Dr.WEB®
для IBM Lotus Domino

Защити созданное

Руководство администратора

Dr.Web для IBM Lotus Domino для Linux
Версия 6.00.2
Руководство администратора
24.04.2013

"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 6

Глава 1. Введение 8

- **Назначение Dr.Web для IBM Lotus Domino** 8
- **Проверяемые объекты** 10
- **Лицензионный ключевой файл** 11

Глава 2. Установка и удаление 13

- **Системные требования** 16
- **Установка Dr.Web для IBM Lotus Domino** 18
  - Дополнительные сведения об установке 21
  - Установка на несколько серверов 21
  - Действия после установки 22
- **Удаление Dr.Web для IBM Lotus Domino** 27
  - Действия после удаления 29

Глава 3. Приступая к работе 31

- **Проверка работоспособности** 31
  - Основные файлы и директории, создаваемые при установке 32
  - Изменения в настройках сервера Lotus Domino 34
  - Запуск сервера Lotus Domino 35
  - Проверка детектирования вирусов 36
- **Компоненты программы** 37
- **Запуск Консоли администратора** 39
- **Получение справки** 42

Глава 4. Администрирование 43

Группы и профили 43

Создание и настройка профилей 44

Настройка уведомлений 45

Настройка Монитора 47

Настройка Антиспама 49

Управление группами клиентов 52

Проверка баз данных Lotus Notes 53

Управление Карантином 56

Просмотр статистики 60

Управление отчетами 62

Ведение Журнала Событий 65

Настройка фильтров баз данных и электронных адресов 67

Фильтр баз данных 68

Черный и белый списки электронных адресов 70

Обновление вирусных баз 71

Экспорт/импорт конфигураций 72

Приложения 74

Приложение А. Работа в режиме централизованной защиты 74

Приложение Б. Техническая поддержка 79

Условные обозначения и сокращения

В зависимости от контекста, **Dr.Web** может означать как название компании – **Доктор Веб**, так и название продукта – **Dr.Web для IBM Lotus Domino**.

В руководстве используются следующие условные обозначения:

Обозначение	Описание
Жирный	Названия кнопок и других элементов графического интерфейса пользователя (GUI)
Зеленый и жирный	Название продуктов **Dr.Web** и их компонентов
Зеленый и подчеркнутый	Гиперссылки на разделы и веб-страницы
`Моноширинный`	Примеры программного кода, вводимый пользователем и выводимый программой текст
Курсив	Указатель места заполнения, в котором пользователю необходимо ввести некоторую информацию, такую как значение параметра командной строки. К тому же, он может означать термин в позиции определения или просто новый термин.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры
Знак плюс ('+')	Комбинация клавиш. Например, ALT+F1 означает, что нужно нажать клавишу F1, зажимая при этом клавишу ALT.
Восклицательный знак	Предупреждения о возможных ошибках или другие важные замечания

В руководстве используются следующие сокращения:

- ОС - операционная система;
- ПО - программное обеспечение;
- ACL - Access Control List (список контроля доступа);
- 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);
- NSD - Notes System Diagnostics (диагностика системы Lotus Notes);
- NSF - Notes Storage Facility (тип файлов баз данных, используемых в Lotus Notes и Lotus Domino);
- RAM - Random Access Memory (оперативная память);
- SMTP - Simple Mail Transfer Protocol (простой протокол пересылки почты);
- UNC - Universal Naming Convention (универсальное соглашение об именовании);
- URL - Uniform Resource Locator (унифицированный указатель ресурса);
- VDB - virus databases (тип файлов, содержащих вирусные базы);
- VGA - Video Graphics Array (логическая матрица видеографики).

Глава 1. Введение

Благодарим вас за приобретение **Dr.Web для IBM Lotus Domino**. Программа предоставляет надежную защиту компьютеров и информации внутри корпоративной сети от угроз, которые распространяются по электронной почте, используя самые современные технологии.

Данное руководство призвано помочь администраторам крупных корпоративных сетей при установке, настройке и управлении программным продуктом **Dr.Web для IBM Lotus Domino**.

Назначение Dr.Web для IBM Lotus Domino

Dr.Web для IBM Lotus Domino – это дополнительный антивирусный модуль, созданный с целью защитить корпоративную почтовую систему, построенную на основе сервера Lotus Domino, от вирусов и спама.

Структура **Dr.Web для IBM Lotus Domino**, применение непревзойденных методов проверки и возможность полностью управлять процессом сканирования - все это обеспечивает высокую скорость проверки и помогает значительно экономить вычислительные ресурсы системы.

Данный антивирусный модуль позволяет проверять электронные письма и документы, хранящиеся в NSF-базах сервера Lotus Domino, «на лету» (в режиме реального времени) и по расписанию. **Dr.Web для IBM Lotus Domino** может изолировать инфицированные и подозрительные документы, перемещая их в **Карантин**. Доступ к списку объектов, находящихся в **Карантине**, а так же ко всем настройкам модуля, осуществляется через **Консоль администратора** - удобный GUI, работа с которым осуществляется либо посредством клиента Lotus Notes, либо через веб-браузер (см. Запуск Консоли администратора). Процесс

обновления вирусных баз осуществляется по запросу пользователя или согласно расписанию при помощи **Automatic Updating Utility**.

Dr.Web для IBM Lotus Domino может выполнять следующие функции:

- проверка всех входящих и исходящих сообщений в режиме реального времени;
- проверка документов в выбранных NSF-базах по расписанию;
- проверка документов при работе с ними;
- проверка трафика репликации по расписанию;
- проверка трафика кластерной репликации;
- изоляция инфицированных и подозрительных объектов в **Карантине**;
- фильтрация входящего спама по протоколу SMTP, а также создание белых и черных списков электронных адресов;
- распределение пользователей по группам;
- отправка уведомлений о вирусных событиях и ведение журнала этих событий;
- рассылка отчетов о вирусной активности и спаме;
- сбор статистики о работе;
- автоматическое обновление вирусных баз и компонентов программы.

Dr.Web для IBM Lotus Domino использует вирусные базы, которые постоянно обновляются и дополняются новыми сигнатурами, что позволяет обеспечить защиту на самом современном уровне. Помимо этого, используется эвристический анализатор.

Dr.Web для IBM Lotus Domino не поддерживает использование технологии DB2 Universal Database (DB2 UDB).

Проверяемые объекты

Dr.Web для IBM Lotus Domino проверяет следующие объекты:

- файлы, вложенные в письма;
- файлы, вложенные в документы баз данных;
- OLE объекты.

Dr.Web для IBM Lotus Domino не проверяет:

- зашифрованные письма;
- файлы, созданные в операционных системах OS/2 и Mac OS;
- локальные реплики баз данных, размещенные на компьютерах пользователей.

Лицензионный ключевой файл

Права пользователя на использование **Dr.Web для IBM Lotus Domino** регулируются при помощи специального файла, называемого *ключевым файлом.*

В ключевом файле содержится, в частности, следующая информация:

- перечень компонентов, которые разрешено использовать данному пользователю (например, наличие **Антиспама** в версии «Антивирус + Антиспам»);
- период, в течение которого разрешено использование антивируса;
- другие ограничения (в частности, количество пользователей, которые будут использовать антивирус).

Ключевой файл имеет расширение **.key**, и его необходимо приобрести до установки **Dr.Web для IBM Lotus Domino**, т.к. во время установки нужно будет указать путь к ключевому файлу.

Для целей ознакомления с антивирусом можно запросить демонстрационный ключевой файл. Для этого необходимо заполнить анкету на официальном сайте «Доктор Веб» (http://download.drweb.com/demoreq/?pid=82). Демонстрационный ключевой файл обеспечивает полную функциональность основных антивирусных компонентов, но имеет ограниченный срок действия.

Чтобы купить лицензионный ключевой файл, воспользуйтесь услугами интернет-магазина «Доктор Веб».

Ключевой файл поставляется в виде файла с расширением **.key** или в виде ZIP-архива, содержащего этот файл.

Параметры ключевого файла, регулирующие права пользователя, установлены в соответствии с Пользовательским договором. В этот же файл заносится информация о пользователе и продавце антивируса.

Ключевой файл защищен от редактирования. Редактирование файла делает его недействительным, поэтому не следует открывать ключевой файл в текстовых редакторах во избежание его случайной порчи.

Для продолжения работы **Dr.Web для IBM Lotus Domino** после истечения срока пользования ключевым файлом необходимо получить новый ключевой файл, заменить им истекший и перезапустить сервер Lotus Domino.

Глава 2. Установка и удаление

Dr.Web для IBM Lotus Domino поставляется в виде самораспаковывающегося архива **drweb-domino-600-linux-x86.run**.

Рекомендуется использовать только файлы на фирменных дисках **«Доктор Веб»** или загруженные из раздела загрузок веб-сайта компании.

В архиве содержатся следующие пакеты, которые автоматически устанавливаются после распаковки:

Название	Описание
drweb-common	Содержит: • основной конфигурационный файл **drweb32.ini** • библиотеки • файлы документации • структуру директорий В ходе установки данного пакета создаются: • пользователь drweb • группа **drweb**
drweb-bases	Содержит: • антивирусное ядро (Scan Engine) • вирусные базы (VDB) Для установки требуется пакет drweb-common.
drweb-libvaderetro	Содержит библиотеку антиспама **libvaderetro.so**
drweb-updater	Содержит модуль обновления антивирусного ядра, вирусных баз и библиотеки антиспама. Для установки требуется пакет drweb-common.

Название	Описание
drweb-daemon	Содержит исполняемые файлы **Dr.Web Daemon** и документацию к нему. Для установки требуется пакет drweb-bases.
drweb-scanner	Содержит исполняемые файлы консольного сканера **Dr.Web Scanner** и документацию к нему. Для установки требуется пакет drweb-bases.
drweb-lotus-plugin7	Содержит: • бинарные файлы • конфигурационные файлы • скрипт для финальной настройки • init-скрипты
drweb-lotus-plugin8	Содержит: • бинарные файлы • конфигурационные файлы • скрипт для финальной настройки • init-скрипты
drweb-lotus-plugin-templates-en	Содержит английские шаблоны служебных баз данных. Несовместим с drweb-lotus-plugin-templates-ru.
drweb-lotus-plugin-templates-ru	Содержит русские шаблоны служебных баз данных. Несовместим с drweb-lotus-plugin-templates-en.
drweb-libs	Содержит библиотеки, общие для всех компонентов продукта.
drweb-epm6.0.0-libs	Содержит библиотеки для графических инсталлятора и деинсталлятора. Для установки требует пакет drweb-libs.
drweb-epm6.0.0-uninst	Содержит файлы графического деинсталлятора. Для установки требует пакет drweb-epm6.0.0-libs.

Название	Описание
drweb-agent	Содержит исполняемые файлы **Dr.Web Agent**, необходимые библиотеки и документацию к нему. Для установки требует пакеты drweb-boost144 и drweb-common.
drweb-boost144	Содержит библиотеки, которые использует **Dr.Web Agent**. Для установки требует пакет drweb-libs.
drweb-monitor	Содержит исполняемые файлы **Dr.Web Monitor**, необходимые библиотеки и документацию к нему. Для установки требует пакеты drweb-boost144 и drweb-common.

Перед установкой **Dr.Web для IBM Lotus Domino** тщательно проанализируйте состав и конфигурацию среды Lotus Domino в вашей сети и выберите сервер, который будет служить центром ее защиты от вирусов и спама.

Для установки и удаления **Dr.Web для IBM Lotus Domino** пользователь должен обладать правами "суперпользователя" (root) или иметь возможность выполнять действия, используя команду "sudo", на том компьютере, где установлен сервер Lotus Domino.

Dr.Web для IBM Lotus Domino несовместим с другими антивирусными программами. Установка двух антивирусов на один компьютер может привести к ошибкам в системе и потере важных данных. Если на компьютере уже установлена какая-либо версия **Dr.Web для IBM Lotus Domino** или другой антивирус, то его необходимо удалить, используя установочный файл или стандартные средства ОС (см. Удаление Dr.Web для IBM Lotus Domino).

Системные требования

Данный раздел посвящен системным требованиям, необходимым для установки и работы **Dr.Web для IBM Lotus Domino** на вашем компьютере.

Аппаратные требования:

Характеристика	Требование
CPU	Pentium 133 или более мощный; совместимый с системой команд i80386
RAM	64 МБ или больше
Свободное место на диске	90 МБ или больше
Монитор	VGA-совместимый монитор, желательно способный отображать как минимум 1280 x 1024 пикселов с 256 цветами

Требования к ОС и программному обеспечению:

Характеристика	Требование
ОС	32-битные: • Red Hat Enterprise Linux (RHEL) 4, 5 и 6 версии • Novell SuSE Linux Enterprise Server (SLES) 9, 10 и 11 версии
ПО Lotus	Lotus Domino 7.x для Linux Lotus Domino 8.x для Linux Lotus Notes 6.5 (или более поздний) для Windows
Прочее	Для работы продукта (в частности, антивирусного демона drwebd) необходимо отключить систему Security-Enhanced Linux.

Dr.Web для IBM Lotus Domino не поддерживает 64-битные версии IBM Lotus Domino.

Доктор Веб не гарантирует корректную работу **Dr.Web для IBM Lotus Domino** на альфа-, бета- и других некоммерческих версиях сервера Lotus Domino.

Установка Dr.Web для IBM Lotus Domino

Перед установкой настоятельно рекомендуется:

- установить все критические обновления, выпущенные для ОС, которая используется на компьютере
- проверить файловую систему при помощи стандартных средств и исправить обнаруженные ошибки

Чтобы установить Dr.Web для IBM Lotus Domino с помощью графической программы установки:

1. Завершите работу сервера Lotus Domino.
2. Удалите предыдущие версии антивирусного модуля и любые другие антивирусы для IBM Lotus Domino, установленные на компьютере.
3. Разрешите исполнение архива **drweb-domino-600-linux-x86.run**. Например, вы можете воспользоваться следующей командой:
   ```
   # chmod +x drweb-domino-600-linux-x86.run
   ```
4. Запустите файл на исполнение следующей командой:
   ```
   # ./drweb-domino-600-linux-x86.run
   ```
5. Во время распаковки будет создана директория **drweb-lotus-6.0.[release].[path]-[build]_linux** с набором файлов внутри, после чего запуститься графическая программа установки.
6. Выберите установочный пакет в зависимости от версии сервера IBM Lotus Domino. Нажмите кнопку **Next**.
7. На следующем шаге ознакомьтесь с лицензионным соглашением (вы можете выбрать язык отображения лицензионного соглашения в списке **Languages**). Для продолжения установки его необходимо принять. Нажмите кнопку **Next**.
8. Начнется установка программы **Dr.Web для IBM Lotus Domino**.
9. После успешной установки будет выведено окно с

сообщением **Installation complete**. Чтобы запустить скрипт для настройки программы, установите флажок **Run interactive postinstall script** и нажмите кнопку **Next**. В результате работы скрипта будут выполнены следующие действия:

- лицензионный ключ программы будет скопирован в директорию /opt/drweb;
- путь к ключевому файлу будет записан в конфигурационных файлах модуля **Dr.Web Agent** и демона **drwebd**;
- для **Dr.Web Monitor**, а также демонов **drwebd** и **drweb-lotusd** будет настроен автоматический запуск;
- будет осуществлен запуск **Dr.Web Monitor** и демонов **drwebd** и **drweb-lotusd**.

10. Нажмите **Close**, чтобы завершить работу программы установки.

Чтобы установить Dr.Web для IBM Lotus Domino из консоли (не запуская графическую программу установки):

1. Завершите работу сервера Lotus Domino.
2. Удалите предыдущие версии антивирусного модуля и любые другие антивирусы для IBM Lotus Domino, установленные на компьютере.
3. Разрешите исполнение архива **drweb-domino-600-linux-x86.run**. Например, вы можете воспользоваться следующей командой:
   ```
   # chmod +x drweb-domino-600-linux-x86.run
   ```
4. Во время распаковки будет создана директория drweblotus-6.0.[release].[path]-[build]_linux с набором файлов.
5. Выберите установочный пакет в зависимости от версии сервера IBM Lotus Domino.
6. Откроется лицензионное соглашение. Для продолжения установки его необходимо принять.
7. Начнется установка программы **Dr.Web для IBM Lotus Domino**.
8. Далее вам будет предложено настроить основные компоненты программы. В случае вашего согласия будут выполнены следующие действия:
   - лицензионный ключ программы будет скопирован в директорию /opt/drweb;
   - путь к ключевому файлу будет записан в конфигурационные файлы **Dr.Web Agent** и демона drwebd;
   - для **Dr.Web Monitor**, а также демонов drwebd и drweb-lotusd будет настроен автоматический запуск;
   - будет осуществлен запуск **Dr.Web Monitor** и демонов drwebd и drweb-lotusd.
9. По окончании установки будет выведено сообщение о том, что установка завершилась успешно.

Дополнительные сведения об установке

Во время установки компонентов **Dr.Web для IBM Lotus Domino** происходит следующее:

- В директорию **/etc/drweb/software/conf** записываются оригиналы конфигурационных файлов дистрибутива (***.N**).
- Конфигурационные файлы устанавливаются в соответствующие директории системы.
- Устанавливаются остальные файлы, причем, если файл с таким именем уже существует (например, случайно остался после удаления пакетов других типов), то он заменяется новым, а копия старого сохраняется как **[имя_файла].O**.

Установка на несколько серверов

При установке **Dr.Web для IBM Lotus Domino** на несколько серверов в одном Domino-домене, после каждой установки необходимо реплицировать адресную книгу сервера (база данных **names.nsf**, которая находится в папке **Data** сервера Lotus Domino) на все остальные сервера Lotus Domino в этом домене. Если этого не делать, то возможно появление дубликатов группы **DrWeb Admin** в адресной книге, что приведет к невозможности отправки служебных уведомлений от антивируса администратору.

В случае, если это уже произошло:

1. Перенесите пользователей из одной группы **DrWeb Admin** в другую простым редактированием документа группы в базе данных **names.nsf**.
2. Удалите пустой дубликат группы **Drweb Admin**.
3. Реплицируйте базу данных **names.nsf** на все сервера Lotus Domino в домене (см. документацию IBM Lotus Domino: http://www.ibm.com/developerworks/lotus/documentation/domino/).

Действия после установки

Настройка взаимодействия между компонентами

Для настройки взаимодействия используется скрипт **drweb-lotus-install.sh**. Он использует настройки по умолчанию, которые может быть необходимо изменить:

- В файле **/etc/drweb/drweblotus-setup.conf** вы можете задать путь к серверу Lotus Domino, имя пользователя и группы запуска сервера, используемые сокеты для демонов **drwebd** и **drweblotusd**, а также некоторые другие параметры.
- Если во время установки **Dr.Web для IBM Lotus Domino** не был установлен флажок **Run interactive postinstall script**, в файлах **/etc/drweb/drwebd.enable** и **/etc/drweb/drweb-lotusd.enable** необходимо установить параметр `ENABLE=1`, чтобы разрешить запуск демонов (**drwebd** и **drweblotusd**).

После того, как вы убедились, что все настройки заданы верно, выполните скрипт **/opt/drweb/scripts/lotus/drweb-lotus-install.sh**, который настроит взаимодействие сервера Lotus Domino с антивирусным модулем **Dr.Web**. Данный скрипт выполняет следующие действия:

- Создает необходимые базы NSF в директории **/local/notesdata/DrWeb**
- Создает необходимые символические ссылки на бинарные файлы антивирусного модуля **Dr.Web для IBM Lotus Domino**
- Добавляет необходимые параметры в файл **notes.ini** сервера Lotus Domino (см. Изменения в настройках сервера Lotus Domino)

Подписание служебных баз

До начала использования антивирусного модуля необходимо подписать новые базы сервера Lotus Domino, которые использует **Dr.Web для IBM Lotus Domino**. Если этого не сделать, то модуль не сможет автоматически генерировать отчеты и чистить карантин.

Чтобы подписать базы, сделайте следующее:

1. Убедитесь, что вы обладаете правами администратора сервера Lotus Domino.
2. Запустите сервер Lotus Domino.
3. Запустите клиент Domino Administrator.
4. Выберите пункт **Open Server** в меню **File** и укажите сервер, на котором установлен **Dr.Web для IBM Lotus Domino**.
5. В закладке **Files** выделите все базы **Dr.Web для IBM Lotus Domino**, находящиеся в подпапке **DrWeb** каталога **Data**. Это следующие базы: **DrWebAdmin.nsf, DrWebDesign.nsf, Quarantine.nsf**, **DrWebReports.nsf, DrWebHelp.nsf**, **DrWebLog.nsf, DrWebSpam.nsf**.
6. Нажмите правой кнопкой на выбранных базах и выберите пункт **Sign** (Подписать) либо нажмите кнопку **Sign** в меню **Tools** -> **Database** в правой части клиента Domino Administrator.
7. Выберите **Active Server's ID** в окне **Sign Database** и нажмите кнопку **OK**.

Настройка доступа к ключевому файлу

В случае, если во время установки **Dr.Web для IBM Lotus Domino** не был установлен флажок **Run interactive postinstall script**, для компонентов, которым требуется ключевой файл, необходимо указать путь к нему и разрешить доступ:

- После получения ключевого файла для антивируса **Dr.Web для IBM Lotus Domino** необходимо разрешить его чтение для той учетной записи, из-под которой запускается сервер Lotus Domino. После этого необходимо указать путь к ключевому файлу в качестве значения параметра **LicenseFile** в разделе **StandaloneMode** конфигурационного файла **/etc/drweb/agent.conf**.
- Если вы также получили ключевой файл для антивирусного демона (**drwebd**), необходимо разрешить его чтение пользователю **drweb**. После этого необходимо убедиться, что в файле настроек демона (**/etc/drweb/drweb32.ini**) указан полный путь к ключевому файлу в параметре **Key**, например: `Key=/opt/drweb/drweb32.key`.

Запуск демонов

Если во время установки **Dr.Web для IBM Lotus Domino** не был установлен флажок **Run interactive postinstall script** и, соответственно, не запускался скрипт настройки компонентов программы, необходимо запустить демоны **drwebd** и **drweblotusd**.

Чтобы запустить антивирусный демон drwebd:

- Выполните команду `service drwebd start`

В дальнейшем демон будет запускаться автоматически при загрузке ОС.

Чтобы запустить вспомогательный демон drweblotusd:

- Выполните команду `service drweb-lotusd start`

В дальнейшем демон будет запускаться автоматически при загрузке ОС.

Запуск и настройка компонента Dr.Web Monitor

Если во время установки **Dr.Web для IBM Lotus Domino** не был установлен флажок **Run interactive postinstall script** и, соответственно, не запускался скрипт настройки компонентов программы, необходимо настроить работу компонента **Dr.Web Monitor**. Для этого выполните следующие действия:

1. Откройте файл **/etc/drweb/drweb-monitor.enable** и установите значение параметра `ENABLE=1`.
2. Запустите компонент **Dr.Web Monitor** следующей командой:
   `/etc/init.d/drweb-monitor start`

   Убедитесь, что при загрузке не возникло ошибок.

Удаление Dr.Web для IBM Lotus Domino

При удалении **Dr.Web для IBM Lotus Domino** теряются все настройки отчетов и заданий на сканирование, все группы и профили, а также удаляется база карантина и инцидентов.

Чтобы удалить Dr.Web для IBM Lotus Domino при помощи графической программы удаления:

1. Завершите работу сервера Lotus Domino.
2. Запустите следующий скрипт: **/opt/drweb/scripts/lotus/drweb-lotus-remove.sh**
3. Перейдите в каталог **drweb-lotus-6.0.[release].[path]-[build]_linux**, который создается в директории, откуда был запущен установочный пакет **Dr.Web для IBM Lotus Domino**.
4. Выполните команду `# ./uninst`
5. Нажмите кнопку **Удалить**.
6. По завершении процесса удаления нажмите кнопку **Закрыть**.

Чтобы удалить Dr.Web для IBM Lotus Domino из консоли (не запуская графическую программу удаления):

1. Завершите работу сервера Lotus Domino.
2. Запустите следующий скрипт: **/opt/drweb/scripts/lotus/drweb-lotus-remove.sh**
3. Запустите по очереди все файлы удаления (***.remove**) установленных пакетов: `# /drweb-lotus-6.0.[release].[path]-[build]_linux/[`*имя_файла*`].remove`

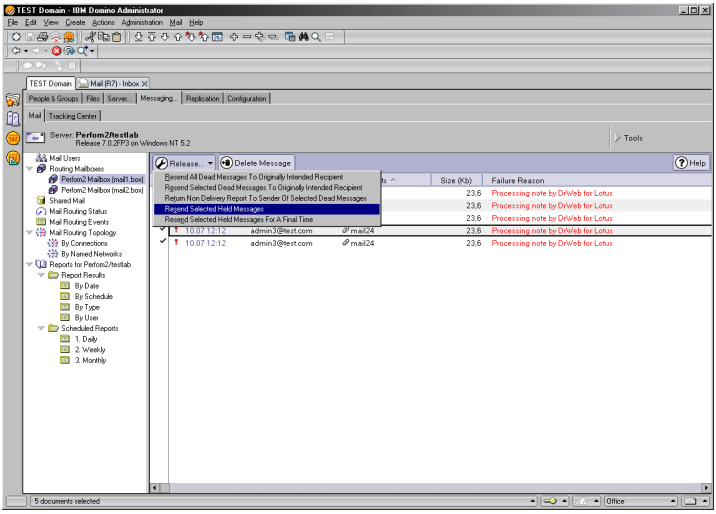
После удаления антивирусного модуля **Dr.Web для IBM Lotus Domino** необходимо вручную удалить группу **DrWeb Admin**.

Действия после удаления

После удаления **Dr.Web для IBM Lotus Domino** на сервере Lotus Domino могут остаться задержанные непроверенные электронные письма. Это происходит из-за того, что всем письмам присваивается статус **HOLD** перед тем, как они подвергаются проверке антивирусным модулем.

Чтобы доставить эти письма получателям:

1. Запустите сервер Lotus Domino.
2. Запустите клиент Domino Administrator.
3. Выберите пункт **Open Server** в меню **File** и выберите сервер, на котором был установлен **Dr.Web для IBM Lotus Domino**.
4. Откройте вкладку **Messaging** и найдите в почтовых ящиках (пункт **Routing Mailboxes** в меню в левой части вкладки) электронные письма с комментарием **Processing note by DrWeb for Lotus** в колонке **Failure Reason** (см. иллюстрацию ниже).



5. Выберите письма, задержанные **Dr.Web для IBM Lotus Domino** и нажмите кнопку **Release** над списком.
6. Нажмите правой кнопкой на выбранных письмах и выберите пункт **Resend Selected Held Messages**.

Освобожденные письма будут доставлены получателям и не будут проверены антивирусным модулем **Dr.Web для IBM Lotus Domino**, т.к. он уже удален.

Глава 3. Приступая к работе

В данной главе описано как проверить работоспособность антивирусного модуля и как запустить Консоль Администратора.

Проверка работоспособности

Перед запуском **Dr.Web для IBM Lotus Domino** необходимо убедиться, что антивирусный модуль установлен правильно и является полностью работоспособным. В данном разделе содержится вся необходимая информация, требующаяся для проверки работоспособности.

Основные файлы и директории, создаваемые при установке

Убедитесь, что все следующие директории были созданы во время установки **Dr.Web для IBM Lotus Domino** и содержат все необходимый файлы:

Директория	Имя файла	Описание
/opt/drweb	drwebd	Антивирусный демон.
	drweblotusd	Вспомогательный демон (антиспам, статистика и др.).
	update.pl	Скрипт обновления.
	drwebd.key	Ключевой файл антивирусного демона **drwebd**.
	drweb-agent	Файл модуля **Dr.Web Agent**.
	drweb-monitor	Файл модуля **Dr.Web Monitor**.
/opt/drweb/lotus	libdrwebmonitor.so	Библиотека с хуком.
	drwebmonitor	Бинарный исполняемый файл — монитор проверки почты (задача сервера).
	drwebscanner	Бинарный исполняемый файл — сканер для проверки баз NSF по расписанию (задача сервера).
	setup	Бинарный исполняемый файл для создания баз NSF из одноименных шаблонов NTF. Запускается во время установки, после - удаляется.
/opt/drweb/lotus/templates	*.ntf	Шаблоны баз, по которым создаются базы NSF.
/local/notesdata/DrWeb	DrWebAdmin.nsf	Консоль администратора.
	DrWebDesign.nsf	Служебная база данных.
	Quarantine.nsf	База данных карантина и инцидентов.

Директория	Имя файла	Описание
	DrWebReports.nsf	База данных отчетов.
	DrWebHelp.nsf	База встроенной справочной системы.
	DrWebLog.nsf	База журнала событий.
	DrWebSpam.nsf	База для хранения SPAM-сообщений.
/etc/drweb	drweblotusd.conf	Конфигурационный файл вспомогательного демона **drweblotusd**.
	agent.conf	Конфигурационный файл модуля **Dr.Web Agent**.
	monitor.conf	Конфигурационнный файл модуля **Dr.Web Monitor**.
/var/drweb/run	drweblotusd.pid	Файл, содержащий текущий идентификатор процесса для вспомогательного демона **drweblotusd**.
	drweb-agent.pid	Файл, содержащий текущий идентификатор процесса для демона drweb-agent.
	drweb-monitor.pid	Файл, содержащий текущий идентификатор процесса для модуля **Dr.Web Monitor**.
/var/drweb/lib	libvaderetro.so	Библиотека антиспама.

Изменения в настройках сервера Lotus Domino

Во время установки **Dr.Web для IBM Lotus Domino** в адресной книге (база данных **names.nsf**) сервера Lotus Domino автоматически создается группа **DrWeb Admin**. Эта группа указывается в *списке контроля доступа* (ACL) всех баз антивирусного модуля. В группу по умолчанию добавляется администратор сервера, указанный в файле **notes.ini** (параметр **Admin**). Он может добавлять других пользователей Lotus Domino в группу **DrWeb Admin**, чтобы они могли исполнять обязанности администратора **Dr.Web для IBM Lotus Domino**. Удаление этой группы приведет к проблемам с уведомлениями и доступом к базам данных антивирусного модуля.

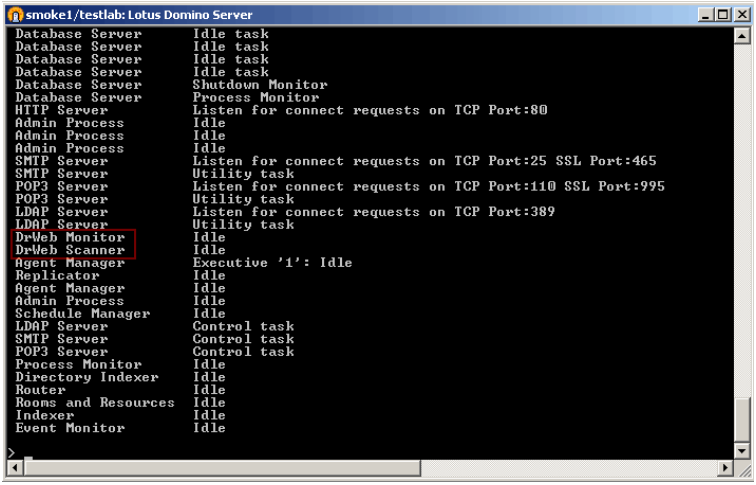
Помимо этого, в файл **notes.ini** вносятся следующие изменения:

- В параметр **EXTMGR_ADDINS** добавляется значение **drwebmonitor**.
- В параметр **ServerTasks** добавляются задачи монитора и сканера (**drwebmonitor** и **drwebscanner**).
- Добавляется параметр **DrWebBuild**, в котором указывается полный номер сборки.
- Добавляются параметры **DrWebSocket** и **DrWebVRSocket** в которых указывается UNIX-сокет, TCP-сокет или PID-файл для взаимодействия с антивирусным демоном **drwebd** (по умолчанию **pid:/var/drweb/run/drwebd.pid**) и вспомогательным демоном **drweblotusd** (по умолчанию **/var/drweb/lotus/.vrsocket**) соответственно.

Если вы не желаете автоматически загружать антивирусные компоненты при запуске сервера Lotus Domino, то необходимо удалить значение **drwebmonitor** в параметре **EXTMGR_ADDINS**, а также значения **drwebmonitor** и **drwebscanner** в параметре **ServerTasks**.

Запуск сервера Lotus Domino

Если установка **Dr.Web для IBM Lotus Domino** прошла успешно, то можно запустить сервер Lotus Domino. Чтобы убедиться, что задания **Монитор** и **Сканер** запущены, воспользуйтесь командой `sh task`. На иллюстрации внизу изображено командное окно сервера Lotus Domino с корректно отработавшей командой `sh task`.



Проверка детектирования вирусов

Для проверки конфигурации и способности **Dr.Web для IBM Lotus Domino** обнаруживать вирусы рекомендуется использовать тестовый файл EICAR (European Institute for Computer Antivirus Research). Файл, содержащий только текстовую строку длиной 68 или 70 байт, 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 (http://www.eicar.org) или создать его самостоятельно.

Чтобы создать тестовый файл EICAR:

- Создайте текстовый файл со следующей строкой:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$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:

```
Dr.Web для IBM Lotus Domino обнаружил что письмо инфицировано.

Дата: Wed Jul 02 17:43:32 2008

Отправитель: admin@test.com
Получатели: mail21@perf2.test.com
Тема письма: Тест 1
Вирусы: eicar.com ( EICAR Test File (NOT a Virus!) ) отправлен в карантин
```

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

Компоненты программы

Dr.Web для IBM Lotus Domino - это комплексный антивирусный продукт, состоящий из нескольких дополняющих друг друга компонентов, которые взаимодействуют между собой и обеспечивают высочайший уровень защиты. Работой этих компонентов можно управлять при помощи **Консоли администратора** (см. Запуск Консоли администратора).

Ниже приведен список этих компонентов с кратким описанием каждого:

- **Антивирусный демон** (**drwebd**) используется для осуществления антивирусной проверки.
- **Монитор** (бинарный исполняемый файл **drwebmonitor**) проверяет mail.box сервера Lotus Domino, т.е. все входящие и исходящие письма в режиме реального времени по мере того, как их обрабатывает сервер. Как только проверка письма завершается и оно признается безопасным, оно сразу отправляется пользователю. Если письмо содержит зараженный или подозрительный объект, то над ним производится соответствующее предустановленное действие.
- **Сканер** (бинарный исполняемый файл **drwebscanner**) позволяет периодически проверять документы в выбранных NSF базах. Он запускается по расписанию или вручную и, также как и **Монитор**, применяет предустановленные действия к зараженным и подозрительным объектам.
- **Вспомогательный демон** (**drweblotusd**) проверяет письма на спам и загружает обновленные библиотеки антиспама (**libvaderetro.so**). Используя специальные

алгоритмы, основанные на выявлении признаков спама в письмах, компонент с большой вероятностью определяет является ли письмо спамом и затем, в случае необходимости, добавляет к теме письма предустановленный префикс (по умолчанию - **[СПАМ]**).

- **Карантин** (**quarantine.nsf**) используется для изоляции зараженных и подозрительных объектов. Доступ к объектам, находящимся в карантине осуществляется из базы **Консоли администратора** (**DrWebAdmin.nsf**).
- **Модуль обновления** (скрипт **update.pl**), который входит в состав антивирусного пакета **Dr.Web для IBM Lotus Domino**, предназначен для автоматического обновления вирусных баз. Модуль загружает копии вирусных баз из сети Интернет либо из папки или сервера в локальной сети.
- Компонент **Статистика** (является частью базы **quarantine.nsf**) сохраняет информацию о типах проверенных объектов и произведенных над ними действиями. Вы можете просматривать данную информацию, чтобы следить за работой **Dr.Web для IBM Lotus Domino**.
- Компонент **Отчеты** (**DrWebReports.nsf**) предназначен для рассылки регулярных отчетов о работе **Dr.Web для IBM Lotus Domino** на указанные адреса и согласно определенным критериям.
- **Журнал событий** предоставляет администраторам серверов Lotus Domino возможность эффективно отслеживать события, связанные с работой **Dr.Web для IBM Lotus Domino** (например, обновление вирусных баз, обнаружение вируса, изменение настроек и др.). В базе данных **Журнала событий** (**DrWebLog.nsf**) может быть собрана информация с одного или нескольких серверов Lotus Domino, защищенных антивирусным модулем. Документы о событиях доставляются в базу **Журнала событий** с помощью почтовой системы сервера Lotus Domino

Параметры работы **Монитора** и **Антиспама** можно настроить для каждого профиля таким образом, чтобы удовлетворить потребностям каждого клиента или группы. Работа остальных компонентов настраивается для всего программного модуля.

Запуск Консоли администратора

Настройка работы **Dr.Web для IBM Lotus Domino** осуществляется посредством **Консоли администратора**. Консоль представляет собой графический интерфейс пользователя (GUI), который запускается в среде Lotus Notes или через любой из поддерживаемых веб-браузеров при помощи базы **DrWebAdmin.nsf**.

Для правильного отображения **Консоли администратора** рекомендуется установить разрешение экрана не менее 1280 на 1024 пикселов.

Для работы с веб-консолью на сервере Lotus Domino должна быть запущена задача HTTP-сервера.

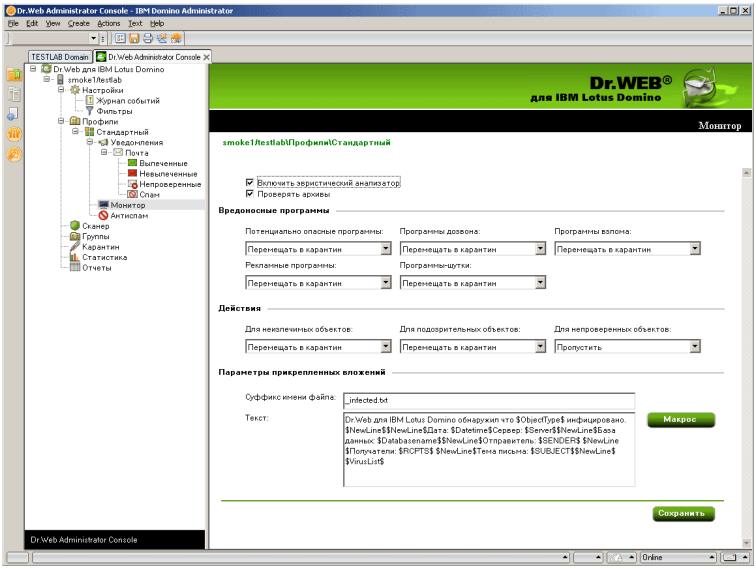
Чтобы запустить Консоль администратора в среде Lotus Notes:

1. Запустите сервер Lotus Domino.
2. Запустите приложение Lotus Notes.
3. Откройте меню **File**, выберите пункт **Database** и нажмите **Open**. Откроется окно **Open Database** (чтобы открыть это окно, вы также можете нажать комбинацию клавиш CTRL+O на клавиатуре).
4. Выберите сервер Lotus Domino, на котором установлен антивирусный модуль, из выпадающего списка в верхней части окна **Open Database**.
5. Выберите базу **Консоли администратора** (**DrWebAdmin.nsf**) в папке **DrWeb** и нажмите **Open**.

Чтобы запустить Консоль администратора в веб-браузере:

1. Запустите сервер Lotus Domino.
2. Запустите веб-браузер.
3. Перейдите по следующему адресу: http://domino.server/drweb/drwebAdmin.nsf
4. Введите имя и Интернет-пароль (*Internet password*) учетной записи администратора, указанного в группе **DrWeb Admin**.

Консоль администратора состоит из двух частей (см. иллюстрацию ниже). Слева находится иерархическое меню для навигации по разделам настройки программы. В правой части расположен фрейм с рабочей областью, в котором отображаются настраиваемые параметры для выбранного раздела. В верхней части фрейма с рабочей областью находится логотип **Dr.Web для IBM Lotus Domino** и название выбранного раздела.



Получение справки

В **Dr.Web for IBM Lotus Domino** реализована встроенная справочная система, которая устанавливается в виде отдельной базы **DrWebHelp.nsf** в директорию **/local/notesdata/DrWeb**. Откройте эту базу в клиенте Lotus Notes, чтобы получить доступ к основной части справочной системы.

Чтобы открыть определенный раздел справочной системы в зависимости от контекста (т.е. чтобы получить справку о том разделе **Консоли администратора**, который открыт в данный момент), нажмите клавишу F1 на клавиатуре.

Раздел **О Dr.Web для IBM Lotus Domino**, в котором содержится информация о версии **Dr.Web для IBM Lotus Domino**, можно открыть через верхний пункт в иерархическом меню **Консоли администратора** (см. иллюстрацию в разделе Запуск Консоли администратора). Здесь собрана информация о ключевом файле, номерах версий программных компонентов и о последнем обновлении вирусных баз. Эта информация необходима для анализа ошибок и сбоев при обращении в службу технической поддержки.

Глава 4. Администрирование

В данной главе описана структура **Dr.Web для IBM Lotus Domino** и выполнение административных задач, необходимых для создания максимально безопасной среды Lotus Domino.

Группы и профили

Для упрощения организации антивирусной защиты среды Lotus Domino, в **Dr.Web для IBM Lotus Domino** 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 Lotus Domino. Настройки профиля находятся в разделе иерархического меню **Профили**, который разделен на следующие подразделы:

- Уведомления - в данном разделе вы можете настроить уведомления, которые информируют администратора и других пользователей о различных событиях (например, об обнаружении зараженных или подозрительных сообщений и о попытках их лечения, о фильтрации сообщений и т.д.)
- Монитор - в данном разделе вы можете управлять работой вашего основного резидентного компонента для обнаружения вирусов
- Антиспам - в данном разделе вы можете настроить работу компонента **Антиспам** (настройки в разделе доступны только для версии "Антивирус + Антиспам", т.е. в том случае, если у вас есть соответствующий лицензионный ключевой файл (см. Лицензионный ключевой файл))

Более подробно о работе с профилями читайте в разделе Создание и настройка профилей.

Любой профиль можно присвоить группе клиентов. Эти группы формируются в разделе иерархического меню **Группы** (см. Управление группами клиентов).

Создание и настройка профилей

Профили определяют параметры антивирусного сканирования, фильтрации спама, действий, применяемых по отношению к обнаруженным объектам, а также рассылки уведомлений.

Во время установки **Dr.Web для IBM Lotus Domino** создается **Стандартный** профиль. Этот профиль останется активным для всех клиентов сервера Lotus Domino до тех пор, пока им не будет назначен другой профиль.

Стандартный профиль невозможно удалить. При создании нового профиля, его параметры принимают текущие значения параметров **Стандартного** профиля.

Чтобы создать новый профиль, сделайте следующее:

1. Выберите пункт **Профили** в иерархическом меню и нажмите кнопку **Создать** под списком профилей в основном фрейме справа.
2. Введите имя профиля и нажмите кнопку **ОК**. Новый профиль отобразится под пунктом **Профили** в иерархическом меню.

   Чтобы изменить имя профиля:

   - Выберите его в иерархическом меню, введите желаемое имя в поле ввода **Имя** и нажмите кнопку **Сохранить**.

Для имени профиля не допускается использование следующих символов: **! / \ | ; : " * ,**

3. Параметры нового профиля будут совпадать с параметрами **Стандартного** профиля.

   Чтобы изменить параметры профиля:

   - Выберите профиль в иерархическом меню и настройте параметры в соответствующих пунктах (Уведомления,

Монитор и Антиспам).

Настройка уведомлений

Уведомления используются для своевременного информирования администратора и других пользователей о различных событиях (об обнаружении инфицированных или подозрительных документов, о попытках их лечения, о фильтрации спама и т.д.).

Чтобы открыть фрейм с настройками уведомлений для профиля:

- Выберите этот профиль в иерархическом меню и нажмите на кнопку **Уведомления**.

По умолчанию все уведомления отключены.

Чтобы настроить почтовые уведомления:

1. Выберите раздел **Почта** в пункте **Уведомления** для определенного профиля и нажмите на том типе событий, для которых вы желаете настроить уведомления:
   - **Вылеченные** - если обнаруженный инфицированный объект удалось вылечить
   - **Невылеченные** - если обнаруженный инфицированный объект не удалось вылечить
   - **Непроверенные** - если сообщение не удалось проверить
   - **Спам** - если письмо признано спамом
2. Для каждого типа событий вы можете задать отдельные уведомления для администратора, получателя и отправителя письма. Для этого выберите соответствующую вкладку в верхней части основного (см. иллюстрацию ниже).

3. Чтобы включить отправку уведомлений для определенного

типа событий:

- Установите флажок **Посылать почтовые уведомления**.

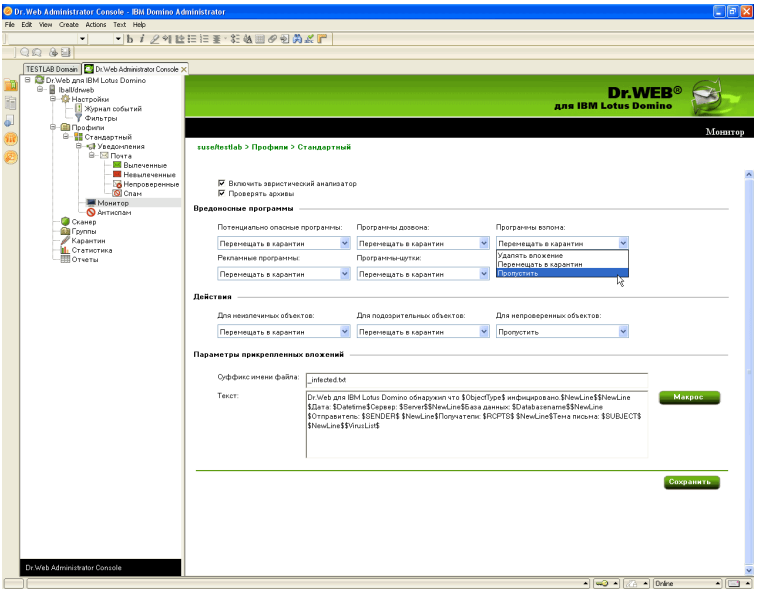
4. При необходимости отредактируйте шаблон почтового уведомления в соответствующих полях ввода. Вы можете добавить макросы в текст уведомления нажав кнопку Макрос и выбрав нужные из списка.
5. В поле ввода **Отправитель** вы можете указать отправителя выбранного типа уведомлений.
6. Получателей определенного типа уведомлений вы можете настроить только во вкладке **Администратор**. Вы можете добавить пользователей в данное поле ввода, нажав кнопку **Добавить** и выбрав их в окне **Select Addresses**.
7. Когда вы закончите редактировать параметры уведомлений, нажмите кнопку **Сохранить**.

Настройка Монитора

Монитор проверяет все входящие и исходящие письма в режиме реального времени по мере того, как их обрабатывает сервер Lotus Domino. Параметры его работы можно настроить для различных профилей с учетом требований определенных групп клиентов (см. Группы и профили).

Чтобы настроить параметры работы Монитора:

- Выберите профиль, для которого вы желаете настроить работу монитора и зайдите в раздел **Монитор**.



На иллюстрации сверху изображен фрейм **Монитор**.

По умолчанию эвристический анализатор и проверка архивов во вложениях включены, что обеспечивает высокий уровень защищенности за счет некоторого снижения производительности сервера. Чтобы отключить эти средства, снимите флажки **Включить эвристический анализатор** и **Проверять архивы**

в верхней части фрейма **Монитор**.

Настоятельно не рекомендуется отключать эвристический анализатор, т.к. это значительно снижает уровень защищенности сервера. В версии **Dr.Web для IBM Lotus Domino** для ОС Linux проверка архивов включена всегда, даже если снят соответствующий флажок.

В группе настроек **Вредоносные программы** вы можете выбрать действия для различных типов нежелательного ПО, а в группе настроек **Действия** - для неизлечимых, подозрительных и непроверенных объектов. Для этого воспользуйтесь соответствующими выпадающими списками:

- **Удалить вложение** - означает, что тело сообщения будет пропущено и доставлено получателю, а вложение заменено на текстовый файл с информацией о времени обнаружения, найденном вирусе и выполненном действии (доступно для неизлечимых, подозрительных объектов и вредоносных программ).
- **Поместить вложение в Карантин** - означает, что тело сообщения будет пропущено и доставлено получателю, а вложение будет отправлено в базу Карантина (см. Управление Карантином). Вместо вложения к сообщению прикрепляется текстовый файл с информацией о времени обнаружения, найденном вирусе и выполненном действии.
- **Пропустить** - означает, что сообщение вместе с вложением будет доставлено получателю и никаких действий к нему применено не будет (доступно для непроверенных объектов и вредоносных программ).

В группе настроек **Параметры вложений** вы можете изменить суффикс имени текстового файла, прикрепляемого к зараженному сообщению после того, как над ним производится какое-либо действие (т.е. имя файла будет состоять из исходного имени с указанным суффиксом на конце). В поле **Текст** вы можете, при необходимости, изменить содержимое прикрепляемого текстового файла.

Чтобы добавить макрос в шаблон текстового файла:

- Нажмите кнопку **Макрос** и выберите нужный из списка.

Когда вы закончите редактировать параметры работы **Монитора**, нажмите **Сохранить**.

Настройка Антиспама

Выявление спама осуществляется компонентом **Антиспам**, который анализирует содержимое письма и определяет, является ли оно спамом в зависимости от значения показателя, рассчитываемого по различным критериям. Спам-сообщению присваивается определенная категория, в зависимости от того, насколько вероятна принадлежность письма к спаму: *Спам*, *Возможно спам*, *Сомнительные письма*. Для каждой категории можно задать отдельные действия (см. описание настроек ниже).

Компонент **Антиспам** доступен только для версии «Антивирус + Антиспам». Если ваш ключевой файл поддерживает **Антиспам**, то фильтрация спама будет включена по умолчанию.

Если настройки в разделе **Антиспам** недоступны, то скорее всего ваш лицензионный ключевой файл не поддерживает **Антиспам** (см. Лицензионный ключевой файл). Чтобы проверить так ли это, откройте ключевой файл (**/local/notesdata/drweb32.key**) текстовым редактором и найдите следующую строчку: `LotusSpamFilter=No`.

Чтобы настроить работу компонента Антиспам:

1. Убедитесь, что ваша версия программы поддерживает работу компонента **Антиспам**.

2. Выберите профиль, для которого вы желаете настроить выявление спама и зайдите в раздел настроек профиля **Антиспам**.
3. По умолчанию компонент **Антиспам** включен. Если нет, то установите флажок **Включить** в верхней части фрейма.
4. Если вы хотите, чтобы к теме спам-сообщения определенной категории добавлялся префикс, установите флажок **Изменить тему** напротив нужной категории. Вы можете изменить префикс в поле ввода **Префикс темы** (по умолчанию - **[СПАМ]**).
5. Помимо добавления префикса к теме, вы можете задать определенные действия для различных категорий спама:
   - **Переместить в базу для спама** - означает, что спам-сообщение будет перемещено в базу данных, указанную в поле ввода **База для спама** (если указанную базу не удается найти, то сообщение будет доставлено получателю). Вы также можете задать определенную папку внутри базы данных в поле **Папка** , чтобы перемещать спам-сообщения в эту папку (если указанную папку не удается найти в базе, то спам-сообщение все равно будет помещаться в эту базу данных, но без определенной папки).
   - **Не принимать письмо** - означает, что спам-сообщение будет принято сервером и сразу удалено. Получатель не получит сообщения, но соответствующий документ об инциденте будет создан в базе **Quarantine.nsf**.
   - **Пропустить** - означает, что никакого действия над сообщением совершено не будет, и оно будет доставлено получателю (тема сообщения все равно будет изменена, если установлен флажок **Изменить тему**).

В качестве базы для хранения спам-писем вы можете назначить любую базу данных Notes, созданную по стандартному почтовому шаблону, например, Mail7.ntf. Дополнительно, в комплекте с модулем **Dr.Web** поставляется база данных DrWebSpam.nsf, устанавливаемая в подкаталог Drweb каталога данных сервера Lotus Domino. Эта база данных создана по шаблону, похожему на базу карантина и инцидентов, и предоставляет некоторые дополнительные функции, которые могут быть удобны при обработке спам-писем: несколько видов фильтров, блокировка от удаления, автоматическое удаление старых сообщений, доставка сообщения пользователю (ошибочно классифицированного как спам), возможность добавления отправителей в белый или черный список.

6. Когда вы закончите редактировать параметры компонента **Антиспам**, нажмите **Сохранить**.

Если какие-либо письма неправильно распознаются **Антиспамом**, следует отправлять их на специальные почтовые адреса, для анализа и повышения качества работы фильтра. Письма, ошибочно оцененные как спам, отправляйте на адрес vrnonspam@drweb.com, а спам, не распознанный системой - на адрес vrspam@drweb.com. Все сообщения следует пересылать только в виде вложения (а не в теле письма).

Управление группами клиентов

По умолчанию **Dr.Web для IBM Lotus Domino** применяет параметры **Стандартного** профиля ко всем пользователям. Если вы желаете использовать параметры другого профиля для определенных пользователей (см. Создание и настройка профилей), то добавьте этих пользователей в группу и назначьте для нее желаемый профиль. Таким образом, для упрощения работы с клиентами сервера Lotus Domino вы можете разделить их на группы, у каждой из которых будет свой набор параметров защиты.

Чтобы создать группу и назначить ей определенный профиль:

1. Выберите пункт **Группы** в иерархическом меню и нажмите кнопку **Создать** под списком групп в основном фрейме справа.
2. Введите имя группы и нажмите кнопку **OK**. Новая группа отобразится под пунктом **Группы** в иерархическом меню.

   ### Чтобы изменить имя группы:

   - Выберите ее в иерархическом меню и введите желаемое имя в поле ввода **Имя**.

Для имени группы не допускается использование следующих символов: **! / \ | ; : " * ,**

3. В поле **Члены** добавьте имена Lotus-групп с помощью кнопки **Добавить**.
4. В поле **Профиль** выберите тот профиль, который вы желаете назначить данной группе.
5. Когда вы закончите изменять параметры группы, нажмите кнопку **Сохранить**.

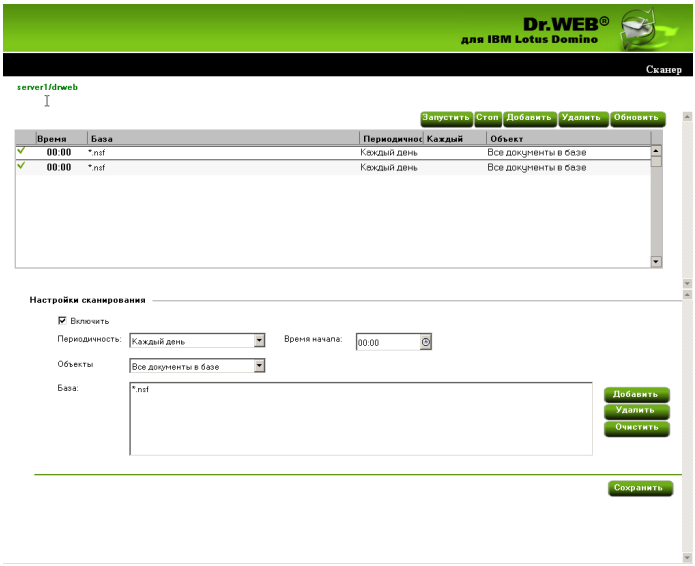
Проверка баз данных Lotus Notes

В **Dr.Web для IBM Lotus Domino** реализована возможность сканирования документов в выбранных базах NSF по расписанию, а также запуск процесса сканирования вручную при помощи **Сканера**.

Расписание состоит из заданий, которые определяют периодичность, день и время начала сканирования, а также те базы, которые необходимо проверить.

Чтобы создать задание на сканирование:

1. Выберите пункт **Сканер** в иерархическом меню и нажмите кнопку **Создать** под списком заданий в верхней половине фрейма **Сканер** (см. иллюстрацию ниже). В списке появится новое неактивное задание со значениями по умолчанию.



2. Выберите созданное задание и укажите для него параметры периодичности, дня и времени начала сканирования

(нижняя часть фрейма **Сканер**). Затем внесите базы, документы в которых вы желаете проверить, в список. Для этого воспользуйтесь кнопкой **Добавить** и выберите необходимые базы.

Для каждой папки вы можете выбрать как отдельные базы, так и добавить в список все базы из этой папки, выбрав пункт ***.nsf**.

3. В выпадающем меню **Объекты** вы можете выбрать, хотите ли вы сканировать все документы в указанных базах или только те, которые были созданы или изменены с момента последнего сканирования (т.е. выполнять инкрементальное сканирование, при котором можно существенно сэкономить время и вычислительные ресурсы сервера).

Если вы выберете проверку только новых и измененных документов и при этом **Сканер** не обнаружит вредоносную программу в зараженном документе из-за устаревших вирусных баз, то этот документ никогда не будет перепроверен при инкрементальном сканировании, если только он не будет изменен. Поэтому рекомендуется регулярно обновлять вирусные базы и производить полную ручную проверку (не реже, чем раз в неделю).

4. Когда вы закончите настраивать параметры задания, установите флажок **Включить**, чтобы задание стало активным.

Каждую минуту **Сканер** сверяет параметры всех активных заданий в списке. Если параметры какого-либо задания совпадают с текущим значением даты и времени, то **Сканер** начинает проверку документов в указанных базах.

Чтобы запустить процесс сканирования вручную:

- Выберите необходимое задание из списка и нажмите кнопку **Запустить**. Задание будет запущено и **Сканер** начнет проверять документы в указанных базах NSF в течение 1 минуты.

Чтобы завершить сканирование:

- Выберите задание и нажмите **Стоп** (на завершение процесса сканирования может уйти до 1 минуты).

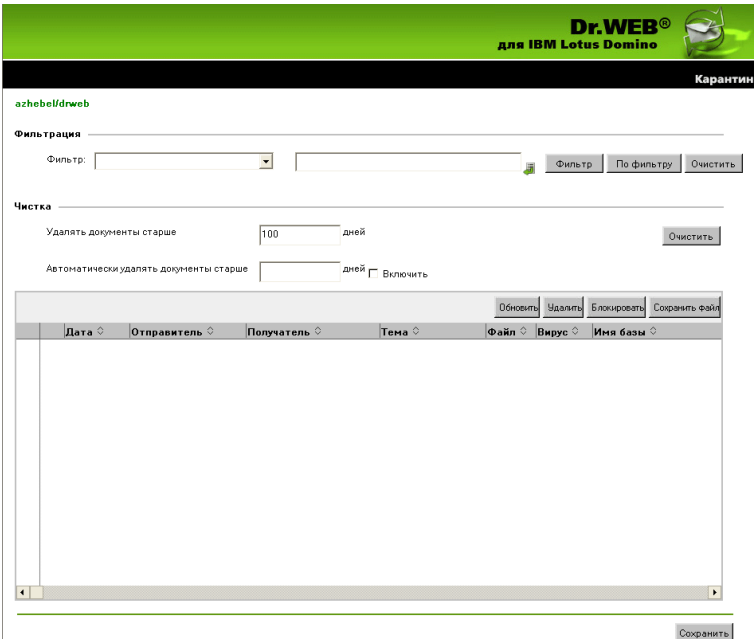
Вы можете запускать и останавливать любое количество заданий, независимо друг от друга.

Когда вы закончите настраивать задания на сканирование, нажмите **Сохранить**.

Управление Карантином

Компонент **Карантин** - это служебная база (**quarantine.nsf**), которая используется для изоляции инфицированных и подозрительных объектов. Эти объекты помещаются туда **Монитором** или **Сканером** в виде документов, если им назначено действие **Перемещение в карантин**.

Фрейм раздела **Карантин** (см. иллюстрацию ниже) состоит из списка объектов, находящихся в карантине и ряда настроек для управления этим списком и документами в базе **quarantine.nsf**. Чтобы отсортировать список согласно определенному критерию, нажмите на заголовок соответствующей колонки списка.



В группе настроек **Фильтрация** вы можете отфильтровать записи в списке, чтобы там отображались только документы с определенной датой, типом вируса и т.д.

Чтобы отфильтровать список:

1. Выберите тип фильтра в выпадающем меню **Фильтр** и укажите значение для этого фильтра в поле ввода рядом.
2. Нажмите кнопку **Фильтр** или **По фильтру**:
   - **Фильтр** - отфильтровать все документы в **Карантине**.
   - **По фильтру** - отфильтровать только те документы, которые указаны в списке (если фильтрация к списку уже применялась).

Фильтры применяются не к самим объектам, а к записям в списке. Чтобы увидеть полный список объектов без фильтров, нажмите кнопку **Очистить**.

В группе настроек **Чистка** вы можете удалить из карантина объекты, которые находились там больше определенного количества дней.

Чтобы почистить список:

- Укажите требуемое количество дней и нажмите кнопку **Очистить**.

Чтобы удалить из базы карантина все документы, введите значение **0** дней в разделе **Чистка**. В этом случае, при нажатии кнопки **Очистить**, программа спросит вас, уверены ли вы, что хотите удалить все данные из карантина.

Также, вы можете задать определенное количество дней в поле **Автоматически удалять документы старше** и установить флажок **Включить**, чтобы удалять старые объекты автоматически. Автоматическое удаление документов из карантина выполняет агент **Automatically delete objects** в базе **quarantine.nsf**. По умолчанию этот агент запускается на сервере

каждый день в 01:30 ночи. Вы можете изменить параметры его запуска, используя стандартные средства Lotus Domino (см. документацию IBM Lotus Domino: http://www.ibm.com/developerworks/lotus/documentation/domino/).

Чтобы удалить документ из базы Карантина

- Выберите этот документ из списка и нажмите кнопку **Удалить**.

Чтобы сохранить объект, который помещен в Карантин, на жестком диске:

1. Выберите объект в списке.
2. Нажмите кнопку **Сохранить файл**, чтобы открыть окно с деревом объектов файловой системы.
3. Выберите папку, в которую вы хотите сохранить объект и нажмите кнопку **ОК**.

Чтобы документ нельзя было удалить ни автоматически, ни вручную:

- Выберите его в списке и нажмите кнопку **Блокировка**. Повторное нажатие разблокирует выбранный заблокированный документ.

Список автоматически обновляется каждые 12 часов, однако вы можете сделать это вручную в любое время, нажав на кнопку **Обновить**.

Процесс обновления может занять некоторое время (до нескольких минут) в зависимости от количества объектов в карантине.

Кнопка **Сохранить** под списком используется для сохранения изменений во фрейме **Карантин**.

Просмотр статистики

Компонент **Статистика** собирает информацию о всех событиях, касающихся основных функций **Dr.Web для IBM Lotus Domino** (обнаружение инфицированных объектов, применение действий к ним, фильтрация спама и т.д.). Для просмотра этой информации выберите пункт **Статистика** в иерархическом меню. Раздел состоит из двух вкладок:

- **Статистика** - содержит краткую сводку о том, сколько объектов проверено, сколько из них инфицировано, сколько вылечено и т.д. (обновление данных статистики происходит при возникновении события, но не чаще, чем 1 раз в минуту).
- **Инциденты** - содержит список документов, в которых записывается информация о событиях **Dr.Web для IBM Lotus Domino** (обнаружение вируса или спама и т.п.). По этим документам формируются отчеты (см. Управление отчетами).

Настройки во вкладке **Инциденты** похожи на настройки в разделе **Карантин** (см. Управление Карантином). Вы можете отфильтровать документы в списке, чтобы там отображались только документы с определенной датой, типом вируса и т.д.

Чтобы отфильтровать доументы:

1. Выберите тип фильтра в выпадающем меню **Фильтр** и укажите значение для этого фильтра в поле ввода рядом.
2. Нажмите кнопку **Фильтр** или **По фильтру**:
    - **Фильтр** - отфильтровать все документы **Статистики**.
    - **По фильтру** - отфильтровать только те документы, которые указаны в списке (если фильтрация к списку уже применялась).

Чтобы удалить из списка инцидентов документы, пролежавшие там больше определенного количества дней, укажите это в группе настроек **Чистка** и нажмите кнопку **Очистить**.

В этой же группе настроек вы можете задать количество дней для

автоматического удаления объектов, пролежавших в карантине больше определенного количества дней. Автоматическое удаление документов выполняет агент **Automatically delete objects** в базе **quarantine.nsf**.

По умолчанию этот агент запускается на сервере каждый день в 01:30. Вы можете изменить параметры его запуска, используя стандартные средства Lotus Domino (см. документацию IBM Lotus Domino: http://www.ibm.com/developerworks/lotus/documentation/domino/).

Чтобы удалить документ из списка инцидентов:

- Выберите его в списке и нажмите кнопку **Удалить**.

Чтобы документ нельзя было удалить ни автоматически, ни вручную:

- Выберите его в списке и нажмите кнопку **Блокировка**. Повторное нажатие разблокирует выбранный заблокированный документ.

Список автоматически обновляется каждые 12 часов, однако вы можете сделать это вручную в любое время, нажав на кнопку **Обновить**.

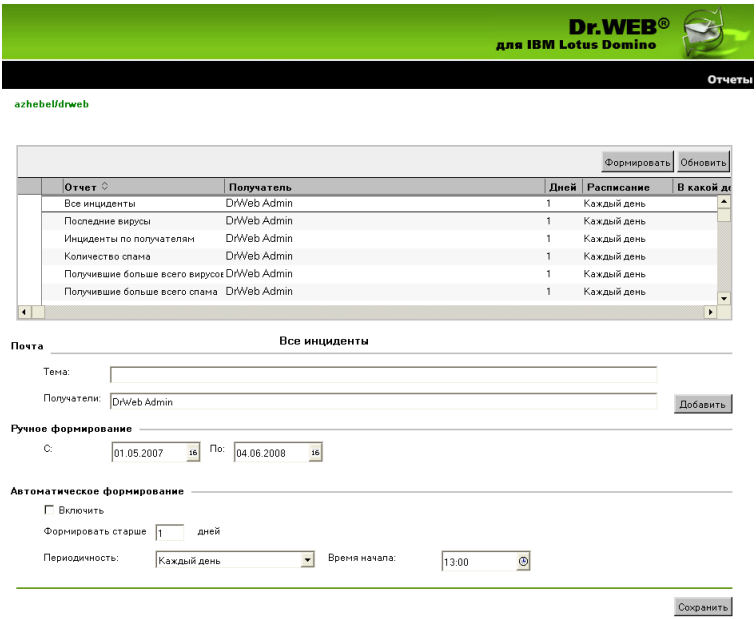
Процесс обновления может занять некоторое время (до нескольких минут) в зависимости от количества объектов в базе инцидентов.

Кнопка **Сохранить** под списком используется для сохранения изменений во фрейме **Статистика**.

Управление отчетами

В **Dr.Web для IBM Lotus Domino** реализована возможность создания отчетов о работе антивирусного модуля. Эти отчеты о различных типах инцидентов могут посылаться на указанные адреса в виде HTML-файлов, приложенных к письму. Отчеты основаны на списке документов во вкладке **Инциденты** раздела **Статистика** (см. Просмотр статистики).

Настройка рассылки отчетов осуществляется в разделе **Отчеты** (см. иллюстрацию ниже).



В верхней части фрейма **Отчеты** находится список из шести типов отчетов, которые вы можете настроить:

- Все инциденты
- Инциденты по получателям

- Последние вирусы
- Количество спама
- Получившие больше всего вирусов
- Получившие больше всего спама

В группе настроек **Почта** под списком типов отчета вы можете указать тему и получателей письма с отчетом в полях ввода **Тема** и **Получатели**. В качестве получателей вы можете указать одного, нескольких или группу клиентов сервера Lotus Domino.

Чтобы добавить получателей:

- Нажмите кнопку **Добавить** и выберите их в открывшемся диалоговом окне.

В группе настроек **Ручное формирование** вы можете настроить даты инцидентов, для которых вы желаете вручную разослать выбранный тип отчетов.

Чтобы разослать отчеты вручную:

1. Выберите желаемый тип отчетов.
2. Укажите диапазон дат в полях **С** и **По.**
3. Нажмите кнопку **Формировать** над списком типов отчетов.

В группе настроек **Автоматическое формирование** вы можете задать расписание для автоматической рассылки выбранного типа отчетов.

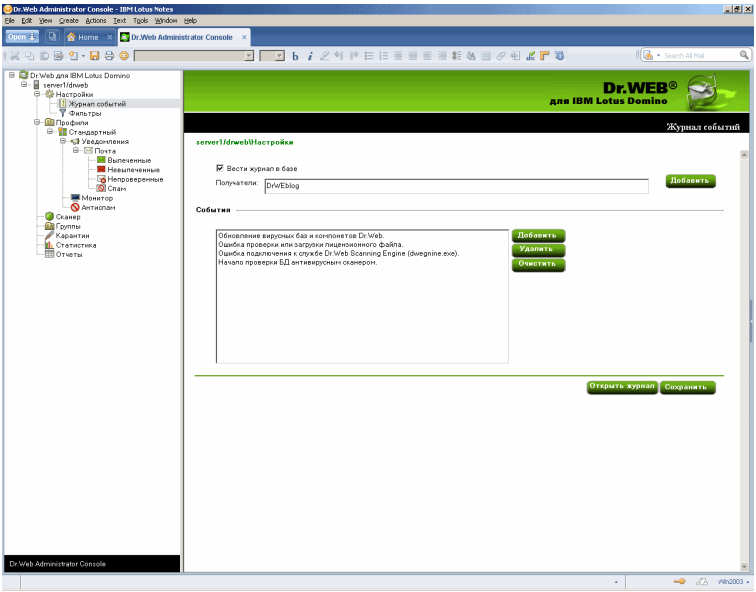
Чтобы включить рассылку отчетов по расписанию:

1. Установите флажок **Включить**.
2. Укажите количество дней, предшествовавших сегодняшнему, для которых вы желаете генерировать отчеты (т.е. если указать «**1**», то в отчет будут включены только вчерашние инциденты; «**2**» - инциденты за последние два дня и т.д.).
3. Задайте периодичность, дату и время рассылки отчетов.
4. Нажмите **Сохранить**.

Задать автоматическую рассылку отчетов по расписанию для инцидентов, произошедших в течение текущего дня, невозможно. Если вы хотите послать отчет с инцидентами за сегодняшний день, то сгенерируйте его, указав диапазон с сегодняшней датой в группе настроек **Ручное формирование**.

Ведение Журнала Событий

Журнал событий может использоваться сетевыми администраторами для контроля событий, происходящих в ходе работы **Dr.Web для IBM Lotus Domino** (особенно если в сети работает более одного сервера Lotus Domino). Управление **Журналом событий** осуществляется из одноименного подраздела в пункте иерархического меню **Настройки**. Администратор может выбрать события, информация о которых записывается в журнал, а также базу данных, в которой эта информация будет храниться.

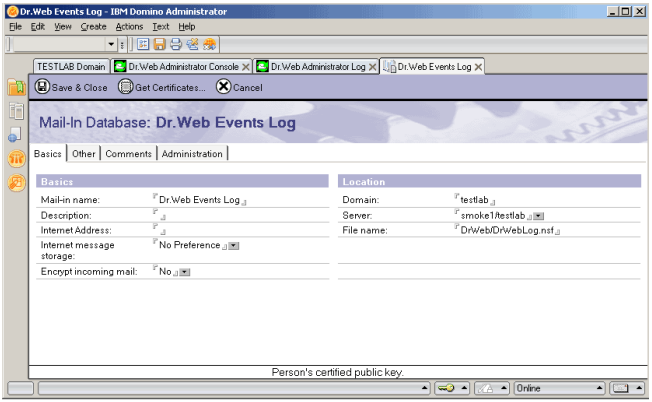


Чтобы настроить ведение Журнала событий:

1. Выберите пункт **Настройки** в иерархическом меню и откройте раздел **Журнал событий**.
2. Установите флажок **Вести журнал в базе данных**.
3. Вы можете указать почтовый адрес баз NSF, в которые будет записываться информация, добавляя их в поле **Получатели**

при помощи кнопки **Добавить**. До этого необходимо задать почтовый адрес для желаемой базы данных:

1) Запустите клиент Domino Administrator.
2) Выберите сервер и откройте вкладку **People and Groups**.
3) Выберите пункт **Mail-In databases and resources**.
4) Нажмите кнопку **Add Mail-In Database**.
5) Выберите имя базы данных, укажите почтовый домен и сервер.
6) В поле **File Name** укажите `DrWeb/DrWebLog.nsf`.



7) Сохраните документ и реплицируйте файл **names.nsf** на другие сервера Lotus Domino в домене (если их больше одного).

4. В группе настроек **События** вы можете сформировать список событий, информация о которых должна попадать в журнал. Кнопками **Добавить** и **Удалить** вы можете редактировать состав списка, а нажатие на кнопку **Очистить** удалит из него все события.

Нажмите **Сохранить**, чтобы применить внесенные изменения.

Настройка фильтров баз данных и электронных адресов

Фильтры используются для задания общих ограничений работы **Dr.Web для IBM Lotus Domino**. Они настраиваются в подразделе **Фильтры** (пункт **Настройки**), который разделен на две вкладки:

- Вкладка Базы позволяет задать список баз данных NSF, которые должны быть включены или исключены из проверки **Монитором**.
- Вкладка Антиспам позволяет создать белый и черный списки электронных адресов.

Вы можете задать списки вручную (в соответствующих вкладках раздела **Фильтры**) или воспользоваться возможностью импорта данных из текстового файла. Для списков включения/исключения баз данных из проверки на каждой строке файла записывается относительный путь (в каталоге **DATA**) и полное имя файла или маска. Например:

```
mail/gendir.nsf
trustbase/*.nsf
```

Для черного/белого списка антиспама на каждой строке записывается электронный адрес или маска. Например:

```
spamer1@spam.ru
*@spamers.ru
spamer2@spam.ch
```

Чтобы импортировать данные из файла в список:

1. Выберите пункт **Настройки** в иерархическом меню и откройте раздел **Фильтры**.
2. Нажмите кнопку **Импорт** в нижней части раздела.
3. Выберите один из четырех типов списка, в который необходимо импортировать данные из файла.
4. Укажите путь и имя файла для импорта.

5. Нажмите кнопку **Импорт**.

Во вкладке **Результат** вы можете просмотреть информацию и статистику по последнему импортированному файлу.

Фильтр баз данных

По умолчанию **Монитор Dr.Web для IBM Lotus Domino** проверяет «на лету» все базы NSF, кроме некоторых служебных баз сервера Lotus Domino. При помощи списков **Включить** и **Исключить** во вкладке **Базы** раздела **Фильтры** (пункт **Настройки**) вы можете задать свои ограничения работы **Монитора**.

Списки **Включить** и **Исключить** влияют только на работу **Монитора** и не применяются к задачам сканирования баз NSF вручную или по расписанию (см. Проверка баз данных Lotus Domino).

Чтобы настроить фильтр баз данных Lotus Domino:

1. Установите флажок **Включить фильтрацию** в верхней части вкладки **Базы**.
2. Нажмите кнопку **Добавить** рядом с соответствующим списком, выберите базу в диалоговом окне и нажмите **ОК**.
   - в список **Включить** добавляются базы, которые являются обязательными к проверке **Монитором** (базы, не указанные в списке **Включить**, проверяться НЕ БУДУТ);
   - в список **Исключить** добавляются базы, которые должны быть исключены из проверки **Монитором** (базы, не указанные в списке **Исключить**, БУДУТ проверяться).

Вы также можете добавлять в списки шаблоны путей, т.е. пути к папкам, содержащим необходимые базы, оканчивающиеся следующей комбинацией символов: ***.nsf**. Например, если вы укажете путь **mail*.nsf**, то в список будут добавлены все базы NSF в папке **mail** каталога данных сервера (базы в подпапках добавлены не будут).

Чтобы удалить базу из списка:

- Выберите ее и нажмите **Удалить**.

Чтобы очистить список:

- Нажмите **Очистить**.

Когда вы закончите составлять список, нажмите **Сохранить**. При этом изменения вступят в силу через 1 минуту после сохранения.

Черный и белый списки электронных адресов

Вы можете составить черный и белый списки электронных адресов (адресов, которым вы не доверяете или, наоборот, доверяете) во вкладке **Антиспам** подраздела **Фильтры** (пункт **Настройки**).

Чтобы добавить адрес в список:

1. Установите флажок **Включить**.
2. Введите адрес или имя домена в поле ввода под соответствующим списком.
3. Нажмите **Добавить**.

Добавляйте адреса, которым вы доверяете, в белый список (письма с этих адресов не будут проверяться на наличие спама), а адреса, которым вы не доверяете - в черный список (письмам с этих адресов будет без проверки присваиваться статус *Точно спам* и к ним будут применены действия, настроенные в разделе **Антиспам** для писем с таким статусом).

При добавлении адресов и имен доменов вы можете задавать их в виде шаблонов. Для этого вы можете пользоваться символом *****. Шаблоны позволяют задавать диапазон электронных адресов или доменов (например, запись ***@mail.com** означает любой адрес из домена **mail.com**).

Чтобы удалить адрес из списка:

- Выберите его и нажмите **Удалить**.

Чтобы очистить список:

- Нажмите **Очистить**.

Когда вы закончите составлять списки, нажмите **Сохранить**. При этом изменения вступят в силу через 1 минуту после сохранения.

Обновление вирусных баз

Для автоматизации получения и установки обновлений вирусных баз и библиотеки антиспама рекомендуется использовать **Модуль обновления**. Модуль содержится в пакете **drweb-updater**, который входит в состав продукта **Dr.Web для IBM Lotus Domino**. **Модуль обновления** представляет собой скрипт, написанный на языке Perl, который находится в директории, содержащей исполняемые файлы программного комплекса (по умолчанию: **/opt/drweb/update.pl**).

Настройки **Модуля обновления** хранятся в секции **[Updater]** главного конфигурационного файла (по умолчанию: **/etc/drweb/drweb32.ini**). Для использования другого конфигурационного файла полный путь к нему необходимо указать параметром командной строки при запуске скрипта.

При установке пакета **drweb-updater** создается задание на периодический (раз в пол часа) запуск скрипта **update.pl** с помощью стандартного планировщика (**cron**). Для этого в каталоге **/etc/cron.d** создается файл **drweb-update** со следующей строкой:

```
*/30 * * * * drweb /opt/drweb/update.pl
```

При обновлении библиотеки антиспама (**libvaderetro.so**) происходит следующее:

1. Скрипт обновления передает сигнал SIGHUP демону **drweblotusd**, используя его PID из файла **drweblotusd.pid** (путь к этому файлу задан в параметре **Lotusdpidfile** в файле **drweb32.ini**).
2. Демон **drweblotusd** копирует новую версию библиотеки в **/var/drweb/lotus/libvaderetro.so.cache** и загружает ее в память, удаляя при этом старую версию.

Экспорт/импорт конфигураций

В **Dr.Web для IBM Lotus Domino** предусмотрена возможность сохранять текущую конфигурацию в файл с целью последующего использования настроек на других серверах с установленным антивирусным модулем.

Чтобы экспортировать текущие настройки:

1. Откройте **Консоль администратора Dr.web**.
2. Выберите пункт с названием сервера в иерархическом меню.
3. Откройте меню **Actions** в верхней части окна клиента Lotus Notes и выберите пункт **Export**.
4. В появившемся диалоговом окне установите флажок **Включить** и задайте путь и имя выходного файла в разделе **Экспорт конфигураций**.
5. Нажмите **Экспорт**.

Чтобы импортировать настройки из файла:

1. Откройте **Консоль администратора Dr.web**.
2. Выберите пункт с названием сервера в иерархическом меню.
3. Откройте меню **Actions** в верхней части окна клиента Lotus Notes и выберите пункт **Import**.
4. Выберите сервер, на который необходимо импортировать конфигурацию и укажите базу **DrWeb/DrWebAdmin.nsf** на этом сервере.
5. В группе настроек **Импорт конфигураций** выберите настройки, которые необходимо импортировать и укажите XML-файл конфигурации.
6. Нажмите **Импорт**.

При импорте конфигураций, настройки элементов (групп и профилей) с одинаковыми названиями будут заменены, а новые - добавлены. Например, если на сервере существует группа Group 1, а в импортируемом файле созданы группы Group 1 и Group 2, то Group 1 на сервере будет заменена одноименной группой из импортируемого файла, а также будет добавлена группа Group 2.

При необходимости вы также можете экспортировать/ импортировать отчеты (см. соответствующие настройки в диалоговых окнах **Экспорт** и **Импорт**).

Приложения

Приложение А. Работа в режиме централизованной защиты

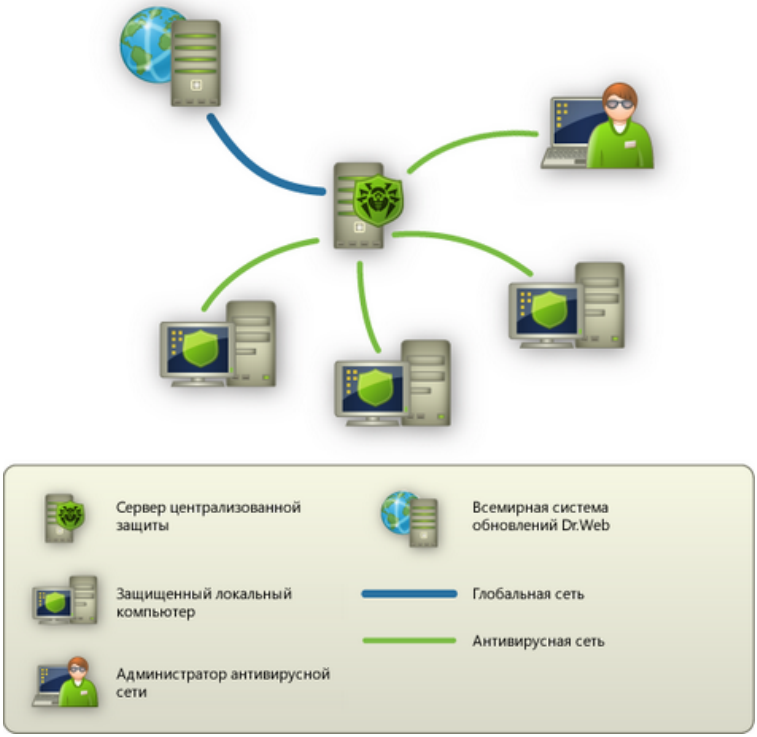
Dr.Web для IBM Lotus Domino может функционировать в сети, контролируемой **Центром Управления Dr.Web**. Данное решение по организации централизованной антивирусной защиты позволяет автоматизировать и упростить настройку и управление информационной безопасностью компьютеров, объединенных в единую логическую 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 конечный пользователей.

Взаимодействие компонентов антивирусной сети

Решения компании **«Доктор Веб»** по организации централизованной антивирусной защиты имеют клиент-серверную архитектуру.

Компьютеры компании или пользователей поставщика IT-услуг защищаются от угроз безопасности и спама *локальными антивирусными компонентами* (клиентами; в данном случае – **Dr.Web для IBM Lotus Domino**), 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.



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.

Для работы **Dr.Web для IBM Lotus Domino** в режиме централизованной защиты необходимо, чтобы в операционной системе был установлен и корректно работал **Dr.Web Agent**.

Dr.Web for IBM Lotus Domino версии 6.0 совместим с версией **Dr.Web Agent** 6.0 и выше.

Для **Dr.Web для IBM Lotus Domino** в режиме централизованной защиты реализованы следующие возможности работы:

- регистрация запуска и остановки сервера IBM Lotus Domino с установленным модулем **Dr.Web**. События запуска и остановки будут отображаться в таблице **Запуск/ Завершение Центра Управления Dr.Web**;
- отправка статистики работы антивирусного модуля **Dr.Web для IBM Lotus Domino**. Статистика работы отображается в таблицах **Статистика** и **Суммарная статистика Центра Управления Dr.Web**;
- отправка оповещений об обнаружении вирусов, с информацией об инфекции и предпринятом действии. Эти события отображаются в таблице **Инфекции Центра Управления Dr.Web**;
- отправка URL на WEB-консоль администратора **Dr.Web для IBM Lotus Domino** в **Центр Управления Dr.Web**. Это позволяет в консоли **Центра Управления Dr.Web** видеть URL на консоль управления антивирусным модулем **Dr.Web** на конкретном сервере IBM Lotus Domino. URL может быть задан администратором системы или автоматически сформирован на основе настроек серверного документа в

адресной книге сервера Lotus Domino.

Чтобы установить значение URL:

1. Задайте параметр DrWebAdminURL в файле сервера notes.ini. Например:

   ```
   DrWebAdminURL=http://domino-server.domain.name/drweb/DrWebAdmin.nsf
   ```

2. Перезагрузите сервер Lotus Domino.

Чтобы установить значение параметра без перезагрузки сервера Lotus Domino:

1. В консоли сервера выполните команду:

   ```
   set config DrWebAdminURL=http://domino-server.domain.name/drweb/DrWebAdmin.nsf
   ```

2. Передача значения URL в **Центр Управления Dr.Web** выполнится в течение минуты.

- обновление вирусных баз, антивирусного ядра и ядра **Антиспама** 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 **Dr.Web для IBM Lotus Domino**, зарегистрированного для данной станции в сети **Центра Управления Dr.Web**. Чтобы включить эту функцию, необходимо перевести модуль в режим **Enterprise**. Для этого необходимо выполнить следующие действия:
  - перевести **Dr.Web Agent** в режим **Enterprise**, установив значение **Yes** для параметра **UseEnterpriseMode** в конфигурационном файле **/etc/drweb/agent.conf**;
  - выполнить команду `/etc/init.d/drweb-monitor restart`;

- в файл **notes.ini** сервера Lotus Domino добавить параметр **DrWebEdition=Enterprise** и перезагрузить сервер Lotus Domino.

В режиме **Enterprise** **Dr.Web для IBM Lotus Domino** не использует локальный лицензионный ключевой файл, указанный в конфигурационном файле **/etc/drweb/agent.conf** в качестве значения параметра **LicenseFile** раздела **StandaloneMode**. В режиме **Enterprise** ключ запрашивается у **Центра Управления Dr.Web**, и если ключ не получен, программа не осуществляет антивирусную проверку.

Приложение Б. 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, настоятельно рекомендуется попробовать найти решение одним из следующих способов:

- Прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/faq/
- Посетить форумы **Dr.Web** по адресу http://forum.drweb.com/

Если после этого вам не удалось решить проблему, то вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки:

- Заполнить специальную веб-форму по адресу http://support.drweb.com/new/
- Написать электронное письмо по адресу 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.