Dr.WEB

Enterprise Security Suite

Управление станциями под Android

Dr.Web Enterprise Security Suite. Управление станциями под Android
Версия 12.0
Руководство администратора
05.03.2021

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

Глава 1. Введение

1.1. Назначение документа

Данное руководство является частью пакета документации администратора антивирусной сети, описывающей детали реализации комплексной антивирусной защиты компьютеров и мобильных устройств компании с помощью Dr.Web Enterprise Security Suite.

Руководство адресовано администратору антивирусной сети — сотруднику организации, которому поручено руководство антивирусной защитой рабочих станций и серверов этой сети.

В руководстве приведена информация о централизованной настройке антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web. Руководство описывает настройки антивирусного решения Dr.Web для Android и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство пользователя** антивирусного решения Dr.Web для Android содержит информацию о настройке антивирусного ПО, осуществляемой непосредственно на станции.
- **Документация администратора** антивирусной сети Dr.Web Enterprise Security Suite (включает **Руководство администратора**, **Руководство по установке** и **Приложения**) содержит основную информацию по установке и настройке антивирусной сети и, в частности, по работе с Центром управления безопасностью Dr.Web.

Перед прочтением документов убедитесь, что это последняя версия руководств. Руководства постоянно обновляются, и последнюю их версию можно найти на официальном сайте компании «Доктор Веб» https://download.drweb.com/doc/.

1.2. Условные обозначения

В данном руководстве используются следующие условные обозначения:

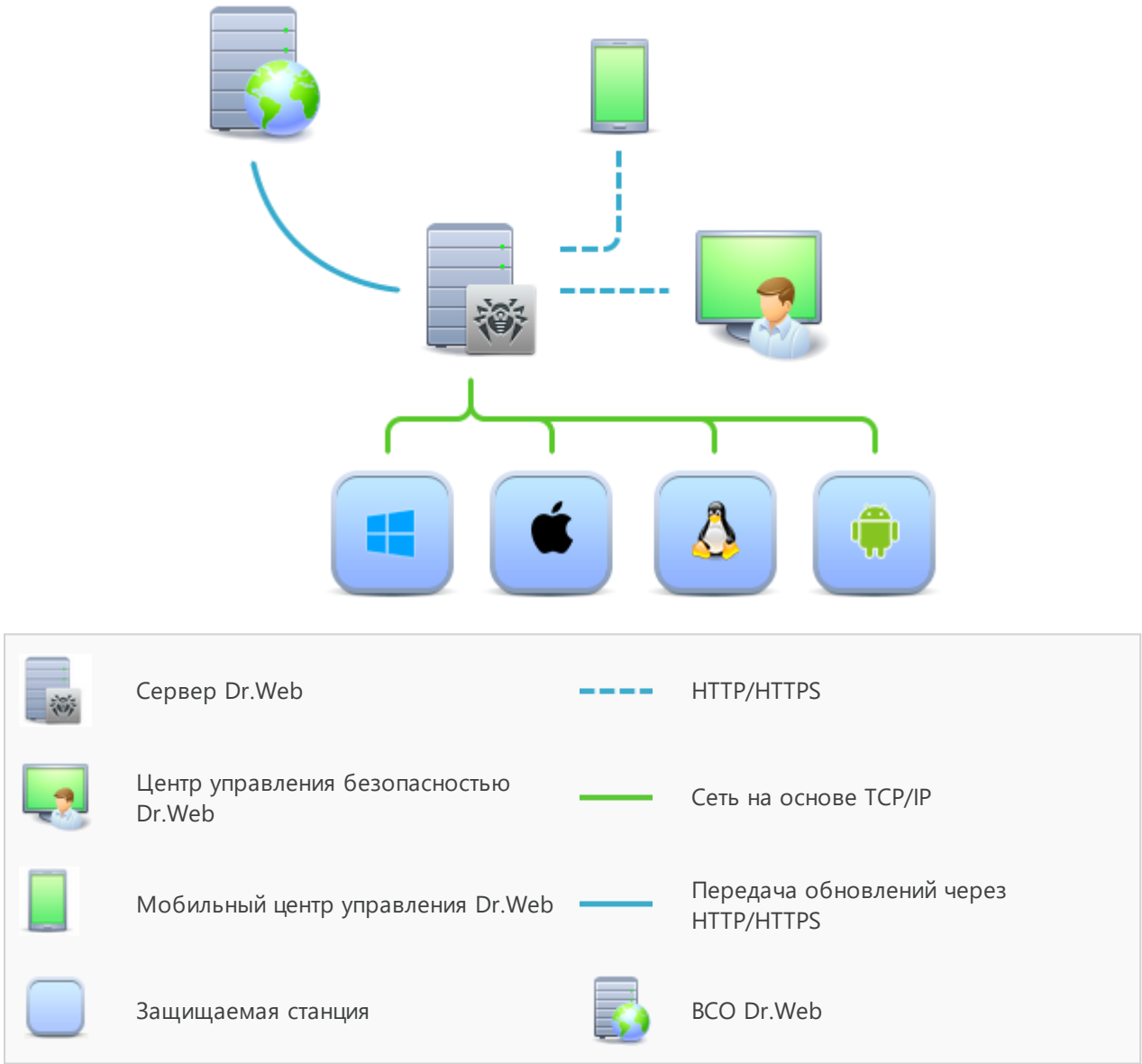
Обозначение	Комментарий
	Важное замечание или указание.
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими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

Глава 2. Dr.Web Enterprise Security Suite

2.1. О продукте

Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой как внутренней сети компании, включая мобильные устройства, так и домашних компьютеров сотрудников.

Совокупность компьютеров и мобильных устройств, на которых установлены взаимодействующие компоненты Dr.Web Enterprise Security Suite, представляет собой единую *антивирусную сеть*.



Логическая структура антивирусной сети

Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на компьютеры и мобильные устройства пользователей и администраторов, а также на компьютеры, выполняющие функции серверов ЛВС. Компоненты антивирусной сети обмениваются информацией, используя сетевые протоколы TCP/IP. Антивирусное ПО на защищаемые станции возможно устанавливать (и впоследствии управлять ими) как через ЛВС, так и через Интернет.

2.2. Защита станций сети

Защита рабочих станций осуществляется антивирусными пакетами Dr.Web, разработанными для соответствующих операционных систем.

Защищаемый компьютер с установленным антивирусным пакетом, в соответствии с его функциями в антивирусной сети, именуется *рабочей станцией* антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией или мобильным устройством, так и сервером локальной сети.

Антивирусные пакеты устанавливаются на защищаемых станциях и подключаются к Серверу Dr.Web. Каждая станция входит в состав одной или нескольких групп, зарегистрированных на этом Сервере. Передача информации между станцией и Сервером осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Локальная установка антивирусного пакета для ОС Android осуществляется на мобильном устройстве пользователя. Может производиться как администратором, так и пользователем.

Подробное описание процедур установки антивирусных пакетов на рабочие станции приведено в Руководстве по установке Dr.Web Enterprise Security Suite.

Управление

При поддержке связи с Сервером Dr.Web администратору доступны следующие возможности, реализуемые антивирусным пакетом на станции:

- Централизованная настройка Антивируса на рабочих станциях при помощи Центра управления.

  При этом администратор может как запретить, так и оставить возможность пользователю самостоятельно изменять настройки Антивируса на станции.

- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии станции.

Обновление

Сервер Dr.Web загружает обновления и распространяет их на подключенные к нему станции. Таким образом автоматически устанавливается, поддерживается и регулируется оптимальная стратегия защиты от угроз независимо от уровня квалификации пользователей рабочих станций.

В случае временного отключения рабочей станции от антивирусной сети Антивирус на станции использует локальную копию настроек, антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), но обновление ПО не производится. Если для станции разрешено функционирование в *Мобильном режиме*, при потере связи с Сервером будет доступно обновление вирусных баз непосредственно с серверов ВСО.

Принцип работы станций в мобильном режиме описан в Руководстве администратора Dr.Web Enterprise Security Suite.

Глава 3. Dr.Web для Android

Dr.Web для Android надежно защищает мобильные устройства, работающие под управлением операционной системы Android™, а также телевизоры, медиапроигрыватели и игровые консоли, работающие на платформе Android TV™, от различных вирусных угроз, созданных специально для этих устройств.

В приложении применены наиболее передовые разработки и технологии «Доктор Веб» по обнаружению и обезвреживанию вредоносных объектов, которые могут представлять угрозу функционированию устройства и его информационной безопасности.

Dr.Web для Android использует Origins Tracing™ for Android — уникальную технологию детектирования вредоносных программ для платформы Android. Данная технология позволяет определять новые семейства вирусов на основе базы знаний о предыдущих угрозах. Origins Tracing for Android способна распознавать как перекомпилированные вирусы, такие как Android.SMSSend, Android.MobileSpy, так и приложения, зараженные Android.ADRD, Android.Geinimi, Android.DreamExploid. Названия угроз, обнаруженных при помощи Origins Tracing for Android, имеют вид Android.VirusName.origin.

3.1. Компоненты Dr.Web для Android

Для защиты станций под ОС Android предоставляются следующие антивирусные компоненты:

Сканер Dr.Web

Сканирование мобильного устройства по запросу пользователя, а также согласно расписания. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления.

SpIDer Guard

Постоянная проверка файловой системы в режиме реального времени. Сканирование всех файлов при попытке их сохранения в памяти мобильного устройства.

Фильтр звонков и СМС

Фильтрация СМС-сообщений и телефонных звонков позволяет блокировать нежелательные сообщения и звонки, например, рекламные рассылки, а также звонки и сообщения с неизвестных номеров.

Антивор

Обнаружение местоположения или оперативная блокировка функций мобильного устройства в случае его потери или кражи.

URL-фильтр

URL-фильтр позволяет оградить пользователя мобильного устройства от нежелательных интернет-ресурсов.

Брандмауэр (настройки доступны только на мобильном устройстве)

Защита мобильного устройства от несанкционированного доступа извне и предотвращение утечки важных данных по сети. Контроль подключения и передачи данных по сети Интернет и блокировка подозрительных соединений на уровне пакетов и приложений.

Аудитор безопасности (настройки доступны только на мобильном устройстве)

Диагностика и анализ безопасности мобильного устройства и устранение выявленных проблем и уязвимостей.

Фильтр приложений

Запрет запуска на мобильном устройстве тех приложений, которые не включены в список разрешенных администратором.

3.2. Настройка Dr.Web для Android

Чтобы просмотреть или изменить настройки антивирусных компонентов на рабочей станции

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В открывшемся окне в иерархическом списке нажмите на название станции под ОС Android или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Конфигурация**, в подразделе **Android** выберите требуемый компонент:
   - Dr.Web для Android
   - SpIDer Guard
   - Антиспам
   - Антивор
   - Фильтр приложений
   - Сканер
   - URL-фильтр
4. Откроется окно настроек соответствующего антивирусного компонента.

   Управление настройками антивирусных компонентов через Центр управления имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса на станции:

   - для управления отдельными параметрами используйте кнопки, расположенные справа от соответствующих настроек:

Установить в начальное значение — восстановить значение, которое параметр имел до редактирования (последнее сохраненное значение).

Сбросить в значение по умолчанию — установить для параметра значение по умолчанию.

- для управления совокупностью всех параметров раздела используйте кнопки на панели инструментов:

  Установить все параметры в начальные значения — восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

  Установить все параметры в значения по умолчанию — установить для всех параметров данного раздела значения, заданные по умолчанию.

  Распространить эти настройки на другой объект — скопировать настройки из данного раздела в настройки другой станции, группы или нескольких групп и станций.

  Установить наследование настроек от первичной группы — удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы.

  Скопировать настройки из первичной группы и установить их в качестве персональных — скопировать настройки данного раздела из первичной группы и задать их для выбранных станций. Наследование при этом не устанавливается, и настройки станции считаются персональными.

  Экспортировать настройки из данного раздела в файл — сохранить все настройки из данного раздела в файл специального формата.

  Импортировать настройки в данный раздел из файла — заменить все настройки в данном разделе настройками из файла специального формата.

5. После внесения каких-либо изменений в настройки при помощи Центра управления, чтобы принять эти изменения, нажмите **Сохранить**. Настройки будут переданы на станции. Если станции были отключены в момент внесения изменений, настройки будут переданы в момент подключения станций к Серверу.

Администратор может запретить пользователю редактировать настройки на станции (см. раздел Права пользователей станции в Руководстве администратора Dr.Web Enterprise Security Suite). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.2.1. Dr.Web для Android

Общие настройки Dr.Web для Android и настройки обновлений задаются в разделе **Dr.Web для Android**.

Общие

- Установите флажок **Включить звуковые уведомления**, чтобы включить использование звуковых уведомлений при обнаружении угрозы, ее удалении или перемещении в карантин.
- Установите флажок **Отображать значок Dr.Web в строке состояния**, чтобы включить отображение значка приложения в строке состояния при включении SpIDer Guard.
- Установите флажок **Отслеживать местоположение**, чтобы разрешить Серверу получать информацию о текущих координатах устройства.

  В списке **Периодичность передачи координат** выберите значение, в соответствии с которым будут обновляться данные о местоположении устройства. Минимальное значение составляет 5 минут.

Для станций под ОС Android возможна настройка автоматического определения местоположения. Подробную информацию по использованию и настройке данной функции вы можете найти в документе Приложения к Руководству администратора Dr.Web Enterprise Security Suite, в разделе Автоматическое определение местоположения станции под ОС Android.

Обновления

- Установите флажок **Обновлять вирусные базы только по Wi-Fi**, чтобы не использовать при загрузке обновлений мобильные сети. Если активные сети Wi-Fi не будут обнаружены, вам будет предложено воспользоваться сетями 3G или GPRS. Изменение данной настройки не влияет на использование мобильных сетей остальными функциями приложения и мобильного устройства.
- Установите флажок **Проверять наличие новой версии**, чтобы включить проверку доступности новой версии при каждом обновлении вирусных баз приложения. При появлении новой версии приложения вы получите стандартное уведомление и сможете оперативно загрузить и установить ее.

3.2.2. SpIDer Guard

SpIDer Guard проверяет файловую систему в режиме реального времени, сканирует все файлы при попытке их сохранения в памяти устройства, защищая тем самым систему от появления угроз безопасности.

Настройки SpIDer Guard задаются в разделе **SpIDer Guard**.

- Установите/снимите флажок **Включить SpIDer Guard**, чтобы включить/отключить SpIDer Guard. При включении SpIDer Guard начинает защищать систему. Он продолжает работать независимо от того, запущено приложение или нет.
- Установите флажок **Проверять архивы**, чтобы включить проверку файлов в архивах. По умолчанию проверка архивов отключена. Включение проверки архивов может

сказаться на быстродействии системы и увеличить расход заряда батареи. При этом отключение проверки архивов не сказывается на уровне защиты, поскольку SpIDer Guard проверяет установочные файлы Android (.apk) в любом случае, независимо от установленного значения данного параметра.

- Установите флажок **Проверять SD-карты**, чтобы включить проверку SD-карты при каждом ее подключении к устройству.
- Установите флажки **Проверять на наличие рекламных программ** и **Проверять на наличие потенциально опасных программ**, чтобы включить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе программ взлома и программ-шуток).

3.2.3. Антиспам

Фильтрация звонков и СМС позволяет блокировать нежелательные звонки и сообщения, например, рекламные рассылки, а также звонки и сообщения со скрытых номеров.

Настройки фильтрации звонков и СМС задаются в разделе **Антиспам**.

В списке **Текущий профиль** выберите режим фильтрации:

- **Принимать все**. Данный режим отключает фильтрацию, в результате чего все входящие звонки и СМС-сообщения будут приняты.
- **Блокировать все**. В данном режиме все входящие звонки и СМС-сообщения будут заблокированы.
- **Корпоративный черный список**. При выборе данного режима будут заблокированы входящие звонки и СМС-сообщения только с номеров, добавленных в черный список.

  В данном режиме доступен флажок **Скрытые номера запрещены**, при установке которого все входящие звонки и СМС со скрытых номеров будут блокироваться.
- **Корпоративный белый список**. При выборе данного режима будут пропущены входящие звонки и СМС-сообщения только с номеров, добавленных в белый список.

  В данном режиме доступен флажок **Скрытые номера разрешены**, при установке которого все входящие звонки и СМС со скрытых номеров будут разрешены.

3.2.4. Антивор

Антивор Dr.Web позволяет обнаружить местоположение или оперативно заблокировать функции мобильного устройства в случае его потери или кражи.

Настройки Антивора Dr.Web задаются в разделе **Антивор**.

- В поле **Пароль** введите пароль (он должен содержать не менее четырех символов). Этот пароль будет использоваться для управления всеми функциями Антивора Dr.Web. При необходимости вы можете включить опцию просмотра символов при вводе пароля. Для этого нажмите значок справа от поля ввода.

- Установите флажок **Блокировать после перезагрузки**, чтобы заблокировать устройство в случае его перезагрузки.
- Установите флажок **Блокировать при замене SIM-карты**, чтобы в случае смены SIM-карты устройство пользователя было заблокировано.
- Установите флажок **Удалить данные после 10 ошибок при вводе пароля**, чтобы полностью стереть личную информацию с устройства после 10 ошибок при вводе пароля.
- В поле **Текст на экране заблокированного телефона** введите текст сообщения, например, координаты для связи для возвращения потерянного мобильного устройства.
- В список **Список друзей** добавьте телефонные номера, на которые можно настроить отправку СМС-команд без указания пароля. Кроме того, с этих номеров можно отправить СМС-команду отключения Антивора Dr.Web и сброса установленного для него пароля.
- Установите флажок **Сообщить друзьям о замене SIM-карты**, чтобы информировать друзей о смене SIM-карты на мобильном устройстве.

3.2.5. Фильтр приложений

В разделе **Фильтр приложений** вы можете задать список приложений, которые могут запускаться на мобильных устройствах, подключенных к антивирусной сети.

При использовании данной опции все остальные приложения (за исключением системных), не входящие в заданный список, не смогут запускаться на мобильном устройстве пользователя.

Чтобы настроить список разрешенных приложений

Перед настройкой списка разрешенных приложений убедитесь, что вы установили флажок в пункте **Изменение конфигурации Фильтра приложений Dr.Web** в разделе **Права** для рабочих станций под Android. В противном случае раздел **Администрирование** не отобразится на мобильном устройстве пользователя.

1. На одном из мобильных устройств, подключенных к Серверу, задайте список разрешенных приложений:
   a) На главном экране приложения Dr.Web, установленного на мобильном устройстве, откройте раздел **Администрирование**.
   b) Выберите приложения, которые будут доступны на устройстве.
   c) Нажмите **Разрешить выбранные**.

После того, как вы сохраните настройки на устройстве, они будут переданы на Сервер и сохранены как персональные настройки для данного устройства.

2. В Центре управления откройте раздел **Фильтр приложений** (см. Настройка Dr.Web для Android) для станции с персональными настройками, заданными на шаге 1.

   В разделе **Разрешенные приложения** отображается список приложений, полученный с устройства. Приложения определяются по следующим параметрам:

   - Имя приложения,
   - Имя пакета,
   - MD5 приложения.

3. Через настройки в Центре управления не разрешается:
   - Добавлять приложения в список разрешенных. Добавить приложение можно только через настройки мобильного устройства.
   - Редактировать параметры приложений в списке разрешенных.
4. Через настройки в Центре управления вы можете:
   a) Удалять приложения из списка разрешенных. Для этого нажмите кнопку напротив соответствующего приложения.

   > Если вы удалите все приложения из списка разрешенных, но сам Фильтр приложений оставите включенным, ни одно пользовательское приложение не сможет запуститься на мобильном устройстве.

   b) Разрешать те же приложения для другого мобильного устройства или группы устройств антивирусной сети. Для этого нажмите на панели инструментов данного раздела кнопку **Распространить эти настройки на другой объект**. Откроется окно с деревом антивирусной сети, выберите один или несколько объектов для распространения настроек и нажмите **Сохранить**.

   c) Отключать Фильтр приложений. Для этого снимите флажок **Включить фильтр приложений**.

   > Обратите внимание: если первоначально Фильтр приложений был отключен на станции, вы можете включить его в настройках в Центре управления, однако не сможете добавить приложения в список разрешенных. При этом ни одно пользовательское приложение не сможет запуститься на мобильном устройстве.
   >
   > Если целью фильтрации не является запрет всех пользовательских приложений, рекомендуется начинать настройку на мобильном устройстве, как описано в шаге 1 данной процедуры.

5. После редактирования настроек нажмите **Сохранить**. Изменения будут переданы на мобильное устройство.

3.2.6. Сканер

С помощью Сканера Dr.Web можно выполнить быструю или полную проверку файловой системы, а также проверить отдельные файлы и папки.

Настройки Сканера Dr.Web задаются в разделе **Сканер**.

Общие

- Установите флажок **Проверять архивы**, чтобы включить проверку файлов в архивах. По умолчанию проверка архивов отключена. Включение проверки архивов может замедлить работу системы и увеличить расход заряда батареи. При этом отключение проверки архивов не сказывается на уровне защиты, поскольку Сканер Dr.Web проверяет установочные файлы Android (.apk) в любом случае, независимо от установленного значения данного параметра.

Дополнительно

- Установите флажки **Проверять на наличие рекламных программ** и **Проверять на наличие потенциально опасных программ**, чтобы включить проверку системы на наличие рекламных программ и потенциально опасных программ (в том числе программ взлома и программ-шуток).

3.2.7. URL-фильтр

URL-фильтр позволяет оградить пользователя мобильного устройства от нежелательных интернет-ресурсов. С помощью URL-фильтра можно заблокировать доступ к различным категориям нерекомендованных и потенциально опасных сайтов.

Настройки URL-фильтра задаются в разделе **URL-фильтр**.

Чтобы заблокировать доступ к сайтам по категориям:

1. Установите флажок **Блокировать по категориям**.

   Флажок **Блокировать по категориям** включает URL-фильтр на мобильном устройстве. При этом блокируются сайты, известные как источники распространения вирусов.

2. Установите флажки напротив тех категорий сайтов, доступ к которым нужно заблокировать.

В продукте Dr.Web для Android начиная с версии 10.0.0 не используется опция блокировки категории «Известные источники вирусов». Изменение состояния флажка Центра управления **Источники распространения вирусов** игнорируется, настройка считается всегда включенной.

Данная опция может быть отключена только при отключении всего модуля URL-фильтр.

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/.