



## Установка агента Dr.Web с помощью полного дистрибутива агента

- Минимизирует трафик между сервером и инсталлятором агента во время установки;
- Экономит примерно 400 Мб \* кол-во агентов, сетевого трафика.



[Мастер скачиваний](#)  
[Документация](#)  
[Видео по продуктам](#)  
[Брошюры](#)  
[Локализации](#)

#### Защита для бизнеса

[Демо для бизнеса](#)  
[Демо для комплектов](#)  
[Dr.Web LiveDemo](#)  
[Демо для лечащих утилит Dr.Web](#)

**Новое!** [Демо Dr.Web ATM Shield](#)

#### Защита для дома



[защита для дома](#)  
[Light для Mac](#)  
[защита криптографа](#)  
  
[защита мобильных устройств](#)  
[защита мобильных устройств для Android](#)

#### Лечащие утилиты

- [Dr.Web CureNet!](#)
- [Dr.Web CureIt!](#)
- [Dr.Web LiveDisk](#)

#### Проверка ссылок

- [для IE](#)
- [для Mozilla](#)
- [для Opera](#)
- [для Safari](#)
- [для Google Chrome](#)

## Результат работы Мастера скачиваний

Серийный номер:

Срок действия: 20.02.2020-20.02.2021

Для скачивания согласно Вашему серийному номеру доступны следующие продукты:

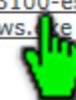
### Центр Управления

[Описание](#) | [Карточка продукта](#)

#### (+) Поддерживаемые ОС

В состав Центра Управления входят Веб-администратор, Антивирусный сервер и антивирусные агенты для установки на ОС семейства Windows (рабочие станции и серверы).

Выберите версию Центра Управления

Номер версии	Программы, Документация	
12.0	<p>Сервер Dr.Web Enterprise Security Suite</p> <input type="text" value="выберите"/>	<p>Руководство администратора</p> <input type="text" value="русский"/> <a href="#">Скачать</a>
	<p>Полный антивирусный агент для защиты ОС Windows</p> <p><a href="#">drweb-12.00.1-202003100-esuite-agent-full-windows.exe</a></p> 	<p>Инструкция по развертыванию антивирусной сети</p> <input type="text" value="русский"/> <a href="#">Скачать</a>

## Администрирование &gt; Ключи шифрования ☆

## ▼ Администрирование

• Сервер Dr.Web

• Ключи шифрования

## ▼ Лицензии

• Менеджер лицензий

• Отчет об использовании лицензий

## ▼ Журналы

• Журнал в реальном времени

• Журнал аудита

• Журнал выполнения заданий

• Журнал Сервера Dr.Web

• Журнал обновлений репозитория

• Журнал сообщений

• Журнал аварийно завершенных соединений

## ▼ Конфигурация

• Администраторы

• Аутентификация

• Конфигурация Сервера Dr.Web

• Удаленный доступ к Серверу Dr.Web

• Конфигурация SNMP-агента Dr.Web

• Планировщик заданий Сервера Dr.Web

• Конфигурация веб-сервера

• Пользовательские процедуры

## ▼ Оповещения

• Оповещения веб-консоли

• Неотправленные оповещения

• Конфигурация оповещений

• Шаблоны сообщений

## ▼ Репозиторий

• Состояние репозитория

## Ключи шифрования

Экспортировать

<input type="checkbox"/>	▼ ^	Объект ▼ ^	Идентификатор ▼ ^	🔽
<input type="checkbox"/>	certificate	Сертификат	5aa33821-2ffd-466a-b85f-cc5ad0e652fe	
<input checked="" type="checkbox"/>	public_key	Открытый ключ	5aa33821-2ffd-466a-b85f-cc5ad0e652fe	
<input checked="" type="checkbox"/>	private_key	Закрытый ключ	5aa33821-2ffd-466a-b85f-cc5ad0e652fe	

## Администрирование &gt; Конфигурация Сервера Dr.Web

## Администрирование

- Сервер Dr.Web
- Ключи шифрования

## Лицензии

- Менеджер лицензий
- Отчет об использовании лицензий

## Журналы

- Журнал в реальном времени
- Журнал аудита
- Журнал выполнения заданий
- Журнал Сервера Dr.Web
- Журнал обновлений репозитория
- Журнал сообщений
- Журнал аварийно завершенных соединений

## Конфигурация

- Администраторы
- Аутентификация
- Конфигурация Сервера Dr.Web
- Удаленный доступ к Серверу Dr.Web
- Конфигурация SNMP-агента Dr.Web
- Планировщик заданий Сервера Dr.Web
- Конфигурация веб-сервера
- Пользовательские процедуры

## Оповещения

- Оповещения веб-консоли
- Неотправленные оповещения
- Конфигурация оповещений
- Шаблоны сообщений

## Репозиторий

- Состояние репозитория

## Общие

## Трафик

## Сеть

## Статистика

## Безопасность

## Кеш

## База данных

## Модули

## Расположение

## Лицензии

## Журнал

Сохранить

Название Сервера

3

Язык Сервера

Русский

Количество параллельных запросов от клиентов

5

Режим регистрации новичков

Автоматически разрешать доступ

Первичная группа по умолчанию

Бухгалтерия

 Переводить неавторизованных в новички Автоматически создавать учетные записи станций

Допустимая разница между временем Сервера и Агента

6

3

 Заменять IP-адреса Заменять NetBIOS-имена Синхронизировать описания станций Синхронизировать географическое положение

Стартовая синхронизация

0

 Использовать политики

Dr.Web Agent Русский ▾

## Установка Dr.Web Agent

Чтобы продолжить установку, заполните обязательные поля: адрес сервера и путь к открытому ключу или сертификату.

Сервер централизованной защиты

Открытый ключ или сертификат

Dr.Web 

---

 **Компьютер защищен**

 Центр безопасности

 Поддержка

Ru        РУС 23:30  
21.04.2020 



## Антивирусная сеть ☆

## ▼ Выбранные объекты

📁 Everyone

## ▼ Общие

- Графики
- Идентификаторы безопасности
- Компоненты защиты
- Карантин
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Неактивные станции
- Свойства

## ▼ Статистика

- Угрозы
- Ошибки
- Сводные данные
- Статистика сканирования
- Запуск/Завершение
- Статистика угроз
- Состояние
- Задания
- Заблокированные устройства
- Продукты
- События Превентивной защиты
- События Контроля приложений
- Инсталляции Агентов
- Деинсталляции Агентов

## ▼ Конфигурация

- Права
- Планировщик заданий
- Ограничения обновлений

Антивирусная сеть

- ▶ Everyone
- ▶ Operating system
- ▶ Status
- ▶ Transport
- ▶ Отдел продаж
- ▶ Удаленка
  - ▶ Бухгалтерия (LAB1)
  - ▶ Отдел продаж

Частота обновления: 15 с [Обновить]

## Свойства группы Everyone

## Общие

Идентификатор*	20e27d73-d21d-b211-a788-85419c46f0e6
Название*	Everyone
Родительская группа	Нет родительской группы
Описание	All stations

## Сведения о станциях

Всего станций	1
Первичная группа для	0
Станций в сети	1
Расположение	Нет объектов для отображения на карте

## Конфигурация

- 🔒 **Права.** Заданы персональные настройки.
- 📅 **Планировщик заданий.** Заданы персональные настройки.
- 🔑 **Лицензионные ключи.** Заданы персональные настройки.
- 🔄 **Ограничения обновлений.** Заданы персональные настройки.
- 📦 **Устанавливаемые компоненты.** Заданы персональные настройки.
- ⚙️ **Параметры подключения.** Заданы персональные настройки. Настройки не унаследовала 1 группа.

## Установка агента Dr.Web с помощью группового установочного агента

- Установка за пару кликов мышью;
- Автоматическое добавление станции в нужную группу;
- Автоматическое создание учетной записи станции в нужной группе.



## Антивирусная сеть ☆

## Выбранные объекты

Бухгалтерия

## Общие

- Графики
- Идентификаторы безопасности
- Компоненты защиты
- Карантин
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Неактивные станции
- Свойства
- Правила членства в группе

## Статистика

- Угрозы
- Ошибки
- Сводные данные
- Статистика сканирования
- Запуск/Завершение
- Статистика угроз
- Состояние
- Задания
- Заблокированные устройства
- Продукты
- События Превентивной защиты
- События Контроля приложений
- Инсталляции Агентов
- Деинсталляции Агентов

## Конфигурация

- Права
- Планировщик заданий

Антивирусная сеть

- Everyone
- Status
- Отдел продаж
- Удаленка
  - Бухгалтерия
  - Отдел продаж

Частота обновления: 15 с. Обновить

## Свойства группы Бухгалтерия

Сохранить

## Общие

Идентификатор\* 7c0efd31-fd09-460c-8e65-c226e58b8b68

Название\* Бухгалтерия

Родительская группа Удаленка

Описание

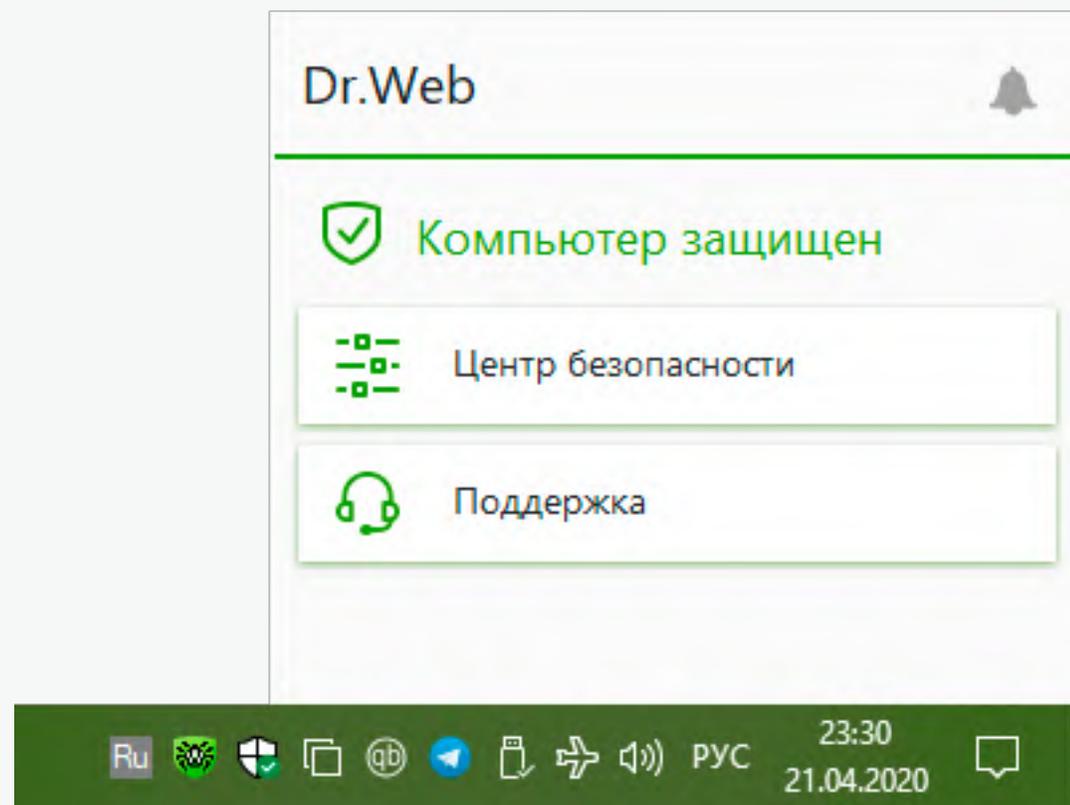
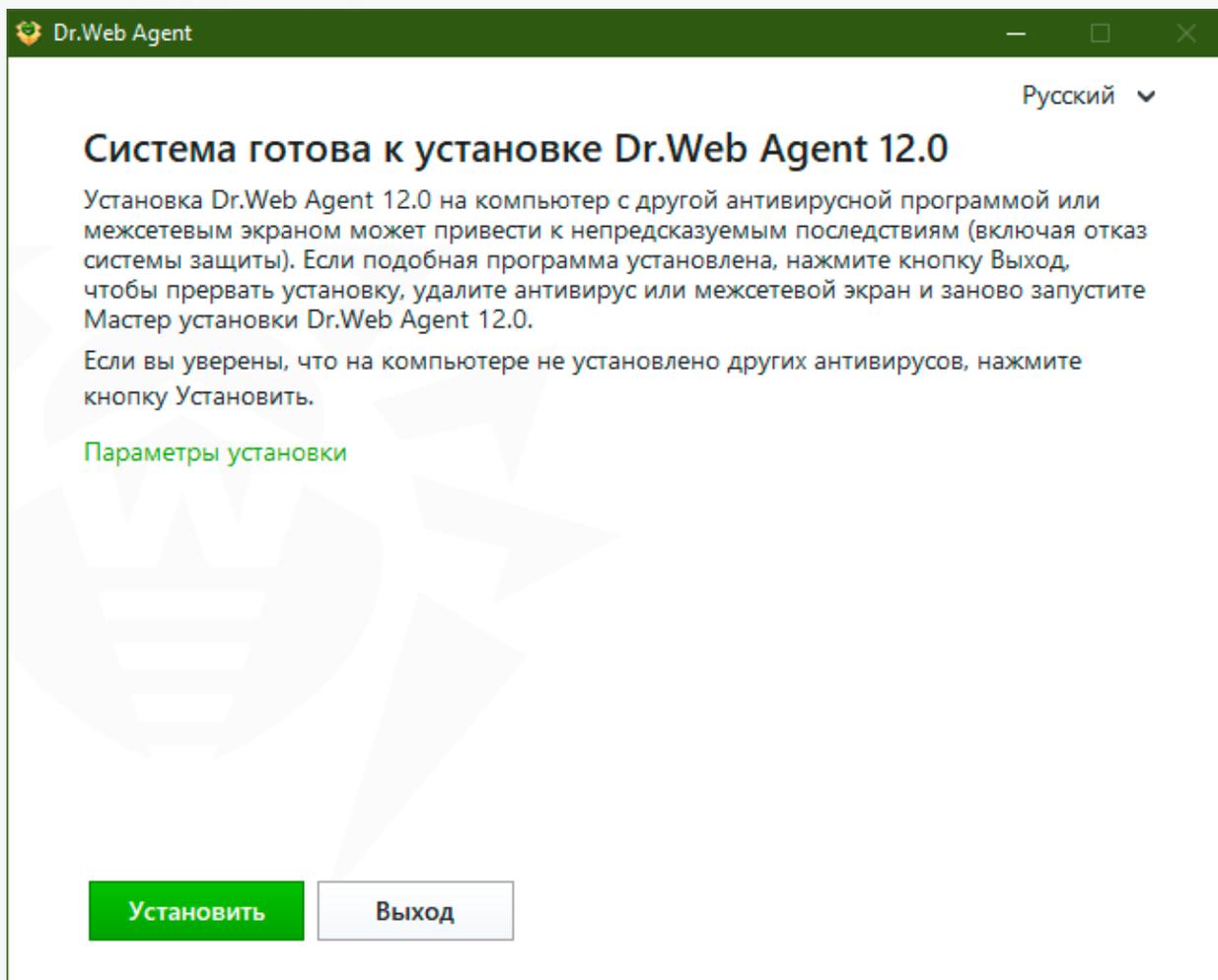
Инсталляционный файл Windows

## Сведения о станциях

Всего станций	0
Первичная группа для	0
Станций в сети	0
Расположение	Нет объектов для отображения на карте

## Конфигурация

- Права.** Настройки унаследованы от группы **Everyone**.
- Планировщик заданий.** Настройки унаследованы от группы **Everyone**.
- Лицензионные ключи.** Настройки унаследованы от группы **Everyone**.
- Ограничения обновлений.** Настройки унаследованы от группы **Everyone**.
- Устанавливаемые компоненты.** Настройки унаследованы от группы



## Антивирусная сеть ☆

## ▼ Выбранные объекты

- Бухгалтерия

## ▼ Общие

- Графики
- Идентификаторы безопасности
- Компоненты защиты
- Карантин
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Неактивные станции
- Свойства
- Правила членства в группе

## ▼ Статистика

- Угрозы
- Ошибки
- Сводные данные
- Статистика сканирования
- Запуск/Завершение
- Статистика угроз
- Состояние
- Задания
- Заблокированные устройства
- Продукты
- События Превентивной защиты
- События Контроля приложений
- Инсталляции Агентов
- Деинсталляции Агентов

## ▼ Конфигурация

- Права
- Планировщик заданий

Антивирусная сеть

- Everyone
- Operating system
- Status
- Отдел продаж
- Удаленка
  - Бухгалтерия**
    - LAB1
  - Отдел продаж

Частота обновления: 15 с Обновить

## Свойства группы Бухгалтерия

Сохранить

## Общие

Идентификатор\* 7c0efd31-fd09-460c-8e65-c226e58b8b68

Название\* Бухгалтерия

Родительская группа Удаленка

Описание

Инсталляционный файл Windows

## Сведения о станциях

Всего станций	1
Первичная группа для	1
Станций в сети	1
Расположение	Нет объектов для отображения на карте

## Конфигурация

- Права.** Настройки унаследованы от группы **Everyone**.
- Планировщик заданий.** Настройки унаследованы от группы **Everyone**.
- Лицензионные ключи.** Настройки унаследованы от группы **Everyone**.
- Ограничения обновлений.** Настройки унаследованы от группы **Everyone**.
- Устанавливаемые компоненты.** Настройки унаследованы от группы

## Установка агента Dr.Web с помощью персонального установочного агента

- Установка за пару кликов мышью;
- Для случаев, когда нужно привязать установку агента к конкретной учетной записи.



## Антивирусная сеть ☆

## ▼ Выбранные объекты

🖥️ Новая станция

## ▼ Общие

- Графики
- Идентификаторы безопасности
- Оборудование и программы
- Обнаруженные устройства
- Сессии пользователей
- Свойства

## ▼ Конфигурация

- Права
- Устанавливаемые компоненты

1

2

Частота обновления 15 с Обновить

## Свойства станции Новая станция

Сохранить

## Общие

Идентификатор станции \* 719f98ad-32e7-4384-808b-793288f2c0bf

Название\* Новая станция

Дата создания 22-04-2020 00:34:25

Пароль .....

Подтвердите пароль .....

MAC-адрес

Дата последнего подключения

Сетевой адрес

Описание

Инсталляционный файл Windows

Конфигурационный файл macOS &amp; Android &amp; Linux

3

## Группы

## Членство

- Everyone
- Отдел продаж
- Удаленка
  - Бухгалтерия
  - Отдел продаж

# Оптимизация трафика обновлений

- Ограничение обновлений
- Мобильный режим



Выбранные объекты

- Удаленка
  - Общие
  - Статистика
  - Конфигурация
    - Права
    - Планировщик заданий
    - Ограничения обновлений
    - Установка новых компонентов
    - Параметры обновления
  - Windows
    - Сканер
    - Агент Dr.Web
    - Офисный контроль
    - SpIDer Mail и SpIDer Gate
    - SpIDer Guard для рабочих станций
    - Dr.Web для Microsoft Outlook
    - Брандмауэр Dr.Web
    - Превентивная защита
    - Монитор сетевых портов
    - Контроль приложений
  - macOS
  - UNIX

## Удаленка. Заданы персональные настройки.

Ограничение обновлений  ↶ ↷

Снизить серьезность устаревания вирусных баз ↶ ↷

Интервал актуальности ревизий  дни ↶ ↷

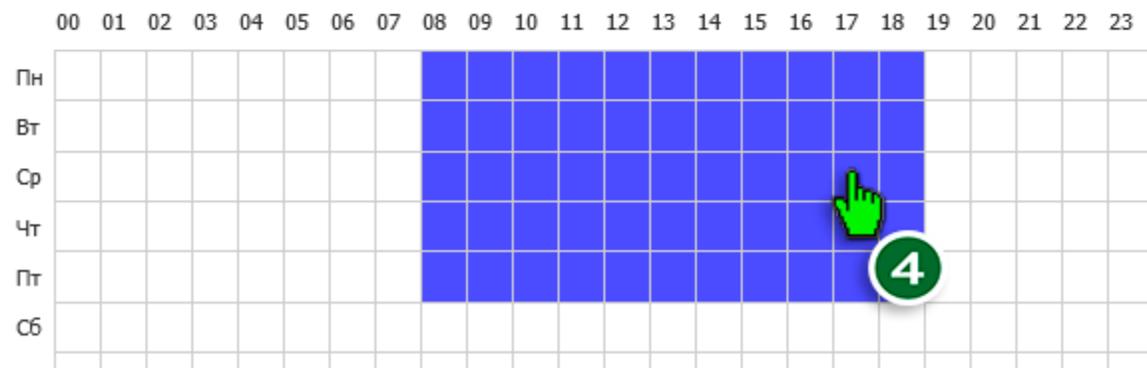
Получать последние обновления ↶ ↷

Разрешить переход на более ранние ревизии ↶ ↷

Ограничить трафик обновлений ↶ ↷

Скорость по умолчанию (КБ/с)  ↶ ↷

Максимальная скорость передачи (КБ/с)  - +



## Выбранные объекты

## Удаленка

- Общие
- Статистика
- Конфигурация
  - Права
  - Планировщик заданий
  - Ограничения обновлений
  - Устанавливаемые компоненты
  - Параметры подключения
  - Windows
    - Сканер
    - Агент Dr.Web
    - Офисный контроль
    - SpIDer Gate
    - SpIDer Gate для рабочих станций
    - Dr.Web для Microsoft Outlook
    - Брандмауэр Dr.Web
    - Превентивная защита
    - Монитор сетевых портов
    - Контроль приложений
  - macOS
  - UNIX

## Удаленка. Заданы персональные настройки.

Общие Мобильность Журнал Интерфейс События

 Использовать мобильный режим

Периодичность обновления

30 минут

 Использовать прокси-сервер

Прокси-сервер

Порт прокси-сервера

3128

Пользователь прокси-сервера

Пароль пользователя прокси-сервера

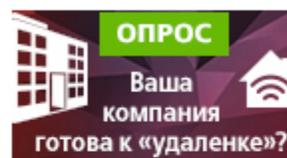
Тип авторизации

None

Сохранить

## Настрой-ка Dr.Web ESS

- ✓ [Защита удаленных сотрудников средствами Dr.Web Enterprise Security Suite](#)
- ✓ [Список задач при переводе сотрудников на удаленную работу](#)
- ✓ [Инструкция по переходу на версию 12](#)



## Новая версия 12

- ✓ [Возможности модуля Контроль приложений](#)
- ✓ [Запрет запуска программ с помощью Контроля приложений](#)
- ✓ [Запрет запуска приложений по известным контрольным суммам](#)
- ✓ [Запрет запуска устаревшего ПО с помощью Контроля приложений](#)
- ✓ [Функциональный анализ](#)
- ✓ [Установка на станцию только Контроля приложений и Сканера Dr.Web](#)
- ✓ [Запрет запуска новейших вредоносных приложений с помощью Контроля приложений](#)
- ✓ [Контроль съемных устройств](#)



## Фильтрация почты средствами Dr.Web Mail Security Suite

- ✓ [Расширение функционала для почтовых серверов Unix. Обработка сообщений по ключевым словам и отправителям](#)
- ✓ [Расширение функционала Dr.Web для почтовых серверов Unix. Обработка спам-сообщений](#)
- ✓ [Фильтрация почтового трафика при использовании компанией внешних почтовых сервисов](#)

# Рекомендации по настройке антивирусной защиты ПК удаленных сотрудников



Выбранные объекты

Удаленка

- Общие
- Статистика
- Конфигурация

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты

- Параметры подключения

Windows

- Сканер
- Агент Dr.Web
- Офисный контроль
- SpIDer Mail и SpIDer Gate
- SpIDer Guard для рабочих станций
- Dr.Web для Microsoft Outlook
- Брандмауэр Dr.Web
- Превентивная защита
- Монитор сетевых портов
- Контроль приложений

macOS

UNIX

Сохранить

## Удаленка. Заданы персональные настройки.

Агент Dr.Web для Windows	Должен быть установлен
Dr.Web Agent Сканер для Windows	Должен быть установлен
Сканер Dr.Web для Windows	Должен быть установлен
SpIDer Guard для рабочих станций Windows	Должен быть установлен
SpIDer Guard для серверов Windows	Не может быть установлен
SpIDer Mail для Windows	Должен быть установлен
SpIDer Gate для рабочих станций Windows	Должен быть установлен
Офисный контроль Dr.Web	Должен быть установлен
Dr.Web для Microsoft Outlook	Должен быть установлен
Антиспам Dr.Web	Должен быть установлен
Брандмауэр Dr.Web	Может быть установлен

## Антивирусная сеть ☆

## ▼ Выбранные объекты

## 📁 Удаленка

▶ **Общие**  
▶ **Статистика**  
▶ **Конфигурация**

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты
- Параметры подключения

▲ **Windows**

- Сканер
- Агент Dr.Web
- Офисный контроль
- SpIDer Mail и SpIDer Gate
- SpIDer Guard для рабочих станций
- Dr.Web для Microsoft Outlook
- Брандмауэр Dr.Web
- Превентивная защита
- Монитор сетевых портов
- Контроль приложений

## ▶ macOS

## ▶ UNIX

Антивирусная сеть

- ▶ Отдел продаж
- ▶ Status
- ▶ Transport
- ▶ Отдел продаж
- ▶ Удаленка
  - ▶ Бухгалтерия
  - ▶ Отдел продаж

Частота обновления 15 с Обновить

## Dr.Web Agent Сканер. Полное сканирование

Сканировать

## Общие

Приоритет сканирования

обычный



Уровень загрузки ресурсов компьютера

Оптимальный (рекомендуется)



Количество используемых ядер

0



Действия после сканирования

ничего не делать



## Действия

Инфицированные

Лечить



Подозрительные

Перемещать в карантин



Неизлечимые

Перемещать в карантин

Инфицированные  
инсталляционные пакеты

Перемещать в карантин



Инфицированные архивы

Перемещать в карантин





## Аптечка сисадмина

### Dr.Web LiveDisk

- ✓ **БЕСПЛАТНОЕ** аварийное восстановление системы с диска DVD или загрузочного USB-накопителя в случаях если действия вредоносных программ сделали невозможной загрузку компьютера под управлением Windows
- ✓ Поможет не только очистить компьютер от инфицированных и подозрительных файлов, но и скопировать важную информацию на сменные носители или другой компьютер, а также попытается вылечить зараженные объекты.

[Скачать для записи на DVD](#)[Скачать для записи на USB](#)

После скачивания Вы будете перенаправлены на наши страницы в социальных сетях.

**Внимание!** Утилита записи предназначена для работы в операционных системах Windows (32- и 64-битные версии). Для загрузки с флеш-накопителя BIOS вашего компьютера должен поддерживать устройство USB-HDD в качестве загрузочного.



Корзина



Терминал  
среды MATE



Dr.Web CureIt!



Файловый  
менеджер



Midnight  
Commander



Веб



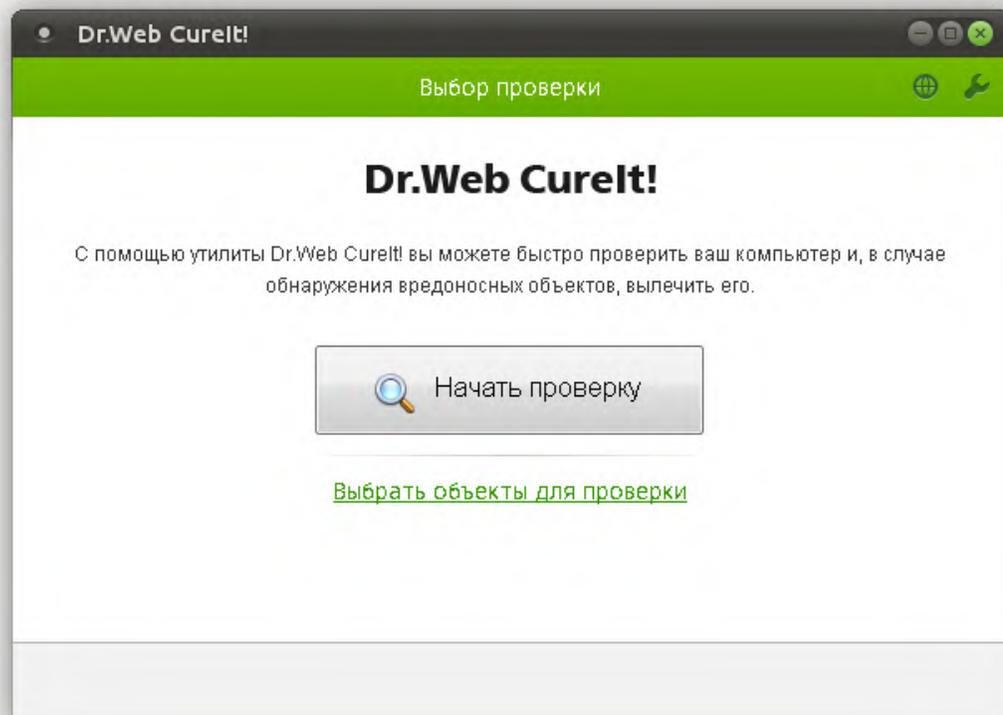
Обновить  
вирусные ба...



Перезапустит  
ь Dr.Web



Редактор  
реестра Dr....



Dr.Web CureIt!



en Cp, 22 апр, 01:47



## Выбранные объекты

## Удаленка

- Общие
- Статистика
- Конфигурация
  - Права
    - Планировщик заданий
    - Ограничение обновлений
    - Установка новых компонентов
    - Параметры подключения
    - Windows
      - Сканер
      - Агент Dr.Web
      - Офисный контроль
      - SpIDer Mail и SpIDer Gate
      - SpIDer Guard для рабочих станций
      - Dr.Web для Microsoft Outlook
      - Брандмауэр Dr.Web
      - Превентивная защита
      - Монитор сетевых портов
      - Контроль приложений
    - macOS
    - UNIX

## Удаленка. Настройки унаследованы от группы Everyone.

## Windows

## macOS

## Linux

## Клиенты

## Общие

3

4

все

Запуск Сканера

Изменение конфигурации Сканера

Запуск SpIDer Guard для рабочих станций

Изменение конфигурации SpIDer Guard для рабочих станций

Останов SpIDer Guard для рабочих станций

Запуск SpIDer Gate

Изменение конфигурации SpIDer Gate

Останов SpIDer Gate

Запуск SpIDer Mail

Изменение конфигурации SpIDer Mail

Останов SpIDer Mail

Запуск Офисного контроля Dr.Web

Изменение конфигурации Офисного контроля Dr.Web

Останов Офисного контроля Dr.Web

Запуск Dr.Web для Microsoft Outlook

Изменение конфигурации Dr.Web для Microsoft Outlook

Запуск превентивной защиты

Изменение конфигурации превентивной защиты

Сохранить

Центр безопасности

Центр безопасности    Статистика

✓ **Dr.Web: Компьютер защищен**

 <b>Файлы и сеть</b> Проверка файловой системы и защита от сетевых угроз	 <b>Превентивная защита</b> Контроль активности сторонних приложений
 <b>Устройства</b> Настройка правил доступа к устройствам	 <b>Офисный контроль</b> Контроль доступа к компьютеру, сети Интернет, файлам и папкам
 <b>Менеджер карантина</b> Просмотр и управление обнаруженными угрозами	 <b>Исключения</b> Исключения из проверки компонентами защиты

У вас нет прав для изменения параметров компонента. ✕

Нажмите, чтобы запретить изменения



## Выбранные объекты

## Удаленка

- Общие
- Статистика
- Конфигурация

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты
- Параметры подключения
- Windows
  - Сканер
  - Агент Dr.Web
  - Офисный контроль
  - SpIDer Mail и SpIDer Gate
  - SpIDer для рабочих станций
  - Dr.Web для Microsoft Outlook
  - Брандмауэр Dr.Web
  - Превентивная защита
  - Монитор сетевых портов
  - Контроль приложений

macOS

UNIX

## Общие Пользовательские

Удаленка. Заданы персональные настройки.

- Пользователи
  - Администраторы
  - Гости
  - Польз

## Общие Разрешенные устройства

Сохранить

## Веб-фильтр

- Без ограничений
- Блокировать по категориям
  - Сайты для взрослых
  - Насилие
  - Оружие
  - Азартные игры
  - Онлайн-игры
  - Наркотики
  - Терроризм
  - Пулы для добычи криптовалют
  - Нецензурная лексика
  - Чаты
  - Электронная почта
  - Социальные сети

## Выбранные объекты

## Удаленка

- Общие
- Статистика
- Конфигурация

- Права
- Планировщик заданий
- Ограничения обновлений
- Устанавливаемые компоненты
- Параметры подключения

## Windows

- Сканер
- Агент Dr.Web
- Офисный контроль
- SpIDer Mail и SpIDer Gate
- SpIDer Guard для рабочих станций
- Dr.Web для Microsoft Outlook
- Брандмауэр Dr.Web
- Превентивная защита
- Мониторинг сетевых портов
- Контроль приложений

## macOS

## UNIX

Удаленка. Настройки унаследованы от группы Everyone.

## Общие

Защита от эксплойтов

Блокировать исполнение неавторизованного кода



Уровень блокировки подозрительных действий

Оптимальный



Защищаемый объект	Разрешать	Спрашивать	Запрещать
Целостность запущенных приложений	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Целостность файлов пользователей	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Файл HOSTS	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Низкоуровневый доступ к диску	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Загрузка драйверов	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Параметры запуска приложений (IFEO)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Драйверы мультимедийных устройств	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Параметры оболочки Winlogon	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Нотификаторы Winlogon	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Автозапуск оболочки Windows	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ассоциации исполняемых файлов	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## Выбранные объекты

## Удаленка

- Общие
- Статистика
- Конфигурация
  - Права
  - Планировщик заданий
  - Ограничения обновлений
  - Устанавливаемые компоненты
  - Параметры подключения
  - Windows
    - Сканер
    - Агент Dr.Web
    - Офисный контроль
    - SpIDer Mail и SpIDer Gate
    - SpIDer Guard для рабочих станций
    - Dr.Web для Microsoft Outlook
    - Брандмауэр Dr.Web
    - Превентивная защита
    - Монитор сетевых портов
    - Контроль приложений

mac

UNIX

Удаленка. Настройки унаследованы от группы Everyone.

Название профиля ▾ ▴

Режим работы ▾ ▴

Критерии функционального анализа ▾ ▴

Запрещающие правила ▾ ▴

Разрешающие правила ▾ ▴

Данные не найдены

# Услуга «Антивирус Dr.Web»

Альтернатива корпоративному антивирусу



# Возможности управления услугой



- Подключение
- Автопродление
- Расширение или уменьшение кол-ва защищаемых объектов
- Смена тарифа
- Приостановка
- Отключение



#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!  
Задавайте вопросы!