ClamAV

Пакет антивирусного ПО, работающий во многих операционных системах, включая Unix-подобные ОС, OpenVMS, Microsoft Windows и Apple Mac OS X.

Выпускается под GNU General Public License и является свободным программным обеспечением.

http://www.clamav.net

http://sourceforge.net/projects/clamav/

Установка

```
apt-get install clamav-daemon
```

Настройка

Fix Me!

```
service clamav-daemon
Usage:   /etc/init.d/clamav-daemon   {start|stop|restart|force-reload|reload-log|reload-database|status}

service clamav-freshclam
Usage:   /etc/init.d/clamav-freshclam   {no-daemon|start|stop|restart|force-reload|reload-log|skip|status}

/etc/clamav
/var/log/clamav
```

Работа через proxy

В файл `/etc/clamav/freshclam.conf` нужно добавить:

```
HTTPProxyServer proxy
HTTPProxyPort 3128
```

Список URL, например для работы через Squid

/usr/local/etc/squid/ClamAV.urls

```
db.ru.clamav.net
db.local.clamav.net
current.cvd.clamav.net
clamav.net
clamwin.sourceforge.net
clamtk.sourceforge.net
clamsentinel.sourceforge.net
www.clamwin.com
downloads.sourceforge.net/clamwin
sourceforge.net/projects/clamwin
```

AMaViSd

Настройка ClamAV для AMaViSd

Перед использованием ClamAV с сторонними программами нужно сначала обновить его базы.

ClamSMTPd

ClamSMTP — это служба SMTP-прокси, которая проверяет проходящие письма с помощью антивирусного ПО ClamAV. Она может работать как обычный SMTP-прокси на общедоступных портах или как прозрачный прокси, если SMTP-трафик перенаправляется на ClamSMTP с помощью маршрутизатора.

Можно использовать с Postfix

Установка

```
apt-get install clamsmtp
```

Настройка

Файл `etc/clamsmtpd.conf`

Отключение

```
service clamav-daemon stop
service clamav-freshclam stop

systemctl disable clamav-daemon
systemctl disable clamav-freshclam
```

ClamTk

Графический интерфейс для `ClamAV`

```
apt-get install clamtk
```

ClamFS

ClamFS — основанная на FUSE файловая система для Linux с встроенным антивирусным сканированием посредством `clamd`.

```
apt install clamfs
```

Samba+ClamAV. Создаем защищенную от вирусов папку общего сетевого обмена. | Блокнот обычного админа =)

BlackDiver.Net | ClamFS — сканирование антивирусом ClamAV папок на лету.

ClamWin

Свободный антивирусный сканер для платформ Microsoft Windows 98/Me/2000/XP/2003/Vista.

Он обеспечивает графический интерфейс пользователя к программе `ClamAV`

http://ru.clamwin.com/

http://sourceforge.net/projects/clamwin/

Clam Sentinel

Это программа с иконкой в системном трее которая обнаруживает изменения в файловой системе и сканирует измененные файлы используя ClamWin (требуется установка этого антивируса).

Также обнаруживает подключение новых дисков (как правило USB-накопителей) и проверяет эти устройства пока её не закроют или не отключат устройство.

http://clamsentinel.sourceforge.net/

http://sourceforge.net/projects/clamsentinel/

EICAR

Тестовый вирус EICAR для проверки работоспособности.

EICAR (или EICAR-Test-File — от European Institute for Computer Antivirus Research) — стандартный файл, применяемый для проверки, работает ли антивирус.

EICAR

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

http://www.eicar.org/86-0-Intended-use.html

https://ru.wikipedia.org/wiki/EICAR-Test-File

http://sysadminmosaic.ru/clamav/clamav

2023-01-13 16:47