Dr.WEB

для macOS

Руководство пользователя

Dr.Web для macOS
Версия 11.1
Руководство пользователя
19.12.2018

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

«Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. Введение 6
   1.1. Условные обозначения 6
   1.2. О программе 6
   1.3. Основные компоненты и функции 7
2. Установка и удаление 8
   2.1. Системные требования 8
   2.2. Установка и удаление Dr.Web 8
3. Управление лицензиями 9
   3.1. Лицензионный ключевой файл 9
   3.2. Менеджер лицензий 10
   3.3. Активация лицензии 10
4. Основные функции 13
   4.1. Запуск и завершение работы Dr.Web 14
   4.2. Обновление вирусных баз 15
   4.3. Постоянная антивирусная защита 15
   4.4. Проверка системы по требованию 16
   4.5. Обезвреживание угроз 18
   4.6. Проверка HTTP-трафика и контроль доступа к интернет-ресурсам 20
   4.7. Получение справки 22
5. Дополнительные функции 24
   5.1. Карантин 24
   5.2. Настройка автоматических действий 25
   5.3. Исключение объектов из проверки 26
   5.4. Проверка зашифрованного трафика 27
   5.5. Уведомления 27
   5.6. Административные права 28
   5.7. Оптимальное использование батареи 28
   5.8. Dr.Web Cloud 29
   5.9. Режим работы 29
   5.10. Восстановление настроек по умолчанию 31
6. Приложения 32
   6.1. Приложение А. Виды компьютерных угроз 32
   6.2. Приложение Б. Методы обнаружения угроз 36

6.3. Приложение В. Централизованная антивирусная защита **38**

6.4. Приложение Г. Комбинации клавиш **41**

6.5. Приложение Д. Техническая поддержка **42**

1. Введение

Благодарим вас за приобретение Dr.Web для macOS (далее – Dr.Web). Приложение обеспечивает надежную защиту от различных типов компьютерных угроз, используя наиболее современные технологии обнаружения и обезвреживания вирусов.

Данное руководство предназначено для помощи пользователям компьютеров под управлением macOS в установке и использовании Dr.Web.

1.1. Условные обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`/Volumes/Macintosh HD/`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

1.2. О программе

Dr.Web создан с целью помочь пользователям компьютеров под управлением macOS защитить рабочие машины от вирусов и прочих типов угроз.

Основные компоненты программы (*антивирусное ядро* и *вирусные базы*) являются не только крайне эффективными и нетребовательными к ресурсам, но и кросс-платформенными, что позволяет специалистам «Доктор Веб» создавать надежные антивирусные решения для различных операционных систем (ОС). Компоненты Dr.Web постоянно обновляются, а вирусные базы дополняются новыми сигнатурами, что обеспечивает защиту на наиболее современном уровне. Для дополнительной защиты от неизвестных вирусов используется эвристический анализатор.

1.3. Основные компоненты и функции

Dr.Web состоит из следующих компонентов, каждый из которых выполняет свой набор функций:

Компонент	Функции
SpIDer Guard	Резидентный антивирусный компонент, проверяющий все используемые файлы в режиме реального времени.
SpIDer Gate	Модуль антивирусной проверки HTTP-трафика и контроля доступа к интернет-ресурсам.
Сканер	Основной компонент для обнаружения вирусов, который может выполнять: • быструю, полную или выборочную проверку системы по запросу пользователя; • обезвреживание обнаруженных угроз (Лечение, Удаление, Перемещение в карантин; пользователь может вручную выбрать необходимое действие, либо задать автоматическое применение действия, указанного для данного типа угроз в настройках приложения).
Карантин	Специальная папка, которая используется для изоляции зараженных файлов и других угроз, чтобы они не могли нанести вред системе.
Модуль обновления	Данный компонент используется для обновления вирусных баз и других компонентов приложения через сеть Интернет.
Менеджер лицензий	Данный компонент используется для работы с лицензиями: он позволяет просмотреть информацию о текущей лицензии, активировать лицензию или демонстрационный период или получить новую лицензию.

Гибкие и удобные настройки Dr.Web позволяют настроить звуковые и экранные уведомления для различных событий, автоматические действия, применяемые к обнаруженным угрозам, интервалы обновлений вирусных баз, а также создать список файлов и папок, которые следует исключить из проверки.

2. Установка и удаление

Dr.Web поставляется в виде монтируемого образа диска.

Данный файл находится на дистрибутивном диске продукта. Вы также можете загрузить его с официального сайта «Доктор Веб».

> ⚠ Dr.Web несовместим с другими антивирусными программами. Установка двух антивирусов на один компьютер может привести к ошибкам в системе и потере важных данных.
>
> Поэтому перед установкой Dr.Web необходимо удалить его предыдущую версию или другой установленный антивирус.

2.1. Системные требования

Использование Dr.Web возможно на компьютере под управлением операционной системы macOS 10.7 или более поздних версий. Остальные требования к конфигурации совпадают с таковыми для соответствующих операционных систем.

2.2. Установка и удаление Dr.Web

Dr.Web поставляется в виде монтируемого образа диска.

Установка приложения

1. Скачайте установочный файл с сайта https://download.drweb.com/mac/;
2. Запустите данный файл;
3. Дважды нажмите на иконку приложения Dr.Web для macOS или перетащите ее в папку Applications.
4. Примите условия Лицензионного соглашения. Начнется процесс установки программы;
5. Введите пароль администратора и нажмите на кнопку «Установить Helper»
6. Dr.Web для macOS скопируется в папку Программы и запустится.

Удаление приложения

Для удаления Dr.Web достаточно переместить приложение в Корзину. При необходимости введите имя и пароль учетной записи администратора в соответствующем диалоговом окне.

3. Управление лицензиями

Для работы Dr.Web требуется лицензия. Приобретение лицензии возможно вместе с продуктом, а также на сайте компании «Доктор Веб». Лицензия позволяет полноценно использовать все возможности продукта на протяжении всего срока действия. Лицензия регулирует права пользователя, установленные в соответствии с пользовательским договором. Для активации лицензии, ее продления по истечении срока ее действия или приобретения новой лицензии используется Менеджер лицензий.

Если на вашем компьютере установлено приложение Server.app, операционная система определяется как macOS Server. В таком случае для работы Dr.Web необходимо либо удалить приложение Server.app, либо приобрести лицензию на Dr.Web для macOS Server.

Активировать лицензию рекомендуется сразу после установки приложения, так как это необходимо для обновления приложения, а также активации функций постоянной антивирусной защиты и проверки по требованию вашего Mac.

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете активировать демонстрационный период. Он обеспечивает полную функциональность основных компонентов, но срок его действия существенно ограничен.

Активация демонстрационного периода на одном и том же компьютере возможна не чаще, чем один раз в год.

Демонстрационный период может быть активирован сроком:

- На 3 месяца. Вам необходимо зарегистрироваться на сайте компании «Доктор Веб» и получить серийный номер.
- На 1 месяц. При этом серийный номер не требуется, регистрационные данные не запрашиваются.

3.1. Лицензионный ключевой файл

Тип лицензии определяется с помощью специального файла, называемого *лицензионным ключевым файлом*. В лицензионном ключевом файле содержится, в частности, следующая информация:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование приложения;
- другие ограничения (в частности, количество пользователей, которые будут использовать приложение).

Лицензия для Dr.Web является действительной при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- лицензия распространяется на все используемые программой модули;
- целостность лицензионного ключевого файла не нарушена.

При нарушении любого из условий лицензия становится *недействительной*, при этом Dr.Web перестает находить и обезвреживать угрозы.

Лицензионный ключевой файл имеет расширение `.key`, и вы можете получить его во время активации лицензии при первом запуске Dr.Web с помощью компонента Менеджер лицензий.

Параметры лицензионного ключевого файла, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением. В этот же файл заносится информация о пользователе и продавце приложения.

Рекомендуется сохранять ключевой файл до истечения срока действия лицензии или демонстрационного периода.

> ⚠ Лицензионный ключевой файл, полученный для активации демонстрационного периода, может использоваться только на том компьютере, на котором вы проходили активировали лицензию.

3.2. Менеджер лицензий

Для упрощения работы с лицензиями используется компонент Менеджер лицензий.

Чтобы открыть Менеджер лицензий, выполните одно из следующих действий:

- Выберите пункт **Менеджер лицензий** в меню приложения (полоса меню в верхней части рабочего стола).
- В главном окне приложения нажмите на раздел с информацией о лицензии.

В окне **Лицензия на продукт Dr.Web** вы можете просмотреть информацию о состоянии текущей лицензии. Чтобы активировать новую лицензию Dr.Web или продлить уже существующую, нажмите кнопку **Получить новую лицензию**.

3.3. Активация лицензии

После установки вам необходимо активировать лицензию Dr.Web. Активация подтверждает, что вы являетесь полноправным пользователем приложения и делает доступными функции обновления, постоянной антивирусной защиты и проверки по требованию.

Окно активации появляется автоматически, когда вы впервые запускаете Dr.Web. Также вы можете запустить активацию из окна Менеджер лицензий, нажав кнопку **Получить новую лицензию**.

Активация лицензии

1. Если у вас есть серийный номер для активации лицензии или демонстрационного периода на 3 месяца, на первом шаге процедуры активации нажмите **Активировать лицензию**.
2. Введите серийный номер и нажмите **Далее**. В случае активации демонстрационного периода перейдите к шагу 5.
3. При наличии предыдущей лицензии, укажите ее серийный номер. Выберите необходимую опцию, затем введите серийный номер или перетащите лицензионный ключевой файл в соответствующую область (вы также можете щелкнуть по этой области, чтобы выбрать файл).

   Если вы уже являлись пользователем Dr.Web и активируете новую лицензию, ее действие будет продлено на 150 дополнительных дней. Для этого необходимо указать данные о вашей предыдущей лицензии: серийный номер или лицензионный ключевой файл.

   Если вы уже являлись пользователем Dr.Web и активируете лицензию продления, вам необходимо указать серийный номер или лицензионный ключевой файл предыдущей лицензии. Если вы не укажете ни то, ни другое, срок действия новой лицензии будет сокращен на 150 дней.

   Нажмите **Далее**.
4. Для активации лицензии введите персональные сведения (регистрационное имя, регион, город и др.). Поле **Регистрационное имя** является обязательным. Если вы хотите получать по электронной почте новости о продукте, установите соответствующий флажок.

   Нажмите **Далее**.
5. Лицензия будет активирована. Данная процедура, как правило, не требует вмешательства пользователя. Если активация закончилась успешно, выводится соответствующее сообщение и указывается срок действия лицензии или активации демонстрационного периода.

   Нажмите на кнопку **Готово**. Если активация завершилась неудачно, выводится сообщение об ошибке.

Активация демонстрационного периода

Если вы планируете только ознакомиться с функциями Dr.Web, на первом шаге процедуры активации выберите вариант **Получить демо**. Для ознакомления с работой Dr.Web вы можете активировать демонстрационный период:

- На 3 месяца. Для этого вам необходимо зарегистрироваться на сайте и получить серийный номер. Серийный номер будет отправлен на указанный вами в процессе

заполнения анкеты адрес электронной почты. Далее вы можете активировать его, нажав **Активировать лицензию** в окне Менеджер лицензий.

- На 1 месяц. При этом серийный номер не требуется, регистрационные данные не запрашиваются. Лицензия будет активирована автоматически.

Покупка лицензии

Если у вас нет серийного номера, на первом шаге процедуры активации выберите **Приобрести лицензию**, чтобы перейти на страницу онлайн-магазина «Доктор Веб».

Рекомендуется сохранять лицензионный ключевой файл до истечения срока его действия. При переустановке продукта или в случае его установки на несколько компьютеров вы можете использовать лицензионный ключевой файл, полученный при первой активации.

Установка имеющегося лицензионного ключевого файла

1. На первом шаге процедуры активации выберите вариант **Другие виды активации**.
2. Если у вас уже имеется лицензионный ключевой файл или конфигурационный файл для подключения к антивирусной сети и работы в режиме централизованной защиты, перетащите его в пунктирную область или щелкните по этой области, чтобы выбрать файл.
3. Чтобы активировать лицензию, нажмите **Далее**.

Повторная активация

Повторная активация лицензии или демонстрационного периода может потребоваться, если лицензионный ключевой файл утерян.

В случае повторной активации лицензии или демонстрационного периода выдается тот же лицензионный ключевой файл, который был выдан ранее, при условии, что срок его действия не истек.

Повторная активация демонстрационного периода на 3 месяца может осуществляться только на том компьютере, на котором он был активирован ранее.

Активация лицензии с одним и тем же серийным номером допускается не более 25 раз. Если это число превышено, лицензия активирована не будет. В этом случае обратитесь в службу технической поддержки (в запросе следует подробно описать ситуацию, указать персональные данные, введенные при активации лицензии, и серийный номер). Лицензионный ключевой файл будет выслан вам службой технической поддержки по электронной почте.

4. Основные функции

Доступ к основным функциям Dr.Web осуществляется из главного окна программы (см. иллюстрацию ниже), которое состоит из следующих разделов, используемых для управления и доступа к функциям приложения:

Раздел	**Описание**
Пульт	В этом разделе вы можете: • включить/выключить постоянную антивирусную защиту; • включить/выключить проверку веб-трафика; • ознакомиться с информацией о последней проведенной проверке системы и запустить быструю или полную проверку системы, а также выборочную проверку отдельных файлов и папок; • ознакомиться с информацией о последнем обновлении вирусных баз и при необходимости запустить обновление вручную; • ознакомиться с информацией о текущей лицензии и запустить при необходимости Менеджер лицензий; • переключиться на разделы **Угрозы** и **Мой Dr.Web**.
Угрозы	В данном разделе вы можете просмотреть список обнаруженных при проверке угроз, применить к ним действия по обезвреживанию, а также перейти к просмотру и управлению содержимым карантина.
Мой Dr.Web	В данном разделе вы можете ознакомиться с новостями компании «Доктор Веб», проводимыми акциями и последней информацией о вирусах и перейти на вашу персональную страницу на официальном сайте компании «Доктор Веб». На данной странице вы сможете получить информацию о вашей лицензии, количестве записей в вирусных базах и дате последнего обновления, продлить срок действия лицензии, задать вопрос службе поддержки и многое другое.

Рисунок 1. Главное окно программы

4.1. Запуск и завершение работы Dr.Web

Запуск приложения

Чтобы запустить Dr.Web, выполните одно из следующих действий:

- откройте папку Программы в Finder и запустите программу **Dr.Web для macOS**;
- вызовите Launchpad и запустите программу **Dr.Web для macOS**.

При запуске приложения выполняется проверка настроек обновления и, в случае необходимости, происходит загрузка обновлений программы и вирусных баз.

> При первом запуске программы начинается процесс обновления, включающий загрузку вирусных баз, что может занять продолжительное время.

Завершение работы приложения

Чтобы завершить работу Dr.Web, выполните одну из следующих операций:

- выберите пункт **Завершить Dr.Web для macOS** в меню приложения (полоса меню в верхней части рабочего стола);
- нажмите и удерживайте значок приложения в Dock, затем выберите в меню **Завершить**;

- нажмите на комбинацию клавиш COMMAND-Q на клавиатуре.

Компонент SpIDer Guard остается активным даже после завершения работы Dr.Web. Он является резидентным антивирусным монитором, который проверяет любые используемые файлы в реальном времени.

4.2. Обновление вирусных баз

Для обнаружения вредоносных объектов антивирусные продукты компании «Доктор Веб» используют специальные вирусные базы Dr.Web, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вирусные угрозы, эти базы требуют периодического обновления. Такое обновление позволяет обнаруживать ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев – излечивать ранее неизлечимые зараженные файлы. Время от времени совершенствуются антивирусные алгоритмы, реализованные в виде исполняемых файлов и программных библиотек. Благодаря опыту эксплуатации антивирусов Dr.Web исправляются обнаруженные в программах ошибки, обновляется система помощи и документация. Для поддержания актуальности вирусных баз и программных алгоритмов компанией «Доктор Веб» реализована система распространения обновлений через сеть Интернет.

Обновление вирусных баз и других компонентов Dr.Web гарантирует соответствие защиты вашего Mac современным требованиям и ее готовность к новым угрозам. Обновление выполняет специальный компонент, называемый Модулем обновления.

При первом запуске Dr.Web перед началом работы необходимо выполнить обновление вирусных баз до актуального состояния. Дальнейшее обновление будет происходить автоматически с периодичностью, которую вы можете задать в настройках Dr.Web.

Настройка интервала обновления вирусных баз

1. В меню приложения откройте **Настройки** и выберите вкладку **Обновление**.
2. При необходимости поменяйте интервал загрузки обновлений.

4.3. Постоянная антивирусная защита

Постоянная антивирусная защита осуществляется при помощи компонента SpIDer Guard. Компонент в режиме реального времени проверяет все файлы, к которым осуществляется доступ пользователем или запущенными программами, и процессы, запущенные на вашем Mac. SpIDer Guard запускается сразу после установки и активации лицензии Dr.Web. При обнаружении угрозы SpIDer Guard выводит на экран сообщение и применяет действие, заданное в настройках приложения.

macOS блокирует загрузку системных расширений (модулей ядра). Для корректной работы SplDer Guard разрешите загрузку системного ПО от Doctor Web Ltd. в панели «Защита и безопасность» Системных настроек.

Данная проблема актуальна для пользователей операционных систем macOS High Sierra 10.13 и более поздних версий.

Включение и отключение SplDer Guard

Чтобы временно приостановить или возобновить работу компонента SplDer Guard, выполните одно из следующих действий:

- В разделе **Пульт** главного окна Dr.Web включите/выключите опцию **SplDer Guard** (см. Рисунок 1);
- щелкните значок Dr.Web в строке меню в верхней части экрана и выберите соответствующий пункт.

Отключать компонент SplDer Guard могут только пользователи, обладающие правами администратора.

Прибегайте к отключению SplDer Guard с исключительной осторожностью! В период отключения постоянной антивирусной защиты не следует подключаться к сети Интернет, а также считывать файлы с носителей, не проверенных Сканером.

4.4. Проверка системы по требованию

Dr.Web осуществляет проверку объектов файловой системы по запросу пользователя, обнаруживая угрозы, скрывающие свое присутствие в системе. Для надежной защиты вашего Mac необходимо время от времени запускать проверку системы с помощью Dr.Web.

Чтобы быстро проверить наиболее уязвимые части системы, выполните **Быстрая проверка**, чтобы проверить всю файловую систему — **Полная проверка**, или выберите файлы и папки для проверки.

При проверке увеличивается нагрузка на процессор, что может сказаться на уровне заряда аккумулятора. На портативных компьютерах рекомендуется проводить проверку системы при питании от сети.

Запуск проверки системы

1. В главном окне Dr.Web выберите режим проверки:

- **Быстрая проверка** – быстро проверить наиболее уязвимые части системы.
- **Полная проверка** – полная проверка всей файловой системы.

Кроме того, вы можете использовать специальные комбинации клавиш CONTROL-COMMAND-E и CONTROL-COMMAND-F на клавиатуре для запуска быстрой и полной проверки соответственно.

2. Чтобы проверить отдельные файлы и папки, перетащите их в главное окно приложения или щелкните по пунктирной области в левой части главного окна программы, чтобы открыть окно выбора объектов проверки.

   В открывшемся списке объектов укажите файлы и папки, которые вы хотите проверить:

   - чтобы добавить объект в список, нажмите кнопку + под списком объектов или перетащите этот объект в список;
   - чтобы исключить объект из списка, выделите его и нажмите кнопку − или перетащите его за границы окна программы.

   Нажмите кнопку **Запустить проверку**, чтобы начать проверку выбранных объектов.

Запуск проверки файлов из контекстного меню

Чтобы запустить проверку отдельного файла или папки с файлами:

1. Выделите нужный файл или папку на Рабочем столе или в Finder.
2. Выполните команду контекстного меню **Проверить с Dr.Web**.

При запуске процесса проверки главное окно переключается на окно результатов (см. иллюстрацию ниже). В ходе проверки в данном окне показывается следующая информация:

- время запуска проверки;
- количество проверенных объектов;
- время, оставшееся до окончания проверки;
- количество обнаруженных угроз;
- имя файла, который проверяется в данный момент.

В нижней части окна приводится краткий статистический отчет по текущей сессии проверки.

Вы можете приостановить или прервать проверку, используя кнопки управления **Пауза** и **Стоп**.

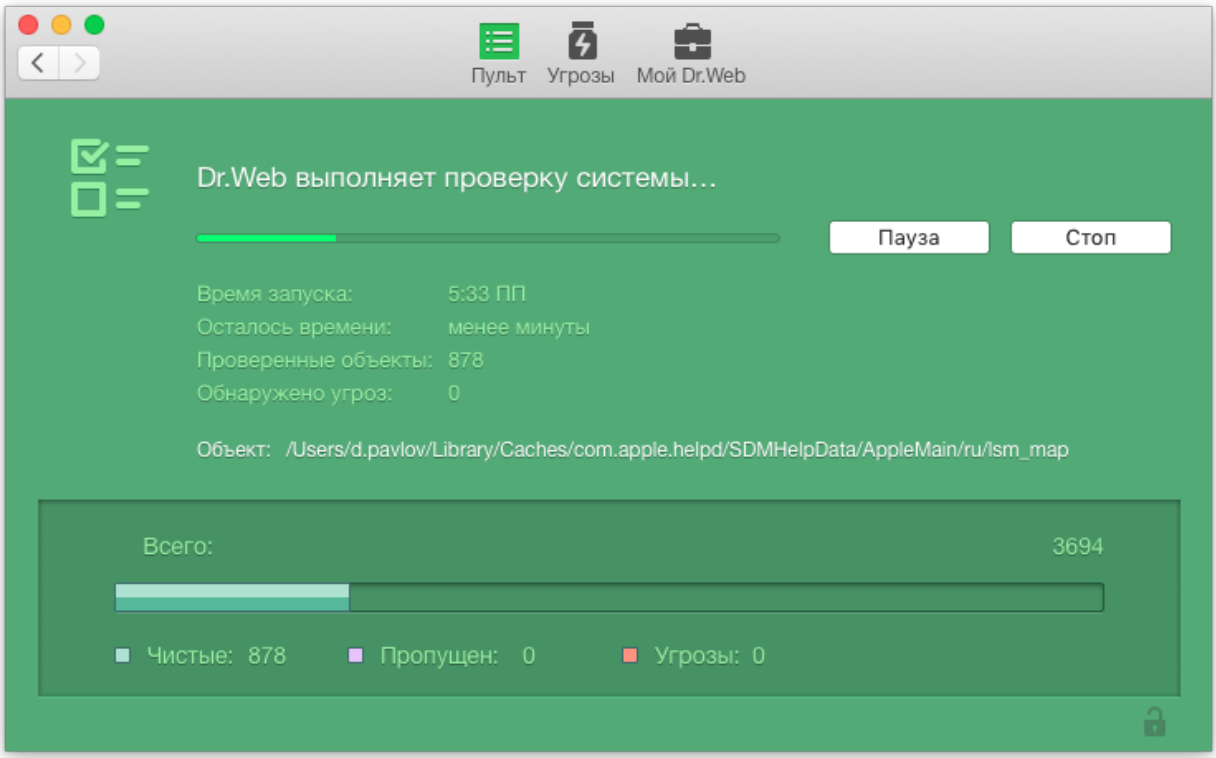


Рисунок 2. Окно результатов проверки

Некоторые файлы могут быть пропущены при проверке, например, если они повреждены или защищены паролем. Если в списке пропущенных файлов есть архивы, попробуйте распаковать их перед проверкой.

Для работы Dr.Web могут потребоваться права администратора для проверки критических областей жесткого диска. Чтобы предоставить приложению административные права, выполните следующие действия:

- нажмите комбинацию клавиш COMMAND-SHIFT-A на клавиатуре, далее введите пароль администратора;
- нажмите на изображение замка в нижней части окна и введите пароль администратора.

4.5. Обезвреживание угроз

Для обезвреживания угроз вы можете настроить автоматические действия или применять действия к обнаруженным угрозам вручную. Чтобы просмотреть список угроз и применить к ним действия по обезвреживанию, перейдите на вкладку **Угрозы** на главном окне приложения (см. рисунок ниже).

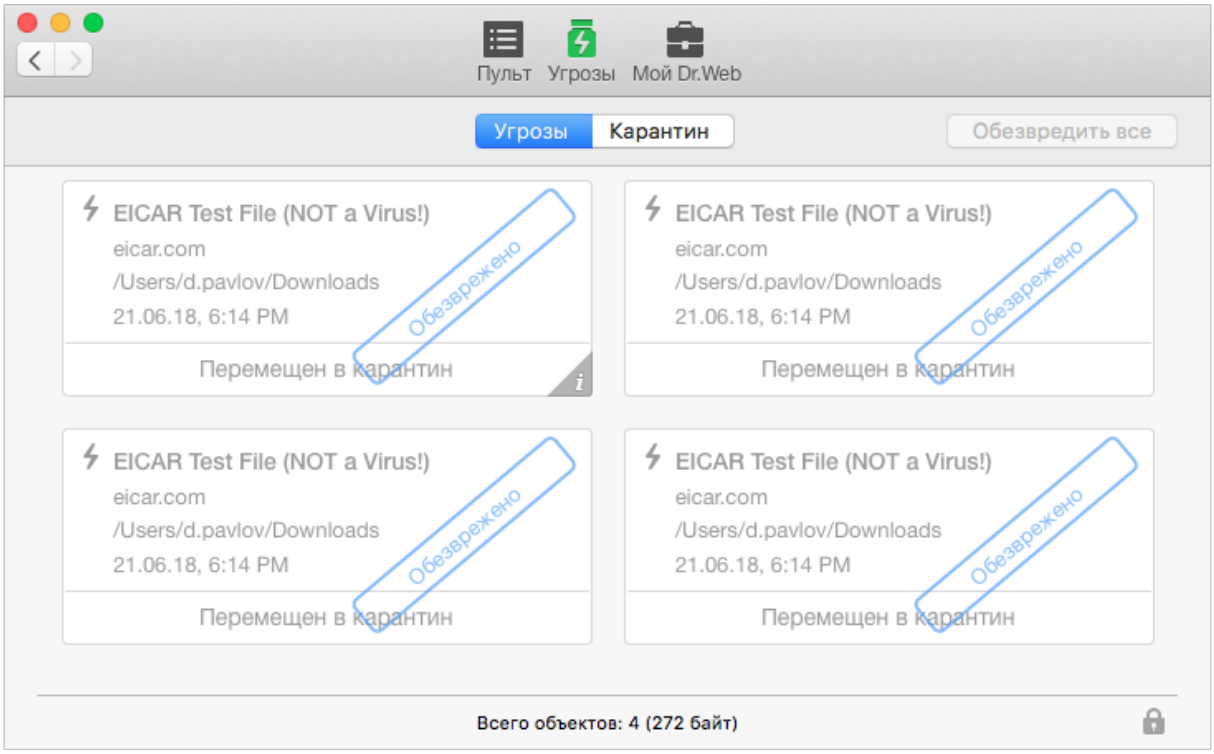


Рисунок 3. Вкладка Угрозы

Просмотр информации об угрозах

1. Чтобы просмотреть список обнаруженных угроз, откройте раздел **Угрозы**. В строке состояния в нижней части окна показывается общее количество обнаруженных угроз, суммарный размер и количество и размер выделенных объектов.
2. Для просмотра подробной информации об угрозе нажмите кнопку  или дважды щелкните по этой угрозе.
3. Чтобы ознакомиться с информацией о типе выбранной угрозы на сайте компании «Доктор Веб», в окне с подробной информацией об угрозе нажмите кнопку слева от ее имени.

Обработка вредоносных объектов

1. Откройте раздел **Угрозы**.
2. Чтобы применить к угрозе действие, указанное в настройках приложения для соответствующего типа угроз, нажмите кнопку с этим действием под угрозой. Чтобы выбрать для угрозы альтернативное действие, в окне с подробной информацией о данной угрозе нажмите стрелку на кнопке с рекомендованным действием.
3. Чтобы применить действие к нескольким угрозам, выделите их удерживая клавишу SHIFT, после чего в разделе **Действия** в главном меню приложения или в контекстном меню списка угроз выберите действие для обезвреживания выбранных угроз.

4. Чтобы обезвредить все обнаруженные угрозы, нажмите кнопку **Обезвредить все**. К угрозам будут применены действия, указанные в настройках приложения для соответствующих типов угроз.

Кроме того, при обезвреживании угроз вы можете использовать специальные комбинации клавиш клавиатуры.

4.6. Проверка HTTP-трафика и контроль доступа к интернет-ресурсам

Проверка веб-трафика и контроль доступа к интернет-ресурсам осуществляется при помощи компонента SpIDer Gate. SpIDer Gate проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих угрозы безопасности. Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, т. е. работающие с сетью Интернет.

SpIDer Gate также позволяет контролировать доступ к интернет-ресурсам и тем самым оградить пользователей от просмотров нежелательных веб-сайтов (сайтов, посвященных насилию, азартным играм и т. п.).

Данный компонент запускается сразу после установки и активации лицензии Dr.Web.

Другие приложения для проверки веб-трафика и контроля доступа к веб-ресурсам, установленные на вашем Mac, могут работать некорректно, если включен SpIDer Gate.

macOS блокирует загрузку системных расширений (модулей ядра). Для корректной работы SpIDer Gate разрешите загрузку системного ПО от Doctor Web Ltd. в панели «Защита и безопасность» Системных настроек.

Данная проблема актуальна для пользователей операционных систем macOS High Sierra 10.13 и более поздних версий.

Включение и отключение SpIDer Gate

Чтобы временно приостановить или возобновить работу компонента SpIDer Gate, выполните одно из следующих действий:

- включите/выключите опцию **SpIDer Gate** в разделе **Пульт** главного окна Dr.Web (см. Рисунок 1);
- щелкните значок Dr.Web в строке меню в верхней части экрана и выберите соответствующий пункт.

Отключать компонент SplDer Gate могут только пользователи, обладающие правами администратора.

Настройка проверки HTTP-трафика

При базовых настройках SplDer Gate блокирует получаемые по сети объекты, если они содержат вредоносные программы. Вы можете выбрать типы блокируемых вредоносных программ, настроить действия для объектов, проверить которые не удалось, а также максимальное время проверки одного файла. Для этого выполните следующие действия:

1. В меню приложения откройте **Настройки** и выберите вкладку **SplDer Gate**. Настройки компонента SplDer Gate могут изменять только пользователи, обладающие правами администратора. При необходимости, нажмите изображение замка в нижней части вкладки настроек и введите имя и пароль администратора.
2. Нажмите кнопку **Дополнительно**.
3. Выберите типы вредоносных программ, передачу которых вы хотите блокировать.
4. Задайте максимальное время проверки одного файла.
5. По умолчанию, передача объектов, проверка которых не удалась, блокируется. Если вы хотите разрешить передачу таких объектов, снимите флажок **Блокировать непроверенные объекты**.
6. Нажмите **OK**, чтобы сохраните сделанные изменения.

Настройка доступа к интернет-ресурсам

Помимо антивирусной проверки HTTP-трафика, SplDer Gate по умолчанию блокирует доступ к URL, добавленным по обращению правообладателя и нерекомендуемым сайтам. Вы можете отключить данные функции на вкладке **SplDer Gate** настроек Dr.Web. Кроме того, вы можете выбрать категории веб-сайтов, доступ к которым должен быть заблокирован, а также создать черный и белый списки веб-адресов, чтобы автоматически разрешить или запретить доступ к определенным сайтам независимо от других настроек SplDer Gate.

Предустановленные настройки SplDer Gate являются оптимальными для большинства применений, их не следует изменять без необходимости.

Выбор категорий сайтов для блокировки доступа

1. В меню приложения откройте **Настройки** и выберите вкладку **SplDer Gate**. Настройки компонента SplDer Gate могут изменять только пользователи, обладающие правами администратора. При необходимости, нажмите изображение замка в нижней части вкладки настроек и введите имя и пароль администратора.
2. Выберите категории сайтов, доступ к которым должен быть заблокирован.

Белый и черный списки

1. В меню приложения откройте **Настройки** и выберите вкладку **Исключения**.
2. Нажмите кнопку **Сайты**. Черный и белый списки могут изменять только пользователи, обладающие правами администратора. При необходимости, нажмите изображение замка в нижней части вкладки настроек и введите имя и пароль администратора.
3. По умолчанию списки пусты. При необходимости вы можете добавить адреса веб-сайтов в белый и черный списки. Нажмите кнопку +, расположенную под соответствующим списком, и введите доменное имя или часть доменного имени веб-сайта, доступ к которому вы хотите разрешить или запретить:
   - чтобы добавить в список определенный сайт, введите его полный адрес (например, **www.example.com**). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью;
   - чтобы настроить доступ к тем веб-сайтам, в адресе которых содержится определенный текст, введите в поле этот текст. Пример: если вы введете текст example, то доступ к адресам **example.com**, **example.test.com**, **test.com/example**, **test.example222.ru** и т. п. будет определяться данной записью;
   - чтобы настроить доступ к определенному домену, укажите имя домена с символом «.». В таком случае доступ ко всем ресурсам, находящиеся на этом домене, будет определяться данной записью. Если при указании домена используется символ «/», то та часть подстроки, что стоит слева от символа «/», будет считаться доменным именем, а части справа от символа – частью разрешенного на данном домене адреса. Пример: если вы введете текст **example.com/test**, то будут обрабатываться такие адреса как **example.com/test11**, **template.example.com/test22** и т.п.

   Чтобы удалить веб-сайты из черного или белого списка, выделите их в соответствующем списке и нажмите кнопку − или перетащите их за пределы окна настроек программы.
4. Нажмите кнопку **ОК**, чтобы сохранить изменения.

Безопасный поиск

Чтобы функция безопасного поиска включалась автоматически в поисковых системах:

1. В меню приложения откройте **Настройки** и выберите вкладку **SplDer Gate**.
2. Установите соответствующий флажок в разделе **Безопасный поиск**.

4.7. Получение справки

Для получения справки о приложении воспользуйтесь **Справка Dr.Web для macOS**, доступ к которой осуществляется при помощи программы просмотра Apple Help.

Чтобы вызвать **Справка Dr.Web для macOS**, в верхней части рабочего стола в меню **Справка** выберите пункт **Справка Dr.Web для macOS** или введите интересующее вас слово в соответствующее поле.

Если вам не удается решить проблему или найти ответ на интересующий вас вопрос о Dr.Web, обратитесь в службу технической поддержки.

5. Дополнительные функции

Дополнительные функции Dr.Web позволяют настроить оптимальные параметры защиты в зависимости от нужд пользователя.

5.1. Карантин

Карантин предоставляет возможность изоляции обнаруженных угроз от остальной системы в том случае, если объект вам нужен и его не удается вылечить (возможно, его удастся вылечить после очередного обновления программы, так как алгоритмы лечения постоянно совершенствуются).

> Из соображений конфиденциальности для каждого пользователя создается отдельная папка карантина. Поэтому, если вы перешли в режим работы с правами администратора, обнаруженные угрозы будут перемещены в карантин администратора и не будут доступны в карантине пользователей.

Для просмотра и управления списком объектов, перемещенных в карантин, откройте вкладку **Карантин** раздела **Угрозы** (см. иллюстрацию ниже). В строке состояния в нижней части окна показывается общее количество объектов в карантине и их суммарный размер, а также количество и размер выделенных объектов.

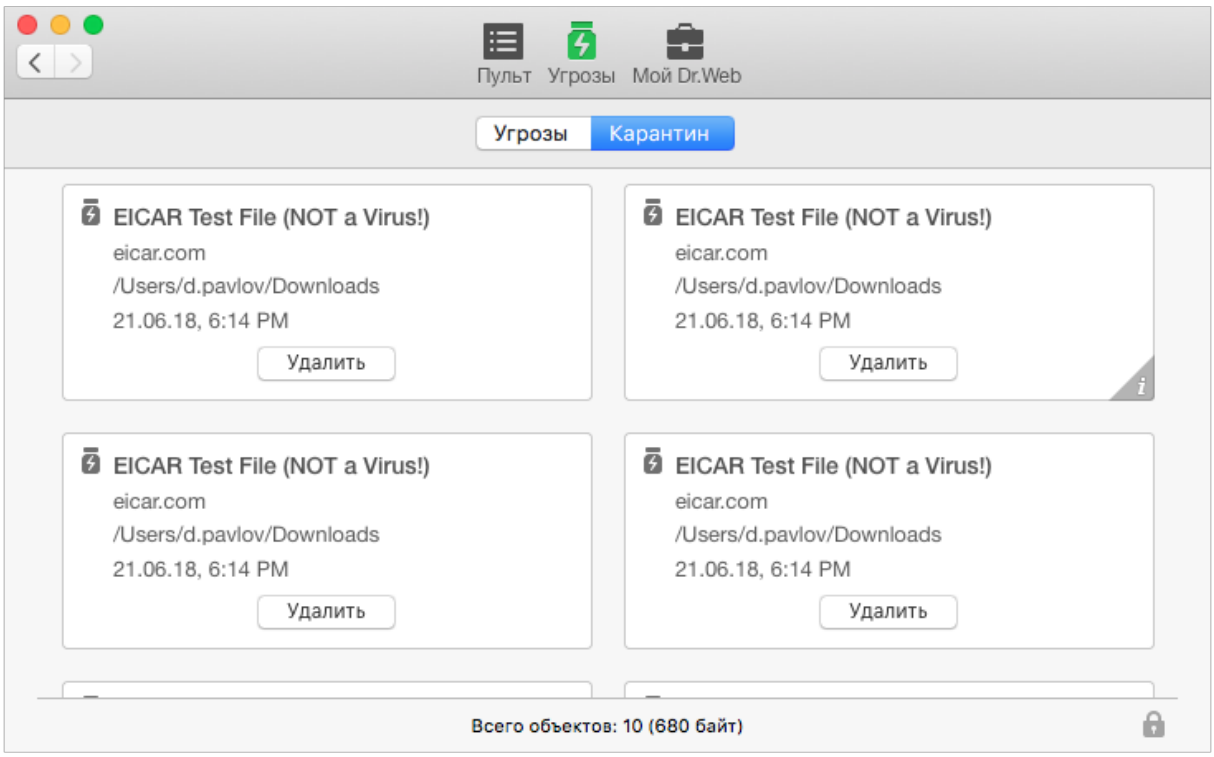


Рисунок 4. Список объектов, перемещенных в карантин

Просмотр информации об объектах в карантине

1. Чтобы просмотреть информацию об объекте в карантине, нажмите кнопку  или дважды щелкните по нему.
2. Чтобы ознакомиться с информацией о типе угроз, которые предположительно содержит выбранный объект, в окне с подробной информацией об объекте нажмите кнопку  слева от его имени. В результате откроется страница с информацией о данном типе угроз на сайте компании «Доктор Веб».

Обработка объектов в карантине

1. Чтобы применить рекомендованное действие к объекту в карантине, нажмите кнопку с этим действием под объектом. Чтобы выбрать для объекта альтернативное действие, в окне с подробной информацией о выбранном объекте нажмите стрелку на кнопке с рекомендованным действием. Вы можете выбрать одно из следующих действий:
   - **Удалить** – навсегда удалить объект из файловой системы;
   - **Восстановить** – поместить объект из карантина туда, откуда он был перемещен;
   - **Восстановить в** – указать путь для восстановления объекта из карантина.
2. Чтобы применить действие к нескольким объектам одновременно, выделите их удерживая клавишу SHIFT, после чего в разделе **Действия** в главном меню приложения или в контекстном меню списка объектов выберите действие для обезвреживания выбранных объектов.

Кроме того, для применения действий к объектам в карантине вы можете использовать специальные комбинации клавиш клавиатуры.

5.2. Настройка автоматических действий

Вы можете задать действия, которые должны применяться к различным типам компьютерных угроз автоматически, если не требуется выбрать необходимое действие вручную. Автоматическая реакция настраивается отдельно для Сканера и компонента SpIDer Guard.

Настройка автоматических действий

1. Чтобы открыть настройки действий, которые должны применяться автоматически компонентами Dr.Web, выполните одно из следующих действий:
   - чтобы настроить реакцию Сканера, в меню приложения откройте **Настройки** и выберите вкладку **Сканер**;
   - чтобы настроить реакцию компонента SpIDer Guard, в меню приложения откройте **Настройки** и выберите вкладку **SpIDer Guard**.
2. При необходимости поменяйте автоматические действия для инфицированных и подозрительных объектов.

3. Щелкните по ссылке **Другие**, чтобы настроить действия, которые следует применять к различным типам вредоносного ПО (рекламным программам, программам дозвона, программам-шуткам, программам взлома и потенциально опасным программам).
4. Действия, указанные в настройках SpIDer Guard, будут применены автоматически к угрозам, обнаруженным данным компонентом. Чтобы при проверке системы Сканером действия по обезвреживанию угроз также применялись в автоматическом режиме, установите флажок **Применять действия автоматически** в разделе настроек Сканера.
5. Нажмите кнопку **Дополнительно**, чтобы настроить проверку комплексных объектов (архивов и почтовых файлов), а также задать максимальное время проверки одного файла. При этом необходимо учитывать, что проверка содержимого архивов и почтовых файлов, а также увеличение времени проверки одного файла может увеличить общее время проверки системы и в некоторых случаях привести к замедлению работы вашего Mac.

Предустановленные настройки автоматической реакции являются оптимальными для большинства применений, их не следует изменять без необходимости.

По умолчанию настройки компонента SpIDer Guard заблокированы, чтобы пользователи без прав администратора не могли эти настройки изменить. Чтобы разблокировать настройки, откройте раздел **SpIDer Guard**, нажмите изображение замка в нижней части окна и введите имя и пароль администратора.

5.3. Исключение объектов из проверки

При необходимости вы можете исключить из проверки следующие объекты:

- файлы и папки;
- веб-сайты;
- приложения.

Настройка списка исключений

1. В меню приложения откройте **Настройки** и выберите вкладку **Исключения**.
2. Чтобы перейти к спискам исключений файлов и папок, веб-сайтов или приложений, нажмите соответствующую кнопку. По умолчанию настройки исключений заблокированы. Чтобы разблокировать настройки, нажмите изображение замка в нижней части окна настроек и введите имя и пароль учетной записи администратора.
3. При необходимости измените список исключений:
   - Чтобы добавить файл, папку или приложение в список исключений, нажмите кнопку + и укажите нужный объект или перетащите его в список.
   - Чтобы добавить веб-сайт в список исключений, нажмите кнопку + под белым списком и введите доменное имя или часть доменного имени веб-сайта.

- Чтобы удалить объекты из списка исключений, выделите их в списке и нажмите кнопку − или перетащите их за границы окна программы.

> Предустановленные настройки исключений являются оптимальными для большинства применений, их не следует изменять без необходимости.
>
> ---
>
> Все папки карантина добавлены в список исключений по умолчанию. Эти папки предназначены для изоляции опасных объектов, поэтому доступ к ним заблокирован и проверять их нет смысла.

5.4. Проверка зашифрованного трафика

По умолчанию Dr.Web не проверяет данные, передаваемые по криптографическому протоколу SSL.

Включение проверки зашифрованного трафика

1. В меню приложения откройте **Настройки** и выберите вкладку **Сеть**.
2. Если настройки заблокированы, нажмите изображение замка в нижней части окна и введите имя и пароль учетной записи администратора.
3. Установите флажок **Проверять зашифрованный трафик**.

Получение сертификата «Доктор Веб»

Если проверка зашифрованного трафика включена, для работы браузеров и почтовых клиентов, которые передают и получают этот трафик и не обращаются при этом к системному хранилищу сертификатов, может потребоваться сертификат компании «Доктор Веб».

1. В меню приложения откройте **Настройки** и выберите вкладку **Сеть**.
2. Нажмите кнопку **Экспортировать** и сохраните сертификат в удобную для вас папку.

5.5. Уведомления

Вы можете настроить уведомления о различных событиях, которые могут происходить в ходе работы Dr.Web, на вкладке **Основные** настроек приложения.

Типы уведомлений

- сообщения, выводимые на экран;
- звуковые уведомления.

Настройка звуковых оповещений

По умолчанию звуковые уведомления включены. Чтобы включить или отключить использование звуков, установите или снимите флажок **Звуковое сопровождение событий** на вкладке **Основные** настроек приложения.

Настройка экранных уведомлений

1. По умолчанию экранные уведомления включены. Чтобы отключить или включить экранные оповещения, снимите или установите флажок **Использовать уведомления** на вкладке **Основные** настроек приложения.
2. Выберите тип системы уведомлений:
   - **Dr.Web** (установлен по умолчанию);
   - **Системные** (стандартные уведомления macOS);
   - **Growl**
3. Для уведомлений Dr.Web вы можете настроить дополнительные параметры, нажав кнопку **Настроить**:
   - укажите длительность отображения уведомлений на экране;
   - выберите область экрана, в которой будут отображаться уведомления.

Чтобы сохранить сделанные изменения в настройках уведомлений Dr.Web, нажмите кнопку **ОК**.

5.6. Административные права

Для работы Dr.Web могут потребоваться права администратора, чтобы получить доступ и проверить критические области жесткого диска. Чтобы запускать проверку от имени администратора, выполните следующие действия:

1. В меню приложения откройте **Настройки** и выберите вкладку **Основные**.
2. Установите флажок **Запускать проверку от имени администратора**. Вам потребуется ввести имя и пароль администратора перед началом проверки (быстрой, полной или выборочной).

5.7. Оптимальное использование батареи

По умолчанию при переходе вашего Mac на питание от аккумулятора проверка приостанавливается, чтобы предотвратить быстрый расход заряда батареи. При этом Dr.Web выдает соответствующее предупреждение, позволяющее вам подтвердить приостановку проверки или продолжить ее. Вы можете отключить опцию приостановки проверки при переходе на питание от аккумулятора, выполнив следующие действия:

1. В меню приложения откройте **Настройки** и выберите вкладку **Основные**.

2. Если вы не хотите, чтобы проверка приостанавливалась при переходе на питание от аккумулятора, снимите флажок **Приостанавливать проверку при работе от аккумулятора**.

5.8. Dr.Web Cloud

Облачные сервисы Dr.Web Cloud позволяют антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени. В зависимости от настроек обновления информация об угрозах, используемая компонентами вашей антивирусной защиты, может устаревать. Использование облачных сервисов позволяет гарантированно оградить пользователей вашего компьютера от сайтов с нежелательным содержимым.

Подключение к сервисам

1. В меню приложения откройте **Настройки** и выберите вкладку **Dr.Web Cloud**.
2. Установите переключатель **Я хочу подключиться к сервисам (рекомендуется)**.

5.9. Режим работы

При необходимости вы можете использовать установленный Dr.Web для работы в антивирусной сети вашей компании или IT-провайдера. Для антивирусной защиты в таком централизованном режиме вам не потребуется устанавливать дополнительные программные модули или удалять установленный Dr.Web.

В режиме централизованной защиты обновления вирусных баз загружаются автоматически с сервера централизованной защиты. Если на сервере централизованной защиты разрешен запуск приложения в мобильном режиме, при отсутствии соединения с сервером, если вирусные базы устарели, обновления будут загружаться через Интернет с серверов обновлений Dr.Web. При восстановлении соединения Dr.Web автоматически перейдет на загрузку обновлений с сервера централизованной защиты.

Кроме того, некоторые настройки Dr.Web, в частности, возможности управления постоянной защитой и проверкой системы по требованию, могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг. Ключевой файл для работы в таком режиме получается автоматически с сервера централизованной защиты, и ваша персональная лицензия не используется.

По умолчанию настройки режима работы Dr.Web заблокированы, чтобы пользователи без прав администратора не могли эти настройки изменить. Чтобы разблокировать настройки, нажмите изображение замка в нижней части вкладки настроек режима работы и введите имя и пароль администратора.

Настройка режима централизованной защиты

1. Обратитесь к администратору антивирусной сети компании или IT-провайдера за лицензией и параметрами подключения к серверу централизованной защиты.
2. В меню приложения откройте **Настройки** и выберите вкладку **Режим**.
3. Чтобы подключиться к антивирусной сети компании или услуге по антивирусной защите, предоставляемой вашим IT-провайдером, установите флажок **Включить режим централизованной защиты**.

   В режиме централизованной защиты антивирусная проверка вашего компьютера может быть запущена непосредственно с сервера вручную или по расписанию.

4. При включении централизованного режима восстанавливаются последние параметры подключения. Если вы подключаетесь к серверу впервые или параметры подключения изменились, выполните следующие действия:

   Настройки подключения к серверу централизованной антивирусной защиты содержатся в файле `install.cfg`, который предоставляется администратором антивирусной сети. Чтобы использовать файл:

   1. В окне Менеджер лицензий перейдите по ссылке **Другие виды активации**.
   2. В открывшееся окно перетащите файл с настройками или щелкните по пунктирной области, чтобы открыть диалог для выбора файла.

   После подключения файла поля для ввода параметров подключения к серверу будут заполнены автоматически.

   - Укажите IP-адрес сервера централизованной антивирусной защиты, предоставленный администратором антивирусной сети.
   - Укажите порт, использующийся для подключения к серверу.
   - Перетащите лицензионный ключевой файл, выданный администратором антивирусной сети, в окно настроек или дважды щелкните в области для лицензионного ключевого файла, чтобы указать его с помощью стандартного окна выбора файла.
   - Укажите дополнительные параметры для авторизации рабочей станции: идентификатор станции (присвоенный вашему компьютеру для регистрации на сервере) и пароль. Указанные значения параметров сохраняются с помощью функции Keychain. Таким образом, при повторном подключении к серверу не требуется вводить их заново.
   - Нажмите **Подключиться**, чтобы выполнить подключение к серверу централизованной защиты с заданными параметрами.

   В зависимости от настроек авторизации станций на сервере централизованной защиты подключение может осуществляться в следующих режимах:

- в качестве новой станции (новичка). В данном случае может потребоваться подтверждение станции на сервере (идентификатор станции и пароль для станции будут созданы автоматически), или же станция будет авторизована автоматически при соответствующих настройках доступа на сервере;
- если станция уже создана на сервере, т.е. для нее заданы идентификатор и пароль, то при подключении к серверу станция будет авторизована автоматически вне зависимости от настроек сервера.

С информацией о подключении станций к серверу антивирусной защиты можно ознакомиться в руководствах администратора Центра Управления Dr.Web и Dr.Web AV-Desk.

Настройка режима автономной работы

1. В меню приложения откройте **Настройки** и выберите вкладку **Режим**.
2. Чтобы перейти в режим автономной работы Dr.Web, снимите флажок **Включить режим централизованной защиты**.

   При включении режима автономной работы восстанавливаются все настройки приложения, установленные до перехода в централизованный режим, или настройки по умолчанию. Также возобновляется доступ ко всем функциональным возможностям Dr.Web.
3. Для работы в автономном режиме требуется действительный персональный ключевой файл. Лицензия, полученная автоматически с сервера централизованной защиты, в данном режиме использоваться не может. При необходимости активируйте персональную лицензию с помощью компонента Менеджер лицензий.

5.10. Восстановление настроек по умолчанию

Если у вас возникли трудности, связанные с использованием Dr.Web после изменения его настроек, вы можете восстановить настройки по умолчанию.

По умолчанию, опция восстановления настроек заблокирована, чтобы пользователи без прав администратора не могли ей воспользоваться. Чтобы разблокировать ее, нажмите изображение замка в нижней части вкладки настроек и введите имя и пароль администратора.

1. В меню приложения откройте **Настройки** и выберите вкладку **Основные**.
2. Нажмите кнопку **Настройки по умолчанию**. Подтвердите восстановление исходных настроек приложения, нажав кнопку **Восстановить** в соответствующем окне.

6. Приложения

6.1. Приложение А. Виды компьютерных угроз

Под термином «угроза» в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они могут нанести вред пользователю.

В продуктах и документации компании «Доктор Веб» угрозы принято разделять на два типа в соответствии с уровнем опасности:

- **значительные угрозы** – классические компьютерные угрозы, которые сами по себе способны выполнять различные деструктивные и незаконные действия в системе (удаление и кража важной информации, нарушение работы сети и т. д.). Этот тип компьютерных угроз состоит из программ, которые традиционно называют вредоносными (вирусы, черви и троянские программы);
- **незначительные угрозы** – компьютерные угрозы, которые считаются менее опасными по сравнению со значительными угрозами, но могут быть использованы третьими лицами для совершения вредоносных действий. Помимо этого, само присутствие незначительных угроз в системе является несомненным свидетельством низкого уровня ее защищенности. Специалисты в области информационной безопасности иногда называют этот тип компьютерных угроз «серым» программным обеспечением или потенциально нежелательными программами. К незначительным угрозам относятся рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

Значительные угрозы

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.

В компании «Доктор Веб» вирусы делят по типу файлов, которые они инфицируют:

- **файловые вирусы** инфицируют файлы операционной системы (обычно, исполняемые файлы и динамические библиотеки) и активизируются при обращении к зараженному файлу;
- **макро-вирусы** инфицируют файлы документов, используемые приложениями Microsoft® Office или другими программами, допускающими наличие макрокоманд, написанных, чаще всего на языке Visual Basic. Макрокоманды – это встроенные программы (макросы), написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в Microsoft® Word макросы могут запускаться при открытии, закрытии или сохранении документа);
- **скрипт-вирусы** пишутся на языках сценариев (скриптов) и в большинстве случаев заражают другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях;
- **загрузочные вирусы** заражают загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- **шифрованные вирусы** шифруют свой код при каждом новом заражении, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры;
- **полиморфные вирусы** используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на ассемблере, высокоуровневых языках программирования, языках сценариев и т. д.) и по поражаемым операционным системам.

Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании «Доктор Веб» червей делят по способу (среде) распространения:

- **сетевые черви** распространяются посредством различных сетевых протоколов и протоколов обмена файлами;
- **почтовые черви** распространяются посредством почтовых протоколов (POP3, SMTP и т. д.).

Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы производят какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т. д.), либо делают возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловые сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.

Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- **бэкдоры** – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы, они прописывают себя в реестре, модифицируя ключи;
- **дропперы** – это файлы-носители, которые содержат в своем теле вредоносные программы. При запуске дроппера он копирует на диск пользователя вредоносные файлы, не оповещая пользователя, и запускает их;
- **клавиатурные перехватчики** (кейлоггеры) используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т. д.);
- **кликеры** переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь

перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DoS-атак);

- **прокси-трояны** предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы;
- **руткиты** предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (User Mode Rootkits (UMR)), и руткиты, работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (Kernel Mode Rootkits (KMR)).

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Незначительные угрозы

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и

угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

Это специальные компьютерные программы, использующие доступ к сети Интернет с разрешения пользователя для того, чтобы попасть на определенные сайты. Обычно имеют подписанный сертификат и уведомляют о всех своих действиях.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-сервера и т. д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типом компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать в карантин, а также отправлять на анализ специалистам антивирусной лаборатории «Доктор Веб».

6.2. Приложение Б. Методы обнаружения угроз

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Методы обнаружения угроз

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он основан на поиске в содержимом анализируемого объекта сигнатур уже известных угроз. *Сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом

однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах Dr.Web составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing™

Это уникальная технология Dr.Web, которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы заражения или вредоносное поведение. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения Dr.Web, от таких угроз, как троянская программа-вымогатель Trojan.Encoder.18 (также известная под названием «gpcode»). Кроме того, использование технологии Origins Tracing позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing, добавляется постфикс `.Origin`.

Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и шифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* – программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (*буфером эмуляции*). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

Работа эвристического анализатора основывается на наборе *эвристик* (предположений, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного и, наоборот, безопасного исполняемого кода. Каждый признак кода имеет определенный вес (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует технологию FLY-CODE™ – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчикам продукта Dr.Web, но и новыми, ранее не исследованными программами. При проверке упакованных

объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».

Во время любой из проверок все компоненты антивирусных продуктов Dr.Web используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории «Доктор Веб» обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web, то она будет обнаружена в списке процессов и нейтрализована после получения обновленных вирусных баз.

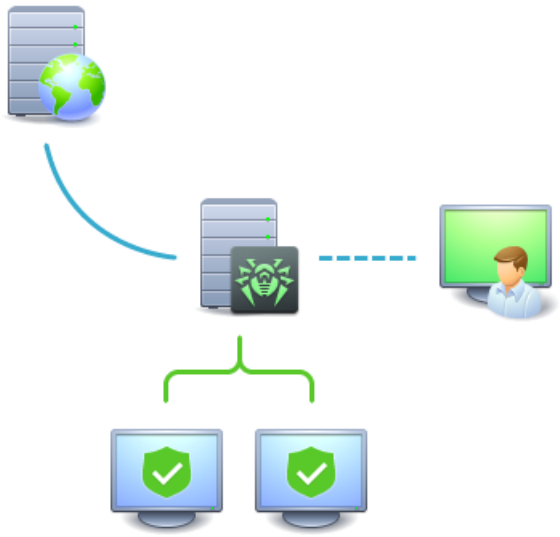
6.3. Приложение В. Централизованная антивирусная защита

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты позволяют автоматизировать и упростить настройку и управление информационной безопасностью компьютеров, объединенных в единую логическую структуру (например, компьютеры одной компании, расположенные как внутри локальной сети, так и вне ее). Защищаемые компьютеры объединяются в единую *антивирусную сеть*, безопасность которой контролируется и управляется администраторами с центрального сервера. Подключение к системам централизованной защиты позволяет получить гарантированно высокий уровень защиты компьютера при минимальных усилиях со стороны конечных пользователей.

Взаимодействие компонентов антивирусной сети

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру (см. иллюстрацию ниже).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз безопасности и спама локальными антивирусными *компонентами* (клиентами; в данном случае – Dr.Web для macOS), которые обеспечивают антивирусную защиту и упрощают соединение с сервером централизованной защиты.



	Сервер централизованной защиты		Сеть на основе TCP, NetBIOS
	Администратор антивирусной сети		Доступ через HTTP/HTTPS
	Защищенный локальный компьютер		Передача обновлений через HTTP
	Сервер обновлений компании «Доктор Веб»		

Рисунок 5. Логическая структура антивирусной сети

Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и антивирусным сервером может быть весьма значительным, поэтому предусматривается возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.

Все необходимые обновления загружаются на сервер централизованной защиты с серверов обновлений Dr.Web.

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется антивирусным сервером по указанию *администраторов антивирусной сети*. Администраторы управляют конфигурацией центрального сервера и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной

станции к сети), а также при необходимости задают настройки работы конкретных локальных антивирусных компонентов.

Локальные антивирусные компоненты несовместимы с антивирусным программным обеспечением как других компаний, так и антивирусными решениями Dr.Web, не поддерживающими режим централизованной защиты (например, Dr.Web версии 5.0). Установка двух антивирусных программ на одном компьютере может привести к отказу системы и потере важных данных.

Решения для централизованной защиты

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite представляет собой комплексное антивирусное решение для корпоративных сетей, которое обеспечивает надежную защиту как рабочих станций, так и файловых и почтовых серверов от любых видов компьютерных угроз на предприятиях любого масштаба. Данное решение также предоставляет разнообразный инструментарий для администраторов корпоративной сети, позволяющий отслеживать и управлять работой установленных антивирусных компонентов, включая развертывание, обновление вирусных баз Dr.Web и программных модулей компонентов, мониторинг состояния сети, извещения о вирусных событиях и сбор статистики.

Интернет-сервис Dr.Web AV-Desk

Dr.Web AV-Desk представляет собой инновационный сервис компании «Доктор Веб» для провайдеров различного рода интернет-услуг. С помощью этого интернет-сервиса провайдеры могут предоставлять своим пользователям (как частным лицам, так и компаниям) услуги по защите от вирусов, спама и прочих компьютерных угроз. Предоставление услуг осуществляется путем приобретения подписки на любой необходимый клиенту тарифный пакет и срок. Услуги предоставляются в режиме онлайн.

Подробную информацию об интернет-услуге Dr.Web AV-Desk можно получить на официальном сайте компании «Доктор Веб» по адресу https://www.av-desk.com/.

6.4. Приложение Г. Комбинации клавиш

Для запуска проверки, применения действий к обнаруженным угрозам, а также для настройки работы Dr.Web вы можете использовать специальные комбинации клавиш:

Комбинация		**Описание**
Меню проверок	CONTROL-COMMAND-E	Быстрая проверка
	CONTROL-COMMAND-F	Полная проверка
	CONTROL-COMMAND-C	Выбор объектов проверки
Меню действий	COMMAND-SHIFT-C	Лечить
	COMMAND-SHIFT-M	Переместить в карантин
	COMMAND-SHIFT-I	Игнорировать
	COMMAND-SHIFT-D	Удалить
	COMMAND-SHIFT-R	Восстановить
	COMMAND-SHIFT-P	Восстановить в
	COMMAND-SHIFT-A	Работать с правами администратора
Общие	COMMAND-,	Настройки
	COMMAND-A	Выделить все
	COMMAND-W	Закрыть

6.5. Приложение Д. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.