

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОДДЕРЖКИ И РАЗРАБОТКИ 125375, г. Москва, ул. Тверская, дом 7, подъезд 7, 2-ой этаж, офис 1а.

телефон: +7 (495) 988-27-09 факс: +7 (495) 745-40-81 www.ncpr.su



Основные функциональные возможности Dr.WEB Security Suite для Linux

- Поиск и обезвреживание вредоносных и нежелательных программ
- Изоляция инфицированных и подозрительных объектов в специальном хранилище
- Отслеживание обращения к файлам с данными и попыток запуска исполняемых файлов
- Проверка объектов файловой системы как по запросу, так и по расписанию
- Отслеживание попыток и блокировка доступа к веб-сайтам Интернет
- Обнаружение вирусных угроз методами сигнатурного и эвристического анализа
- Автоматическое обновление компонентов и пополнение вирусных баз
- Возможность использования как в локальном, так и в сетевом вариантах
- Наличие версий, сертифицированных по требованиям безопасности информации



Последовательность установки Dr.WEB Desktop Security Suite

Войдите в систему от имени суперпользователя root, выберите Приложения → Системные → Терминал и с помощью команды *mkdir/путь_к_каталогу/имя_каталога* создайте на жёстком диске каталог для размещения файла дистрибутива антивирусной программы Dr.WEB Desktop Security Suite (для Linux), например:

Σ				root@lo	ocalhost:~ _ 🗆	×
Файл	Правка	Вид	Поиск	Терминал	Справка	
[root@ [root@	localhost localhost	:~]# :~]#	mkdir 	/home/admin	n/Distributives	^
						=
						~



Вставьте оптический диск, содержащий файл с дистрибутивом антивирусной программы, в привод для чтения оптических дисков и с помощью команды *lsblk* определите путь его монтирования, после чего скопируйте файл дистрибутива на жёсткий диск с помощью команды *ср*, например:

🗉 root@localhost:~ _ 🗆	×
Файл Правка Вид Поиск Терминал Справка	
<pre>[root@localhost ~]# cp -av /media/DrWeb\ 10.0\ 3-3/files/drweb-workstations_10.1 .0.0-1510201250+fstek~linux_amd64.run /home/admin/Distributives/ «/media/DrWeb 10.0 3-3/files/drweb-workstations_10.1.0.0-1510201250+fstek~linux_ amd64.run» -> «/home/admin/Distributives/drweb-workstations_10.1.0.0-1510201250+ fstek~linux_amd64.run» [root@localhost ~]# []</pre>	
	III



Разрешите исполнение файла дистрибутива антивирусной программы с помощью команды *chmod*



и перейдите в каталог с файлом дистрибутива с помощью команды cd /home/admin/Distributives



Временно переведите подсистему безопасности SELinux в режим Permissive (разрешающий) с помощью команды setenforce 0. Узнать текущий режим SELinux можно командой getenforce

root@localhost:/home/admin/Distributives	_ 🗆 🗙
Файл Правка Вид Поиск Терминал Справка	
[root@localhost Distributives]# getenforce	^
Entorcing [root@localbost Distributives]# setenforce 0	
[root@localhost Distributives]# getenforce	
Permissive	
[root@localhost Distributives]# []	
	=
	~



Запустите файл дистрибутива на исполнение

🗉 root@localhost:/home/admin/Distributives _ 🗆 ×
Файл Правка Вид Поиск Терминал Справка
[root@localhost Distributives]# ./drweb-workstations_10.1.0.0-1510201250+fstek~l inux amd64.run
Creating directory drweb-workstations_10.1.0.0-1510201250+fstek~linux_amd64
Uncompressing Dr.Web for Linux workstations
<pre>'/home/admin/Distributives/drweb-workstations_10.1.0.0-1510201250+fstek~linux_am d64/setup.sh'</pre>
No printers found!



После запуска файла дистрибутива откроется окно установки. Нажмите кнопку «Продолжить», а затем, ознакомившись с условиями лицензионного соглашения, нажмите кнопку «Установить»

後	Dr.Web для Linux _ ×
	Благодарим вас за выбор Dr.Web для Linux 10 Dr.Web для Linux 10 обеспечивает многоуровневую защиту операционной системы, жестких дисков и сменных носителей от проникновения вирусов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов из любых внешних источников.
	Нажимая кнопку Установить, вы соглашаетесь с условиями Лицензионного соглашения ✓ Я хочу подключиться к облачным сервисам Dr.Web Cloud Установить Отменить
	© «Доктор Веб», 1992-2015



Дождитесь успешного завершения установки



и верните подсистему безопасности SELinux в режим Enforce (обеспечивающий соблюдение), выполнив команду setenforce 1



Запуск антивирусной программы может быть произведен с помощью меню Приложения — Dr.Web — Dr.Web для Linux







При первом запуске программы предлагается ее активировать. Это можно сделать с помощью подключения к сети Интернет или автономно, выбрав «Другие виды активации» и указав путь к ключевому файлу, который, в свою очередь, можно получить зарегистрировав серийный номер программы по адресу: https://products.drweb.ru/register/2015/?lng-ru

*	Мастер регистрации		×
	Активация посредством файла		
	Укажите имеющийся ключевой файл или файл настроек подключения к серверу централизованной защиты		
	/media/344F-1846/agent.key	Обзор	
	Что такое лицензионный ключевой файл?		
	Что такое файл настроек подключения?		
	Назад Готово		



После успешного завершения процесса активации выдается соответствующее сообщение, увидев которое нажмите кнопку «ОК» и появится главная страница программы







Подключитесь к Интернет и обновите вирусные базы, выбрав пункт меню «Ошибка обновления», нажав в появившемся окне кнопку «Повторить» и дождавшись завершения процесса обновления

*	Dr.Web для Linux _ 🗆 🗙
	Ошибка обновления
9	Dr.Web для Linux использует вирусные базы для выявления и устранения вирусов и других нежелательных программ на вашем компьютере
•	Послелнее обновление
	12:44 21/11/2016
	Ошибка x94. Нет доступных серверов обновлений. <mark>Подробнее</mark>
\odot	
?	Повторить



После обновления вирусных баз необходимо вручную собрать модуль, обеспечивающий работоспособность монитора SpiDer Guard. Для этого с помощью команды *cd* перейдите в *каталог /opt/drweb.com/share/drweb-spider-kmod/src*

Σ	root@	locall	nost:/op	t/drweb.co	m/share/drweb-spider-kmod/src	-	×
Файл	Правка	Вид	Поиск	Терминал	Справка		
[root@ [root@	localhos† localhos†	t ~]# t src]	cd /opt]# []	t/drweb.com	/share/drweb-spider-kmod/src/		^
							Ξ
							\sim



Распакуйте содержимое архива с исходными кодами в текущий каталог с помощью команды *tar*

root@localhost:/opt/drweb.com/share/drweb-spider-kmod/src	×
Файл Правка Вид Поиск Терминал Справка	
[root@localhost src]# tar -xf drweb-spider-kmod-10.1.0.0-1505261016.tar.bz2 [root@localhost src]# []	
	=



С помощью команды *cd* перейдите в созданный каталог с исходными кодами







Выполните команду таке

🔄 root@localhost:/opt/drweb.com/share/drweb-spider-kmod/src/drweb-spid 🚊 🗆	×
Файл Правка Вид Поиск Терминал Справка	
<pre>[root@localhost drweb-spider-kmod-10.1.0.0-1505261016]# depmod [root@localhost drweb-spider-kmod-10.1.0.0-1505261016]#]</pre>	



После завершения *таке* выполните команду *таке install*

토 root@localh	10st:/opt/drw	eb.com/sha	re/drweb-spider-kmod/src/drweb-spid 💷 🗆 🗙
Файл Правка	Вид Поиск	Терминал	Справка
[root@localhos make -C /lib/m re/drweb-spide make[1]: Enter INSTALL /opt 1505261016/drw DEPMOD 2.6. make[1]: Leavi [root@localhos	t drweb-spid odules/2.6.3 r-kmod/src/d ing director /drweb.com/s web.ko 32-431.17.1. ng directory t drweb-spid	er-kmod-10 2-431.17.1 rweb-spiden y `/usr/sro hare/drweb sp6.x86_64 `/usr/src/ er-kmod-10	<pre>1.1.0.0-1505261016]# make install .sp6.x86_64/build SUBDIRS=/opt/drweb.com/sha r-kmod-10.1.0.0-1505261016 modules_install c/kernels/2.6.32-431.17.1.sp6.x86_64' -spider-kmod/src/drweb-spider-kmod-10.1.0.0- /kernels/2.6.32-431.17.1.sp6.x86_64' .1.0.0-1505261016]# ■</pre>



Затем выполните команду depmod

Файл Правка Вид Поиск Терминал Справка [root@localhost drweb-spider-kmod-10.1.0.0-1505261016]# depmod [root@localhost drweb-spider-kmod-10.1.0.0-1505261016]#]
<pre>[root@localhost drweb-spider-kmod-10.1.0.0-1505261016]# depmod [root@localhost drweb-spider-kmod-10.1.0.0-1505261016]#]</pre>



После завершения depmod выполните команду drweb-ctl cfset LinuxSpider.Mode LKM

🗵 roo	t@localho	ost:/o	pt/drw	eb.com/s	hare/d	rweb-	spider-km	od/src/drv	veb-sp	ider-kmod	-10.1.0	_ 0	×
Файл	Правка	Вид	Поиск	Термина	л Спр	равка							
[root@	localhost	drwe	b-spid	er-kmod-1 er-kmod-1	0.1.0	.0-150 .0-150	5261016]# 5261016]#	drweb-ctl	cfset	LinuxSpid	er.Mode	LKM	<
													=



Теперь после запуска антивирусной программы Dr.Web для Linux ее главное окно будет выглядеть следующим образом







Спасибо за внимание

