



Dr.WEB

Security Space для мобильных устройств
(Аврора)

Руководство пользователя



© «Доктор Веб», 2025. 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, SplDer Mail, SplDer 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 Security Space для мобильных устройств (Аврора)

Версия 3.3

Руководство пользователя

07.04.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 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. О документе	5
2. О продукте	6
2.1. Основные функции	6
2.2. Системные требования	6
3. Установка Dr.Web Security Space для мобильных устройств	7
4. Удаление Dr.Web Security Space для мобильных устройств	9
5. Интерфейс	10
6. Учетные записи	17
7. Лицензирование	18
7.1. Страница Лицензия	18
7.2. Пробный период	20
7.3. Покупка лицензии	22
7.4. Активация лицензии	24
7.5. Восстановление лицензии	28
8. Компоненты Dr.Web	29
8.1. Сканер Dr.Web: проверка по запросу пользователя	29
8.2. Статистика	35
8.3. Карантин	39
9. Настройки	43
9.1. Общие настройки	44
9.2. Настройки Сканера	44
9.3. Настройки обновлений	44
9.4. Сброс настроек	45
10. Обновление вирусных баз	47
11. Обновление Dr.Web	49
12. Техническая поддержка	50



1. О документе

Руководство призвано помочь администраторам и пользователям устройств под управлением оперативной системы «Аврора» установить и настроить приложение Dr.Web Security Space для мобильных устройств, а также ознакомиться с его основными функциями.

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
<i>Антивирусная сеть</i>	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.
/home/user	Наименования файлов и каталогов, фрагменты программного кода.
<u>Приложение A</u>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.



2. О продукте

Dr.Web Security Space для мобильных устройств (далее — Dr.Web) защищает от вирусных угроз мобильные устройства, работающие под управлением операционной системы «Аврора».

В приложении применены разработки и технологии компании «Доктор Веб» по обнаружению и обезвреживанию вредоносных объектов, которые представляют угрозу информационной безопасности устройства и могут повлиять на его работу.

Dr.Web использует технологию Origins Tracing™, которая находит вредоносные программы для различных платформ, включая ОС «Аврора». Эта технология позволяет определять новые семейства вирусов на основе базы знаний об уже найденных и изученных угрозах.

2.1. Основные функции

Dr.Web выполняет следующие функции:

- проверяет все файлы в памяти или отдельные файлы по запросу пользователя;
- проверяет архивы;
- удаляет обнаруженные угрозы безопасности или перемещает их в карантин;
- обновляет вирусные базы Dr.Web через интернет;
- ведет статистику активности приложения (события Сканера, обновление вирусных баз, действия над обнаруженными угрозами), а также журнал событий.

2.2. Системные требования

Перед установкой проверьте, что ваше устройство соответствует следующим требованиям и рекомендациям:

Параметр	Требования
Операционная система	Аврора 5.1.0 и более поздние сборки версии 5
Архитектура процессора	ARMv7, ARMv8
Свободная оперативная память	Не менее 512 МБ
Свободная основная память	Не менее 20 МБ (для хранения данных)
Разрешение экрана	Не менее 800×480
Прочее	Интернет-соединение (для обновления вирусных баз)



3. Установка Dr.Web Security Space для мобильных устройств

Вы можете установить Dr.Web:

- [вручную](#),
- [с помощью приложения RuStore](#).

Чтобы установить Dr.Web, вам может понадобиться разрешить установку приложений без подписи источника. Для этого:

1. В настройках устройства откройте вкладку **Система** и выберите пункт **Источники приложений**.
2. Коснитесь переключателя **Разрешить установку приложений без подписи источника**. При необходимости введите пароль.

Ручная установка Dr.Web

Ручная установка приложения возможна только при наличии прав администратора.

Чтобы установить Dr.Web вручную

1. Скачайте установочный файл Dr.Web или скопируйте его на устройство.
2. На экране приложений откройте приложение «Файлы».
3. Найдите установочный файл Dr.Web и коснитесь его.
4. В диалоговом окне нажмите **Установить**.

В случае успешной установки вверху экрана отобразится соответствующее уведомление. Приложение Dr.Web также появится на экране приложений устройства пользователя.

Для дальнейшей работы необходимо активировать [коммерческую](#) или [демонстрационную](#) лицензию.

Установка из RuStore

1. Откройте RuStore на устройстве.
2. Найдите в списке приложений Dr.Web.



Если Dr.Web не отображается в RuStore, значит, ваше устройство не удовлетворяет [системным требованиям](#).

3. Воспользуйтесь любым из вариантов установки:
 - 1) Нажмите кнопку **Скачать** справа от названия приложения.
 - 2) Для начала работы с приложением нажмите кнопку **Открыть**.



или:

- 1) Нажмите на карточку приложения.
- 2) В открывшемся окне нажмите **Скачать**.
- 3) Для начала работы с приложением нажмите **Открыть**.



4. Удаление Dr.Web Security Space для мобильных устройств

Чтобы удалить Dr.Web с экрана приложений

1. Откройте экран приложений.
2. Коснитесь экрана приложений и удерживайте его до появления значков .
3. Коснитесь  на значке Dr.Web, чтобы удалить приложение.



5. Интерфейс

Используйте следующие элементы интерфейса, чтобы настраивать и управлять Dr.Web:

- [жесты](#),
- [кнопка возврата](#),
- [меню действий](#),
- [контекстное меню](#),
- [переключатель](#),
- [панель оповещений](#),
- [таймер отмены](#),
- [обложку приложения](#).

Жесты

Чтобы открыть приложение, на домашнем экране устройства проведите снизу вверх. В открывшемся экране приложений выберите Dr.Web.

Если вы хотите свернуть приложение и вернуться на домашний экран устройства, в открытом приложении проведите от нижнего края вверх. На домашнем экране отобразится [обложка](#) Dr.Web. Коснитесь ее, чтобы снова открыть приложение.

Кнопка возврата

В Dr.Web некоторые компоненты интерфейса находятся во вложенных страницах. Отличительный элемент такой страницы — кнопка возврата в виде светящейся точки или вертикальной полосы в левом верхнем углу (см. [Рисунок 1](#)). Коснитесь кнопки, чтобы вернуться на предыдущую страницу с сохранением всех внесенных изменений.



Рисунок 1. Кнопка возврата на предыдущую страницу в виде точки (слева) и полосы (справа)

Вы также можете вернуться на предыдущую страницу, проведя слева направо на вложенной странице.

Меню действий

Меню действий открывает меню Dr.Web. Также оно позволяет выполнить действия на текущей странице.



На наличие такого меню указывает светящаяся горизонтальная полоса в верхней части экрана приложения.

Чтобы открыть меню действий, коснитесь экрана ниже полосы и проведите вниз.

Чтобы в открывшемся меню выбрать нужный пункт, коснитесь его. Вы также можете коснуться экрана ниже полосы, провести вниз и прокрутить до нужного пункта меню или кнопки.

Контекстное меню

Контекстное меню открывает список доступных действий или дополнительную информацию, в зависимости от выбранного элемента страницы. Например, с помощью контекстного меню вы можете просмотреть список действий для обнаруженных угроз (см. [Рисунок 2](#)).

Чтобы открыть контекстное меню, коснитесь нужного элемента страницы и удерживайте его.

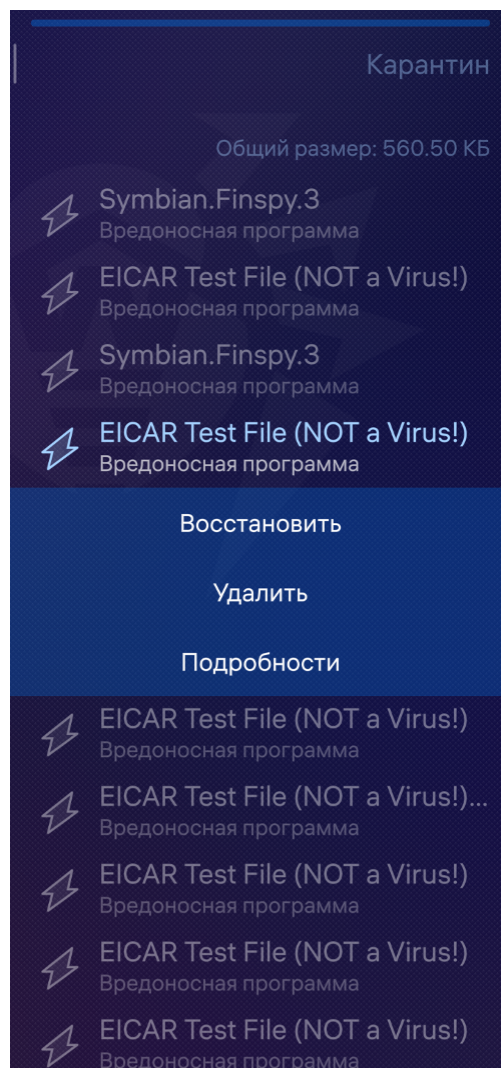


Рисунок 2. Контекстное меню

Переключатель

Настройки приложения изменяются с помощью переключателей, имеющих два положения:  — опция включена,  — опция отключена. Чтобы включить или отключить опцию, коснитесь переключателя.

Панель оповещений

Панель оповещений (см. [Рисунок 3](#)) появляется в нижней части страницы, когда по завершении процесса требуется действие пользователя. Например, панель оповещений появляется, если в результате проверки были найдены угрозы.

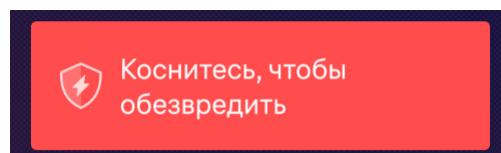


Рисунок 3. Панель оповещений

Коснитесь панели, чтобы перейти на страницу с доступными действиями.

Таймер отмены

Таймер отмены (см. [Рисунок 4](#)) появляется в верхней части страницы после запуска действия (например, сброса настроек). Чтобы отменить действие, коснитесь таймера отмены.

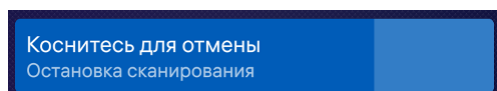


Рисунок 4. Таймер отмены

Обложка приложения и остановка Dr.Web

Если вы свернете Dr.Web, проведя по открытой странице приложения от нижнего края вверх, на домашней странице устройства отобразится обложка приложения (см. [Рисунок 5](#)). Коснитесь обложки, чтобы снова открыть приложение.

Если вы свернете приложение во время проверки устройства, на домашней странице отобразится обложка с прогрессом проверки.



Рисунок 5. Обложка приложения

Чтобы полностью остановить работу приложения и завершить связанные процессы

1. В открытом приложении проведите от нижнего края экрана вверх.
2. На домашней странице устройства коснитесь любой точки и удерживайте ее, пока не появится значок .
3. Коснитесь значка.

Если вы полностью остановите работу приложения во время проверки, при следующем запуске приложения на главной странице вы увидите оповещение о количестве обнаруженных угроз (см. [Рисунок 6](#)). Если угрозы не были обнаружены, оповещение не появится. Чтобы просмотреть результаты проверки в этом случае, повторно откройте страницу выбранного ранее типа [проверки](#).

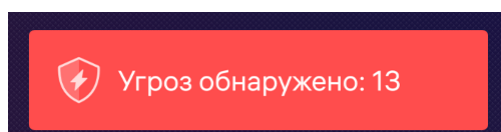


Рисунок 6. Оповещение о количестве обнаруженных угроз



Главная страница

На главной странице приложения (см. [Рисунок 7](#)) располагается список основных компонентов Dr.Web.

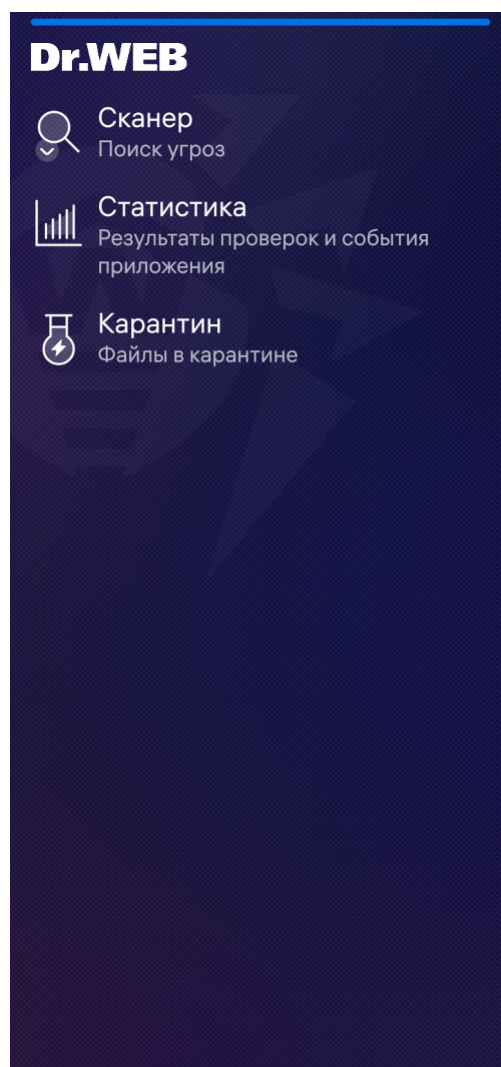


Рисунок 7. Главный экран приложения

Чтобы увидеть остальные функции и настройки, коснитесь экрана ниже светящейся полосы и проведите вниз.

С помощью открывшегося меню (см. [Рисунок 8](#)) вы можете:

- [Обновить вирусные базы.](#)
- Перейти к [настройкам приложения.](#)
- Открыть [экран с информацией о лицензии.](#)
- Просмотреть информацию о приложении и открыть справку.

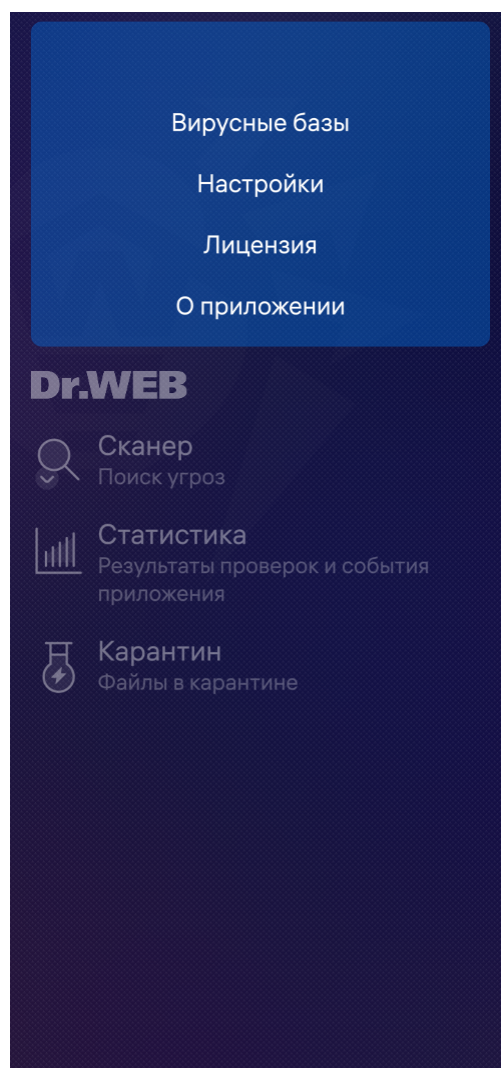


Рисунок 8. Меню приложения



6. Учетные записи

Возможность использования некоторых функций Dr.Web Security Space для мобильных устройств зависит от типа учетной записи: администратор или пользователь.

В отличие от администратора пользователь не может:

- просматривать [статистику](#);
- производить действия над угрозами, помещенными в карантин под иной учетной записью.



Как администраторы, так и пользователи могут находить и обезвреживать угрозы только в тех областях системы, к которым они имеют доступ на чтение и изменение.



7. Лицензирование

Для работы Dr.Web требуется лицензия. Лицензия позволяет использовать все функции приложения на протяжении всего срока действия и регулирует права пользователя, установленные в соответствии с пользовательским договором.

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете активировать [пробный период](#).

7.1. Страница Лицензия

На странице **Лицензия** (см. [Рисунок 9](#)) вы можете [купить](#) или [активировать](#) коммерческую лицензию, а также получить [пробный период](#).

Чтобы перейти на страницу, откройте приложение, коснитесь ниже светящейся полосы и проведите вниз. В открывшемся меню выберите пункт **Лицензия**.



Страница с предложением об активации лицензии откроется сразу после открытия приложения, если у вас нет активированной демонстрационной лицензии.

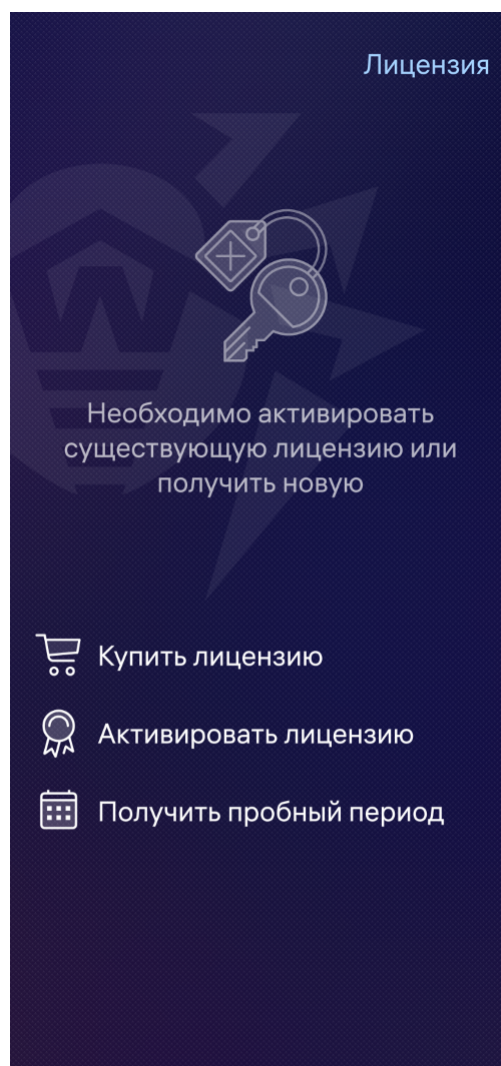


Рисунок 9. Страница Лицензия

Когда лицензия активна, на странице **Лицензия** (см. [Рисунок 10](#)) вы можете просмотреть информацию о лицензии: серийный номер, имя пользователя лицензии, даты начала и окончания срока действия лицензии и количество оставшихся до него дней.

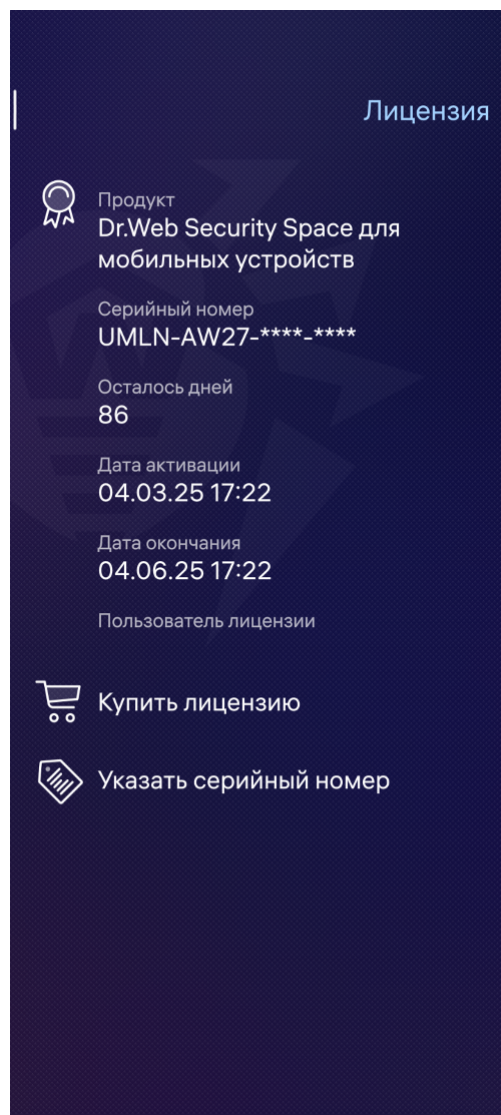


Рисунок 10. Информация о лицензии

Если срок действия лицензии скоро закончится, вы можете приобрести новую и пользоваться ей, не переустанавливая приложение. Для этого коснитесь пункта **Купить лицензию** и следуйте инструкциям из разделов [Покупка лицензии](#) и [Активация лицензии](#).

7.2. Пробный период

Если вы хотите ознакомиться с функциями приложения перед покупкой лицензии, вы можете активировать пробный период на 14 дней.

Чтобы активировать пробный период

1. Экран с предложением о покупке лицензии (см. [Рисунок 11](#)) появится сразу после открытия приложения.

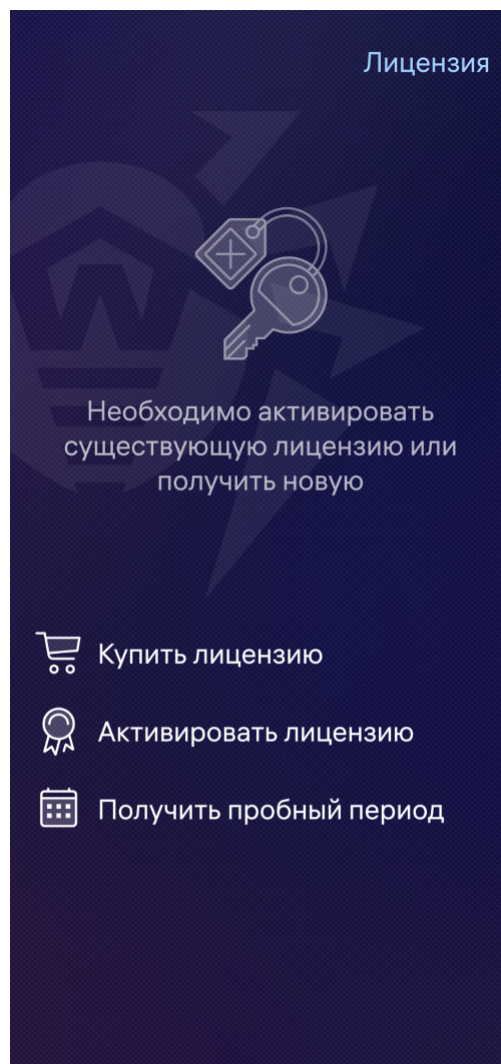


Рисунок 11. Экран Лицензия

2. Выберите **Получить пробный период**.
3. Укажите ваши личные данные (см. [Рисунок 12](#)):
 - имя и фамилию,
 - действующий адрес электронной почты,
 - страну.
4. По желанию установите флажок **Получать рассылки на эту почту**.
5. Коснитесь кнопки **Активировать**. Пробный период будет активирован.



Рисунок 12. Получение пробного периода

7.3. Покупка лицензии

Чтобы приобрести лицензию

1. На [главной странице](#) приложения коснитесь ниже светящейся полосы и проведите вниз. В меню действий выберите пункт **Лицензия**.
Если у вас нет активированной лицензии, экран с предложением о покупке лицензии (см. [Рисунок 13](#)) появится сразу после открытия приложения.

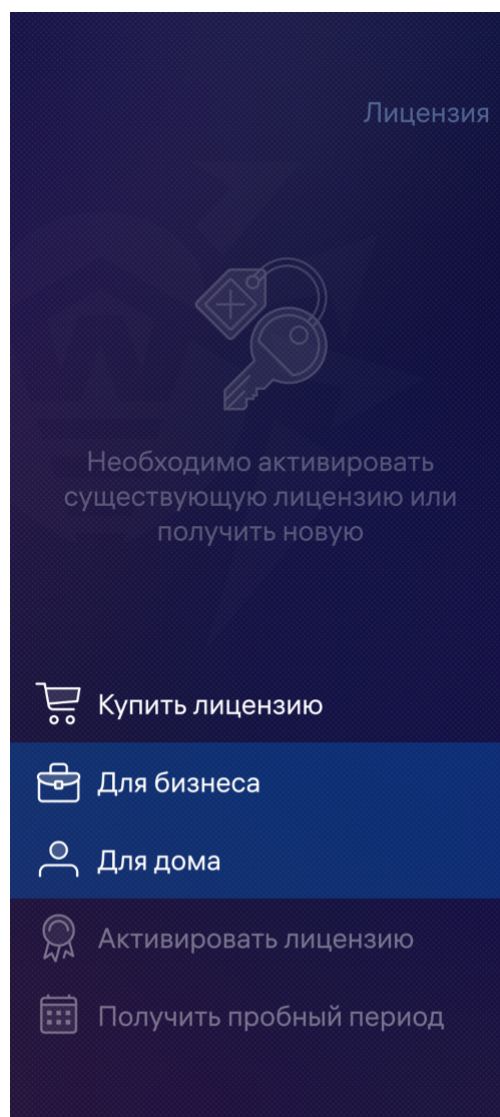


Рисунок 13. Покупка Лицензии

2. Выберите **Купить лицензию**. Если вы пользуетесь демонстрационной лицензией или у вас нет активированной лицензии, выберите **Для дома**. Откроется страница интернет-магазина «Доктор Веб».

Вы также можете перейти в магазин по ссылке <https://estore.drweb.com/mobile/>.

3. Выберите срок действия лицензии и количество защищаемых устройств.
4. Нажмите **Купить**.
5. Заполните форму покупки и нажмите **Сделать заказ**.

После оформления заказа серийный номер будет выслан на указанный вами адрес электронной почты. Кроме того, вы можете выбрать вариант получения серийного номера в виде СМС-сообщения на указанный номер телефона. На ваш адрес электронной почты также будет отправлен [лицензионный ключевой файл](#). Вы можете использовать его для активации или восстановления лицензии.

6. Вернитесь в приложение. На экране **Лицензия** выберите **Указать серийный номер** или [Использовать ключевой файл](#).



Если вы выбрали **Указать серийный номер**, введите полученный серийный номер и нажмите кнопку **Активировать**.

Если вы выбрали **Использовать ключевой файл**, найдите папку, в которой лежит ключевой файл или ZIP-архив с файлом и выберите его.

Если из-за возможных технических сбоев лицензия не активируется, обратитесь в службу технической поддержки: <https://support.drweb.com/>.

7.4. Активация лицензии

После [покупки лицензии](#) вам необходимо ее активировать.



Начиная с 01.09.2024, Dr.Web Security Space для мобильных устройств не входит в состав лицензий на программные продукты Dr.Web для ПК. Если вы приобрели такую лицензию позднее 31.08.2024, для работы с Dr.Web Security Space для мобильных устройств вам потребуется [приобрести отдельную лицензию](#).

Чтобы активировать лицензию

- Зарегистрируйте серийный номер:
 - либо [в приложении](#), если на устройстве с установленным приложением есть активное интернет-соединение;
 - либо [на сайте компании «Доктор Веб»](#), если на устройстве с установленным приложением нет интернет-соединения.
- [Используйте ключевой файл](#).

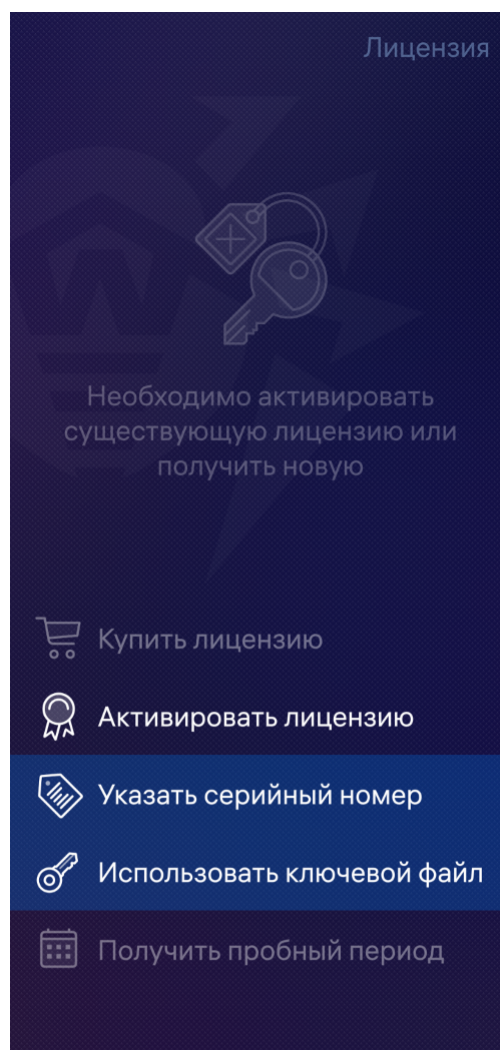


Рисунок 14. Активация лицензии

Регистрация серийного номера в приложении

Чтобы зарегистрировать серийный номер и активировать лицензию в приложении

1. Если у вас нет активной лицензии, экран с предложением об активации появится сразу после открытия приложения. Если у вас есть активная лицензия, на [главной странице](#) приложения коснитесь ниже светящейся полосы и проведите вниз. Затем в меню действий выберите пункт **Лицензия**.
2. Если у вас нет активной лицензии, выберите пункт **Активировать лицензию** и коснитесь пункта **Указать серийный номер** (см. [Рисунок 14](#)). Если у вас есть активная лицензия, коснитесь пункта **Указать серийный номер**.
3. На открывшейся странице введите серийный номер, который вы получили после покупки.



4. Если вы ранее не регистрировали введенный серийный номер, укажите ваши личные данные (см. [Рисунок 15](#)):
 - имя и фамилию,
 - действительный адрес электронной почты,
 - страну.
5. По желанию установите флажок **Получать рассылки на эту почту**.
6. Коснитесь кнопки **Активировать**.

Рисунок 15. Регистрация лицензии

Откроется страница с данными о владельце лицензии. Вверху экрана появится сообщение о том, что лицензия активирована.

Регистрация серийного номера на сайте

Если на устройстве с установленным приложением нет интернет-соединения, вы можете зарегистрировать серийный номер с помощью другого устройства с активным интернет-соединением. В этом случае вам будет выслан [лицензионный ключевой файл](#), который нужно скопировать на устройство, чтобы активировать лицензию.

Чтобы зарегистрировать серийный номер на сайте

1. Зайдите на сайт <https://products.drweb.com/register/>.



2. Введите серийный номер, полученный при покупке Dr.Web.
3. Укажите регистрационные данные владельца лицензии.
4. Лицензионный ключевой файл будет выслан в ZIP-архиве по указанному вами адресу электронной почты.

Лицензионный ключевой файл

Лицензионный ключевой файл содержит права пользователя на использование продукта Dr.Web.

Файл имеет расширение `.key` и содержит, в частности, следующую информацию:

- период, в течение которого разрешено использование приложения;
- перечень компонентов, разрешенных к использованию;
- другие ограничения.

Лицензионный ключевой файл является действительным при одновременном выполнении следующих условий:

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

При нарушении любого из условий лицензионный ключевой файл становится недействительным, при этом антивирус перестает обезвреживать вредоносные программы.



Редактирование лицензионного ключевого файла делает его недействительным. Поэтому не рекомендуется открывать его без крайней необходимости в текстовых редакторах во избежание его случайной порчи.

Использование ключевого файла

Вы можете активировать лицензию с помощью ключевого файла.



При наличии активной лицензии использовать ключевой файл нельзя. Дождитесь окончания срока действия лицензии или используйте [серийный номер](#).

Чтобы использовать ключевой файл

1. Скопируйте ключевой файл на ваше устройство.

Вы можете распаковать архив и скопировать только файл с расширением `.key` или перенести на устройство ZIP-архив целиком.



2. На странице [Лицензия](#) выберите пункт **Активировать лицензию**.
3. Выберите пункт **Использовать ключевой файл** (см. [Рисунок 14](#)).
4. Найдите папку, в которой лежит ключевой файл или ZIP-архив с файлом и выберите его.

Ключевой файл будет установлен и готов к использованию. Откроется экран с данными о владельце лицензии. Вверху экрана появится сообщение, что лицензия активирована.

7.5. Восстановление лицензии

Восстановление лицензии может понадобиться, если вы переустановили приложение или хотите использовать Dr.Web на другом устройстве.

Вы можете восстановить лицензию двумя способами:

- [зарегистрировать серийный номер](#),
- [использовать ключевой файл](#).

Чтобы восстановить демонстрационную лицензию

1. На открывшемся после запуска приложения экране коснитесь пункта **Получить пробный период**.
2. Укажите ваши личные данные:
 - имя и фамилию,
 - действительный адрес электронной почты,
 - страну.
3. Коснитесь кнопки **Активировать**.

Демонстрационная лицензия привязана к устройству. При смене устройства вы не восстанавливаете демонстрационную лицензию, а получаете новую.



8. Компоненты Dr.Web

На [главной странице](#) приложения находится список компонентов:

- [Сканер](#) проверяет систему по запросу пользователя. Возможны три типа проверки: быстрая, полная и выборочная.
- [Статистика](#) регистрирует события Сканера Dr.Web, [обновления вирусных баз](#) и действия, примененные к обнаруженным угрозам.
- [Карантин](#) позволяет просмотреть и обработать угрозы, перемещенные в карантин.

8.1. Сканер Dr.Web: проверка по запросу пользователя

Сканер Dr.Web проверяет систему по запросу пользователя. Вы можете провести быструю или полную проверку файловой системы, а также проверить отдельные файлы.



Администраторы и пользователи могут находить и обезвреживать угрозы только в тех областях системы, к которым они имеют доступ на чтение и изменение.

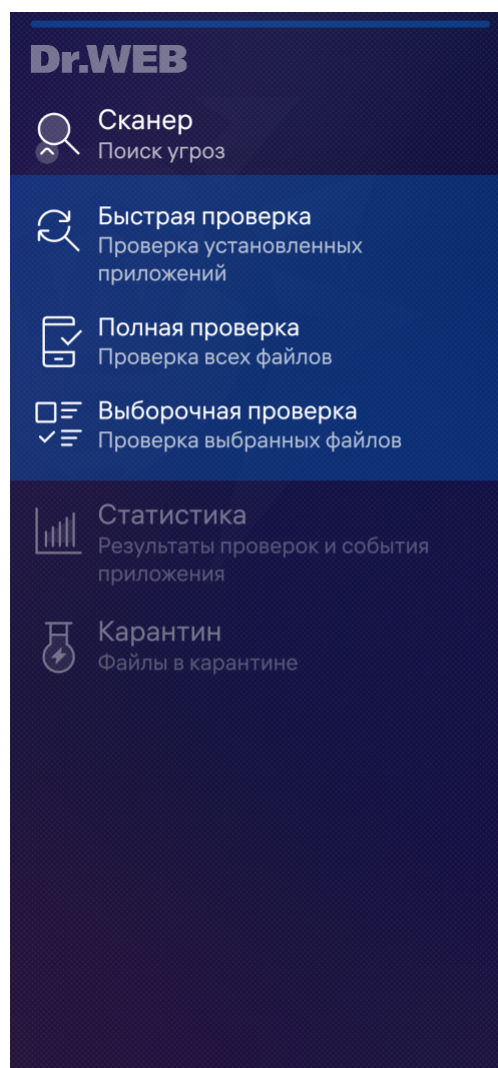


Рисунок 16. Сканер Dr.Web

Проверка

Чтобы проверить систему, на [главной странице](#) приложения выберите пункт **Сканер**, затем в открывшемся подменю (см. [Рисунок 16](#)) выполните одно из следующих действий:

- Чтобы запустить сканирование только установленных приложений, выберите пункт **Быстрая проверка**.
- Чтобы запустить сканирование всех файлов, выберите пункт **Полная проверка**.
- Чтобы проверить отдельные файлы или папки, выберите пункт **Выборочная проверка**, затем выберите необходимые объекты в появившемся списке объектов файловой системы. Чтобы открыть папку, коснитесь ее. Чтобы выбрать папку, коснитесь и удерживайте ее (см. [Рисунок 17](#)). Чтобы выбрать файл, коснитесь его. После выбора объектов коснитесь кнопки **Подтвердить**.

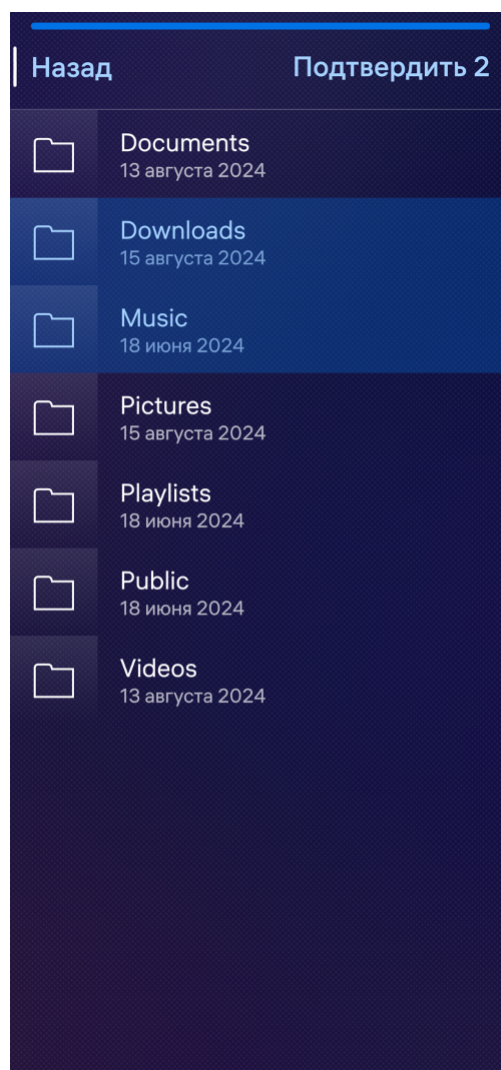


Рисунок 17. Выборочная проверка

Остановка проверки

Чтобы остановить проверку, коснитесь точки в левом верхнем углу.

Чтобы отменить остановку проверки, коснитесь [таймера отмены](#) в верхней части экрана (см. [Рисунок 18](#)).

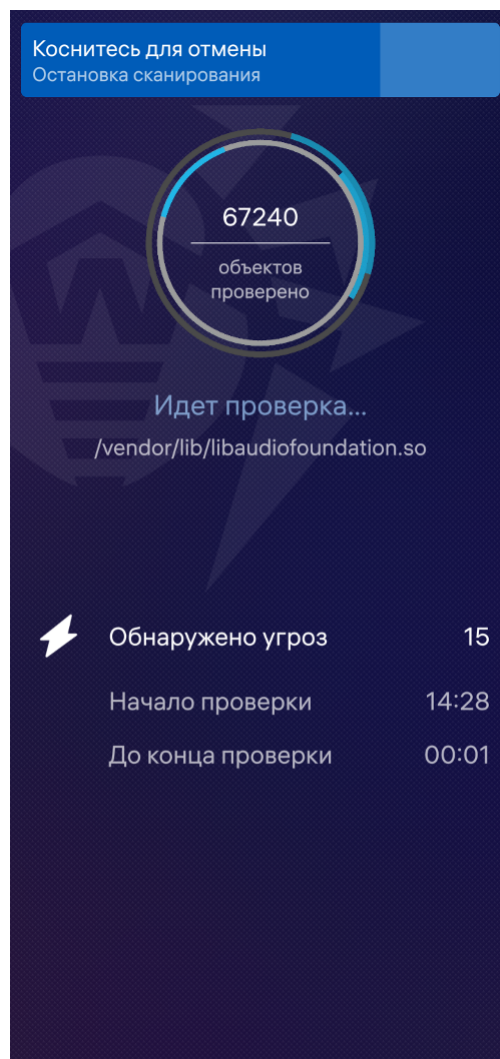


Рисунок 18. Остановка проверки

Настройки Сканера Dr.Web

Вы можете изменить настройки Сканера Dr.Web (см. раздел [Настройки Сканера](#)).

Статистика Сканера

Приложение регистрирует события, связанные с работой Сканера Dr.Web. Они отображаются в подразделе **События** в разделе **Статистика** и в зависимости от настроек фильтрации отсортированы либо по дате, либо по алфавиту (см. раздел [Статистика](#)).

Результаты проверки

После завершения проверки вы можете просмотреть результаты проверки, коснувшись панели **Коснитесь, чтобы обезвредить** (см. [Рисунок 19](#)) или точки в левом верхнем углу.



Если вы свернули приложение во время проверки Сканером Dr.Web, коснитесь обложки, чтобы вернуться на страницу **Проверка завершена**, с которой вы можете перейти к результатам проверки.

Если вы полностью остановили работу приложения во время проверки Сканером Dr.Web, при следующем запуске приложения на главной странице вы увидите оповещение о количестве обнаруженных угроз. Коснитесь его, чтобы перейти к результатам проверки. Если угрозы не были обнаружены, оповещение не появится. Чтобы просмотреть результаты проверки в этом случае, повторно откройте страницу выбранного ранее типа проверки.

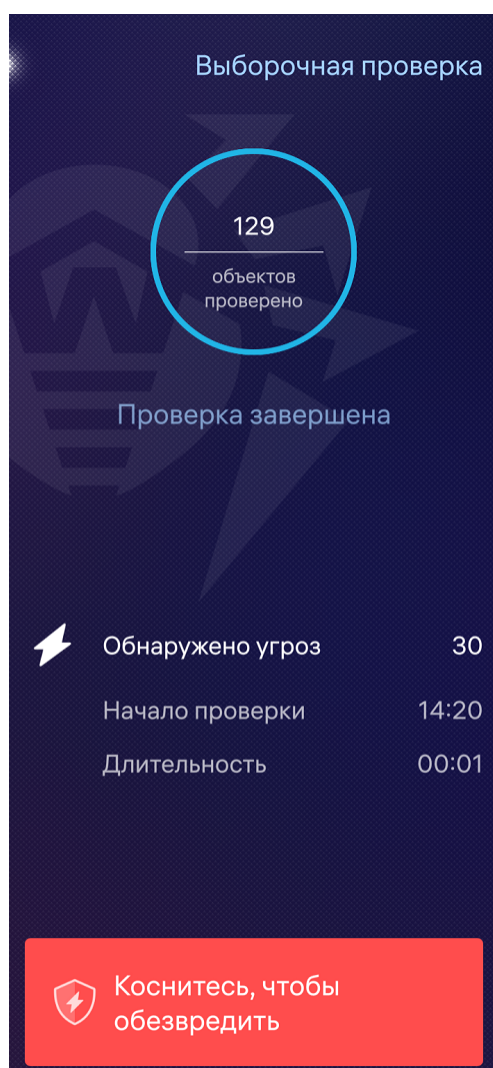


Рисунок 19. Проверка завершена

Обезвреживание угроз

Результаты проверки отображаются на странице **Угрозы**, где вы можете ознакомиться со списком угроз и обезвредить их.



Обезвреживание всех угроз одновременно

Чтобы удалить сразу все угрозы

1. На странице **Угрозы** коснитесь ниже светящейся полосы и проведите вниз.
2. Выберите **Удалить все** (см. [Рисунок 20](#)).

Чтобы переместить в карантин сразу все угрозы

1. На странице **Угрозы** коснитесь ниже светящейся полосы и проведите вниз.
2. Выберите **Все в карантин** (см. [Рисунок 20](#)).



Системные угрозы невозможно удалить или переместить в карантин, так как это может отразиться на работе устройства.

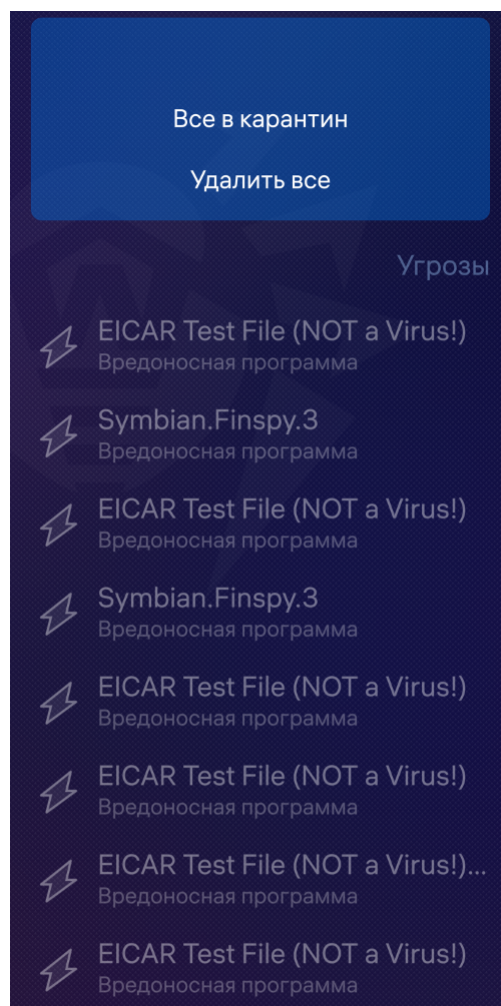


Рисунок 20. Обезвреживание угроз



Обезвреживание угроз по одной

Чтобы просмотреть действия, доступные для угрозы, коснитесь имени угрозы. Выберите одно из действий:

- **В карантин**, чтобы переместить угрозу в изолированную папку (см. раздел [Карантин](#)).
- **Удалить**, чтобы полностью удалить угрозу из памяти устройства. Если угроза обнаружена в установленном приложении, удаление для нее невозможно. В этом случае опция **Удалить** недоступна.
- **Игнорировать**, чтобы временно оставить угрозу нетронутой.
- **Подробности**, чтобы открыть страницу с описанием обнаруженного объекта на сайте компании «Доктор Веб».

8.2. Статистика

Dr.Web регистрирует остановку или завершение всех типов проверок, [обновления вирусных баз](#) и действия, примененные к обнаруженным угрозам.

Для просмотра статистики на [главной странице](#) выберите пункт **Статистика**.



Пользователям доступна только опция **Сохранить журнал**. Чтобы просматривать статистику, вы должны обладать правами администратора (см. раздел [Учетные записи](#)).

Просмотр статистики

На странице **Статистика** находятся два информационных раздела (см. [Рисунок 21](#)):

- **Всего** содержит информацию об общем количестве проверенных файлов, обнаруженных и обезвреженных угроз.
- **События** отражает следующую информацию:
 - завершение или остановка полной, быстрой, выборочной проверок;
 - удачное или неудачное обновление вирусных баз;
 - действия, примененные к обнаруженным угрозам — удаление, перемещение в карантин, игнорирование угрозы.

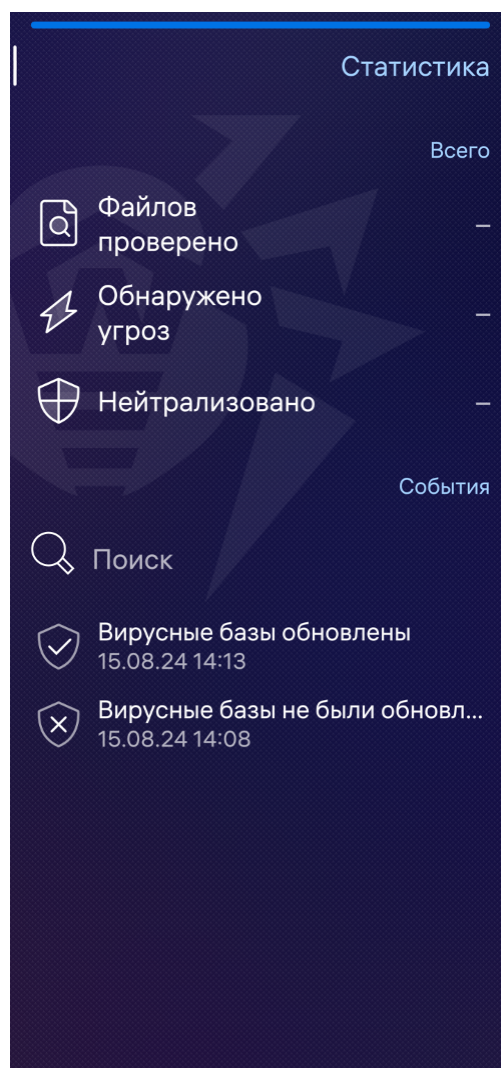


Рисунок 21. Статистика

Просмотр информации о событии

Коснувшись имени события, вы можете просмотреть информацию о событии:

- тип события,
- дата и время события,
- инициатор события.

В зависимости от типа события может быть доступна дополнительная информация:

- количество обнаруженных угроз,
- статус события,
- количество проверенных файлов,
- тип обнаруженной угрозы,
- имя обнаруженной угрозы,



- имя вредоносного файла,
- путь к файлу.

Поиск по событиям

Вы можете искать интересующие вас события:

- по имени события,
- по дате события,
- по времени события,
- по имени угрозы,
- по имени вредоносного файла.

Чтобы искать по событиям в статистике, введите запрос в строку **Поиск** в разделе **События** (см. [Рисунок 21](#)).

Сортировка событий

События в статистике можно сортировать по дате или алфавиту.

Чтобы сортировать события по дате или алфавиту

1. На странице **Статистика** коснитесь ниже светящейся полосы и проведите вниз.
2. В появившемся меню выберите пункт **Фильтрация событий** (см. [Рисунок 22](#)).
3. На открывшейся странице в пункте **Сортировать по** выберите способ фильтрации.

Также вы можете просмотреть только определенные события, если на странице **Фильтрация событий** выберите любое событие в пункте **Показать**.

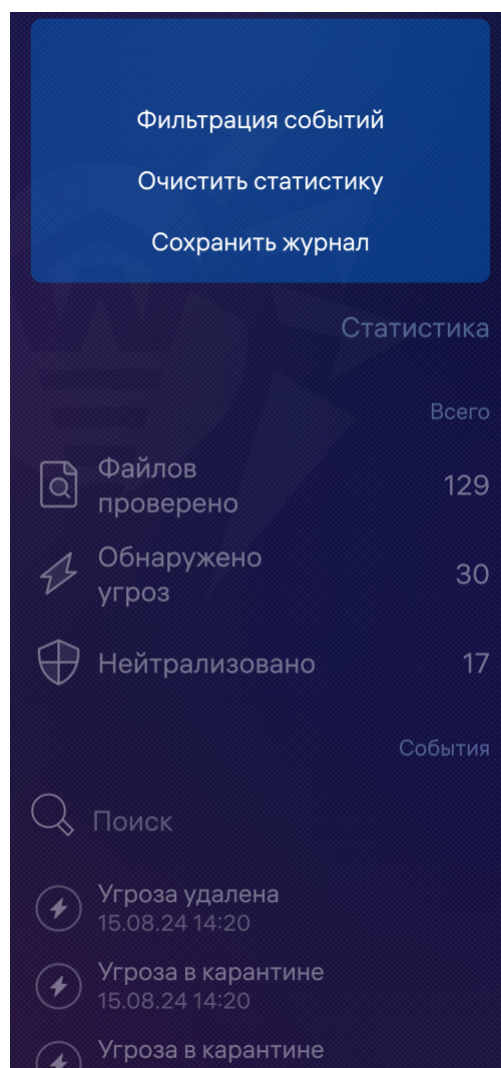


Рисунок 22. Меню Статистики

Очистка статистики

Чтобы удалить всю собранную статистику работы приложения, на странице **Статистика** коснитесь ниже светящейся полосы и проведите вниз, а затем выберите пункт **Очистить статистику** (см. [Рисунок 22](#)).

Сохранение журнала событий

Вы можете сохранить журнал событий приложения для анализа в случае возникновения проблем при работе с приложением.

1. На странице **Статистика** коснитесь ниже светящейся полосы и проведите вниз.
2. Выберите пункт **Сохранить журнал**.



3. Журнал сохраняется в файле `DrWeb_Log.txt`, расположенном во внутренней памяти устройства в папке `/home/<user>/Documents/drweb/`, где `<user>` обозначает текущего пользователя.

8.3. Карантин

Обнаруженные угрозы можно переместить в карантин — особую папку, предназначенную для изоляции и безопасного хранения угроз (см. [Рисунок 23](#)).

В правом верхнем углу страницы **Карантин** отображается общий размер файлов, перемещенных в карантин.

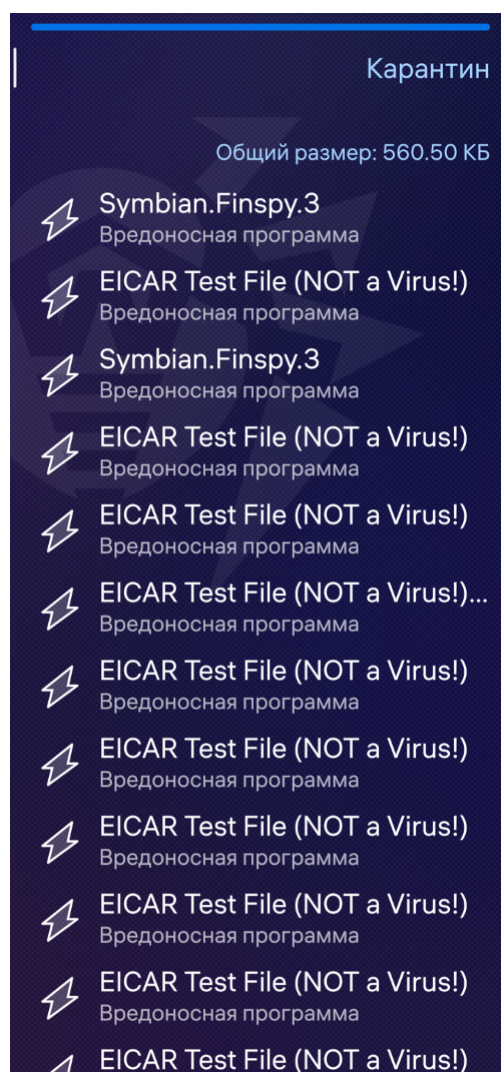


Рисунок 23. Карантин

Просмотр списка объектов в карантине

Чтобы просмотреть список угроз, перемещенных в карантин, на [главной странице](#) коснитесь пункта **Карантин**.



Откроется список всех угроз, находящихся в карантине.

Просмотр информации об угрозах

Коснувшись имени угрозы в списке, вы можете просмотреть следующую информацию:

- имя файла,
- тип угрозы,
- путь к файлу,
- дата и время перемещения в карантин.

Доступные опции

Чтобы просмотреть опции, коснитесь угрозы в списке и удерживайте ее.

Для угроз доступны следующие опции (см. [Рисунок 24](#)):

- **Восстановить** — для возвращения файла в ту папку, в которой файл находился до перемещения. Пользуйтесь этой функцией, только если вы уверены, что файл безопасен.
- **Удалить** — для удаления файла из карантина и из системы.
- **Подробности** — для просмотра описания угрозы на сайте компании «Доктор Веб».

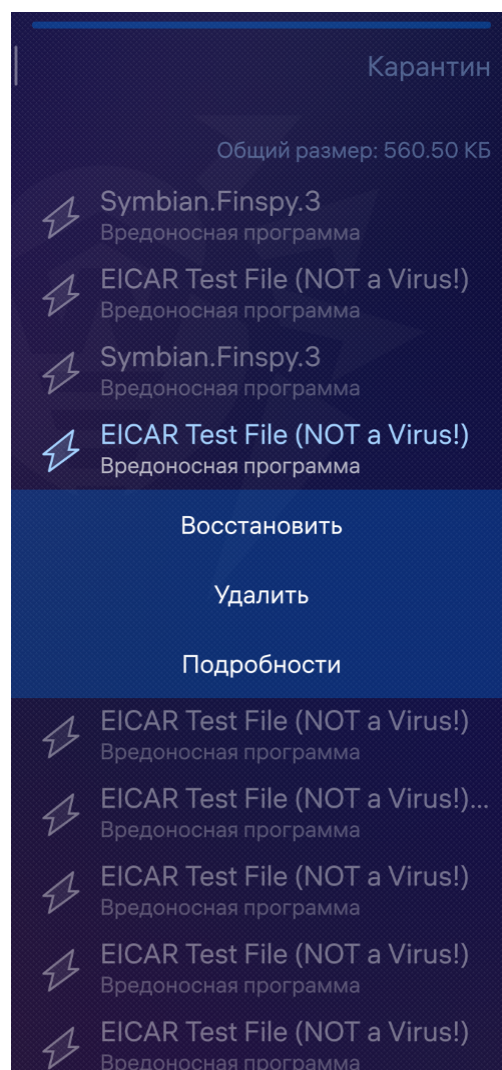


Рисунок 24. Действия для угрозы

Удаление всех объектов из карантина

Чтобы удалить все объекты, перемещенные в карантин

1. На странице **Карантин** коснитесь ниже светящейся полосы и проведите вниз.
2. Выберите **Удалить все** (см. [Рисунок 25](#)).

Чтобы отменить удаление, коснитесь [таймера отмены](#) в верхней части экрана приложения.

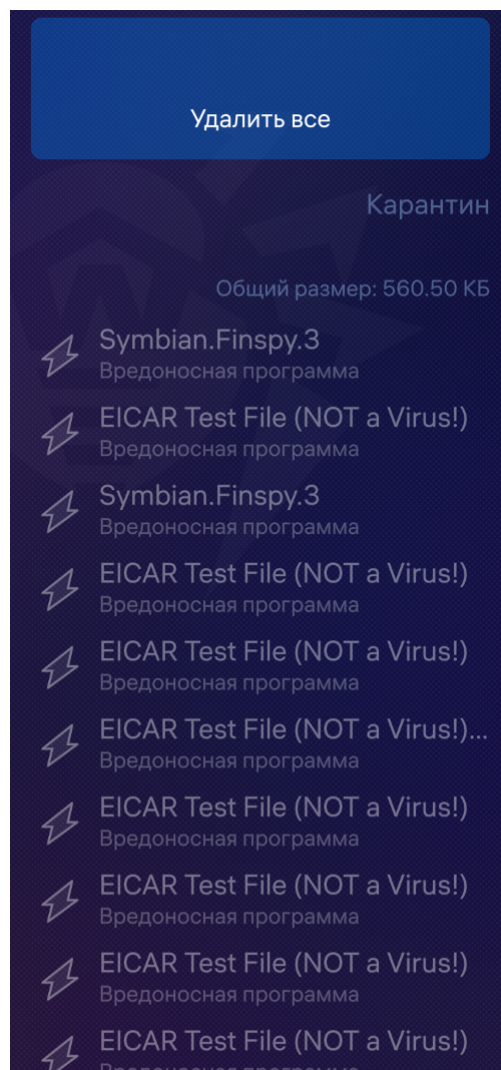


Рисунок 25. Удаление всех угроз из карантина



9. Настройки

Чтобы перейти к настройкам приложения, на [главной странице](#) приложения коснитесь ниже светящейся полосы и проведите по экрану вниз, а затем выберите пункт **Настройки** (см. [Рисунок 26](#)).

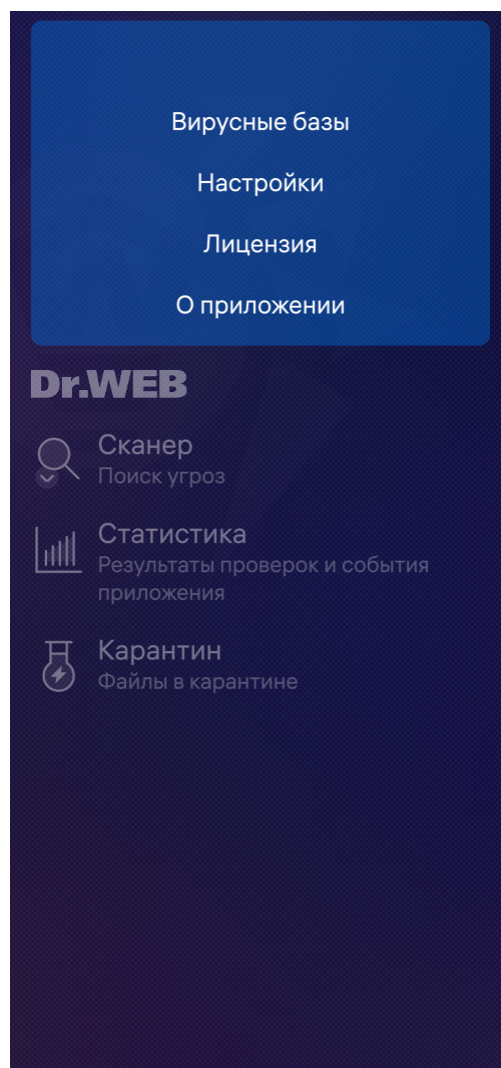


Рисунок 26. Настройки

На странице **Настройки** доступны следующие разделы:

- **Общие настройки** — позволяет включить и отключить звуковые оповещения.
- **Сканер** — позволяет настроить компонент Сканер, который проверяет устройство по запросу пользователя (см. раздел [Настройки Сканера](#)).
- **Вирусные базы** — позволяет управлять автоматическим обновлением вирусных баз и использованием мобильного интернета для обновления (см. раздел [Настройки обновлений](#)).



9.1. Общие настройки

В разделе **Общие настройки** вы можете настроить звуковые оповещения об обнаружении угроз, их удалении или перемещении в карантин ( — опция отключена,  — опция включена).

По умолчанию звуковые оповещения включены.

9.2. Настройки Сканера

Раздел **Сканер** позволяет задать параметры проверки, выполняемой Сканером Dr.Web.

- Чтобы включить проверку файлов в архивах, в разделе **Сканер** коснитесь поля **Файлы в архивах** ( — опция отключена,  — опция включена). По умолчанию проверка архивов включена.
- Чтобы включить/отключить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе, программ взлома, программ-шуток, программ дозвона и уязвимых программ), коснитесь полей **Рекламные программы** и **Потенциально опасные программы** соответственно ( — опция отключена,  — опция включена). По умолчанию обе опции включены.

9.3. Настройки обновлений

В разделе **Вирусные базы** вы можете разрешить или запретить обновление вирусных баз с использованием мобильного трафика, а также настроить параметры автоматического обновления баз.

Чтобы разрешить или запретить использование мобильной сети при загрузке обновлений

- В разделе **Вирусные базы** коснитесь поля **Обновлять только по Wi-Fi** ( — опция отключена,  — опция включена). По умолчанию опция включена.

Если активные сети Wi-Fi не будут обнаружены, вам будет предложено изменить настройку. Изменение этой настройки не влияет на использование мобильной сети остальными функциями приложения и мобильного устройства.



При обновлении происходит загрузка данных по сети. За передачу данных может взиматься дополнительная плата. Уточняйте подробности у вашего мобильного оператора.



Чтобы разрешить или запретить автоматическое обновление вирусных баз

- В разделе **Вирусные базы** коснитесь поля **Автоматическое обновление** ( — опция отключена,  — опция включена). По умолчанию опция включена.

Дополнительно вы можете изменить следующие настройки обновления:

- Чтобы изменить периодичность проверки на устаревание вирусных баз и их обновления, коснитесь поля **Интервал обновления** и выберите нужное вам значение из доступных в выпадающем списке: **30 минут**, **1 час**, **4 часа**, **8 часов** или **1 день**. По умолчанию проверка на устаревание баз и автоматическое обновление будут производиться каждые 4 часа.
- Чтобы изменить протокол подключения к серверу обновления, коснитесь поля **Соединение** и выберите тип устанавливаемого соединения в выпадающем списке: **Защищенное (HTTPS)** или **Незащищенное (HTTP)**. Обновление вирусных баз будет производиться только по выбранному протоколу. По умолчанию обновление будет выполняться по протоколу HTTPS.

9.4. Сброс настроек

Вы можете в любой момент сбросить пользовательские настройки приложения и восстановить настройки по умолчанию.

Чтобы сбросить настройки

1. На странице **Настройки** коснитесь ниже светящейся полосы и проведите вниз.
2. Выберите пункт **Сброс настроек** (см. [Рисунок 27](#)).

Чтобы отменить сброс настроек, коснитесь [таймера отмены](#) в верхней части приложения.

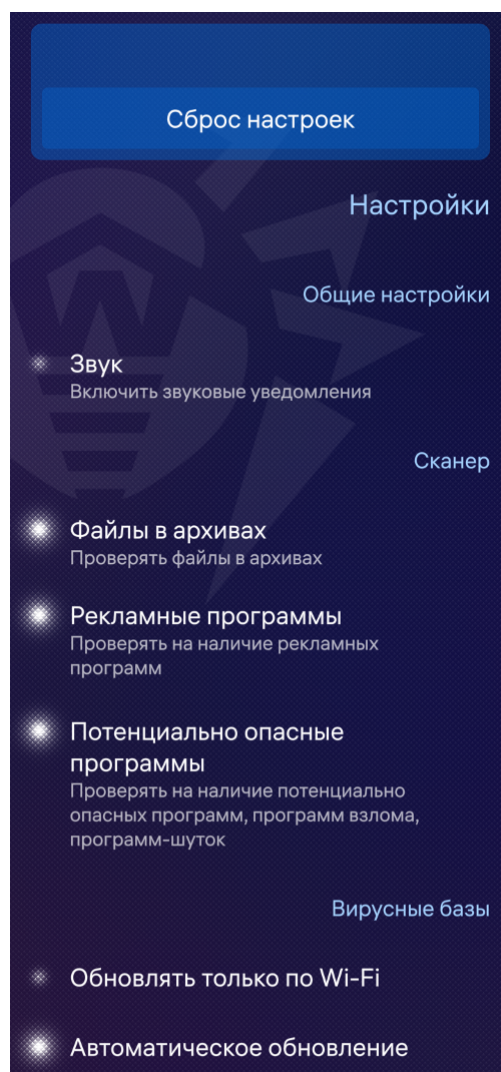


Рисунок 27. Сброс настроек



10. Обновление вирусных баз

Для обнаружения угроз безопасности Dr.Web использует специальные вирусные базы, в которых содержится информация обо всех информационных угрозах для устройств под управлением ОС Android и Аврора, известных специалистам компании «Доктор Веб». Базы требуют периодического обновления, поскольку новые вредоносные программы появляются регулярно. Для этого в приложении реализована возможность обновления вирусных баз через интернет.

Обновление

По умолчанию вирусные базы обновляются автоматически. Отключить автоматическое обновление или изменить его частоту и тип соединения, устанавливаемого с сервером обновлений, можно в настройках приложения в разделе [настройки обновления](#).

Если автоматическое обновление отключено, приложение выполняет проверку на устаревание вирусных баз с периодичностью, заданной в настройках. По умолчанию это каждые 4 часа.

Если вирусные базы устарели, в приложении появится соответствующее оповещение в нижней части экрана. Оповещение будет отображаться до тех пор, пока вирусные базы не будут обновлены. Коснитесь оповещения, чтобы обновить вирусные базы вручную. Вы также можете запустить обновление из раздела меню **Вирусные базы**.



Сразу после установки приложения рекомендуется выполнить обновление вирусных баз, чтобы Dr.Web мог использовать самую свежую информацию об известных угрозах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляются сразу же, как только специалисты вирусной лаборатории компании «Доктор Веб» обнаруживают новые угрозы, иногда до нескольких раз в час.

Чтобы запустить обновление

1. На [главной странице](#) приложения коснитесь ниже светящейся полосы и проведите вниз.
2. В открывшемся меню выберите **Вирусные базы**.
3. В открывшемся окне вы увидите статус вирусных баз и дату последнего обновления. Если вирусные базы устарели, отобразится соответствующий статус.
4. На странице **Вирусные базы** коснитесь ниже светящейся полосы и проведите вниз.
5. Выберите пункт **Проверить обновления** (см. [Рисунок 28](#)).

Обновление запустится автоматически.

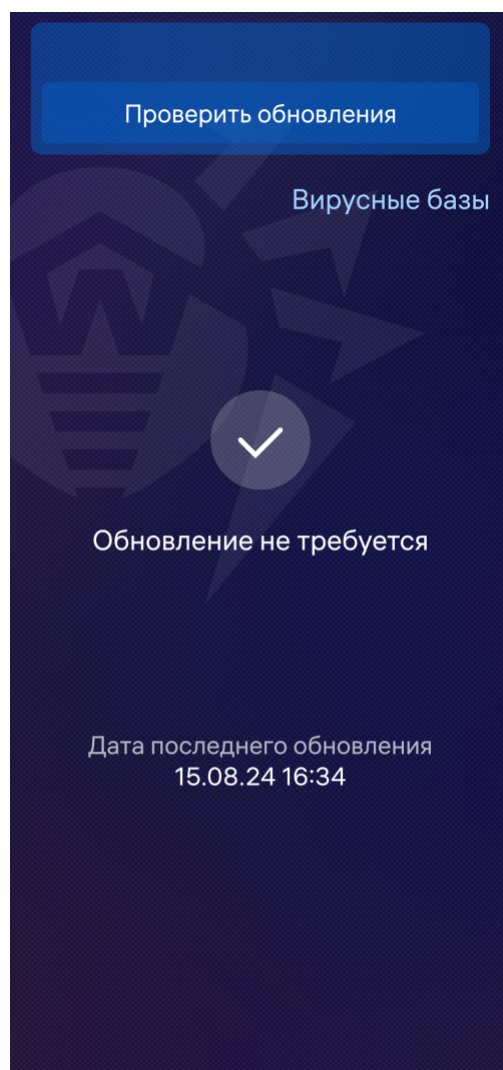


Рисунок 28. Обновление вирусных баз



11. Обновление Dr.Web

Обновление через RuStore

По умолчанию в RuStore включено автоматическое обновление приложений. Если вы отключили автоматическое обновление, вы можете запустить обновление вручную:

1. Откройте RuStore.
2. В списке приложений найдите Dr.Web и нажмите  **Обновить** или нажмите на карточку приложения и в открывшемся окне нажмите **Обновить**.



Кнопка **Обновить** доступна, если новая версия приложения уже вышла.

Для начала работы с приложением нажмите кнопку  **Открыть**.



12. 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:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу <https://download.drweb.com/doc/>.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. 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»:

1. Заполните веб-форму в соответствующей секции раздела <https://support.drweb.com/>.
2. 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/>.

