Dr.WEB

Enterprise Security Suite

Управление Microsoft Exchange Server

Dr.Web Enterprise Security Suite. Управление Microsoft Exchange Server
Версия 11.0
Руководство администратора
15.04.2020

ООО «Доктор Веб», Центральный офис в России

Адрес: 125040, 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 Mircosoft Exchange Server и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство администратора** антивирусного решения Dr.Web для Mircosoft Exchange Server 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 веб-сайте компании «Доктор Веб» https://download.drweb.ru/doc/.

1.2. Условные обозначения и сокращения

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.
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства будут употребляться без расшифровки следующие сокращения:

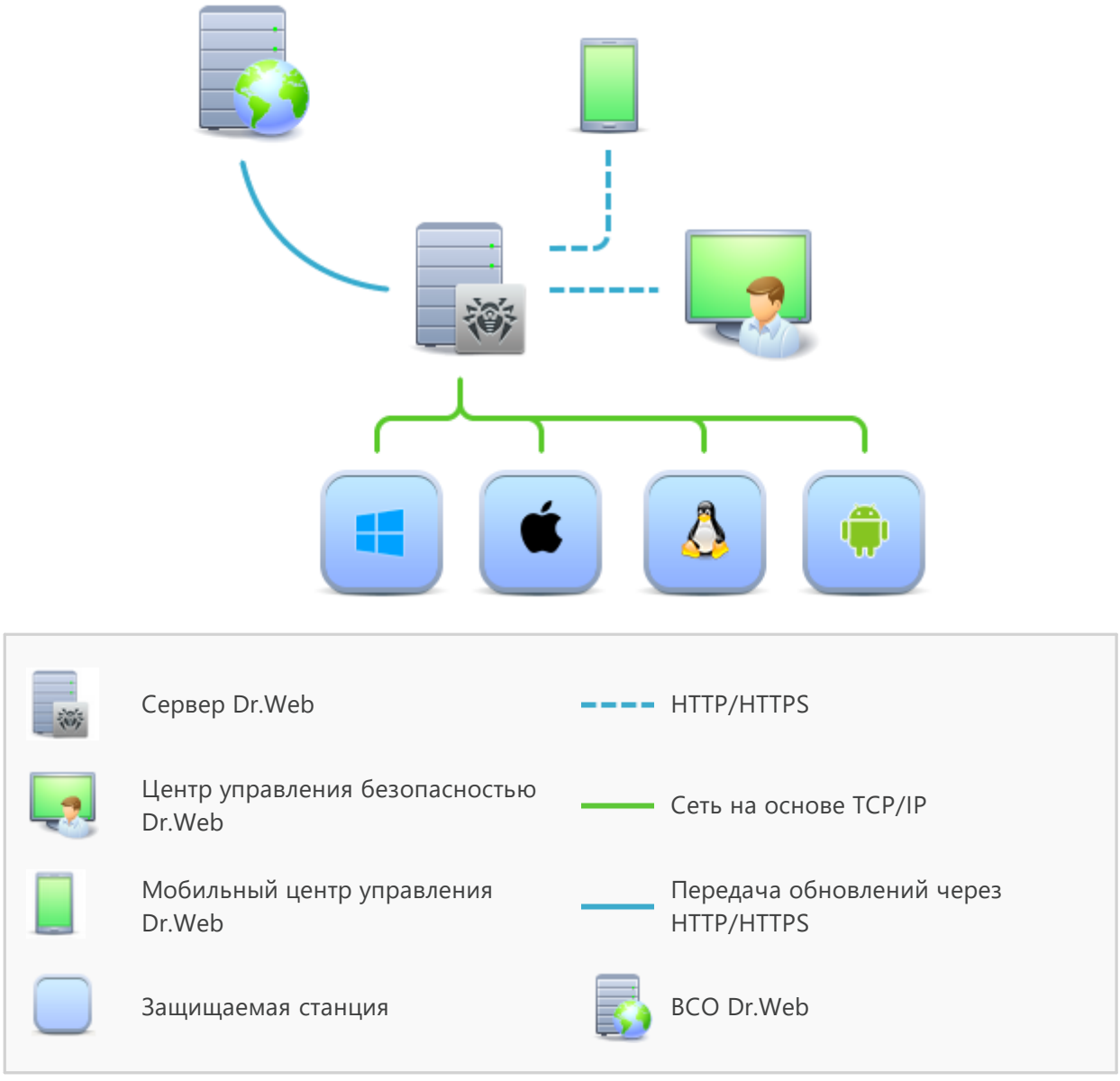
- DNS — система доменных имен (Domain Name System),
- GUI — графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы — версия, использующая средства GUI,
- NAP — Network Access Protection,
- ВСО Dr.Web — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

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 серверов Microsoft Exchange

Защита серверов Microsoft Exchange осуществляется антивирусными пакетами Dr.Web.

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

Установка

Антивирусный пакет устанавливается на сервер локально. Настройка производится администратором.

Управление

При поддержке связи с Сервером Dr.Web администратору доступна централизованная настройка Антивируса на серверах Microsoft Exchange при помощи Центра управления.

Обновление

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

В случае временного отключения сервера от антивирусной сети, подключаемый модуль на узле антивирусной сети использует локальную копию настроек, антивирусная защита на сервере сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии). Если для узла антивирусной сети разрешено использование «Мобильного режима», то при потере связи с Сервером обновляются только вирусные базы через подключение к серверам ВСО. Обновление подключаемого модуля при этом не производится.

Принцип работы в Мобильном режиме описан в руководстве администратора Dr.Web Enterprise Security Suite, описание настроек Мобильного режима работы на стороне Dr.Web Agent приведено в Руководстве пользователя Агент Dr.Web для Windows.

Глава 3. Управление Dr.Web для Mircosoft Exchange Server

3.1. Dr.Web для Mircosoft Exchange Server

Dr.Web для Mircosoft Exchange Server — это антивирусное приложение, созданное с целью защитить корпоративную почтовую систему от вирусов и спама. Оно надежно интегрируется в систему и проверяет все письма и вложения, поступающие серверу для обработки. Все сообщения проверяются до того, как они передаются клиенту.

Dr.Web для Mircosoft Exchange Server может выполнять следующие функции:

- Сканирование всех входящих и исходящих сообщений в реальном времени.
- Фильтрация и блокировка спама, а также создание белых и черных списков адресов.
- Изоляция инфицированных и подозрительных объектов в карантине.
- Фильтрация электронных писем по различным критериям.
- Распределение пользователей по группам для упрощения администрирования.
- Отправка уведомлений о вирусных событиях в журнал событий операционной системы и ведение внутренней базы событий **cmstracedb**.
- Сбор статистики.
- Поддержка единых настроек приложения на распределенной системе почтовых серверов, в том числе, объединенных в кластер.
- Автоматическое обновление вирусных баз и компонентов программы.

Для упрощения работы с приложением были реализованы полностью автоматический запуск (при запуске системы) и удобный механизм обновлений посредством добавления задания на обновление в расписание Планировщика Задач Windows.

Dr.Web для Mircosoft Exchange Server использует вирусные базы, которые постоянно пополняются новыми записями, что обеспечивает высокий уровень защиты и своевременное реагирование на появление новых угроз. Также в программе реализован эвристический анализатор для дополнительной защиты от неизвестных вирусов.

Приложение функционирует на платформе Dr.Web CMS (Central Management Service), поддерживающей централизованное управление настройками приложения и его компонентов с возможностью удаленного администрирования через браузер по защищенному протоколу HTTPS. Платформа Dr.Web CMS имеет встроенный веб-сервер Dr.Web CMS Web Console с аутентификацией клиента, что обеспечивает доступ к управлению приложением только авторизованным администраторам.

Интерфейсы взаимодействия и управления компонентами приложения реализованы посредством внутренних служебных протоколов, работающих поверх TCP. Упомянутые служебные протоколы позволяют управляющему сервису Dr.Web CMS выполнять его основную задачу: предоставлять компонентам приложения канал связи с управляющей базой

данных **cmsdb** и базой событий приложения **cmstracedb**, находящихся в папке установки приложения и реализованных встраиваемой реляционной базой SQLite.

Взаимодействие компонентов приложения с платформой Dr.Web CMS осуществляются следующим образом:

1. Компонент приложения при запуске (если компонент является сервисом) или загрузке (если компонент является библиотекой) подключаются к сервису Dr.Web CMS посредством служебного протокола поверх TCP.
2. Dr.Web CMS регистрирует подключение приложения и создает в базе **cmsdb** структуру данных, отвечающих подключившемуся компоненту приложения.
3. Dr.Web CMS контролирует работу компонента приложения, отслеживая состояние TCP-сессии и обмен служебными сообщениями с компонентом приложения.
4. В случае изменения состояния компонента приложения Dr.Web CMS изменяет переменные в базе **cmsdb**, отражающие состояние приложения.

Сервисы Dr.Web CMS, установленные на разных серверах, могут быть объединены администратором в единое иерархическое дерево для поддержки репликации параметров базы **cmsdb** с атрибутом **Shared** всех компонентов-подписчиков Dr.Web CMS. Репликация производится от главного сервера на подчиненный. Таким образом, управление настройками дерева серверов возможно с корневого хоста.

3.2. Настройка Dr.Web для Mircosoft Exchange Server

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 Windows или группы, содержащей такие станции.
3. В открывшемся управляющем меню в разделе **Подключаемые модули** выберите **Dr.Web для Microsoft Exchange Server**.
4. Откроется окно настроек 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.

  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, для принятия этих изменений, нажмите кнопку **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**). При этом редактировать настройки сможет только сам администратор через Центр управления.

3.2.1. Настройка общих параметров

На вкладке **Общие** доступны настройки подключаемого модуля **Dr.Web для Microsoft Exchange Server**:

- Опция **Использовать эвристический анализ** позволяет Dr.Web для Mircosoft Exchange Server обнаруживать еще неизвестные вредоносные программы. По умолчанию опция включена. Если опция отключена, проверка проводится только по сигнатурам известных вирусов.
- Опция **Проверять архивы** предназначается для антивирусной проверки архивных вложений на MS Exchange Server. По умолчанию опция включена. Если опция отключена, то проверка архивов не производится.
- Опция **Проверять инсталляционные пакеты** предназначается для антивирусной проверки инсталляционных пакетов на MS Exchange Server. По умолчанию опция включена. Если опция отключена, то проверка инсталляционных пакетов не производится.
- Опция **Рассматривать архивы с паролем как поврежденные** предназначается для проверки архивов, защищённых паролем в качестве повреждённых обычных архивов. По умолчанию опция включена. Если опция отключена, то архивы, защищённые паролем, проверяются в обычном режиме.

При подключении станции на вкладке **Общие** отображается дополнительное поле, содержащее ссылку на адрес административной консоли для управления подключаемым модулем в следующем виде: **URL консоли администратора Dr.Web** <*address*>, где <*address*> — адрес административной консоли станции в сети.

Данное поле отображается лишь в случае персональных настроек станции. В случае наследуемых настроек либо настроек группы поле не отображается.

Группа **Вредоносные программы** содержит следующие опции:

- **Рекламные программы**
- **Программы дозвона**
- **Программы взлома**
- **Программы-шутки**
- **Потенциально опасные**

По умолчанию опции группы **Вредоносные программы** отключены. Для проверки требуемых групп вредоносных программ активируйте соответствующие опции.

Группа **Действия** содержит следующие настройки:

- **Инфицированные**. Данная настройка предназначается для выполнения соответствующего действия с объектом, определённым подключаемым модулем как инфицированный. Доступны следующие действия:
  - **Перемещать в карантин**
  - **Удалять**
  - **Архивировать**
- **Подозрительные**. Данная настройка предназначается для выполнения соответствующего действия с объектом, определённым Dr.Web для Mircosoft Exchange Server как подозрительный. Доступны следующие действия:
  - **Перемещать в карантин**
  - **Удалять**
  - **Игнорировать**
  - **Архивировать**

После настройки опций и действий нажмите **Сохранить** в правом верхнем углу рабочего пространства страницы конфигурации подключаемого модуля.

3.2.2. Настройка параметров антиспама

На вкладке **Антиспам** доступны настройки диагностирования спама и последующих действий с ним в подключаемом модуле **Dr.Web для Mircosoft Exchange Server**:

- Опция **Проверять почту на наличие спама** позволяет Dr.Web для Mircosoft Exchange Server обнаруживать письма, определяемые подключаемым модулем как спам. По умолчанию опция включена. Если опция отключена, проверка на наличие спама не производится.
- Опция **Использовать белый и черный списки** предназначается для использования списков, содержащих перечни доверенных и ненадежных адресов. По умолчанию опция включена. Если опция отключена, то белый и черный списки не используются.

Группа **Действия** содержит следующие настройки:

- **Точно спам**. Данная настройка предназначается для выполнения соответствующего действия с объектом, определённым подключаемым модулем как спам. Доступны следующие действия:
  - **Добавлять префикс к теме спам-писем**. При выборе данного действия тема письма, определенного как спам, будет отображаться с префиксом, установленным в поле **Префикс**.
  - **Блокировать**. При выборе данного действия письмо, определенное как спам, будет блокировано подключаемым модулем.
  - **Перенаправлять**. При выборе данного действия письмо, определенное как спам, будет перенаправлено на адрес, указанный в поле **Адрес перенаправления**.
  - **Перемещать в папку нежелательной почты**. При выборе данного действия письму, определенному как спам, будет добавлен служебный заголовок **X-MS-Exchange-Organization-SCL**, в значении которого указывается индекс недоверия к письму. Если значение индекса больше 4, но меньше 7, почтовые клиенты, для которых установлены необходимые настройки, смогут перемещать такое сообщение в папку нежелательной почты.
- **Возможно спам**. Данная настройка предназначается для выполнения соответствующего действия с объектом, определённым подключаемым модулем как возможный спам. Доступны следующие действия:
  - **Добавлять префикс к теме спам-писем**. При выборе данного действия тема письма, определенного как возможный спам, будет отображаться с префиксом, установленным в поле **Префикс**.
  - **Блокировать**. При выборе данного действия письмо, определенное как возможный спам, будет блокировано подключаемым модулем.
  - **Перенаправлять**. При выборе данного действия письмо, определенное как возможный спам, будет перенаправлено на адрес, указанный в поле **Адрес перенаправления**.
  - **Перемещать в папку нежелательной почты**. При выборе данного действия письму, определенному как возможный спам, будет добавлен служебный заголовок **X-MS-Exchange-Organization-SCL**, в значении которого указывается индекс недоверия к

письму. Если значение индекса больше 4, но меньше 7, почтовые клиенты, для которых установлены необходимые настройки, смогут перемещать такое сообщение в папку нежелательной почты.

- **Маловероятно, что спам**. Данная настройка предназначается для выполнения соответствующего действия с объектом, определённым подключаемым модулем как маловероятный спам. Доступны следующие действия:
  - **Добавлять префикс к теме спам-писем**. При выборе данного действия тема письма, определенного как маловероятный спам, будет отображаться с префиксом, установленным в поле **Префикс**.
  - **Блокировать**. При выборе данного действия письмо, определенное как маловероятный спам, будет блокировано подключаемым модулем.
  - **Перенаправлять**. При выборе данного действия письмо, определенное как маловероятный спам, будет перенаправлено на адрес, указанный в поле **Адрес перенаправления**.
  - **Перемещать в папку нежелательной почты**. При выборе данного действия письму, определенному как маловероятный спам, будет добавлен служебный заголовок **X-MS-Exchange-Organization-SCL**, в значении которого указывается индекс недоверия к письму. Если значение индекса больше 4, но меньше 7, почтовые клиенты, для которых установлены необходимые настройки, смогут перемещать такое сообщение в папку нежелательной почты.
- **Адрес перенаправления**. Данное поле предназначается для указания адреса, на который будут перенаправлены письма, определенные как спам, возможный спам и маловероятный спам. Для указания адреса перенаправления введите соответствующий адрес в поле.
- **Префикс**. Данное поле предназначается для установки префикса для писем, определенных как спам, возможный спам и маловероятный спам. Значение поля по умолчанию: *****SPAM*****. Для изменения префикса введите новый префикс в поле.

Формирование списков доверенных и ненадежных адресов

- **Черный список**. Для добавления адреса в черный список введите адрес в поле. При необходимости добавления нескольких адресов в черный список, используйте кнопку  , после нажатия которой будет сформировано новое поле для ввода ненадежного адреса. Для удаления адреса из черного списка нажмите кнопку  .
- **Белый список**. Для добавления адреса в белый список введите адрес в поле. При необходимости добавления нескольких адресов в белый список, используйте кнопку  , после нажатия которой будет сформировано новое поле для ввода доверенного адреса. Для удаления адреса из белого списка нажмите кнопку  .

После настройки опций и действий нажмите **Сохранить** в правом верхнем углу рабочего пространства страницы конфигурации подключаемого модуля.

Приложение А. 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/.