Dr.WEB

Mail Security Suite (IBM Lotus Domino Windows)

Руководство администратора

Dr.Web Mail Security Suite (IBM Lotus Domino Windows)
Версия 12.0
Руководство администратора
18.03.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

1. О документе

Назначение документа

Благодарим вас за приобретение Dr.Web Mail Security Suite (IBM Lotus Domino Windows). Данный продукт обеспечивает надежную защиту компьютеров и информации внутри корпоративной сети от распространяющихся по почте угроз, используя самые современные технологии.

Настоящее руководство призвано помочь администраторам корпоративных сетей установить и настроить приложение Dr.Web Mail Security Suite (IBM Lotus Domino Windows) (далее — Dr.Web), а также ознакомиться с его основными функциями.

Перейдите по ссылке, чтобы получить ответы на часто задаваемые вопросы.

Условные обозначения

В данном руководстве используются следующие условные обозначения:

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

Сокращения

В руководстве используются сокращения:

Сокращение	Комментарий
Dr.Web	Dr.Web Mail Security Suite (IBM Lotus Domino Windows) (подключаемый антивирусный модуль)
HTTP	от англ. *Hypertext Transfer Protocol* — протокол передачи гипертекста
NSD	от англ. *Notes System Diagnostics* — диагностика системы Lotus Notes
NSF	от англ. *Notes Storage Facility* — тип файлов баз данных, используемых в Lotus Notes и Lotus Domino
SMTP	от англ. *Simple Mail Transfer Protocol* — простой протокол пересылки почты
URL	от англ. *Uniform Resource Locator* — унифицированный указатель ресурса, адрес веб-страницы
ОС	Операционная система
ПО	Программное обеспечение

2. О продукте

Dr.Web — это подключаемый антивирусный модуль, который защищает корпоративную почтовую систему, построенную на основе сервера Lotus Domino, от вирусов и спама.

Dr.Web может выполнять следующие функции:

- проверка всех входящих и исходящих сообщений «на лету» (в режиме реального времени);
- проверка документов в выбранных базах NSF (*Notes Storage Facility*) 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 (*Simple Mail Transfer Protocol*), а также создание белых и черных списков электронных адресов;
- распределение пользователей по группам;
- отправка уведомлений о вирусных событиях и ведение журнала событий;
- рассылка отчетов о вирусной активности и спаме;
- сбор статистики о работе;
- автоматическое обновление вирусных баз и компонентов программы по запросу пользователя или согласно расписанию.

Dr.Web не поддерживает использование технологии DB2 Universal Database (DB2 UDB).

Компоненты продукта постоянно обновляются, а вирусные базы и база правил спам-фильтрации сообщений регулярно дополняются новыми записями. Постоянное обновление обеспечивает актуальный уровень защиты устройств пользователей, а также используемых ими приложений и данных.

Для дополнительной защиты от неизвестного вредоносного программного обеспечения используются методы эвристического анализа, реализованные в антивирусном ядре.

Структура приложения Dr.Web, применение и возможность управления различными методами антивирусной проверки — все это обеспечивает высокую скорость проверки и помогает значительно экономить вычислительные ресурсы системы. Приложение предоставляет широкие возможности для администраторов по контролю защиты от вирусов и спама в сетях Domino любого масштаба.

2.1. Проверяемые объекты

Dr.Web проверяет следующие объекты:

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

Dr.Web не проверяет:

- зашифрованные письма;
- документы в зашифрованных базах данных Lotus Domino;
- локальные реплики баз данных, размещенные на компьютерах пользователей.

2.2. Компоненты приложения

Dr.Web — это комплексный антивирусный продукт, состоящий из нескольких дополняющих друг друга компонентов, которые взаимодействуют между собой и обеспечивают высокий уровень защиты.

- *Монитор* проверяет все входящие и исходящие письма в режиме реального времени по мере того, как их обрабатывает сервер Lotus Domino. Как только письмо проверено и признано безопасным, оно сразу отправляется пользователю. Если письмо содержит зараженный или подозрительный объект, то над ним производится соответствующее предустановленное действие (см. Настройка Монитора).
- *Сканер* позволяет периодически проверять документы в выбранных базах NSF. Он запускается по расписанию или вручную и так же, как и монитор, применяет предустановленные действия к зараженным и подозрительным объектам (см. Проверка баз данных Lotus Domino).
- *Карантин* используется для изоляции зараженных и подозрительных объектов (см. Управление Карантином). Он представляет собой базу NSF (`Quarantine.nsf`), которая расположена в каталоге `\DATA\DRWEB` сервера Lotus Domino. Доступ к объектам, находящимся в Карантине, осуществляется из базы *Консоли администратора* (`DrWebAdmin.nsf`).
- *Модуль автоматического обновления* предназначен для автоматического обновления вирусных баз. Модуль загружает копии вирусных баз из интернета либо из каталога или сервера в локальной сети. Запустить модуль можно двумя способами: автоматически и в режиме командной строки (см. Обновление вирусных баз).
- Компонент *Антиспам* проверяет все входящие по протоколу SMTP сообщения в режиме реального времени по мере того, как их обрабатывает сервер Lotus Domino (см. Настройка Антиспама). Используя специальные алгоритмы, основанные на выявлении признаков спама в письмах, компонент с большой вероятностью определяет, является ли письмо спамом, и, в случае необходимости, добавляет к теме письма предустановленный префикс (по умолчанию `[СПАМ]`).

Компонент Антиспам доступен только в версии продукта «Антивирус + Антиспам» (см. Лицензирование).

- Компонент *Статистика* сохраняет информацию о типах проверенных объектов и произведенных над ними действиями. Вы можете просматривать данную информацию, чтобы следить за работой Dr.Web (см. Просмотр статистики).
- Компонент *Отчеты* предназначен для рассылки регулярных отчетов о работе приложения на указанные адреса и согласно определенным критериям (см. Управление отчетами).
- *Журнал событий* предоставляет администраторам серверов Lotus Domino возможность эффективно отслеживать события, связанные с работой Dr.Web (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.

Работой этих компонентов можно управлять при помощи *Консоли администратора* — графического интерфейса, работа с которым осуществляется либо посредством клиента Lotus Notes, либо через веб-браузер (см. Запуск Консоли администратора).

3. Лицензирование

Права пользователя на использование копии программного продукта Dr.Web подтверждаются и регулируются лицензией, приобретенной у компании «Доктор Веб» или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. https://license.drweb.com/agreement/), условия которого принимаются пользователем при установке программного продукта на компьютер.

В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии продукта, в частности:

- перечень компонентов, которые разрешено использовать (например, наличие компонента Антиспам в версии продукта «Антивирус + Антиспам»);
- период, в течение которого разрешено использование Dr.Web;
- наличие или отсутствие технической поддержки;
- другие ограничения (например, количество компьютеров, на которых разрешено использовать Dr.Web).

Имеется также возможность активировать для приобретенной копии продукта демонстрационный период. В этом случае, если не нарушены условия активации, пользователь получает право на полноценное использование Dr.Web в течение демонстрационного периода.

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу компонентов продукта в соответствии с параметрами лицензии. Он называется *лицензионным ключевым файлом*. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый *демонстрационным*.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов Dr.Web блокируются, кроме того, становится недоступен сервис регулярных обновлений вирусных баз с серверов обновлений компании «Доктор Веб».

3.1. Регистрация и активация лицензии

Приобретение, регистрация и активация лицензии

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов обновлений компании «Доктор Веб», а также получать стандартную техническую поддержку компании «Доктор Веб» и ее партнеров.

Приобрести любой антивирусный продукт компании «Доктор Веб» или серийный номер для него можно у наших партнеров или через интернет-магазин. Дополнительную информацию о возможных вариантах лицензий можно найти на официальном сайте компании «Доктор Веб» https://license.drweb.com/products/biz/.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем продукта Dr.Web, и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки.

При активации приобретенной лицензии необходимо указать ее серийный номер. Этот номер может поставляться вместе с продуктом или по электронной почте, при покупке или продлении лицензии онлайн. Приобретенная лицензия может быть активирована непосредственно на официальном сайте компании «Доктор Веб» по адресу https://products.drweb.com/register/.

Если имеется комплект лицензий, выданных для использования продукта на нескольких серверах, то при регистрации имеется возможность указать, что Dr.Web будет использоваться только на одном сервере. В этом случае все лицензии из комплекта будут объединены в одну и срок ее действия будет автоматически увеличен.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации необходимо указать те же персональные данные, которые были введены при первой регистрации лицензии. Допускается использовать другой адрес электронной почты — в таком случае лицензионный ключевой файл будет выслан по новому адресу.

После получения ключевого файла по электронной почте, вам необходимо выполнить процедуру его установки.

3.2. Запрос демонстрационного периода

Для получения демонстрационного периода на использование продукта Dr.Web следует отправить запрос с официального сайта компании «Доктор Веб» по адресу https://download.drweb.com/demoreq/biz/. После выбора продукта и заполнения анкеты вы получите по электронной почте серийный номер или ключевой файл для активации демонстрационного периода.

Демонстрационный период использования продукта может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

3.3. Ключевой файл

Права пользователя на использование программного продукта Dr.Web хранятся в специальном файле, называемом *ключевым*. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

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

- срок действия лицензии не истек,
- ключевой файл распространяется на все компоненты, используемые Dr.Web,
- целостность ключевого файла не нарушена.

При нарушении любого из этих условий ключевой файл становится *недействительным*, при этом Dr.Web перестает обнаруживать вредоносные программы и пропускает объекты без изменений.

Содержимое ключевого файла защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

Установка ключевого файла

Для работы Dr.Web необходим действительный ключевой файл, путь к которому указывается в процессе установки подключаемого модуля.

При работе Dr.Web ключевой файл по умолчанию должен находиться в каталоге `C:\Program Files\DrWeb for Lotus Domino` и называться `drweb32.key`.

Компоненты подключаемого модуля регулярно проверяют наличие и корректность ключевого файла. При отсутствии действительного ключевого файла (лицензионного или демонстрационного), а также по истечении срока его действия, антивирусные функции всех компонентов блокируются до установки *действительного* ключевого файла.

Рекомендуется сохранять имеющийся лицензионный ключевой файл до истечения срока его действия. В этом случае при переустановке продукта или переносе его на другой сервер повторная регистрация серийного номера лицензии не потребуется. Можно использовать лицензионный ключевой файл, полученный при первом прохождении процедуры регистрации.

При наличии ключевого файла, соответствующего действующей лицензии на Dr.Web (например, он был получен от продавца по электронной почте после регистрации, или

приложение переносится на другой сервер), имеется возможность активировать продукт, просто указав путь к имеющемуся ключевому файлу. Это можно сделать следующим образом:

1. Распакуйте ключевой файл, если он был получен в архиве, и сохраните его в любой доступный каталог (например, в домашний каталог или на съемный носитель).

   По электронной почте ключевые файлы обычно передаются запакованными в zip-архивы. Архив, содержащий ключевой файл для активации продукта, обычно имеет имя `agent.zip` (обратите внимание, что если в сообщении содержится несколько архивов, то нужно использовать именно архив `agent.zip`).

2. Далее в каталог `C:\Program Files\DrWeb for Lotus Domino` скопируйте ключевой файл и, если необходимо, переименуйте в `drweb32.key`.
3. Перезапустите сервер Lotus Domino.

3.4. Определение параметров лицензирования

Лицензионный ключевой файл регулирует использование Dr.Web.

Определение параметров лицензирования

1. Чтобы определить параметры лицензирования, записанные в вашем ключевом файле, откройте файл для просмотра.

   Ключевой файл имеет формат, защищенный от редактирования, поэтому редактирование этого файла делает его недействительным. Чтобы избежать порчи ключевого файла, не сохраняйте его при закрытии текстового редактора.

2. Проверьте следующие параметры лицензирования:

Параметр	Комментарий
Группа `[Key]`, параметр `Applications`	Указывает компоненты, которые разрешено использовать владельцу лицензии. Для использования ключевого файла с Dr.Web в списке компонентов обязательно должен присутствовать компонент DominoPlugin.
Группа `[Key]`, параметр `Expires`	Указывает срок действия лицензионного ключевого файла в формате: `Год-Месяц-День`.
Группа `[User]`, параметр `Name`	Указывает регистрационное имя владельца лицензии.

Параметр	Комментарий
Группа `[User]`, параметр `Computers`	Указывает количество пользователей, защищаемых модулем.

3. Закройте файл, не сохраняя изменений.

3.5. Обновление лицензии

В некоторых случаях, например, при изменении характеристик защищаемой системы или требований к ее безопасности либо при окончании срока действия лицензии вы можете принять решение о приобретении новой или расширенной лицензии на Dr.Web. В таком случае потребуется заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. Приложение поддерживает обновление лицензии «на лету», при котором не требуется переустанавливать Dr.Web.

Замена ключевого файла

1. Чтобы обновить лицензию, скопируйте новый ключевой файл в каталог `C:\Program Files\DrWeb for Lotus Domino`.
2. Чтобы Dr.Web переключился на использование нового ключевого файла, необходимо перезапустить сервер Lotus Domino.

Дополнительную информацию о видах лицензий можно найти на официальном сайте компании «Доктор Веб» по адресу https://license.drweb.com/products/biz/.

4. Установка и удаление приложения

Dr.Web поставляется в виде установочного файла `drweb-[version]-av-lotus-windows.exe`, где `[version]` — номер текущей версии антивирусного приложения. Убедитесь, что у вашего установочного файла есть цифровая подпись компании «Доктор Веб». Для этого проверьте вкладку **Цифровые подписи** в свойствах файла.

Перед установкой приложения внимательно проанализируйте состав и конфигурацию среды Lotus Domino в вашей сети и выберите сервер, который будет служить центром ее защиты от вирусов и спама. Поместите установочный файл на локальный диск выбранного сервера Lotus Domino и убедитесь, что он доступен пользователю LOCALSYSTEM.

Для установки и удаления Dr.Web вам необходимо состоять в группе локальных администраторов на том компьютере, где установлен сервер Lotus Domino. При включенной системе контроля учетной записи осуществляйте установку из консоли, запущенной от имени администратора.

Приложение несовместимо с другими антивирусными программами (см. Совместимость).

4.1. Системные требования

Ниже приведены системные требования к компьютеру, на который устанавливается Dr.Web.

Параметр	Требования
Процессор	Совместимый с системой команд i686
Оперативная память	512 МБ или больше
Место на жестком диске	750 МБ или больше. Временные файлы, создаваемые в ходе установки, потребуют дополнительного места
Разрешение экрана	Рекомендуется не менее 1280 × 1024 с поддержкой не менее 256 цветов
Файловая система	NTFS или FAT32
Операционная система	Для 32-разрядных операционных систем: • Windows Server 2008, • Windows Server 2008 R2.

Параметр	Требования
	Для 64-разрядных операционных систем: • Windows Server 2008, • Windows Server 2008 R2, • Windows Server 2012, • Windows Server 2012 R2, • Windows Server 2016, • Windows Server 2019, • Windows Server 2022
Прочее ПО	ПО Lotus: • IBM Lotus Domino для Windows версии 8.5 - 9.0.1, • IBM Lotus Notes для Windows версии 7.0.2 - 9.0.1, • IBM Domino для Windows 10.1, • IBM Notes для Windows 10.0, • HCL Domino для Windows 11.0, • HCL Notes для Windows 11.0. Браузеры для работы с веб-интерфейсом: • Internet Explorer 8 или более поздней версии, • Mozilla Firefox 3 или более поздней версии, • Opera 9 или более поздней версии

Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой необходимо убедиться, что система поддерживает алгоритм хеширования SHA-256. Для этого установите все рекомендуемые обновления из Центра обновления Windows. Подробную информацию о необходимых пакетах обновлений вы можете найти на официальном сайте компании «Доктор Веб».

Если кроме подключаемого модуля в системе функционирует файловый монитор SpIDer Guard, разработанный компанией «Доктор Веб», то измените настройки SpIDer Guard, добавив маски `dwat*`, `st*.tmp` и `c*.dtf` в список исключаемых путей и файлов. В таком случае сетевой трафик будет проверять подключаемый модуль Dr.Web.

Компания «Доктор Веб» не гарантирует корректную работу антивирусного приложения на альфа-, бета- и других некоммерческих версиях сервера Lotus Domino.

4.2. Совместимость

Перед установкой Dr.Web обратите внимание на информацию о совместимости программы.

1. Приложение Dr.Web версии 12.0 совместимо с компонентами других продуктов версии 12.0, разработанных компанией «Доктор Веб».
2. В режиме централизованной защиты подключаемый модуль совместим только с Dr.Web Enterprise Security Suite версии 12.0.
3. Приложение несовместимо 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 или другая антивирусная программа, то удалите ее, используя установочный файл или стандартные средства операционной системы (см. Удаление приложения).

4.3. Установка приложения

Перед установкой Dr.Web настоятельно рекомендуется

1. Установить все критические обновления, выпущенные компанией Microsoft, для ОС Windows, которая используется на компьютере (они доступны на сайте обновлений по адресу https://support.microsoft.com/help/12373/windows-update-faq).
2. Проверить файловую систему при помощи стандартных средств и исправить обнаруженные ошибки.

Чтобы установить антивирусное приложение

1. Завершите работу сервера Lotus Domino.
2. Удалите предыдущие версии приложения и любые другие антивирусные программы для IBM Lotus Domino, установленные на компьютере, используя стандартные средства ОС Windows.
3. Запустите установочный файл `drweb-[version]-av-lotus-windows.exe`. Откроется окно Мастера установки. Нажмите кнопку **Далее**.
4. Откроется окно с текстом Лицензионного соглашения. Для продолжения установки, прочитайте и установите переключатель в положение **Я принимаю условия лицензионного соглашения**. Нажмите кнопку **Далее**.
5. Если на вашем компьютере установлен Агент Dr.Web, в открывшемся окне укажите вариант лицензирования. Вы также можете использовать локальный ключ. Нажмите кнопку **Далее**.

6. Если на предыдущем шаге установки вы выбрали пункт **Использовать локальный ключ** или на вашем компьютере не установлен Агент Dr.Web, то в открывшемся окне укажите путь к лицензионному ключевому файлу. Для этого нажмите кнопку **Обзор** и выберите необходимый файл в проводнике файловой системы. Нажмите кнопку **Далее**.
7. Откроется окно со списком серверов Lotus Domino, на которые вы хотите установить антивирусный модуль.

   Чтобы добавить необходимый сервер в список, нажмите кнопку **Обзор** и выберите файл `notes.ini` сервера.

   Чтобы очистить список серверов, нажмите кнопку **Очистить список**. Нажмите кнопку **Далее**, когда закончите выбирать необходимые сервера Lotus Domino.
8. Программа установки выведет список серверов Lotus Domino, на которые будет установлен модуль. Нажмите кнопку **Далее**.
9. В следующем окне нажмите кнопку **Установка**, чтобы начать процесс установки приложения.
10. Выполните перезагрузку операционной системы после завершения установки.

При установке Dr.Web на несколько серверов в одном Domino-домене, после каждой установки необходимо реплицировать адресную книгу сервера (база данных `names.nsf`, которая находится в каталоге `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 сервера, что приведет к невозможности отправки служебных уведомлений администратору от приложения.

Чтобы удалить дубликат группы DrWeb Admin в адресной книге

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/).

4.3.1. Действия после установки

После установки Dr.Web необходимо подписать новые базы сервера Lotus Domino, которые использует приложение, иначе оно не сможет автоматически генерировать отчеты и чистить Карантин.

Чтобы подписать базы

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 установлено антивирусное приложение.
5. На вкладке **Files** выделите все базы Dr.Web, находящиеся в каталоге `\DATA\DRWEB`:
   - `DrWebAdmin.nsf`,
   - `DrWebDesign.nsf`,
   - `Quarantine.nsf`,
   - `DrWebReports.nsf`,
   - `DrWebHelp.nsf`,
   - `DrWebLog.nsf`,
   - `DrWebSpam.nsf`.
6. Нажмите правой кнопкой мыши 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**.

4.3.2. Проверка корректности установки

Чтобы проверить корректность установки Dr.Web, удостоверьтесь, что следующие каталоги созданы и содержат все необходимые файлы:

- `%PROGRAMFILES%\DrWeb for Lotus Domino\`

Имя файла	Описание
`drweb32.key`	Лицензионный ключевой файл

- `%COMMONPROGRAMFILES%\Doctor Web\Scanning Engine\`

Имя файла	Описание
`drweb32.dll`	Антивирусное ядро
`vrcpp.dll`	Ядро антиспама
`dwinctl.dll`	Dr.Web Scanning Engine CTL
`dwengine.exe`	Сервис Dr.Web Scanning Engine
`dwsewsc.exe`	Dr.Web Action Center Control
`arkdb.bin`	-
`dwarkapi.dll`	Dr.Web Anti-rootkit API
`dwarkdaemon.exe`	Dr.Web Anti-Rootkit Server

Имя файла	Описание
dwqrui.exe	Dr.Web Quarantine Manager

- %ProgramData%\Doctor Web\Bases\

Имя файла	Описание
*.vdb	Вирусные базы

- C:\Lotus\Domino\ (путь может быть другим, в зависимости от того, где установлен сервер Lotus Domino)

Имя файла	Описание
ndrwebmonitor.exe	Исполняемый файл Монитора
ndrwebscanner.exe	Исполняемый файл Сканера
ndrwebhook.dll	-
drwebupdate.bat	Командный файл для запуска модуля обновления с дополнительными параметрами командной строки

- C:\Lotus\Domino\DATA\DRWEB (путь может быть другим, в зависимости от того, где установлен сервер Lotus Domino)

Имя файла	Описание
DrWebAdmin.nsf	Консоль администратора
DrWebDesign.nsf	Служебная база данных
Quarantine.nsf	База данных карантина и инцидентов
DrWebReports.nsf	База данных отчетов
DrWebHelp.nsf	База встроенной справочной системы
DrWebLog.nsf	База журнала событий
DrWebSpam.nsf	База для хранения SPAM-сообщений

Не рекомендуется применять штатную утилиту Compact к базам DrWebAdmin.nsf, DrWebDesign.nsf и DrWebHelp.nsf, т. к. это может привести к ошибкам в работе антивирусного модуля.

Если в процессе установки приложения возникли ошибки, вы можете обратиться за помощью в службу технической поддержки компании «Доктор Веб».

4.4. Удаление приложения

При удалении Dr.Web теряются все настройки отчетов и заданий на антивирусную проверку, все группы и профили, а также удаляется база карантина (`Quarantine.nsf`) и инцидентов.

Чтобы удалить антивирусное приложение

1. Завершите работу сервера Lotus Domino.
2. Запустите установочный файл `drweb-[version]-av-lotus-windows.exe`. Откроется окно Мастера установки.

Мастер установки можно запустить при помощи стандартного средства ОС Windows **Установка и удаление программ** на Панели управления).

3. Нажмите кнопку **Удалить**.
4. По завершении удаления нажмите кнопку **Закрыть**.

После удаления приложения необходимо вручную удалить группу DrWeb Admin в адресной книге сервера Lotus Domino (в базе данных `names.nsf` в каталоге `DATA` сервера) и документ `DrWebUpdate.bat`.

Чтобы удалить документ DrWebUpdate.bat

1. Запустите сервер Lotus Domino.
2. Запустите клиент Domino Administrator.
3. Откройте вкладку **Configuration**, затем выберите пункт **Programs** в категории **Server**.
4. Выберите документ **DrWebUpdate.bat** в правой части окна и удалите его.

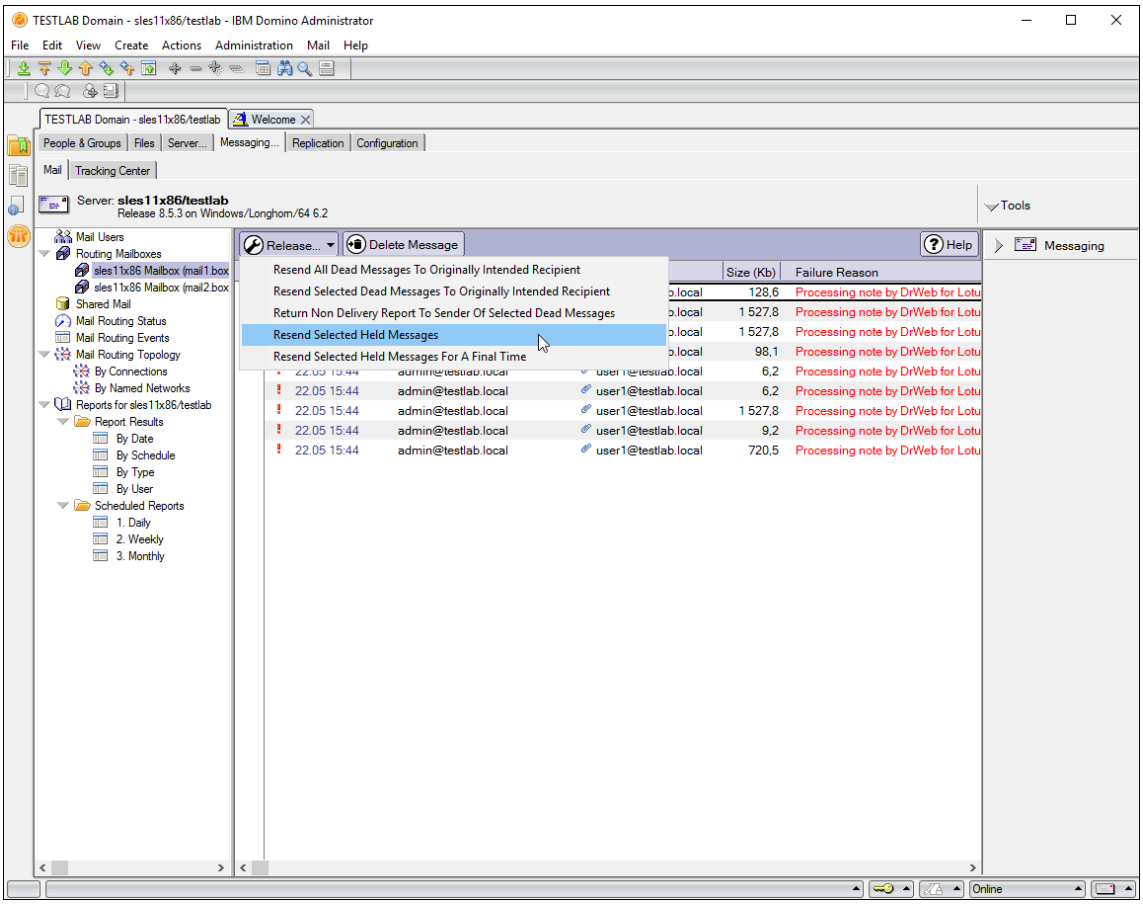
4.4.1. Действия после удаления

После удаления Dr.Web на сервере Lotus Domino могут остаться задержанные непроверенные письма. Это происходит из-за того, что антивирусное приложение присваивает всем письмам статус **HOLD** перед тем, как они подвергаются проверке.

Чтобы доставить задержанные 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 подключаемый модуль.

4. Откройте вкладку **Messaging**. Найдите в почтовых ящиках (пункт **Routing Mailboxes** в меню в левой части вкладки) письма с комментарием **Processing note by DrWeb for Lotus** в столбце **Failure Reason**.



Клиент Domino Administrator. Отправка задержанных писем

5. Выберите письма, задержанные антивирусным модулем, 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 модулем Dr.Web, т. к. он уже удален.

5. Подготовка к работе

5.1. Изменения в настройках сервера Lotus Domino

Во время установки Dr.Web в адресной книге (база данных `names.nsf`) сервера Lotus Domino автоматически создается группа DrWeb Admin. Эта группа указывается в *списке контроля доступа* (*Access Control List*) всех баз антивирусного модуля. В группу по умолчанию добавляется администратор сервера, указанный в файле `notes.ini` (параметр `Admin`). Администратор может добавлять других пользователей Lotus Domino в группу DrWeb Admin, которые могут исполнять обязанности администратора антивирусного модуля.

Удаление группы DrWeb Admin приведет к проблемам с уведомлениями и доступом к базам данных антивирусного модуля.

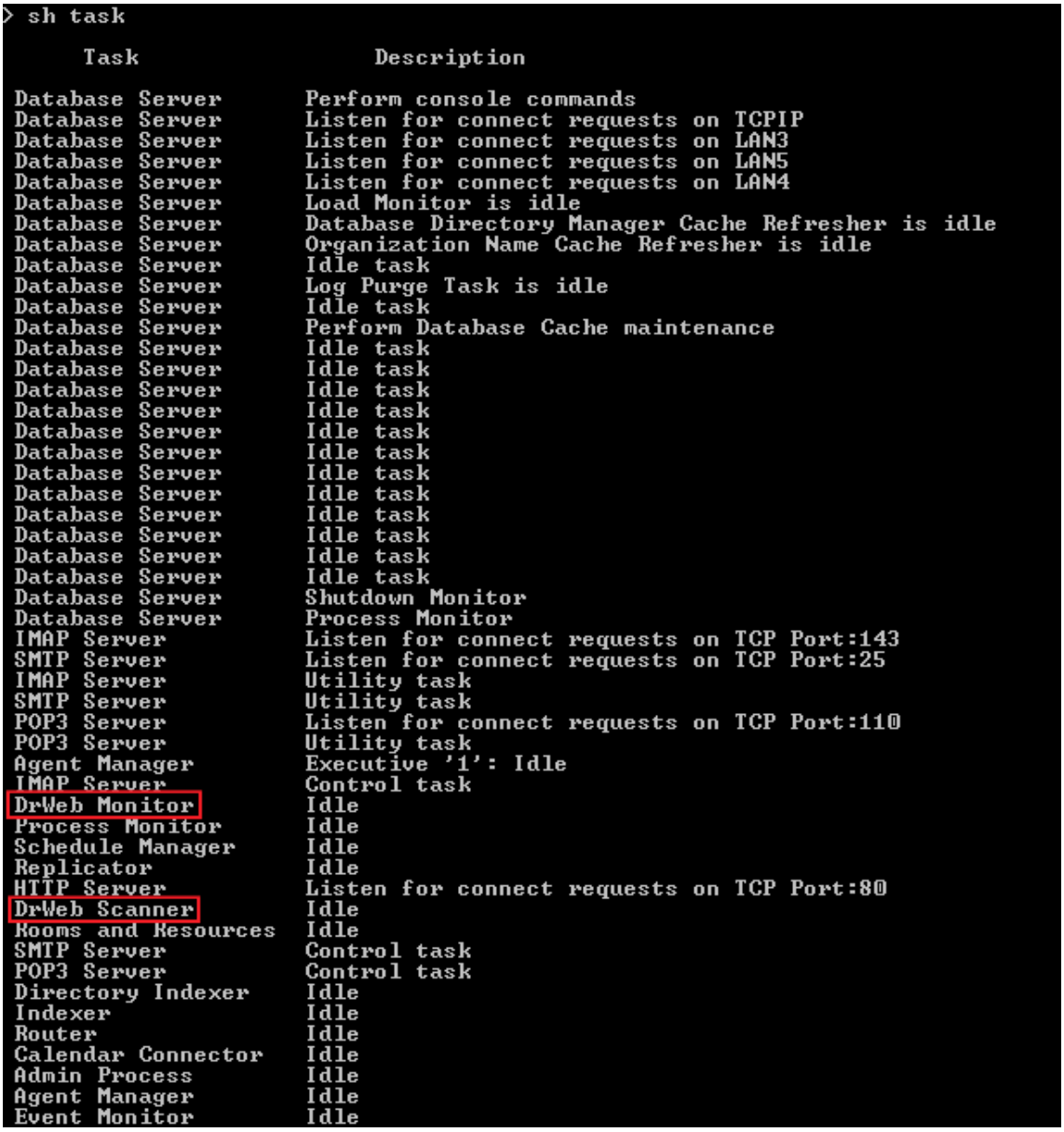
Также во время установки в файл `notes.ini` вносятся изменения:

- в параметр `EXTMGR_ADDINS` добавляется значение `ndrwebhook.dll`;
- в параметр `ServerTasks` добавляются задачи монитора и сканера (`monitor` и `scanner`);
- добавляются параметры `DrWebKey` и `DrWebBuild`, в которых указываются путь к ключевому файлу и полный номер сборки соответственно.

Если вы не хотите автоматически загружать антивирусные компоненты при запуске сервера Lotus Domino, то удалите значение `ndrwebhook.dll` в параметре `EXTMGR_ADDINS`, а также значения `monitor` и `scanner` в параметре `ServerTasks`.

5.2. Запуск сервера Lotus Domino

Если установка Dr.Web прошла успешно, запустите сервер Lotus Domino (`nserver.exe`). Чтобы убедиться, что компоненты Монитор и Сканер запущены, воспользуйтесь командой `sh task`.



Командное окно сервера Lotus Domino с корректно отработавшей командой sh task

5.3. Проверка детектирования вирусов

Для проверки конфигурации и способности Dr.Web 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, но определяется антивирусными программами как вирус. Вы можете загрузить тестовый файл с сайта EICAR (http://www.eicar.org) или создать его самостоятельно.

Чтобы создать тестовый файл EICAR

1. Создайте текстовый файл со строкой:

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

2. Сохраните файл с расширением `.com` (вы можете использовать любое имя, например, `eicar.com`), прикрепите его к 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 2016
Отправитель: admin@test.com
Получатели: mail21@perf2.test.com
Тема письма: Тестовое сообщение
Вирусы: eicar.com ( EICAR Test File (NOT a Virus!) ) отправлен в карантин
```

Обратите внимание, что нельзя использовать настоящие вирусы для проверки работоспособности антивирусных программ.

5.4. Проверка детектирования спама

Компонент Антиспам доступен только в версии «Антивирус + Антиспам», при наличии соответствующей лицензии.

Чтобы проверить способность Dr.Web обнаруживать спам, рекомендуется использовать письмо с тестовой строкой.

Чтобы создать тестовое письмо

1. В теме письма укажите `Test spam mail`.
2. Скопируйте в тело нового письма следующую строку:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

3. Отправьте письмо по протоколу SMTP на любой тестовый адрес.

Тестовое письмо не должно содержать вложений, подписей или другой информации, кроме темы и тестовой строки.

5.5. Запуск Консоли администратора

Настройка работы Dr.Web осуществляется посредством Консоли администратора. Консоль представляет собой графический интерфейс пользователя, 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 пикселей (см. Системные требования).

Для работы с веб-консолью на сервере Lotus Domino должна быть запущена задача сервера HTTP (*Hypertext Transfer Protocol*).

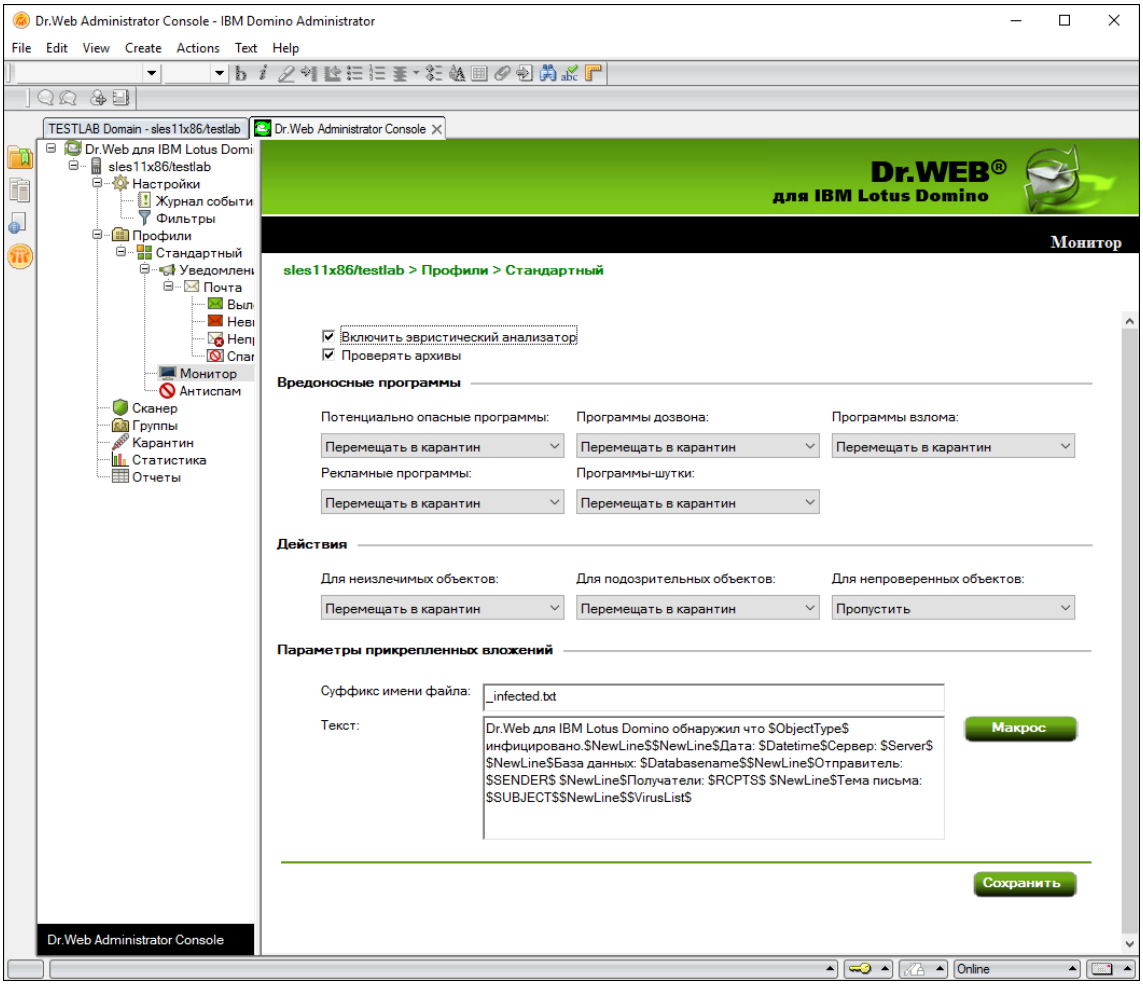
Чтобы запустить Консоль администратора в среде Lotus Notes

1. Запустите сервер Lotus Domino.
2. Запустите приложение Lotus Notes.
3. Откройте меню **File**, выберите пункт **Database** и нажмите **Open** (либо нажмите комбинацию клавиш CTRL+O на клавиатуре). Откроется окно **Open Database**.
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 каталоге `\DATA\DRWEB` и нажмите **Open**.

Чтобы запустить Консоль администратора в веб-браузере

1. Запустите сервер Lotus Domino.
2. Запустите веб-браузер.
3. Перейдите по 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. 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 находятся логотип антивирусного продукта и название выбранного раздела.



Консоль администратора

5.6. Получение справки

В продукте Dr.Web Mail Security Suite (IBM Lotus Domino Windows) реализована встроенная справочная система, которая устанавливается в виде отдельной базы `DrWebHelp.nsf` в каталоге `\DATA\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 сейчас), нажмите клавишу F1 на клавиатуре.

Чтобы получить справочную информацию о продукте, выберите раздел **Dr.Web для IBM Lotus Domino** в иерархическом меню Консоли администратора. В этом разделе собрана информация о версии продукта, ключевом файле, номерах версий программных компонентов и последнем обновлении вирусных баз. Эта информация необходима для анализа ошибок и сбоев при обращении в службу технической поддержки.

6. Администрирование

Чтобы упростить организацию антивирусной защиты для среды Lotus Domino, в Dr.Web реализована возможность создавать группы клиентов и присваивать им определенные профили. Профиль представляет собой набор настраиваемых параметров обработки сообщений, от которых зависит, как именно будет осуществляться защита среды Lotus Domino.

Настройки профилей находятся в разделе **Профили** иерархического меню, в котором для каждого профиля есть следующие подразделы:

- Уведомления — настройки уведомлений, 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 — управление работой вашего основного резидентного компонента для обнаружения вирусов;
- Антиспам — настройки работы компонента Антиспам (доступны только для версии «Антивирус + Антиспам», при наличии соответствующей лицензии).

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

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

6.1. Создание и настройка профилей

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

Во время установки Dr.Web создается **Стандартный** профиль. Этот профиль останется активным для всех клиентов сервера Lotus Domino до тех пор, пока для них 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

1. Выберите раздел **Профили** в иерархическом меню и нажмите кнопку **Добавить** под списком профилей в основном фрейме справа.
2. Введите имя профиля и нажмите кнопку **ОК**.

   Новый профиль отобразится внутри раздела **Профили** в иерархическом меню.

Чтобы изменить имя профиля

1. Выберите изменяемый профиль в иерархическом меню.
2. Введите новое значение в поле **Имя** и нажмите кнопку **Сохранить**.

> Для имени профиля не допускается использование символов «!», «/», «\», «|», «;», «:», «"», «*» и «,».

Параметры нового профиля будут совпадать с параметрами стандартного профиля.

Чтобы изменить параметры профиля

1. Выберите изменяемый профиль в иерархическом меню.
2. Настройте параметры в соответствующих подразделах (Уведомления, Монитор и Антиспам).

6.1.1. Настройка уведомлений

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

> По умолчанию все уведомления отключены.

Чтобы настроить почтовые уведомления

1. Выберите изменяемый профиль в иерархическом меню.
2. Перейдите в подраздел **Уведомления** и выберите пункт **Почта**.
3. Выберите тот тип 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.
4. Для каждого типа событий вы можете задать отдельные уведомления для администратора, получателя и отправителя письма. Для этого выберите соответствующую вкладку в верхней части основного фрейма.

5. Чтобы включить отправку уведомлений для определенного типа событий, установите флажок **Посылать уведомления по почте**.
6. При необходимости отредактируйте шаблон почтового уведомления в соответствующих полях.
7. Вы можете добавить макросы в текст уведомления, нажав кнопку **Макрос** и выбрав нужные из списка.
8. В поле **Отправитель** вы можете указать отправителя выбранного типа уведомлений.
9. Получателей определенного типа уведомлений можно настроить только на вкладке **Администратор**. Вы можете добавить пользователей, нажав кнопку **Добавить** и выбрав их в окне **Список адресов**.
10. Когда вы закончите редактировать параметры уведомлений, нажмите кнопку **Сохранить**.

6.1.2. 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

1. Выберите изменяемый профиль в иерархическом меню и перейдите в подраздел **Монитор**.

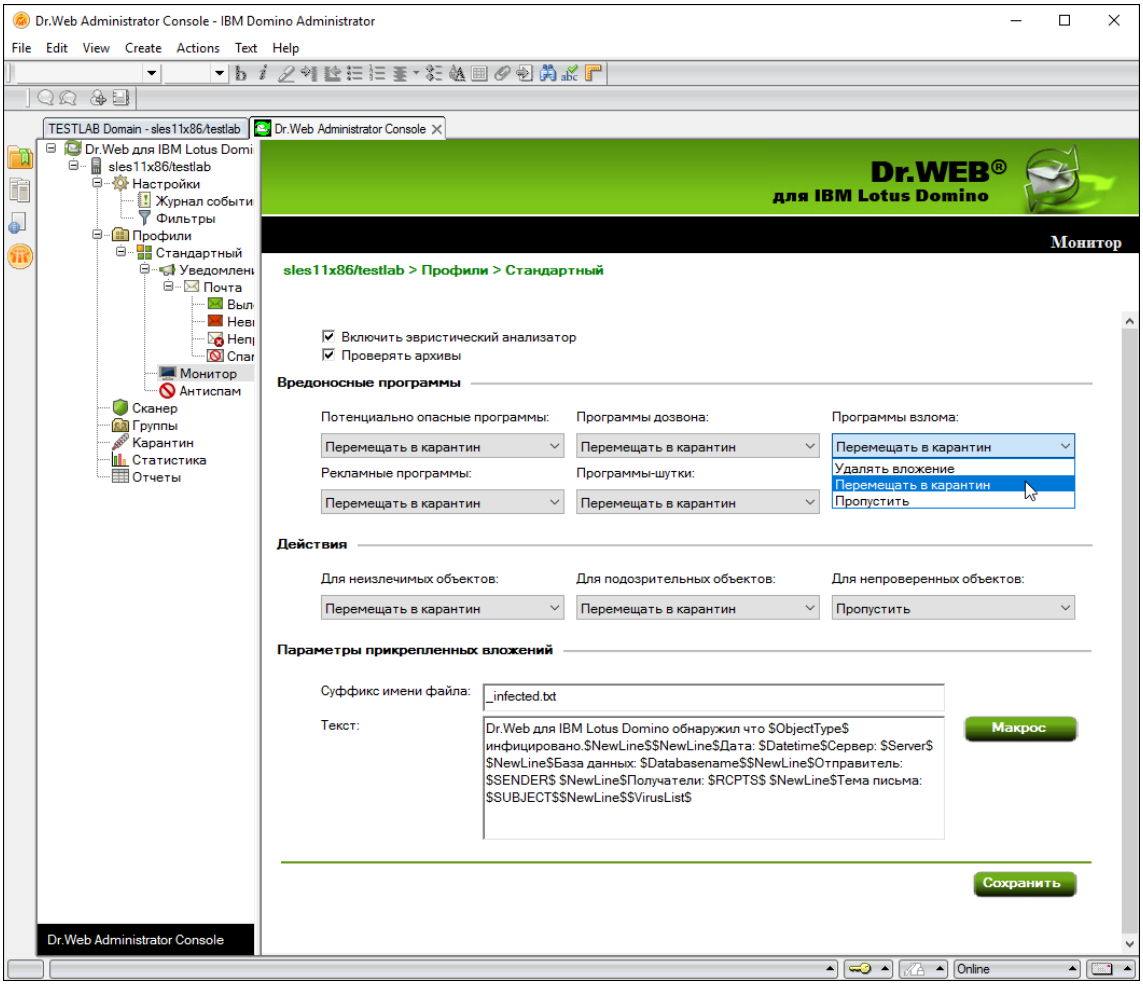
   По умолчанию эвристический анализатор и проверка архивов во вложениях включены, что обеспечивает высокий уровень защищенности за счет некоторого снижения производительности сервера. Чтобы отключить эти средства, снимите флажки **Включить эвристический анализатор** и **Проверять архивы** в верхней части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

   Настоятельно не рекомендуется отключать эвристический анализатор и проверку архивов во вложениях, поскольку это значительно снижает уровень защищенности сервера.

2. 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:
   - **Удалять 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 только для неизлечимых, подозрительных объектов и вредоносных программ).

- **Перемещать 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).



Фрейм Монитор. Выбор действий для вредоносных программ

3. В группе настроек **Параметры прикрепленных 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.
4. Чтобы добавить макрос в шаблон текстового файла, нажмите кнопку **Макрос** и выберите нужный из списка.
5. Когда вы закончите редактировать параметры работы Монитора, нажмите **Сохранить**.

6.1.3. Настройка Антиспама

Выявление спама осуществляется компонентом Антиспам. Компонент 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.

Если настройки в разделе **Антиспам** недоступны, скорее всего, ваш ключевой файл не поддерживает проверку на спам (см. Определение параметров лицензирования). Чтобы проверить это, откройте ключевой файл (`drweb32.key`) в текстовом редакторе и найдите строку: `LotusSpamFilter=No`.

Чтобы настроить работу компонента Антиспам

1. Убедитесь, что ваша версия программы поддерживает работу компонента Антиспам.
2. Выберите изменяемый профиль в иерархическом меню и перейдите в подраздел **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 добавлялся префикс, установите флажок **Изменить тему**. Вы можете изменить префикс в поле **Префикс темы** (по умолчанию `[СПАМ]`).
5. Кроме 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 **База данных** (если указанную базу не удастся найти, то сообщение будет доставлено получателю). Вы также можете указать папку внутри базы данных в поле **Название папки**, чтобы перемещать спам-сообщения в эту папку (если указанную папку не удастся найти в базе, то спам-сообщение все равно будет помещаться в эту базу данных, но без определенной папки).

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 подключаемым модулем поставляется база данных `DrWebSpam.nsf`, устанавливаемая в каталог `\DATA\DRWEB` 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. В Lotus Notes Client предоставляется также возможность доставки пользователю сообщения, ошибочно классифицированного как спам.

- **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 не будет совершено никакого действия над сообщением и оно будет доставлено получателю (тема сообщения все равно будет изменена, если установлен флажок **Изменить тему**).

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 nonspam@drweb.com, а спам, не распознанный системой, — на адрес spam@drweb.com. Все сообщения следует пересылать только в виде вложения, а не в теле письма.

6.2. Управление группами клиентов

По умолчанию Dr.Web применяет параметры профиля **Стандартный** ко всем пользователям. Если вы хотите 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 раздел **Группы** в иерархическом меню и нажмите кнопку **Добавить** под списком групп в основном фрейме справа.
2. Введите имя группы и нажмите кнопку **OK**.

   Новая группа отобразится внутри раздела **Группы** в иерархическом меню.

Чтобы изменить параметры группы

1. Выберите изменяемую группу в иерархическом меню и введите новое значение в поле **Имя**.

Для имени группы не допускается использование символов «!», «/», «\», «|», «;», «:», «"», «*» и «,».

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

7. Настройка работы приложения

7.1. Настройка фильтров

Фильтры используются для задания общих ограничений работы Dr.Web. Ограничения устанавливаются в подразделе **Фильтры** раздела **Настройки** иерархического меню. Подраздел **Фильтры** разделен на две вкладки.

- Вкладка **База данных** 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 подраздела **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 раздел **Настройки** в иерархическом меню и откройте подраздел **Фильтры**.
2. Нажмите кнопку **Импорт\Экспорт** в нижней части раздела.
3. Выберите тип 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.

7.1.1. Фильтр баз данных

Монитор — это компонент Dr.Web, который по умолчанию проверяет «на лету» все базы NSF, кроме некоторых служебных баз сервера Lotus Domino (см. В каких базах данных не производится проверка на вирусы?). При помощи списков **Включить** и **Исключить**, которые находятся во вкладке **База данных** подраздела **Фильтры** раздела **Настройки**, вы можете задать свои ограничения работы Монитора.

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

Чтобы настроить фильтр баз данных Lotus Domino

1. Выберите раздел **Настройки** в иерархическом меню и откройте подраздел **Фильтры**.
2. Выберите вкладку **База данных** и установите флажок **Включить** в верхней части вкладки.
3. Чтобы добавить базу в список:

   1.) Нажмите кнопку **Добавить** рядом с соответствующим списком:

   - **Включить** — список баз, которые являются обязательными к проверке Монитором (базы, не указанные в списке **Включить**, проверяться не будут).
   - **Исключить** — список баз, которые должны быть исключены из проверки Монитором (базы, не указанные в списке **Исключить**, будут проверяться).

   2.) Выберите базу в диалоговом окне.

   3.) Нажмите **ОК**.

   Вы также можете добавлять в списки шаблоны путей, т. е. пути к каталогам с необходимыми базами, оканчивающиеся следующей комбинацией символов `*.nsf`. Например, если вы укажете путь `mail\*.nsf`, то в список будут добавлены все базы NSF в каталоге `\DATA\mail` сервера (базы в подкаталогах добавлены не будут).

4. Чтобы удалить базу из списка, выберите ее и нажмите **Удалить**.
5. Чтобы очистить список, нажмите **Очистить**.
6. Когда вы закончите составлять список, нажмите **Сохранить**. При этом изменения вступят в силу через 1 минуту после сохранения.

7.1.2. Черный и белый списки адресов

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

Чтобы сформировать списки адресов

1. Чтобы добавить адрес в список:

   1.) Установите флажок **Включить**.

   2.) Введите адрес или имя домена в поле под соответствующим списком.

   3.) Нажмите **Добавить**.

   Письма с адресов, добавленных в белый список, не проверяются на наличие спама. Письма с адресов, добавленных в черный список, без проверки получают статус *Точно спам*, после чего к ним применяются действия, которые настроены в разделе **Антиспам** для писем с таким статусом.

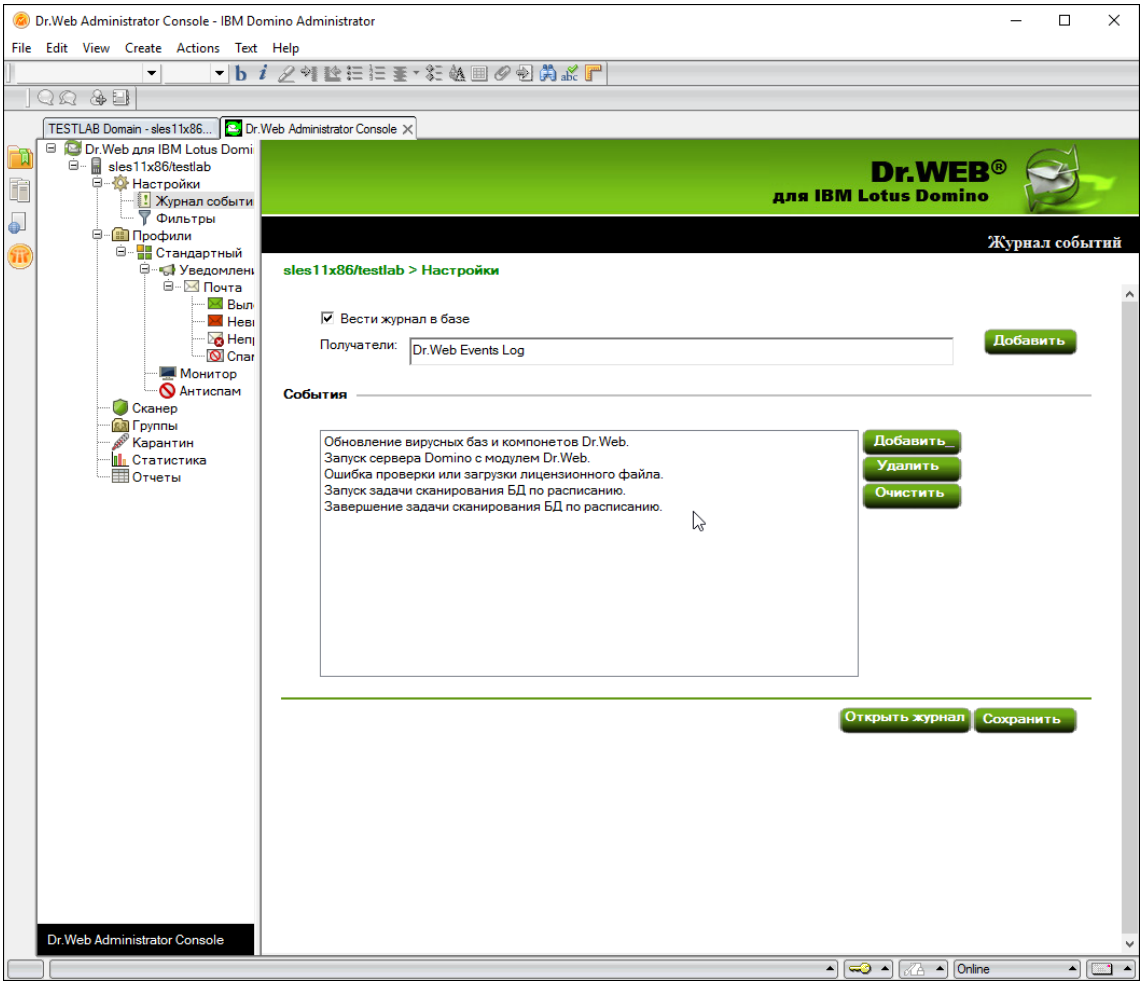
При добавлении адресов и имен доменов вы можете задавать их в виде шаблонов. Для этого вы можете пользоваться символом «*». Шаблоны позволяют задавать диапазон электронных адресов или доменов (например, запись `*@mail.com` означает любой адрес из домена `mail.com`).

Шаблоны вида `admin@*.com`, `*@*.com` работать не будут.

2. Чтобы удалить адрес из списка, выберите его и нажмите **Удалить**.
3. Чтобы очистить список, нажмите **Очистить**.
4. Когда вы закончите составлять списки, нажмите **Сохранить**. При этом изменения вступят в силу через 1 минуту после сохранения.

7.2. Ведение Журнала Событий

Журнал событий может использоваться сетевыми администраторами для контроля событий, происходящих в ходе работы Dr.Web (особенно полезен, если в сети работает более одного сервера Lotus Domino). В подразделе **Журнал событий** (в разделе **Настройки** иерархического меню) вы можете выбрать события, информация о которых будет записываться в журнал, а также базу данных, в которой эта информация будет храниться.



Консоль администратора. Фрейм Журнал событий

Чтобы настроить ведение Журнала событий

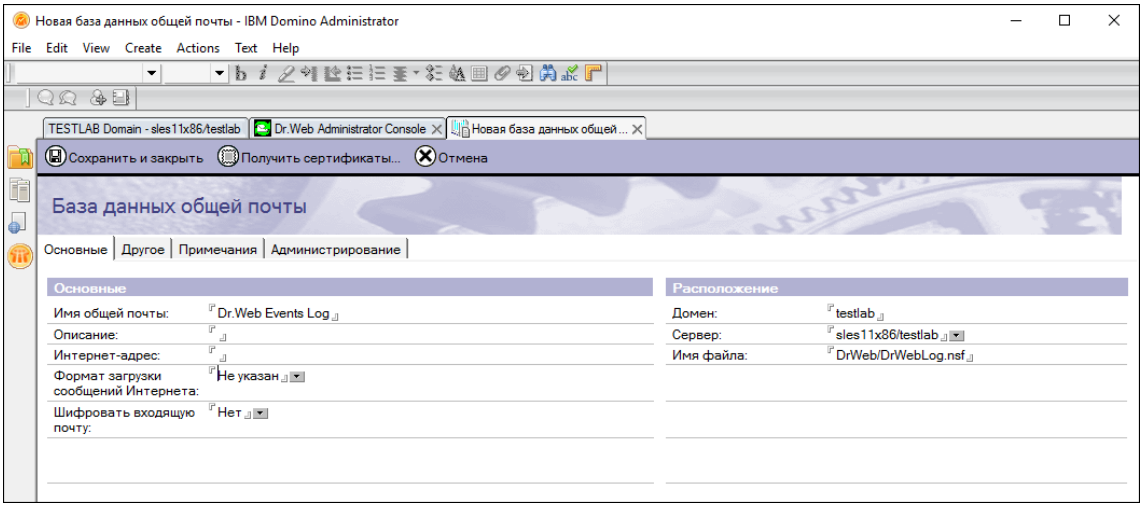
1. Выберите раздел **Настройки** в иерархическом меню и откройте подраздел **Журнал событий**.
2. Установите флажок **Вести журнал в базе**.
3. Вы можете указать почтовый адрес баз NSF, в которые будет записываться информация, добавляя их в поле **Получатели** при помощи кнопки **Добавить**. До этого необходимо задать почтовый адрес для желаемой базы данных:

   1.) Запустите клиент Domino Administrator и выберите сервер.

   2.) Откройте вкладку **People and Groups**, выберите пункт **Mail-In databases and resources** и нажмите кнопку **Add Mail-In Database**.

   3.) Выберите имя базы данных, укажите почтовый домен и сервер.

   4.) В поле **Имя файла** укажите `DRWEB/DrWebLog.nsf`.



Клиент Domino Administrator. Новая база данных общей почты

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

4. В группе настроек **События** сформируйте список событий, информация о которых должна попадать в журнал.
   - Кнопки **Добавить** и **Удалить** позволяют редактировать состав списка событий.
   - Нажатие кнопки **Очистить** удалит из списка все события.
5. Нажмите **Сохранить**, чтобы применить внесенные изменения.

7.3. Экспорт/импорт конфигураций

В приложении Dr.Web предусмотрена возможность сохранять текущую конфигурацию в файл для 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 **Действия** 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 **Действия** 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 настройки добавлены. Например, если на сервере есть 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**).

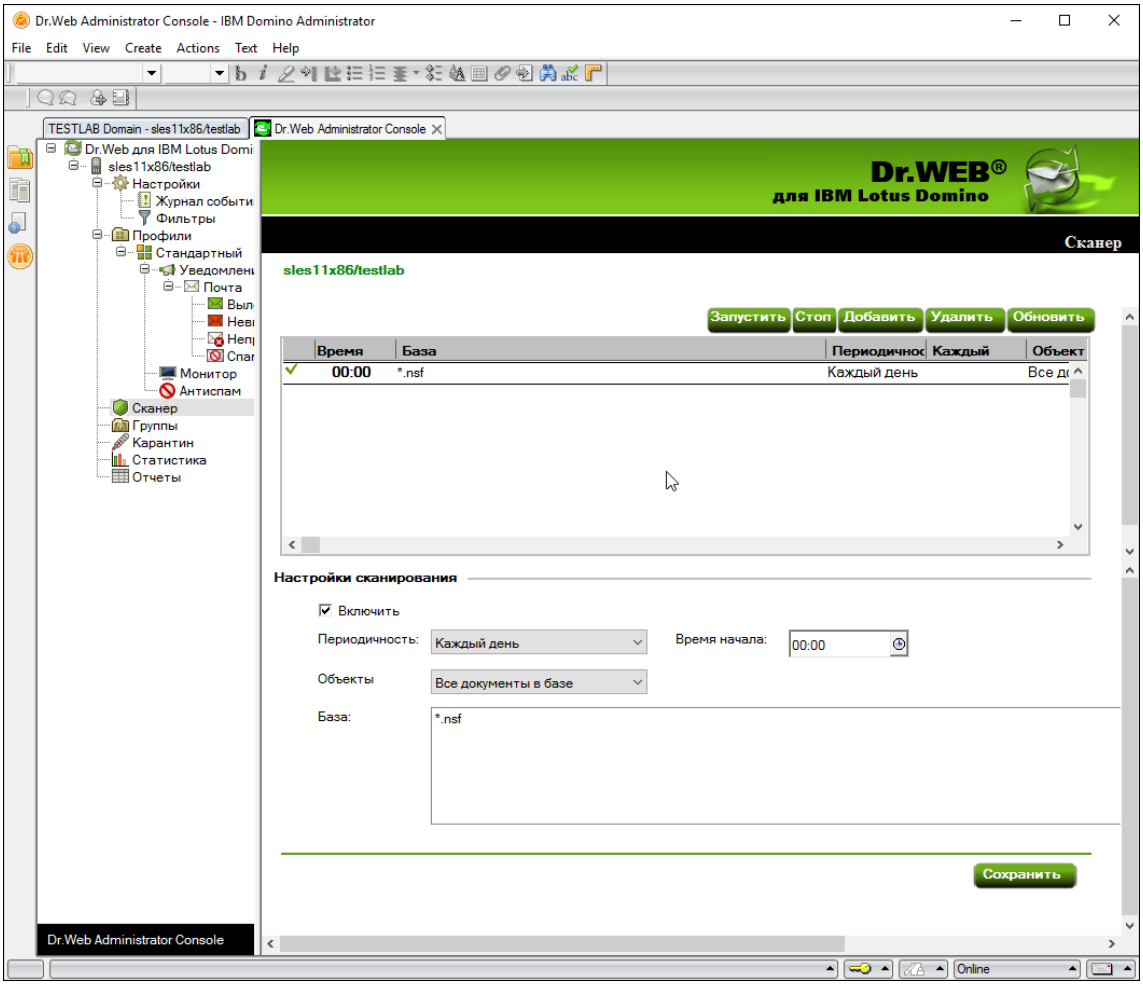
8. Антивирусная проверка

8.1. Проверка баз данных Lotus Domino

В приложении Dr.Web реализована антивирусная проверка документов в выбранных базах NSF по расписанию. Расписание состоит из заданий, которые определяют периодичность, день и время начала проверки, а также те базы, которые необходимо проверить.

Чтобы создать задание на антивирусную проверку

1. Выберите раздел **Сканер** в иерархическом меню и нажмите кнопку **Добавить** над списком заданий в верхней половине фрейма **Сканер**. В списке появится новое неактивное задание со значениями по умолчанию.



Консоль администратора. Фрейм Сканер

2. Выберите созданное задание и укажите для него параметры периодичности, дня и времени начала проверки (нижняя часть фрейма **Сканер**).

3. С помощью кнопки **Добавить** внесите в список базы, документы в которых вы хотите проверить. Для каждого каталога вы можете как выбрать отдельные базы, так и добавить в список все базы из этого каталога, выбрав пункт ***.nsf**.
4. В выпадающем меню **Объекты** вы можете выбрать проверку всех документов в указанных базах или только тех, которые были созданы или изменены с момента последней антивирусной проверки (т. е. выполнять инкрементальную проверку, при которой 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 инкрементальной проверке, если только он не будет изменен. Поэтому рекомендуется регулярно обновлять вирусные базы и производить полную ручную проверку (не реже, чем раз в неделю).

5. 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.

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

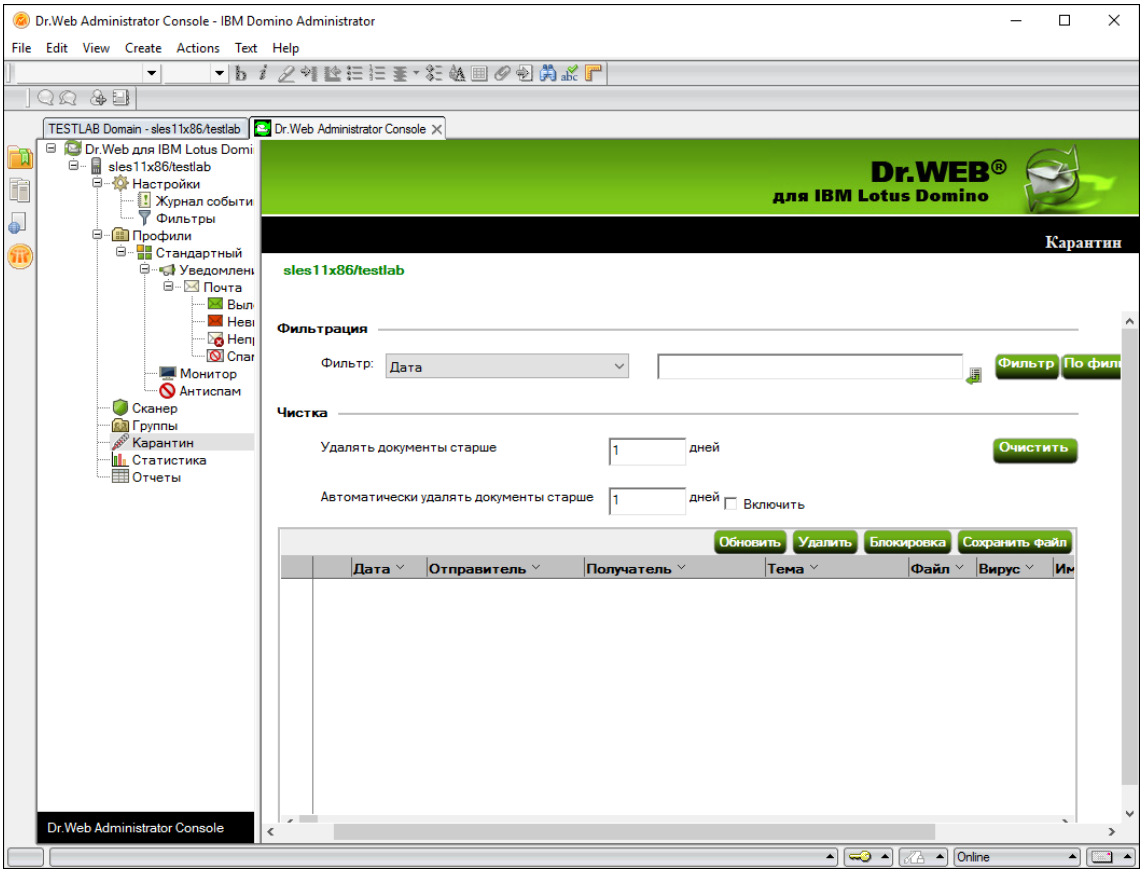
Администратор Lotus Domino может устанавливать квоту на размер каждой базы для конкретного пользователя. Если подключаемый модуль проверяет базу, у которой превышена эта квота, и обнаруживает угрозу, это событие заносится в базу данных DrWebLog и журнал Сканера, но никакие действия к зараженному объекту не применяются.

Когда вы закончите настраивать задания на антивирусную проверку, нажмите кнопку **Сохранить**.

8.2. 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 **Перемещать в карантин**.

Фрейм раздела **Карантин** содержит список объектов, находящихся в карантине, и ряд настроек для управления этим списком и документами в базе `Quarantine.nsf`. Чтобы отсортировать список согласно определенному критерию, нажмите заголовок соответствующего столбца таблицы.



Консоль администратора. Фрейм Карантин

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 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 дольше определенного количества дней.

Чтобы почистить список

1. Задайте количество дней в поле **Удалять документы старше**.

2. Нажмите кнопку **Очистить**.

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

Чтобы удалять старые объекты автоматически

1. Задайте количество дней в поле **Автоматически удалять документы старше**.
2. Установите флажок **Включить**.

Автоматическое удаление документов из Карантина выполняет агент Automatically delete objects в базе `Quarantine.nsf`. По умолчанию этот агент запускается на сервере ежедневно 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 базы Карантина

1. Выберите документ из списка.
2. 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 каталог, в который вы хотите сохранить объект, и нажмите кнопку **ОК**.

Чтобы запретить удаление документа из Карантина

1. Выберите документ в списке.
2. Нажмите кнопку **Блокировка**.

   Повторное нажатие снимет блокировку удаления с выбранного документа.

Список файлов в Карантине обновляется автоматически каждые 12 часов, но вы можете обновить список вручную в любое время, нажав кнопку **Обновить**.

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

Нажмите кнопку **Сохранить** под списком для сохранения изменений во фрейме **Карантин**.

8.3. Просмотр статистики

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

- Вкладка **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).
- Вкладка **Инциденты** содержит список документов, в которых записывается информация о событиях в работе антивирусного приложения (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 документы

1. Выберите тип фильтра в выпадающем меню **Фильтр** и укажите значение для этого фильтра в поле 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 документ из списка инцидентов

1. Выберите документ в списке.
2. Нажмите кнопку **Удалить**.

Чтобы удалить старые документы из списка инцидентов

1. Задайте количество дней в группе настроек **Чистка**.
2. Нажмите кнопку **Очистить**.

В группе настроек **Чистка** вы также можете задать количество дней для автоматического удаления объектов, которые находились в Карантине дольше определенного количества дней. Автоматическое удаление выполняет агент Automatically delete objects в базе `Quarantine.nsf`. По умолчанию этот агент запускается на сервере ежедневно в 01:30. Вы можете изменить параметры его запуска, используя стандартные средства Lotus Domino (см. документацию IBM Lotus Domino).

Чтобы запретить удаление документа из списка

1. Выберите документ в списке.
2. Нажмите кнопку **Блокировка**.

   Повторное нажатие снимет блокировку удаления с выбранного документа.

Список автоматически обновляется каждые 12 часов, но вы можете обновить список вручную в любое время, нажав кнопку **Обновить**.

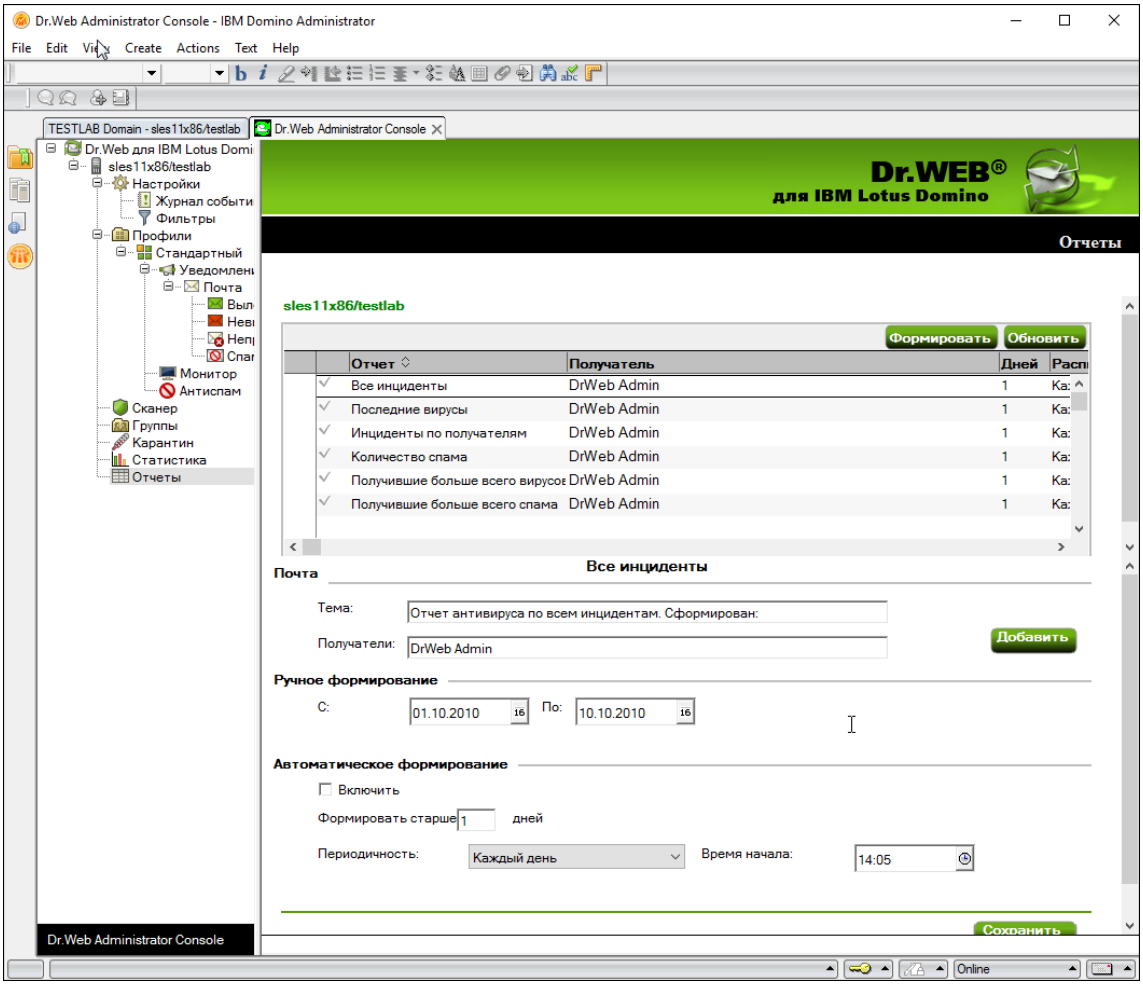
Процесс обновления может занять некоторое время (до нескольких минут) в зависимости от количества объектов в базе инцидентов.

Нажмите кнопку **Сохранить** под списком для сохранения изменений во фрейме **Статистика**.

9. Управление отчетами

В приложении Dr.Web реализована возможность создавать отчеты о работе антивирусного модуля и отправлять их на указанные адреса в виде файлов в формате HTML, приложенных к письму. Отчеты основаны на списке документов во вкладке **Инциденты** раздела **Статистика**.

Рассылку отчетов вы можете настроить в разделе **Отчеты**.



Консоль администратора. Фрейм Отчеты

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 клиента, нескольких клиентов или группу клиентов сервера Lotus Domino. Нажмите кнопку **Добавить** и выберите получателей в открывшемся диалоговом окне.

В группе настроек **Ручное формирование** вы можете настроить даты инцидентов, для которых требуется 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 до текущей даты, для которых вы хотите генерировать отчеты (т. е. если указать «1», то в отчет будут включены только вчерашние инциденты; «2» — инциденты за последние 2 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**.

10. Обновление вирусных баз

Для обнаружения вредоносных объектов Dr.Web использует специальные вирусные базы, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вредоносные программы, то эти базы требуют периодического обновления. Вирусные базы считаются устаревшими по истечении 24 часов с момента последнего успешного обновления.

Обновление вирусных баз Dr.Web реализовано посредством Модуля обновления, который запускается по расписанию, заданному в документе `drwebupdate.bat`. Данный документ создается в каталоге `Domino` адресной книги сервера во время установки. По умолчанию Модуль обновления запускается каждые 30 минут. Документ `drwebupdate.bat` можно изменить посредством клиента Domino Administrator.

Чтобы изменить расписание обновлений

1. Запустите сервер Lotus Domino.
2. Запустите клиент Domino Administrator.
3. Перейдите на вкладку **Configuration** и выберите пункт **Server** в иерархическом меню слева.
4. Выберите пункт **Programs** в открывшемся подменю и затем программу **drwebupdate.bat** в списке.
5. Нажмите кнопку **Edit Program** в верхней части окна и внесите необходимые изменения.

Модуль обновления можно запустить вручную в режиме командной строки, для этого необходимо запустить файл `drwebupdate.bat`. При запуске в режиме командной строки вы можете задавать дополнительные параметры (см. Настройка параметров обновления).

Если вы используете прокси-сервер, то дополнительно настройте Модуль обновления на работу через прокси-сервер. Для этого добавьте соответствующие параметры в `drwebupdate.bat` (см. Настройка параметров обновления).

10.1. Настройка параметров обновления

Для настройки обновления вирусных баз и компонентов Dr.Web доступен файл `C:\Program Files\DrWeb for Lotus Domino\drwebupdate.bat`.

Команда `-c update` выполняет обновление вирусных баз и компонентов антивирусного приложения. Чтобы установить настройки обновления, укажите необходимые параметры для команд `-c update`.

Параметры команды –c update

Параметр	Описание
`--type=update-revision`	Тип обновления `update-revision` — обновлять текущие ревизии компонентов, если есть различия между зоной и локальным репозиторием.
`--disable-postupdate`	Последующее обновление выполняться не будет. Работа модуля обновления будет завершена после выполнения обновления.
`--verbosity=arg`	Уровень детализации журнала: • `error` — стандартный; • `info` — расширенный; • `debug` — отладочный.
`--interactive`	Если параметр указан, при выполнении некоторых команд будет задействовано большее количество ресурсов.
`-p [ --product ] arg`	Применить только к данному продукту. Если параметр указан, будут обновлены все компоненты данного продукта. Если параметр опущен, будут обновлены все продукты, доступные для обновления.
`-g [ --proxy ] agr`	Прокси-сервер для обновления в формате <*адрес*>: <*порт*>
`-u [ --user ] agr`	Имя пользователя прокси-сервера
`-k [ --password ] arg`	Пароль пользователя прокси-сервера

Пример команды `-c update` для обновления вирусных баз через прокси-сервер:

```
-c update --type=update-revision --disable-postupdate --verbosity=debug
```

```
--interactive -p BasesForLotusPlugin -p AntispamForLotusPlugin -p LotusSetup
```

```
--proxy=192.168.134.128:808 --user=qwerty --password=qwerty
```

11. Работа в режиме централизованной защиты

Dr.Web 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 конечных пользователей.

Взаимодействие компонентов антивирусной сети

Решения компании «Доктор Веб» по организации централизованной антивирусной защиты основаны на *клиент-серверной архитектуре*.

Компьютеры компании или пользователей поставщика услуг в сфере информационных технологий защищаются от угроз безопасности и спама *локальными антивирусными компонентами* (клиентами), которые обеспечивают антивирусную защиту и упрощают подключение к серверу централизованной защиты.

Обновление и конфигурация локальных компонентов производятся 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.

Dr.Web в режиме централизованной защиты

Для работы подключаемого антивирусного модуля в режиме централизованной защиты необходимо, чтобы в операционной системе был установлен и корректно работал Агент Dr.Web.

В режиме централизованной защиты реализованы следующие возможности работы Dr.Web:

- 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 подключаемого антивирусного модуля. 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 указателя (*URL*) на веб-консоль администратора Dr.Web в Центр Управления Dr.Web. Это позволяет в консоли Центра Управления Dr.Web видеть URL на консоль управления подключаемым антивирусным модулем 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;
- обновление вирусных баз, антивирусного ядра и баз 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, зарегистрированного для данной станции в сети Центра Управления Dr.Web. Чтобы включить эту функцию, необходимо во время установки на 5 шаге выбрать **Использовать лицензионный ключ Центра Управления Dr.Web**.

Если подключаемый антивирусный модуль установлен в режиме **Enterprise**, в файл `notes.ini` будет добавлена запись `DrWebEdition=Enterprise`.

Dr.Web в режиме **Enterprise** не будет использовать локальный ключевой файл, указанный при установке приложения и заданный в файле `notes.ini` параметром `DrWebKey`. В режиме **Enterprise** делается запрос права на антивирусную проверку у Центра Управления Dr.Web и, если такая проверка запрещена, подключаемый антивирусный модуль не будет ее выполнять.

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

- В консоли сервера выполните команду:

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

Передача значения в Центр Управления Dr.Web выполнится в течение минуты.

12. Часто задаваемые вопросы

В данном разделе описаны наиболее частые вопросы и ответы, проблемы и их решения, а также дополнительная информация, которая может быть полезной при работе с приложением Dr.Web.

12.1. Что делать при возникновении ошибок?

При возникновении ошибок или в случае аварийного завершения работы сервера Lotus Domino после установки или в процессе работы Dr.Web необходимо убедиться, что это вызвано именно приложением. Для этого либо удалите приложение, либо отключите загрузку его компонентов (см. Как отключить проверку на вирусы?). После этого подключаемый модуль не должен оказывать на работу сервера Lotus Domino никакого влияния. И если сервер продолжает работать нестабильно, то ошибки в его работе не могут быть вызваны приложением. Но если ошибки в работе сервера вызывает Dr.Web, то необходимо собрать как можно больше информации перед обращением в службу технической поддержки.

Чтобы собрать всю необходимую информацию

1. Установите приложение Dr.Web, если оно было удалено.
2. Отключите загрузку компонентов подключаемого модуля (см. Как отключить проверку на вирусы?).
3. Откройте конфигурационный файл `notes.ini` сервера Lotus Domino.
4. Добавьте в файл `notes.ini` параметр `DrWebDebugLog=5`. Закройте файл, сохранив изменения.
5. Запустите сервер Lotus Domino.

6. Откройте окно консоли сервера Lotus Domino. Запустите команду `sh server` и сохраните ее результат.
7. Убедитесь, что на сервере включен запуск NSD (*Notes System Diagnostics*):
   1.) Запустите клиент Domino Administrator и откройте вкладку **Configuration**.
   2.) Выберите **Server** → **Current server document** → **Basics** → **Fault Recovery**.
   3.) Убедитесь, что параметр **Run NSD To Collect Diagnostic Information** включен.
8. Остановите сервер Lotus Domino.
9. Включите загрузку компонентов подключаемого модуля (см. Как отключить проверку на вирусы?).
10. Запустите сервер Lotus Domino.
11. Постарайтесь максимально точно воспроизвести все действия, которые привели к возникновению ошибок или аварийному завершению работы сервера.

При обращении в службу технической поддержки по вопросам возникновения ошибок или аварийного завершения работы сервера, вызванного подключаемым антивирусным модулем, необходимо предоставить следующую информацию:

- несколько последних журналов NSD (они сохраняются в каталог `\Lotus\Domino\DATA\IBM_TECHNICAL_SUPPORT\` при каждом аварийном завершении работы сервера Lotus Domino);
- журналы работы подключаемого модуля (они сохраняются в каталог `\Lotus\Domino\DATA\DRWEB\Log`);
- информацию, выдаваемую консолью сервера в результате выполнения команды `sh server`;
- разделы **Система** и **Приложения** (желательно в формате `.evt`) из журнала событий Windows (Event Viewer);
- информацию об операционной системе. Чтобы сохранить информацию о системе:
  1.) Нажмите **Пуск** → **Выполнить**.
  2.) Введите `msinfo32` и нажмите **ОК**.
  3.) Нажмите **Файл** → **Сохранить** и сохраните информацию о системе в файл с расширением NFO.
- версии компонентов подключаемого модуля: Монитора, Сканера, Антиспама, Hook и Scan Client. Эту информацию можно найти:
  - в разделе **О Dr.Web для IBM Lotus Domino**, который открывается через верхний пункт иерархического меню Консоли администратора;
  - в консоли сервера Domino при его запуске;
  - вручную посмотрев версии файлов `ndrwebhook.dll`, `ndrwebscanner.exe`, `ndrwebmonitor.exe`, `vrcpp.dll` и `dwenine.exe`, используя проводник Windows. Расположение файлов см. в разделе Проверка корректности установки.

Всю необходимую информацию приложите к запросу в службу технической поддержки компании «Доктор Веб».

12.2. Почему не открываются некоторые базы данных?

Базы данных `Quarantine.nsf`, `DrWebReports.nsf` и `DrWebDesign.nsf` являются служебными и не предусматривают возможность работы с ними с помощью клиента Lotus Notes. Доступ к этим базам осуществляется модулем через интерфейс базы Консоли Администратора (`DrWebAdmin.nsf`).

12.3. Почему не работает Антиспам?

Если Dr.Web не выявляет спам и настройки Антиспама недоступны, скорее всего, ваш ключевой файл не поддерживает проверку на спам (см. Определение параметров лицензирования). Чтобы проверить это, в текстовом редакторе откройте ключевой файл `C:\Program Files\DrWeb for Lotus Domino\drweb32.key` и найдите строку: `LotusSpamFilter=No`.

Если в ключевом файле указано `LotusSpamFilter=Yes`, то файл должен поддерживать работу Антиспама. В этом случае обратитесь в службу технической поддержки компании «Доктор Веб».

12.4. Что делать, если задача AMgr выдает ошибку?

Если служебные базы данных Dr.Web (`Quarantine.nsf` и `DrWebReports.nsf`) не были подписаны учетной записью сервера, то их агенты не смогут выполнять автоматическую очистку инцидентов и объектов в Карантине, а также автоматическое формирование отчетов. В этом случае на консоли сервера Lotus Domino периодически (каждые 5 минут) будет появляться сообщение об ошибке примерно следующего содержания:

```
AMgr: Error executing agent 'GenerateToScheduleReport' in
'drweb\DrWebReports.nsf': Note item not found
```

В разделе Действия после установки указано, что вам необходимо сделать, чтобы подписать базы.

12.5. Как отключить проверку на вирусы?

Чтобы отключить проверку на вирусы без удаления приложения Dr.Web, необходимо отключить загрузку его антивирусных компонентов: Монитора и Сканера.

Чтобы отключить загрузку компонентов

1. Откройте файл `notes.ini` сервера Lotus Domino, на котором установлено антивирусное приложение.
2. Удалите задачи `monitor` и `scanner` из параметра `ServerTasks`.
3. Удалите значение `ndrwebhook.dll` из параметра `EXTMGR_ADDINS`.

4. Запустите сервер или перезагрузите его, если он был запущен.

Чтобы включить загрузку компонентов

1. Откройте файл `notes.ini` сервера Lotus Domino, на котором установлено антивирусное приложение.
2. Добавьте задачи `monitor` и `scanner` в параметр `ServerTasks`.
3. Добавьте значение `ndrwebhook.dll` в параметр `EXTMGR_ADDINS`.
4. Запустите сервер или перезагрузите его, если он был запущен.

12.6. В каких базах данных не производится проверка на вирусы?

Некоторые служебные базы данных сервера Lotus Domino не проверяются в режиме реального времени, т. к. обращение к ним происходит слишком часто, их проверка может привести к возникновению большой нагрузки на сервер.

Ниже приведен список таких служебных баз NSF:

- `drweb\Quarantine.nsf`,
- `drweb\DrWebDesign.nsf`,
- `drweb\DrWebAdmin.nsf`,
- `drweb\DrWebReports.nsf`,
- `admin4.nsf`,
- `events4.nsf`,
- `log.nsf`,
- `catalog.nsf`,
- `webadmin.nsf`,
- `dbdirman.nsf`,
- `names.nsf`,
- `certlog.nsf`,
- `cldbdir.nsf`,
- `namagent.nsf`,
- `reports.nsf`,
- `schema.nsf`,
- `activity.nsf`,
- `AgentRunner.nsf`,
- `busytime.nsf`,
- `certsrv.nsf`,

- `dba4.nsf`,
- `doladmin.nsf`,
- `lndfr.nsf`,
- `statrep.nsf`.

12.7. Как менять настройки антивируса через веб-интерфейс?

В приложении Dr.Web реализована возможность изменять настройки антивирусного модуля через веб-браузер, используя HTTP-сервер Lotus Domino.

Чтобы запустить Консоль администратора в веб-браузере

1. Запустите сервер Lotus Domino.

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

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

12.8. Какие файлы обновляются с помощью Модуля обновления?

Модуль обновления в составе Dr.Web загружает и обновляет следующие компоненты:

- вирусные базы (`*.vdb`),
- ядро компонента Антиспам (`vrcpp.dll`),
- антивирусное ядро (`drweb32.dll`),
- сам модуль обновления (`drwebupw.exe`).

Не обновляются компоненты:

- дизайн служебных баз NSF (`DrWebAdmin.nsf`, `Quarantine.nsf`, `DrWebReports.nsf` и `DrWebDesign.nsf`);
- бинарные файлы задач антивирусного модуля (`ndrwebhook.dll`, `ndrwebscanner.exe` и `ndrwebmonitor.exe`).

12.9. Какие бывают виды репликации?

Два основных вида репликации

- PULL (вытягивание) — сервер, инициировавший репликацию, загружает с удаленного сервера обновленные документы.
- PUSH (выталкивание) — сервер, инициировавший репликацию, отсылает обновленные документы на удаленный сервер.

Если приложение Dr.Web установлено на обоих серверах, участвующих в репликации, то обнаружение вирусов и лечение документов происходит без проблем, но следует учитывать особенности работы антивирусного модуля в условиях, когда защищен только один из серверов:

Действие	**Задача, выполняющая репликацию и проверку на вирусы**	**Комментарии**
Защищенный сервер осуществляет PUSH-репликацию на незащищенный	replica	Если зараженное вложение находится на защищенном сервере, то оно будет обезврежено в процессе репликации, т. е. на незащищенный сервер будет отправлен «чистый» документ. На защищенном сервере вложение НЕ будет обезврежено, даже после повторной репликации.
Незащищенный сервер осуществляет PUSH-репликацию на защищенный	nserver	При первой репликации защищенный сервер обнаруживает вирусы в полученных документах. При повторной репликации обезвреженные документы реплицируются на незащищенный сервер.
Защищенный сервер осуществляет PULL-репликацию с незащищенного	replica	Защищенный сервер обнаруживает вирусы в загружаемых документах и сохраняет обезвреженные документы. На незащищенном остаются зараженные документы, которые не обновляются при последующих репликациях.
Незащищенный сервер осуществляет PULL-репликацию с защищенного	nserver	Если на защищенном сервере будет обнаружено зараженное вложение, процесс репликации будет прерван. На защищенном сервере вложение будет вылечено. Обезвреженный документ будет загружен при повторной репликации.

13. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. Посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

1. Заполните веб-форму в соответствующей секции раздела https://support.drweb.com/.
2. Позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.