Dr.WEB

Enterprise Security Suite

Управление станциями под Windows

Dr.Web Enterprise Security Suite. Управление станциями под Windows
Версия 13.0
Руководство администратора
11.06.2025

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

Глава 1. Введение

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 Windows и особенности централизованного управления данным ПО.

Для получения дополнительной информации обращайтесь к следующим руководствам:

- **Руководство пользователя** антивирусного решения Dr.Web для Windows 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/.

1.1. Условные обозначения и сокращения

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.

Сокращения

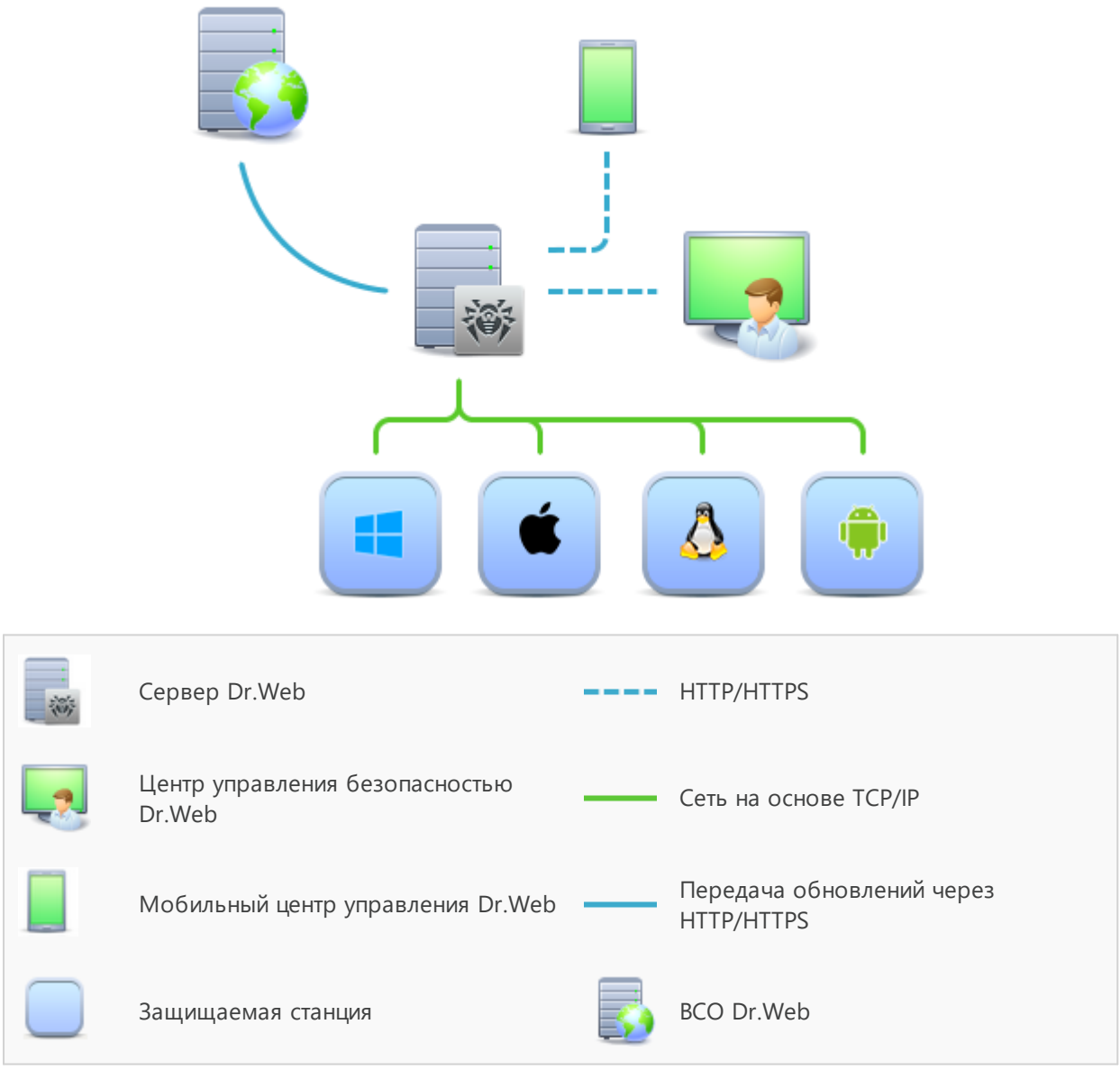
В тексте Руководства будут употребляться без расшифровки следующие сокращения:

- 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

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.

2.1. 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 Dr.Web. Передача информации между станцией и Сервером Dr.Web осуществляется по протоколу, используемому в локальной сети (TCP/IP версии 4 или 6).

Установка

Антивирусный пакет может быть установлен на рабочую станцию двумя способами:

1. Локально. Локальная установка осуществляется на компьютере или мобильном устройстве пользователя непосредственно. Может производится как администратором, так и пользователем.
2. Удаленно. Удаленная установка осуществляется в Центре управления через ЛВС. Производится администратором антивирусной сети. При этом вмешательство пользователя не требуется.

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 функции, 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.

- Настройка расписания антивирусных проверок и других заданий, выполняемых на станции.
- Получение статистики сканирования и прочей информации о работе антивирусных компонентов и о состоянии станции.
- Запуск и завершение антивирусного сканирования и т. п.

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 Dr.Web будет доступно обновление вирусных баз непосредственно с серверов ВСО.

Принцип работы в Мобильном режиме описан в **Руководстве администратора** Dr.Web Enterprise Security Suite.

Глава 3. Dr.Web для Windows

Агент Dr.Web обеспечивает многоуровневую защиту системной памяти, жестких дисков и съемных носителей от проникновений любых вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и всех возможных типов вредоносных объектов из любых внешних источников.

Dr.Web использует удобную и эффективную процедуру обновления вирусных баз и версий программного обеспечения через интернет.

Dr.Web способен также обнаруживать и удалять с компьютера различные нежелательные программы (рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы, программы взлома). Для обнаружения нежелательных программ и действий над содержащими их файлами применяются стандартные средства антивирусных компонентов программы Dr.Web.

3.1. Компоненты Dr.Web для Windows

Для защиты станций под ОС Windows предоставляются следующие антивирусные компоненты:

Сканер Dr.Web, Dr.Web Agent Сканер

Сканирование компьютера по запросу пользователя, а также согласно расписанию. Также поддерживается возможность запуска удаленной антивирусной проверки станций из Центра управления, в том числе на наличие руткитов.

Описания настроек Dr.Web Agent Сканера и удаленного запуска сканирования через Центр управления приведены в **Руководстве администратора** Dr.Web Enterprise Security Suite.

SpIDer Guard

Постоянная проверка файловой системы в режиме реального времени. Проверка всех запускаемых процессов, а также создаваемых файлов на жестких дисках и открываемых файлов на сменных носителях.

SpIDer Mail

Проверка всей входящей и исходящей почты при использовании почтовых клиентов.

Также возможно использование спам-фильтра (при условии, что лицензия позволяет использование такой функции).

SpIDer Gate

Проверка всех обращений к сайтам по протоколам HTTP, XMPP (Jabber) и TLS (SSL). Нейтрализация угроз в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокировка доступа к подозрительным или некорректным ресурсам.

Офисный контроль

Управление доступом к локальным и сетевым ресурсам, в частности, контроль доступа к сайтам. Позволяет контролировать целостность важных файлов, предотвращает случайное изменение или заражение вредоносными программами и запрещает служащим доступ к нежелательной информации.

Брандмауэр

Контроль подключения и фильтрация соединений на уровне пакетов и приложений.

Карантин

Изоляция вредоносных и подозрительных объектов в специальном каталоге.

Описание работы с Карантином через Центр управления приведено в **Руководстве администратора** Dr.Web Enterprise Security Suite.

Самозащита

Защита файлов и каталогов Dr.Web Enterprise Security Suite от несанкционированного или невольного удаления или модификации пользователем, а также вредоносным ПО. При включенной самозащите доступ к файлам и каталогам Dr.Web Enterprise Security Suite разрешен только для процессов Dr.Web.

Превентивная защита

Включает в себя Поведенческий анализ, Защиту от эксплойтов и Защиту от вымогателей.

Предотвращение потенциальных угроз безопасности. Контроль доступа к критическим объектам операционной системы, контроль за загрузкой драйверов, автоматическим запуском программ и работой системных служб, а также отслеживание запущенных процессов и их блокировка в случае обнаружения вредоносной активности.

Контроль приложений

Осуществляет мониторинг активности всех процессов на станциях. Позволяет администратору антивирусной сети регулировать, какие приложения разрешать, а какие — запрещать запускать на защищаемых станциях.

3.2. Настройка Dr.Web для Windows

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 **Конфигурация**, в подразделе **Windows** выберите требуемый компонент.
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.

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

     Скопировать настройки из родительской группы и установить их в качестве персональных — скопировать настройки данного раздела из родительской 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 внесении 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 Dr.Web.

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. Сканер

В этом разделе:

- Настройка работы Сканера Dr.Web
- Действия Сканера Dr.Web при обнаружении угроз
- Исключение из проверки Сканером Dr.Web
- Журнал событий Сканера Dr.Web

3.2.1.1. Общие

На вкладке **Общие** задайте общие параметры работы Сканера Dr.Web.

- Включите опцию **Проигрывать звуки**, чтобы Сканер Dr.Web сопровождал каждое событие звуковым сигналом. По умолчанию опция отключена.
- Включите опцию **Автоматически применять действия к угрозам**, чтобы Сканер Dr.Web автоматически применял заданные действия к обнаруженным угрозам. Если опция отключена, пользователю будет выдан запрос на необходимое действие.
- Включите опцию **Прерывать проверку при переходе на питание от аккумулятора**, чтобы при переходе компьютера пользователя на питание от аккумулятора проверка была прервана. По умолчанию опция отключена.

На этой вкладке вы также можете выбрать максимально допустимый уровень загрузки ресурсов компьютера Сканером Dr.Web по время проверки. По умолчанию задано оптимальное значение 50 %.

3.2.1.2. Действия

На вкладке **Действия** выберите действия, которые будут применяться к угрозам, обнаруженным Сканером Dr.Web, в зависимости от их типа.

- **Лечить, перемещать в карантин неизлечимые**. Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских

программ и вредоносных файлов внутри составных объектов.

- **Лечить, удалять неизлечимые**. Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и вредоносных файлов внутри составных объектов.
- **Перемещать в карантин**. Обнаруженная угроза помещается в специальную папку, изолированную от остальной системы.
- **Удалять**. Наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- **Игнорировать**. К объекту не применяется никакое действие, оповещение об обнаруженном объекте не появляется.

Предустановленные настройки являются оптимальными для большинства случаев, не изменяйте их без необходимости.

Действия Сканера Dr.Web над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Перемещать в карантин**	**Удалять**	**Игнорировать**
Вредоносные	+/*	+	+	+	
Подозрительные			+/*	+	+
Вредоносные инсталляционные пакеты			+/*	+	
Вредоносные архивы			+/*	+	
Вредоносные почтовые файлы			+/*		+
Рекламные программы			+/*	+	+
Программы дозвона			+/*	+	+
Программы-шутки			+/*	+	+
Потенциально опасные			+/*	+	+

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Перемещать в карантин**	**Удалять**	**Игнорировать**
Программы взлома			+/*	+	+

Условные обозначения

+	действие разрешено для данного типа объектов
+/*	действие установлено как реакция по умолчанию для данного типа объектов

3.2.1.3. Исключения

На вкладке **Исключения** вы можете указать каталоги и файлы, которые будут исключены из проверки Сканером Dr.Web.

Формирование списка исключений

1. Чтобы добавить папку или файл к списку исключений, выполните одно из следующих действий:
   - чтобы указать конкретный файл или папку, вручную введите полный путь к файлу или папке в поле ввода (вы можете использовать переменные среды);
   - чтобы исключить из проверки все файлы или папки с определенным именем, введите это имя в поле ввода. Указывать путь к папке или файлу при этом не требуется;
   - чтобы исключить из проверки файлы или папки определенного вида, введите определяющую их маску в поле ввода. Маска задает общую часть имени объекта, при этом:
     - символ «*» заменяет любую, возможно пустую, последовательность символов;
     - символ «?» заменяет любой, но только один символ;
     - остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.
2. В каждом поле задается только один объект. Чтобы добавить еще один объект в список, нажмите кнопку  .
3. Чтобы удалить объект из списка исключений, нажмите кнопку  напротив элемента списка, соответствующего этому объекту.

Вы также можете отключить проверку архивов, почтовых файлов и инсталляционных пакетов. По умолчанию проверка этих объектов включена.

3.2.1.4. Журнал

Включите опцию **Вести подробный журнал**, чтобы фиксировались такие события Сканера Dr.Web, как обновления, запуск и его остановка, обнаруженные угрозы, а также данные об именах упаковщиков и содержимом проверяемых архивов.

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

При включении опции **Вести подробный журнал**, запись журнала работы соответствующего компонента осуществляется в режиме отладки с максимальной детализацией. Ограничения на размер файла в данном режиме снимаются. Это приводит к значительному увеличению размера файла журнала. Также обратите внимание, что ротация файла журнала не осуществляется (относится ко всем режимам ведения журнала).

Отладочный режим ведения журнала снижает производительность работы антивируса и операционной системы станции. Использовать этот режим следует только при возникновении проблем в работе компонентов и по запросу службы технической поддержки. Не рекомендуется включение отладочного режима ведения журнала на длительный срок.

На стороне Центра управления настройки ведения журнала задаются отдельно для каждого компонента в разделах **Журнал**. На станции настройки ведения журнала задаются в едином разделе **Дополнительно**.

3.2.2. SpIDer Mail

В этом разделе:

- Действия SpIDer Mail при обнаружении угроз
- Фильтрация подключений к почтовым серверам
- Параметры работы Антиспама
- Журнал событий компонента SpIDer Mail

3.2.2.1. Общие

На вкладке **Общие** выберите действия, которые будут применяться к угрозам, обнаруженным SpIDer Mail, в зависимости от их типа.

- **Лечить, перемещать в карантин неизлечимые**. Восстановить состояние объекта до

заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и вредоносных файлов внутри составных объектов.

- **Лечить, удалять неизлечимые**. Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и вредоносных файлов внутри составных объектов.
- **Перемещать в карантин**. Обнаруженная угроза помещается в специальную папку, изолированную от остальной системы.
- **Удалять**. Наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- **Игнорировать**. К объекту не применяется никакое действие, оповещение об обнаруженном объекте не появляется.

Предустановленные настройки являются оптимальными для большинства случаев, не изменяйте их без необходимости.

Действия SpIDer Mail над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Перемещать в карантин**	**Удалять**	**Игнорировать**
Вредоносные сообщения	+/*	+	+	+	
Подозрительные сообщения			+/*	+	+
Непроверенные сообщения			+	+	+/*
Поврежденные сообщения			+	+	+/*
Рекламные программы			+/*	+	+
Программы дозвона			+/*	+	+

Объект	Действие				
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Перемещать в карантин**	**Удалять**	**Игнорировать**
Программы-шутки			+	+	+/*
Программы взлома			+	+	+/*
Потенциально опасные			+	+	+/*

Условные обозначения

+	действие разрешено для данного типа объектов
+/*	действие установлено как реакция по умолчанию для данного типа объектов

Особенности проверки

Эта группа настроек задает дополнительные параметры проверки электронной почты:

- **Использовать эвристический анализ** — данный режим позволяет выявить в электронной почте подозрительные объекты, с большой вероятностью зараженные еще неизвестными вредоносными программами. Отключите опцию, чтобы не использовать эвристический анализатор.
- **Проверять инсталляционные пакеты** — проверка файлов инсталляционных пакетов. Эта настройка по умолчанию отключена.

Оптимизация проверки

Вы можете задать условие, при выполнении которого сложноустроенные письма, проверка которых является чрезмерно трудоемкой, признаются непроверенными. Для этого включите опцию **Тайм-аут проверки письма (с)** и задайте максимальное время, в течение которого письмо проверяется. По истечении указанного времени SpIDer Mail прекратит проверку письма. По умолчанию задано значение 250 секунд.

Действия над письмом

В данной группе настроек указываются дополнительные действия над электронными письмами, обработанными SpIDer Mail.

- **Добавлять заголовок "X-Antivirus"**. При включении этой опции в заголовок всех писем, обработанных компонентом SpIDer Mail, добавляется информация о проверке электронного сообщения и версии Dr.Web. Вы не можете изменить формат добавляемого заголовка. Опция включена по умолчанию.
- **Удалять модифицированные письма на сервере**. При включении этой опции входящие письма, удаленные или перемещенные в карантин SpIDer Mail, удаляются с почтового сервера независимо от настроек почтовой программы.
- **Проверять архивы**. При включении этой опции SpIDer Mail проверяет содержимое архивов, передаваемых по электронной почте. При активации настройки будут доступны следующие опции:
  - **Максимальный размер файла при распаковке**. Если распакованный архив превысит указанный размер, то SpIDer Mail не будет распаковывать и проверять его. По умолчанию задано значение 30720 КБ;
  - **Максимальный коэффициент сжатия архива**. Если коэффициент сжатия архива превышает указанный, то SpIDer Mail не будет распаковывать и проверять его. По умолчанию задано значение 0;
  - **Максимальный уровень вложенности в архив**. Если уровень вложенности превышает заданное значение, то SpIDer Mail проверит архив только до указанного уровня. По умолчанию задано значение 64.

3.2.2.2. Фильтр приложений

Настройка Фильтра приложений компонента SpIDer Mail возможна только на стороне Сервера Dr.Web. Соответствующие настройки на станции не предоставляются.

Фильтр приложений позволяет настроить ручной перехват подключений к почтовым серверам. В данном режиме SpIDer Mail выступает в роли прокси-сервера между почтовыми клиентами и почтовыми серверами и отслеживает только те соединения, которые указаны в настройках в явном виде. Использование данного типа перехвата требует изменения настроек подключения почтовых клиентов на станциях.

Список перехватываемых адресов состоит из записей, каждая из которых устанавливает соответствие между настройками SpIDer Mail и почтового сервера.

По умолчанию список перехвата пуст. Вы можете добавить в него необходимые записи.

Настройка перехвата соединений

1. Составьте список почтовых серверов, обращения к которым вы хотите перехватывать, и присвойте номера портов для этих серверов в произвольном порядке. При этом используйте только свободные, несистемные порты. Эти порты далее будут именоваться *портами SpIDer Mail*.

SplDer Mail поддерживает почтовые серверы, работающие по протоколам POP3, SMTP, IMAP4 или NNTP.

2. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
3. В открывшемся окне в иерархическом списке нажмите на название станции или группы.
4. В открывшемся управляющем меню выберите пункт **Конфигурация** → **Windows** → **SplDer Mail**. Перейдите на вкладку **Фильтр приложений**.
5. В разделе **Настройка соединений SplDer Mail** задайте следующие параметры:
   - **Порт SplDer Mail** — порт SplDer Mail, выбранный для почтового сервера на шаге 1;
   - **Сервер** — доменное имя или IP-адрес почтового сервера;
   - **Порт** — номер порта, который использует почтовый сервер.
6. При необходимости повторите шаг 5 для других серверов. Чтобы добавить еще один почтовый сервер в список, нажмите кнопку  .
7. Чтобы прекратить перехватывать подключения к определенному почтовому серверу, нажмите кнопку  напротив элемента списка, соответствующего этому серверу.
8. После задания всех необходимых настроек нажмите кнопку **Сохранить** для применения изменений на станции.
9. Настройте почтовый клиент на станции для работы с компонентом SplDer Mail при перехвате соединений вручную.

Настройка почтового клиента

Если SplDer Mail настроен на ручной перехват соединений с почтовыми серверами, измените настройки почтового клиента на станции соответствующим образом:

1. В качестве адреса сервера входящей и исходящей почты укажите `localhost`.
2. В качестве порта почтового сервера укажите *порт SplDer Mail*, назначенный вами для соответствующего почтового сервера.

Как правило, для этого необходимо в настройках адреса почтового сервера указать:

`localhost:`<*порт_SplDer_Mail*>

где <*порт_SplDer_Mail*> — порт, назначенный вами соответствующему почтовому серверу.

Пример

Если почтовому серверу с адресом `pop.mail.ru` и портом `110` назначен *порт SplDer Mail* `7000`, то в настройках почтового клиента необходимо указать `localhost` в качестве сервера входящей почты и `7000` в качестве порта.

3.2.2.3. Антиспам

Вы можете настроить следующие параметры работы **Антиспама**:

- **Включить антиспам**. При включении этой опции активируется модуль Антиспама.
- **Разрешить текст на кириллице**. Эта опция указывает почтовому монитору SpIDer Mail без предварительного анализа не причислять к спаму письма, написанные в кириллической кодировке. Если эта опция отключена, то такие письма с большой вероятностью будут отмечены фильтром как спам. Опция включена по умолчанию.
- **Разрешить текст на азиатских языках**. Данная настройка указывает почтовому монитору SpIDer Mail без предварительного анализа не причислять к спаму письма, написанные в соответствии с наиболее распространенными кодировками азиатских языков. Если эта опция отключена, то такие письма с большой вероятностью будут отмечены фильтром как спам. Опция включена по умолчанию.
- **Добавлять префикс к теме спам-писем**. Эта опция указывает почтовому монитору SpIDer Mail добавлять строку, указанную в поле **Префикс**, к темам писем, распознаваемых как спам. Опция включена по умолчанию. Добавление префикса поможет вам создать правила для фильтрации почтовых сообщений, помеченных как спам, в тех почтовых клиентах (например, MS Outlook Express), в которых невозможно настроить фильтры по заголовкам писем.

  По умолчанию добавляется префикс **[SPAM]**.
- Также вы можете настроить белые и черные списки для фильтрации писем.
  - В каждом поле задается только один объект. Чтобы добавить еще один объект в список, нажмите кнопку  .
  - Чтобы удалить объект из списка исключений, нажмите кнопку  .

3.2.2.4. Журнал

Включите опцию **Вести подробный журнал**, чтобы фиксировались такие события, как время обновлений, запуск и остановка SpIDer Mail, информация об обнаруженных угрозах, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов.

Рекомендуется использовать этот режим для проверки настроек перехвата соединений с почтовыми серверами.

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

При включении опции **Вести подробный журнал**, запись журнала работы соответствующего компонента осуществляется в режиме отладки с максимальной детализацией. Ограничения на размер файла в данном режиме снимаются. Это приводит к значительному увеличению размера файла журнала. Также обратите внимание, что ротация файла журнала не осуществляется (относится ко всем режимам ведения журнала).

Отладочный режим ведения журнала снижает производительность работы антивируса и операционной системы станции. Использовать этот режим следует только при возникновении проблем в работе компонентов и по запросу службы технической поддержки. Не рекомендуется включение отладочного режима ведения журнала на длительный срок.

На стороне Центра управления настройки ведения журнала задаются отдельно для каждого компонента в разделах **Журнал**. На станции настройки ведения журнала задаются в едином разделе **Дополнительно**.

3.2.3. SpIDer Gate

В этом разделе:

- Настройка проверки компонентом SpIDer Gate
- Проверка трафика и URL в IM-клиентах
- Журнал событий компонента SpIder Gate

3.2.3.1. Действия

На вкладке **Действия** задайте основные настройки проверки станций компонентом SpIDer Gate.

- **Режим проверки**. Выберите необходимый режим проверки трафика. По умолчанию выбрана опция **Проверять входящий трафик (рекомендуется)**.
- **Блокировать вредоносные программы**. Эта группа настроек позволяет вам выбрать вредоносные программы, которые подлежат блокировке. По умолчанию SpIDer Gate блокирует подозрительные и рекламные программы, а также программы дозвона.
- **Блокировать объекты**. SpIDer Gate может блокировать непроверенные или повреждённые объекты. По умолчанию эти опции выключены.
- **Дополнительно**. Эта группа настроек позволяет включить проверку архивов и инсталляционных пакетов. По умолчанию опция проверки архивов и инсталляционных пакетов отключена.
- **Приоритет сканирования**. Эта настройка позволяет вам регулировать распределение ресурсов в зависимости от приоритетности проверки трафика. При меньшем приоритете проверки скорость работы с сетью интернет уменьшается, поскольку веб-антивирусу SpIDer Gate приходится дольше ждать загрузки данных и проверять

больший объем информации. При увеличении приоритета проверка производится чаще, что позволяет монитору отдавать данные быстрее, тем самым повышая скорость работы с сетью. Однако при более частых проверках повышается нагрузка на процессор.

- **Параметры блокировки**. В этой группе вы можете установить автоматическую блокировку доступа к URL, добавленных по обращению правообладателя, а также к нерекомендуемым сайтам, известным как неблагонадежные. Доступ к сайтам из белого списка будет разрешен, несмотря на установленные ограничения.

  SpIDer Gate по умолчанию блокирует доступ к сайтам, известным как источники угроз. При этом учитывается список приложений, исключаемых из проверки.

- **Белый список**. Задайте список сайтов, доступ к которым будет разрешаться вне зависимости от остальных настроек.
  1. Укажите в соответствующем поле сайт, который вы хотите добавить в белый список.
  2. В каждом поле задается только один сайт. Чтобы добавить еще один сайт в список, нажмите кнопку  .
  3. Чтобы удалить сайт из белого списка, нажмите кнопку  напротив элемента списка, соответствующего этому сайту.

3.2.3.2. Фильтр приложений

Включите опцию **Проверять трафик и URL в IM-клиентах**, чтобы проводилась проверка ссылок и данных, передаваемых клиентами систем обмена мгновенными сообщениями (Mail.RU Агент, ICQ и клиентов, работающих по протоколу Jabber). Проверяется только входящий трафик. По умолчанию опция включена.

3.2.3.3. Журнал

Включите опцию **Вести подробный журнал**, чтобы фиксировались такие события, как время обновлений, запуск и остановка веб-антивируса SpIDer Gate, информация об обнаруженных угрозах, параметры перехвата соединений, а также данные о проверяемых файлах, именах упаковщиков и содержимом проверяемых архивов.

Рекомендуется использовать этот режим для получения более детальной информации о проверенных объектах и работе веб-антивируса.

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает

разрешенный размер.

При включении опции **Вести подробный журнал**, запись журнала работы соответствующего компонента осуществляется в режиме отладки с максимальной детализацией. Ограничения на размер файла в данном режиме снимаются. Это приводит к значительному увеличению размера файла журнала. Также обратите внимание, что ротация файла журнала не осуществляется (относится ко всем режимам ведения журнала).

Отладочный режим ведения журнала снижает производительность работы антивируса и операционной системы станции. Использовать этот режим следует только при возникновении проблем в работе компонентов и по запросу службы технической поддержки. Не рекомендуется включение отладочного режима ведения журнала на длительный срок.

На стороне Центра управления настройки ведения журнала задаются отдельно для каждого компонента в разделах **Журнал**. На станции настройки ведения журнала задаются в едином разделе **Дополнительно**.

3.2.4. Агент Dr.Web

В этом разделе:

- Настройка работы Агента Dr.Web
- Работа Агента Dr.Web в Мобильном режиме
- Журнал событий Агента Dr.Web
- Параметры интерфейса Агента Dr.Web
- Отправка событий Агента Dr.Web на Сервер Dr.Web

3.2.4.1. Общие

На вкладке **Общие** вы можете настроить следующие параметры Агента:

- В поле **Задержка запуска Планировщика заданий (мин.)** задайте величину тайм-аута между запуском ОС и началом выполнения стартового задания на сканирование, если оно задано в расписании заданий Агента. По умолчанию указана задержка в 1 минуту. При указании значения 0 задание на сканирование будет запущено без задержки, т. е. сразу после загрузки ОС.
- В поле **Периодичность отправки статистики (мин.)** задайте значение временного интервала в минутах для отправки Агентом на Сервер Dr.Web всей статистической информации, собранной на станции компонентами SpIDer Guard, SpIDer Mail и SpIDer Gate. Задайте значение 0, чтобы отключить отправку статистики.
- В поле **Срок актуальности вирусных баз** задайте значение временного интервала, в течение которого вирусные базы, установленные на станциях, будут считаться актуальными. Начало интервала — момент создания вирусных баз. В данный период

уведомления о том, что вирусные базы устарели, не показываются на станции. Описание аналогичной настройки Сервера Dr.Web (**Снизить серьезность устаревания вирусных баз**) приведено в разделе Ограничение обновлений рабочих станций в **Руководстве администратора** Dr.Web Enterprise Security Suite.

- В выпадающем списке **Язык** задается язык интерфейса Агента и компонентов Антивируса Dr.Web на рабочей станции или на группе рабочих станций.
- Включите опцию **Включить Microsoft Network Access Protection**, чтобы включить мониторинг состояния станции с использованием технологии *Microsoft Network Access Protection (NAP)*. При этом активируется *Агент работоспособности системы* (System Health Agent — SHA), который автоматически устанавливается вместе с ПО Агента Dr.Web на рабочую станцию.
- Включите опцию **Разрешить удаленное управление карантином** чтобы разрешить удаленное управление карантином на рабочих станциях с Сервера Dr.Web.

Пункт **Разрешить удаленное управление карантином** доступен, если в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Статистика** включена опция **Состояние карантина**.

- Включите опцию **Собирать информацию о станциях**, чтобы разрешить собирать информацию о программно-аппаратном обеспечении станций. При включенной опции выберите в выпадающем списке **Периодичность сбора информации о станциях** значение временного интервала отправки Агентами на Сервер Dr.Web актуальной информации о программно-аппаратном обеспечении на станции. Минимальное значение составляет 10 минут.
- Включите опцию **Отслеживать местоположение**, чтобы разрешить Серверу Dr.Web получать информацию о текущих координатах станции. При включенной опции выберите в выпадающем списке **Периодичность передачи координат** значение, в соответствии с которым будут обновляться данные о местоположении станции. Минимальное значение составляет 5 минут.
- Включите опцию **Очищать статистику**, чтобы включить автоматическое удаление записей статистики. При включенной опции выберите в выпадающем списке **Периодичность очистки** значение, в соответствии с которым будут удаляться записи статистики. Доступны следующие значения: 1 неделя, 2 недели, 1 месяц.
- Включите опцию **Удалять объекты из карантина**, чтобы включить автоматическое удаление объектов из карантина по истечении указанного периода. При включенной опции выберите в выпадающем списке **Срок хранения** периодичность, с которой будут удаляться объекты из карантина. Доступны следующие значения: 2 недели, 1 месяц, 6 месяцев, 1 год.
- Включите опцию **Отслеживать события Контроля приложений**, чтобы отслеживать активность процессов на станциях, зафиксированную Контролем приложений, и отправлять события на Сервер Dr.Web. При отсутствии подключения к Серверу Dr.Web события накапливаются и отправляются при подключении. Если опция отключена, могут отправляться события только о блокировках.

- Включите опцию **Синхронизировать время** для включения синхронизации системного времени на ПК с установленным Агентом и времени на ПК, на котором установлен Сервер Dr.Web.
- Включите опцию **Запрещать изменение даты и времени системы**, чтобы запретить ручное и автоматическое изменение системных даты и времени, а также часового пояса, за исключением синхронизации времени с Сервером Dr.Web (включается при помощи опции **Синхронизировать время**).
- Включите опцию **Запрещать эмуляцию действий пользователя**, чтобы запретить любые изменения в работе Dr.Web, кроме вносимых пользователем вручную. Данная опция позволяет предотвратить любые изменения в работе программы Dr.Web, производимые автоматизированно. В том числе будет запрещено исполнение скриптов, эмулирующих работу пользователя с программой Dr.Web и запущенных самим пользователем.
- Включите опцию **Защищать паролем настройки Dr.Web**, чтобы ограничить доступ к настройкам Dr.Web на станции при помощи пароля. Пароль будет запрашиваться каждый раз при обращении к настройкам Dr.Web и параметрам компонентов.
- Включите опцию **Включить поддержку ПО для чтения с экрана**, чтобы разрешить использование программ экранного доступа, таких как JAWS и NVDA, для озвучивания элементов интерфейса Dr.Web.
- Включите опцию **Собирать информацию о дисковом пространстве**, чтобы собирать информацию о дисках, используемых на станции, общем объеме дисков и свободном пространстве. При включенной опции выберите в выпадающем списке **Периодичность сбора информации о дисковом пространстве на станциях** значение временного интервала для отправки Агентом на Сервер Dr.Web актуальной информации о дисках, используемых на станции. Минимальное значение составляет 1 минуту.
- Включите опцию **Собирать информацию о пользователях**, чтобы предоставить Серверу Dr.Web доступ к информации об учетных записях пользователей на станции.
- Включите опцию **Собирать информацию об устройствах**, чтобы предоставить Серверу Dr.Web доступ к информации об устройствах, подключенных к станции.

3.2.4.2. Мобильность

На вкладке **Мобильность** вы можете настроить параметры работы Агента в Мобильном режиме:

- В поле **Периодичность обновления** укажите временной промежуток между обновлениями антивирусного ПО на станции с серверов ВСО.

  При выборе варианта **Вручную** автоматические обновления будут отключены. В этом случае для получения последних вирусных баз пользователь должен самостоятельно запустить обновление в настройках Агента на станции.
- Включите опцию **Использовать прокси-сервер** для использования HTTP прокси-сервера при получении обновлений через интернет. При этом станут активными поля настроек используемого прокси-сервера.

Обновление мобильных Агентов Dr.Web

Если компьютер пользователя долгое время не будет иметь связи с Сервером Dr.Web, для своевременного получения обновлений с серверов ВСО Dr.Web рекомендуется установить мобильный режим работы Агента Dr.Web на станции.

В мобильном режиме Агент пытается подключиться к Серверу Dr.Web, делает три попытки и, если не удалось, выполняет HTTP-обновление. Попытки найти Сервер Dr.Web идут непрерывно с интервалом около минуты.

Включение мобильного режима в настройках Агента будет доступно при условии, что использование мобильного режима разрешено в Центре управления в разделе **Антивирусная сеть** → **Права** → **Windows** → **Общие** → **Изменение конфигурации Агента Dr.Web**.

Во время функционирования Агента в мобильном режиме связь Агента с Сервером Dr.Web прерывается. Все изменения, которые задаются на Сервере Dr.Web для такой станции, вступят в силу, как только мобильный режим работы Агента будет выключен, и связь Агента с Сервером Dr.Web возобновится.

В мобильном режиме производится обновление только вирусных баз.

Описание настроек Мобильного режима на стороне Агента приведено в **Руководстве пользователя** Агент Dr.Web для Windows.

3.2.4.3. Журнал

На вкладке **Журнал** вы можете настроить параметры ведения журнала Агента и некоторых компонентов Антивируса Dr.Web:

- **Уровень детализации журнала Агента** определяет уровень подробности ведения журналов по работе Агента (файлы `dwservice.log` и `es-service.log`).
- **Уровень детализации журнала движка** определяет уровень подробности ведения журнала по работе поискового движка (записывается в системный журнал событий).
- **Уровень детализации журнала обновлений** определяет уровень подробности ведения журнала по работе модуля обновлений Dr.Web (файл `dwupdater.log`).
- Включите опцию **Создавать дампы памяти при ошибках проверки**, чтобы создавать дампы памяти в случаях возникновения ошибок при сканировании. Рекомендуется включать данную настройку для анализа ошибок в работе Dr.Web.
- Включите опцию **Установить ограничения на файл журнала Агента**, чтобы ограничить количество файлов журнала, размер каждого файла или длительность их записи.

- **Максимальное количество файлов** — максимальное количество файлов журнала (включая текущий и архивные), которые будут храниться.
  - Включите опцию **Архивировать файлы журнала**, чтобы упаковывать в архив старые файлы журнала в процессе ротации.
- **Режим ротации журнала** — режим ротации работы журнала. Выберите одно из представленных значений:
  - **ротация по размеру** определяет ограничение на размер каждого из файлов журнала.

  Максимальный размер каждого файла — максимально допустимый размер каждого файла журнала. Когда текущий файл достигает заданного размера, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.
  - **ротация по времени** определяет длительность записи каждого из файлов журнала.

  Максимальное время записи файла — максимальная длительность для записи каждого файла журнала. Когда время записи файла достигает заданной длительности, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.

3.2.4.4. Интерфейс

На вкладке **Интерфейс** вы можете настроить параметры интерфейса Агента Dr.Web:

- Включите опцию **Отображать значок на панели задач**, чтобы выводить значок Агента на панели задач. Если значок отключен, пользователь не сможет просматривать и изменять настройки Агента и антивирусного пакета.
- Включите опцию **Отображать запрос на перезагрузку при обновлении компонентов**, чтобы выводить запрос на перезагрузку станции, если были получены обновления антивирусных компонентов для применения которых требуется перезагрузка. Если опция отключена, оповещение на станции не выводится, автоматическая перезагрузка не осуществляется. В статистике станции, получаемой Центром управления, будет сообщено о необходимости перезагрузки станции. Информация о состоянии, требующем перезагрузку, отображается в таблице **Состояния**. При необходимости администратор может перезагрузить станцию из Центра управления.

Опция **Отображать запрос на перезагрузку при обновлении компонентов** не влияет на отображение запросов о перезагрузке, требуемых для завершения лечения обнаруженных угроз или изменения состояния аппаратной виртуализации. Данные запросы будут отображаться всегда.

Чтобы отметить типы сообщений о событиях, которые будет получать пользователь, включите соответствующие опции:

- **Критические оповещения** — получать только критические оповещения о следующих событиях:

- обнаружены соединения, ожидающие ответа Брандмауэра;
- имя пользователя (идентификатор) станции и пароль уже используются для подключения к Серверу Dr.Web.

Сообщение выводится только в том случае, если пользователь имеет права администратора.

- **Оповещения об угрозах** — получать только оповещения об угрозах. К данному типу оповещений относятся сообщения об обнаружении угроз безопасности одним из компонентов антивирусного ПО.
- **Важные оповещения** — получать только важные оповещения о следующих событиях:
  - истекает время работы за компьютером;
  - доступ к устройству заблокирован;
  - доступ к защищаемому объекту заблокирован Превентивной защитой;
  - заблокирована попытка изменения системных даты и времени;
  - вирусные базы устарели (при работе в Мобильном режиме);
  - доступна новая версия продукта;
  - запуск процесса заблокирован администратором из Центра управления;
  - установка пакета MSI заблокирована администратором из Центра управления;
  - запуск скрипта заблокирован администратором из Центра управления;
  - процессу запрещена загрузка объекта;
  - процессу запрещено создание исполняемого файла;
  - процессу запрещена модификация исполняемого файла.
- **Малозначительные оповещения** — получать только малозначительные оповещения о следующих событиях:
  - успешное обновление;
  - ошибка обновления;
  - истекает время работы в интернете;
  - URL заблокирован модулем Офисный контроль;
  - URL заблокирован SpIDer Gate;
  - доступ к защищаемому объекту заблокирован модулем Офисный контроль;
  - процесс сканирования станции запущен администратором из Центра управления;
  - процесс сканирования станции запущен согласно централизованному расписанию;
  - сканирование станции завершено.

Если вы хотите, чтобы пользователь получал все группы сообщений, включите все четыре опции. В противном случае будут выводиться только сообщения указанных групп.

Оповещения о некоторых событиях не входят в перечисленные группы и всегда показываются пользователю:

- установка приоритетных обновлений, для которых требуется перезагрузка;
- перезагрузка для завершения обезвреживания угроз;
- запрос на разрешение процессу модификации объекта;
- сообщение, отправленное администратором из Центра управления;
- USB-устройство (клавиатура) подключено/заблокировано в рамках защиты от BadUSB-уязвимости;
- успешное подключение к серверу.

В подразделе **Дополнительно** задаются следующие настройки:

- Включите опцию **Не показывать уведомления в полноэкранном режиме**, чтобы отключить всплывающие уведомления, если какая-либо программа запущена в полноэкранном режиме.
- Включите опцию **Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме**, чтобы уведомления от Брандмауэра Dr.Web отображались на отдельном рабочем столе, т. е. поверх запущенного полноэкранного приложения. Рекомендуется включить данную настройку, чтобы избежать блокировки сетевых подключений, используемых приложением, запущенным в полноэкранном режиме, без возможности их разрешения в момент поступления требования от Брандмауэра Dr.Web.

3.2.4.5. События

Агент Dr.Web передает на Сервер Dr.Web сообщения о следующих событиях:

- запуске и завершении работы программы;
- обнаружении угроз;
- выполнении заданий Планировщиком;
- блокировке устройств.

Сообщения передаются на Сервер Dr.Web в момент наступления события. Если передача данных запрещена, сообщения накапливаются в базе данных. Сообщения будут отправлены на Сервер Dr.Web, когда отправка событий будет разрешена.

Чтобы изменить режим отправки событий, включите опцию **Ограничить отправку событий**. По умолчанию опция выключена.

В таблице временных промежутков задается режим ограничения отправки событий в цветовой градации, приведенной под таблицей:

- белый цвет — **Без ограничений**;
- красный цвет — **Передача данных запрещена**: полная блокировка отправки событий.

При этом ограничение задается отдельно на каждые 30 минут каждого дня недели.

Для изменения режима ограничений доступа нажмите на соответствующий блок таблицы. Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей. Также поддерживается выбор нескольких временных блоков по принципу drag-and-drop.

3.2.5. Офисный контроль

В этом разделе:

- Общие настройки
- Групповые настройки

3.2.5.1. Общие настройки

В разделе **Общие настройки** вы можете:

- настроить доступ к ресурсам локальной файловой системы;
- запретить доступ к определенным классам и шинам устройств;
- настроить доступ приложений к веб-камерам и микрофонам, подключенным к станции.

3.2.5.1.1. Устройства

На вкладке **Устройства** вы можете настроить доступ к ресурсам локальной файловой системы и ограничить их использование:

- Включите опцию **Запрещать передачу данных по сети**, чтобы блокировать передачу данных по локальным сетям и через интернет. Обратите внимание, передача данных блокируется по сетевым протоколам NetBIOS и HTTP/HTTPS. Передача данных по протоколу ICMP не блокируется.

  Включение опции может нарушить подключение станций к Серверу Dr.Web. Рекомендуется сначала активировать ее для ограниченного числа станций и убедиться, что подключение стабильно, и после этого распространять опцию на все станции.

- Включите опцию **Блокировать отправку заданий на принтер**, чтобы запретить передачу на принтер задания на печать.
- Включите опцию **Проверять подключенные USB-устройства на наличие BadUSB-уязвимости**, чтобы проверять, действительно ли подключаемое USB-устройство является клавиатурой.
- Включите опцию **Контролировать доступ к защищаемым объектам**, чтобы получить возможность редактировать список блокируемых шин и классов устройств.

Блокировка устройств

Вы можете ограничить доступ к определенным шинам и классам устройств, а также настроить список разрешенных устройств.

Под классами устройств понимаются устройства, выполняющие одинаковые функции, например, устройства для печати. Под шинами — подсистемы передачи данных между функциональными блоками компьютера, например, шина USB.

Вы можете заблокировать один или несколько классов устройств на всех шинах или заблокировать все устройства, подключенные к одной или нескольким шинам.

Если вы не знаете, к какому классу относится устройство и на какой шине расположен определенный класс устройств, воспользуйтесь Диспетчером устройств Windows.

1. В Диспетчере устройств Windows найдите нужное устройство. При необходимости раскройте пункты указанных типов устройств.

   Пункт, к которому относится устройство, является классом устройства (например, флеш-накопитель относится к классу **Дисковые устройства**).
2. Выберите это устройство, вызовите контекстное меню и нажмите **Свойства**.
3. На вкладке **Сведения** в выпадающем списке **Свойство** выберите **Родитель**.
4. В поле **Значение** будет указана строка вида *Шина\UID устройства*.

   Например, для флеш-накопителя будет указана строка *USB\VID_1EAB&PID_0501\03421*, где USB — это шина, на которой расположен класс устройства.

Чтобы настроить список заблокированных классов устройств

1. Убедитесь, что опция **Контролировать доступ к защищаемым объектам** включена.
2. В разделе **Классы устройств** нажмите  , чтобы добавить устройство в список **Блокируемых классов**.
3. В открывшемся окне выберите те классы устройств, доступ к которым должен быть заблокирован. Для этого установите опцию **Запрещать** напротив соответствующего класса в приведенном списке.
4. Нажмите **Сохранить**.
5. Чтобы удалить устройство из списка, выберите его в списке и нажмите  .
6. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

Чтобы настроить список заблокированных шин

1. Убедитесь, что опция **Контролировать доступ к защищаемым объектам** включена.
2. В разделе **Шины устройств** нажмите  , чтобы добавить устройство в список **Блокируемых шин**.

3. Выберите из выпадающего списка те шины, доступ к которым должен быть заблокирован.
4. Выберите классы, которые будут заблокированы на этой шине. Чтобы заблокировать шину целиком, выберите все классы.
5. Нажмите **Сохранить**.
6. Чтобы удалить устройство из списка, выберите его в списке и нажмите  .
7. Чтобы отредактировать список классов, заблокированных на данной шине, выберите ее в списке **Блокируемых шин** и нажмите  .
8. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

Пример

Если вам нужно заблокировать все флеш-накопители:

1. Убедитесь, что опция **Контролировать доступ к защищаемым объектам** включена.
2. В разделе **Шины устройств** нажмите  .
3. Выберите из выпадающего списка шину **Устройства USB**.
4. Выберите класс **Дисковые устройства**, который будет заблокирован на этой шине.
5. Нажмите **Сохранить**.

Если вы хотите отдельно разрешить доступ к определенному устройству, добавьте его в список разрешенных устройств.

В разделе **Антивирусная сеть** > **Статистика** > **Заблокированные устройства** может отсутствовать значение в столбце **Пользователь**. Это происходит, если задана блокировка устройств по классу или шине и для устройства такого типа не заданы индивидуальные настройки доступа к операциям чтения и записи для определенных пользователей или групп. Блокировка устройства производится без привязки к пользователю.

При включении опции **Контролировать доступ к защищаемым объектам** > **Классы устройств** > **Сетевые адаптеры** станции не смогут подключиться к Серверу Dr.Web.

Данная опция запрещает все сетевое взаимодействие для станции. При этом любое удаленное изменение настроек через Центр управления также невозможно.

Блокировка работает только для устройств, подключенных после активации функции. Чтобы активировать блокировку уже подключенного устройства, выполните одно из следующих действий:

- подключите устройство заново;
- перезапустите устройство с помощью диспетчера устройств;
- перезагрузите компьютер.

3.2.5.1.2. Камеры и микрофоны

На вкладке **Камеры и микрофоны** вы можете настроить доступ приложений к подключенным веб-камерам и микрофонам:

- **Разрешать** — всегда разрешать доступ к веб-камерам и микрофонам для приложений.
- **Запрещать** — всегда запрещать доступ к веб-камерам и микрофонам для приложений.
- **Спрашивать** — выводить диалоговое окно для задания необходимого действия самим пользователем для конкретных веб-камер и микрофонов.

Исключения

Вы можете добавить в список исключений приложения, для которых будут применяться отдельные правила. По умолчанию список пуст.

Формирование списка исключений

1. В поле ввода задайте путь к приложению.
2. Выберите, какое действие будет применяться к указанному приложению: **Разрешать**, **Запрещать**, **Спрашивать**.
3. В каждом поле задается только одно приложение. Чтобы добавить еще одно приложение в список, нажмите кнопку  .
4. Чтобы удалить приложение из списка исключений, нажмите  напротив элемента списка, соответствующего этому приложению.

3.2.5.2. Групповые настройки

В разделе **Групповые настройки** вы можете:

- настроить доступ пользователей станции к локальным и сетевым ресурсам;
- контролировать время работы в интернете и за компьютером;
- добавить доверенные устройства в список разрешенных.

3.2.5.2.1. Настройки доступа

На вкладке **Настройки доступа** задаются параметры доступа пользователей станции к сайтам, локальным каталогам и файлам компьютера, а также контролируется время работы в интернете и за компьютером.

Параметры Офисного контроля распространяются одновременно на всех пользователей компьютера, на котором установлен Dr.Web для ОС Windows. По умолчанию для всех учетных записей разрешен неограниченный доступ к локальным ресурсам и к интернет-ресурсам, ограничения по времени отсутствуют.

Параметры Офисного контроля

Настройки, задаваемые на вкладке, распространяются одновременно на все учетные записи пользователей. Как настроить параметры для отдельных пользователей и групп пользователей, описано в разделе Отдельные настройки для пользователей и групп пользователей.

Веб-фильтр

- Выберите режим **Без ограничений**, чтобы доступ к сайтам не контролировался. При этом адреса из белого и черного списков не обрабатываются. Этот режим установлен по умолчанию.
- Выберите режим **Блокировать по категориям**, чтобы самостоятельно указать категории тех ресурсов, доступ к которым будет запрещаться или разрешаться вне зависимости от других ограничений. При этом обрабатываются адреса из белого и черного списков.
- Выберите режим **Блокировать всё, кроме сайтов из белого списка**, чтобы запретить доступ ко всем веб-ресурсам, кроме указанных в белом списке. При этом адреса из черного списка не обрабатываются.

В любом из режимов, кроме режима **Без ограничений**, вы можете активировать опцию **Включить безопасный поиск**, которая влияет на выдачу результатов поисковых систем. Эта функция позволяет исключить нежелательные ресурсы из результатов поиска.

Белый и черный списки сайтов

Вы можете задать списки сайтов, доступ к которым разрешается или блокируется. По умолчанию списки пусты. При необходимости вы можете добавить адреса сайтов в белый и черный список (если выбран режим **Блокировать по категориям**) или только в белый список (если выбран режим **Блокировать всё, кроме сайтов из белого списка**).

Формирование списка доменных адресов

1. Введите доменное имя или часть доменного имени сайта в поле **Белый список** или **Черный список**, в зависимости от того, хотите ли вы разрешить или запретить доступ к нему соответственно:
   a) Чтобы добавить в список определенный сайт, введите его адрес (например, `www.example.com`). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью.
   b) Чтобы настроить доступ к сайтам с похожими именами, введите в поле общую часть их доменных имен. Пример: если вы введете текст `example`, то доступ к `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` и другим похожим сайтам будет определяться данной записью.

c) Чтобы настроить доступ к сайтам на определенном домене, укажите имя домена с символом «.», например, `.ru`. В таком случае доступ ко всем ресурсам, находящимся на этом домене, будет определяться данной записью.

Если при указании домена используется символ «/», то та часть подстроки, что стоит слева от символа «/», будет считаться доменным именем, а части справа от символа — частью разрешенного на данном домене адреса. Пример: если вы введете текст `example.com/test`, то будут обрабатываться такие адреса как `example.com/test11`, `template.example.com/test22` и т. п.

d) Чтобы добавить в исключения определенные сайты, введите определяющую их маску в поле ввода. Маски добавляются в формате: `mask://...`

Маска задает общую часть имени объекта, при этом:

- символ «*» заменяет любую, возможно пустую, последовательность символов;
- символ «?» заменяет любой, в том числе пустой, но только один символ.

Примеры

- `mask://*.ru/` или `.ru` — в исключения будут добавлены все сайты в домене .ru;
- `mask://mail` — в исключения будут добавлены все сайты, в именах которых содержится слово "mail";
- `mask://???.ru/` — будут открываться все сайты зоны .ru, имена которых состоят из трех или менее знаков.

Введенная строка при добавлении в список может быть преобразована к универсальному виду. Например: адрес `http://www.example.com` будет преобразован в запись `www.example.com`.

2. Чтобы добавить еще один объект в список, нажмите  .
3. Чтобы удалить адрес из списка, нажмите  напротив элемента списка, соответствующего этому адресу.
4. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

Для зашифрованного трафика (HTTPS-сайты) белый и черный списки могут содержать только доменные адреса (например, `https://example.com`).

Доступ к отдельным страницам домена можно настроить только для незашифрованного трафика (HTTP-сайты) (например, `http://example.com/test`).

Каталоги и файлы

Включите опцию **Защищать каталоги и файлы**, чтобы заблокировать доступ ко всем объектам, указанным в списке ниже.

Для формирования списка защищаемых объектов

1. Чтобы добавить необходимый объект, задайте путь к нему в соответствующем поле.
2. Выберите режим ограничения:
   a) **Только чтение** — добавленный объект будет доступен пользователю только для чтения.
   b) **Заблокировано** — полностью заблокировать доступ к заданному объекту.
3. В каждом поле задается только один объект. Чтобы добавить еще один объект в список, нажмите  .
4. Чтобы удалить объект из списка, нажмите  напротив элемента списка, соответствующего этому объекту.
5. Чтобы снять все ограничения сразу для всех объектов списка, отключите опцию **Защищать каталоги и файлы**.

Ограничение времени

Вы можете задать промежутки времени, в течение которых пользователям будет запрещен доступ к интернету или полностью заблокирован доступ к компьютеру. По умолчанию пользователям разрешено работать за компьютером и в интернете неограниченное время.

Чтобы установить режим ограничения времени для конкретного профиля

1. Нажмите  , чтобы добавить профиль в список.
2. В появившемся поле укажите имя для нового профиля.
3. Нажмите **Сохранить**.
4. Чтобы удалить профиль из списка, выберите его в списке и нажмите  .
5. При необходимости повторите шаги 1–3 для добавления других профилей.
6. Задайте режим ограничения доступа с помощью таблицы временных промежутков.

Также вы можете внести изменения в таблицу, не добавляя новый профиль. В этом случае все изменения будут сохранены в профиле **Пользовательский**.

Работа с таблицей ограничения времени

С помощью таблицы можно указать дни недели и часы, когда пользователь может работать за компьютером, а также в интернете. При этом ограничение задается отдельно на каждые 30 минут каждого дня недели.

Цвет	Режим ограничения	Описание режима

Белый	Без ограничений	В указанный период доступ к компьютеру и интернет-ресурсам разрешен. Установлен по умолчанию.
Синий	Блокировать доступ в интернет	В указанный период доступ ко всем интернет-ресурсам заблокирован. С началом действия ограничений доступ ко всем сайтам будет заблокирован.
Красный	Запретить все	В указанный период доступ к компьютеру полностью заблокирован. С началом действия ограничений произойдет выход пользователя из учетной записи.

Чтобы ограничить время доступа в интернет

Выберите дни недели и часы, когда требуется *ограничить пользователю выход в интернет*, и выделите соответствующие временные ячейки синим цветом:

- чтобы выделить одну ячейку, нажмите по ней один раз левой кнопкой мыши;
- чтобы одновременно выделить несколько расположенных рядом ячеек, один раз нажмите левой кнопкой мыши по первой ячейке и, удерживая кнопку нажатой, выделите весь необходимый период.

Чтобы ограничить время работы за компьютером

Выберите дни недели и часы, когда требуется *ограничить пользователю работу за компьютером*, и выделите соответствующие временные ячейки красным цветом:

- чтобы выделить одну ячейку, дважды нажмите по ней левой кнопкой мыши;
- чтобы одновременно выделить несколько расположенных рядом ячеек, дважды нажмите левой кнопкой мыши по первой ячейке и, удерживая кнопку нажатой, выделите весь необходимый период.

Отдельные настройки для пользователей и групп пользователей

При необходимости вы можете задать настройки для отдельных пользователей или групп пользователей, отличные от общих настроек.

Чтобы задать отдельные настройки для пользователей или групп пользователей

1. Нажмите кнопку **Особые настройки**.

2. Выберите пользователя или группу пользователей в подразделах дерева в левой части окна.
3. Если настройки еще не заданы, нажмите ссылку **Задать настройки**. Скопируются настройки из корневой группы, которые можно по желанию изменять. Изменение настроек происходит аналогично основным настройкам Офисного контроля.
4. Если пользовательские настройки заданы, их можно удалить. Для этого выберите соответствующую группу пользователей или пользователя и нажмите  . При этом будут использоваться настройки корневой группы.
5. Закройте окно **Особые настройки для групп пользователей**. Изменения сохраняются при закрытии окна.

Структура пользователей станции

- Структура пользователей станции отображается в виде дерева, состоящего из групп пользователей и самих пользователей. По умолчанию заданы группы **Администраторы**, **Гости** и **Пользователи**.
- Все существующие группы пользователей становятся доступны после подключения станции к Серверу Dr.Web.
- Если в вашей локальной сети развернута служба Active Directory, вы можете добавить ее пользователей. Для этого необходимо выполнить задание **Синхронизация с Active Directory** в **Планировщике заданий Сервера Dr.Web** (см. раздел Настройка расписания Сервера Dr.Web в **Руководстве администратора** Dr.Web Enterprise Security Suite).

Типы пользовательских настроек

- *Общие* — настройки корневой группы **Пользователи**, которые используются по умолчанию.
- *Наследуемые* — настройки, которые наследуются от корневой группы **Пользователи** в случае, если настройки для групп пользователей и отдельных пользователей не заданы. При этом раздел пользовательских настроек пуст.
- *Персональные* — настройки групп пользователей и отдельных пользователей, которые не наследуются от корневой группы.

Для пользователей, не имеющих персональных настроек и состоящих в одной или нескольких группах, объединяются все настройки для групп и общие настройки с приоритетом запрета.

3.2.5.2.2. Разрешенные устройства

Если вы ограничили доступ к каким-либо шинам или классам устройств, вы можете отдельно разрешить доступ к определенным устройствам, добавив их в список разрешенных.

В список можно добавлять любые типы устройств, в том числе устройства на съемных носителях (USB флеш-накопителях, дискетах, CD/DVD приводах, ZIP-дисках и т. п.), клавиатуры, принтеры, сетевые адаптеры и др. Также в список разрешенных можно добавить конкретное устройство, чтобы не проверять его на наличие BadUSB-уязвимости.

Чтобы составить общий список разрешенных устройств

1. Включите опцию **Разрешить использование заданных устройств**. Доступ к разрешенным устройствам из общего списка предоставляется всем пользователям компьютера, на котором установлен Dr.Web для Windows.
2. Нажмите кнопку  , чтобы добавить устройство в список.
3. В окне **Добавление устройств в список разрешенных** воспользуйтесь следующими возможностями:
   - Выберите устройство в поле **Устройства, подключаемые ранее** и с помощью стрелочки перенесите его в поле **Устройства для добавления в список разрешенных**.

     Выбранный элемент можно добавить в поле **Устройства для добавления в список разрешенных** как устройство или как маску. Маска позволяет исключить из проверки устройство, которое генерирует новый ID при каждом подключении к станции. Добавление устройства по маске возможно только в формате `USBSTOR\DISK*\*` (т. е. присутствуют все символы «\»).

   - Задайте ID устройства вручную в соответствующем поле и нажмите  .

     Список устройств, подключенных ранее, становится доступен после подключения станции к Серверу Dr.Web.

4. Нажмите **Сохранить**.
5. Чтобы удалить устройство из списка, выберите его в списке и нажмите  .
6. При необходимости повторите шаги 2 и 3 для добавления других ресурсов.
7. Для устройств с собственной файловой системой вы можете задать отдельно права только на чтение или на чтение и запись. Для этого в таблице **Разрешенные устройства** включите опцию **Чтение** для просмотра устройств и **Запись** для их изменения. Права на запись нельзя задать без активных прав на чтение.

Для устройств с собственной файловой системой доступна настройка отдельных правил для пользователей и групп пользователей.

Чтобы задать отдельные права для пользователей или групп пользователей

1. В таблице **Разрешенные устройства** выберите устройство с файловой системой, доступ к которому вы хотите настроить. Нажмите . Откроется окно **Настройка прав доступа к устройству**.
2. Выберите группу пользователей или пользователя (см. Типы пользовательских настроек) в левой части окна. С помощью стрелочки перенесите группу пользователей или пользователя в поле **Группы с особыми правами доступа**.
3. Включите опцию **Запись**, чтобы предоставить полные права доступа. Опция **Чтение** дает возможность только просматривать устройства.
4. Закройте окно **Настройка прав доступа к устройству**. Изменения сохраняются при закрытии окна.

Права, заданные в таблице **Разрешенные устройства**, применяются к группе **Everyone**, а именно ко всем пользователям станции. Права, заданные в поле **Группы с особыми правами доступа**, настраивают доступ для отдельных пользователей или групп пользователей и имеют приоритет над общими правами.

Если для устройства заданы настройки доступа пользователей или групп пользователей к операциям чтения и записи, в разделе **Антивирусная сеть** > **Статистика** > **Заблокированные устройства** в таблице также приводится информация о пользователе, от лица которого была запущена заблокированная операция.

Чтобы составить список разрешенных устройств для групп станций

1. Выберите соответствующую группу станций.
2. Перейдите в раздел **Разрешенные устройства**.
3. Включите опцию **Разрешить использование заданных устройств**.
4. Нажмите кнопку , чтобы добавить устройство в список.
5. В окне **Добавление устройств в список разрешенных** выберите станцию. Откроется список устройств, подключенных ранее на этой станции.
6. Затем в поле **Устройства, подключаемые ранее** выберите устройство и с помощью стрелочки перенесите его в поле **Устройства для добавления в список разрешенных**. ID устройства появится в поле **Задайте ID устройств вручную**.

Выбранный элемент можно добавить в поле **Устройства для добавления в список разрешенных** как устройство или как маску. Маска позволяет исключить из проверки устройство, которое генерирует новый ID при каждом подключении к станции. Добавление устройства по маске возможно только в формате `USBSTOR\DISK*\*` (т. е. присутствуют все символы «\»).

7. Нажмите **Сохранить**.
8. Чтобы удалить устройство из списка, выберите его в списке и нажмите .

9. Для устройств с собственной файловой системой вы можете задать отдельно права только на чтение или на чтение и запись. Для этого в таблице **Разрешенные устройства** включите опцию **Чтение** для просмотра устройств и **Запись** для их изменения. Правила обращения к устройствам с собственной файловой системой можно задать также для отдельных пользователей и групп пользователей.

3.2.6. SpIDer Guard

Для защиты файловой системы станций под управлением ОС Windows Enterprise multi-session (Windows Enterprise for Virtual Desktops) требуется лицензия, в состав которой входит компонент **SpIDer Guard для серверов Windows**.

В этом разделе:

- Настройка работы компонента SpIDer Guard
- Настройка проверки компонентом SpIDer Guard
- Исключение из проверки компонентом SpIder Guard
- Журнал событий компонента SpIder Guard

3.2.6.1. Общие

На вкладке **Общие** доступны настройки проверки рабочих станций и серверов компонентом SpIDer Guard.

1. **Режим проверки**:
   - **Оптимальный** (выбран по умолчанию). В этом режиме SpIDer Guard осуществляет проверку только в следующих случаях:
     - для объектов на жестких дисках — при запуске или создании файлов, а также попытке записи в существующие файлы или загрузочные секторы;
     - для объектов на съемных носителях — при любом обращении к файлам или загрузочным секторам (чтение, запись, выполнение).
   - **Параноидальный**. В этом режиме при любом обращении (создание, чтение, запись, выполнение) SpIDer Guard производит проверку всех файлов и загрузочных секторов на жестких и сетевых дисках, а также съемных носителях. Установка этого режима обеспечивает максимальный уровень защиты, но значительно увеличивает нагрузку на компьютер.
2. Опция **Использовать эвристический анализ** позволяет SpIDer Guard обнаруживать еще неизвестные вредоносные программы. По умолчанию опция включена. Если опция отключена, проверка проводится только по сигнатурам известных угроз.
3. Опция **Проверять на наличие руткитов** позволяет в фоновом режиме проводить проверку операционной системы станции на наличие сложных угроз и при необходимости проводит лечение активного заражения. При проведении фоновой

проверки на наличие руткитов из проверки исключаются файлы и папки, заданные на вкладке **Исключения**.

Выключение SpIDer Guard не влияет на фоновую проверку на наличие руткитов. Если опция включена, фоновая проверка осуществляется независимо от того, включен или выключен SpIDer Guard.

Дополнительные возможности

В этой группе настроек вы можете включить проверку определенных типов объектов, а также **Блокировать автозапуск со съемных носителей**. В любом из режимов (оптимальный или параноидальный) проверка объектов на сетевых дисках и съемных носителях производится только при включении соответствующих опций.

Проверка съемных носителей

SpIDer Guard по умолчанию проверяет файлы на съемных носителях информации (CD/DVD-дисках, флеш-накопителях и т. д.) при создании, чтении, изменении и запуске этих файлов, а также блокирует автоматический запуск их активного содержимого. Этот метод помогает предотвратить заражение вашего компьютера через съемные носители, так как SpIDer Guard в режиме реального времени отслеживает обращения к файловой системе и блокирует исполнение вредоносного кода.

Изменение названия файла без перемещения его со съемного носителя не является операцией модификации, поскольку меняются только метаданные файла, но не сам файл, поэтому проверка SpIDer Guard в таком случае не запустится.

Некоторые съемные носители (в частности, мобильные жесткие диски с интерфейсом USB) могут представляться в системе как жесткие диски. В этом случае в области уведомлений Windows не отображается значок «Безопасное извлечение устройств и дисков». При чтении файла с такого диска SpIDer Guard не осуществляет проверку, если не выбран параноидальный режим, поэтому такие диски рекомендуется проверять на наличие угроз при подключении к компьютеру с помощью Сканера Dr.Web.

3.2.6.2. Действия

На вкладке **Действия** выберите действия, которые будут применяться к угрозам, обнаруженным компонентом SpIDer Guard, в зависимости от их типа.

- **Лечить, перемещать в карантин неизлечимые**. Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и вредоносных файлов внутри составных объектов.

- **Лечить, удалять неизлечимые**. Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и вредоносных файлов внутри составных объектов.
- **Перемещать в карантин**. Обнаруженная угроза помещается в специальную папку, изолированную от остальной системы.
- **Удалять**. Наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- **Игнорировать**. К объекту не применяется никакое действие, оповещение об обнаруженном объекте не появляется.
- **Сообщать**. Выводить оповещение и пропустить объект без выполнения каких-либо действий.

Предустановленные настройки являются оптимальными для большинства случаев, не изменяйте их без необходимости.

Действия SpIDer Guard над обнаруженными вредоносными объектами

Объект	Действие					
	Лечить, перемещать в карантин неизлечимые	**Лечить, удалять неизлечимые**	**Перемещать в карантин**	**Удалять**	**Игнорировать**	**Сообщать**
Вредоносные	+/*	+	+	+		
Подозрительные			+/*	+	+	+
Вредоносные инсталляционные пакеты			+/*	+	+	+
Вредоносные архивы			+/*	+	+	+
Вредоносные почтовые файлы			+/*		+	+
Рекламные программы			+/*	+	+	+
Программы дозвона			+/*	+	+	+
Программы-шутки			+	+	+	+/*

Объект	Действие					
	Лечить, перемещать в карантин неизлечимые	Лечить, удалять неизлечимые	Перемещать в карантин	Удалять	Игнорировать	Сообщать
Потенциально опасные			+	+	+	+/*
Программы взлома			+	+	+	+/*

Условные обозначения

+	действие разрешено для данного типа объектов
+/*	действие установлено как реакция по умолчанию для данного типа объектов

3.2.6.3. Исключения

На вкладке **Исключения** задается список каталогов и файлов, исключаемых из проверки компонентом SpIDer Guard.

При включении опции **Исключать из сканирования системные файлы** из проверки исключаются системные файлы, входящие во внутренний список компонента SpIDer Guard. Список составляется для каждой версии ОС Windows на основе рекомендаций от компании Microsoft по использованию антивирусных программ.

При включении этой опции станут доступны следующие настройки:

- **Исключать файлы БД Prefetcher** — предписывает исключение из проверки файлов базы данных системного компонента Prefetcher.
- **Исключать файлы БД Windows поиска** — предписывает исключение из проверки файлов базы данных службы поиска ОС Windows.

Формирование списка исключений

1. Чтобы добавить файл, каталог или процесс к списку исключений, выполните одно из следующих действий:
   - чтобы указать конкретный существующий объект, вручную задайте полный путь в соответствующем поле ввода (вы можете использовать переменные среды);
   - чтобы исключить из проверки все объекты с определенным именем, задайте это имя в поле ввода. Указывать путь к объекту при этом не требуется;
   - чтобы исключить из проверки объекты определенного вида, задайте определяющую их маску в поле ввода.;

Маска задает общую часть имени объекта, при этом

- символ «*» заменяет любую, возможно пустую, последовательность символов;
- символ «?» заменяет любой, но только один символ;
- остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.

Примеры:

- `отчет*.doc` — маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например, файлы `отчет-февраль.doc`, `отчет121209.doc` и т. д.;
- `*.exe` — маска, задающая все исполняемые файлы с расширением EXE, например, `setup.exe`, `iTunes.exe` и т. д.;
- `photo????09.jpg` — маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например, `photo121209.jpg`, `photomama09.jpg` или `photo----09.jpg`.
- `file*` — исключает из проверки все файлы с любыми расширениями, имя которых начинается с `file`, во всех папках.
- `file.*` — исключает из проверки все файлы с именем `file` и любым расширением во всех папках.
- `C:\folder\**` — исключает из проверки все файлы в папке `C:\folder` и всех подпапках на любом уровне вложенности.
- `C:\folder\*` — исключает из проверки файлы в папке `C:\folder`. В подпапках файлы будут проверяться.
- `C:\folder\*.txt` — исключает из проверки файлы `*.txt` в папке `C:\folder`. В подпапках файлы `*.txt` будут проверяться.
- `C:\folder\*\*.txt` — исключает из проверки файлы `*.txt` только в подпапках первого уровня вложенности папки `C:\folder`.
- `C:\folder\**\*.txt` — исключает из проверки файлы `*.txt` в подпапках любого уровня вложенности папки `C:\folder`. В самой папке `C:\folder` файлы `*.txt` будут проверяться.

2. В каждом поле задается только один объект. Чтобы добавить еще один объект в список, нажмите кнопку  .
3. Чтобы удалить объект из списка исключений, нажмите кнопку  напротив элемента списка, соответствующего этому объекту.

3.2.6.4. Журнал

Включите опцию **Вести подробный журнал**, чтобы фиксировались такие события компонента SpIDer Guard, как обновления, запуск и его остановка, обнаруженные угрозы, а также данные об именах упаковщиков и содержимом проверяемых архивов.

Рекомендуется использовать этот режим для определения объектов, которые SpIDer Guard проверяет наиболее часто. При необходимости вы можете добавить такие объекты в список исключений, что может снизить нагрузку на компьютер.

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

При включении опции **Вести подробный журнал**, запись журнала работы соответствующего компонента осуществляется в режиме отладки с максимальной детализацией. Ограничения на размер файла в данном режиме снимаются. Это приводит к значительному увеличению размера файла журнала. Также обратите внимание, что ротация файла журнала не осуществляется (относится ко всем режимам ведения журнала).

Отладочный режим ведения журнала снижает производительность работы антивируса и операционной системы станции. Использовать этот режим следует только при возникновении проблем в работе компонентов и по запросу службы технической поддержки. Не рекомендуется включение отладочного режима ведения журнала на длительный срок.

На стороне Центра управления настройки ведения журнала задаются отдельно для каждого компонента в разделах **Журнал**. На станции настройки ведения журнала задаются в едином разделе **Дополнительно**.

3.2.7. Dr.Web для Microsoft Outlook

В этом разделе:

- Настройка работы модуля Dr.Web для Outlook
- Настройка проверки модулем Dr.Web для Outlook
- Журнал событий модуля Dr.Web для Outlook
- Параметры работы Антиспама

3.2.7.1. Общие

- Опция **Включить проверку** позволяет включить модуль Dr.Web для Outlook.
- Опция **Проверять архивы** позволяет включить или отключить проверку вложенных файлов, представляющих собой архивы.

3.2.7.2. Действия

На вкладке **Действия** вы можете выбрать действия, которые будут применяться к угрозам, обнаруженным компонентом Dr.Web для Outlook, в зависимости от их типа.

- **Лечить**. Восстановить состояние объекта до заражения. Если угроза неизлечима или попытка лечения не была успешной, то будет применено действие, заданное в списке **Неизлечимые**. Данное действие возможно только для объектов, в которых обнаружена известная излечимая угроза, за исключением троянских программ и вредоносных файлов внутри составных объектов.
- **Перемещать в карантин**. Обнаруженная угроза помещается в специальную папку, изолированную от остальной системы.
- **Удалять**. Наиболее эффективный способ устранения компьютерных угроз любых типов. Применение данного действия подразумевает полное удаление объекта, представляющего угрозу.
- **Игнорировать**. К объекту не применяется никакое действие, оповещение об обнаруженном объекте не появляется.

Предустановленные настройки являются оптимальными для большинства случаев, не изменяйте их без необходимости.

Действия Dr.Web для Outlook над обнаруженными вредоносными объектами

Объект	Действие			
	Лечить	Перемещать в карантин	Удалять	Игнорировать
Вредоносные	+/*	+	+	
Неизлечимые		+/*	+	
Подозрительные		+/*	+	+
Непроверенные		+	+	+/*
Рекламные программы		+/*	+	+
Программы дозвона		+/*	+	+
Программы-шутки		+/*	+	+
Потенциально опасные		+/*	+	+
Программы взлома		+/*	+	+

Условные обозначения

+	действие разрешено для данного типа объектов
+/*	действие установлено как реакция по умолчанию для данного типа объектов

3.2.7.3. Журнал

Включите опцию **Вести подробный журнал**, чтобы фиксировались сообщения об ошибках записи или чтения файлов, ошибках анализа архивов или файлов, защищенных паролем; а также параметры модулей программы: сканера, ядра, вирусных баз; сообщения об экстренных остановках ядра программы.

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

При включении опции **Вести подробный журнал**, запись журнала работы соответствующего компонента осуществляется в режиме отладки с максимальной детализацией. Ограничения на размер файла в данном режиме снимаются. Это приводит к значительному увеличению размера файла журнала. Также обратите внимание, что ротация файла журнала не осуществляется (относится ко всем режимам ведения журнала).

Отладочный режим ведения журнала снижает производительность работы антивируса и операционной системы станции. Использовать этот режим следует только при возникновении проблем в работе компонентов и по запросу службы технической поддержки. Не рекомендуется включение отладочного режима ведения журнала на длительный срок.

На стороне Центра управления настройки ведения журнала задаются отдельно для каждого компонента в разделах **Журнал**. На станции настройки ведения журнала задаются в едином разделе **Дополнительно**.

3.2.7.4. Антиспам

Для настройки параметров спам-фильтра:

- Включите опцию **Проверять почту на наличие спама** для активации спам-фильтра.

- Если вы хотите добавлять специальный текст в заголовок сообщения, распознанного как спам, включите опцию **Добавлять префикс к теме спам-писем**. Добавляемый текст введите в поле **Префикс**. По умолчанию добавляется префикс *****SPAM*****.
- Проверенные сообщения могут отмечаться как прочитанные в свойствах письма. Для этого необходимо включить опцию **Помечать как прочитанные**. По умолчанию опция **Помечать как прочитанные** включена.
- Также вы можете настроить белые и черные списки почтовых адресов и доменов для фильтрации писем:
  a) Укажите в соответствующем поле адрес. Правила задания адресов приведены ниже.
  b) В каждом поле задается только один адрес. Чтобы добавить еще один адрес в список, нажмите кнопку  .
  c) Чтобы удалить адрес из списка, нажмите кнопку  напротив элемента списка, соответствующего этому адресу.

Черный список

Если адрес отправителя добавлен в черный список, то письму без дополнительного анализа присваивается статус спам.

- Чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `spam@spam.ru`). Все письма, полученные с этого адреса, будут автоматически распознаваться как спам.
- Каждый элемент списка может содержать только один почтовый адрес или одну маску почтовых адресов.
- Чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ «`*`», который заменяет любую (в том числе пустую) последовательность любых символов.

  Например, допускаются следующие варианты:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

  Знак «`*`» может ставиться только в начале или в конце адреса.

  Символ «`@`» обязателен.

- Чтобы гарантированно помечать как спам письма с почтовых адресов в конкретном домене, используйте в адресе символ «`*`» вместо имени пользователя. Например,

чтобы помечать как спам все письма от адресантов из домена `spam.ru`, введите `*@spam.ru`.

- Чтобы гарантированно помечать как спам письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте в адресе символ «*» вместо имени домена. Например, чтобы помечать как спам все письма от адресантов с названием почтового ящика `ivanov`, введите `ivanov@*`.

Белый список

Если адрес отправителя добавлен в белый список, письмо не подвергается анализу на содержание спама.

- Чтобы добавить в список определенного отправителя, введите его полный почтовый адрес (например, `mail@example.net`). Все письма, полученные с этого адреса, будут доставляться без проверки на спам.
- Каждый элемент списка может содержать только один почтовый адрес или одну маску почтовых адресов.
- Чтобы добавить в список отправителей адреса определенного вида, введите маску, определяющую данные адреса. Маска задает шаблон для определения объекта. Она может включать обычные символы, допустимые в почтовых адресах, а также специальный символ «*», который заменяет любую (в том числе пустую) последовательность любых символов.

  Например, допускаются следующие варианты:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

  Знак «*» может ставиться только в начале или в конце адреса.

  Символ «@» обязателен.

- Чтобы гарантированно получать письма с почтовых адресов в конкретном домене, используйте в адресе символ «*» вместо имени пользователя. Например, чтобы получать все письма от адресантов из домена `example.net` без проверки, введите `*@example.net`.
- Чтобы гарантированно получать письма с почтовых адресов с конкретным именем пользователя с любого домена, используйте в адресе символ «*» вместо имени домена. Например, чтобы получать все письма от адресантов с названием почтового ящика `ivanov`, введите `ivanov@*`.

3.2.8. Брандмауэр Dr.Web

Если пользователю станции предоставлено право менять настройки **Брандмауэра Dr.Web**, то указывается, что заданы персональные настройки.

В этом разделе:

- Фильтрация на уровне приложений
- Фильтрация на уровне пакетов
- Ведение подробного журнала

3.2.8.1. Фильтр приложений

Большинство настроек **Фильтра приложений** задается только на станции, см. **Агент Dr.Web для Windows. Руководство пользователя**.

Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам, а также разрешить или запретить этим приложениям запуск других процессов. Вы можете задавать правила как для пользовательских, так и для системных приложений.

Выбор режима работы

Выберите один из следующих режимов фильтрации трафика на уровне приложений:

- Разрешать неизвестные соединения — режим, при котором всем неизвестным приложениям предоставляется доступ к сетевым ресурсам;
- Блокировать неизвестные соединения — режим, при котором все неизвестные подключения автоматически блокируются. Известные соединения обрабатываются Брандмауэром согласно заданным правилам фильтрации;
- Интерактивный режим — режим обучения, при котором пользователю предоставляется полный контроль над реакцией Брандмауэра;
- Разрешать соединения для доверенных приложений — режим, при котором всем доверенным приложениям предоставляется доступ к сетевым ресурсам, для всех остальных приложений выдается предупреждение, где вы можете задать правило (используется по умолчанию).

Разрешать неизвестные соединения

В этом режиме доступ к сетевым ресурсам, включая интернет, предоставляется всем неизвестным приложениям, для которых не заданы правила фильтрации. При обнаружении попытки подключения Брандмауэр не выводит никаких сообщений.

Блокировать неизвестные соединения

В этом режиме все неизвестные подключения к сетевым ресурсам, включая интернет, автоматически блокируются.

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым ресурсам Брандмауэр проверяет, заданы ли для этих программ правила фильтрации. Если правила фильтрации отсутствуют, то Брандмауэр автоматически блокирует доступ к сети и не выводит никаких сообщений. Если правила фильтрации для данного подключения заданы, то выполняются указанные в них действия.

Интерактивный режим

В этом режиме вам предоставляется полный контроль над реакцией Брандмауэра на обнаружение неизвестного подключения, и таким образом производится обучение программы в процессе вашей работы за компьютером.

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым ресурсам Брандмауэр проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вам предлагается выбрать либо временное решение, либо создать правило, по которому в дальнейшем подобные подключения будут обрабатываться.

Разрешать соединения для доверенных приложений

Этот режим используется по умолчанию.

В этом режиме всем доверенным приложениям разрешается доступ к сетевым ресурсам, включая интернет. К доверенным приложениям относятся: системные или имеющие сертификат Microsoft приложения, а также приложения с действительной цифровой подписью. Правила для таких приложений не отображаются в списке правил. Для других приложений Брандмауэр предоставляет вам возможность вручную запрещать или разрешать неизвестное соединение, а также создавать для него правило.

При обнаружении попытки со стороны операционной системы или пользовательского приложения получить доступ к сетевым ресурсам Брандмауэр проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вам предлагается выбрать либо временное решение, либо создать правило, по которому в дальнейшем подобные подключения будут обрабатываться.

Опция **Разрешать локальные соединения** позволяет всем приложениям беспрепятственно устанавливать локальные соединения (с интерфейса или на

интерфейс 127.0.0.1 (localhost)) на вашем компьютере. Эта опция применяется после проверки соединений на соответствие заданным правилам. Отключите эту опцию, чтобы применять правила фильтрации вне зависимости от того, происходит ли соединение по сети или в рамках вашего компьютера.

3.2.8.2. Пакетный фильтр

По умолчанию пакетный фильтр на Сервере Dr.Web отключен. При подключении станции к Серверу Dr.Web задаются настройки пакетного фильтра, установленные на Сервере Dr.Web, поэтому пакетный фильтр будет отключен, даже если на станции он был включен и настроен.

По умолчанию пакетный фильтр на Агенте Dr.Web, который поставляется с Enterprise Security Suite 13.0, отключен. При этом если Агент уже был установлен с предыдущей версией, то пакетный фильтр будет отключен при обновлении. Если нет, то Агент устанавливается с отключенным по умолчанию пакетным фильтром.

Фильтрация на уровне пакетов позволяет контролировать доступ к сети вне зависимости от программ, инициирующих подключение. Правила применяются ко всем сетевым пакетам определенного типа, которые передаются через один из сетевых интерфейсов вашего компьютера.

Чтобы задать настройки фильтрации пакетов, включите/отключите следующие опции:

Опция	Описание
Включить пакетный фильтр	Используйте эту опцию, чтобы включить и настроить фильтрацию пакетов для известных сетевых интерфейсов. Если опция отключена, настройка доступа к сетевым ресурсам будет возможна только для конкретных приложений, а настройки пакетного фильтра будут недоступны.
Включить динамическую фильтрацию пакетов	Используйте эту опцию, чтобы учитывать при фильтрации состояние TCP-соединения и пропускать только те пакеты, содержимое которых соответствует текущему состоянию. В таком случае все пакеты, передаваемые в рамках соединения, но не соответствующие спецификации протокола, блокируются. Этот механизм позволяет лучше защитить ваш компьютер от DoS-атак (отказ в обслуживании), сканирования ресурсов, внедрения данных и других злонамеренных операций. Также рекомендуется устанавливать этот флажок при использовании протоколов со сложными алгоритмами передачи данных (FTP, SIP и т. п.). Выключите эту опцию, чтобы фильтровать пакеты без учета TCP-соединений.

Опция	Описание
Обрабатывать фрагментированные IP-пакеты	Используйте эту опцию, чтобы корректно обрабатывать передачу больших объемов данных. Размер максимального пакета (MTU — Maximum Transmission Unit) для разных сетей может варьироваться, поэтому часть IP-пакетов при передаче может быть разбита на несколько фрагментов. При использовании данной опции ко всем фрагментарным пакетам применяется одно и то же действие, предусмотренное правилами фильтрации для головного (первого) пакета. Выключите эту опцию, чтобы обрабатывать все пакеты по отдельности.

Правила пакетного фильтра

Брандмауэр Dr.Web поставляется со следующими предустановленными наборами правил:

- **Default Rule** — правила, описывающие наиболее часто встречающиеся конфигурации сети и распространенные атаки (используется по умолчанию для всех новых интерфейсов);
- **Allow All** — все пакеты пропускаются;
- **Block All** — все пакеты блокируются. При этом возможна блокировка соединения Агент — Сервер Dr.Web. Перед распространением настроек рекомендуется проверить работу данного набора правил на ограниченном числе станций.

Для удобства использования и быстрого переключения между режимами фильтрации вы можете задать дополнительные наборы правил.

- чтобы использовать существующий набор правил в качестве набора правил по умолчанию, выберите его в списке и нажмите ✔;
- чтобы отредактировать существующий набор правил, выберите его в списке и нажмите ✎;
- чтобы скопировать существующий набор правил, выберите его в списке и нажмите ;
- чтобы удалить существующий набор правил, выберите его в списке и нажмите 🗑.

Чтобы создать новый набор правил

1. В окне **Наборы правил** нажмите ✚.
2. Введите название нового набора правил.
3. Нажмите **Сохранить**. Откроется форма **Создания нового правила**.
4. Задайте необходимые параметры правила.

Если параметры нового правила не будут сохранены, набор правил не будет создан.

Чтобы добавить новое правило

1. В окне **Наборы правил** выберите набор, в который вы хотите добавить новое правило.
2. В окне **Правила** нажмите ✚, чтобы создать новое правило. Откроется окно создания правила пакетной фильтрации.
3. Задайте следующие параметры правила:

Параметр	Описание
Название правила	Имя создаваемого/редактируемого правила.
Описание	Краткое описание правила.
Действие	Указывает на действие, выполняемое Брандмауэром при обработке пакета: • **Разрешать пакеты** — передать пакет; • **Блокировать пакеты** — блокировать пакет.
Направление	Направление соединения: • **Входящее** — правило применяется, если пакет принимается из сети; • **Исходящее** — правило применяется, если пакет отправляется с вашего компьютера; • **Любое** — правило применяется вне зависимости от направления соединения.
Ведение журнала	Режим регистрации событий. Указывает на то, какая информация должна быть занесена в журнал: • **Отключено** — не сохранять информацию о пакете; • **Только заголовки** — заносить в журнал только заголовки пакетов; • **Весь пакет** — заносить в журнал пакеты целиком.
Критерий	Критерий фильтрации. Например, транспортный или сетевой протокол. Чтобы добавить критерий фильтрации, выберите нужный критерий в **Списке критериев** и с помощью стрелочки перенесите его в поле слева. Вы можете добавить любое необходимое количество критериев. Для некоторых критериев доступны дополнительные параметры: • **Любой** — задает правило для всех хостов или портов. • **Равен** или **Не равен** — задает правило для конкретного адреса или порта.

Параметр	Описание
	• **В диапазоне** или **Вне диапазона** — задает правило для диапазона адресов или портов, например, `192.168.0.1-192.168.0.2`. • **Соответствует маске** или **Не соответствует маске** — задает правило для маски конкретной подсети, например, `192.168.1.0/255.255.255.0` (только для IPv4, IPv6, Ethernet). Для MAC-адресов использование масок не допускается. Создайте новое правило или добавьте адреса всех устройств через запятую (без пробела), чтобы добавить новое устройство. • **Совпадает с IP-адресом станции** или **Не совпадает с IP-адресом станции** — задает правило для IP-адреса сетевого интерфейса (только для IPv4, IPv6). • **Совпадает с MAC-адресом станции** или **Не совпадает с MAC-адресом станции** — задает правило для MAC-адреса сетевого интерфейса (только для Ethernet). Чтобы удалить критерий из списка, выберите его и нажмите  .

Если вы не добавите ни одного критерия фильтрации, то данное правило будет разрешать или блокировать все пакеты (в зависимости от настройки в поле **Действие**).

Некоторые критерии фильтрации несовместимы с другими. При добавлении/удалении критерия, в **Списке критериев** отображаются только критерии, совместимые с заданными.

4. По окончании редактирования нажмите кнопку **Сохранить** для сохранения внесенных изменений.

Чтобы действие из правила было применено к пакету, пакет должен соответствовать всем критериям правила.

Включение и отключение правила

- Чтобы включить правило, установите флажок слева от его названия.
- Чтобы отключить правило, снимите флажок слева от его названия.

Чтобы изменить порядок применения правил

1. Выберите правило, порядок которого вы хотите изменить.

2. Переместите курсор в область слева от опции включения или отключения правила.
3. Удерживая нажатой левую клавишу мыши, перетащите правило вверх или вниз списка правил.

Чтобы отредактировать правила фильтрации

1. В окне **Наборы правил** выберите набор, в котором вы хотите отредактировать правило.
2. В окне **Правила** выберите правило из списка.
3. Нажмите . Откроется окно редактирования правила пакетной фильтрации.
4. Внесите необходимые изменения в параметры правила.
5. По окончании редактирования нажмите кнопку **Сохранить** для сохранения внесенных изменений.
6. Чтобы удалить правило, выберите его в списке и нажмите .

Сетевые интерфейсы

Данная настройка доступна только при выборе станции.

В разделе **Сетевые интерфейсы** вы можете задать набор правил, который будет использоваться для фильтрации пакетов, передающихся через определенный сетевой интерфейс.

Найдите в списке интересующий вас интерфейс и сопоставьте ему соответствующий набор правил. Если подходящий набор правил отсутствует в списке, создайте его.

Набор правил, назначенный для группы станций, применяется на станциях однократно и только для тех сетевых интерфейсов, которые присутствуют на станции на момент применения правил. Последующие изменения необходимо вносить в конфигурацию конкретной станции и ее сетевых интерфейсов.

3.2.8.3. Журнал

Включите опцию **Вести подробный журнал** для сбора данных о сетевых пакетах (журналы pcap).

По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает

разрешенный размер.

При включении опции **Вести подробный журнал**, запись журнала работы соответствующего компонента осуществляется в режиме отладки с максимальной детализацией. Ограничения на размер файла в данном режиме снимаются. Это приводит к значительному увеличению размера файла журнала. Также обратите внимание, что ротация файла журнала не осуществляется (относится ко всем режимам ведения журнала).

Отладочный режим ведения журнала снижает производительность работы антивируса и операционной системы станции. Использовать этот режим следует только при возникновении проблем в работе компонентов и по запросу службы технической поддержки. Не рекомендуется включение отладочного режима ведения журнала на длительный срок.

На стороне Центра управления настройки ведения журнала задаются отдельно для каждого компонента в разделах **Журнал**. На станции настройки ведения журнала задаются в едином разделе **Дополнительно**.

3.2.9. Превентивная защита

В этом разделе:

- Поведенческий анализ
- Защита от эксплойтов
- Защита от вымогателей

3.2.9.1. Поведенческий анализ

В подразделе **Поведенческий анализ** вы можете настроить реакцию Dr.Web на обращение приложений к защищаемым сущностям и задать ограничения для конкретных групп сущностей.

3.2.9.1.1. Общие

На вкладке **Общие** вы можете настроить реакцию Dr.Web на действия сторонних приложений, которые могут привести к заражению рабочей станции.

При этом вы можете задать отдельный режим защиты для конкретных приложений и общий режим, настройки которого будут применяться ко всем остальным процессам.

Уровень защиты

В разделе **Уровень защиты** вы можете задать общий режим защиты, настройки которого будут применяться ко всем процессам, если для них не заданы исключения.

Выберите один из уровней защиты, обеспечиваемой антивирусом:

- **Параноидальный** — максимальный уровень защиты при необходимости полного контроля за доступом к критическим объектам ОС Windows.

  В данном режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

- **Средний** — уровень защиты при повышенной опасности заражения. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.
- **Оптимальный** — уровень защиты, запрещающий автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему.
- **Без ограничений** — минимальный уровень защиты, при котором процессам разрешается беспрепятственно модифицировать объекты на станции.

  Чтобы добавить новый профиль, нажмите кнопку  . В открывшемся окне задайте название для нового уровня защиты и нажмите **Добавить**.

  Для задания пользовательских настроек уровня превентивной защиты включите в таблице данного раздела опции в одно из следующих положений:

  a) **Разрешать** — всегда разрешать действия с данным объектом или со стороны данного объекта.

  b) **Спрашивать** — выводить диалоговое окно для задания необходимого действия самим пользователем для конкретного объекта.

  c) **Запрещать** — всегда запрещать действия с данным объектом или со стороны данного объекта.

  Вы можете создать несколько независимых пользовательских профилей.

  Чтобы удалить созданный вами пользовательский профиль, выберите его из списка **Уровень защиты** и нажмите кнопку  . Возможность удалять предустановленные профили не предоставляется.

Защищаемые сущности

Настройки превентивной защиты позволяют контролировать следующие сущности:

- **Целостность запущенных приложений** — отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности

компьютера. Не отслеживается поведение тех процессов, которые добавлены в исключения компонента SpIDer Guard.

- **Файл HOSTS** — данный файл используется операционной системой для упрощения интернет-доступа. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
- **Низкоуровневый доступ к диску** — запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
- **Загрузка драйверов** — запрещать приложениям загрузку новых или неизвестных драйверов.

Остальные настройки отвечают за критические области ОС Windows и позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей).

Защищаемые ветки реестра

Настройка	Ветка реестра
Параметры запуска приложений (IFEO)	Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Драйверы мультимедийных устройств	Software\Microsoft\Windows NT\CurrentVersion\Drivers32 Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Параметры оболочки Winlogon	Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Нотификаторы Winlogon	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Автозапуск оболочки Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib
Ассоциации исполняемых файлов	Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи)
Политики ограничения запуска программ (SRP)	Software\Policies\Microsoft\Windows\Safer
Плагины Internet Explorer (BHO)	Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Автозапуск программ	Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\RunOnce

Настройка	Ветка реестра
	Software\Microsoft\Windows\CurrentVersion\RunOnceEx Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup Software\Microsoft\Windows\CurrentVersion\RunServices Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
Автозапуск политик	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Конфигурация безопасного режима	SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Параметры Менеджера сессий	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
Системные службы	System\CurrentControlXXX\Services

Если при установке важных обновлений от Microsoft или при установке и работе программ (в том числе программ дефрагментации) возникают проблемы, отключите соответствующие опции в этой группе настроек.

3.2.9.1.2. Исключения

На вкладке **Исключения** вы можете задать отдельный режим защиты для конкретных приложений. Ко всем остальным процессам будут применяться настройки, заданные в разделе **Уровень защиты**.

Редактирование правил

1. Чтобы добавить еще одно правило, нажмите кнопку  .
   a) Чтобы задать настройки добавленного правила, нажмите кнопку  напротив этого правила.
   b) В открывшемся окне укажите путь к исполняемому файлу приложения на защищаемой станции. Вы можете вручную ввести полный путь к файлу или папке в поле ввода или использовать маску.

      Маска задает общую часть имени объекта, при этом:

      - символ «*» заменяет любую, возможно пустую, последовательность символов;
      - символ «?» заменяет любой, но только один символ;

- остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.

c) Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.

d) Нажмите **Сохранить**.

2. Чтобы отредактировать существующее правило, нажмите кнопку  напротив нужного правила и выполните шаги из пункта 1.a)–1.d).
3. Чтобы удалить существующее правило, нажмите кнопку  напротив нужного правила.

3.2.9.1.3. Ограничения

На вкладке **Ограничения** вы можете выбрать категории сущностей, которые следует ограничить:

- **Файл HOSTS** — обезвреживать записи в файле `HOSTS`, перенаправляющие на небезопасные адреса.
- **Системные программы** — восстанавливать значение по умолчанию для групповых политик запуска `cmd.exe` и `regedit.exe`.
- **Системные сертификаты** — обезвреживать записи групповых политик ограниченного использования программ по сертификату.
- **Бесфайловые скрипты** — блокировать запуск бесфайловых скриптов.
- **Выполнение LoLBins** — блокировать выполнение `LoLBins`.
- **Загрузка уязвимых драйверов** — блокировать приложения, загружающие уязвимые драйверы для доступа к ядру системы.
- **Блокировка дочерних процессов** — блокировать запуск дочерних процессов некоторыми приложениями (`chm`, `wordpad` и др.).
- **Блокировка дочерних процессов с повышенными правами** — блокировать загрузку посторонних модулей в системных приложениях с автоматическим повышением прав.
- **Блокировка скомпрометированных учетных записей пользователей** — блокировать учетную запись пользователя, от имени которого были совершены вредоносные действия в сессии удаленного рабочего стола.

3.2.9.2. Защита от эксплойтов

В подразделе **Защита от эксплойтов** вы можете настроить режим блокировки вредоносных объектов, которые используют уязвимости в приложениях. В соответствующем выпадающем списке выберите подходящий уровень защиты от эксплойтов.

Уровень защиты	Описание
Блокировать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически заблокирована.
Интерактивный режим	При попытке вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы, Dr.Web выведет соответствующее сообщение. Ознакомьтесь с информацией и выберите нужное действие.
Разрешать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически разрешена.

3.2.9.3. Защита от вымогателей

В подразделе **Защита от вымогателей** вы можете настроить реакцию Dr.Web на попытки приложений зашифровать пользовательские файлы. В выпадающем меню выберите действие, которое будет применяться для всех приложений:

- **Разрешать** — всем приложениям будет разрешено модифицировать файлы пользователя.
- **Блокировать** — всем приложениям будет запрещено шифровать файлы пользователя. Этот режим установлен по умолчанию.
- **Спрашивать** — при попытке приложения зашифровать файл пользователя будет показываться уведомление, где пользователь сможет запретить приложению это действие или проигнорировать его.

Исключения

Вы можете добавить приложения, которые не будут проверяться компонентом **Защита от вымогателей**. По умолчанию список пуст.

Формирование списка исключений

1. Нажмите  , чтобы добавить приложение в список.
2. Задайте путь к исполняемому файлу приложения. Вы можете вручную ввести полный путь к файлу или папке в поле ввода или использовать маску.

   Маска задает общую часть имени объекта, при этом:
   - символ «*» заменяет любую, возможно пустую, последовательность символов;
   - символ «?» заменяет любой, но только один символ;
   - остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.

3. Нажмите **Сохранить**.
4. Чтобы удалить приложение из списка исключений, нажмите  напротив элемента списка, соответствующего этому приложению.

3.2.10. Монитор сетевых портов

В этом разделе:

- Настройка работы Монитора сетевых портов
- Исключение из проверки Монитором сетевых портов

3.2.10.1. Общие

Настройки **Монитора сетевых портов** задаются только на Сервере Dr.Web и не видны пользователям станции.

Монитор сетевых портов проверяет порты, используемые транспортными протоколами TCP. Перехваченное соединение анализируется, и по содержанию трафика определяется тип протокола. В зависимости от типа протокола используются необходимые настройки. Почтовые протоколы проверяются в соответствии с настройками SpIDer Mail, а остальные — в соответствии с настройками SpIDer Gate и Офисного контроля.

- **SpIDer Mail** перехватывает обращения любых почтовых клиентов компьютера к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP (под IMAP4 имеется в виду IMAPv4rev1), обнаруживает и обезвреживает почтовые угрозы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер.
- **SpIDer Gate** проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы (при настройках по умолчанию). Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, то есть работающие с сетью интернет.
- **Офисный контроль** осуществляет ограничение доступа пользователей к сайтам в соответствии с настройками Веб-фильтра, Белого и Черного списков сайтов.

Если в **Мониторе сетевых портов** задана проверка указанного порта, а приложение, использующее данный порт, добавлено в список Приложений, исключаемых из проверки, то соответствующая программа или процесс будет исключена из проверки **SpIDer Gate** и **SpIDer Mail**.

Если в **Мониторе сетевых портов** задана проверка портов, используемых HTTP протоколами, а веб-ресурс внесен в **Белый список Офисного контроля**, то данный сайт будет исключен из проверки.

По умолчанию **Монитор сетевых портов** проверяет входящий и исходящий трафик по всем портам. Включите опцию **Проверять трафик только по указанным портам**, чтобы компонент проверял трафик только по портам, указанным в **Списке портов**.

По умолчанию в **Списке портов** указаны номера портов, которые используются почтовыми и HTTP протоколами.

- Чтобы добавить новый порт в список, нажмите  .
- Чтобы удалить порт, нажмите кнопку  напротив элемента списка, соответствующего этому порту.

3.2.10.2. Исключения

В списке **Приложения, исключаемые из проверки** вы можете задать список программ и процессов, которые исключаются из проверки SpIDer Gate и SpIDer Mail.

По умолчанию список пуст.

Формирование списка исключений

1. Нажмите  , чтобы добавить приложение в список.
2. В поле **Путь к приложению** задайте путь к исполняемому файлу приложения. Чтобы добавить программу или процесс к списку исключений, выполните одно из следующих действий:
   - чтобы указать конкретное существующее приложение, вручную задайте полный путь в соответствующем поле ввода (вы можете использовать переменные среды);
   - чтобы исключить из проверки все приложения с определенным именем, задайте это имя в поле ввода. Указывать путь к приложению при этом не требуется;
   - чтобы исключить из проверки приложения определенного вида, задайте определяющую их маску в поле ввода. Маска задает шаблон для определения приложения. При этом:
     - символ «*» заменяет любую, возможно пустую, последовательность символов;
     - символ «?» заменяет любой, но только один символ;
     - остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.
3. Укажите дополнительные настройки.

Настройка	Описание
Независимо от наличия цифровой подписи приложения	Выберите эту настройку, если приложение должно быть исключено из проверки вне зависимости от наличия у него действительной цифровой подписи.

Настройка	Описание
При наличии действительной цифровой подписи приложения	Выберите эту настройку, если приложение должно быть исключено из проверки только при наличии действительной цифровой подписи приложения. В противном случае приложение будет проверено компонентами SpIDer Mail и SpIDer Gate.
Любой трафик	Выберите эту настройку, чтобы исключить из проверки и зашифрованный, и незашифрованный трафик приложения.
Зашифрованный трафик	Выберите эту настройку, чтобы исключить из проверки только зашифрованный трафик приложения.
По всем IP-адресам и портам	Выберите эту настройку, чтобы исключить из проверки трафик, передаваемый на любые IP-адреса и порты.
По указанным IP-адресам и портам	Выберите эту настройку, чтобы указать IP-адреса или порты для исключения из проверки переданного с них трафика. Трафик, переданный с остальных IP-адресов или портов, будет проверен (если не исключен другими настройками).
Задание адресов и портов	Для тонкой настройки исключений используйте следующие рекомендации: • чтобы исключить из проверки определенный домен по определенному порту, укажите, например, `site.com:80`; • для исключения из проверки трафика по нестандартному порту (например, 1111) необходимо указать: `*:1111`; • для исключения из проверки трафика от домена по любому порту укажите: `site:*`.

4. Нажмите **Сохранить**.
5. Чтобы удалить приложение из списка исключений, нажмите ➖ напротив элемента списка, соответствующего этому приложению.
6. Чтобы отредактировать параметры исключения приложения из проверки, выберите приложение в списке и нажмите ✏.

3.2.11. Контроль приложений

Настройки **Контроля приложений** задаются только на Сервере Dr.Web и не видны пользователям станции.

Компонент Контроль приложений появляется в списке компонентов на станции только при заданных правилах. На вкладке **Контроль приложений** отображается информация

о профилях, распространяемых на станцию или группу станций, и конфигурации Контроля приложений.

Для настройки свойств определенного профиля нажмите на название этого профиля. Откроется окно свойств профиля вкладке **Администрирование**. Подробная информация о настройке профилей приведена в **Руководстве администратора**.

Чтобы отредактировать отображение данных в таблице

1. При помощи значка задайте произвольную строку для поиска по всем разделам таблицы.
2. При помощи значка вы можете настроить следующие опции:
   - Задать настройки отображения строк в таблице.
   - Выбрать столбцы, которые будут отображаться в таблице. Для включения/отключения столбца нажмите на строку с его названием.

Столбец	Обозначение
Идентификатор	Идентификатор станции пользователя.
Название профиля	Профиль, правила которого распространяются на станцию.
Режим работы	Режим работы Контроля приложений.
Функциональный анализ	Количество заданных предустановленных правил на станции.
Запрещающий режим	Количество запрещающих правил, заданных в профиле.
Разрешающие правила	Количество разрешающих правил, заданных в профиле.
Доверенные приложения	Количество списков приложений, которые разрешены для запуска на станциях.

   - Выбрать порядок следования столбцов в таблице. Для изменения порядка перетащите соответствующий столбец в списке на требуемое место.

Информацию в каждом столбце можно отсортировать по возрастанию или убыванию.

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:

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/.