



Dr.WEB®

для IBM Lotus Domino

Защити созданное

Руководство администратора

© "Доктор Веб", 2012. Все права защищены.

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

ТОРГОВЫЕ ЗНАКИ

Dr.Web и логотипы Dr.WEB являются зарегистрированными товарными знаками «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

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

**Dr.Web для IBM Lotus Domino для Windows
Версия 6.00.2
Руководство администратора
15.02.2012**

"Доктор Веб", Центральный офис в России
125124
Россия, Москва
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: www.drweb.com
Телефон: +7 (495) 789-45-87

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

«Доктор Веб»

«Доктор Веб» - российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

Условные обозначения и сокращения	7
Глава 1. Введение	9
Назначение Dr.Web для IBM Lotus Domino	9
Проверяемые объекты	11
Лицензионный ключевой файл	12
Глава 2. Установка и удаление	14
Системные требования	15
Установка Dr.Web для IBM Lotus Domino	17
<i>Действия после установки</i>	19
Удаление Dr.Web для IBM Lotus Domino	20
<i>Действия после удаления</i>	21
Глава 3. Приступая к работе	23
Проверка работоспособности	23
Файлы и папки, создаваемые при установке	24
Изменения в настройках сервера Lotus Domino	26
Запуск сервера Lotus Domino	27
Проверка детектирования вирусов	28
Проверка детектирования спама	29
Запуск Консоли администратора	30
Получение справки	32
Глава 4. Администрирование	33
Компоненты программы	33
Группы и профили	36



Создание и настройка профилей	37
Настройка уведомлений	38
Настройка Монитора	40
Настройка Антиспама	42
Управление группами клиентов	45
Проверка баз данных Lotus Domino	46
Управление Карантином	49
Просмотр статистики	52
Управление отчетами	54
Ведение Журнала Событий	57
Настройка фильтров баз данных и электронных адресов	59
Фильтр баз данных	60
Черный и белый списки электронных адресов	62
Обновление вирусных баз	63
Экспорт/импорт конфигураций	65
Приложения	67
Приложение А. Параметры командной строки для модуля обновления	67
Приложение Б. Часто задаваемые вопросы	69
Что делать при возникновении ошибок?	70
Почему не открываются некоторые базы данных?	72
Почему не работает Антиспам?	72
Что делать, если задача AMgr выдает ошибку?	73
Как отключить проверку на вирусы?	73
В каких базах данных не производится проверка на вирусы?	75



Как менять настройки антивируса через веб-интерфейс?	76
Какие файлы обновляются с помощью модуля обновления?	77
Какие бывают виды репликации?	78
Приложение В. Работа в режиме централизованной защиты	80
Приложение Г. Техническая поддержка	85



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.
<u>Зеленый и подчеркнутый</u>	Гиперссылки на разделы и веб-страницы.
Моноширинный	Примеры программного кода, вводимый пользователем и выводимый программой текст.
<i>Курсив</i>	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);
- VGA - Video Graphics Array (логическая матрица видеогарфики).



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 **Модуля автоматического обновления. Dr.Web для IBM Lotus Domino** также предоставляет широкие возможности для администраторов по контролю защиты от вирусов и спама в сетях Domino любого масштаба.

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 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;
- документы в зашифрованных базах данных Lotus Domino;
- 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) (<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 одного установочного файла (drweb-domino-600-windows-nt-x86.exe для 32-битных версий сервера Lotus Domino и drweb-domino-600-windows-nt-x64.exe для 64-битных версий сервера Lotus Domino). Убедитесь, что ваш установочный файл имеет цифровую подпись компании «**Доктор Веб**». Для этого проверьте вкладку **Цифровые подписи** в свойствах файла.

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. Поместите установочный файл на локальный диск выбранного сервера Lotus Domino и убедитесь, что он доступен пользователю LOCALSYSTEM.



Для установки и удаления **Dr.Web для IBM Lotus Domino** пользователь должен состоять в группе локальных администраторов на том компьютере, где установлен сервер Lotus Domino. При включенной системе контроля учетной записи UAC установка осуществляется из консоли, запущенной от имени администратора.

Dr.Web для IBM Lotus Domino не совместим 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	128 МБ или больше
Свободное место на диске	120 МБ или больше
Монитор	VGA-совместимый монитор, желательно способный отображать как минимум 1280 x 1024 пикселей с 256 цветами

Требования к ОС и программному обеспечению:

Характеристика	Требование
ОС	Одна из следующих: <ul style="list-style-type: none">• Microsoft® Windows® 2000 Server с пакетом обновлений SP4 и Update Rollup 1;• Microsoft® Windows® 2000 Advanced Server с пакетом обновлений SP4 и Update Rollup 1;• Microsoft® Windows Server® 2003 R2;• Microsoft® Windows Server® 2003 Standard Edition;• Microsoft® Windows Server® 2003 Enterprise Edition;• Microsoft® Windows Server® 2003 Datacenter Edition;• Microsoft® Windows Server® 2008 R2;



Характеристика	Требование
	<ul style="list-style-type: none">• Microsoft® Windows Server® 2008 Standard Edition;• Microsoft® Windows Server® 2008 Enterprise Edition;• Microsoft® Windows Server® 2008 Datacenter Edition. Поддерживаются 32- и 64-битные версии операционных систем.
Файловая система	NTFS или FAT-32
ПО Lotus	Lotus Domino 6.5 для Windows или более поздний Lotus Notes 6.5 для Windows или более поздний
Прочее ПО	Microsoft Windows Installer 3.1 или более поздний Microsoft Internet Explorer 6, Mozilla Firefox 3, Opera 9 или более поздние версии этих веб-браузеров (требуется для работы с веб-интерфейсом) Dr.Web Enterprise Suite 6.0 или выше



Если помимо **Dr.Web для IBM Lotus Domino** в системе функционирует антивирусный файловый сторож **SpIDer Guard**, то для того чтобы проверка сетевого трафика осуществлялась программой **Dr.Web для IBM Lotus Domino**, необходимо в настройках файлового сторожа исключить из проверки файлы, выгружаемые IBM Lotus Domino, добавлением в **Список исключаемых путей и файлов** масок `dwat*`, `st*.tmp` и `c*.dtf`.

«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 компанией Microsoft, для ОС, которая используется на компьютере (они доступны на сайте обновлений по адресу <http://windowsupdate.microsoft.com>);
- проверить файловую систему при помощи стандартных средств и исправить обнаруженные ошибки.

Чтобы установить Dr.Web для IBM Lotus Domino:

1. Завершите работу сервера Lotus Domino.
2. Удалите предыдущие версии антивирусного модуля и любые другие антивирусы для IBM Lotus Domino, установленные на компьютере, используя стандартные средства операционной системы Windows.
3. Запустите установочный файл программы (drweb-domino-600-windows-nt-x86.exe для 32-битных версий сервера Lotus Domino и drweb-domino-600-windows-nt-x64.exe для 64-битных версий сервера Lotus Domino). Откроется окно Мастера установки InstallShield. 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 **Dr.Web Agent**, в открывшемся окне укажите вариант лицензирования. Для лицензирования работы **Dr.Web для IBM Lotus Domino** вы можете использовать локальный ключ либо ключ **Центра управления Dr.Web**. Нажмите кнопку **Далее**.
6. Если на предыдущем шаге установки вы выбрали пункт **Использовать локальный ключ** или на вашем компьютере не установлен **Dr.Web Agent**, то в открывшемся окне необходимо указать 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 **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 **Dr.Web для IBM Lotus Domino**.
 10. По завершении процесса установки рекомендуется произвести обновление антивирусных баз. Для этого установите флажок **Запустить обновление антивирусных баз** и нажмите на кнопку **Готово**.
 11. Выполните перезагрузку операционной системы после завершения установки.

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

После установки 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**.



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:

1. Завершите работу сервера Lotus Domino.
2. Запустите установочный файл программы `drweb-domino-600-windows-nt-x86.exe` (или `drweb-domino-600-windows-nt-x64.exe` для 64-битных версий). Откроется окно Мастера установки InstallShield.



Мастер установки можно запустить при помощи стандартного средства операционной системы **Установка и удаление программ** в Панели управления).

3. Нажмите кнопку **Удалить**.
4. По завершении процесса удаления нажмите кнопку **Заккрыть**.

После удаления антивирусного модуля **Dr.Web для IBM Lotus Domino** необходимо вручную удалить группу **DrWeb Admin** и программный документ **DrWebUpdate.bat**.

Чтобы удалить программный 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.

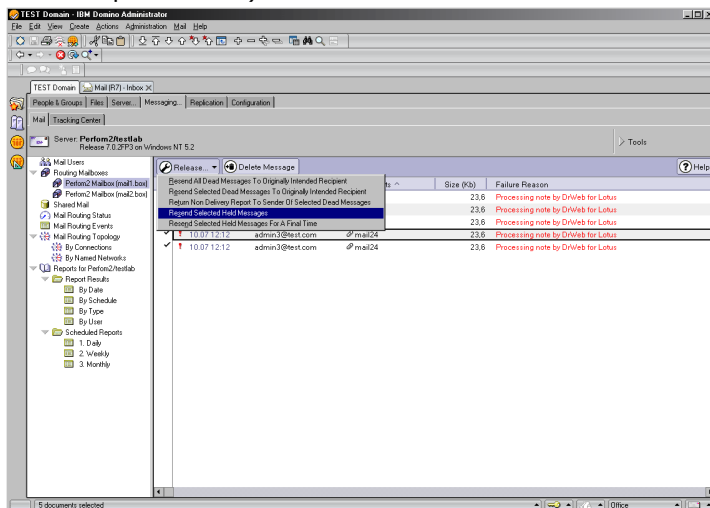


Действия после удаления

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** вы можете проверить, что антивирусный модуль был установлен правильно и является полностью работоспособным. В данном разделе содержится вся необходимая информация, требующаяся для проверки работоспособности.



Файлы и папки, создаваемые при установке

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

- %PROGRAMFILES%\DrWeb for Lotus Domino\

Имя файла	Описание
drwebupw.exe	Исполняемый файл модуля обновления
update.drl	Список URL-адресов для обновления
drweb32.key	Лицензионный ключевой файл

- %COMMONPROGRAMFILES%\Doctor Web\Scanning Engine\

Имя файла	Описание
drweb32.dll	Антивирусное ядро
vrcpp.dll	Ядро антиспама
dwinctl.dll	-
dwengine.exe	Сервис Dr.Web Scanning Engine
dwsewsc.exe	-

- %ProgramData%\Doctor Web\Bases\
(для Windows 2000 и Windows 2003 –
%ALLUSERSPROFILE%\Application Data\Doctor
Web\Bases\)

Имя файла	Описание
*.vdb	Вирусные базы
drweb32.lst	Список файлов, загружаемых Модулем обновления



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

Имя файла	Описание
ndrwebmonitor.exe	Задача Монитора
ndrwebscanner.exe	Задача 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



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 **ndrwebhook.dll**.
- В параметр **ServerTasks** добавляются задачи монитора и сканера (**monitor** и **scanner**).
- Добавляются параметры **DrWebKey** и **DrWebBuild**, в которых указывается путь к ключевому файлу и полный номер сборки соответственно.

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



Запуск сервера Lotus Domino

Если установка **Dr.Web для IBM Lotus Domino** прошла успешно, то можно запустить сервер Lotus Domino (запустите **nserver.exe**). 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`.

```
> sh task
Task                Description
Database Server    Perform console commands
Database Server    Listen for connect requests on TCPIP
Database Server    Listen for connect requests on LAN3
Database Server    Listen for connect requests on LAN5
Database Server    Listen for connect requests on LAN4
Database Server    Load Monitor is idle
Database Server    Database Directory Manager Cache Refresher is idle
Database Server    Organization Name Cache Refresher is idle
Database Server    Idle task
Database Server    Log Purge Task is idle
Database Server    Idle task
Database Server    Perform Database Cache maintenance
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Idle task
Database Server    Shutdown Monitor
Database Server    Process Monitor
IMAP Server        Listen for connect requests on TCP Port:143
SMTP Server        Listen for connect requests on TCP Port:25
IMAP Server        Utility task
SMTP Server        Utility task
POP3 Server        Listen for connect requests on TCP Port:110
POP3 Server        Utility task
Agent Manager      Executive '1': Idle
IMAP Server        Control task
DrWeb Monitor      Idle
Process Monitor    Idle
Schedule Manager   Idle
Replicator         Idle
HTTP Server        Listen for connect requests on TCP Port:80
DrWeb Scanner      Idle
Rooms and Resources Idle
SMTP Server        Control task
POP3 Server        Control task
Directory Indexer  Idle
Indexer            Idle
Router             Idle
Calendar Connector Idle
Admin Process      Idle
Agent Manager      Idle
Event Monitor      Idle
```



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-  
ANTI VIRUS-TEST-FILE! $H+H*
```

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

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

Вирусъ: eicar.com (EICAR Test File (NOT a Virus!)) отправлен в карантин



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

Проверка детектирования спама



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

Для проверки способности **Dr.Web для IBM Lotus Domino** обнаруживать спам рекомендуется использовать письмо с тестовой строкой GTUBE (Generic Test for Unsolicited Bulk Email).

Чтобы создать тестовое письмо GTUBE:

- Скопируйте следующую строку в тело нового электронного письма:

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

Отправьте письмо по протоколу SMTP на любой тестовый адрес. В теме полученного письма должен появиться префикс **[СПАМ]**.



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 пикселей.

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

Чтобы запустить Консоль администратора в среде Lotus Notes:

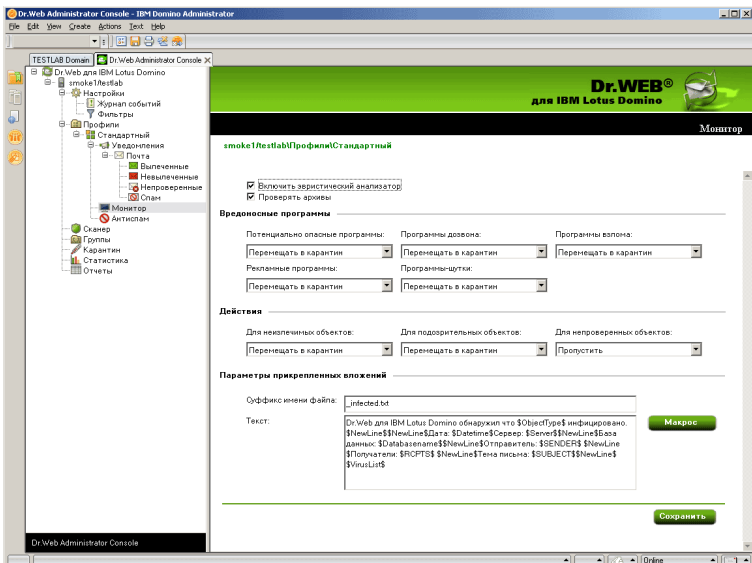
1. Запустите сервер Lotus Domino.
2. Запустите приложение Lotus Notes.
3. Откройте меню **File**, выберите пункт **Database** и нажмите **Open**. Откроется окно **Open Database** (чтобы открыть это окно, вы также можете нажать комбинацию клавиш CTRL+O на клавиатуре).
4. Выберите сервер Lotus Domino, 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 папку `\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 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.

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:

- **Монитор** проверяет все входящие и исходящие письма в режиме реального времени по мере того, как их обрабатывает сервер Lotus Domino. 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** 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.
- **Карантин** используется для изоляции зараженных и подозрительных объектов. Он представляет собой NSF базу (**quarantine.nsf**), которая расположена в подкаталоге **drweb** в папке **Data** сервера Lotus Domino. Доступ к объектам, находящимся в карантине осуществляется из базы **Консоли администратора** (**DrWebAdmin.nsf**).



- **Модуль автоматического обновления**, 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. Запустить модуль можно двумя способами: автоматически и в режиме командной строки (см. [Обновление вирусных баз](#)).
- **Антиспам** проверяет все входящие по протоколу SMTP сообщения в режиме реального времени по мере того, как их обрабатывает сервер Lotus Domino. 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]**).



Антиспам доступен только в версии "Антивирус + антиспам" (см. [Лицензионный ключевой файл](#)).

- Компонент **Статистика** 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** 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 **Антиспам** можно настроить для каждого профиля таким образом, чтобы удовлетворить потребностям каждого клиента или группы. Работа остальных компонентов настраивается для всего программного модуля.



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**.

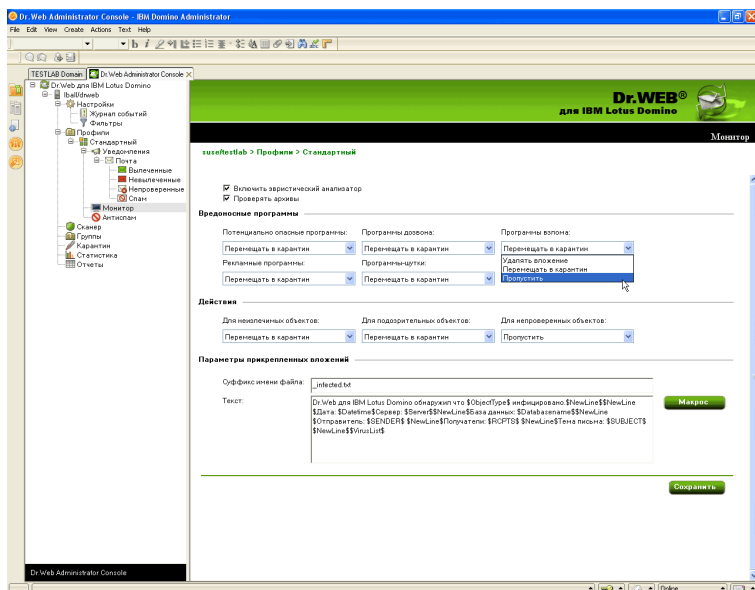


Настройка Монитора

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 и проверку архивов во вложениях, т.к. это значительно снижает уровень защищенности сервера.

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 только 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 вероятно принадлежность письма к спаму: *Спам*, *Возможно спам*, *Сомнительные письма*. Для каждой категории можно задать отдельные действия (см. описание настроек ниже).



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 (**C:\Program Files\DrWeb for Lotus Domino\drweb32.key**) текстовым редактором и найдите следующую строку: `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 добавлялся префикс, установите флажок **Изменить тему**. 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 удастся 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 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 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), добавление адресов в черный и белый списки.

- **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).

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 **ОК**. 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 Domino

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.

The screenshot shows the 'Сканер' (Scanner) interface. At the top, there is a header with the Dr.Web logo and the text 'для IBM Lotus Domino'. Below the header, there is a table with columns: 'Время', 'База', 'Периодичность', 'Каждый', and 'Объект'. The table contains two rows, both with checkmarks in the first column. The first row has '00:00' in the 'Время' column, '*.*' in the 'База' column, 'Каждый день' in the 'Периодичность' column, and 'Все документы в базе' in the 'Объект' column. The second row has '00:00' in the 'Время' column, '*.*' in the 'База' column, 'Каждый день' in the 'Периодичность' column, and 'Все документы в базе' in the 'Объект' column. Below the table, there is a section titled 'Настройки сканирования' (Scanning settings) with the following fields: 'Включить' (checked), 'Периодичность' (dropdown menu with 'Каждый день' selected), 'Время начала' (input field with '00:00' and a clock icon), 'Объекты' (dropdown menu with 'Все документы в базе' selected), and 'База' (input field with '*.*'). There are buttons for 'Добавить', 'Удалить', 'Очистить', and 'Сохранить'.

Время	База	Периодичность	Каждый	Объект
✓ 00:00	*.*	Каждый день	Каждый	Все документы в базе
✓ 00:00	*.*	Каждый день	Каждый	Все документы в базе

Настройки сканирования

Включить

Периодичность: Время начала:

Объекты:

База:

Добавить
Удалить
Очистить

Сохранить

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.

Dr. WEB[®]
для IBM Lotus Domino

Карантин

azhebel@rweb

Фильтрация

Фильтр:

Чистка

Удалить документы старше дней

Автоматически удалять документы старше дней Включить

Обновить Удалить Блокировать Сохранить файл

Дата	Отправитель	Получатель	Тема	Файл	Вирус	Имя базы
------	-------------	------------	------	------	-------	----------

Сохранить



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 документы:

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).

azhebel@drweb

Dr.WEB®
для IBM Lotus Domino

Отчеты

Отчет	Получатель	Дней	Расписание	В какой д
Все инциденты	DrWeb Admin	1	Каждый день	
Последние вирусы	DrWeb Admin	1	Каждый день	
Инциденты по получателям	DrWeb Admin	1	Каждый день	
Количество спама	DrWeb Admin	1	Каждый день	
Получившие больше всего вирусов	DrWeb Admin	1	Каждый день	
Получившие больше всего спама	DrWeb Admin	1	Каждый день	

Формировать Обновить

Почта **Все инциденты**

Тема:

Получатели:

Ручное формирование

С: По:

Автоматическое формирование

Включить

Формировать старше дней

Периодичность: Вреня начала:

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**.

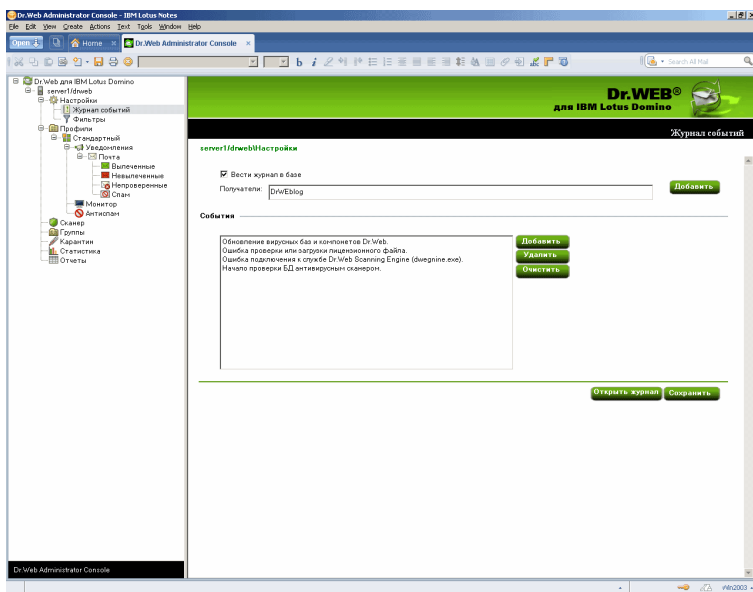


Задать автоматическую рассылку отчетов по расписанию для инцидентов, произошедших в течение текущего дня, невозможно. Если вы хотите послать отчет с инцидентами за сегодняшний день, то сгенерируйте его, указав диапазон с сегодняшней датой в группе настроек **Ручное формирование**.



Ведение Журнала Событий

Журнал событий может использоваться сетевыми администраторами для контроля событий, происходящих в ходе работы **Dr.Web для IBM Lotus Domino** (особенно полезен, 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.



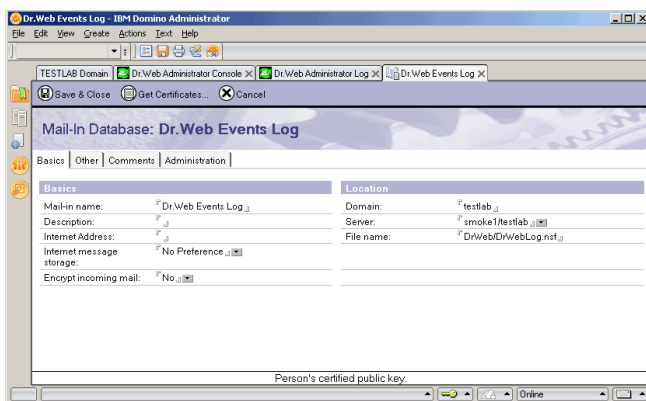
Чтобы настроить ведение Журнала событий:

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 среплицируйте 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  
*@spammers.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 (см. [В каких базах данных не производится проверка на вирусы?](#)). 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

Обновление вирусных баз в **Dr.Web для IBM Lotus Domino** реализовано посредством **Модуля обновления**. Это программный компонент, который запускается по расписанию, заданному в программном документе **drwebupdate.bat**. Данный документ создается в каталоге **Domino** адресной книги сервера во время установки. По умолчанию **Модуль обновления** запускается каждые 30 минут. Программный документ можно изменить посредством клиента Domino Administrator.

Чтобы изменить расписание Модуля обновления:

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 чего необходимо запустить файл **drwebupdate.bat**. При запуске в режиме командной строки, вы можете задавать дополнительные параметры (см. [Параметры командной строки для Модуля обновления](#)).

Если вы пользуетесь прокси, то необходимо дополнительно настроить **Модуль обновления** на работу через прокси.

Чтобы настроить прокси:

1. Запустите на исполнение файл **drwebupw.exe**, хранящийся в каталоге установки программы **Dr.Web для IBM Lotus Domino** (обычно, %PROGRAMFILES%\DrWeb for Lotus Domino).
2. В открывшемся окне нажмите **Settings**.
3. В окне настроек откройте вкладку **Proxy**.



4. Укажите IP-адрес и порт прокси-сервера.
5. При необходимости, в поле **User name** введите имя пользователя, а в поле **Password** – пароль для доступа к прокси-серверу. Если прокси-сервер разрешает анонимный доступ, оставьте поля пустыми.
6. Нажмите кнопку **OK**.



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. Параметры командной строки для модуля обновления

Ниже приведен список параметров командной строки, которые могут быть добавлены в поле запуска для программного документа **drwebupdate.bat**:

/DBG - вести подробный отчет.

/URL: <URL сервера обновления> - допускаются только UNC-пути.

/USER: <имя пользователя HTTP-сервера> - имя пользователя сервера обновлений.

/PASS: <пароль пользователя HTTP-сервера> - пароль пользователя сервера обновлений.

/UPM: <режим прокси> - режим использования прокси-сервера, может принимать следующие значения:

- **direct** - не использовать прокси-сервер
- **ieproxy** - использовать системные настройки
- **userproxy** - использовать настройки, задаваемые пользователем (ключи */PURL*, */PUSER* и */PPASS*)

/PURL: <адрес прокси-сервера> - адрес прокси-сервера.

/PUSER: <имя пользователя прокси> - имя пользователя прокси-сервера.

/PPASS: <пароль пользователя прокси> - пароль пользователя прокси-сервера.

/UA - загружать все файлы, заявленные в списке обновления, независимо от используемой системы и установленных компонентов. Режим предназначен для получения полной локальной копии серверной области обновления **Dr.Web**; этот режим нельзя использовать для обновления антивируса,



установленного на компьютере.

/ST - запускать модуль обновления в невидимом режиме (*stealth mode*).

/LNG: <имя_файла> - имя файла языковых ресурсов; если не указано, используется английский язык.

/GO - пакетный режим работы, без диалоговых остановок.

/QU - принудительно закрывать модуль обновления после окончания сеанса обновления независимо от того, успешно оно прошло или нет. Успешность обновления можно проверить по коду возврата программы **drwebupw.exe** (например, из BAT-файла по значению переменной **errorlevel: 0** = успешно, другие значения = неуспешно).

/DIR: <путь к папке> - переназначение папки, в которую загружаются обновляемые файлы; по умолчанию это папка, из которой модуль обновления был запущен.

/URM: <режим> - режим перезагрузки после обновления; может принимать следующие значения:

- **prompt** - по окончании сеанса обновления, в случае необходимости перезагрузки, спросить пользователя
- **noprompt** - в случае необходимости, перезагружаться, не спрашивая пользователя
- **force** - перезагружать принудительно всегда (независимо от того, требуется перезагрузка или нет)
- **disable** - запретить перезагрузку

/REG - запуск модуля обновления в режиме регистрации и получения регистрационного ключа.

/UPD - обычное обновление; применяется в паре с ключом /REG, чтобы запустить обновление в режиме регистрации.

/UVB - обновлять только вирусные базы и антивирусное ядро **drweb32.dll** (отменяет действие ключа /UA, если он задан).

/RP<имя_файла> или /RP+<имя_файла> - записать отчет о работе программы в файл, имя которого указано в ключе. При отсутствии имени записать в файл по умолчанию. При наличии символа + файл дописывается, при отсутствии - создается заново.

/INI: <путь> - использовать альтернативный конфигурационный файл с указанным именем или по



указанному пути.

/NI - не использовать параметры, записанные в конфигурационном файле **drweb32.ini**.

/NR - не создавать файл отчета.

/SO - включить звуковое сопровождение (только при возникновении ошибок).

Приложение Б. Часто задаваемые вопросы

В данном приложении описаны наиболее частые вопросы и ответы, проблемы и их решения, а также дополнительная информация, которая может быть полезной при работе с **Dr.Web для IBM Lotus Domino**.

[Что делать при возникновении ошибок?](#)

[Почему не открываются некоторые базы данных?](#)

[Почему не работает Антиспам?](#)

[Что делать, если задача AMgr выдает ошибку?](#)

[Как отключить проверку на вирусы?](#)

[В каких базах данных не производится проверка на вирусы?](#)

[Как менять настройки антивируса через веб-интерфейс?](#)

[Какие файлы обновляются с помощью модуля обновления?](#)

[Какие бывают виды репликации?](#)



Что делать при возникновении ошибок?

При возникновении ошибок или в случае аварийного завершения работы сервера Lotus Domino после установки или в процессе работы антивирусного модуля **Dr.Web для IBM Lotus Domino** необходимо убедиться, что это вызвано именно модулем. Для этого, либо удалите антивирусный модуль (см. [Удаление Dr.Web для IBM Lotus Domino](#)), либо отключите загрузку его компонентов (см. [Как отключить проверку на вирусы?](#)). После этого **Dr.Web для IBM Lotus Domino** не должен оказывать на работу сервера Lotus Domino никакого влияния, а значит, если сервер продолжает работать нестабильно, то ошибки в его работе не могут быть вызваны антивирусным модулем. Если же окажется, что ошибки в работе сервера вызывает **Dr.Web для IBM Lotus Domino**, то необходимо собрать как можно больше сведений и информации перед обращением в службу технической поддержки.

Чтобы собрать всю необходимую информацию:

1. Установите антивирусный модуль **Dr.Web для IBM Lotus Domino**, если он был удален.
2. Отключите загрузку компонентов модуля (см. [Как отключить проверку на вирусы?](#)).
3. Запустите сервер Lotus Domino.
4. Откройте конфигурационный файл notes.ini сервера Lotus Domino.
5. Добавьте в файл notes.ini параметр DrWebDebugLog=5.
6. Закройте файл notes.ini, сохранив изменения.
7. Откройте окно консоли сервера Lotus Domino. Запустите команду `sh server` и сохраните ее результат.



8. Убедитесь, что на сервере включен запуск NSD (Notes System Diagnostics):
 - Запустите клиент Domino Administrator и откройте вкладку **Configuration**, затем **Server** -> **Current server document** -> **Basics** -> **Fault Recovery**. Убедитесь, что параметр **Run NSD To Collect Diagnostic Information** включен.
9. Остановите сервер Lotus Domino.
10. Включите загрузку компонентов модуля (см. [Как отключить проверку на вирусы?](#)).
11. Запустите сервер Lotus Domino.
12. 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 антивирусным модулем **Dr.Web для IBM Lotus Domino**, необходимо предоставить следующую информацию:

- несколько последних журналов NSD (они сохраняются в папку **\Lotus\Domino\DATA\IBM_TECHNICAL_SUPPORT** при каждом аварийном завершении работы сервера Lotus Domino);
- журналы работы **Dr.Web для IBM Lotus Domino** (они сохраняются в папку **\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, выполните следующую последовательность действий:
 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 **Dr.Web: Monitor, Scanner, Hook, Anti-Spam, 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 просмотрев версии файлов ndrwebhook.dll, ndrwebscanner.exe, ndrwebmonitor.exe, vrcpp.dll, dwenine.exe, используя проводник Windows. Расположение файлов см. в разделе [Проверка работоспособности](#).

Всю необходимую информацию приложите к запросу в [службу технической поддержки Dr.Web](#).

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)**.

Почему не работает Антиспам?

Если модуль **Dr.Web для IBM Lotus Domino** не выявляет спам, и настройки компонента **Антиспам** недоступны, то скорее всего ваш лицензионный ключевой файл не поддерживает **Антиспам** (см. [Лицензионный ключевой файл](#)). Чтобы проверить так ли это, откройте ключевой файл (**C:\Program Files\DrWeb for Lotus Domino\drweb32.key**) текстовым редактором и найдите следующую строку: LotusSpamFilter=No.

Если в ключевом файле указано LotusSpamFilter=Yes, то файл должен поддерживать работу компонента **Антиспам**. В этом случае обратитесь в [службу технической поддержки Dr.Web](#).



Что делать, если задача AMgr выдает ошибку?

Если служебные базы данных модуля **Dr.Web для IBM Lotus Domino** (**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
```

Чтобы подписать базы, сделайте следующее:

1. Запустите клиент Domino Administrator.
2. Выберите пункт **Open Server** в меню **File** и укажите сервер, на котором установлен **Dr.Web для IBM Lotus Domino**.
3. 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** и **DrWebReports.nsf**.
4. 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.
5. Выберите **Active Server's ID** в окне **Sign Database** и нажмите кнопку **OK**.

Как отключить проверку на вирусы?

Чтобы отключить проверку на вирусы без удаления антивирусного модуля, необходимо отключить загрузку компонентов **Монитор** и **Сканер**.



Чтобы отключить загрузку компонентов:

1. Откройте файл **notes.ini** сервера Lotus Domino, на котором установлен антивирусный модуль **Dr.Web для IBM Lotus Domino**.
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 антивирусных компонентов:

1. Откройте файл **notes.ini** сервера Lotus Domino, на котором установлен антивирусный модуль **Dr.Web для IBM Lotus Domino**.
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.



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, и 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
- clbdir.nsf
- namagent.nsf
- reports.nsf
- schema.nsf
- activity.nsf
- AgentRunner.nsf
- busytime.nsf
- certsrv.nsf
- dba4.nsf
- doladmin.nsf
- lndfr.nsf
- statrep.nsf



Как менять настройки антивируса через веб-интерфейс?

В **Dr.Web для IBM Lotus Domino** 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 следующему адресу: <http://domino.server/drweb/drwebAdmin.nsf>
 4. Введите имя и Интернет-пароль (*Internet password*) учетной записи администратора, указанного в группе **DrWeb Admin**.



Какие файлы обновляются с помощью модуля обновления?

Модуль обновления в составе **Dr.Web для IBM Lotus Domino** загружает и обновляет следующие компоненты:

- Вирусные базы (*.vdb)
- Ядро компонента **Антиспам** (vrcpp.dll)
- Антивирусное ядро (drweb32.dll)
- Сам модуль обновления (drwebupw.exe)

НЕ обновляется:

- 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**)



Какие бывают виды репликации?

Существует два основных вида репликации:

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

Если **Dr.Web для IBM Lotus Domino** установлен на обоих серверах, участвующих в репликации, то обнаружение вирусов и лечение документов происходит без проблем, однако, следует иметь в виду 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.



Действие	Задача, выполняющая репликацию и проверку на вирусы	Комментарии
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.



Приложение В. 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 конечных пользователей.

Взаимодействие компонентов антивирусной сети

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

Компьютеры компании или пользователей поставщика ИТ-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.

Dr.Web для IBM Lotus Domino в режиме централизованной защиты

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 корректной работы **Dr.Web для IBM Lotus Domino** и **Dr.Web Agent** в операционной системе порядок установки продуктов должен быть следующий:

- **Dr.Web Agent**
- **Dr.Web для IBM Lotus Domino**

В противном случае установка **Dr.Web Agent** завершится ошибкой.

Удаление должно проводиться в обратном порядке.

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 в **Центр Управления Dr.Web** выполняется 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 во время [установки на 5 шаге](#) выбрать **Использовать лицензионный ключ Центра Управления Dr.Web**.



В режиме **Enterprise Dr.Web для IBM Lotus Domino** не будет использоваться локальный лицензионный ключевой файл, указанный при установке модуля и заданный в файле notes.ini параметром DrWebKey. В режиме **Enterprise** делается запрос ключа у **Центра Управления Dr.Web** и, если ключ не получен, модуль не будет выполнять антивирусную проверку.



Приложение Г. Техническая поддержка

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

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

- Прочитать раздел [Что делать при возникновении ошибок?](#) в Приложении Б.
- 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>.

