



Dr.WEB®

Антивирус
для Microsoft Exchange Server

Руководство администратора

Защити созданное

© 2003-2013 «Доктор Веб». Все права защищены.

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

ТОВАРНЫЕ ЗНАКИ

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

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

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

Dr.Web для Microsoft Exchange Server

Версия 6.00.1

Руководство администратора

19.07.2013

«Доктор Веб», Центральный офис в России
125124

Россия, Москва

3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com

Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

«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

Условные обозначения и сокращения	7
Введение	9
Назначение Dr.Web для Microsoft Exchange Server	9
Проверяемые объекты	11
Лицензирование	12
Лицензионный ключевой файл	12
Получение ключевого файла	13
Обновление лицензии	15
Антивирусное сканирование для Microsoft Exchange Server	16
Поддержка VSAPI	16
Серверные роли	18
Транспортные агенты	19
Принципы работы Dr.Web для Microsoft Exchange Server	20
Этапы проверки на вирусы и спам	21
Карантин	23
Мониторинг вирусных событий	23
Установка и удаление	25
Системные требования	26
Совместимость	28
Установка Dr.Web для Microsoft Exchange Server	28
Удаление Dr.Web для Microsoft Exchange Server	31
Приступая к работе	32



Запуск Консоли Администратора	32
Запуск Веб-консоли Администратора	34
Администрирование	36
Группы и профили	36
Создание и настройка профилей	37
Приоритет профиля	40
Уведомления	41
Сканирование	46
Антиспам	50
Фильтрация	53
Сопроводительный текст	56
Управление группами клиентов	58
Создание новой группы	58
Формирование группы	60
Управление Карантином	64
Просмотр статистики	67
Управление отчетами	70
Общие настройки	75
Обновление антивирусных баз	79
Регистрация событий	80
Журнал операционной системы	80
Текстовый журнал программы установки	81
Текстовый журнал отладки	82
Диагностика	83
Проверка установки	83
Проверка модуля обновления	84



Проверка детектирования вирусов	85
Проверка детектирования спама	86
Приложения	87
Приложение А. Параметры командной строки для модуля обновления	87
Приложение Б. Настройки антивирусного сканирования Microsoft Exchange Server	90
Приложение В. Работа в режиме централизованной защиты	94
Приложение Г. Техническая поддержка	98
Предметный указатель	99



Условные обозначения и сокращения

В зависимости от контекста, **Dr.Web** может означать как название компании – «**Доктор Веб**», так и название продукта – **Dr.Web для Microsoft Exchange Server**.

В руководстве используются следующие условные обозначения:

Обозначение	Комментарий
Полужирный	Названия кнопок и других элементов пользовательского интерфейса, а так же данные, которые вам необходимо ввести именно так, как они приведены в руководстве.
Зеленый полужирный	Названия продуктов компании « Доктор Веб » и их компонентов.
<u>Зеленое подчеркивание</u>	Ссылки на разделы документа и веб-сайты.
<i>Курсив</i>	Текст, замещающий информацию, которую вам нужно ввести. В примерах ввода команд такое выделение указывает на участки команды, которые вам необходимо заменить актуальным значением. Так же могут выделяться термины.
ПРОПИСНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Символ «плюс» (+)	Указывает на одновременное нажатие нескольких клавиш. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
	Важные замечания и указания.



В руководстве используются следующие сокращения:

- ОС – операционная система;
- ПО – программное обеспечение;
- AD – Active Directory;
- CPU – Central Processing Unit (центральное процессорное устройство);
- GUI – Graphical User Interface (графический интерфейс пользователя);
- HTML – Hypertext Mark-up Language (язык гипертекстовой разметки);
- HTTP – Hypertext Transfer Protocol (протокол передачи гипертекста);
- RAM – Random Access Memory (оперативная память);
- SMTP – Simple Mail Transfer Protocol (простой протокол пересылки почты);
- SP1, SP2, etc. – Service Packs (служебные пакеты обновления для ОС Windows).



Введение

Благодарим вас за приобретение **Dr.Web для Microsoft Exchange Server**. Данный антивирусный продукт использует наиболее передовые технологии и предоставляет надежную защиту компьютеров и информации внутри корпоративной сети от угроз, распространяемых посредством электронной почты.

Настоящее руководство призвано помочь администраторам корпоративных сетей при установке и настройке **Dr.Web для Microsoft Exchange Server**. Руководство содержит информацию обо всех основных особенностях использования данного программного обеспечения, а также контактную информацию службы технической поддержки.

Назначение Dr.Web для Microsoft Exchange Server

Dr.Web для Microsoft Exchange Server – это антивирусное приложение, созданное с целью защитить корпоративную почтовую систему от вирусов и спама. Оно надежно интегрируется в систему и проверяет все письма и вложения, поступающие серверу для обработки. При этом проверяются не объекты файловой системы, а буферы памяти, что значительно ускоряет процесс сканирования.

Важной особенностью интеграции продукта является возможность проверки почтовых сообщений согласно приоритету, который устанавливается для сообщений сервером. При помещении нового почтового сообщения в хранилище информации Microsoft Exchange Server этому сообщению присваивается низкий приоритет. Сообщения, к которым происходит обращение клиентов сервера, получают более высокий приоритет и проверяются в первую очередь. Все сообщения проверяются до того, как они передаются клиенту. Изменение приоритетности сообщений обеспечивает максимальный уровень защиты и эффективное использование



ресурсов системы.

Помимо входящих и исходящих электронных сообщений **Dr.Web для Microsoft Exchange Server** также проверяет объекты, уже находящиеся в хранилищах информации Microsoft Exchange Server, что значительно повышает эффективность сканирования. Кроме того, для упрощения работы с антивирусным приложением, в нем реализован полностью автоматический запуск (при запуске системы) и удобный механизм обновлений (путем добавления задания на обновление в расписание Планировщика Задач Windows).

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

- сканирование всех входящих и исходящих сообщений в реальном времени;
- фильтрация и блокировка спама, а также создание белых и черных списков адресов;
- изоляция инфицированных и подозрительных объектов в Карантине;
- фильтрация электронных писем по различным критериям;
- добавление сопроводительного текста к исходящим с сервера сообщениям;
- распределение пользователей по группам для упрощения администрирования;
- отправка уведомлений о вирусных событиях и ведение журнала этих событий;
- рассылка отчетов о работе программы;
- сбор статистики;
- автоматическое обновление антивирусных баз и компонентов программы.



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

Проверяемые объекты

Dr.Web для Microsoft Exchange Server производит проверку входящих и исходящих сообщений в реальном времени. Проверке подвергаются следующие элементы электронных писем:

- тело письма;
- вложения (включая архивированные и упакованные файлы);
- вложенные OLE-объекты.

Dr.Web для Microsoft Exchange Server сканирует все объекты до того, как они передаются клиенту для обработки.



Лицензирование

Права пользователя на использование программы **Dr.Web для Microsoft Exchange Server** регулируются при помощи специального файла, называемого *лицензионным ключевым файлом*.

Лицензионный ключевой файл

Ключевой файл имеет расширение .key и содержит, в частности, следующую информацию:

- срок действия лицензии;
- перечень компонентов, разрешенных к использованию (например, компонент **Антивирус** доступен только в версии «Антивирус + Антиспам»);
- другие ограничения (в частности, количество пользователей, защищаемых приложением).

Ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- ключ распространяется на все используемые программой модули;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится *недействительным*, при этом программа **Dr.Web для Microsoft Exchange Server** перестает обнаруживать вредоносные программы. Факт нарушения корректности ключевого файла записывается в журнал регистрации событий операционной системы, а также в текстовый журнал регистрации событий программы.



Ключевой файл имеет формат, защищенный от редактирования. Редактирование файла делает его недействительным. Поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Получение ключевого файла

Вы можете получить лицензионный ключевой файл одним из следующих способов:

- в виде ZIP-архива по электронной почте;
- вместе с дистрибутивом продукта, если лицензионный файл был включен в состав дистрибутива при его комплектации;
- на отдельном носителе в виде файла с расширением .key.

Ключевой файл необходимо приобрести до установки **Dr.Web для Microsoft Exchange Server**, т.к. для установки потребуется указать путь к вашему ключевому файлу.

Получение ключевого файла по электронной почте

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.
2. Заполните форму со сведениями о покупателе.
3. Введите регистрационный серийный номер (находится на регистрационной карточке).
4. Ключевой файл будет выслан по указанному вами адресу электронной почты в виде ZIP-архива, содержащего файл с расширением .key.
5. Извлеките ключевой файл на компьютер, на который вы планируете установить **Dr.Web для Microsoft Exchange Server**.



Для ознакомления с программой можно получить *демонстрационный ключевой файл*. Такой ключевой файл обеспечивает полную функциональность основных антивирусных компонентов, но имеет ограниченный срок действия и не предполагает оказание технической поддержки пользователю.

Для получения демонстрационного ключевого файла (по электронной почте) следует зарегистрироваться на веб-сайте <http://download.drweb.com/demoreq/>.

Чтобы купить лицензионный ключевой файл, свяжитесь с ближайшим партнером **«Доктор Веб»** в вашем регионе либо воспользуйтесь услугами интернет-магазина на сайте компании по адресу <http://buy.drweb.com/>.

Дополнительную информацию о лицензировании и ключевых файлах можно найти на официальном сайте компании **«Доктор Веб»** по адресу <http://www.drweb.com/>.



Обновление лицензии

В некоторых случаях, например, при окончании срока действия лицензии или при изменении характеристик защищаемой системы или требований к ее безопасности, вы можете приобрести новую или расширенную лицензию на программу **Dr.Web для Microsoft Exchange Server**. В таком случае вам потребуется заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. Приложение поддерживает обновление лицензии «на лету», при котором его не требуется переустанавливать или прерывать его работу.

Замена ключевого файла

1. Чтобы обновить лицензию выполните следующие действия:
 - замените имеющийся ключевой файл в каталоге установки программы (C:\Program Files\DrWeb for Exchange) новым ключевым файлом;
 - кроме того, при использовании сервера Exchange версии 2007/2010 необходимо заменить ключевой файл на новый в каталоге модуля обновления (C:\Program Files (x86)\DrWeb for Exchange\).
2. Программа **Dr.Web для Microsoft Exchange Server** автоматически переключится на использование нового ключевого файла.

Дополнительную информацию о сроках и типах лицензирования можно найти на официальном сайте компании «**Доктор Веб**» по адресу <http://www.drweb.com/>.



Антивирусное сканирование для Microsoft Exchange Server

Антивирусное приложение **Dr.Web для Microsoft Exchange Server** поддерживает интерфейс VSAPI (программный интерфейс приложений вирусного сканирования, разработанный Microsoft для серверов Exchange).

Dr.Web для Microsoft Exchange Server проверяет на вирусы и спам все электронные сообщения (входящие, исходящие и внутренние), обрабатываемые сервером Exchange (спам проверяется при наличии лицензии «Антивирус + Антиспам» и только для писем принимаемых сервером по протоколу SMTP).

Кроме того, программа поддерживает такие концепции организации Exchange Server 2007/2010, как серверные роли и транспортные агенты, и может быть установлена на серверах с разными ролями, при этом сканирование писем на предмет наличия вирусов и спама может выполняться как на уровне транспортных агентов, так и на уровне модуля поддержки интерфейса VSAPI.

Поддержка VSAPI

Антивирусные решения для серверов Exchange, работающие на основе VSAPI, проверяют все почтовые сообщения, поступающие на сервер, до отправки клиенту. Проверка осуществляется в трех режимах:

- упреждающем (proactive);
- по запросу (on-demand);
- фоновом (background).



Упреждающее сканирование

Все электронные сообщения, поступающие на сервер Exchange, помещаются в общую очередь на проверку антивирусным приложением. Сообщениям в очереди присваивается одинаковый низкий приоритет. Если приоритет сообщений не меняется, то проверка осуществляется по принципу «first in, first out» (FIFO), то есть в порядке поступления сообщений.

Сканирование по запросу

Если приоритет какого-либо сообщения повышается, что происходит при его запросе почтовым клиентом, то проверка этого сообщения будет выполнена досрочно, поскольку очередь на проверку обслуживается несколькими потоками. Изначально низкий приоритет вновь поступающих сообщений гарантирует, что их проверка не будет мешать проверке сообщений с высоким приоритетом.

Процессы упреждающего сканирования и сканирования по запросу обеспечивают проверку всех писем, проходящих через сервер. При этом система приоритетов позволяет оптимизировать нагрузку на сервер и время ожидания сообщения клиентом.

Фоновое сканирование

В режиме фонового сканирования производится проверка сообщений, уже находящихся в хранилище, что позволяет обнаруживать вирусы, попавшие в хранилище до установки **Dr. Web для Microsoft Exchange Server**, а также ранее неизвестные вирусы в сообщениях, проверенных до последнего обновления антивирусных баз. Данный режим сканирования запускается администратором Exchange с помощью набора ключей реестра.

Более подробную информацию о настройках антивирусного сканирования на основе VSAPI см. в [Приложении Б](#).



Серверные роли

Exchange Server 2007/2010 может быть установлен в нескольких конфигурациях, определяющих режимы работы сервера и поддерживаемую им функциональность. Для этого при развертывании задаются роли сервера в организации Exchange.

Exchange Server 2007/2010 дает возможность создания 5 ролей сервера – почтовый ящик Mailbox, клиентский доступ Client Access, транспортный концентратор Hub Transport, унифицированная работа с сообщениями Unified Messaging и граничный транспорт Edge Transport. Три из них поддерживают проверку на вирусы и спам – это граничный транспорт, транспортный концентратор и почтовый ящик.

1. **Почтовый ящик (Mailbox)** – реализует основные службы, в частности, для хранения данных и поддержки клиентских папок и позволяет проверять сообщения на вирусы через интерфейс VSAPI;
2. **Транспортный концентратор (Hub Transport)** – распределяет сообщения внутри организации, позволяет применять для сообщений политики безопасности, осуществлять антивирусную проверку и фильтрацию спама;
3. **Граничный транспорт (Edge Transport)** – данная роль присваивается автономному серверу, находящемуся в демилитаризованной зоне и не использующему внутренние ресурсы организации (за исключением односторонней синхронизацией с Active Directory для регистрации топологии серверов транспортных концентраторов), что позволяет данному серверу выступать в качестве SMTP-шлюза и осуществлять фильтрацию спама и вирусов.

Dr.Web для Microsoft Exchange Server может быть установлен на сервер, для которого задана любая из этих ролей и их комбинации.



Антивирусная защита для разных ролей сервера

Граничный транспорт (Edge Transport) выполняет функции первой линии защиты, поэтому наиболее важной представляется обеспечение защиты именно на данном уровне организации Exchange. При установке **Dr.Web для Microsoft Exchange Server** на сервер граничного транспорта антивирусная проверка осуществляется на транспортном уровне, для чего необходимо зарегистрировать только транспортные агенты программы.

Для повышения эффективности защиты организации и создания дополнительной линии защиты приложение **Dr.Web для Microsoft Exchange Server** может быть установлено на транспортный концентратор (Hub Transport), при этом проверка на вирусы и спам будет также осуществляться на уровне транспорта.

Почтовый ящик (Mailbox) осуществляет непосредственную работу с хранилищами информации (Exchange Information Stores), антивирусная проверка на данном сервере реализуется только через поддержку интерфейса VSAPI, поэтому установка программы **Dr.Web для Microsoft Exchange Server** на данный сервер позволит дополнительно защитить объекты, не передаваемые через транспорт, в частности, содержимое общих папок, отправленные сообщения и элементы календаря, которые не защищены проверкой на вирусы на транспортном уровне.

Транспортные агенты

Концепция организации Microsoft Exchange 2007/2010 использует измененную структуру SMTP-событий. Поток сообщений на разных этапах SMTP-транспортировки обрабатывается транспортными агентами разной функциональности.

При поступлении сообщения на сервер, оно перенаправляется через транспортную сеть SMTP, при этом на каждое SMTP-событие может быть зарегистрировано несколько транспортных агентов, которые получают доступ к сообщению и могут производить над ним определенные действия. Каждый агент выполняет свою проверку, после чего сообщение передается следующему агенту.



Таким образом, транспортные агенты позволяют реагировать на события, связанные с получением письма и его дальнейшим передвижением по сети.

Существует два различных типа транспортных агентов:

- **SMTP Receive Agent** – позволяет реагировать на события, возникающие при получении письма по SMTP;
- **Routing Agent** – позволяет реагировать на события, возникающие при роутинге письма.

Exchange Server 2007/2010 позволяет задавать приоритет агентам транспорта и тем самым управлять очередностью применения агентов к сообщениям. Таким образом, порядок следования агентов определяется не только последовательностью событий, к которым они относятся, но и заданным приоритетом в рамках одного SMTP-события.

Транспортные агенты позволяют использовать специальное программное обеспечение для обработки электронной почты, в частности, для проверки сообщений на вирусы и спам.

Принципы работы Dr.Web для Microsoft Exchange Server

Все антивирусные решения **Dr.Web** содержат следующие основные компоненты, обеспечивающие защиту всех операционных систем и платформ: антивирусное ядро **drweb32.dll** и файлы антивирусных баз (с расширением **.vdb**), в которых хранятся и регулярно обновляются вирусные записи, содержащие различную информацию о вирусах и иных вредоносных кодах.

Антивирусное и антиспам-решение **Dr.Web для Microsoft Exchange Server** интегрирует технологии **Dr.Web** в процесс обработки и хранения почты на серверах Exchange.



Продукт имеет удобный графический интерфейс пользователя для управления настройками сканирования и отслеживания результатов проверки сообщений на сервере. Подробное описание настроек см. в главе [Администрирование](#).

Этапы проверки на вирусы и спам

После получения уведомления о приходе сообщения на сервер поступившее сообщение проходит через следующие этапы проверки:

- 1. Проверка на спам** (выполняется только в случае лицензии «Антивирус + Антиспам» и только для писем принимаемых сервером по протоколу SMTP, настраивается в разделе [Антиспам](#)).

В первую очередь анализируются адреса получателей и отправителей на принадлежность черным и белым спискам, которые задаются в разделе [Настройки](#). Затем антиспам-фильтр Vade Retro проверяет текст сообщения и выдает заключение, на основе которого определяется степень вероятности того, что данное сообщение является спамом. Если письмо является спамом, то об этом оповещается администратор или другие заинтересованные лица, прописанные в соответствующих настройках раздела [Уведомления](#), и к письму применяется действие, установленное администратором для данной категории спама в разделе [Антиспам](#).

- 2. Применение правил фильтрации** (настраиваются в разделе [Фильтрация](#)).

А. Правила антидистрибуции (ограничение списков рассылки). Можно задать правила, задающие максимальное число адресов получателей сообщения (или сообщения с вложениями) и применяющиеся к адресатам-отправителям. Для этих отправителей допускается отправка только тех сообщений, в которых число адресов получателей не превышает указанного максимального значения.



- Б. Правила фильтрации вложенных файлов. Можно задать правила удаления вложенных файлов: по расширению, по маске имени файла, по максимальному размеру файла.

При условии выполнения одного из заданных правил сообщение (или вложение) удаляется, и об этом оповещается администратор или другие заинтересованные лица (при наличии соответствующих настроек в разделе [Уведомления](#)). В случае удаления вложенного файла к письму прикрепляется текстовый файл с сообщением об удалении приложения. Шаблон сообщения об удалении вложения и имя файла такого сообщения задаются также в разделе [Фильтрация](#).

3. Проверка на вирусы (настраивается в разделе [Сканирование](#)).

Сообщения, успешно прошедшие предыдущие этапы проверки (или пропущенные в соответствии с настройками приложения **Dr.Web**), передаются далее для проверки на наличие вредоносного кода. Если объект (вложение или тело письма) содержит вредоносный код, антивирус предпринимает попытку вылечить объект. Если в настройках включено использование эвристического анализатора, становится возможным определение объектов, содержащих модифицированный или неизвестный вредоносный код, таким объектам присваивается категория **Подозрительные**.

По результатам сканирования объектам присваиваются определенные статусы (например, **Невылеченные**, **Подозрительные**, **Поврежденные**, **Вывлеченные**), и на основе такого заключения выполняются дальнейшие действия над этими объектами. К письмам с зараженными объектами прикрепляется текстовый файл с сообщением об обнаруженной инфекции и выполненными над этими объектами действиями программы.



Вылеченные и незараженные объекты передаются серверу с соответствующей пометкой. Невылеченные, поврежденные и подозрительные объекты проходят обработку в соответствии с настройками, указанными в разделе [Сканирование](#).

Администратор может получать оповещения о всех типах вирусных событий при наличии соответствующих настроек в разделе [Уведомления](#).

Карантин

Для невылеченных, поврежденных и подозрительных объектов можно установить действие **Поместить в карантин**. Объекты указанного типа помещаются в служебную базу, выполняющую функции карантина, т.е. блокирующую возможность выполнения кода этих объектов любыми приложениями в системе. Получить информацию об объектах, находящихся в карантине, можно в разделе [Карантин](#).

Мониторинг вирусных событий

Для предоставления администратору, а также другим заинтересованным пользователям структурированной информации о событиях, отслеживаемых **Dr.Web для Microsoft Exchange Server**, администратору необходимо настроить систему оповещения о событиях, которая включает в себя следующие возможности:

- [Уведомления по почте](#). Возможна отправка уведомлений по почте администратору, а также отправителям и получателям писем с вылеченными, невылеченными, отфильтрованными, поврежденными объектами или спамом (устанавливается на выбор);



- **Журнал событий.** Возможно занесение в журнал событий записей о приходе на сервер писем с объектами, которые были вылечены, не вылечены, отфильтрованы или определены как поврежденные или спам (устанавливается на выбор). Просмотр этих событий осуществляется с помощью стандартной утилиты Windows **Просмотр Событий** -> **Приложение (Event Viewer -> Application)**;
- **Отчеты.** Возможна отправка по электронной почте отчетов об установленных типах событий определенному списку адресатов;
- **Статистика.** Предоставляется возможность ознакомиться с информацией о количестве проверенных объектов с момента установки **Dr.Web для Microsoft Exchange Server**, либо с момента очистки данных статистики. Кроме того, в данном разделе также возможен просмотр списка писем, обработанных **Dr.Web для Microsoft Exchange Server**, в которых обнаружены вирусы или спам, а также отфильтрованных писем (вкладка/раздел **События**).



Установка и удаление

Продукт **Dr.Web для Microsoft Exchange Server** поставляется в виде папки, помещенной в ZIP-архив и содержащей установочные файлы **drweb-exchange-20002003-ru.msi** и **drweb-exchange-20072010-ru.msi** для разных версий сервера Exchange.

Извлеките файл установки на локальный диск сервера Exchange.



Для установки и удаления **Dr.Web для Microsoft Exchange Server** пользователь должен обладать правами локального администратора на том компьютере, где установлен Microsoft Exchange Server, а также входить в группу Domain Users.

Если вы пользуетесь компонентом Windows Terminal Services, то для установки **Dr.Web для Microsoft Exchange Server** рекомендуется воспользоваться стандартной утилитой Windows **Установка и удаление программ**.

При большой нагрузке на сервер, в случае повторной установки программы рекомендуется сначала остановить следующие службы:

- Microsoft Exchange Information Store;
- Inetinfo;
- Dr.Web Core Services for MSP;
- Dr.Web Core Services for MSP Attendant.

По завершении повторной установки необходимо перезапустить ручную службу Microsoft Exchange Information Store, запуск остальных служб будет произведен автоматически.



Системные требования

В данном разделе представлены системные требования, необходимые для правильной установки и работы **Dr.Web для Microsoft Exchange Server**.

Аппаратные требования

Характеристика	Требование	
	при использовании Microsoft Exchange Server 2000/2003	при использовании Microsoft Exchange Server 2007/2010
CPU	Процессор Pentium 133 МГц (рекомендуется 733 МГц)	Один из следующих процессоров: • Intel с архитектурой x64 и поддержкой технологии Intel 64; • AMD с поддержкой платформы AMD64.
RAM	256 Мбайт (рекомендуется 512 Мбайт)	2 Гбайт
Свободное пространство на диске	280 Мбайт	265 Мбайт
Монитор	VGA-совместимый монитор	



Требования к ОС и программному обеспечению

Характеристика	Требование	
	при использовании Microsoft Exchange Server 2000/2003	при использовании Microsoft Exchange Server 2007/2010
ОС	Одна из следующих: • Microsoft® Windows® 2000 Server или Advanced Server с установленным SP4; • Microsoft® Windows Server® 2003 (версия Standard, Enterprise или Datacenter) с установленным SP1 или выше.	Одна из следующих: • Microsoft® Windows Server® 2003 R2 x64 с установленным SP2; • Microsoft® Windows Server® 2008 x64; • Microsoft® Windows Server® 2008 R2.
Файловая система	NTFS или FAT32	NTFS
Exchange Server	Microsoft® Exchange Server 2000/2003 (версия Standard или Enterprise)	Microsoft® Exchange Server 2007 x64 с установленным SP1 или Microsoft® Exchange Server 2010 x64
Прочее ПО	Microsoft® Windows Installer 3.1 или выше	
	Microsoft .NET Framework 3.5 (для корректной работы Веб-консоли Администратора)	



При использовании Microsoft Exchange версии 2000/2003 для установки **Dr.Web для Microsoft Exchange Server** под Windows 2000 необходим Internet Explorer 6.



Совместимость

Перед установкой **Dr.Web для Microsoft Exchange Server** необходимо обратить внимание на следующую информацию о совместимости программы:

1. Программа **Dr.Web для Microsoft Exchange Server** версии 6.00.1 совместима только с продуктами **Dr.Web** версии 6.
2. **Dr.Web для Microsoft Exchange Server** не совместим с другими антивирусными программами. Установка нескольких антивирусных продуктов на один компьютер может привести к системным ошибкам и потере важных данных. Если на компьютере уже установлена какая-либо версия **Dr.Web для Microsoft Exchange Server** или другой антивирус, то его необходимо удалить, используя установочный файл или стандартные средства операционной системы (см. [Удаление Dr.Web для Microsoft Exchange Server](#)).

Установка Dr.Web для Microsoft Exchange Server

Перед установкой настоятельно рекомендуется:

- установить все критические обновления, выпущенные компанией Microsoft, для ОС, которая используется на компьютере (они доступны на сайте обновлений по адресу <http://windowsupdate.microsoft.com>);
- проверить файловую систему при помощи стандартных средств и исправить обнаруженные ошибки;
- завершить работу всех приложений.



Если вы устанавливаете **Dr.Web для Microsoft Exchange Server** версии 6.00.1 и хотите сохранить настройки профилей предыдущей версии приложения, выполните экспорт настроек приложения в конфигурационный файл перед ее удалением. В дальнейшем вы сможете загрузить настройки из этого файла и использовать их в новой версии приложения. Для сохранения настроек щелкните правой кнопкой по значку с именем сервера в дереве [консоли](#) или [веб-консоли](#) и выберите соответствующий пункт меню.

Чтобы установить Dr.Web для Microsoft Exchange Server:

1. Запустите установочный файл программы **drweb-exchange-20002003-ru.msi** или **drweb-exchange-20072010-ru.msi** в зависимости от используемой версии сервера Exchange. Откроется окно **Мастера установки**. Нажмите **Далее**.
2. Откроется окно с текстом Лицензионного соглашения. Для продолжения необходимо прочитать и принять соглашение, выбрав пункт **Я принимаю условия лицензионного соглашения**. Нажмите **Далее**.
3. Укажите тип установки, выбрав **Полная** или **Выборочная**. Нажмите **Далее** для продолжения.
4. Если вы выбрали выборочную установку, то откроется окно выбора компонентов, которые вы желаете установить. Внесите необходимые изменения и нажмите **Далее**.
5. В зависимости от наличия в системе компонента **Dr.Web Agent** возможны следующие варианты установки:
 - если **Dr.Web Agent** отсутствует, приложение будет работать в автономном режиме. В данном случае откроется окно **Лицензионный ключевой файл**, в котором необходимо указать путь к действующему ключевому файлу.



Если у вас нет действующего ключевого файла, то нажмите кнопку **Получить ключевой файл**, чтобы перейти на страницу запроса ключевого файла на сайте «Доктор Веб» по адресу <http://www.drweb.com>.

- если в системе установлен **Dr.Web Agent**, установка программы будет продолжена в режиме централизованной защиты, не требующем указания отдельного ключевого файла для программы **Dr.Web для Microsoft Exchange Server**. Лицензионный ключ, зарегистрированный для данной локальной станции в антивирусной сети, будет получен агентом **Dr.Web Agent** с сервера **Центра Управления Dr.Web**. Подробнее о работе в режиме централизованной защиты см. в [Приложении В](#).

Нажмите **Далее**.

6. В соответствующих полях ввода укажите основное имя пользователя (UPN) и пароль учетной записи пользователя, с почтового ящика которой будут рассылаться уведомления. При этом, указанный пользователь должен иметь почтовый ящик на сервере Exchange. Нажмите **Далее**.



Указанная учетная запись должна обладать правами локального системного администратора.

7. Введите адрес администратора сервера, на который будут высылаться уведомления, и нажмите кнопку **Далее**.
8. Если **Dr.Web для Microsoft Exchange Server** устанавливается повторно и была найдена база данных от предыдущей установки, вы можете удалить ее, установив соответствующий флажок. Кроме того, если используется Microsoft Exchange 2000/2003, вы можете также включить транспортное сканирование.



9. Нажмите кнопку **Установить**, чтобы начать установку **Dr. Web для Microsoft Exchange Server** на компьютер. По умолчанию файлы программы помещаются в папку C:\Program Files\DrWeb for Exchange.
10. Последующие действия **Мастера установки** не требуют вмешательства пользователя. По завершении установки нажмите кнопку **Готово**.

Удаление Dr.Web для Microsoft Exchange Server

Чтобы удалить Dr.Web для Microsoft Exchange Server:

1. Запустите установочный файл программы **drweb-exchange-20002003-ru.msi** или **drweb-exchange-20072010-ru.msi** в зависимости от используемой версии сервера Exchange. Откроется окно **Мастера установки**. Нажмите **Далее**.



Вы также можете воспользоваться стандартной утилитой Windows **Установка и удаление программ**, доступной через Панель управления.

2. Выберите пункт **Удалить** и нажмите **Далее**.
3. В открывшемся окне нажмите кнопку **Удалить**.
4. По окончании удаления нажмите кнопку **Заккрыть**.



Приступая к работе

В данной главе описано, как запустить [Консоль Администратора](#) и [Веб-консоль Администратора](#) для управления и настройки программы.

Запуск Консоли Администратора

Настройка работы программы **Dr.Web для Microsoft Exchange Server** может осуществляться посредством **Консоли Администратора** (см. [рис. 1](#)).

Для запуска Консоли Администратора воспользуйтесь одним из следующих способов:

- зайдите в меню **Пуск -> Программы -> Doctor Web -> DrWeb for Microsoft Exchange** и выберите **Консоль управления Dr.Web для Exchange**;
- щелкните дважды на файле запуска консоли (файл **drwexch.msc**), который по умолчанию находится в папке C:\Program Files\DrWeb for Exchange.



Кроме того, **Консоль Администратора** можно запустить дважды щелкнув по исполняемому файлу консоли (**drwexch.msc**), расположенному по умолчанию в папке C:\Program Files\DrWeb for Exchange.

По умолчанию **Консоль Администратора** открывается на том разделе, на котором в предыдущий раз работа программы была завершена.

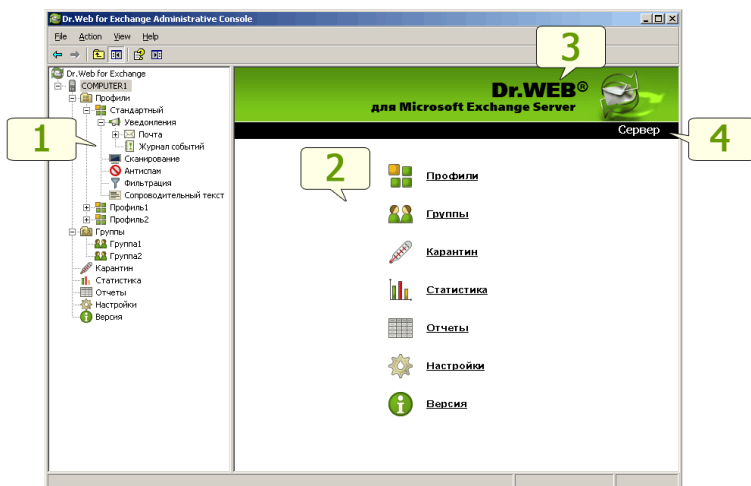


Рисунок 1. Консоль Администратора

Консоль состоит из двух частей:

1. Дерево консоли, используемое для навигации по различным разделам настроек программы.
2. Область сведений, в которой отображаются настройки выбранного в данный момент раздела и в которой их можно изменять.

В верхней части области сведений указано название и логотип **Dr.Web для Microsoft Exchange Server** (3), а также название текущего раздела (4).



Вы можете сохранить текущие настройки **Dr.Web для Microsoft Exchange Server** в конфигурационный файл и загрузить их из этого файла в случае переустановки программы или для использования на другом компьютере. Для этого щелкните правой кнопкой мыши по значку с именем сервера в дереве консоли (на иллюстрации сервер называется **COMPUTER1**) и выберите соответствующий пункт меню.



Запуск Веб-консоли Администратора

Работа приложения **Dr.Web для Microsoft Exchange Server** может быть настроена с помощью **Веб-консоли Администратора** (см. [рис. 2](#)).



Для корректной работы **Веб-консоли Администратора** необходимо использовать следующие браузеры:

- Internet Explorer 8 или выше;
- Mozilla Firefox 3.5 или выше.

Для запуска **Веб-консоли Администратора** выполните одно из следующих действий:

- если программа **Dr.Web для Microsoft Exchange Server** работает в режиме централизованной защиты, **Веб-консоль Администратора** может быть запущена из **Центра Управления Dr.Web**;
- если работа с программой осуществляется в автономном режиме, при использовании Microsoft Exchange Server 2000/2003, откройте в браузере следующую страницу:

`http: // <Exchange Server address>/ DrWebAccess/`

или

`http: // <Exchange Server address>/ DrWebAccess/ DrWebForExchange.aspx,`

где *<Exchange Server address>* – это IP-адрес сервера Exchange.

- если работа с программой осуществляется в автономном режиме, при использовании Microsoft Exchange Server 2007/2010, откройте в браузере следующую страницу:

`https: // <Exchange Server address>/ DrWebAccess/`

или



`https://<Exchange Server address>/DrWebAccess/DrWebForExchange.aspx,`

где *<Exchange Server address>* – это IP-адрес сервера Exchange.



Для доступа к странице веб-консоли необходимо ввести данные учетной записи администратора.

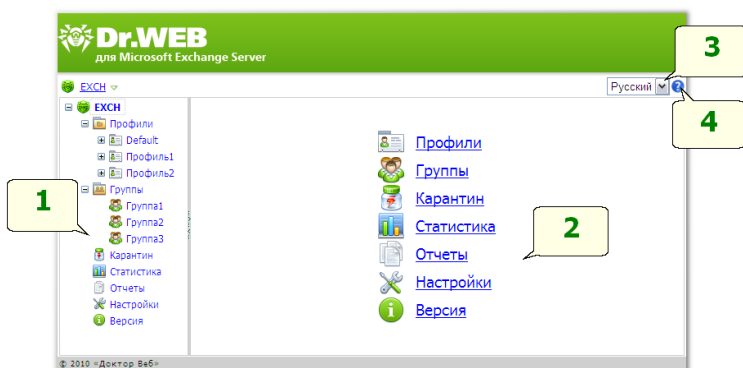


Рисунок 2. Веб-консоль Администратора

Веб-консоль состоит из двух частей:

1. Дерево веб-консоли.
2. Область сведений.

В верхней части области сведений находится опция смены языка **Веб-консоли Администратора** (3). Вы можете выбрать русский или английский язык.

Кроме того, справа от опции выбора языка находится опция вызова справки по веб-консоли (4).



Администрирование

В данной главе описана структура **Dr.Web для Microsoft Exchange Server** и выполнение административных задач, необходимых для создания максимально безопасной среды Exchange.

Группы и профили

Для упрощения организации антивирусной защиты среды Exchange в **Dr.Web для Microsoft Exchange Server** реализована возможность создания групп клиентов и присвоения им определенных профилей. Профиль представляет собой набор настраиваемых параметров обработки сообщений, от которых зависит то, как именно будет осуществляться защита среды Exchange. Настройки профиля находятся в разделе дерева консоли/веб-консоли **Профили**, который разделен на следующие подразделы:

- **Уведомления** – в данном разделе вы можете настроить работу уведомлений, которые используются для сообщения администратору и другим пользователям о различных событиях (например, об обнаружении зараженных или подозрительных объектов, о попытках лечения, о фильтрации сообщений и т.д.);
- **Сканирование** – в данном разделе вы можете настроить работу вашего основного компонента обнаружения вирусов;
- **Антиспам** – в данном разделе вы можете настроить работу **Антиспама** (настройки в данном разделе доступны только при наличии версии «Антивирус + Антиспам», т.е. в том случае, если у вас есть соответствующий ключевой файл (см. **Лицензионный ключевой файл**);
- **Фильтрация** – в данном разделе вы можете создать правила для фильтрации электронных писем;



- [Сопроводительный текст](#) – в данном разделе вы можете настроить добавление сопроводительного текста во все исходящие с сервера электронные сообщения.

Более подробно о работе с профилями читайте в разделе [Создание и настройка профилей](#).

Любой профиль можно назначить группе клиентов. Эти группы формируются в разделе дерева консоли **Группы** (см. [Управление группами клиентов](#)).

Создание и настройка профилей

В процессе установки **Dr.Web для Microsoft Exchange Server** автоматически создает **Стандартный** профиль, который нельзя ни удалить, ни переименовать. Этот профиль будет применяться ко всем письмам, пока вы не создадите другой профиль и не назначите его определенной группе клиентов. При создании нового профиля его параметры принимают текущие значения настроек **Стандартного** профиля.

Для управления существующими профилями и создания новых перейдите к области сведений раздела **Профили**, выбрав пункт **Профили** в дереве **Консоли Администратора** или **Веб-консоли Администратора** (см. [рис. 3, 4](#)).



**Рисунки 3 и 4. Раздел Профили**

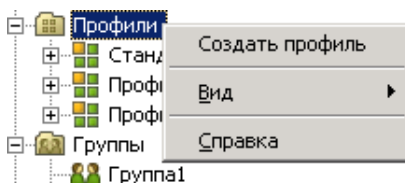
Для каждого профиля в списке содержится также информация о его настройках и приоритете.

Чтобы создать новый профиль:

- нажмите кнопку **Создать** (при использовании веб-консоли обозначена изображением ) , расположенную над списком существующих профилей.



Либо, если вы используете **Консоль Администратора** для настройки работы программы, для создания нового профиля щелкните правой кнопкой на пункте **Профили** в дереве консоли и выберите **Создать профиль** в появившемся контекстном меню (см. иллюстрацию ниже).



Будет создан новый профиль с именем **Профиль1**, который появится в дереве консоли под пунктом **Профили**. Если профиль с таким именем уже существует, то имя нового профиля будет **Профиль2** и т.д.



Чтобы изменить имя профиля:

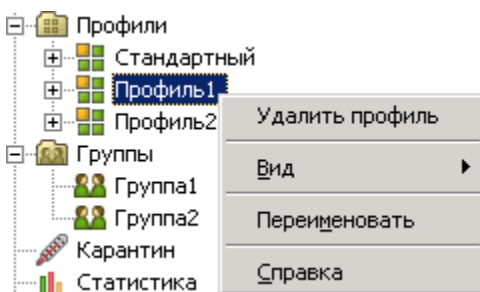
- при использовании **Консоли Администратора** выберите нужный профиль в списке, расположенном в области сведений раздела **Профили**, и нажмите кнопку **Переименовать**;
- при использовании **Веб-консоли Администратора**, укажите новое имя профиля в соответствующем текстовом поле и нажмите кнопку **Переименовать**, которая появится справа от него.

Чтобы удалить профиль:

- выберите его в списке, расположенном в области сведений раздела **Профили**, и нажмите кнопку **Удалить** (при использовании веб-консоли обозначена изображением ).



Либо, если вы используете **Консоль Администратора** для настройки работы программы, чтобы удалить или переименовать профиль, щелкните правой кнопкой на имени этого профиля в дереве консоли и выберите соответствующий пункт в появившемся контекстном меню (см. иллюстрацию ниже).



По умолчанию настройки созданного профиля будут такими же, как настройки **Стандартного** профиля.



Чтобы изменить настройки профиля:

- выберите имя профиля в дереве консоли и перейдите к желаемому разделу: [Уведомления](#), [Сканирование](#), [Антиспам](#), [Фильтрация](#) или [Сопроводительный текст](#).

Приоритет профиля

У каждого профиля есть определенный уровень приоритета, назначаемый администратором. В случае если клиент состоит в нескольких группах, которым назначены разные профили, при обработке сообщений, получаемых или отправляемых этим клиентом, будет использован профиль с наибольшим уровнем приоритета.

Приоритет профиля изменяется в области сведений раздела **Профили** перемещением существующих профилей вверх или вниз по списку:

- при использовании **Консоли Администратора**, для перемещения существующих профилей используйте кнопки ↑ и ↓ справа от списка;
- при использовании **Веб-консоли Администратора**, для перемещения профиля нажмите кнопку слева от текстового поля с его именем и перетащите профиль на желаемую позицию.

Чем выше профиль расположен в списке, тем выше уровень его приоритета;



Стандартный профиль всегда обладает самым низким уровнем приоритета, и его нельзя переместить выше нижней строчки в списке профилей.



Уведомления

Уведомления используются для информирования администратора и пользователей сети о различных событиях, связанных с работой **Dr.Web для Microsoft Exchange Server** (например, связанных с обнаружением зараженных или подозрительных объектов, попытками вылечить их, фильтрацией сообщений и т.д.). Программа поддерживает два типа уведомлений: почтовые уведомления и ведение журнала событий.



По умолчанию ведение журнала включено для всех событий, а почтовые уведомления для администратора отсылаются обо всех событиях, кроме получения спама.

Чтобы настроить уведомления по почте:

1. Нажмите **Почта** в области сведений раздела **Уведомления** или выберите подпункт **Почта** в пункте **Уведомления** дерева консоли/веб-консоли.
2. В открывшейся области сведений раздела **Почта** нажмите кнопку с названием того типа объектов, для которых вы желаете настроить уведомления (**Вывлеченные**, **Невылеченные**, **Спам**, **Отфильтрованные**, **Подозрительные** или **Поврежденные**).
3. Откроется область сведений с настройками параметров почтовых уведомлений для выбранного типа объектов (см. [рис. 5, 6](#)).



Dr.WEB®
для Microsoft Exchange Server

Администраторы Отправителю Получателю Вылеченные письма

☒ Посылать администратору уведомления по почте

Настройте параметры уведомлений для администратора

Тема уведомления: Dr.Web для Exchange обнаружил вирус!

Текст уведомления: Dr.Web для Exchange обнаружил, что %ObjectType% заражен вирусом. %ObjectType% %State%. %NewLine%/Имя файла: %FileName% %NewLine%/Вирусы: %Viruses% %NewLine%/T

Кому: Administrator@EXCHSRV-WORK.com

Сохранить

Администратор

☒ Посылать администратору уведомления по почте

Настройте параметры уведомлений для администратора

Тема: Dr.Web для Exchange обнаружил вирус!

Макрос: ObjectType Вставить

Текст: Dr.Web для Exchange обнаружил, что %ObjectType% заражен вирусом. %ObjectType% %State%. %NewLine%/Имя файла: %FileName% %NewLine%/Вирусы: %NewLine%/Тема письма: %MessageSubject% %NewLine%/От: %MessageSender% %NewLine%/Кому: %MessageRecipients% %NewLine%/Получатели копии: %MessageCCRecipients%

Кому: administrator@exchsrv-work.com

Сохранить

Отправитель

Получатель

Рисунки 5 и 6. Раздел настройки почтовых уведомлений

С помощью расположенных в области сведений вкладок/разделов вы можете настроить уведомления для администратора, отправителя и получателя.



4. С помощью опции **Посылать ... уведомления по почте** вы можете включить/выключить отправку уведомлений выбранному адресату для выбранного типа объектов. Кроме того, вы можете настроить следующие параметры уведомлений:
 - тему для шаблона уведомлений;
 - шаблон текста уведомлений. При редактировании текста вы можете использовать макросы (например, %FileName% добавляет имя файла в текст);
 - электронные адреса получателей данного типа уведомлений.
5. Нажмите кнопку **Сохранить**, когда закончите изменять настройки почтовых уведомлений.



Чтобы настроить ведение журнала событий:

1. Нажмите **Журнал событий** в области сведений раздела **Уведомления** или выберите подпункт **Журнал событий** в пункте **Уведомления** дерева консоли/веб-консоли. Откроется область сведений для настройки параметров ведения журнала (см. [рис. 7, 8](#)).

Dr.WEB®
для Microsoft Exchange Server

Журнал событий

Вылеченные

☐ Включить
Текст сообщения: Инфицированный вирусом файл %FileName% был %State% Dr. Web для Exchange%NewLine%%Viruses%%NewLine%Тема письма: %MessageSubject%%NewLine%От: %MessageSender%%NewLine%Кому: %MessageRecipients%%NewLine%Получатели копии: %MessageCCRecipients%

Невылеченные

☒ Включить
Текст сообщения: Инфицированный вирусом файл %FileName% был %State% Dr. Web для Exchange%NewLine%%Viruses%%NewLine%Тема письма: %MessageSubject%%NewLine%От: %MessageSender%%NewLine%Кому: %MessageRecipients%%NewLine%Получатели копии: %MessageCCRecipients%

Спам

☐ Включить
Текст сообщения: Dr. Web для Exchange обнаружили спам: %NewLine%Тема письма: %MessageSubject%%NewLine%От: %MessageSender%%NewLine%Кому: %MessageRecipients%%NewLine%Получатели копии: %MessageCCRecipients%

Отфильтрованные

☒ Включить
Текст сообщения: Dr. Web для Exchange отфильтровал %ObjectType%, %ObjectType% удален. %NewLine%Имя файла: %FileName%%NewLine%Подробности фильтрации: %FilteringDetails%%NewLine%Тема письма: %MessageSubject%%NewLine%От: %MessageSender%%NewLine%Кому: %MessageRecipients%%NewLine%Получатели копии: %MessageCCRecipients%

Подозрительные

☒ Включить
Текст сообщения: Dr. Web для Exchange обнаружили, что %ObjectType% является подозрительным. %ObjectType% %State%. %NewLine%Имя файла: %FileName%%NewLine%%Viruses%%NewLine%Тема письма: %MessageSubject%%NewLine%От: %MessageSender%%NewLine%Кому: %MessageRecipients%%NewLine%Получатели копии: %MessageCCRecipients%

Поврежденные

☒ Включить
Текст сообщения: Поврежденный файл %FileName% был %State% Dr. Web для Exchange%NewLine%%NewLine%Тема письма: %MessageSubject%%NewLine%От: %MessageSender%%NewLine%Кому: %MessageRecipients%%NewLine%Получатели копии: %MessageCCRecipients%

Сохранить



Выявленные

Макрос: ObjectType Вставить

☐ Включить

Текст сообщения: Инфицированный вирусом файл %FileName% был %State%
Dr.Web для Exchange%NewLine%%Viruses%%NewLine%Тема
письма: %MessageSubject%%NewLine%От: %MessageSender%%
NewLine%Кому: %MessageRecipients%%NewLine%Получатели
копии: %MessageCCRecipients%

Невыявленные

Макрос: ObjectType Вставить

☒ Включить

Текст сообщения: Инфицированный вирусом файл %FileName% был %State%
Dr.Web для Exchange%NewLine%%Viruses%%NewLine%Тема
письма: %MessageSubject%%NewLine%От: %MessageSender%%
NewLine%Кому: %MessageRecipients%%NewLine%Получатели
копии: %MessageCCRecipients%

Спам

Макрос: MessageSubject Вставить

☐ Включить

Текст сообщения: Dr.Web для Exchange обнаружил спам.%NewLine%Тема
письма: %MessageSubject%%NewLine%От: %MessageSender%%
NewLine%Кому: %MessageRecipients%%NewLine%Получатели
копии: %MessageCCRecipients%

Отфильтрованные

Макрос: ObjectType Вставить

☒ Включить

Текст сообщения: Dr.Web для Exchange отфильтровал %ObjectType%. %
ObjectType% удален.%NewLine%Имя файла: %FileName%%
NewLine%Подробности фильтрации: %FilteringDetails%%
NewLine%Тема письма: %MessageSubject%%NewLine%От: %
MessageSender%%NewLine%Кому: %MessageRecipients%%

Подозрительные

Поврежденные

Сохранить

Рисунки 7 и 8. Раздел настройки журнала событий

- Чтобы включить ведение журнала для определенного типа объектов, установите флажок **Включить** напротив соответствующего типа (например, на [рис. 7, 8](#) ведение журнала событий включено для **Невыявленных**, **Отфильтрованных**, **Подозрительных** и **Поврежденных** писем и отключено для **Выявленных** писем и **Спама**).



3. В поле **Текст сообщения** вы можете изменить шаблон для сообщения, которое сохраняется в журнале событий. При редактировании текста вы можете использовать макросы.
4. Нажмите кнопку **Сохранить**, когда закончите изменять настройки журнала событий.

Сканирование

Процесс сканирования настраивается в разделе настроек **Сканирование**. Изменение параметров в этом разделе влияет на типы проверяемых объектов, а следовательно, на уровень защищенности сервера. С другой стороны, увеличение числа типов объектов для проверки может привести к снижению производительности сервера.

Чтобы настроить параметры сканирования:

1. Выберите пункт **Сканирование** для настраиваемого профиля в дереве консоли/веб-консоли. Откроется область сведений для настройки сканирования (см. [рис. 9, 10](#)).



Dr.WEB®
для Microsoft Exchange Server

Сканирование

☒ Включить эвристический анализатор
☒ Проверять архивы

Время ожидания: 10000 мс
☐ Рассматривать архивы с паролем как поврежденные

Обнаруживать

☒ Потенциально опасные программы
☐ Программы дозвона
☒ Программы взлома

☐ Рекламные программы
☐ Программы-шутки

Выберите действия

Для неизлечимых и поврежденных объектов:
Удалить вложенный файл

Для подозрительных объектов:
Поместить в карантин

Прикреплять следующий файл к зараженным письмам:

Суффикс имени: _infected.txt

Текст: Инфицированный вирусом файл %FileName% был %State% Dr.Web для Exchange%NewLine%%Viruses%

Макрос...

Сохранить

☒ Включить эвристический анализатор
☒ Проверять архивы

Время ожидания: 10000 мс
☐ Рассматривать архивы с паролем как поврежденные

Обнаруживать

☐ Потенциально опасные программы
☐ Программы дозвона
☐ Программы взлома

☐ Рекламные программы
☐ Программы-шутки

Выберите действия

Для неизлечимых и поврежденных объектов:
Удалить вложенный файл

Для подозрительных объектов:
Поместить в карантин

Прикреплять следующий файл к зараженным письмам

Суффикс имени: _infected.txt

Макрос: ObjectType Вставить

Текст: Инфицированный вирусом файл %FileName% был %State% Dr.Web для Exchange%NewLine%%Viruses%

Сохранить

Рисунки 9 и 10. Раздел настроек сканирования



2. По умолчанию включены эвристический анализатор и проверка прикрепленных архивов. Это обеспечивает более надежную защиту, но приводит к некоторому уменьшению производительности сервера. Чтобы отключить эти режимы, снимите флажки **Включить эвристический анализатор** и **Проверять архивы** в верхней части области сведений раздела **Сканирование**.



Отключать эвристический анализатор и проверку прикрепленных архивов не рекомендуется, т.к. это приведет к существенному снижению уровня защищенности сервера.

Рядом с этими флажками находится поле ввода для времени ожидания на сканирование одного файла. Если при проверке файла время ожидания истекло, то файл считается поврежденным. По умолчанию задано 10000 мс. При необходимости вы можете изменить это значение.

Флажок **Рассматривать архивы с паролем как поврежденные** определяет, будет ли программа игнорировать такие архивы или применять к ним действия, заданные для поврежденных объектов.

3. В группе настроек **Обнаруживать** вы можете указать типы вредоносных объектов, которые следует искать в письмах. Для этого установите соответствующие флажки.
4. Ниже, в группе настроек **Выберите действия**, укажите желаемые действия для неизлечимых и поврежденных, а также подозрительных объектов, используя соответствующие выпадающие списки. Вы можете выбрать одно из следующих действий:
 - **Заблокировать сообщение** – означает, что письмо будет заблокировано в почтовом ящике на сервере;
 - **Запросить удаление** – означает, что **Dr.Web для Microsoft Exchange Server** пошлет запрос серверу на удаление данного письма (результат будет зависеть от настроек сервера Exchange);



- **Поместить в карантин** – означает, что тело письма будет пропущено, а вложенный файл отправлен в карантин (см. [Управление Карантином](#));
- **Удалить вложенный файл** – означает, что тело письма будет пропущено, а вложенный файл удален;
- **Пропустить** – означает, что письмо будет пропущено и направлено получателю (действие доступно только для подозрительных объектов).



По умолчанию для неизлечимых и поврежденных объектов выбрано действие **Удалить вложенный файл**, для подозрительных – **Поместить в карантин**.

5. В группе настроек **Прикреплять следующий файл к зараженным письмам** вы можете изменить суффикс имени файла, который прилагается к зараженному письму после того, как программа совершит над ним выбранное действие. В поле **Текст** вы можете изменить содержимое прикрепленного текстового файла. При редактировании текста вы можете использовать макросы, выбирая их в списке **Макрос**.
6. Нажмите кнопку **Сохранить**, когда закончите изменять настройки параметров сканирования.



Антиспам

Работа **Антиспама** настраивается в разделе настроек профиля **Антиспам**. Он доступен только для версии «Антивирус + Антиспам». Если ваш ключевой файл поддерживает использование компонента **Антиспам**, то фильтрация спама должна быть включена по умолчанию (т.е. должен быть установлен флажок **Включить антиспам** в верхней части области сведений раздела **Антиспам**).



Если настройки в разделе **Антиспам** недоступны, то скорее всего ваша лицензия не поддерживает компонент **Антиспам** (см. [Лицензионный ключевой файл](#)).

Чтобы проверить, поддерживается ли компонент **Антиспам** вашей лицензией, откройте ваш ключевой файл (файл drweb32.key, расположенный в каталоге C:\Program Files\DrWeb for Exchange\), в текстовом редакторе и найдите в нем значение параметра SpamFilter. Если SpamFilter=Yes, то это означает, что ваша лицензия поддерживает использование компонента **Антиспам**, если SpamFilter=No, компонент **Антиспам** не поддерживается.

Любое редактирование ключевого файла делает его недействительным! Поэтому не сохраняйте ключевой файл при закрытии текстового редактора.

Антиспам анализирует содержимое электронных сообщений и делает заключение о том, являются ли они спамом, на основе подсчета различных параметров, характерных для спама.

Чтобы настроить работу Антиспама:

1. Выберите пункт **Антиспам** для настраиваемого профиля в дереве консоли/веб-консоли. Откроется область сведений раздела **Антиспам** (см. [рис. 11, 12](#)).



Dr.WEB® 
для Microsoft Exchange Server

Антиспам

☒ Включить антиспам
☐ Добавлять predetermined SMTP-заголовки

Префикс в теме:
Получатель спама:

Точно спам

 Действие: ☐ Добавлять префикс в тему

Возможно, спам

 Действие: ☒ Добавлять префикс в тему

Маловероятно, что спам

 Действие: ☐ Добавлять префикс в тему

☒ Включить Антиспам
☐ Добавлять predetermined SMTP-заголовки

Префикс в теме:
Получатель спама:

Точно спам

Действие: ☐ Добавлять префикс в тему

Возможно, спам

Действие: ☒ Добавлять префикс в тему

Маловероятно, что спам

Действие: ☐ Добавлять префикс в тему

Рисунки 11 и 12. Раздел настроек Антиспама

- Чтобы отключить **Антиспам**, снимите флажок **Включить антиспам**. При этом все настройки параметров компонента **Антиспам** станут недоступны. Чтобы включить фильтрацию спама, установите флажок **Включить антиспам**.



3. Установите флажок **Добавлять predeterminedенные SMTP-заголовки**, если вы хотите, чтобы к проверяемым письмам добавлялся заголовок вида:

```
X-AntiVirus: Checked by Dr.Web [plugin:  
6.00.00.201101170, scanner: 6.0.12080.3,  
engine: 5.0.3300.2, virus records:  
1821073, updated: 18.01.2011]
```

```
X-DrWeb-SpamRate: 100
```

```
X-DrWeb-SpamReason: 1 random string(s)  
(100)
```

```
X-DrWeb-SpamState: Yes
```

```
X-DrWeb-SpamVersion: 1.310.07
```

4. В поле **Префикс в теме** вы можете изменить префикс, добавляемый в тему письма, которое признано спамом. По умолчанию установлен префикс ***** SPAM *****.
5. В поле **Получатель спама** вы можете указать адрес, на который будут перенаправлены письма, относящиеся к категориям спама, для которых выбрано действие **Отправить заданному получателю спама**.
6. В полях ниже вы можете задать действия программы по отношению к сообщениям в зависимости от степени вероятности их принадлежности к спаму (**Точно спам, Возможно, спам, Маловероятно, что спам**). Для этого выберите желаемые действия из выпадающих списков для каждой категории:
- **Не принимать письмо** – означает, что сообщение не будет принято сервером и доставлено получателю;
 - **Переместить в папку Junk E-mail** – означает, что сообщение будет помещено в специальную папку Junk E-mail почтового ящика получателя; Данная папка поддерживается системой фильтрации нежелательной почты Microsoft Junk E-mail Filter;
 - **Отправить заданному получателю спама** – означает, что письмо будет перенаправлено на адрес, указанный в поле **Получатель спама**;
 - **Пропустить** – означает, что письмо будет пропущено и доставлено получателю;
 - **Удалить** – означает, что письмо будет удалено.



7. Если вы хотите, чтобы префикс (указанный в поле **Префикс в теме**) добавлялся к теме определенной категории писем, то установите флажок **Добавлять префикс в тему** для этой категории.
8. Нажмите кнопку **Сохранить**, когда закончите изменять настройки **Антиспама**.

Фильтрация

Фильтрация писем настраивается в разделе настроек профиля **Фильтрация**. Работа фильтров определяется набором правил, которые могут добавляться администратором. Правила задают условия для фильтрации сообщений по основным свойствам вложений. Кроме того, при помощи правил антидистрибуции вы можете предотвратить нежелательные массовые рассылки.

Чтобы настроить фильтрацию сообщений:

1. Включите фильтрацию, установив флажок **Включить фильтрацию** в верхней части области сведений раздела **Фильтрация**. При этом, настройки в данном разделе станут доступными.
2. В поле **Суффикс имени файла** вы можете при необходимости изменить суффикс, который добавляется к имени файла, прикрепляемого к отфильтрованному письму.
3. В поле **Текст** вы можете изменить текст, содержащийся в прикрепляемом файле. При редактировании текста вы можете использовать макросы, выбирая их в списке **Макрос**.

В нижней части области сведений раздела **Фильтрация** находится список правил, который по умолчанию пуст.

Чтобы создать правило:

- если вы используете **Консоль Администратора**, для создания нового правила нажмите кнопку **Создать** под списком. Откроется окно **Правило** (см. [рис. 13](#)), в котором вы можете выбрать тип правила и указать значение, соответствующее этому типу;

**Рисунок 13. Настройка правила фильтрации**

- если вы используете **Веб-консоль Администратора**, выберите тип правила под списком правил и нажмите кнопку **Создать** (см. [рис. 14](#)).

Рисунок 14. Настройка правил фильтрации

Вам доступны следующие типы правил:

- **Расширение** – означает, что **Dr.Web для Microsoft Exchange Server** будет фильтровать электронные письма с приложенными файлами указанного типа (в поле **Значение** необходимо указать расширение файла, например, `exe`, `com`, `dll` и т.п.);
- **Маска** – означает, что подвергаться фильтрации будут электронные письма с приложенными файлами, в названии которых содержится текст, указанный в поле **Значение** (должно быть указано имя вместе с расширением файла);



Вы можете использовать подстановочные символы «*» и «?» вместо любой последовательности символов или одного любого символа вводимого текста соответственно.

- **Максимальный размер файла** – означает, что подвергаться фильтрации будут электронные письма с приложенными файлами больше определенного размера (размер указывается в байтах);



- Типы **Максимум получателей** и **Максимум получателей писем с приложениями** определяют максимальное число получателей, разрешенное для одного электронного письма.

Первые три типа правил используются для блокировки вложений, получаемых адресатами групп с редактируемым в данный момент профилем. Например, если вы создадите правило с типом **Расширение** и укажете `exe` в поле **Значение**, то все файлы с расширением `exe`, приложенные к электронным письмам адресатов групп, которым назначен указанный профиль, будут блокироваться на сервере, а сами письма будут доставляться их получателям с прикрепленным текстовым уведомлением. Шаблон таких уведомлений можно изменить в поле **Текст** в области сведений раздела **Фильтрация**. Имя текстового файла с уведомлением будет состоять из имени вложенного файла и суффикса, указанного в поле **Суффикс имени файла**. Таким образом, по умолчанию, при фильтрации вложенного файла `filename.ext`, имя файла уведомления будет следующим: `filename.ext_filtered.txt`.

Последние два типа правил используются для предотвращения массовых рассылок в среде Exchange и применяются к адресатам группы с указанным профилем, как к отправителям. Создайте правило типа **Максимум получателей** или **Максимум получателей писем с приложениями** и задайте максимальное число получателей в поле **Значение**. Письма с числом получателей равным или меньшим этому значению будут доставлены. В противном случае (если число получателей письма будет больше указанного значения) письмо будет удалено, и администратору будет направлено уведомление об этом.



Чтобы изменить или удалить существующее правило:

- если вы используете **Консоль администратора**, выберите правило в списке и нажмите кнопку **Изменить** или **Удалить** под списком правил;
- в случае использования **Веб-консоли Администратора**, для изменения параметров правила нажмите **Изменить** слева от типа фильтра, отредактируйте значения параметров и нажмите **Обновить**. Для удаления правила, нажмите **Удалить** слева от его типа фильтра.

Нажмите кнопку **Сохранить**, когда закончите изменять настройки фильтрации.

Сопроводительный текст

В разделе настроек профиля **Сопроводительный текст** (см. [рис. 15, 16](#)) вы можете настроить добавление дополнительного текста в конец всех исходящих с сервера сообщений.

Установите флажок **Включить (сопроводительный текст)** в верхней части области сведений, чтобы добавлять сопроводительный текст к исходящим сообщениям. Ниже расположены два поля ввода. В первом можно ввести текст в формате HTML (для писем, посылаемых в формате HTML), а во втором поле можно ввести чистый текст (для простых текстовых сообщений).



Dr.WEB®
для Microsoft Exchange Server

Сопроводительный текст

☒ Включить сопроводительный текст

Параметры

HTML:
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0/EN">
<html>
<head meta http-equiv="Content-Type" content="text/html; charset=windows-1251"></head>
<body>
This message has been checked by Dr.Web for Microsoft Exchange Server

With best regards, My Company (c)

</body>
</html>

Чистый текст:

This message has been checked by Dr.Web for Microsoft Exchange Server
With best regards, My Company (c)

Сохранить

☒ Включить

Чистый текст:

This message has been checked by Dr.Web for Microsoft Exchange Server
With best regards, My Company (c)

HTML:

This message has been checked by Dr.Web for Microsoft Exchange Server
With best regards, My Company (c)

Font default
Size default

Сохранить

Рисунки 15 и 16. Настройка сопроводительного текста

Нажмите кнопку **Сохранить**, когда закончите изменять настройки сопроводительного текста.



Сопроводительный текст добавляется только в те электронные сообщения, которые посылаются с сервера, защищаемого **Dr.Web для Microsoft Exchange Server**, на другой сервер.

Управление группами клиентов

По умолчанию **Dr.Web для Microsoft Exchange Server** применяет параметры **Стандартного** профиля для всех клиентов. Если вы желаете применить параметры другого профиля для определенных клиентов (см. [Создание и настройка профилей](#)), то вам необходимо объединить этих клиентов в группу и присвоить ей созданный профиль. Таким образом, вы можете разделить всех клиентов Exchange на группы, для каждой из которых будут установлены отдельные параметры защиты.

Создание новой группы

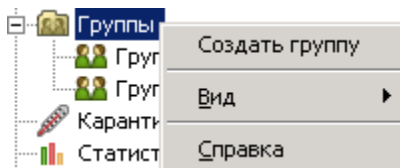
Чтобы создать новую группу:

1. Выберите пункт **Группы** в дереве **Консоли Администратора** или **Веб-консоли Администратора**.
2. В открывшейся справа области сведений раздела **Группы** нажмите кнопку **Создать** (при использовании веб-консоли

обозначена изображением , расположенную над списком существующих групп.



Либо, если вы используете **Консоль Администратора** при настройке работы программы, щелкните правой кнопкой на пункте **Группы** в дереве консоли и нажмите **Создать группу** в появившемся контекстном меню (см. иллюстрацию ниже).



Будет создана новая группа с именем **Группа1**, которая появится в дереве консоли/веб-консоли под пунктом **Группы**. Если группа с таким именем уже существует, то именем новой группы будет **Группа2** и т.д. По умолчанию, новой группе назначается **Стандартный** профиль.

Чтобы изменить имя группы:

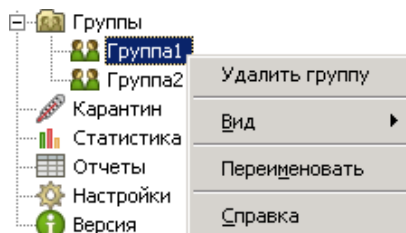
- при использовании **Консоли Администратора** выберите нужную группу в списке в области сведений раздела **Группы** и нажмите кнопку **Переименовать**;
- при использовании **Веб-консоли Администратора** введите новое имя группы в соответствующее текстовое поле, затем нажмите кнопку **Переименовать** , которая появится рядом с текстовым полем.

Чтобы удалить группу:

- выберите ее в списке в области сведений раздела **Группы** и нажмите кнопку **Удалить** (при использовании веб-консоли обозначена изображением ).



Либо, если вы используете **Консоль Администратора** при настройке работы программы, чтобы удалить или переименовать группу, щелкните правой кнопкой на имени этой группы в дереве консоли и выберите соответствующий пункт в появившемся контекстном меню (см. иллюстрацию ниже).



Чтобы открыть настройки группы

- чтобы открыть область сведений с настройками группы, выберите ее имя в дереве консоли/веб-консоли.

В поле **Имя группы** вы можете, при необходимости, изменить имя выбранной группы, а в выпадающем списке **Профиль** – выбрать профиль, который будет применяться для созданной группы. Кроме того, вы можете выбрать тип группы, определяющий способ ее формирования. Существует два способа формирования групп клиентов Exchange: **Группы Active Directory** и **Указать адреса клиентов** (см. [Формирование группы](#)).

Когда вы закончите создание и формирование необходимых вам групп, нажмите кнопку **Сохранить**.

Формирование группы

Для выбранной группы вы можете изменить ее настройки, в том числе определить способ ее формирования. Существует 2 типа групп клиентов Exchange: **Группы Active Directory** и **Указать адреса клиентов**.



Группы Active Directory

Если выбран тип группы **Группы Active Directory**, то группа клиентов Exchange должна состоять из групп AD.

Чтобы создать группу клиентов из групп Active Directory:

- при использовании **Консоли Администратора**, добавьте имена групп AD в поле **Параметры** или выберите необходимые группы посредством окна выбора групп **Select Groups**, которое открывается при нажатии кнопки **Выбрать** (см. [рис. 17](#)).

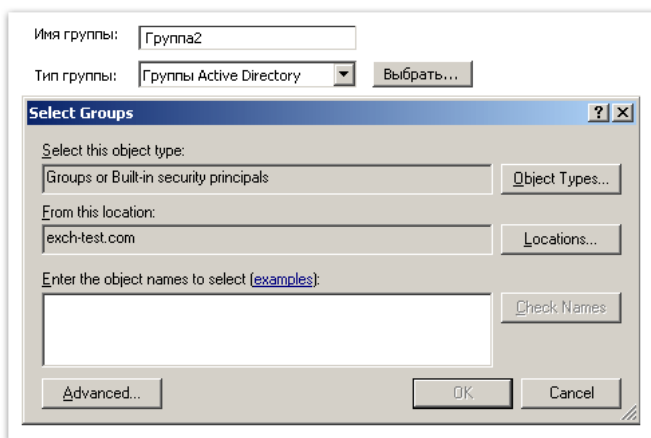


Рисунок 17. Окно Select Groups

В окне **Select groups** выберите тип и местоположение объекта, введите его имя и нажмите кнопку **ОК**. Если группа AD с таким именем существует, то она будет добавлена к группе Exchange и ее имя появится в поле **Параметры** в настройках группы.

Для поиска необходимых групп AD вы можете воспользоваться расширенными настройками окна **Select Groups**, для доступа к которым нажмите кнопку **Advanced**.



Чтобы найти группу, выберите тип объекта и его местоположение, укажите примерное или полное имя в поле ввода **Name** и нажмите кнопку **Find Now**. Затем выберите нужную(ые) группу(ы) в списке **Search Results** в нижней части окна и нажмите **OK**.



Вы можете оставить поле **Name** пустым, и тогда в списке будут отображены все объекты выбранного типа в указанном месте.

- при использовании **Веб-консоли Администратора**, с помощью списка **Параметры** выберите группы Active Directory, которые вы хотите добавить в редактируемую группу клиентов Exchange. Для добавления выбранной группы нажмите кнопку **Вставить**. (см. [рис. 18](#)).

Рисунок 18. Создание группы Active Directory

Указать адреса клиентов

Если выбран тип группы **Указать адреса клиентов**, то группа Exchange должна быть сформирована из диапазона электронных адресов клиентов, указываемых в поле ввода **Параметры** (см. [рис. 19, 20](#)).



Имя группы:

Тип группы:

Параметры:

user3@mycompany.com
user5@mycompany.com
user7@mycompany.com

Группа: Группа1

Профиль:

Тип:

Параметры:

user1@mycompany.com
user2@mycompany.com
user5@mycompany.com

Рисунки 19 и 20. Создание группы с помощью ввода адресов клиентов



Вы можете использовать подстановочные символы «*» и «?» вместо любой последовательности символов или одного любого символа вводимого текста соответственно.



В **Dr.Web** для **Microsoft Exchange Server** работа **Карантина** осуществляется при помощи служебной базы, в которой также хранится информация о событиях (действиях над зараженными письмами и спамом, см. [Просмотр статистики](#)). Когда к объекту, вложенному в письмо, применяется действие **Поместить в карантин** (см. раздел [Сканирование](#)), то объект помещается в эту служебную базу, и информация о нем добавляется в список в нижней части области сведений раздела **Карантин** (см. [рис. 21, 22](#)).

Руководство администратора



☐	Дата/Время	Название вируса	Отправитель	Тема	Получатели	Имя файла
☐	04.10.2010 14:56:53	Trojan.PWS.Lineage	Administrator@EXCHSR V-WORK.com	Test Message From XML Config #1	Administrator@EXCHSR V-WORK.com	cannotcure.exe
☐	04.10.2010 14:56:54	Trojan.PWS.Lineage	Administrator@EXCHSR V-WORK.com	Test Message From XML Config #2	Administrator@EXCHSR V-WORK.com	cannotcure.exe
☐	04.10.2010 14:56:55	Trojan.PWS.Lineage	Administrator@EXCHSR V-WORK.com	Test Message From XML Config #3	Administrator@EXCHSR V-WORK.com	cannotcure.exe

Очистка списка

Удалить записи старше дней

Автоматически удалять записи старше дней

Рисунки 21 и 22. Карантин

Для каждого объекта, перемещенного в **Карантин**, в списке отображается следующая информация:

- дата и время перемещения в **Карантин**;
- название вируса;
- электронный адрес отправителя письма, содержавшего зараженный объект;
- тема письма, содержавшего зараженный объект;
- электронные адреса получателей письма, содержавшего зараженный объект;
- имя зараженного файла.

При использовании **Консоли Администратора** вы можете применить один или несколько фильтров к списку **Карантина** согласно определенным критериям, чтобы было удобнее просматривать информацию о помещенных в **Карантин** объектах.



Чтобы настроить фильтрацию записей в списке Карантина:

1. Чтобы включить фильтрацию, установить флажок **Фильтр**. При этом настройки в данном разделе станут доступными. Вы можете применить один или несколько фильтров к списку согласно определенным критериям, чтобы было удобнее просматривать информацию о помещенных в **Карантин** объектах.
2. Чтобы добавить новый фильтр, нажмите кнопку добавления фильтра  справа от параметров любого фильтра.
3. Для настройки фильтра выберите тип критерия фильтрации в двух выпадающих списках и введите значение критерия.
4. Для удаления фильтра нажмите кнопку удаления фильтра  справа от его параметров.
5. Нажмите кнопку **Применить**, чтобы сохранить сделанные изменения.

Действия над объектами в Карантине

1. Чтобы удалить один или несколько объектов из **Карантина**, выделите их в списке и нажмите кнопку **Удалить**.
2. Чтобы сохранить один или несколько объектов, перемещенных в **Карантин**, в файловой системе, выделите их в списке и нажмите кнопку **Копировать**.
3. Вы можете повторно сканировать находящиеся в **Карантине** объекты, например, чтобы обезвредить новые угрозы после обновления антивирусных баз. Для этого выделите один или несколько объектов в списке и нажмите кнопку **Сканировать**.
4. Для обновления списка **Карантина** нажмите кнопку **Обновить**.



Список помещенных в **Карантин** объектов обновляется при каждом запуске **Консоли Администратора** и обновлении страницы **Веб-консоли Администратора**, но если консоль была запущена или страница веб-консоли не обновлялась в течение некоторого времени, то рекомендуется периодически обновлять список вручную.

Чтобы очистить список Карантина:

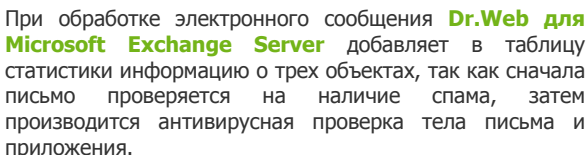
1. Чтобы удалить из списка записи старше определенного количества дней, в группе настроек **Очистка списка** укажите количество дней в соответствующем поле и нажмите кнопку **Удалить**.
2. Укажите количество дней для автоматического удаления из списка записей старше этого количества дней. По умолчанию из списка автоматически удаляются записи старше 20 дней.

Нажмите кнопку **Сохранить**, чтобы сохранить изменения настроек в разделе **Карантин**.

Просмотр статистики

Выберите пункт **Статистика** в дереве **Консоли Администратора** или **Веб-консоли Администратора**, чтобы перейти к просмотру статистики работы **Dr.Web для Microsoft Exchange Server**. Область сведений раздела **Статистика** состоит из двух вкладок/разделов:

- на вкладке/в разделе **Статистика** вы можете просмотреть таблицу с обзором общего количества объектов, обработанных **Dr.Web для Microsoft Exchange Server**. Вы можете очистить или обновить статистическую информацию, нажав на соответствующую кнопку под этой таблицей;



- на вкладке/в разделе **События** (см. [рис. 23, 24](#)) вы можете просмотреть список писем, обработанных **Dr.Web для Microsoft Exchange Server**, в которых обнаружены вирусы или спам, а также отфильтрованных писем. Он аналогичен списку в области сведений раздела **Карантин** (см. [Управление Карантином](#)), так как использует ту же базу.

Руководство администратора



Статистика	
Проверено объектов:	0
Зараженных объектов:	0
Подозрительных объектов:	0
Спан-писем:	0
Вылечено объектов:	0
Чистых объектов:	0
Удалено объектов:	0
Перенесено объектов:	0
Заблокировано рассылок:	0
Заблокировано объектов:	0
Отфильтровано объектов:	0
Поврежденных объектов:	0

События	
---------	--

Рисунки 23 и 24. Вкладка/раздел События

При использовании **Консоли Администратора** список можно отсортировать по тому или иному критерию, нажимая на соответствующие заголовки колонок. Кроме того, к списку можно применить один или несколько фильтров, используя группу настроек **Фильтр**.

При работе со списком событий вам доступны следующие действия:

- список событий можно сохранить в виде текстового файла. Для этого нажмите кнопку **Экспорт**;
- для обновления списка нажмите кнопку **Обновить**;
- с помощью группы настроек **Очистка списка** вы можете удалить из списка записи старше определенной даты. Чтобы удалить из списка записи о событиях, произошедших ранее определенной даты, укажите дату в соответствующем поле и нажмите кнопку **Очистить**. По умолчанию из списка автоматически удаляются все записи старше 30 дней. При необходимости вы можете изменить это значение в соответствующем поле ввода.



Управление отчетами

Выберите пункт **Отчеты** в дереве **Консоли Администратора** или **Веб-консоли Администратора**, чтобы настроить рассылку отчетов о работе **Dr.Web для Microsoft Exchange Server**. Отчеты рассылаются в виде приложенных файлов на адреса, которые задаются администратором.

В верхней части области сведений раздела **Отчеты** (см. [рис. 25, 26](#)) находится список из 6 доступных типов отчетов:

- все вирусные события;
- подсчет спама/количество спам-писем;
- получатели самого большого количества спама;
- получатели самого большого числа зараженных сообщений;
- последние обнаруженные вирусы;
- события по получателям.

Dr.WEB®
для Microsoft Exchange Server

Отчеты

Отчеты

Отчет	Тема	Получатели	Дни	Расписание
☐ Все вирусные события	Отчёт Dr.Web...		5	Задание не запланировано
☐ Подсчет спама	Отчёт Dr.Web...		5	Задание не запланировано
☐ Получатели самого большого количества спама	Отчёт Dr.Web...		5	Задание не запланировано
☐ Получатели самого большого числа зараженных сообще...	Отчёт Dr.Web...		5	Задание не запланировано
☐ Последние обнаруженные вирусы	Отчёт Dr.Web...		5	Задание не запланировано

Отправить

Расписание...

Настройки

Письмо

Тема:

Текст:

Получатели:

Не отсылать отчеты старше дней

Сохранить



Отчет	Тема	Получатели	Дни	Расписание
☒ Все вирусные события	Отчет Dr.Web для Microsoft Exchange: Все вирусные события	Administrator@EXCHSRV-WORK.com	5	Задание не запланировано
☐ События по получателям	Отчет Dr.Web для Microsoft Exchange: События по получателям	Administrator@EXCHSRV-WORK.com	5	Задание не запланировано
☐ Последние обнаруженные вирусы	Отчет Dr.Web для Microsoft Exchange: Последние обнаруженные вирусы	Administrator@EXCHSRV-WORK.com	5	Задание не запланировано
☐ Получатели самого большого количества спама	Отчет Dr.Web для Microsoft Exchange: Получатели самого большого количества спама	Administrator@EXCHSRV-WORK.com	5	Задание не запланировано
☐ Получатели самого большого числа зараженных сообщений	Отчет Dr.Web для Microsoft Exchange: Получатели самого большого числа зараженных сообщений	Administrator@EXCHSRV-WORK.com	5	Задание не запланировано
☐ Количество спам-писем	Отчет Dr.Web для Microsoft Exchange: Подсчет спама	Administrator@EXCHSRV-WORK.com	5	Задание не запланировано

Настройки

Тема: Отчет Dr.Web для Microsoft Exchange: Все вирусные события

Текст: Отчет находится в прикрепленном файле.

Кому: Administrator@EXCHSRV-WORK.com

Отправлять отчет за последние 5 дней

Рисунки 25 и 26. Раздел настроек рассылки отчетов о работе программы

По умолчанию все типы отчетов выключены, для них не созданы расписания и не назначены получатели.

Чтобы включить определенный тип отчетов:

1. Установите флажок в соответствующей строке списка.
2. При необходимости измените шаблон темы и текста письма с отчетом данного типа.
3. Укажите электронные адреса получателей отчетов выбранного типа.

Кроме того, вы можете задать количество дней, в течение которых собирается информация для отчета. События, произошедшие ранее указанного периода, не будут отражены в отчете.

Вы можете отправить отчеты выбранных типов вручную, нажав кнопку **Отправить**, расположенную под списком, или создать расписание для них.



Чтобы составить расписание для определенного типа отчетов:

1. Выберите тип отчета и нажмите кнопку **Расписание** под списком. Откроется окно для настройки расписания (см. [рис. 27, 28](#)).

The screenshot shows a Windows-style dialog box titled "SettingsTask". It has a tab labeled "Расписание" (Schedule). Inside the dialog, there is a text box containing the text "1. В 9:00, ежедневно, начиная с 30.12.2008" with a dropdown arrow on the right. Below this text box are two buttons: "Создать" (Create) and "Удалить" (Delete). Further down, there are two labels: "Назначить задание:" (Assign task:) and "Время начала:" (Start time:). Under "Назначить задание:" is a dropdown menu showing "Ежедневно" (Daily). Under "Время начала:" is a time picker showing "9:00" and a button labeled "Дополнительно..." (More...). Below these is a section titled "Расписание по дням" (Schedule by day) containing the text "каждый" (every), a spinner box with the number "1", and the word "день" (day). At the bottom left, there is a checked checkbox labeled "Показывать несколько расписаний" (Show multiple schedules). At the bottom right, there are two buttons: "ОК" and "Отмена" (Cancel).



Рисунки 27 и 28. Окно настроек расписания для отправки отчетов

2. Нажмите кнопку **Создать**, чтобы добавить новое задание.



Чтобы удалить существующее задание, выберите его в выпадающем списке в верхней части окна и нажмите кнопку **Удалить**.

3. Настройте частоту и время отсылки отчетов для выбранного задания в выпадающем списке **Назначить задание** и в поле **Время начала**, а также дополнительные условия в группе настроек ниже. Вы можете выбрать периодичность отправки отчетов – каждый день, в определенные дни недели или месяца, при включении системы, при входе в систему, либо при простое системы в течении некоторого времени.
4. При использовании **Консоли Администратора** вы также можете использовать расширенные настройки параметров расписания, для перехода к которым нажмите кнопку **Дополнительно**. Откроется окно **Дополнительные настройки расписания** (см. [рис. 29](#)).



Рисунок 29. Расширенные настройки расписания отчетов

Внесите необходимые изменения в дополнительных параметрах расписания и нажмите кнопку **ОК**.

5. Когда вы закончите составление расписания для выбранного типа отчетов, нажмите кнопку **ОК**, чтобы сохранить изменения.

Нажмите кнопку **Сохранить**, когда вы закончите настраивать необходимые типы отчетов.



Изменения в расписании и параметрах сохраняются только для включенных типов отчетов (т.е. для которых установлен флажок в списке типов отчетов).



Общие настройки

В разделе **Настройки** задаются общие параметры работы программы. В разделе настроек **Протокол уведомлений** вы можете выбрать и настроить протокол отправки уведомлений программы, а также задать сервер, с которого будет осуществляться отправка уведомлений. В разделе настроек **Учетная запись** вы можете изменить параметры учетной записи для администрирования программы. В разделе настроек **Черные/Белые списки** вы можете создавать и редактировать черный и белый списки электронных адресов для компонента **Антиспам**.

Протокол уведомлений

Вы можете выбрать и настроить отработку уведомлений через один из следующих протоколов:

- **MAPI.** Для использования данного протокола укажите электронный адрес и пароль администратора, а также имя сервера, с которого будет осуществляться отправка уведомлений;



При использовании Microsoft Exchange версии 2007/2010 для отправки уведомлений и отчетов через протокол MAPI необходимо установить пакет Microsoft Exchange Server MAPI Client and Collaboration Data Objects, доступный на официальном сайте компании Microsoft по адресу <http://www.microsoft.com/downloads/details.aspx?FamilyID=E17E7F31-079A-43A9-BFF2-0A110307611E&displaylang=en>.

- **SMTP.** Для данного протокола необходимо указать электронный адрес и пароль администратора, а также имя сервера и номер порта для отправки уведомлений;
- **HTTP.** В данном случае необходимо указать электронный адрес и пароль администратора, а также URL-адрес и версию сервера Exchange.

Чтобы проверить правильность настроек выбранного протокола,



отправьте тестовое сообщение. В группе настроек **Протестировать выбранную конфигурацию** задайте следующие параметры тестового сообщения:

- адрес получателя;
- тема сообщения;
- текст сообщения;
- вложенный файл.

Чтобы отправить тестовое сообщение, нажмите кнопку **Отправить тестовое письмо**.

Чтобы сохранить настройки протокола, нажмите кнопку **Сохранить**.

Учетная запись сервиса

В данном разделе вы можете указать основное имя пользователя (UPN) и пароль учетной записи (не обязательно принадлежащей администратору) для управления приложением.

Черные/Белые списки

В разделе настроек **Черные/Белые списки** (см. [рис. 30, 31](#)) вы можете настроить использование черного и белого списков.

Dr.WEB®
для Microsoft Exchange Server

Протокол уведомления | Учетная запись сервиса | **Черные/Белые списки** | Настройки

☒ Включить

E-Mail

Добавить в белый список

e-mail
trusted_address1@mail.com
trusted_address2@mail.com

Убрать из белого списка

Добавить в черный список

e-mail
distrusted_address@mail.com
*@distrusted_domain.com

Убрать из черного списка

Импорт | Экспорт | Сохранить



Рисунки 30 и 31. Раздел настроек черного и белого списков

Установите флажок **Включить**, чтобы включить использование списков. Вы можете добавить электронные адреса, которым вы доверяете, в белый список. Письма с данных адресов не будут проходить проверку на спам. Если же вы добавите адрес в черный список, то всем письмам с этого адреса будет присваиваться статус **Точно спам**.

Для того, чтобы добавить электронный адрес, введите его в поле **E-mail**, а затем нажмите кнопку **Добавить в белый список** или **Добавить в черный список** для добавления в нужный список.

Для того, чтобы удалить электронный адрес из списка, выберите его в нужном списке и нажмите кнопку **Удалить из белого списка** или **Удалить из черного списка**.



Вы можете также использовать кнопки **Импорт** и **Экспорт** для сохранения списков в специальный файл с расширением **.lst** или их загрузки из файла, при этом создавать и редактировать списки можно вручную с помощью текстового редактора, например, Блокнота.

При создании и редактировании файлов черного и белого списков вручную, электронные адреса должны указываться с префиксом «+» (для добавления адреса в белый список) или «-» (для добавления адреса в черный список), например **+trusted_address@mail.com** и **-distrusted_address@mail.com**, а сам текстовый файл должен быть сохранен с расширением **.lst** в формате Unicode.



Вы можете использовать подстановочный символ «*» вместо части адреса (например, запись вида ***@domain.org** означает все адреса в домене **domain.org**).

Нажмите кнопку **Сохранить**, чтобы принять изменения настроек черного и белого списков.



Обновление антивирусных баз

Во время установки **Dr.Web для Microsoft Exchange Server** в Планировщик Задач Windows (**C:\Windows\Tasks**) добавляется задание на обновление (**DrWeb for Microsoft Exchange Update Task**). Каждые 30 минут оно запускает модуль обновления **DrWebUpW.exe**, который загружает антивирусные базы и компоненты программы.

Вы можете настроить данное задание, изменяя его параметры (для этого дважды щелкните по нему в списке заданий). Вы также можете настроить работу самого модуля обновления, добавляя параметры командной строки (см. [Приложение А](#)) в поле ввода **Выполнить** в параметрах задания.

Например, если вам необходимо настроить обновление без подключения к сети Интернет, сделайте следующее:

1. Создайте папку с любым именем на локальном диске (например, C:\MyDocs\DrWebUpdate).
2. Поместите туда обновляемые компоненты (список доступных компонентов вы можете найти в файле **drweb32.lst**, расположенном в каталоге C:\Documents and Settings\All Users\Application Data\Doctor Web\Bases\).
3. Добавьте следующий параметр командной строки в поле **Выполнить** в настройках задания **DrWeb for Microsoft Exchange Update Task**: /URL: <путь к созданной папке> (например, /URL: "C: \MyDocs\DrWebUpdate").



Регистрация событий

Dr.Web для Microsoft Exchange Server регистрирует ошибки и происходящие события в следующих журналах регистрации:

- журнале регистрации событий операционной системы (Event Log);
- текстовом журнале регистрации событий программы установки;
- текстовых журналах отладки программы.

Информация об обновлениях заносится в отдельный текстовый журнал **drwebupw.log**, расположенный в каталоге %alluserprofile%\AppData\Doctor Web\Logs\ (см. главу [Проверка модуля обновления](#)).

Журнал операционной системы

В журнал регистрации операционной системы (Event Log) заносится следующая информация:

- сообщения о запуске и остановке программы;
- параметры лицензионного ключевого файла: действительность или недействительность лицензии, срок действия лицензии, наличие или отсутствие лицензии на компонент **Антиспам**;
- параметры модулей программы: сканера, ядра, антивирусных баз (информация заносится при запуске программы и при обновлении модулей);
- сообщение о недействительности лицензии: отсутствие ключевого файла, отсутствие в ключевом файле разрешения на использование модулей программы, лицензия заблокирована, нарушение целостности ключевого файла (информация заносится при запуске программы и в процессе ее работы);



- уведомления о завершении срока действия лицензии (информация заносится за 30, 15, 7, 3, 2 и 1 дней до окончания срока).
- информация о поступлении на сервер писем с объектами, которые были вылечены, не вылечены, отфильтрованы или определены как поврежденные или спам (см. раздел [Ведение журнала событий](#)).

Просмотр журнала регистрации операционной системы

1. Чтобы просмотреть журнал регистрации событий операционной системы, откройте **Панель управления** операционной системы.
2. Выберите **Администрирование**, а затем выберите **Просмотр Событий**.
3. В левой части окна **Просмотр Событий** выберите **Приложение**. Откроется список событий, зарегистрированных в журнале пользовательскими приложениями. Источниками сообщений **Dr.Web для Microsoft Exchange Server** являются приложения Dr.Web® Engine, Dr.Web Core Service for MSP и Dr.Web Core Services for MSP Attendant.

Текстовый журнал программы установки

Для упрощения процесса отладки в случае возникновения проблем и ошибок в процессе установки, программа установки ведет регистрацию событий. Файл регистрации событий создается в корневом каталоге диска C:\ и называется **Dr.Web Core Services for MSP.log**. Этот файл содержит информацию об установке сервиса Dr.Web Core Services for MSP. Вы можете удалить данный файл после того, как убедитесь, что установка прошла успешно (см. [Проверка установки](#)).



Кроме того, вы можете включить расширенную регистрацию событий во время процесса установки приложения. Для этого необходимо запустить установочный файл со следующими параметрами: **msiexec /i** <путь к установочному файлу программы> **/lvx*** <путь у журналу программы установки> **CHECK_MAIL_LOG=**<путь к дополнительному журналу программы установки>. В этом случае программа установки создаст два файла по указанным путям, с большей степенью детализации процесса установки приложения.

Текстовый журнал отладки

После установки **Dr.Web для Microsoft Exchange Server** ведение журналов отладки приложения по умолчанию выключено. Включить регистрацию событий для отладки приложения можно с помощью редактирования параметров раздела реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Doctor Web\Core Services for MSP\Logging**, установив значение параметра **DumpToLog** равным 5 (по умолчанию это значение равно 0, т. е. ведение журналов отладки программы выключено).

Все текстовые журналы отладки формируются в каталоге **%alluserprofile%\AppData\Doctor Web\Logs**.



При возникновении ошибок в работе приложения рекомендуется включать ведение журналов отладки только в случае их запроса **Службой Технической поддержки Dr. Web**. Процесс регистрации событий может значительно снизить производительность сервера.



Диагностика

Для проверки работоспособности приложения выполните следующие тесты, приведенные в данной главе:

- проверку правильности установки антивирусного приложения;
- проверку модуля обновления;
- проверку способности обнаруживать вирусы и спам.

Проверка установки

Dr.Web для Microsoft Exchange Server должен быть установлен в следующие папки:

- C:\Program Files\DrWeb for Exchange;
- C:\Documents and Settings\All Users\Application Data\Doctor Web.

Кроме того, при работе с Microsoft Exchange версии 2000/2003 **Dr.Web для Microsoft Exchange Server** должен быть также установлен в папку C:\Program Files\Common Files\Doctor Web, при работе с Microsoft Exchange версии 2007/2010 – в папки C:\Program Files(x86)\DrWeb for Exchange и C:\Program Files(x86)\Common Files\Doctor Web.

Убедитесь, что эти папки созданы и содержат файлы программы.

После этого откройте стандартную утилиту Windows **Просмотр Событий (Event Viewer)** и убедитесь, что не было зафиксировано ошибок, связанных с **Dr.Web для Microsoft Exchange Server**. Затем проверьте отсутствие ошибок в файле Dr.Web Core Services for MSP.log, который создается в корневом каталоге диска C:\ во время установки (см. [Установка Dr. Web для Microsoft Exchange Server](#)).



Наконец, убедитесь, что запущены следующие локальные сервисы:

- Dr.Web® Scanning Engine (DrWebEngine);
- Dr.Web Core Services for MSP;
- Dr.Web Core Services for MSP Attendant.

Проверка модуля обновления

Модуль обновления **DrWebUpW.exe** автоматически запускается после установки **Dr.Web для Microsoft Exchange Server**. Он загружает последние версии антивирусного ядра **drweb32.dll** и ядра антиспама **vrcpp.dll**, а также обновляет антивирусные базы.

Чтобы убедиться, что обновление прошло успешно:

1. В зависимости от версии операционной системы выполните команду **Tasks**, чтобы открыть папку C:\WINDOWS\Tasks или откройте Планировщик заданий Windows.
2. Проверьте наличие задания **Dr.Web для Microsoft Exchange Server** в открывшейся папке (для правильно отработавшего задания код возврата в столбце **Последний результат** должен быть 0x0).
3. Затем откройте файл журнала событий модуля обновления **%allusersprofile%\Application Data\Doctor Web\Logs\drwebupw.log** и убедитесь, что в нем не зафиксировано ошибок.



Проверка детектирования вирусов

Для проверки конфигурации и способности **Dr.Web для Microsoft Exchange Server** обнаруживать вирусы рекомендуется использовать тестовый скрипт EICAR (European Institute for Computer Antivirus Research). Текстовый файл, содержащий только тестовый скрипт EICAR, не является вирусом, не способен к саморепликации и не представляет опасности, однако определяется антивирусными программами как вирус. Вы можете загрузить тестовый файл с веб-сайта EICAR по адресу <http://www.eicar.org/> или создать его самостоятельно.

Чтобы создать тестовый файл EICAR:

Откройте Блокнот и скопируйте в него следующую строку:

```
X5O! P%@AP[ 4\PZX54( P^ ) 7CC) 7} $EICAR-STANDARD  
-ANTI VIRUS-TEST-FILE! $H+H*
```

Сохраните файл с расширением **.com** (вы можете использовать любое имя, например, **eicar.com**), прикрепите его к электронному письму и отправьте на любой тестовый адрес. Полученное на этот адрес письмо должно содержать текстовый файл с суффиксом **_infected.txt** и следующим содержанием:

Инфицированный вирусом файл eicar.com был удален Dr.Web для Exchange. Имя вируса: EICAR Test File (NOT a Virus!).

Помимо этого, **Dr.Web для Microsoft Exchange Server** отправит уведомление с таким же текстом на адрес администратора, указанный во время установки.



Ни в коем случае не используйте настоящие вирусы для проверки работоспособности антивирусных программ!



Проверка детектирования спама



Компонент **Антиспам** доступен только в версии «Антивирус + Антиспам», т.е. в том случае, если у вас есть соответствующий ключевой файл (см. [Лицензионный ключевой файл](#)).

Для проверки способности компонента **Антиспам** обнаруживать спам рекомендуется использовать письмо с тестовой строкой.

Чтобы создать тестовое письмо:

Скопируйте следующую строку в тело нового электронного письма:

```
Start enjoying the benefits of Generic  
Medicine. Order quickly and easily, and save  
a ton of money. Try them out, they're 100%  
money back guarantee.
```

Отправьте письмо по протоколу SMTP на любой тестовый адрес. Откройте стандартную утилиту Windows **Просмотр событий** -> **Приложение (Event Viewer -> Application)** и найдите сообщение о том, что **Dr.Web для Microsoft Exchange Server** обнаружил спам.



Приложения

Приложение А. Параметры командной строки для модуля обновления

Ниже приведен список параметров командной строки, которые могут быть добавлены в поле **Выполнить** в настройках задания на обновление (**DrWeb for Microsoft Exchange Update Task**), чтобы настроить работу модуля обновления.

Параметр	Описание
/DBG	Вести подробный отчет.
/DIR: <каталог>	Переназначение папки, в которую загружаются обновляемые файлы; по умолчанию это папка, из которой модуль обновления был запущен.
/INI: <путь>	Использовать альтернативный конфигурационный файл с указанным именем или по указанному пути.
/NI	Не использовать параметры, записанные в конфигурационном файле drweb32.ini .
/GO	Пакетный режим работы, без диалоговых остановок.
/LNG: <имя файла>	Имя файла языковых ресурсов; если не указано, используется английский язык.
/PASS: <пароль>	Пароль пользователя сервера обновлений.
/USER: <имя>	Имя пользователя сервера обновлений.
/PPASS: <пароль>	Пароль пользователя прокси-сервера.
/PUSER: <имя>	Имя пользователя прокси-сервера.
/PURL: <адрес>	Адрес прокси-сервера.



Параметр	Описание
/ URL: <URL сервера обновлений>	Допускаются только UNC-пути.
/ QU	Принудительно закрывать модуль обновления после окончания сеанса обновления независимо от того, успешно оно прошло или нет. Успешность обновления можно проверить по коду возврата программы drwebupw.exe , например, из BAT-файла по значению переменной errorlevel : • нулевое значение указывает на успех; • другие значения указывают на неудачу.
/ REG	Запуск модуля обновления в режиме регистрации и получения регистрационного ключа.
/ UPD	Обычное обновление; применяется в паре с ключом / REG, чтобы запустить обновление в режиме регистрации.
/ RP <имя файла> или / RP+ <имя файла>	Записать отчет о работе программы в файл, имя которого указано в ключе. При отсутствии имени записать в файл по умолчанию. При наличии символа «+» файл дописывается, при отсутствии – создается заново.
/ NR	Не создавать файл отчета.
/ SO	Включить звуковое сопровождение (только при возникновении ошибок).
/ ST	Запускать модуль обновления в невидимом режиме (<i>stealth mode</i>).



Параметр	Описание
/UA	Загружать все файлы, заявленные в списке обновления, независимо от используемой системы и установленных компонентов. Режим предназначен для получения полной локальной копии серверной области обновления Dr.Web ; этот режим нельзя использовать для обновления антивируса, установленного на компьютере.
/UVB	Обновлять только антивирусные базы и антивирусное ядро drweb32.dll (отменяет действие ключа /UA, если он задан).
/UPM: <режим>	Режим использования прокси-сервера, может принимать следующие значения: • direct – не использовать прокси-сервер; • ieproxy – использовать системные настройки; • userproxy – использовать настройки, задаваемые пользователем (ключи /PURL, /PUSER и /PPASS).
/URM: <режим>	Режим перезагрузки после обновления; может принимать следующие значения: • prompt – по окончании сеанса обновления, в случае необходимости перезагрузки, спросить пользователя; • noprompt – в случае необходимости, перезагружаться, не спрашивая пользователя; • force – перезагружать принудительно всегда (независимо от того, требуется перезагрузка или нет); • disable – запретить перезагрузку.



Приложение Б. Настройки антивирусного сканирования Microsoft Exchange Server

Настройки антивирусного сканирования на основе VSAPI осуществляются с помощью набора ключей реестра и могут быть разделены на следующие типы:

1. Общие настройки

Общие настройки используются по умолчанию для всех почтовых хранилищ на сервере.

Сканирование при доступе

Ключ реестра:

```
[ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\MSExchangeIS\VirusScan]

"Enabled"=dword: 00000001
```

Данная настройка обеспечивает включение антивирусной проверки для всех почтовых хранилищ. Сканирование будет осуществляться всякий раз при обращении клиента к письму.

Фоновое сканирование

Ключ реестра:

```
[ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\MSExchangeIS\VirusScan]

"BackgroundScanning"=dword: 00000001
```



Данная настройка отвечает за включение фоновое сканирования. Фоновое сканирование подразумевает создание отдельного потока (thread), в котором происходит сканирование всех писем для данного почтового хранилища. Включение фоновое сканирования может отрицательно сказаться на производительности почтового сервера.

Упреждающее сканирование

Ключ реестра:

```
[ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\MSExchangeIS\VirusScan]

"ProactiveScanning"=dword: 00000001
```

Данная настройка включает упреждающее сканирование. В этом случае происходит проверка всех писем сразу после того, как они попадают в данное почтовое хранилище. При этом письма с неизменными штампами времени (TimeStamp), прошедшие упреждающее сканирование, не проверяются повторно при поступлении запроса письма от клиента.

Отключение проверки исходящих сообщений

Ключ реестра:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\S
ervices\MSExchangeIS\VirusScan

"TransportExclusion"=reg_dword: 00000000
```

Данная настройка позволяет отключить/включить (при выборе значения 1 или 0 соответственно) проверку на наличие вредоносных программ исходящих сообщений при их поступлении в транспортную систему из почтового хранилища. По умолчанию такая проверка включена.



Ограничение числа потоков для интерфейса антивирусного сканирования

Число потоков для интерфейса антивирусного сканирования VSAPI 2.6 определяется по умолчанию настройками Exchange Server, однако, его можно отрегулировать вручную путем создания переменной ScanningThreads в указанном ниже разделе реестра.

Ключ реестра:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIS\VirusScan
```

```
"ScanningThreads"=reg_dword
```

Данный параметр определяет максимальное число потоков, создаваемых для сканирования. Изменение данного параметра влияет на сканирование при доступе и упреждающее сканирование, но не влияет на фоновое сканирование, для которого всегда используется один поток на базу данных.

По умолчанию значение данной переменной считается равным $2 * \text{<количество процессоров>} + 1$.

2. Настройки базы данных

С помощью настроек данного типа можно задать параметры сканирования для каждой почтовой базы данных, имеющейся на почтовом сервере. Настройки записываются в реестр по следующему пути:

```
[ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\<ID Base>],
```

где <Server-Name> – имя сервера, <ID Base> – идентификатор почтовой базы, например, Private-ae39732e-fb7f-426d-98a0-298f3f014c77.



Параметры:

- "VirusScanEnabled"=dword: 00000001 – включение антивирусного сканирования для указанной базы данных;
- "VirusScanBackgroundScanning"=dword: 00000001 – включение фонового сканирования для указанной базы данных;
- "VirusScanProactiveScanning"=dword: 00000001 – включение упреждающего сканирования для указанной базы данных.

3. Сканирование транспорта SMTP



Настройки сканирования транспорта доступны только для сервера Exchange версии 2000/2003.

Ключ реестра:

```
[ HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\TransportAVAPI\]
```

```
"Enabled"=dword: 00000001
```

Транспортное сканирование по умолчанию выключено. Вы можете включить его на последнем шаге [установки](#) программы. В результате первое антивирусное сканирование письма будет выполнено на SMTP-событие OnSubmission постановки в очередь обработки сообщений, т.е. на уровне транспорта. Повторное сканирование будет произведено уже на уровне хранилища информации Exchange при запросе письма клиентом.



Приложение В. Работа в режиме централизованной защиты

Dr.Web для Microsoft Exchange Server может функционировать в сети, контролируемой **Центром Управления Dr.Web**. Организация централизованной антивирусной защиты позволяет автоматизировать и упростить настройку и управление информационной безопасностью компьютеров, объединенных в единую логическую структуру (например, компьютеры одной компании, расположенные как внутри локальной сети, так и вне ее). Защищаемые компьютеры объединяются в единую *антивирусную сеть*, безопасность которой контролируется и управляется администраторами с центрального сервера (**Центра Управления Dr.Web**). Подключение к системам централизованной защиты позволяет получить гарантированно высокий уровень защиты компьютера при минимальных усилиях со стороны конечных пользователей.

Взаимодействие компонентов антивирусной сети

Решения компании **«Доктор Веб»** по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру ([рис. 32](#)).

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз безопасности и спама *локальными антивирусными компонентами* (клиентами; в данном случае – **Dr.Web для Microsoft Exchange Server**), которые обеспечивают антивирусную защиту и упрощают соединение с сервером централизованной защиты.

Обновление и конфигурация локальных компонентов производится через *центральный сервер*. Весь поток команд, данных и статистической информации в антивирусной сети также проходит через сервер централизованной защиты. Объем трафика между защищенными компьютерами и антивирусным сервером может быть весьма значительным, поэтому предусматривается



возможность его сжатия. Использование шифрования при передаче данных позволяет избежать разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищенные компьютеры.



Рисунок 32. Логическая структура антивирусной сети.



Все необходимые обновления на сервер централизованной защиты загружаются с сервера **Всемирной системы обновлений Dr.Web**.

Изменения в конфигурации локальных антивирусных компонентов и передача команд осуществляется антивирусным сервером по указанию *администраторов антивирусной сети*. Администраторы управляют конфигурацией центрального сервера и формированием антивирусной сети (в частности, подтверждают правомерность подключения локальной станции к сети), а также при необходимости задают настройки работы конкретных локальных антивирусных компонентов.

Работа Dr.Web для Microsoft Exchange Server в режиме централизованной защиты

Для работы **Dr.Web для Microsoft Exchange Server** в режиме централизованной защиты необходимо, чтобы в операционной системе был установлен и корректно работал **Dr.Web Agent** версии 6.



Dr.Web для Microsoft Exchange Server версии 6.00.1 не совместим с версиями **Dr.Web Agent**, отличными от 6.

Для **Dr.Web для Microsoft Exchange Server** реализованы следующие возможности работы в режиме централизованной защиты:

- отправка статистики работы программы **Dr.Web для Microsoft Exchange Server**. Статистика работы отображается в таблицах **Статистика** и **Суммарная статистика Центра Управления Dr.Web**;
- отправка оповещений об обнаружении вирусов и предпринятых действиях. Эти события отображаются в таблице **Инфекции Центра Управления Dr.Web**;



- обновление антивирусных баз и антивирусного ядра из репозитория **Центра Управления Dr.Web**. Это позволяет отключить стандартный модуль обновления **Dr.Web Updater**, запускаемый по расписанию. В этом случае обновление компонентов будет выполняться согласно расписанию **Центра Управления Dr.Web** и из его репозитория;
- использование лицензионного ключевого файла программы **Dr.Web для Microsoft Exchange Server**, зарегистрированного для данной локальной станции в антивирусной сети. При установке **Dr.Web для Microsoft Exchange Server** лицензионный ключ будет получен агентом **Dr.Web Agent**.



Приложение Г. Техническая поддержка

Страница службы технической поддержки **«Доктор Веб»** находится по адресу <http://support.drweb.com/>.

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу <http://download.drweb.com/>;
- прочитать раздел часто задаваемых вопросов по адресу <http://support.drweb.com/>;
- попытаться найти ответ в базе знаний Dr.Web по адресу <http://wiki.drweb.com/>;
- посетить форумы Dr.Web по адресу <http://forum.drweb.com/>.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела <http://support.drweb.com/>.

Найти ближайшее к вам представительство **«Доктор Веб»** и всю контактную информацию, необходимую пользователю, вы можете по адресу <http://company.drweb.com/contacts/moscow>.



Предметный Указатель

D

Dr.Web для Microsoft Exchange Server
VSAPI 16
администрирование 36
введение 9
веб-консоль администратора 34
консоль администратора 32
назначение 9
принципы работы 20
приступая к работе 32
проверяемые объекты 11
регистрация событий 80
серверные роли 16
системные требования 26
статистика работы 67
техническая поддержка 98
транспортные агенты 16
удаление 25, 31
установка 25, 28
функции 9
централизованная защита 94

E

event log 80

V

VSAPI 16
ключи реестра 90
настройка 90

A

агенты транспорта 16, 19
администрирование 36
антиспам
лицензия 50
настройка 50

Б

белый список 75

В

веб-консоль администратора
дерево веб-консоли 34
запуск 34
область сведений 34
вирусные события
журнал событий 23
мониторинг 23
отчеты 23
статистика 23, 67
уведомления 23

Г

группы 36, 58
группы AD 60
создание 58
типы 60
формирование 60



Предметный Указатель

Д

диагностика 83, 85, 86

Ж

журнал Dr.Web для Microsoft Exchange Server 81, 82

журнал отладки 82

журнал программы установки 81

журнал событий 23, 41

журнал отладки 82

журнал программы установки 81

операционной системы 80

К

карантин 23, 64

ключевой файл

действительность 12

обновление 15

поддержка антиспама 50

получение 13

консоль администратора

дерево консоли 32

запуск 32

область сведений 32

Л

лицензия

антиспам 50

действительность 12

ключевой файл 12

обновление 15

получение 13

М

модуль обновления 79, 87

Н

настройка

VSAPI 90

антиспама 50

протокола уведомлений 75

сканирования 46

сопроводительного текста 56

учетной записи сервиса 75

фильтрации 53

начало работы 32

О

обновление

вирусные базы 79

диагностика 84

лицензии 15

модуль обновления 84

параметры командной строки 87

общие настройки

протокол уведомлений 75

учетная запись сервиса 75

черные/белые списки 75

отчеты 23



Предметный Указатель

отчеты 23

расписание 70

типы 70

П

получение ключевого файла 13

почтовые уведомления 23

правила фильтрации 21, 53

проверка

детектирования вирусов 85

детектирования спама 86

модуля обновления 84

на вирусы 21

на спам 21, 50

работоспособности 83

установки 83

этапы 21

проверяемые объекты 11

программа установки 28

регистрация событий 81

просмотр статистики 67

протокол уведомлений 75

профили 36

антиспам 50

настройка 37

приоритет 40

сканирование 46

создание 37

сопроводительный текст 56

уведомления 41

фильтрация 53

Р

регистрация событий 80

журнал операционной системы 80

журнал отладки 82

журнал программы установки 81

режим работы 94

роли сервера 16, 18

С

серверные роли 16, 18

системные требования 26

сканирование

настройка 46

по запросу 16

упреждающее 16

фоновое 16

сканирование по запросу 16

события

мониторинг 23

статистика 67

сокращения 7

сопроводительный текст 56

статистика 23

просмотр 67

события 67



Предметный Указатель

Т

- тестовое письмо 86
- тестовый файл EICAR 85
- техническая поддержка 98
- транспортные агенты 16, 19
- требования 26

У

- уведомления
 - протокол 75
- уведомления по почте 23, 41
- удаление Dr.Web для Microsoft Exchange Server 25, 31
- управление
 - группами 58
 - карантином 64
 - отчетами 70
 - профилями 37
 - списками 75
- упреждающее сканирование 16
- условные обозначения 7
- установка Dr.Web для Microsoft Exchange Server 25, 28
 - проверка 83
- системные требования 26
- учетная запись 75

Ф

- фильтрация
 - настройка 53

- правила 21, 53

- фоновое сканирование 16

Ц

- централизованная защита 94

Ч

- черный список 75

