Dr.WEB

для macOS

Руководство пользователя

© «Доктор Веб», 2021. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах ООО «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web для macOS
Версия 12.0
Руководство пользователя
22.01.2021

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «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. Dr.Web для macOS

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 для macOS надежно защищает Mac от угроз любого типа: вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов, используя самые современные технологии обнаружения и обезвреживания вирусов.

Компоненты Dr.Web постоянно обновляются, а вирусные базы и базы категорий веб-ресурсов регулярно дополняются новыми сигнатурами угроз. Обновления обеспечивают актуальный уровень защиты устройств. Для обезвреживания неизвестных угроз используются методы эвристического анализа.

Основные функции

- постоянная проверка всех файлов на Mac;
- проверка системы по запросу пользователя;
- проверка данных, которые передаются по незащищенному протоколу HTTP;
- контроль подключений приложений к сети и блокировка подозрительных соединений;
- защита камеры и микрофона от несанкционированного доступа.

Информация о программе

Чтобы открыть окно с информацией о программе, в главном окне нажмите значок .

Информация о программе сгруппирована по пяти вкладкам:

- **О Dr.Web** — версия программы, дата последнего обновления, версия антивирусного ядра.
- **Справка** — справка по работе с Dr.Web для macOS.
- **Новости** — последние новости, которые публикуются на сайте компании «Доктор Веб».
- **Акции** — акции компании «Доктор Веб».
- **О вирусах** — новости о вирусах, которые обнаружили аналитики «Доктор Веб».

1.3. Системные требования

Чтобы установить Dr.Web необходимо:

- Mac под управлением операционной системы macOS.
- 2 ГБ свободного места диске.

Полный список поддерживаемых версий

- OS X 10.10 Yosemite,
- OS X 10.11 El Capitan,
- macOS 10.12 Sierra,
- macOS 10.13 High Sierra,
- macOS 10.14 Mojave,
- macOS 10.15 Catalina.

Как узнать версию операционной системы Mac

1. Перейдите в меню Apple .
2. Выберите **Об этом Mac**.
3. Номер версии указан на вкладке **Обзор** под названием операционной системы.

Как узнать, сколько свободного места на Mac

1. Перейдите в меню Apple .
2. Выберите **Об этом Mac**.
3. Затем перейдите на вкладку **Хранилище**. Вы увидите количество свободного места

на Mac.

4. Нажмите кнопку **Управлять**, чтобы посмотреть рекомендации для оптимизации хранилища.

2. Установка и удаление

Установка Dr.Web

1. Скачайте установочный файл с сайта https://download.drweb.com/mac/;
2. Запустите файл;
3. Нажмите **Установить Dr.Web**.
4. Нажмите **Далее**. Начнется процесс установки программы.
5. Введите пароль и нажмите кнопку **Установить вспомогательную программу**.
6. Dr.Web для macOS скопируется в папку **Программы** и запустится.

После завершения установки на верхней панели macOS появится значок  . Он открывает основное окно Dr.Web.

Во время первого запуска Dr.Web обновит вирусные базы до актуального состояния. В дальнейшем Dr.Web обновляет вирусные базы каждые 30 мин. Вы можете изменить частоту обновлений.

Ошибки при установке

Операционная система не поддерживается

Dr.Web можно установить только на Mac под управлением поддерживаемой версии операционной системы macOS. Обновите операционную систему.

Как узнать версию операционной системы Mac

1. Перейдите в меню Apple .
2. Выберите **Об этом Mac**.
3. Номер версии указан на вкладке **Обзор** под названием операционной системы.

Недостаточно памяти на диске

Чтобы установить Dr.Web, необходимо около 2 ГБ свободного места на диске.

Как узнать, сколько свободного места на Mac

1. Перейдите в меню Apple .

2. Выберите **Об этом Mac**.
3. Затем перейдите на вкладку **Хранилище**. Вы увидите количество свободного места на Mac.
4. Нажмите кнопку **Управлять**, чтобы посмотреть рекомендации для оптимизации хранилища.

Установлен другой антивирус

Dr.Web несовместим с другими антивирусными программами. Также невозможно установить две версии Dr.Web на один Mac.

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.

Информацию о том, как удалить сторонний антивирус см. в справочных материалах или на официальном сайте необходимого приложения.

Ошибка №

Обратитесь в техническую поддержку компании «Доктор Веб». Прикрепите к запросу журнал установки, который находится в папке `\Library\DrWeb`.

Список ошибок

Удаление Dr.Web

1. В **Finder** найдите программу **Удалить Dr.Web** и запустите ее.
2. Введите имя и пароль пользователя.
3. Dr.Web для macOS будет удален из папки **Программы**.

После удаления Dr.Web на Mac остаются ключевой и конфигурационный файлы и файл с настройками программы.

Не используйте сторонние приложения для удаления Dr.Web. Это может привести к неполному удалению программы.

Если программа не удалилась полностью, вы можете удалить ее вручную.

Чтобы удалить Dr.Web вручную

Последовательно введите следующие команды в **Терминал**:

- `sudo /bin/launchctl remove com.drweb.pro.configd`
- `sudo rm -f /Library/PrivilegedHelperTools/com.drweb.agent`
- `sudo rm -f /Library/LaunchDaemons/com.drweb.agent.plist`
- `sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove /Library/Application Support/DrWeb/bin/drweb-gated`
- `sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove /Library/Application Support/DrWeb/bin/drweb-firewall/bin/sleep`
- `sudo /sbin/kextunload -m com.drweb.kext.DrWebNetMonitor`
- `sudo /sbin/kextunload -m com.drweb.kext.DrWebMonitor`
- `sudo /bin/launchctl remove com.drweb.agent`
- `sudo rm -Rf "/Library/Application Support/DrWeb/lib"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/bin"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/cache"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/update"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/var"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/www"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/version"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/bases"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/dws"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/html"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/mail"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/install.plist"`
- `sudo rm -Rf /var/log/drweb-agent.log`

3. Управление лицензиями

Для работы Dr.Web требуется лицензия, которую можно купить на сайте компании «Доктор Веб» или у партнеров. Лицензия позволяет использовать все возможности программы на протяжении всего срока действия. Лицензия регулирует права пользователя в соответствии с Лицензионным соглашением, условия которого пользователь принимает во время установки программы.

Каждой лицензии сопоставлен уникальный серийный номер, а на компьютере хранится специальный файл с параметрами лицензии. Этот файл называется лицензионным ключевым файлом.

Если перед приобретением лицензии вы хотите ознакомиться с возможностями Dr.Web для macOS, вы можете активировать пробную версию. В пробной версии доступны все функции и компоненты защиты.

3.1. Пробная версия

Если перед покупкой лицензии вы хотите ознакомиться с возможностями Dr.Web для macOS, вы можете активировать пробную версию. Она обеспечивает полную функциональность основных компонентов, но срок ее действия ограничен.

> Вы можете активировать пробную версию на одном и том же компьютере только один раз в год.

Вы можете активировать пробную версию:

- На 1 месяц. Регистрация и серийный номер не требуются. Лицензия будет активирована автоматически.

Чтобы активировать пробную версию

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. В разделе **Активация лицензии** перейдите по ссылке **Получить пробную версию на 30 дней**.

3.2. Покупка лицензии

Если у вас нет действующей лицензии Dr.Web, вы можете купить новую лицензию на странице онлайн-магазина «Доктор Веб».

Чтобы купить новую лицензию

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Купить**. Откроется страница сайта компании «Доктор Веб», на которой вы можете продолжить покупку.

После завершения покупки на адрес, который вы указали при регистрации, придет письмо с серийный номером и ключевым файлом (во вложении).

3.3. Активация лицензии

Чтобы использовать все функции и компоненты программы, активируйте лицензию. Рекомендуем активировать лицензию сразу после установки программы. Это необходимо для обновления антивирусных баз и работы компонентов программы, например, постоянной защиты файловой системы, защиты от сетевых угроз и проверки веб-трафика.

Окно активации появляется автоматически, когда вы впервые запускаете Dr.Web. Вы можете запустить активацию позднее в разделе **Лицензия** главного окна программы. Активация лицензии возможна при помощи ключевого файла или серийного номера.

Как активировать лицензию с помощью серийного номера

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Активировать**.
3. В окне **Активация лицензии** введите серийный номер.
4. Нажмите кнопку **Активировать**.
5. В форме регистрации введите имя, регион и адрес почты. Эта информация понадобится, чтобы при необходимости восстановить лицензию. Нажмите кнопку **Зарегистрироваться**.
6. Если вы уже пользовались лицензионной версией Dr.Web не менее 3 месяцев, вы можете указать ее серийный номер, и срок действия новой лицензии будет продлен на 150 дней.
   - Нажмите **Указать**, если у вас есть серийный номер предыдущей лицензии. Введите номер и нажмите **Далее**.
   - Нажмите **Пропустить**, если у вас нет серийного номера предыдущей лицензии.

Как активировать лицензию с помощью ключевого файла

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Активировать**.

3. В окне **Активация лицензии** откройте вкладку **Файлы активации**.
4. Перетащите ключевой файл формата `.key` в пунктирную область или нажмите, чтобы выбрать файл на Mac.
5. В форме регистрации введите имя, регион и адрес почты. Эта информация понадобится, чтобы при необходимости восстановить лицензию. Нажмите кнопку **Зарегистрироваться**.
6. Если вы уже пользовались лицензионной версией Dr.Web не менее 3 месяцев, вы можете указать ее ключевой файл, и срок действия новой лицензии будет продлен на 150 дней.
   - Нажмите **Указать**, если у вас есть серийный номер предыдущей лицензии. Введите номер и нажмите **Далее**.
   - Нажмите **Пропустить**, если у вас нет серийного номера предыдущей лицензии.

Частые вопросы

Как я могу перенести лицензию на другой компьютер?

Вы можете перенести вашу лицензию на другой компьютер при помощи ключевого файла или серийного номера.

Чтобы перенести лицензию на другой компьютер

- при помощи серийного номера:
  1. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
  2. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию, с помощью серийного номера. Вы можете активировать лицензию во время установки или во время работы программы.
- при помощи ключевого файла:
  1. Скопируйте ключевой файл с компьютера, с которого вы хотите перенести лицензию. По умолчанию ключевой файл хранится в папке установки Dr.Web и имеет расширение `.key`.
  2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
  3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию, с помощью ключевого файла. Вы можете активировать лицензию во время установки или во время работы программы.

> Вы не можете перенести на другой компьютер лицензию, которую вы получили в рамках пробной версии программы.

Я забыл регистрационный email. Как я могу его восстановить?

Если вы забыли адрес почты, который вы указывали во время регистрации, обратитесь в техническую поддержку компании «Доктор Веб».

Если вы сделаете запрос с адреса, отличающегося от того, на который зарегистрирована ваша лицензия, специалист технической поддержки может попросить предоставить: фото- или скан-копию лицензионного сертификата, чек об оплате лицензии, письмо интернет-магазина и другие подтверждающие документы.

Как я могу изменить регистрационный email?

Если вы хотите изменить адрес почты, который вы указали при регистрации, воспользуйтесь специальным сервисом на сайте компании «Доктор Веб».

3.4. Продление лицензии

Вы можете продлить текущую лицензию в разделе **Активация лицензии**.

Как продлить лицензию, если срок действия еще не истек

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Купить**. Откроется страница сайта компании «Доктор Веб», на которой вы можете продолжить покупку.

Как продлить лицензию, если срок действия истек

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Купить**. Откроется страница сайта компании «Доктор Веб», на которой вы можете продолжить покупку.

Dr.Web поддерживает обновление на лету, при котором не требуется переустанавливать программу или прерывать ее работу. Чтобы обновить лицензию Dr.Web, активируйте новую лицензию.

Чтобы активировать лицензию

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Активировать**.
3. В окне **Активация лицензии**:
   - Введите серийный номер и нажмите кнопку **Активировать**.

- Если у вас есть ключевой файл, откройте вкладку **Файлы активации**. Перетащите файл в пунктирную область или нажмите, чтобы выбрать файл на Mac.

Подробная инструкция по активации лицензии доступна в разделе Активация лицензии.

Если срок действия лицензии, которую вы хотите продлить, закончился, Dr.Web начнет использовать новую лицензию.

Если срок действия лицензии, которую вы хотите продлить, еще не закончился, то количество оставшихся дней будет автоматически добавлено к новой лицензии. При этом предыдущая лицензия будет заблокирована. На адрес, который вы указали при регистрации, придет соответствующее уведомление.

3.5. Восстановление лицензии

Если ключевой файл утерян или поврежден, работа всех компонентов Dr.Web блокируется, и безопасность Mac может быть под угрозой. Чтобы повторно активировать лицензию, восстановите ключевой файл с помощью серийного номера.

Как восстановить ключевой файл

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите кнопку **Активировать**.
3. В окне **Активация лицензии** введите серийный номер и нажмите кнопку **Активировать**.

При повторной активации выдается тот же ключевой файл, который вы получали ранее.

Как восстановить серийный номер

Если вы не смогли найти серийный номер, вы можете восстановить его следующими способами:

- Обратитесь к продавцу лицензии (если вы купили не коробочную версию).
- Воспользуйтесь формой восстановления на сайте компании «Доктор Веб».
- Обратитесь в техническую поддержку компании «Доктор Веб». К запросу приложите подтверждение владения лицензий согласно этим правилам.

Вы можете повторно активировать лицензию при условии, что срок ее действия не истек.

Вы можете повторно активировать лицензию с одним и тем же серийным номером не более 25 раз. Если это число превышено, обратитесь в техническую поддержку компании «Доктор Веб». В запросе подробно опишите ситуацию, укажите персональные данные, введенные при регистрации, и серийный номер. Лицензионный ключевой файл будет выслан на адрес, который вы указали при регистрации.

3.6. Серийный номер

Каждой лицензии сопоставлен уникальный *серийный номер*. С его помощью вы можете активировать лицензию на Dr.Web.

Как узнать серийный номер

Если серийный номер не зарегистрирован

- Если вы купили лицензию в интернет-магазине, вы можете узнать серийный номер из письма интернет-магазина о покупке лицензии.
  - Если вы купили лицензию в интернет-магазине компании «Доктор Веб», вы можете узнать серийный номер в Персональном разделе на сайте Allsoft.ru в данных о заказе.
  - Если вы купили лицензию в интернет-магазине компании «Доктор Веб» через аккаунт на сайте и заявили вашу лицензию в программе лояльности, вы можете узнать серийный номер в сервисе Мои покупки.
- Если вы купили коробочную версию, серийный номер можно найти в Лицензионном сертификате, вложенном в коробку.
- Если вы купили лицензию в розничной сети (Евросеть, Связной, МВидео, Мегафон, МТС и т. д.), вы можете узнать серийный номер на кассовом чеке.

Если серийный номер зарегистрирован

- Если Dr.Web установлен на Mac, загрузите этот файл и откройте его. Дважды нажмите по файлу `YSN.cmd`. Будет создан текстовый файл `YourSerialNumber.txt`, который автоматически откроется в текстовом редакторе. Все серийные номера перечислены после приставки «SN=».
- Если Dr.Web не установлен, восстановите серийный номер с помощью формы на сайте компании «Доктор Веб».

Если вы используете Dr.Web на условиях подписки

В этом случае серийный номер или ключевой файл не нужен.

- Если вы купили подписку на сайте компании «Доктор Веб», вы можете узнать идентификатор (ID) подписки в разделе Мои подписки.

- Если вы купили подписку у стороннего поставщика, вы можете узнать ID подписки в личном кабинете на сайте вашего поставщика IT-услуг.

Как восстановить серийный номер

Если вы не смогли найти серийный номер, вы можете восстановить его следующими способами:

- Обратитесь к продавцу лицензии (если вы купили не коробочную версию).
- Воспользуйтесь формой восстановления на сайте компании «Доктор Веб».
- Обратитесь в техническую поддержку компании «Доктор Веб». К запросу приложите подтверждение владения лицензий согласно этим правилам.

3.7. Ключевой файл

Ключевой файл определяет тип лицензии и права пользователя на использование Dr.Web.

Лицензионный ключевой файл имеет расширение `.key`. Вы можете получить его во время активации лицензии.

Ключевой файл содержит информацию о:

- перечне компонентов, которые разрешено использовать пользователю;
- периоде, в течение которого разрешено использование Dr.Web;
- наличии или отсутствии технической поддержки;
- других ограничениях (в частности, количестве компьютеров, на которых разрешено использовать Dr.Web).

Ключевой файл должен находиться в папке установки Dr.Web. Программа регулярно проверяет наличие и корректность ключевого файла. Чтобы не нарушить целостность ключевого файла, не открывайте его в текстовых редакторах и не изменяйте его.

При отсутствии действительного ключевого файла активность всех компонентов Dr.Web блокируется.

Ключевой файл Dr.Web является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек,
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом Dr.Web перестает обезвреживать вредоносные программы.

Сохраняйте ключевой файл до конца срока действия лицензии или пробной версии. Если вы устанавливаете Dr.Web на несколько компьютеров или переустанавливаете его, вы можете использовать лицензионный ключевой файл, полученный при первой активации.

Ключевой файл, полученный для активации пробной версии, можно использовать только на том компьютере, на котором вы проходили регистрацию.

4. Панель управления

На вкладке **Панель управления** главного окна программы вы можете:

- настроить работу компонентов защиты,
- запустить проверку Mac на вирусы,
- задать параметры доступа к камере и микрофону,
- обновить вручную вирусные базы,
- узнать информацию о текущей лицензии,
- посмотреть информацию об обнаруженных угрозах.

Компоненты защиты

- SplDer Guard — монитор файловой системы. Проверяет в режиме реального времени все файлы, к которым обращаются пользователи, и контролирует программы и процессы, запущенные на Mac.
- SplDer Gate — интернет-монитор. Проверяет HTTP-трафик и контролирует доступ к интернет-ресурсам.
- Брандмауэр — сетевой экран. Защищает Mac от несанкционированного доступа извне и утечки важных данных по сети.

Проверить Mac

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). Вы можете вручную выбрать необходимое действие, либо задать автоматическое применение действия, указанного для этого типа угроз в настройках.

Защита приватности

- **Камера** — контроль доступа приложений к камере.
- **Микрофон** — контроль доступа приложений к микрофону.

Обновление

Выберите пункт **Обновление не требуется**/**Требуется обновление**, чтобы обновить вирусные базы вручную. В вирусных базах содержится информация обо всех известных вредоносных программах.

Лицензия

В разделе **Лицензия** собрана информация о текущей лицензии:

- статус лицензии,
- номер,
- имя владельца,
- дата активации,
- дата окончания срока действия,
- количество оставшихся дней.

Вы можете активировать лицензию, если у вас уже есть серийный номер, ключевой или конфигурационный файл, или купить новую лицензию.

Угрозы

- Угрозы — общий список обнаруженных угроз. Вы можете удалить, переместить в карантин или проигнорировать перечисленные угрозы.
- Карантин — специальная папка, которая используется для изоляции зараженных файлов и других угроз, чтобы они не могли нанести вред системе.

5. Уведомления

На вкладке **Уведомления** главного окна программы отображаются сообщения о событиях в работе Dr.Web:

- состоянии лицензии;
- обнаружении угроз, их обезвреживании;
- состоянии вирусных баз;
- возникновении ошибок в работе компонентов защиты;
- статусе соединения с сервером централизованной защиты;
- попытках подключения к микрофону или камере;
- сообщения от администратора сервера централизованной защиты.

Dr.Web использует системные уведомления macOS, чтобы показывать сообщения об обнаружении угроз, их обезвреживании или возникновении ошибок в работе компонентов. Вы можете отключить или настроить системные уведомления от Dr.Web.

Чтобы отключить уведомления

1. Перейдите в меню Apple > **Системные настройки**.
2. Выберите раздел **Уведомления**.
3. Слева в списке программ выберите Dr.Web для macOS и отключите уведомления с помощью переключателя .

> На версии macOS 10.14 и ниже данный переключатель отсутствует. Для отключения уведомлений, снимите все флажки.

Чтобы настроить системные уведомления

1. Перейдите в меню Apple > **Системные настройки**.
2. Выберите раздел **Уведомления**.
3. Слева в списке программ выберите Dr.Web для macOS. Настройте стиль напоминаний программы и соответствующие опции.

6. Обновление вирусных баз

В разделе **Модуль обновления** вы можете настроить частоту обновления вирусных баз. В вирусных базах содержится информация обо всех известных вредоносных программах.

Ежедневно появляются новые типы угроз с более совершенными маскировочными функциями. Обновление Dr.Web позволяет находить ранее неизвестные вирусы, блокировать их распространение, а в ряде случаев излечивать ранее неизлечимые зараженные файлы.

Чтобы Dr.Web мог обновлять вирусные базы, необходимо подключение к интернету.

Во время первого запуска Dr.Web обновляет вирусные базы до актуального состояния. В дальнейшем Dr.Web обновляет вирусные базы каждые 30 мин. Вы можете изменить частоту обновлений.

Чтобы изменить частоту обновления вирусных баз

1. В главном окне нажмите  .
2. В окне **Настройки** выберите раздел **Модуль обновления**.
3. В выпадающем списке **Обновлять вирусные базы** выберите частоту обновления.

Dr.Web будет обновляться автоматически согласно выбранной частоте загрузки обновлений.

Вы также можете запустить процесс обновления вручную.

Чтобы обновить вирусные базы вручную

- В главном окне выберите пункт **Обновление не требуется**/**Требуется обновление**.

Dr.Web проверит и обновит вирусные базы.

Настройка прокси-сервера

Если вы не хотите, чтобы обновления устанавливались на ваш Mac напрямую, вы можете настроить установку обновлений через прокси-сервер.

Чтобы настроить установку обновлений через прокси-сервер

1. В главном окне нажмите  .
2. В окне **Настройки** выберите раздел **Модуль обновления**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите  и введите имя пользователя и пароль.
4. Установите флажок **Использовать прокси-сервер**.
5. Нажмите **Настроить прокси**.
6. Укажите адрес и порт прокси-сервера.
7. Если для прокси-сервера требуется пароль, установите флажок **Защитить прокси-сервер паролем**.
8. Укажите имя пользователя и пароль.
9. Нажмите **Сохранить**.

7. Постоянная защита файловой системы

Монитор файловой системы SpIDer Guard в режиме реального времени проверяет все файлы, к которым обращаются пользователи, и контролирует программы и процессы, запущенные на Mac.

Вы можете исключить из постоянной проверки отдельные папки и файлы.

SpIDer Guard запускается автоматически после установки и активации лицензии Dr.Web. Монитор работает постоянно и запускается при включении Mac.

При обнаружении угроз SpIDer Guard выводит на экран сообщение и применяет действие, заданное в настройках. Вы можете изменить действия, которые автоматически применяются к различным типам угроз, или применять действия вручную.

Включение и отключение SpIDer Guard

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

Если постоянная антивирусная защита отключена, не следует подключаться к интернету, а также открывать файлы с носителей, не проверенных Сканером.

Чтобы временно приостановить или возобновить постоянную защиту файловой системы

1. На вкладке **Панель управления** главного окна выберите **Компоненты защиты**.
2. Включите или отключите монитор файловой системы SpIDer Guard при помощи переключателя  .

SpIDer Guard не работает / Заблокировано системное расширение

В macOS 10.13 и более поздних версиях блокируется загрузка системных расширений (модулей ядра). При этом компонент SpIDer Guard не работает, а на экране появляется сообщение о блокировке системного расширения. Чтобы проверка файловой системы на вашем Mac работала корректно, разрешите загрузку системного ПО от Doctor Web Ltd.

Чтобы разрешить загрузку системных расширений

1. Перейдите в меню Apple .

2. Выберите **Системные настройки**.
3. Перейдите в раздел **Защита и безопасность**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.
5. Нажмите кнопку **Разрешить** рядом с сообщением о блокировке системного ПО от Doctor Web Ltd.

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

7.1. Настройка файлового монитора SpIDer Guard

В разделе настроек **SpIDer Guard** вы можете задать действия, которые Dr.Web будет автоматически применять к угрозам в зависимости от их типа.

SpIDer Guard стремится вылечить инфицированные файлы: объекты, зараженные известным и потенциально излечимыми вирусами. Подозрительные объекты и различные типы вредоносных программ SpIDer Guard перемещает в Карантин.

Вы можете изменить действия, которые SpIDer Guard применяет к каждому типу вредоносных объектов. Выбор доступных действий зависит от типа угрозы:

Действие	Описание
Лечить, перемещать в карантин неизлечимые	Восстанавливает состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри архивов, почтовых файлов или файловых контейнеров.
Лечить, удалять неизлечимые	Восстанавливает состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри архивов, почтовых файлов или файловых контейнеров.
Удалить	Удаляет объект. Для загрузочных секторов никаких действий производиться не будет.
Перемещать в карантин	Изолирует объект в специальной папке Карантин. Позволяет предотвратить случайную потерю ценных данных.

Действие	Описание
	Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропускает объект без выполнения каких-либо действий и оповещений. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

Не следует без необходимости изменять предустановленные настройки автоматических действий.

Чтобы настроить автоматические действия

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **SplDer Guard**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. При необходимости поменяйте автоматические действия для перечисленных типов угроз.

Дополнительные настройки

Вы можете дополнительно настроить SplDer Guard и включить проверку архивов и почтовых файлов и задать максимальное время проверки одного объекта.

Изменение этих настроек может привести к замедлению работы Mac и увеличить общее время проверки.

Чтобы включить проверку архивов и почтовых файлов

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **SplDer Guard**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. Нажмите кнопку **Дополнительно**.
5. Включите опции **Архивы**, **Почтовые файлы**.
6. Нажмите **Сохранить**.

Чтобы задать максимальное время проверки одного объекта

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **SpIDer Guard**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. Нажмите кнопку **Дополнительно**.
5. Включите опцию **Максимальное время проверки одного объекта**.
6. Задайте максимальное время проверки одного объекта в секундах.
7. Нажмите **Сохранить**.

7.2. Исключение файлов и папок из проверки

Вы можете исключить из постоянной проверки отдельные папки и файлы.

Чтобы исключить из проверки файлы и папки

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Исключения**.
3. Перейдите на вкладку **Файлы и папки**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите кнопку и укажите нужную папку или отдельный файл или перетащите его в список.
6. Нажмите **Сохранить**. Теперь SpIDer Guard не будет проверять этот файл.

Если вы хотите временно отменить исключение объекта из проверки, но оставить его в списке, отключите опцию **SpIDer Guard** справа от объекта.

- Чтобы удалить объект из списка исключений, выделите его в списке и нажмите или перетащите за границы окна программы.
- Чтобы очистить список исключений, выделите все элементы в списке (COMMAND-A) и нажмите .

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.

8. Проверка веб-трафика

При каждом подключении к интернету браузеры, менеджеры загрузок и другие приложения обмениваются данными с сервером определенного сайта. При этом данные передаются по незащищенному протоколу HTTP. Интернет-монитор SpIDer Gate проверяет трафик и блокирует передачу объектов, которые могут угрожать безопасности Mac.

SpIDer Gate также поддерживает проверку данных, которые передаются по защищенному протоколу HTTPS. Чтобы настроить проверку зашифрованного трафика, включите соответствующую опцию в разделе Сеть.

SpIDer Gate запускается автоматически после установки и активации лицензии Dr.Web. Монитор работает постоянно и запускается при включении Mac.

SpIDer Gate ограничивает доступ к нерекомендуемым сайтам и страницам, которые содержат материалы, нарушающие законодательство об авторских правах. Вы можете изменить эти опции, а также задать настройки доступа к отдельным сайтам и категориям интернет-ресурсов.

Вы можете исключить из проверки веб-трафика отдельные сайты и сетевые соединения указанных приложений.

Включение и отключение SpIDer Gate

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

Чтобы временно приостановить или возобновить проверку веб-трафика

1. На вкладке **Панель управления** главного окна выберите **Компоненты защиты**.
2. Включите или отключите SpIDer Gate при помощи переключателя  .

SpIDer Gate не работает / Заблокировано системное расширение

В macOS 10.13 и более поздних версиях блокируется загрузка системных расширений (модулей ядра). При этом компонент SpIDer Gate не работает, а на экране появляется сообщение о блокировке системного расширения. Чтобы проверка веб-трафика на вашем Mac работала корректно, разрешите загрузку системного ПО от Doctor Web Ltd.

Чтобы разрешить загрузку системных расширений

1. Перейдите в меню Apple .
2. Выберите **Системные настройки**.
3. Перейдите в раздел **Защита и безопасность**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите кнопку **Разрешить** рядом с сообщением о блокировке системного ПО от Doctor Web Ltd.

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

8.1. Настройка интернет-монитора SpIDer Gate

В разделе настроек **SpIDer Gate** вы можете задать параметры проверки сетевых угроз и доступа к интернет-ресурсам.

SpIDer Gate ограничивает доступ к нерекомендуемым сайтам и страницам, которые содержат материалы, нарушающие законодательство об авторских правах. Также SpIDer Gate блокирует подозрительные, рекламные программы и программы дозвона.

Вы можете настроить проверку веб-угроз, создать правила доступа к отдельным страницам и выбрать дополнительные категории сайтов, доступ к которым будет ограничен.

> Не следует без необходимости изменять предустановленные настройки.

Проверка угроз

На вкладке **Проверка угроз** вы можете задать параметры проверки веб-угроз, настроить блокировку вредоносных программ по типам и указать максимальное время проверки одного объекта.

SpIDer Gate ограничивает доступ к нерекомендуемым сайтам и URL, добавленным по обращению правообладателей. Какие сайты Dr.Web считает нерекомендуемыми?

Вы можете снять ограничения на посещение этих сайтов.

Чтобы снять ограничения

1. В главном окне нажмите  .
2. В окне **Настройки** выберите раздел **SplDer Gate**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.
4. На вкладке **Проверка угроз** отключите опции **Блокировать URL, добавленные по обращению правообладателей**, **Блокировать нерекомендуемые сайты**, **Блокировать непроверенные объекты**.

По умолчанию, Dr.Web пропускает объекты, проверка которых не удалась. Вы можете включить блокировку непроверенных объектов.

Чтобы включить блокировку непроверенных объектов

1. В главном окне нажмите  .
2. В окне **Настройки** выберите раздел **SplDer Gate**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.
4. На вкладке **Проверка угроз** включите опцию **Блокировать непроверенные объекты**.

По умолчанию SplDer Gate блокирует подозрительные, рекламные программы и программы дозвона. Вы можете настроить блокировку типов вредоносных программ.

Чтобы настроить блокировку вредоносных программ

1. В главном окне нажмите  .
2. В окне **Настройки** выберите раздел **SplDer Gate**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.
4. На вкладке **Проверка угроз** выберите типы вредоносных программ, передачу которых вы хотите блокировать.

Вы можете задать максимальное время проверки одного объекта.

Увеличение максимального времени проверки одного объекта может привести к замедлению работы вашего Mac.

Чтобы задать максимальное время проверки одного объекта

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **SpIDer Gate**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. На вкладке **Проверка угроз** в опции **Максимальное время проверки одного объекта** задайте максимальное время проверки одного объекта в секундах.

Доступ к сайтам

На вкладке **Доступ к сайтам** вы можете задать правила доступа к отдельным страницам и выбрать категории сайтов, доступ к которым будет временно ограничен.

Вы можете выбрать категории сайтов, доступ к которым будет временно ограничен независимо от других настроек SpIDer Gate.

Чтобы ограничить доступ к категориям сайтов

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **SpIDer Gate**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. На вкладке **Доступ к сайтам** выберите категории сайтов, доступ к которым будет ограничен:

Категория	Описание
Сайты для взрослых	Сайты, содержащие материалы порнографического или эротического содержания, сайты знакомств и т. д.
Насилие	Сайты, содержащие призывы к насилию, материалы о различных происшествиях с человеческими жертвами и т. д.
Оружие	Сайты, посвященные оружию и взрывчатым веществам, а также материалы с описанием их изготовления и т. д.
Азартные игры	Сайты, на которых размещены онлайн-игры на деньги, интернет-казино, аукционы, а также принимающие ставки и т. д.
Наркотики	Сайты, пропагандирующие употребление, изготовление или распространение наркотиков и т. д.

Терроризм	Сайты, содержащие материалы агрессивно-агитационного характера, описания терактов и т. д.
Нецензурная лексика	Сайты, на которых содержится нецензурная лексика (в названиях разделов, статьях и пр.).
Чаты	Сайты для обмена сообщениями в режиме реального времени.
Почта	Сайты, предоставляющие возможность бесплатной регистрации почтового ящика.
Социальные сети	Социальные сети общего характера, деловые, корпоративные и тематические социальные сети, а также тематические сайты знакомств.

Вы можете указать сайты, доступ к которым будет временно ограничен независимо от других настроек SpIDer Gate.

Чтобы ограничить доступ к отдельному сайту

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **SpIDer Gate**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. На вкладке **Доступ к сайтам** нажмите внизу таблицы и введите адрес сайта.

8.2. Исключение сайтов из проверки

Вы можете исключить из проверки веб-трафика отдельные сайты. Доступ к этим сайтам будет разрешен независимо от настроек интернет-монитора SpIDer Gate.

Чтобы разрешить доступ к определенному сайту

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Исключения**.
3. Перейдите на вкладку **Сайты**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите внизу таблицы и введите адрес сайта.

- Чтобы удалить объект из списка исключений, выделите его в списке и нажмите или перетащите за границы окна программы.

- Чтобы очистить список исключений, выделите все элементы в списке (COMMAND-A) и нажмите −.

8.3. Проверка зашифрованного трафика

При каждом подключении к интернету Mac обменивается данными с сервером определенного сайта. Все больше веб-сервисов переходят на защищенные соединения: обмен информацией происходит по протоколу HTTPS. Защиту при этом обеспечивает криптографический протокол SSL/TLS, который поддерживает шифрование данных.

По умолчанию Dr.Web не проверяет зашифрованный трафик.

Чтобы включить проверку зашифрованного трафика

1. В главном окне нажмите ⚙.
2. В окне **Настройки** выберите раздел **Сеть**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите 🔒 внизу окна и введите имя пользователя и пароль.
4. Выберите **Проверять зашифрованный трафик**.

Чтобы Dr.Web мог проверять зашифрованный трафик, цифровой сертификат сайта, с которым устанавливается соединение, заменяется на сертификат безопасности компании «Доктор Веб».

Что такое сертификат безопасности

Сертификат безопасности — электронный документ, который подтверждает, что программа прошла проверку в одном из центров сертификации.

Сертификат безопасности гарантирует, что связь проходит в защищённом режиме с проверкой подлинности владельца сертификата.

При установке Dr.Web для macOS сертификат безопасности компании «Доктор Веб» автоматически импортируется в список системных сертификатов. Однако некоторые приложения, например браузеры (Opera, Firefox) и почтовые клиенты (Mozilla Thunderbird, The Bat!), не обращаются к системному хранилищу сертификатов.

Для таких приложений вы можете экспортировать сертификат компании «Доктор Веб» вручную, а затем установить (импортировать) его в нужное приложение.

Чтобы экспортировать сертификат «Доктор Веб»

1. В главном окне нажмите ⚙.

2. В окне **Настройки** выберите раздел **Сеть**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите и введите имя пользователя и пароль.
4. Нажмите кнопку **Экспортировать**.
5. Выберите папку, в которую вы хотите сохранить сертификат. Нажмите **Сохранить**.
6. Импортируйте сертификат в нужное приложение. Подробнее о том, как импортировать сертификат, см. в справочных материалах к необходимому приложению.

> Если после включения опции **Проверять зашифрованный трафик** вы столкнулись с проблемами в работе клиентов облачных хранилищ (например, Google Drive, Dropbox, Яндекс.Диск), исключите эти приложения из проверки.

8.4. Исключение приложений из проверки

Вы можете исключить из проверки веб-трафика сетевые соединения указанных приложений. Соединения для этих приложений будут разрешены независимо от настроек интернет-монитора SpIDer Gate.

Чтобы исключить из проверки сетевые соединения приложений

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Исключения**.
3. Перейдите на вкладку **Приложения**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите и укажите нужное приложение или перетащите его в список.

- Чтобы удалить объект из списка исключений, выделите его в списке и нажмите или перетащите за границы окна программы.
- Чтобы очистить список исключений, выделите все элементы в списке (COMMAND-A) и нажмите .

9. Защита от сетевых угроз

Брандмауэр защищает Mac от несанкционированного доступа извне и предотвращает утечку важных данных. Он позволяет контролировать подключения приложений к интернету и передачу данных по сети и блокирует подозрительные соединения.

Брандмауэр запускается автоматически после установки и активации лицензии Dr.Web. Компонент работает постоянно и запускается при включении Mac.

Брандмауэр контролирует весь входящий и исходящий трафик и принимает решение о блокировке или доступе приложений к сетевым ресурсам согласно выбранному режиму работы и отдельным правилам фильтрации.

Включение и отключение Брандмауэра

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

Чтобы временно приостановить или возобновить защиту от сетевых угроз

1. На вкладке **Панель управления** главного окна выберите **Компоненты защиты**.
2. Включите или отключите Брандмауэр при помощи переключателя  .

Брандмауэр не работает / Заблокировано системное расширение

В macOS 10.13 и более поздних версиях блокируется загрузка системных расширений (модулей ядра). При этом Брандмауэр не работает, а на экране появляется сообщение о блокировке системного расширения. Чтобы защита от сетевых угроз на вашем Mac работала корректно, разрешите загрузку системного ПО от Doctor Web Ltd.

Чтобы разрешить загрузку системных расширений

1. Перейдите в меню Apple .
2. Выберите **Системные настройки**.
3. Перейдите в раздел **Защита и безопасность**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.
5. Нажмите кнопку **Разрешить** рядом с сообщением о блокировке системного ПО от Doctor Web Ltd.

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

Брандмауэр заблокировал доступ в интернет

Если приложение, например браузер, не может получить доступ к интернету, создайте для него разрешающее правило в настройках Брандмауэра.

9.1. Настройка Брандмауэра

В разделе настроек **Брандмауэр** вы можете задать параметры проверки входящего и исходящего трафика и настроить доступ отдельных приложений к интернет-ресурсам.

Брандмауэр разрешает доступ к сетевым ресурсам для всех доверенных приложений. Если приложение не входит в список доверенных, Dr.Web показывает уведомление и спрашивает, какое действие нужно применить.

Какие приложения Dr.Web считает доверенными?

К доверенным приложениям относятся системные приложения macOS, приложения, у которых есть сертификат безопасности или действительная цифровая подпись. Правила для таких приложений не отображаются в списке правил фильтрации.

Вы можете изменить режим работы Брандмауэра и задать правила фильтрации для отдельных приложений, которые не распространяются на выбранный режим работы.

Режим работы

Выберите один из следующих режимов работы:

- **Разрешать доверенные приложения** — доступ к сетевым ресурсам для всех доверенных приложений разрешен (используется по умолчанию). Для остальных приложений Dr.Web показывает уведомление и спрашивает, какое действие нужно применить.
- **Разрешить все соединения** — доступ к сетевым ресурсам для всех неизвестных приложений разрешен. Известные соединения обрабатываются Брандмауэром согласно заданным правилам фильтрации.
- **Блокировать все соединения** — доступ к сетевым ресурсам для всех неизвестных приложений заблокирован. Известные соединения обрабатываются Брандмауэром согласно заданным правилам фильтрации.

Чтобы изменить режим работы Брандмауэра

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Брандмауэр**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. В верхней части окна в выпадающем списке **Режим** выберите необходимый режим работы.

Правила фильтрации

Вы можете создать правила фильтрации для отдельных приложения. Заданные правила действуют вне зависимости от выбранный режим работы Брандмауэра.

Правило фильтрации состоит из:

- файла приложения формата `.app`;
- действия: разрешать или блокировать соединение;
- номера порта, по которому идет соединение;
- IP-адреса, имени хоста сайта или сервера, доступ к которому будет контролировать Брандмауэр.

Чтобы создать новое правило

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Брандмауэр**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. Нажмите внизу таблицы. Откроется окно создания нового правила.
5. В поле **Выберите приложение** нажмите .
6. Выберите, будет ли правило относится ко всем приложениям или укажите приложение на Mac.
7. Выберите из выпадающего списка действие: **Блокировать** или **Разрешить**.
8. Укажите номер порта, по которому идет соединение.

Если вы оставите поле **Порт** пустым, то правило будет относится ко всем портам.

Исключение: если вы хотите создать правило для всех приложений, номер порта нужно указать обязательно.

9. В выпадающем списке **Соединение** выберите:
   - **Любой сервер**, если хотите настроить доступ ко всем серверам и по всем IP-адресам.

     Если вы хотите создать правило для всех портов, IP-адрес или хост нужно указать обязательно.

   - **IP-адрес**, если хотите настроить доступ к определенному IP-адресу. Введите адрес в формате IPv4: `192.0.2.235`.
   - **Хост**, если хотите настроить доступ к определенному хосту. Введите хост сайта или сервера в формате `example.com`.
10. Нажмите кнопку **Создать**.

Чтобы отредактировать правило

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Брандмауэр**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. В таблице с правилами фильтрации дважды нажмите нужное правило. Откроется окно редактирования правила.

   Если для одного приложения создано несколько правил, нажмите значок , чтобы раскрыть список.

5. Измените необходимые параметры правила.
6. Нажмите **Сохранить**.

10. Проверка Mac по требованию

Сканер Dr.Web проверяет объекты файловой системы по запросу пользователя и обнаруживает угрозы, скрывающие свое присутствие в системе. Для надежной защиты вашего Mac необходимо время от времени запускать проверку системы с помощью Dr.Web.

Вы можете исключить из проверки по требованию отдельные папки и файлы.

> Когда Mac переходит на питание от аккумулятора, проверка приостанавливается, чтобы предотвратить быстрый расход заряда батареи. При этом Dr.Web предлагает вам решить, продолжать проверку или нет. При переходе на питание от сети проверка будет продолжена автоматически.

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

Типы проверок

Режим проверки	Описание
Быстрая проверка	В этом режиме проверяются: • загрузочные сектора всех дисков; • оперативная память; • корневая папка загрузочного диска; • системная папка; • папка текущего пользователя; • временные файлы; • точки восстановления системы; • наличие руткитов (если процесс проверки запущен от имени администратора). ⚠ Архивы и почтовые файлы в этом режиме не проверяются.
Полная проверка	Полная проверка оперативной памяти и всех жестких дисков (включая загрузочные секторы), а также проверка на наличие руткитов.
Выборочная проверка	Проверка любых файлов и папок, указанных пользователем.

Чтобы запустить быструю проверку

1. На вкладке **Панель управления** главного окна выберите **Проверить Mac**.
2. Нажмите **Быстрая проверка**.

Чтобы запустить полную проверку

1. На вкладке **Панель управления** главного окна выберите **Проверить Mac**.
2. Нажмите **Полная проверка**.

Чтобы запустить проверку отдельных файлов и папок

1. На вкладке **Панель управления** главного окна выберите **Проверить Mac**.
2. Перетащите файлы и папки в пунктирную область или нажмите, чтобы выбрать файл или папку, которые вы хотите проверить. Или перетащите файлы и папки на значок Dr.Web в меню состояния.
3. Нажмите кнопку **Проверить**.

Чтобы запустить проверку отдельных файлов и папок из контекстного меню

1. Выделите нужный файл или папку на рабочем столе или в Finder.
2. Вызовите контекстное меню и нажмите **Проверить с Dr.Web**.

Результаты проверки

Окно с результатами проверки становится доступно, если

- вы прервали проверку (нажали кнопку **Стоп**),
- Dr.Web завершил проверку Mac.

На окне с результатами проверки указывается:

- количество проверенных объектов,
- количество пропущенных объектов,
- количество обнаруженных угроз,
- количество нейтрализованных угроз.

При обнаружении угроз Сканер применяет действия, заданные в настройках. Вы можете изменить действия, которые автоматически применяются к различным типам угроз, или применять действия вручную.

Чтобы посмотреть подробную информацию об угрозах

- На окне с результатами проверки нажмите кнопку **Подробнее**. Откроется вкладка **Подробности проверки**.

На вкладке **Подробности проверки** вы можете посмотреть подробную информацию об угрозах, которые Dr.Web обнаружил во время последней проверки.

Почему некоторые объекты пропущены

Причина	Решение
Не хватает прав, чтобы выполнить действие над объектом.	Запустите проверку от имени администратора.
Размер файла слишком большой.	Увеличьте максимальное время проверки одного объекта в настройках Сканера. Запустите проверку снова.
Файл поврежден или защищен паролем.	Если это архив, распакуйте его. Запустите проверку снова.
В списке пропущенных объектов есть архивы.	В настройках Сканера включите опцию **Архивы** или распакуйте архивы. Запустите проверку снова.
В списке пропущенных объектов есть почтовые файлы.	В настройках Сканера включите опцию **Почтовые файлы**. Запустите проверку снова.

Проверка с правами администратора

Чтобы выполнять действия над некоторыми вредоносными объектами, Dr.Web могут потребоваться права администратора.

Чтобы запустить проверку от имени администратора

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Сканер**.
3. Нажмите кнопку **Дополнительно**.

4. Выберите **Запускать проверку от имени администратора**.
5. Запустите проверку снова.

10.1. Настройка Сканера

В разделе настроек **Сканер** вы можете задать действия, которые Dr.Web будет применять к угрозам в зависимости от их типа.

Сканер стремится вылечить инфицированные файлы: объекты, зараженные известными и потенциально излечимыми вирусами. Подозрительные объекты и различные типы вредоносных программ Сканер перемещает в Карантин.

Вы можете изменить действия, которые Сканер применяет к вредоносным объектам. Выбор доступных действий зависит от типа угрозы:

Действие	Описание
Лечить, перемещать в карантин неизлечимые	Восстанавливает состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри архивов, почтовых файлов или файловых контейнеров.
Лечить, удалять неизлечимые	Восстанавливает состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри архивов, почтовых файлов или файловых контейнеров.
Удалить	Удаляет объект. Для загрузочных секторов никаких действий производиться не будет.
Перемещать в карантин	Изолирует объект в специальной папке Карантин. Позволяет предотвратить случайную потерю ценных данных. Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропускает объект без выполнения каких-либо действий и оповещений. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

Чтобы изменить настройки Сканера, не нужно вводить имя пользователя и пароль. Настройки изменятся для всех пользователей Mac автоматически.

Не следует без необходимости изменять предустановленные настройки автоматических действий.

Чтобы настроить автоматические действия

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Сканер**.
3. Включите опцию **Применять действия к угрозам автоматически**.
4. При необходимости поменяйте автоматические действия для перечисленных типов угроз.

Дополнительные настройки

Проверка с правами администратора

Чтобы выполнять действия над некоторыми вредоносными объектами, Dr.Web могут потребоваться права администратора.

Чтобы запускать проверку от имени администратора

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Сканер**.
3. Нажмите кнопку **Дополнительно**.
4. Выберите **Запускать проверку от имени администратора**.

Теперь перед каждой проверкой Mac будет запрашивать имя пользователя и пароль.

Вы можете дополнительно настроить проверку файлов по требованию и включить проверку архивов и почтовых файлов и задать максимальное время проверки одного объекта.

Изменение этих настроек может привести к замедлению работы Mac и увеличить общее время проверки.

Чтобы включить проверку архивов и почтовых файлов

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Сканер**.
3. Нажмите кнопку **Дополнительно**.
4. Включите опции **Архивы**, **Почтовые файлы**.
5. Нажмите **Сохранить**.

Архивы и почтовые файлы не проверяются в режиме **Быстрая проверка**.

Чтобы задать максимальное время проверки одного объекта

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Сканер**.
3. Нажмите кнопку **Дополнительно**.
4. Включите опцию **Максимальное время проверки одного объекта**.
5. Задайте максимальное время проверки одного объекта в секундах.
6. Нажмите **Сохранить**.

Экономия заряда батареи Mac

Когда Mac переходит на питание от аккумулятора, проверка приостанавливается, чтобы предотвратить быстрый расход заряда батареи. При этом Dr.Web предлагает вам решить, продолжать проверку или нет. При переходе на питание от сети проверка будет продолжена автоматически.

Вы можете отключить опцию приостановки проверки при переходе на питание от аккумулятора.

Чтобы настроить проверку при питании от аккумулятора

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Сканер**.
3. Нажмите кнопку **Дополнительно**.
4. Отключите (или включите) опцию **Приостанавливать проверку при питании от батареи**.
5. Нажмите **Сохранить**.

10.2. Исключение файлов и папок из проверки

Вы можете исключить из проверки по требованию отдельные папки и файлы.

Чтобы исключить из проверки файлы и папки

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Исключения**.
3. Перейдите на вкладку **Файлы и папки**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите кнопку и укажите нужную папку или отдельный файл или перетащите его в список.
6. Нажмите **Сохранить**. Теперь Сканер не будет проверять этот файл, если вы запустите проверку по требованию.

> Если вы хотите временно отменить исключение объекта из проверки, но оставить его в списке, отключите опцию **Сканер** справа от объекта.

- Чтобы удалить объект из списка исключений, выделите его в списке и нажмите или перетащите за границы окна программы.
- Чтобы очистить список исключений, выделите все элементы в списке (COMMAND-A) и нажмите .

> 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.

11. Защита приватности

Dr.Web защищает конфиденциальность вашей частной жизни, контролируя доступ приложений к камере и микрофону на вашем Mac.

По умолчанию доступ к камере и микрофону разрешен для любых приложений. Вы можете включить контроль доступа к камере и микрофону.

Настройки контроля доступа к камере и микрофону отсутствуют на версии macOS 10.14 и выше.

Чтобы включить контроль доступа к камере и микрофону

1. На вкладке **Панель управления** главного окна выберите **Защита приватности**.
2. Включите защиту доступа к камере или микрофону при помощи переключателя  .

Каждый раз, когда приложение пытается получить доступ к камере или микрофону, Dr.Web показывает уведомление и спрашивает, какое действие нужно применить:

- **Блокировать** — запретить приложению доступ к камере или микрофону. При этом доступ блокируется один раз. При повторной попытке доступа, например если приложение будет закрыто и запущено снова, Dr.Web снова покажет уведомление.
- **Разрешить** — разрешить приложению доступ к камере или микрофону.

  Пользователям из группы Администраторы доступны дополнительные варианты контроля доступа:

  - **Разрешить один раз** — разрешить приложению доступ к камере или микрофону только один раз.
  - **Разрешать всегда** — всегда разрешать приложению доступ к камере или микрофону.

  Если вы выберите вариант **Разрешать всегда**, Dr.Web создаст отдельное правило для этого приложения в списке исключений.

Чтобы создать правило в списке исключений, требуются права администратора.

11.1. Разрешить доступ к камере и микрофону

Вы можете разрешить отдельным приложениям доступ к камере и микрофону.

Настройки доступа к камере и микрофону отсутствуют на версии macOS 10.14 и выше.

Чтобы разрешить доступ к камере или микрофону

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Исключения**.
3. Перейдите на вкладку **Камера и микрофон**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите внизу списка **Камера** или **Микрофон** и укажите необходимое приложение или перетащите его в соответствующий список.

- Чтобы удалить объект из списка исключений, выделите его в списке и нажмите или перетащите за границы окна программы.
- Чтобы очистить список исключений, выделите все элементы в списке (COMMAND-A) и нажмите .

12. Обезвреживание угроз

12.1. Угрозы

В разделе **Угрозы** вы можете посмотреть общий список угроз и применить к ним необходимые действия. Чтобы обезвредить угрозы, настройте автоматические действия или примените действия к обнаруженным угрозам вручную.

Чтобы посмотреть информацию об угрозах

1. На вкладке **Панель управления** главного окна нажмите **Угрозы**.

   На вкладке **Угрозы** указаны все обнаруженные угрозы.

   В строке состояния в нижней части окна показывается общее количество угроз и их суммарный размер, а также количество и размер выделенных объектов.
2. Чтобы просмотреть информацию об угрозе, нажмите соответствующее поле.
3. При необходимости вы можете примените действие к угрозе. Для этого из выпадающего списка внизу окна выберите:
   - **Удалить** — навсегда удалить объект из файловой системы;
   - **Перемещать в карантин** — поместить объект в карантин;
   - **Игнорировать** — не применять никаких действий.

Чтобы применить действие к угрозе

1. На вкладке **Панель управления** главного окна нажмите **Угрозы**.
2. Выберите для соответствующей угрозы действие из выпадающего списка:
   - **Удалить** — навсегда удалить объект из файловой системы;
   - **Перемещать в карантин** — поместить объект в карантин;
   - **Игнорировать** — не применять никаких действий.
3. Чтобы обезвредить все обнаруженные угрозы, нажмите кнопку **Обезвредить все**. К угрозам будут применены действия, указанные в настройках программы для соответствующих типов угроз.

Если в списке угроз есть архивы, действие применяется ко всему архиву в целом.

Если вы хотите применить действие к отдельному файлу, распакуйте архив и запустите проверку еще раз.

Чтобы применить действие к нескольким угрозам

1. Выделите несколько угроз с помощью клавиши SHIFT.
2. Используйте специальные комбинации клавиш:
   - COMMAND-SHIFT-D — чтобы удалить угрозы;
   - COMMAND-SHIFT-M — чтобы поместить угрозы в карантин.

12.2. Карантин

В разделе **Карантин** вы можете посмотреть информацию и применить действие к объектам, которые были перемещены в карантин. Карантин — специальная папка, которая позволяет изолировать обнаруженные угрозы от остальной системы в том случае, если объект вам нужен и его не удается вылечить.

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.

Чтобы посмотреть информацию об объектах в карантине

1. На вкладке **Панель управления** главного окна нажмите **Угрозы**.
2. Откройте вкладку **Карантин**.
3. Чтобы просмотреть информацию об объекте в карантине, дважды нажмите соответствующее поле.

Чтобы применить действие к объекту в карантине

1. На вкладке **Панель управления** главного окна нажмите **Угрозы**.
2. Откройте вкладку **Карантин**.
3. Выберите для соответствующего объекта необходимое действие из выпадающего списка:
   - **Удалить** — навсегда удалить объект из файловой системы;
   - **Восстановить** — вернуть объект из карантина туда, откуда он был перемещен;
   - **Восстановить в** — указать путь для восстановления объекта.

Объекты в карантине вылечить невозможно. Вы можете проверить объект еще раз, если сомневаетесь, что файл вредоносный.

Вы также можете восстановить объект. Алгоритмы лечения постоянно совершенствуются. Возможно, объект удастся вылечить после очередного обновления программы.

Если в списке угроз есть архивы, действие применяется ко всему архиву в целом.

Если вы хотите применить действие к отдельному файлу, распакуйте архив и запустите проверку еще раз.

Чтобы применить действие к нескольким угрозам

1. Выделите несколько угроз с помощью клавиши SHIFT.
2. Используйте специальные комбинации клавиш:
   - COMMAND-SHIFT-D — чтобы удалить угрозу;
   - COMMAND-SHIFT-R — чтобы восстановить объект туда, откуда он был перемещен,
   - COMMAND-SHIFT-P — чтобы указать путь для восстановления объекта.

13. Поддержка

13.1. Справка

Чтобы открыть справку Dr.Web

1. В главном окне нажмите .
2. Выберите вкладку **Справка**.

Если вы не нашли нужную информацию в справке, посмотрите список вопросов и ответов. Если вам не удалось найти ответ на интересующий вас вопрос и решить проблему, обратитесь в техническую поддержку компании «Доктор Веб».

13.2. Вопросы и ответы

Ниже приводятся описания некоторых проблем, которые могут возникнуть при работе с Dr.Web, а также предложены варианты их решения. Пожалуйста, прочитайте этот раздел справки перед тем как обращаться в техническую поддержку.

Общие проблемы

Компоненты SpIDer Gate, SpIDer Guard и Брандмауэр не включаются

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

1. Перейдите в меню Apple .
2. Выберите **Системные настройки**.
3. Перейдите в раздел **Защита и безопасность**.
4. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
5. Нажмите кнопку **Разрешить** рядом с сообщением о блокировке системного ПО от Doctor Web Ltd.

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

Лицензия активирована, но Dr.Web не работает

- Возможно, истек срок действия лицензии. Чтобы узнать срок действия лицензии и приобрести новую, перейдите в раздел **Лицензия** главного окна Dr.Web .
- Возможно, вы обновили операционную систему и установленная версия Dr.Web не поддерживает новую версию macOS. Удалите текущую версию Dr.Web и установите программу заново.

Dr.Web работает нестабильно (зависает/притормаживает)

Это может быть вызвано повышенной активностью системных процессов, требующих больших объемов оперативной памяти. Рекомендуем закрыть неиспользуемые приложения, чтобы освободить часть этой памяти. Вы можете посмотреть информацию о запущенных процессах и управлять ими при помощи стандартной утилиты macOS Мониторинг системы.

Если проблема повторяется, попробуйте переустановить приложение.

Брандмауэр заблокировал доступ в интернет

Создайте для приложения, которое не может получить доступ к интернету, разрешающее правило в настройках Брандмауэра.

Звуковые уведомления настроены, но не работают

Проверьте уровень громкости в разделе Системные настройки, а также на колонках.

Настройки заблокированы

Настройки некоторых компонентов защищены. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.

Проблемы при проверке

Проверка файловой системы не работает (не удается запустить Сканер и/или SplDer Guard)

Возможно, истек срок действия лицензии. Чтобы узнать срок действия лицензии и приобрести новую, перейдите в раздел **Лицензия** главного окна Dr.Web .

Вирусные базы загружаются очень долго или проверка происходит медленно

- Dr.Web загружает вирусные базы при запуске проверки и перед каждой попыткой вылечить объект. Поэтому это может занять некоторое время.
- Нестабильная работа может также быть вызвана повышенной активностью системных процессов, требующих больших объемов оперативной памяти. Рекомендуем закрыть неиспользуемые приложения, чтобы освободить часть этой памяти. Вы можете посмотреть информацию о запущенных процессах и управлять ими при помощи стандартной утилиты macOS Мониторинг системы.

Некоторые файлы пропускаются при проверке (не проверяются)

- Возможно, файлы (или папки, в которых они содержатся) исключены из проверки.
- Некоторые файлы могут быть пропущены при проверке, так как они повреждены или защищены паролем, а также если для доступа к ним требуются права администратора. Если список исключенных объектов содержит архивы, попробуйте распаковать их перед запуском проверки.

Сканер зависает

Если Сканер завис, завершите его работу и запустите заново. Если проблема повторяется, попробуйте переустановить приложение.

Проблемы в работе SplDer Gate

SplDer Gate не блокирует сайты по выбранным категориям

- Убедитесь, что на вкладке SplDer Gate установлен флажок напротив соответствующей категории сайтов.
- Если соединение с сайтом было установлено до запуска SplDer Gate, отключите и включите SplDer Gate и перезапустите браузер.

- Проверьте, использует ли сайт защищенное соединение (в случае защищенного соединения, как правило, в адресной строке браузера отображается замок). Если используется защищенное соединение, на вкладке Сеть включите опцию **Проверять зашифрованный трафик** и перезапустите браузер.
- SplDer Gate не блокирует сайты, использующие соединение по протоколам FTP/SPDY или HTTP/2.0.

При открытии сайта появляется сообщение об ошибке сертификата

- Ошибка может возникнуть, поскольку некоторые браузеры и почтовые клиенты при получении и передаче зашифрованного трафика не обращаются к системному хранилищу сертификатов. В таком случае установите сертификат компании «Доктор Веб», получить который можно нажав на кнопку Экспортировать на вкладке Сеть.
- Если браузер или почтовый клиент был запущен сразу после установки, он мог не получить системный сертификат безопасности. В этом случае нужно перезагрузить браузер или почтовый клиент.
- Возможно, оригинальный сертификат сервера является ненадежным. Чтобы проверить это, отключите SplDer Gate и перезапустите браузер или почтовый клиент. Если ошибка повторяется, значит сертификат является ненадежным и в этом случае не рекомендуется посещать этот сайт.

SplDer Gate заблокировал нужный сайт

Возможно, сайт входит в категорию сайтов, доступ к которым заблокирован. Чтобы получить доступ к сайту, внесите его в исключения.

Обновление

Обновления не загружаются

- Убедитесь, что Mac подключен к интернету.
- Если вы используете прокси-сервер, попробуйте его выключить и запустить обновление снова. Чтобы запустить обновление вручную, в главном окне Dr.Web выберите пункт **Требуется обновление**.
- Если маршрутизатор (роутер) работает в режиме «Подключение по требованию», убедитесь, что соединение активно постоянно (максимальное время простоя — 0 минут).
- Возможно, истек срок действия лицензии. Чтобы узнать срок действия лицензии и приобрести новую, перейдите в раздел **Лицензия** главного окна Dr.Web.

Лицензия

Срок пробной версии не истек, но лицензия стала недействительной

- Лицензия на пробную версию привязана к контрольной сумме операционной системы. Возможно, вы обновили операционную систему или другое программное обеспечение или заменили комплектующие компьютера и контрольная сумма изменилась.
- Лицензия на пробную версию привязана к MAC-адресу устройства. Возможно, вы изменили MAC-адрес и лицензия стала недействительной.

Обратитесь в техническую поддержку компании «Доктор Веб» или активируйте новую пробную версию с помощью другого адреса почты.

Не удается активировать лицензию

- Убедитесь, что Mac подключен к интернету.
- Если вы используете прокси-сервер, попробуйте его выключить и запустить обновление снова. Чтобы запустить обновление вручную, в главном окне Dr.Web выберите пункт **Требуется обновление**.
- Если маршрутизатор (роутер) работает в режиме «Подключение по требованию», убедитесь, что соединение активно постоянно (максимальное время простоя — 0 минут).

Если при использовании Dr.Web у вас возникли проблемы, решение которых не описано выше, обратитесь в техническую поддержку компании «Доктор Веб». Для того чтобы специалисты компании «Доктор Веб» смогли помочь вам максимально быстро, постарайтесь сообщить как можно больше информации о проблеме.

13.3. Коды ошибок

Код	Ошибка	Пояснение
1	Ошибка связи с монитором	Ошибка связи некоторого компонента с демоном управления конфигурацией Dr.Web ConfigD.
2	Операция уже выполняется	Операция, запрошенная пользователем, в данный момент уже выполняется.
3	Операция ожидает выполнения	Операция, запрошенная пользователем, в данный момент ожидает выполнения (возможно, производится установление сетевого соединения или осуществляется загрузка и инициализация какого-либо компонента

		программного комплекса, требующая продолжительного времени).
4	Прервано пользователем	Выполнявшееся действие было прервано пользователем (возможно, оно выполнялось слишком долго).
5	Операция отменена	Выполнявшееся действие было отменено (возможно, оно выполнялось слишком долго).
6	Соединение IPC разорвано	IPC-соединение с некоторым компонентом программного комплекса разорвано (скорее всего, компонент завершил свою работу из-за простоя или вследствие команды пользователя).
7	Недопустимый размер сообщения IPC	В процессе обмена данными между компонентами получено сообщение недопустимого размера.
8	Недопустимый формат сообщения IPC	В процессе обмена данными между компонентами получено сообщение недопустимого формата.
9	Не готов	Требуемое действие не может быть выполнено, потому что запрошенный компонент или устройство еще не инициализированы.
10	Компонент не установлен	Некоторая функция программного комплекса Dr.Web для macOS недоступна, поскольку реализующий ее компонент не установлен.
11	Неожиданное сообщение IPC	В процессе обмена данными между компонентами получено недопустимое сообщение.
12	Нарушения протокола IPC	В процессе обмена данными между компонентами произошло нарушение протокола обмена данными.
13	Неизвестное состояние подсистемы	Обнаружено, что некоторая подсистема программного комплекса, требуемая для выполнения операции, находится в неизвестном состоянии.
20	Путь должен быть абсолютным	Требуется абсолютный (т.е. начинающийся от корня файловой системы) путь к файлу или каталогу, а указан относительный путь.
21	Недостаточно памяти для завершения операции	Для выполнения требуемой операции не хватает памяти (например, попытка распаковать слишком большой файл).
22	Ошибка ввода-вывода	Произошла ошибка ввода/вывода (например, дисковое устройство еще не инициализировано или раздел файловой системы более недоступен).
23	Нет такого файла или каталога	Указанный объект файловой системы (файл или каталог) отсутствует, возможно, он был удален.

24	Доступ запрещен	Недостаточно прав для доступа к указанному объекту файловой системы (файлу или каталогу).
25	Не каталог	Ожидался путь к каталогу, однако указанный объект файловой системы не является каталогом.
26	Файл данных поврежден	Данные, к которым производится обращение, повреждены.
27	Файл уже существует	При попытке создать файл было обнаружено, что файл с таким именем уже существует.
28	Файловая система только для чтения	При попытке создать или изменить объект файловой системы (каталог, файл или сокет) было обнаружено, что файловая система доступна только для чтения.
29	Ошибка сети	Произошла сетевая ошибка (возможно, внезапно перестал отвечать удаленный узел или не удается установить требуемое соединение).
30	Не дисковое устройство	Производится попытка обращения к устройству ввода/вывода, которое не является дисковым устройством.
31	Неожиданный конец файла	При чтении данных неожиданно был достигнут конец файла.
32	Файл был изменен	При сканировании файла было обнаружено, что он был изменен.
33	Специальный файл	При доступе к объекту файловой системы было обнаружено, что это не регулярный файл (т.е. это каталог, сокет или иной объект файловой системы).
34	Имя уже используется	При попытке создать объект файловой системы (каталог, файл или сокет) было обнаружено, что объект с таким именем уже существует.
35	Хост отключен	Обнаружено, что удаленный узел недоступен по сети.
36	Достигнут предел использования ресурса	Достигнут предел использования некоторого ресурса.
37	Различные точки монтирования	Производится попытка выполнить восстановление файла, требующая его перемещение между каталогами файловой системы, принадлежащим различным точкам монтирования.
38	Ошибка распаковки	Не удалось распаковать архив (возможно, он защищен паролем или поврежден).
40	Вирусная база повреждена	Обнаружено, что повреждены вирусные базы.

41	Неподдерживаемая версия вирусных баз	Обнаружено, имеющиеся вирусные базы предназначены для старой версии программы.
42	Вирусная база пуста	Обнаружено, что вирусные базы пусты.
43	Объект не может быть вылечен	Попытка применить действие **Лечить** к неизлечимому объекту при нейтрализации угрозы.
44	Неподдерживаемая комбинация вирусных баз	Обнаружено, что имеющийся набор вирусных баз несовместим.
45	Достигнут предел проверки	При сканировании объекта превышены заданные ограничения (например, на величину распакованного файла, на глубину уровней вложенности и т. п.).
47	Неверные учетные данные пользователя	Попытка пройти аутентификацию с неверными учетными данными пользователя.
48	Пользователь не имеет требуемых прав	Попытка пройти авторизацию с учетными данными пользователя, не имеющего требуемых прав.
49	Недопустимый токен доступа	Компонент программного комплекса предъявил некорректный токен авторизации при попытке получения доступа к операции, требующей повышенные права.
60	Недопустимый аргумент	При попытке исполнить некоторую команду был указан недопустимый аргумент.
61	Недопустимая операция	Совершена попытка выполнить недопустимую команду.
62	Требуются права суперпользователя	Требуемое действие может быть выполнено только пользователем, обладающим полномочиями суперпользователя.
63	Не разрешено в режиме централизованной защиты	Требуемое действие может быть выполнено только при работе программного комплекса в одиночном (standalone) режиме.
64	Не поддерживаемая ОС	Операционная система, установленная на узле, не поддерживается программным комплексом.
65	Функция не реализована	Производятся попытки использования функций некоторого компонента, которые не реализованы в текущей версии.
66	Неизвестный параметр	Файл конфигурации содержит параметры, неизвестные или не поддерживаемые в текущей версии программного комплекса.
67	Неизвестная секция	Файл конфигурации содержит секции, неизвестные или не поддерживаемые в текущей версии программного комплекса.

68	Недопустимое значение параметра	Некоторый параметр в файле конфигурации имеет недопустимое для этого параметра значение.
69	Недопустимое состояние	Некоторый компонент или весь программный комплекс находятся в недопустимом состоянии для выполнения запрошенной операции.
70	Разрешено только одно значение	Некоторый параметр в файле конфигурации имеет список значений, что недопустимо для этого параметра.
71	Недопустимое имя тега	Некоторая секция в файле конфигурации, в имя которой включен уникальный идентификатор-тег, имеет недопустимое значение тега.
80	Запись не найдена	При попытке обратиться к информации о найденной угрозе было обнаружено, что информация о ней отсутствует (возможно, угроза уже была обработана другим компонентом программного комплекса).
81	Запись обрабатывается в данный момент	При попытке обратиться к информации о найденной угрозе было обнаружено, что в данный момент времени она уже обрабатывается другим компонентом программного комплекса.
82	Файл уже находится в карантине	При попытке перемещения файла с найденной угрозой в карантин было обнаружено, что он уже в карантине (скорее всего, угроза уже была обработана другим компонентом программного комплекса).
89	Не удалось сохранить резервную копию перед обновлением	Перед началом загрузки обновлений с сервера обновлений не удалось выполнить сохранение резервной копии обновляемых файлов.
90	Недопустимый DRL-файл	Обнаружено, что нарушена структура одного из файлов списков серверов обновлений.
91	Недопустимый LST-файл	Обнаружено, что нарушена структура файла, содержащего перечень обновляемых вирусных баз.
92	Недопустимый сжатый файл	Обнаружено, что нарушена структура загруженного файла, содержащего обновления.
93	Ошибка аутентификации на прокси-сервере	Не удалось подключиться к серверам обновлений через прокси-сервер, заданный в настройках.
94	Нет доступных серверов обновлений	Не удалось подключиться ни к одному из серверов обновлений.
95	Недопустимый формат ключевого файла	Нарушен формат ключевого файла.
96	Срок действия лицензии истек	Срок действия имеющейся у вас лицензии истёк.

97	Истек тайм-аут сетевой операции	Истек тайм-аут сетевой операции.
98	Недопустимая контрольная сумма	Обнаружено, что нарушена контрольная сумма загруженного файла, содержащего обновления.
99	Недопустимый демонстрационный ключевой файл	Используемый демонстрационный ключевой файл недействителен (например, он был получен для другого компьютера).
100	Лицензионный ключевой файл заблокирован	Используемая вами лицензия была заблокирована (возможно, нарушены условия лицензионного соглашения на использование программного продукта Dr.Web).
101	Недопустимая лицензия	Используемая вами лицензия предназначена для другого программного продукта или не содержит необходимых разрешений для работы компонентов установленного у вас продукта.
102	Недопустимая конфигурация	Некоторый компонент программного комплекса не может функционировать из-за неправильных настроек конфигурации.
104	Недопустимый исполняемый файл	Не запускается некоторый компонент программного комплекса, потому что неправильно указан путь к его исполняемому файлу или содержимое файла испорчено.
105	Ядро Virus-Finding Engine недоступно	Отсутствует или недоступен файл антивирусного ядра Dr.Web Virus-Finding Engine (требуется для поиска угроз).
106	Вирусные базы отсутствуют	Обнаружено, что вирусные базы отсутствуют.
107	Процесс завершен по сигналу	Компонент завершил свою работу (возможно, из-за простоя или вследствие команды пользователя).
108	Непредвиденное завершение процесса	Компонент неожиданно завершил свою работу вследствие сбоя.
109	Обнаружено несовместимое программное обеспечение	Компонент программного комплекса не может функционировать, поскольку обнаружено программное обеспечение, препятствующие его корректной работе.
110	Недопустимая библиотека VadeRetro	Отсутствует, недоступен или испорчен файл антиспам-библиотеки VadeRetro (требуется при проверке электронной почты).
112	Базы категорий веб-ресурсов отсутствуют	Обнаружено, что базы категорий веб-ресурсов отсутствуют.
113	Недоступен модуль ядра для SplDer Guard	Модуль ядра, который требуется для работы SplDer Guard отсутствует.

117	Недоступен компонент SpIDer Gate	Отсутствует компонент SpIDer Gate (требуется для проверки сетевых соединений).
118	Недоступен MailD	Отсутствует компонент SpIDer Mail (требуется для проверки электронной почты).
119	Scanning Engine недоступен	Невозможно проверять файлы, поскольку отсутствует или не запускается компонент Scanning Engine, используемый для проверки наличия вредоносного содержимого.
120	Сканер недоступен	Невозможно осуществлять проверку файлов, поскольку отсутствует компонент Сканер, используемый для проверки файлов.
121	Недоступен ESAgent	Отсутствует компонент ESAgent (требуется для подключения к серверу централизованной защиты).
122	Недоступен компонент Firewall	Невозможно контролировать сетевые соединения, поскольку отсутствует или не может быть запущен вспомогательный компонент Firewall, предназначенный для перенаправления соединений.
123	Network Checker недоступен	Невозможно контролировать сетевые соединения, поскольку отсутствует или не может быть запущен вспомогательный модуль Network Checker, предназначенный для проверки файлов, загруженных по сети.
124	Недоступен компонент CloudD	Отсутствует компонент CloudD, который требуется для обращения к сервису Dr.Web Cloud.
125	Непредвиденная ошибка	Возникла непредвиденная ошибка в работе некоторого компонента.

13.4. 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/.

14. Общие настройки

В разделе **Общие** вы можете настроить звуковые и экранные уведомления, выбрать язык, восстановить настройки по умолчанию.

Чтобы изменить общие настройки, не нужно вводить имя пользователя и пароль. Настройки изменятся для всех пользователей Mac автоматически.

Уведомления

Dr.Web использует системные уведомления macOS, чтобы показывать сообщения об обнаружении угроз, их обезвреживании или возникновении ошибок в работе компонентов.

Чтобы отключить уведомления

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Общие**.
3. Отключите опцию **Включить уведомления**.

Звуковые оповещения

Dr.Web использует звуковые оповещения, чтобы сообщить об обнаружении угроз, их обезвреживании и удалении.

Чтобы отключить звуковые оповещения

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Общие**.
3. Отключите опцию **Использовать звуковое оповещение**.

Восстановление настроек по умолчанию

Если после изменения настроек вы столкнулись с проблемами в работе Dr.Web, восстановите настройки по умолчанию. При этом все изменения настроек будут потеряны.

Чтобы восстановить настройки по умолчанию

1. В главном окне нажмите .

2. В окне **Настройки** выберите раздел **Общие**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.
4. Нажмите кнопку **Настройки по умолчанию**.
5. Нажмите кнопку **Восстановить**, чтобы подтвердить восстановление исходных настроек программы.

15. Подключение к облачным сервисам

Dr.Web подключается к облачным сервисам компании «Доктор Веб», чтобы защитить Mac от последних угроз и улучшать работу компонентов программы. Облачные сервисы помогают защитить пользователей от инфицированных файлов и оградить от посещения нежелательных сайтов.

Информация об угрозах на вашем Mac может устаревать в зависимости от настроек обновления вирусных баз. Обработка сведений об угрозах в облачном сервисе происходит быстрее, чем обновление локальных вирусных баз на компьютере.

Также на серверы компании «Доктор Веб» автоматически отправляются обезличенные сведения о работе компонентов Dr.Web. Вы можете ознакомиться с политикой конфиденциальности на официальном сайте компании «Доктор Веб».

Чтобы отключиться от облачных сервисов

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Dr.Web Cloud**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. Отключите опцию **Я хочу подключиться к сервисам (рекомендуется)**.

16. Режим централизованной защиты

Централизованную защиту Mac осуществляет администратор сервера Dr.Web Enterprise Security Suite или IT-провайдер с помощью антивирусной услуги Dr.Web AV-Desk. В этом режиме ваша персональная лицензия не используется.

Настройки и компоненты

Настройки и работа компонентов Dr.Web могут быть изменены или заблокированы в соответствии с политикой безопасности компании или списком оплаченных услуг провайдера. С сервера централизованной защиты могут контролироваться:

- Обновление вирусных баз. Обновления загружаются автоматически с сервера централизованной защиты. Если соединения с сервером нет, обновления будут загружаться через интернет с серверов Dr.Web.
- Постоянная защита файловой системы.
- Проверка веб-трафика.
- Проверка Mac на вирусы. Администратор антивирусной сети может запустить удаленную проверку Mac с сервера вручную или согласно расписанию.

Подключение Mac

Каждый Mac с установленным Dr.Web является отдельной станцией. В зависимости от настроек авторизации станций на сервере централизованной защиты, существует два способа подключения к антивирусной сети:

- Автоматически, если станция уже создана на сервере, и для нее заданы идентификатор и пароль.
- В качестве новой станции («новичка»). Dr.Web создаст новый идентификатор станции и пароль. В данном случае может потребоваться подтверждение станции на сервере, или же станция будет авторизована автоматически при соответствующих настройках доступа на сервере.

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

Автоматическое подключение

Если вы купили подписку на антивирусную услугу Dr.Web AV-Desk, вы можете установить Dr.Web с помощью файла формата `.cdr`, который содержит параметры подключения к серверу. Обратитесь к вашему IT-провайдеру, чтобы получить файл `.cdr`.

Чтобы установить Dr.Web с помощью файла .cdr

1. Запустите полученный файл.
2. Нажмите **Установить Dr.Web**.
3. Примите условия Лицензионного соглашения. Начнется процесс установки программы.
4. Введите пароль администратора и нажмите кнопку **Установить вспомогательную программу**.
5. Dr.Web для macOS скопируется в папку **Программы** и запустится.

Подключение к серверу централизованной защиты будет настроено автоматически.

Если администратор антивирусной сети вашей компании или IT-провайдер предоставил конфигурационный файл формата `.cfg`, вы можете подключить Dr.Web в разделе **Активация лицензии**. Параметры подключения к серверу централизованной защиты будут настроены автоматически.

Чтобы подключить станцию с помощью файла .cfg

1. В главном окне Dr.Web выберите пункт **Лицензия**.
2. Нажмите **Активировать**.
3. В окне **Активация лицензии** откройте вкладку **Файлы активации**.
4. Перетащите файл формата `.cfg` в пунктирную область или нажмите, чтобы выбрать файл на Mac.
5. После того, как активация завершится, параметры подключения к серверу будут настроены автоматически.

Если администратор антивирусной сети вашей компании предоставил открытый ключ шифрования формата `.pub` или сертификат, вы можете настроить параметры подключения вручную.

Чтобы настроить параметры подключения к серверу вручную

1. В главном окне нажмите  .
2. В окне **Настройки** выберите раздел **Режим**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите  внизу окна и введите имя пользователя и пароль.

4. Включите опцию **Включить режим централизованной защиты**. При включении централизованного режима восстанавливаются параметры последнего подключения.
5. Укажите IP-адрес сервера и номер порта, который используется для подключения к серверу.
6. Перетащите открытый ключ шифрования формата `.pub` или сертификат в пунктирную область или дважды нажмите, чтобы выбрать файл.
7. Раскройте подраздел **Идентификация**.
8. Отключите опцию **Подключиться как новичок**. Укажите дополнительные параметры для авторизации рабочей станции:
   - идентификатор станции;
   - пароль (присвоенный вашему компьютеру для регистрации на сервере);
   - режим сжатия трафика;
   - режим шифрования трафика.

   Указанные значения параметров сохраняются с помощью функции Keychain. Таким образом, при повторном подключении к серверу их не придется вводить их заново.
9. Нажмите **Подключиться**.

Подключение в качестве «новичка»

Если администратор еще не создал станцию на сервере, вы можете подключить ее в качестве «новичка». Обратитесь к администратору антивирусной сети вашей компании или к IT-провайдеру за открытым ключом шифрования или сертификатом и параметрами подключения к серверу централизованной защиты.

Чтобы подключить станцию в качестве «новичка»

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Режим**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. Включите опцию **Включить режим централизованной защиты**.
5. Укажите IP-адрес сервера и номер порта, который используется для подключения к серверу.
6. Перетащите открытый ключ шифрования `.pub` или сертификат в пунктирную область или дважды нажмите, чтобы выбрать файл.
7. Убедитесь, что в подразделе **Идентификация** включена опция **Подключиться как новичок**.

8. Нажмите **Подключиться**.

Автономный режим

Вы можете отключить режим централизованной защиты и восстановить автономную работу Dr.Web.

При включении режима автономной работы восстанавливаются все настройки программы, установленные до перехода в централизованный режим, или настройки по умолчанию. Также возобновляется доступ ко всем компонентам Dr.Web.

Для работы в автономном режиме требуется действительный ключевой файл. Лицензия, полученная автоматически с сервера централизованной защиты, в данном режиме использоваться не может. При необходимости активируйте персональную лицензию.

Чтобы восстановить режим автономной работы

1. В главном окне нажмите .
2. В окне **Настройки** выберите раздел **Режим**.
3. Если настройки недоступны, снимите защиту. Для этого нажмите внизу окна и введите имя пользователя и пароль.
4. Отключите опцию **Включить режим централизованной защиты**.
5. Подтвердите действие с помощью кнопки **Отключить**.

17. Справочная информация

17.1. Централизованная защита и антивирусная сеть

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.

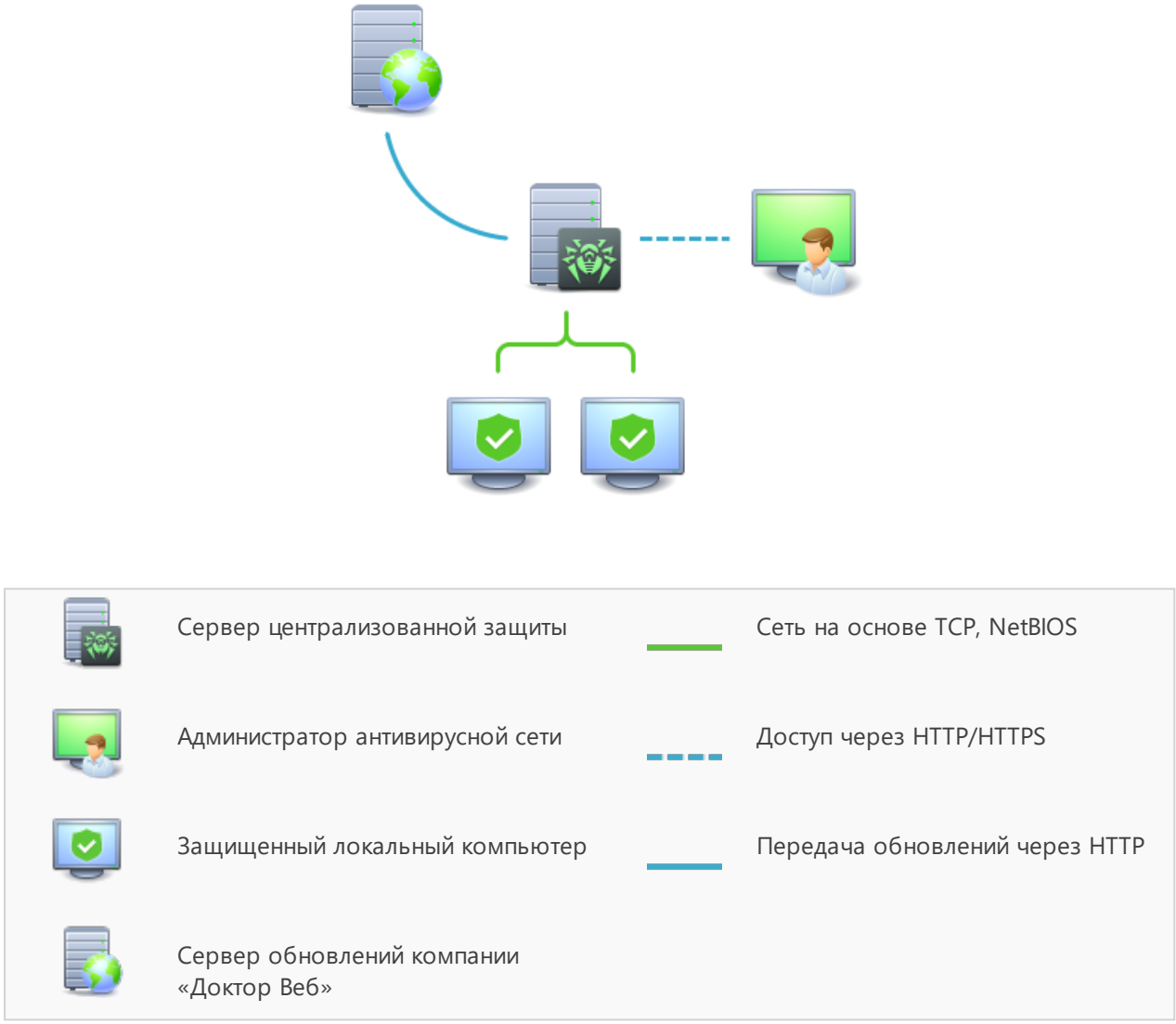

Рисунок 1. Логическая структура антивирусной сети

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 компании «Доктор Веб».

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 «Доктор Веб» по адресу https://www.av-desk.com/.

17.2. Виды 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 также могут нанести вред пользователю.

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 инфицированному файлу.
- *Макро-вирусы* инфицируют документы, которые используют программы из пакета **Microsoft® Office** (и другие программы, которые используют макросы, написанные, например, на языке **Visual Basic**). *Макросы* — это встроенные программы, 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 инфицируют 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* инфицируют 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 инфицировании, 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.
- *Стелс-вирусы* (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т.д.) и по инфицируемым ими 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, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через сеть Интернет) 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.).
- *Чат-черви* распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т.д.).

Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы подменяют какую-либо из часто запускаемых программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т.д.), либо делая 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.

Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. 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.
- *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)*.
- *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 (DDoS-атак).

- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в сеть Интернет через компьютер жертвы.

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).

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, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

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-серверы и т.д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типов 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».

17.3. Методы обнаружения угроз

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

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».

Поведенческий анализ

Dr.Web Process Heuristic

Технология поведенческого анализа Dr.Web Process Heuristic защищает от новейших, наиболее опасных вредоносных программ, которые способны избежать обнаружения традиционными сигнатурными и эвристическими механизмами.

Dr.Web Process Heuristic анализирует поведение каждой запущенной программы, сверяясь с постоянно обновляемыми облачным сервисом Dr.Web, и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности, после чего принимаются необходимые меры по нейтрализации угрозы.

Данная технология защиты данных позволяет свести к минимуму потери от действий неизвестного вируса — при минимальном потреблении ресурсов защищаемой системы.

Dr.Web Process Heuristic контролирует любые попытки изменения системы:

- распознает процессы вредоносных программ, изменяющих нежелательным образом пользовательские файлы (например, действия троянских программ-шифровальщиков);
- препятствует попыткам вредоносных программ внедриться в процессы других приложений;
- защищает от модификаций вредоносными программами критических участков системы;
- выявляет и прекращает вредоносные, подозрительные или ненадежные сценарии и процессы;
- блокирует возможность изменения вредоносными программами загрузочных областей диска с целью невозможности запуска (например, буткитов) на компьютере;
- предотвращает отключение безопасного режима Windows, блокируя изменения реестра;
- не позволяет вредоносным программам изменить правила запуска программ;
- пресекает загрузки новых или неизвестных драйверов без ведома пользователя;
- блокирует автозапуск вредоносных программ, а также определенных приложений, например, анти-антивирусов, не давая им зарегистрироваться в реестре для последующего запуска;

- блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможной установку троянских программ под видом нового виртуального устройства;
- не позволяет вредоносному программному обеспечению нарушить нормальную работу системных служб.

Dr.Web Process Dumper

Комплексный анализатор упакованных угроз Dr.Web Process Dumper значительно повышает уровень детектирования якобы «новых угроз» — известных вирусной базе Dr.Web, но скрытых под новыми упаковщиками, а также исключает необходимость добавления в базы все новых и новых записей об угрозах. Сохранение компактности вирусных баз Dr.Web, в свою очередь, не требует постоянного увеличения системных требований и обеспечивает традиционно малый размер обновлений — при традиционно неизменно высоком качестве детектирования и лечения.

Метод машинного обучения

Применяется для поиска и нейтрализации вредоносных объектов, которых еще нет в вирусных базах. Преимущество этого метода заключается в распознавании вредоносного кода без исполнения, только на основе его характеристик.

Обнаружение угроз строится на классификации вредоносных объектов согласно определенным признакам. С помощью технологии машинного обучения, основанной на методе опорных векторов, происходит классификация и запись в базу фрагментов кода сценарных языков. Затем проверяемые объекты анализируются на основе соответствия признакам вредоносного кода. Технология машинного обучения автоматизирует обновление списка данных признаков и пополнение вирусных баз. Благодаря подключению к облачному сервису обработка больших объемов данных происходит быстрее, а постоянное обучение системы обеспечивает превентивную защиту от новейших угроз. При этом технология может функционировать и без постоянного обращения к облаку.

Метод машинного обучения существенно экономит ресурсы операционной системы, так как не требует исполнения кода для выявления угроз, а динамическое машинное обучение классификатора может осуществляться и без постоянного обновления вирусных баз, которое используется при сигнатурном анализе.

Облачные технологии обнаружения угроз

Облачные методы обнаружения позволяют проверить любой объект (файл, приложение, расширение для браузера и т.п.) по хеш-сумме. Она представляет собой уникальную последовательность цифр и букв заданной длины. При анализе по хеш-сумме объекты проверяются по существующей базе и затем классифицируются на категории: чистые, подозрительные, вредоносные и т.д.

Подобная технология оптимизирует время проверки файлов и экономит ресурсы устройства. Благодаря тому, что анализируется не сам объект, а его уникальная хеш-сумма, решение выносится практически моментально. При отсутствии подключения к серверам Dr.Web, файлы проверяются локально, а облачная проверка возобновляется при восстановлении связи.

Таким образом, облачный сервис компании «Доктор Веб» собирает информацию от многочисленных пользователей и оперативно обновляет данные о ранее неизвестных угрозах, тем самым повышая эффективность защиты устройств.

17.4. Комбинации клавиш

Чтобы запустить проверку, применить действия к обнаруженным угрозам, а также для настройки работы Dr.Web вы можете использовать специальные комбинации клавиш:

Комбинация		**Действие**
Действия над угрозами	COMMAND-SHIFT-C	Лечить угрозу
	COMMAND-SHIFT-M	Переместить угрозу в карантин
	COMMAND-SHIFT-I	Игнорировать угрозу
	COMMAND-SHIFT-D	Удалить угрозу
	COMMAND-SHIFT-R	Восстановить угрозу
	COMMAND-SHIFT-P	Выбрать папку, куда восстановить угрозу
Общие	COMMAND-A	Выделить все
	COMMAND-W	Закрыть

© «Доктор Веб», 2021