



Dr.WEB®

**Антивирус
для Novell NetWare**

Руководство администратора

Защити созданное

© 2003-2009 «Доктор Веб». Все права защищены.

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

ТОРГОВЫЕ ЗНАКИ

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt! и логотипы Dr.WEB и Dr.WEB INSIDE являются зарегистрированными товарными знаками «Доктор Веб». 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).

Антивирус Антивирус Dr.Web для файловых серверов Novell NetWare

Версия 5.0.0

Руководство администратора

06.04.2009

«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.

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

Антивирусные продукты «Доктор Веб» разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

Глава 1. Введение	6
Используемые обозначения и сокращения	7
Техническая поддержка	8
Глава 2. Лицензирование	9
Ключевой файл	9
Получение ключевого файла	10
Глава 3. Установка и запуск программы	12
Комплект поставки	12
Установка программы	13
Выбор языкового режима	14
Запуск программы	15
Глава 4. Настройка параметров	16
Основные параметры работы	16
Дополнительные параметры работы	18
Секция [NetWare]	19
Секция [NetWare:Transit]	20
Параметры антивирусной проверки	21
Общие параметры сканирования	22
Дополнительные параметры сканирования по расписанию	26
Дополнительные параметры сканирования «на лету»	28
Глава 5. Антивирусная проверка	29
Методы обнаружения вирусов	29
Способы запуска антивирусной проверки	31



Действия с активными процессами	32
Глава 6. Регистрация событий	33
Настройка ведения журнала	33
Глава 7. Модуль обновления	34
Настройка модуля обновления	35
Приложения	38
Приложение А. Элементы интерфейса	38



Глава 1. Введение

Данная программа принадлежит к 32-битному семейству антивирусных программ **Dr.Web**. Это семейство включает в себя набор программ для операционных систем как семейств Microsoft® Windows® и Unix® (Linux®, FreeBSD® и т.д.), так и антивирусы для MS-DOS® 386, Novell® NetWare® и IBM® Operating System/2®.

Антивирус Dr.Web для файловых серверов Novell NetWare (далее - **Dr.Web для NetWare**) запускается на сервере как загружаемый модуль (NetWare Loadable Module®, NLM®) в среде сетевой операционной системы Novell NetWare версий 3.12, 3.2, 4.11, 4.2, 5.1, 6.0, 6.5. Управление программой осуществляется с помощью консоли, установленной либо непосредственно на сервере, либо на любой удаленной рабочей станции.

Dr.Web для NetWare позволяет:

- проводить проверку томов сервера по заранее заданному расписанию;
- проводить проверку томов сервера по запросу администратора;
- осуществлять проверку «на лету» файлов, загружаемых на сервер и с него;
- гибко настраивать, какие файлы, каталоги и тома подлежат антивирусной проверке;
- гибко настраивать действия в случае обнаружения вирусов или подозрительных файлов;
- порождать несколько одновременно действующих процессов проверки;
- управлять приоритетом процессов проверки в системе и контролировать их ход;
- вести протокол проверки и управлять его детализацией.



Используемые обозначения и сокращения

В данном руководстве применены следующие условные обозначения:

Обозначение	Комментарий
Полужирное начертание	Названия элементов графического интерфейса и примеры ввода, который необходимо выполнить в точности так, как он приведен в руководстве.
Зеленое и полужирное начертание	Наименования продуктов « Доктор Веб » или их компонентов.
<u>Зеленое и подчеркнутое начертание</u>	Ссылки на страницы руководства и веб-сайты.
Моноширинный шрифт	Примеры кода, ввода для командной строки и информации, выводимой пользователю приложением.
<i>Курсив</i>	Термины и замещающий текст (приводится вместо информации, которую необходимо ввести пользователю). В случае примеров ввода командной строки курсив указывает на значения параметров.
ЗАГЛАВНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Знак плюса (+)	Указывает на одновременность нажатия клавиш клавиатуры. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак	Важное замечание или предупреждение о потенциально опасных или чреватых ошибками ситуациях.

Названия элементов интерфейса приводятся на английском языке. Перевод на русский язык наиболее часто встречающихся названий приведен в [Приложении А](#).



Техническая поддержка

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

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

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

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

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



Глава 2. Лицензирование

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

Ключевой файл

Ключевой файл имеет расширение .key и находится по умолчанию в каталоге установки. Он содержит, в частности, следующую информацию:

- период, в течение которого разрешено использование **Dr.Web для NetWare**;
- перечень компонентов, разрешенных к использованию;
- период, в течение которого разрешено обновление версий (срок подписки – может не совпадать со сроком использования);
- разрешенные версии антивируса;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать антивирус).

Существует два типа ключевых файлов:

- Лицензионный ключевой файл, который приобретается вместе с **Dr.Web для NetWare** и позволяет как пользоваться продуктом так и получать техническую поддержку. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с пользовательским договором. В такой файл также заносится информация о пользователе и продавце продукта.



- Демонстрационный ключевой файл, который используется для ознакомления с продуктом. Такой ключевой файл обеспечивает полную функциональность основных компонентов, но имеет ограниченный срок действия и не предусматривает оказания поддержки.

Ключевой файл **Dr.Web для NetWare** является *действительным* при одновременном выполнении следующих условий:

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

При нарушении любого из условий ключевой файл становится *недействительным*, при этом **Dr.Web для NetWare** перестает обезвреживать вредоносные программы.

Получение ключевого файла

Коммерческие пользователи, приобретающие **Dr.Web для NetWare** у законных поставщиков продукта, получают *лицензионный ключевой файл*. Параметры этого ключевого файла, регулирующие права пользователя, установлены в соответствии с пользовательским договором. В такой файл также заносится информация о пользователе и продавце антивируса.

Вы можете получить ключевой лицензионный файл одним из следующих способов:

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

Получение ключевого файла по электронной почте

1. Зайдите на сайт, адрес которого указан в регистрационной карточке, прилагаемой к продукту.



2. Заполните форму со сведениями о покупателе.
3. Введите регистрационный серийный номер (находится на регистрационной карточке).
4. Ключевой файл будет выслан по указанному вами адресу электронной почты в виде ZIP-архива, содержащего файл с расширением .key.
5. Извлеките ключевой файл при помощи средств операционной системы или архиватора формата ZIP и поместите его в каталог установки **Dr.Web для NetWare**.

В некоторых случаях для ознакомления с программой можно получить *демонстрационный ключевой файл*. Такие ключевые файлы обеспечивают полную функциональность основных антивирусных компонентов, но имеют ограниченный срок действия и не предполагают оказание поддержки пользователю.

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

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



Глава 3. Установка и запуск программы

Все программы семейства **Dr.Web** могут быть установлены в один и тот же каталог. В комплект поставки всех программ семейства входят следующие файлы, одинаковые для всех программ:

- drweb32.dll (основной программный модуль, **ядро Dr.Web**);
- drwebase.vdb (основная **вирусная база Dr.Web**);
- **дополнения вирусных баз** (файлы *.vdb и соответствующие им файлы *.txt);
- drweb32.ini (**конфигурационный файл Dr.Web**).

Конфигурационный файл является общим для всех программ семейства и хранится в каталоге установки. Настройки режимов для разных программ задаются в отдельных разделах конфигурационного файла.

Дополнения вирусных баз следует помещать в каталог установки.

Подробнее о конфигурационном файле см. [Настройка параметров](#).

Подробнее об обновлениях см. [Модуль обновления](#).

Комплект поставки

В дистрибутивный комплект поставки **Dr.Web для NetWare** входят следующие файлы:

- drwebnw.nlm — основной программный модуль;
- drwebnw.imp — компонент, необходимый для установки режима On-access (На лету);
- drweb32.dll — основной программный модуль (**антивирусное ядро Dr.Web**);



- drwebase.vdb — основная вирусная **база Dr.Web** (также в комплект поставки может входить один или более файлов дополнительных вирусных баз, имеющих имена вида DRWvvvnn.VDB, где v.vv — номер версии **Dr.Web для NetWare**, к которой выпущена дополнительная база, и nn - порядковый номер дополнительной базы к данной версии);
- en-drwnw.txt — документация по программе на английском языке;
- ru-drwnw.txt — документация по программе на русском языке (в комплекте могут также присутствовать файлы документации на других языках);
- drwebupn.nlm — **модуль обновления** выполняемых файлов Dr.Web и вирусных баз (подробнее об обновлении см. [Глава 7. Модуль обновления](#)).

Кроме того, в комплект поставки могут входить файлы языковых ресурсов, имеющие имена <язык>-drwnw.dwl (например, ru-drwnw.dwl, de-drwnw.dwl и т.п.).

Установка программы

Установка Dr.Web для NetWare на сервер

1. Создайте на сервере каталог установки (например, с именем DRWEB)
2. Распакуйте в каталог установки файлы дистрибутива **Dr.Web для NetWare**.



Выбор языкового режима

По умолчанию интерфейс программы англоязычный. Установить другой язык можно, изменив настройки в [секции \[NetWare\]](#) конфигурационного файла.

Изменение языка пользовательского интерфейса



Все изменения в конфигурационном файле должны производиться при выгруженном (unloaded) **Dr.Web для NetWare**, иначе при завершении работы антивирус автоматически сохранит свои текущие настройки.

1. Откройте [конфигурационный файл](#) Dr.Web для редактирования в любом текстовом редакторе. По умолчанию, конфигурационный файл называется drweb32.ini и находится в каталоге установки.
2. В строке LngFileName секции [NetWare] укажите в кавычках имя нужного файла языковых ресурсов.
Файлы языковых ресурсов имеют имена вида <язык>-drwnw.dwl. Например, ru-drwnw.dwl, de-drwnw.dwl и т.п.
3. Сохраните изменения в конфигурационном файле.



Запуск программы

Запуск антивируса осуществляется с консоли сервера либо с удаленной консоли.

Запуск Dr.Web для NetWare

Чтобы запустить **Dr.Web для NetWare**, выполните с консоли сервера или удаленной консоли следующую команду:

```
load [ <полный путь на сервере>] drwebnw
```

где <полный путь на сервере> - путь к каталогу установки **Dr.Web для NetWare**. Если каталог входит в путь поиска (search path), то полный путь можно не указывать.



Если drwebnw.nlm не загружается с сообщением вида «...Module drwebnw.nlm cannot be loaded until SLIWAUX loaded...», то это означает, что у Вас не установлены последние обновления для операционной системы Novell NetWare. Вы можете найти необходимые обновления на официальном сайте компании Novell по адресу <http://support.novell.com/patches.html>.

Для функционирования отправки уведомлений администратору по электронной почте на сервере должен быть загружен модуль tcpip.nlm и настроен протокол TCP/IP. Если модуль не загружен, то при запуске **Dr.Web для NetWare** будет выдано следующее сообщение: «tcpip.nlm не загружен (ошибка <номер ошибки>)». Некоторые дополнительные возможности отключены.



Глава 4. Настройка параметров

Настройка параметров работы **Dr.Web для NetWare** осуществляется через меню **Setup**, так и через конфигурационный файл `drweb32.ini`.

Конфигурационный файл

Все параметры работы программ семейства **Dr.Web** отражены в конфигурационном файле `drweb32.ini`. Файл является общим для всех программ семейства и хранится в том же каталоге, что и программный модуль `drwebnw.nlm`. Если при запуске программы конфигурационный файл отсутствует, то работа производится со значениями, принятыми по умолчанию. В любом случае при выходе из программы все параметры сохраняются в конфигурационном файле, который при необходимости создается автоматически.

Основные параметры работы

Настройка основных параметров работы **Dr.Web для NetWare** осуществляется через меню **Setup**.

Меню **Setup** позволяет задать следующие параметры работы программы:

Настройка	Комментарий
Scan settings	Задает настройки стандартных параметров процессов сканирования (см. Общие параметры сканирования). Действуют по умолчанию для всех процессов сканирования.
Virus bases	Задает имена используемых вирусных баз. Использование маски допустимо.



Настройка	Комментарий
Move files to	Задаёт каталог для перемещаемых инфицированных файлов. Этот каталог является общим для всех процессов.
Rename files to	Задаёт маску для генерации расширения переименованных файлов. Эта маска является общей для всех процессов.
If virus found	<p>Задаёт дополнительные действия, которые будут предприниматься в случае обнаружения вируса:</p> <ul style="list-style-type: none">• Create flag file — создавать флаг-файл, т.е. файл нулевой длины, появление которого является индикатором того, что произошло некоторое событие (в данном случае, обнаружение вируса на сервере). Предполагается, что запущено некоторое приложение, реагирующее на такой индикатор. Имя флаг-файла задается в Setup Miscellaneous Flag file name;• Ring the bell — подавать звуковое предупреждение с консоли сервера;• Disconnect station — отключать от сервера станцию, с которой исходит вирусная атака;• Send message — посылать уведомления станции, с которой исходит вирусная атака.
Miscellaneous	<p>Устанавливает следующее:</p> <ul style="list-style-type: none">• Disconnected users — просматривать список отключенных пользователей. При помощи клавиши DEL можно удалять из этого списка отдельных отключенных пользователей — тогда они получают возможность вновь подключиться к серверу;• Send messages to — определить список пользователей и групп, которым всегда нужно направлять уведомления об обнаружении вируса на сервере. Данная версия Dr.Web для NetWare поддерживает эту возможность под NetWare 4.x и выше только в случае, если данный пользователь или группа входит в bindery context, установленный на сервере;• E-mail notification — настроить отсылку по



Настройка	Комментарий
	<p>электронной почте уведомлений, если при проверке «на лету» обнаружен вирус;</p> <ul style="list-style-type: none">• Disconnect message, Virus found message, Suspected file message — задать тексты сообщений для случаев обнаружения вируса, обнаружения подозрительного на вирус файла и отключения станции от сервера;• Flag file name — определить имя флаг-файла.

Дополнительные параметры работы

Практически все параметры могут быть [настроены через систему меню](#) и описаны в соответствующих разделах документации. Однако для некоторых параметров настройка возможна только через [конфигурационный файл](#). Такие параметры описаны в следующих разделах.

Конфигурационный файл представляет собой текстовый файл, и для его редактирования можно использовать любой текстовый редактор. Параметры, используемые **Dr.Web для NetWare**, сосредоточены в следующих секциях:

- [NetWare] — общие настройки;
- [NetWare: Transit] — настройки транзитных каталогов.



Секция [NetWare]

Секция [NetWare] [конфигурационного файла](#) позволяет задать следующие параметры работы программы:

Настройка	Комментарий
LngFileName	<p>Имя файла языковых ресурсов Dr.Web для NetWare.</p> <p>Например, LngFileName = "ru-drwnw.dwl".</p> <p>При пустом значении параметра (LngFileName = "") Dr.Web для NetWare использует встроенный (английский) язык.</p>
TempPath	<p>Каталог для размещения временных файлов, создающихся при работе Dr.Web для NetWare.</p> <p>Например, TempPath = "SYS:\TEMP".</p> <p>Если указанного каталога не существует, то он создается при запуске Dr.Web для NetWare. При пустом значении параметра (TempPath = "") временные файлы размещаются в каталоге установки. Временные файлы удаляются автоматически, как только пропадает необходимость в их использовании.</p>
UpdateFlags	<p>Список файлов, изменение которых автоматически приводит к перезагрузке вирусных баз Dr.Web.</p> <p>В Dr.Web для NetWare реализован механизм автоматической перезагрузки вирусных баз без перезапуска самой программы Dr.Web для NetWare. Для этого один или несколько файлов объявляются флагами (в строке UpdateFlags), т.е. при изменении любого из них (периодичность контроля указана в строке UpdatePeriod), все вирусные базы перезагружаются. В частности, в качестве флаг-файла удобно использовать файл drwtoday.vdb («горячее» дополнение к вирусной базе Dr.Web).</p>
UpdatePeriod	<p>Интервал времени (в минутах), через который регулярно проверяются файлы из списка UpdateFlags.</p> <p>При установке значения параметра равным нулю (UpdatePeriod=0) автоматическая перезагрузка баз запрещается.</p>



Настройка	Комментарий
	При использовании модуля обновления рекомендуется указать UpdatePeriod=0.
EnableDeleteArchiveAction	Разрешение на удаление файловых архивов целиком (о действиях по отношению к инфицированным архивам см. Инфицированные архивы, почтовые файлы и контейнеры). По умолчанию задано значение параметра No, чтобы разрешить удаление, задайте значение Yes.

Настройка параметров конфигурационного файла



Все изменения в конфигурационном файле должны производиться при выгруженном (unloaded) **Dr.Web для NetWare**, иначе при завершении работы антивирус автоматически сохранит свои текущие настройки.

1. Откройте [конфигурационный файл](#) для редактирования в любом текстовом редакторе. По умолчанию конфигурационный файл называется drweb32.ini и находится в каталоге установки.
2. В секции [NetWare] задайте параметры работы программы.
3. Сохраните изменения в конфигурационном файле.

Секция [NetWare:Transit]

Dr.Web для NetWare поддерживает механизм так называемых «транзитных каталогов», применяющийся, в частности, в некоторых системах электронной почты. В рамках этого механизма один из каталогов на сервере объявляется *транзитным* и определяются каталоги для сортировки файлов:

- каталог для безопасных («чистых», неинфицированных) файлов;
- каталог для инфицированных файлов;
- каталог для подозрительных файлов.

При старте и во время работы **Dr.Web для NetWare** перемещает



файлы из транзитного каталога в один из трех сортировочных каталогов в зависимости от результатов проверки.



Для сортировки файлов из транзитного каталога необходимо, чтобы режим проверки «на лету» был включен.

Секция [NetWare:Transit] [конфигурационного файла](#) позволяет задать следующие параметры каталогов:

Настройка	Комментарий
TransitPath	Транзитный каталог.
CheckedFiles	Каталог для безопасных файлов.
InfectedFiles	Каталог для инфицированных файлов.
SuspiciousFiles	Каталог для подозрительных файлов.

Настройка параметров конфигурационного файла



Все изменения в конфигурационном файле должны производиться при выгруженном (unloaded) **Dr.Web для NetWare**, иначе при завершении работы антивирус автоматически сохранит свои текущие настройки.

1. Откройте [конфигурационный файл](#) для редактирования в любом текстовом редакторе. По умолчанию конфигурационный файл называется drweb32.ini и находится в каталоге установки.
2. В секции [NetWare:Transit] задайте параметры работы программы с транзитными каталогами.
3. Сохраните изменения в конфигурационном файле.

Параметры антивирусной проверки

Настройка параметров антивирусной проверки осуществляется в



окне **Scan settings** меню **Setup**, **Scheduler** и **On-access**.

Через меню **Setup** устанавливаются общие настройки проверки, действующие по умолчанию для всех процессов. В меню **Scheduler** и **On-access** можно настраивать индивидуальные параметры для соответствующих процессов.

Общие параметры сканирования

В окне **Scan settings** меню **Setup** вы можете выбрать каталоги и типы файлов, подлежащих (не подлежащих) проверке, варианты действия программы при обнаружении вирусов и др.

Окно **Scan settings** меню **Setup** позволяет задать следующие параметры антивирусной проверки:

Настройка	Комментарий
Options	Задает базовые опции.
Infected files	Задает действия с инфицированными файлами.
Suspicious files	Задает действия с подозрительными на вирус файлами.
Incurable files	Задает действия с инфицированными, но неизлечимыми файлами.
Adware	Задает действия с рекламными программами.
Dialers	Задает действия с программами дозвона.
Jokes	Задает действия с программами-шутками.
Riskware	Задает действия с потенциально опасными программами.
Hacktools	Задает действия с программами взлома.
Infected archives	Задает действия с инфицированными архивами.
Infected mail	Задает действия с инфицированными почтовыми файлами.
Infected containers	Задает действия с инфицированными контейнерами.



Настройка	Комментарий
File types	Задаёт файлы, подлежащие антивирусной проверке.
Exclude paths	Задаёт каталоги, исключённые из проверки.
Exclude files	Задаёт файлы, исключённые из проверки.
CPU usage factor	Задаёт приоритет данного процесса в системе.

Опции

Базовые настройки позволяют задать для указанного процесса следующие параметры:

- **Heuristic analysis** — использовать (не использовать) в процессе сканирования *эвристический анализатор*. Этот метод сканирования призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вредоносных программ, что позволяет с высокой эффективностью обнаруживать неизвестные вирусы;
- **Check archives** — проверять (не проверять) файлы в архивах;
- **Check mail files** — проверять (не проверять) файлы, имеющие формат электронных сообщений (UUENCODE, XXENCODE, BINHEX и MIME).

Инфицированные файлы

Данная настройка определяет, какие действия должна выполнить программа, если в процессе сканирования обнаружены инфицированные файлы. Возможны следующие варианты:

- **Log only** — только фиксировать факт обнаружения вируса, с указанием его названия и имени зараженного файла.
- **Move** — переместить инфицированный файл в специальную директорию. Данная директория указывается в настройках основных параметров **Setup | Move files to**. Эта директория является общей для всех процессов.



- **Delete** — удалить инфицированный файл.
- **Rename** — переименовать инфицированный файл. Переименованный файл сохраняет прежнее имя, но получает другое расширение. Маска для генерации расширения задается в настройках основных параметров **Setup | Rename files to**. Эта маска является общей для всех процессов.
- **Cure** — удалить код вируса из инфицированного файла.

Подозрительные и неизлечимые файлы

Подозрительные файлы — файлы, которые **эвристический анализатор Dr.Web** определил как возможно инфицированные неизвестным вирусом.

Неизлечимые файлы — файлы, которые поражены неизвестным вирусом, но восстановление которых невозможно.

Варианты действий программы по отношению к подозрительным и неизлечимым файлам аналогичны рассмотренным в разделе [Инфицированные файлы](#), однако, опция **Cure** не применяется.

Рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы, программы взлома

Настройка действий с вредоносными программами данных типов аналогична настройке реакции на обнаружение [подозрительных или неизлечимых файлов](#), однако, добавляется также действие **Ignore**.

Инфицированные архивы, почтовые файлы и контейнеры

Настройка действий с означенными файлами и архивами аналогична настройке реакции на обнаружение [подозрительных или неизлечимых файлов](#).



Заданное действие применяется ко всему архиву целиком при обнаружении в нем инфицированного или подозрительного файла, а также вредоносной программы.

Удаление архивов по умолчанию заблокировано. Для того чтобы разрешить удаление, [отредактируйте](#) параметр конфигурационного файла `EnableDeleteArchiveAction`.

Типы файлов

Эта настройка определяет, какие файлы должны проверяться данным процессом сканирования. Возможны следующие варианты:

- **All** — все файлы;
- **By type** — только по заданному списку расширений. Список расширений можно просматривать и редактировать. Добавление нового типа расширения в список производится при помощи клавиши `INS`, удаление — при помощи клавиши `DEL`. При задании расширений допустимо использование масок.

Исключаемые пути и файлы

Здесь определяется, какие каталоги/тома или файлы (без пути) исключаются из проверки в данном процессе сканирования. Допускается использование масок. Если в окне редактирования **Exclude paths** нажать клавишу `INS`, то можно просмотреть файловую структуру сервера.

Загрузка процессора

Здесь определяется приоритет данного процесса в системе. Чем больше числовое значение приоритета, тем выше доля использования времени процессора.



Дополнительные параметры сканирования по расписанию

Осуществляется в окне **Scan settings** меню **Scheduler**.

Чтобы просмотреть список процессов сканирования, включенных в расписание, выберите в панели управления пункт **Scheduler**. Добавление нового процесса в этот список производится при помощи клавиши **INS**, удаление — при помощи клавиши **DEL**.

Для каждого процесса сканирования по расписанию должны быть заданы:

- **Scan settings** — индивидуальные настройки (подробнее об опции см. [Общие параметры сканирования](#)). По умолчанию действуют настройки, заданные в **Setup | Scan settings**;
- **Scan paths** — список каталогов или томов сервера, которые подлежат проверке данным процессом. Если в окне редактирования нажать клавишу **INS**, то становится возможным просмотр файловой структуры сервера;
- **Days of week** — дни недели, в которые должен запускаться данный процесс;
- **Days of month** — дни месяца, в которые должен запускаться данный процесс;
- **Months** — месяцы, в которые должен запускаться данный процесс;
- **Time** или **Interval** — время в формате ЧЧ:ММ; название и интерпретация этого параметра зависят от того, как установлен указанный ниже параметр **Modes**;



• **Modes:**

- если установлен режим запуска **By time**, то процесс запускается точно в указанный параметром **Time** момент времени;
- если установлен режим периодического запуска **By interval**, то процесс запускается каждый раз по истечении указанного промежутка времени; в этом режиме значение параметра **Interval** интерпретируется не как момент времени, а как длительность промежутка (интервала) времени;
- кроме того, в настройках режима запуска процесса можно установить признак (атрибут) временного отключения **Hold**. Процессы, для которых установлен этот атрибут, остаются (вместе со всеми настройками) в списке процессов, запускаемых по расписанию, но в отключенном состоянии — запуск их не производится.

Значение параметров **Days of week**, **Days of month** и **Months** учитывается только для процессов, запускаемых в режиме **By time**; для процессов, запускаемых **By interval**, оно игнорируется.

Процесс, запускаемый в режиме **By time**, запускается в дни, когда одновременно выполняются оба условия, определенные значением параметров **Days of week** и **Days of month**.

Параметры, задающие расписание запуска данного процесса, отображаются в соответствующей этому процессу строке списка процессов, запускаемых по расписанию. В конце каждой такой строки указываются признак активности и режим запуска данного процесса:

- - — процесс включен в расписание, но в данный момент не активен;
- ! — процесс активен, т.е. в данный момент выполняется;
- H — для процесса установлен атрибут **Hold**, т.е. процесс временно исключен из расписания;
- i — по интервалу;
- t — по времени.



Дополнительные параметры сканирования «на лету»

Осуществляется в окне **Scan settings** меню **On-access**.

Этот процесс осуществляет антивирусный контроль файлов, записываемых с рабочих станций на сервер, и файлов, открываемых рабочими станциями на сервере. При этом антивирусная проверка файла на сервере инициируется в тот момент, когда сервер выполняет запрос рабочей станции на соответствующую файловую операцию.

При записи некоторой рабочей станцией нового файла на сервер, а также при изменении (записи) существующего файла, доступ к такому файлу блокируется для всех прочих рабочих станций, пока данный файл не будет проверен.

Настраиваемые опции:

- **Scan settings** – настройки сканирования «на лету» (о настраиваемых опциях см. [Общие параметры сканирования](#)).
- **Modes** – для процесса сканирования «на лету» должны быть заданы режимы его работы, определяющие, запросы каких файловых операций должны перехватываться им для антивирусной проверки:
 - **Open files** — открытие рабочей станцией файла на сервере;
 - **Write files** — запись с рабочей станции в существующий файл на сервере;
 - **Create files** — запись рабочей станцией нового файла на сервер.

Каждый из этих режимов может быть включен или выключен. Отключение всех трех возможных режимов эквивалентно отключению процесса сканирования «на лету».



Глава 5. Антивирусная проверка

В окне программы выводится информация на нескольких полях:

- «Статистика»: **Next Event, Status**, текущие дата и время;
- Основная панель управления;
- Информация о программе;
- Информация о лицензии и текущем режиме.

Через панель управления осуществляются все действия по настройке, управлению и контролю работы антивируса. Ниже перечислены элементы панели управления и их описание:

Элемент	Комментарий
Setup	Настройка основных параметров работы антивируса.
Monitor	Управление, просмотр и запуск по запросу процессов сканирования.
Scheduler	Настройка процессов, запускаемых по расписанию.
On-access	Настройка процесса сканирования «на лету».
Log	Журнал событий.
Exit	Завершение работы с программой.

Методы обнаружения вирусов

Все антивирусы «**Доктор Веб**» одновременно используют несколько методов обнаружения вредоносных объектов, что позволяет максимально тщательно проверить подозрительные файлы и контролировать поведение программ:

1. В первую очередь применяется *сигнатурный* анализ. Он выполняется путем анализа кода подозрительных файлов на предмет соответствия сигнатурам известных вирусов (сигнатурой называется непрерывная конечная последовательность байт, необходимая и достаточная для опознания вируса). При этом сравнение проводится по



контрольным суммам сигнатур, что позволяет значительно снизить размер записей в вирусных базах данных, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения и лечения зараженных файлов. Вирусная база антивирусов Dr.Web составлена таким образом, что благодаря одной записи можно обнаруживать целые классы угроз.

2. После завершения сигнатурного анализа применяется уникальная технология **Origins Tracing**, которая позволяет определить новые или модифицированные вирусы, использующие известные механизмы заражения файлов. Так, например, эта технология защищает пользователей антивирусных решений **Dr.Web** от таких вирусов, как вирус-шантажист Trojan.Encoder.18 (так же известный под названием **gpcode**). Кроме того, именно введение **Origins Tracing** позволяет значительно снизить количество ложных срабатываний эвристического анализатора.
3. Работа эвристического анализатора основывается на неких знаниях (*эвристиках*) о характерных признаках вирусного и, наоборот, безопасного кода. Каждый признак имеет определенный вес (число, показывающее серьезность и достоверность данного признака). На основании суммарного веса, характеризующего каждый конкретный файл, эвристический анализатор вычисляет вероятность заражения файла неизвестным вирусом. Как и любая система проверки гипотез в условиях неопределенности, эвристический анализатор может допускать ошибки как первого (пропуск неизвестных вирусов), так и второго рода (ложная тревога).

Во время любой из проверок компоненты антивирусов **Dr.Web** используют самую свежую информацию обо известных вредоносных программах. Сигнатуры вирусов, информация об их признаках и моделях поведения обновляется сразу же, как только специалисты **Антивирусной Лаборатории «Доктор Веб»** обнаруживают новые угрозы, иногда – до нескольких раз в час. Даже если новейший вирус проникает на компьютер, минуя резидентные средства защиты, после обновления вирусных баз он будет обнаружен в списке процессов и нейтрализован.



Способы запуска антивирусной проверки

Функции антивирусной защиты осуществляются процессами сканирования. Существует три типа таких процессов.

1. Процессы, запускаемые по явному запросу пользователя.
Запуск: **Monitor -> INS -> выбрать путь (path)**. См. [Действия с активными процессами](#).
2. Процессы, запускаемые по заданному расписанию.
Запуск: **Scheduler -> установить параметры времени -> Scan settings**.

О настройке параметров сканирования см. [Общие параметры сканирования](#).

Подробнее о меню **Scheduler** см. [Дополнительные параметры сканирования по расписанию](#).

3. Процесс сканирования «на лету». Выбрать необходимый режим сканирования в меню **On-access | Modes**.

Подробнее о меню **On-access** см. [Дополнительные параметры сканирования «на лету»](#).

Стандартные параметры процессов сканирования можно задать через **Setup | Scan settings**. Эти настройки действуют по умолчанию для всех процессов сканирования.

Для процессов сканирования «на лету» и по расписанию также можно задать индивидуальные параметры. Параметры процессов по расписанию настраиваются через меню **Scheduler | Scan settings**. Параметры сканирования «на лету» устанавливаются в меню **On-access | Scan settings**.



Действия с активными процессами

Чтобы просмотреть список активных на данный момент процессов сканирования, выберите в панели управления пункт **Monitor**.

Также по каждому из процессов можно просмотреть статистику. В окне статистики динамически отображается информация о времени работы каждого процесса, количестве проверенных файлов, количестве обнаруженных этим процессом вирусов и др. Чтобы вызвать окно статистики для конкретного процесса, выберите этот процесс из списка активных и нажмите клавишу ENTER.

Любой процесс из списка активных можно отменить при помощи клавиши DEL.

Чтобы создать новый процесс, нажмите INS. В окне редактирования клавиша INS служит для просмотра файловой структуры сервера. Чтобы немедленно запустить сканирование выбранного каталога или тома сервера (сканирование on-demand), нажмите ENTER.

Стандартные настройки создаваемых таким образом процессов устанавливаются в соответствии с заданными в пункте меню **Setup | Scan settings**.



Глава 6. Регистрация событий

В журнал событий заносится информация, получаемая при работе процессов сканирования.

Просмотр и управление журналом осуществляется из меню **Log** основной панели управления **Dr.Web для NetWare**. Возможны следующие действия с журналом:

- **View** – просмотреть журнал;
- **Options** – [настроить журнал](#);
- **Clear** – очистить журнал.

Настройка ведения журнала

Настройка ведения и просмотр журнала событий осуществляется из меню **Log** основной панели управления **Dr.Web для NetWare**.

В меню **Options** предусмотрены следующие опции ведения журнала событий:

- **Log to file** — вести ли журнал событий;
- **Overwrite log** — перезаписывать или дополнять существующий журнал событий при каждом очередном запуске антивируса;
- **Log scanned files** — заносить ли в журнал информацию о файлах, в которых при проверке вирусов не обнаружено и не зафиксировано подозрений на заражение неизвестным вирусом;
- **Log packed files** — заносить ли в журнал информацию об упаковщиках, использованных в проверенных программных файлах;
- **Log archived files** — заносить ли в журнал информацию об архиваторах, использованных для упаковки проверенных файлов.



Глава 7. Модуль обновления

Для обнаружения вредоносных объектов **Dr.Web для NetWare** использует специальные **вирусные базы Dr.Web**, в которых содержится информация обо всех известных вредоносных программах. Так как каждый день появляются новые вредоносные программы, то эти базы требуют периодического обновления. Для этого в **Dr.Web для NetWare** реализована система обновления вирусных баз через Интернет. В течение срока действия лицензии модуль обновления регулярно скачивает и устанавливает информацию о новых вирусах и вредоносных программах, а так же обновления самого антивируса **Dr.Web для NetWare**.

Модуль обновления (drwebupn.nlm) позволяет получать обновления **вирусных баз Dr.Web** (файлов *.vdb и соответствующих им *.txt), антивирусного ядра сканера (drweb32.dll) и устанавливать их. Также с помощью данной программы можно получать и использовать в процессе обновлений список доступных серверов обновления (update.drl).

Модуль предназначен для работы со сканером версии 4.44 или более поздней.



Для того чтобы обновить необходимые компоненты, необходимо запустить сканер (drwebnw.nlm) прежде программы обновления. В противном случае будет выводиться сообщение о невозможности получения пути к вирусным базам (cannot get path to virus bases). Аналогичное сообщение будет выводиться и в случае использования более ранних (чем 4.44) версий сканера.

При получении обновлений программа сообщает сканеру о необходимости загрузки обновленных компонентов. Загрузка обновлений сканером производится независимо от интервала и флага проверки на наличие обновлений (параметры UpdateFlags и UpdatePeriod в drweb.ini в [секции \[NetWare\]](#) конфигурационного файла).



После запуска программа, в соответствии со стандартными настройками, переходит в режим периодического опроса серверов обновлений. Настройка интервала между запросами и задание адреса сервера обновлений производится с помощью параметров командной строки. Для того чтобы прекратить работу программы в данном режиме, выполните команду операционной системы NetWare `UNLOAD DRWEBUPN`.

Завершение выполнения программы также производится при выключении либо перезагрузке сервера NetWare командами `DOWN`, `RESET SERVER`, `RESTART SERVER`.

При желании вы можете [настроить](#) работу модуля обновления.

Настройка модуля обновления

Настройка программы производится с помощью следующих параметров командной строки (для хранения настроек не используются файлы конфигурации):

- `/url:<url>` адрес сервера обновлений. Если данный параметр не указан, то адреса серверов обновлений читаются из файла `update.drl`, расположенного в каталоге сканера;
- `/user:<user name>` имя пользователя для авторизации по http-протоколу (в настоящее время данная возможность не используется на серверах обновлений компании «**Доктор Веб**»);
- `/pass:<user password>` пароль для авторизации по http-протоколу (в настоящее время данная возможность не используется на серверах обновлений компании «**Доктор Веб**»);
- `/purl:<proxy url>[:<port>]` адрес и порт http-прокси (в случае его использования). Если порт не указан, используется стандартное значение `<port>` равное 80;
- `/puser:<proxy user name>` имя пользователя для авторизации на http-прокси (если используется прокси-сервер);
- `/ppass:<proxy user password>` пароль для авторизации на



http-прокси (если используется прокси-сервер);

- /qf завершить работу программы после выполнения обновления;
- /uvb обновлять только вирусные базы (*.vdb и *.txt) и ядро (drweb32.dll), параметр задан по умолчанию;
- /uvb- обновлять все файлы;
- /dir:<directory>- каталог для хранения обновленных файлов, по умолчанию используется каталог сканера;
- /interval:<minutes> интервал ожидания между получением обновлений, по умолчанию 10 мин. Не может быть меньше 1 мин;
- /pwsepscr создать отдельный экран для сообщений программы. По умолчанию сообщения программы выводятся на системную консоль или Logger Screen сервера NetWare;
- /verbose вывести отчет о связи с сервером обновлений, используется для отладки. Без указания дополнительного параметра отчет выводится в файл журнала программы;
- /verbose:log отчет (см. /verbose) выводится в файл журнала программы;
- /verbose:screen отчет (см. /verbose) выводится на консоль сервера;
- /debugoutput более подробный отчет, чем /verbose, используется для отладки;
- /debugoutput:log отчет (см. /debugoutput) выводится в файл журнала программы;
- /debugoutput:screen отчет (см. /debugoutput) выводится на консоль сервера;
- /uptodate выводить в файл журнала программы сообщения о попытках обновления, даже если обновленных файлов нет;
- /autoupdate автоматически перезапускать сам модуль обновления, если файл drwebupn.nlm был обновлен. Для использования этого параметра необходимо указывать ключ /uvb-;
- /maxlogsize:[<n>] максимальный размер лог-файла, указывается в килобайтах. По умолчанию равен 512 КБ;
- /notifyskipped сообщать о пропущенных (не загруженных с серверов обновлений) файлах;



- `/notifynotrestarted` сообщать о загруженных, но не запущенных исполняемых файлах;
- `/notifyrestarted` сообщать о загруженных и запущенных исполняемых файлах;
- `/notifyaddr:[<username>[;<username>]...]` имена пользователей, получающих уведомления. Если пользователь не указан, получателем уведомлений считается пользователь с именем `admin`;
- `/notifyinterval:<minutes>` интервал между рассылкой одинаковых уведомлений, по умолчанию 30 минут;
- `/notifyonce` рассылать одинаковые уведомления только один раз;
- `/help` вывести краткую подсказку по параметрам и завершить работу.

При указании получателя уведомлений программа будет высылать этому пользователю также уведомление о внештатном завершении своей работы.



Приложения

Приложение А. Элементы интерфейса

Dr.Web для NetWare не поддерживает русский язык. Ниже приведен перевод на русский язык наиболее часто встречающихся элементов интерфейса:

Элемент	Перевод
Adware	Рекламные программы
All	Все
By interval	По интервалу
By time	По времени
By type	По типам
Check archives	Проверка архивированных файлов
Check mail files	Проверка почтовых файлов
Clear	Очистить
CPU usage factor	Загрузка процессора
Create files	Создание файлов
Create flag file	Создание флаг-файла
Cure	Лечить
Days of month	Дни месяца
Days of week	Дни недели
Delete	Удалить
Dialers	Программы дозвона
Disconnect message	Сообщение об отключении
Disconnect station	Отключение станции



Disconnected users	Отключенные пользователи
E-mail notification	Уведомление по e-mail
Exclude files	Исключаемые файлы
Exclude paths	Исключаемые пути
Exit	Выход
File types	Типы файлов
Flag file name	Имя флаг-файла
Hacktools	Программы взлома
Heuristic analysis	Эвристический анализ
Hold	Приостановить
If virus found	Если обнаружен вирус
Ignore	Игнорировать
Incurable files	Неизлечимые файлы
Infected archives	Инфицированные архивы
Infected containers	Инфицированные контейнеры
Infected files	Инфицированные файлы
Infected mail	Инфицированные почтовые файлы
Interval	Интервал
Jokes	Программы-шутки
Log	Журнал
Log archived files	Архивированные
Log only	Только отчет
Log packed files	Упакованные
Log scanned files	Проверенные
Log to file	Файл отчета
Miscellaneous	Прочее
Modes	Режимы
Monitor	Монитор



Months	Месяцы
Move	Переместить
Move files to	Куда перемещать файлы
Next Event	Следующее событие
No	Нет
On-access	На лету
Open files	Открытие файлов
Options	Опции
Overwrite log	Перезаписывать
Rename	Переименовать
Rename files to	Во что переименовывать
Ring the bell	Звуковой сигнал
Riskware	Потенциально опасные программы
Scan paths	Пути для проверки
Scan settings	Настройки проверки
Scheduler	Планировщик
Send message	Посылка сообщения
Send messages to	Кому посылать сообщение
Setup	Настройки
Status	Статус
Suspected file message	Сообщение о подозрении
Suspicious files	Подозрительные файлы
Time	Время
View	Просмотр
Virus bases	Вирусные базы
Virus found message	Сообщение о вирусе
Write files	Запись в файлы
Yes	Да

