

# Что нового в Антивирусе Касперского, работающем на платформе Unix

## Версия 4.0.0.0

### Keeper

Для нормального функционирования процесса проверки почтового трафика необходимо до запуска почтового агента загрузить следующие программы: *kavdaemon*, *kavuss*, *kavkeeper*. Причем *kavdaemon* и *kavuss* должны быть запущены до *kavkeeper*.

### Scanner и Daemon

1. Добавлены ключи командной строки:

**-AE[-]**

отключить распаковку самораспаковывающихся архивов.

**-AS[-]**

отключить проверку OLE-объектов, вложенных в сканируемые файлы.

2. Расширена опция **-W[путь\_к\_файлу]**. Теперь Вы можете задавать как относительный, так и абсолютный путь к файлу отчета.
3. Добавлена возможность включения в область сканирования (файл *defUnix.prf*, параметр **Names** секции **[Object]**) или исключения из нее ссылок. Правила обработки ссылок задаются параметром **Symlincs** секции **[Options]**.

Например, если параметром **Names** секции **[Object]** файла *defUnix.prf* задано сканирование ссылки */home/user/mydoc*, а

**Symlincs=0**, то файлы и папки по данной ссылке проверяться не будут.

## Версия 4.0.0.1

### Updater

Добавлены ключи командной строки:

#### **-g[=base]**

использовать для хранения параметров работы программы базу с именем **base**. По умолчанию **base=defUnix**.

#### **-gd[q]**

сохранить заданные после данного ключа настройки в базе, используемой по умолчанию. Необязательный элемент ключа **q** определяет, будет ли в текущей сессии запущена программа Updater, а именно:

- ключ **-gdq** отменяет запуск программы с заданными параметрами, но указывает на их сохранение в базе;
- ключ **-gd** указывает на запуск программы в текущей сессии с указанными параметрами и сохранение их в базе.

Например, если в командной строке ввести:

```
./kavupdater -gd  
-uik=http://www.kaspersky.com/updates -ws
```

то будет запущено обновление антивирусных баз с заданного адреса, и результаты обновления зафиксируются в системном журнале.

При повторном запуске программы следующей строкой:

```
./kavupdater
```

обновление будет осуществляться с адреса <http://www.kaspersky.com/updates>, а результаты работы также будут отражены в системном журнале, поскольку ключ **-gd** при предыдущем запуске сохранил все параметры запуска программы в базе.

#### **-l[q]**

отразить заданные после данного ключа параметры на экране. Необязательный элемент ключа **q** определяет, будет ли в текущей сессии запущена программа Updater, а именно:

- ключ **-lq** выводит на экран заданные параметры, но не запускает обновление антивирусных баз;
- ключ **-l** выводит на экран параметры работы и запускает программу Updater.

## Версия 4.0.1.0

### Даemon

1. Расширен режим записи в сокет командной строки при проверке объектов без предварительной записи на диск (режим 3). Теперь строка может включать имя файла и принимать следующий вид:

**<3>дата\_и\_время:<ключ|длина|имя\_файла>**

где:

| – символ, разделяющий секции;

**ключ** – значение, полученное при помощи функции **ftok()**;

**длина** – размер разделяемой памяти;

**имя\_файла** – название файла, который необходимо проверить.



Такой режим определяет отражение более конкретной информации (вплоть до названия файла) об объектах сканирования в отчете. Вы можете также использовать прежний способ записи в сокет командной строки (не указывать имя файла)!

2. Добавлен параметр **CopyEqual** в секции **[ActionWithInfected]**, **[ActionWithCorrupted]** и **[ActionWithSuspicion]** файла *defUnix.prf*. Значение **Yes** данного параметра включает режим копирования временных файлов с одинаковыми именами с добавлением к имени файла его порядкового номера.

## Версия 4.0.2.0

### Все программы

Реализован механизм блокировки доступа, а также многопользовательского доступа к базе настроек программ.

### Control Centre

Добавлены ключи командной строки:

**-r[=[hostname:]port]**

управление программой Control Centre с удаленного компьютера.

**-ms=server**

адрес сервера, с которого будет отправляться уведомление о завершении лимита трафика.

**-mf=from**

адрес, с которого будет отправляться уведомление о завершении лимита трафика.

**-mt=to**

адрес, на который будет отправляться уведомление о завершении лимита трафика.

**-mat=Mb**

размер лимита трафика в Mb.

**-cp[w]="prgname -a:arg[:arg1[...]] -u=username  
-e=hour:min"**

запустить программу **prgname** в текущий момент времени с указанными параметрами,

где:

**prgname** – имя исполняемого файла программы **prgname**.

**-a:arg[:arg1[...]]** – параметры работы программы **prgname**.

**-u=username** – имя пользователя, под которым будет запущена программа **prgname**.

**-e=hour:min** – время работы программы **prgname**, по завершении которого она будет закрыта.

Необязательный элемент ключа **w** включает режим ожидания завершения работы программы и выводит код ее возврата на экран и в отчет.

**-cpt**

проверить, запустилась ли программа **prgname** по ключу **-cp[w]**.

**-cpk**

завершить работу программы **prgname**, запущенной по ключу **-cp[w]**.

## Keeper

Расширены возможности утилиты **kldbedit**. Теперь можно импортировать бинарную базу с настройками программы Кеерг в текстовый файл и редактировать ее, а затем экспортировать обратно в бинарный формат. Такой режим работы не требует использования программы WebTuner.

# Версия 4.0.2.1

## Scanner и Daemon

1. Добавлено новое значение для параметра **InfectedFiles** секции **[ActionWithInfected]** файла *defUnix.prf* – **4**, которое позволяет переименовывать инфицированные файлы, если задан режим их копирования в директорию, определяемую параметром **InfectedFider**. При этом используется расширение, заданное параметром **ChangeExt**.
2. Соответственно предыдущему пункту был добавлен ключ командной строки **-I4**.
3. В конфигурационный файл *defUnix.prf* добавлена секция **[Mail]**, включающая следующие параметры отправки уведомлений:

**SendMail** – режим отправки уведомлений об обнаружении инфицированного объекта. Значение **Yes** включает режим, значение **No** – отключает.

**SendOnEach** – режим отправки уведомлений по каждому инфицированному объекту. Значение **Yes** включает режим, значение **No** – отключает.

**SendAtEnd** – режим отправки уведомлений по результатам проверки. Значение **Yes** включает режим, значение **No** – отключает.



**Необходимо включить только один режим: либо **SendOnEach**, либо **SendAtEnd**.**

**SMTPServer** – адрес smtp-сервера, с которого будут отправляться уведомления. Строка имеет следующий синтаксис:

**smtp:имя\_сервера.домен.ru(com и т.п.)**

**SendFrom** – адрес, с которого будут отправляться уведомления.

**SendTo** – адрес, на который будут отправляться уведомления.  
Можно задавать маску адресов.

**CC** – адреса, на которые будут отправляться копии уведомлений.

Например, секция может иметь следующий вид:

```
[Mail]
SendMail=Yes
SendOnEach=Yes
SendAtEnd=No
SMTPServer=smtp:anton.localhost.ru
SendFrom=anton@localhost.ru
SendTo=*@mydomain.com
CC=admin@mydomain.com
```

### WebTuner и Keeper

Добавлены новые макроконструкции, используемые при формировании уведомлений для администраторов, отправителей и получателей сообщений:

- **%SENDER%** – макроконструкция подстановки в текст уведомления адреса отправителя инфицированного сообщения.
- **%RECIPIENT%** – макроконструкция подстановки в текст уведомления адреса получателя инфицированного сообщения.
- **%KAVANSWER%** – макроконструкция подстановки в текст уведомления отчета программы Daemon о результатах проверки инфицированного сообщения.

## Версия 4.0.2.2

### Все программы

При открытии файла с отчетом о результатах работы выполняется проверка на существование файла с аналогичным именем. Такая операция реализована для предотвращения потери информации при ошибочном создании пользователем файла с именем уже существующего файла-отчета.

### Updater

Добавлены ключи командной строки:

**-gu**

удаление из конфигурационной базы значений всех параметров – "очистка" базы.

## **-gdu**

запись параметров работы программы с предварительной очисткой базы.

# Версия 4.0.4.0

## **Daemon**

1. Программа Daemon помимо командной строки может быть также запущена из startup-файла */etc/rc.d/init.d/kavd*. Посредством данного файла можно обеспечить автоматический старт процесса-демона при загрузке операционной системы. Для этого необходимо поместить скрипт *kavd* в каталог */etc/rc.d/init.d/*, после чего любым образом (с помощью утилит *ntsysv*, *chkconfig* или команды *ln -s*) добавить символическую ссылку в нужный вам уровень запуска.
2. Для того чтобы процесс-демон осуществлял лечение инфицированных объектов, необходимо либо в командной строке при запуске программы, либо в script-файле *kavd* (параметр **DPARMS**) указать ключ **-I2**.

## **Keeper**

Поскольку программа Кеерг является клиентской программой процесса-демона (осуществляет обработку и лечение зараженных писем, используя программу Daemon для антивирусной обработки тела и вложений письма), то для лечения почтовых сообщений необходимо включить соответствующую опцию программы Daemon. Возможны следующие варианты:

Вариант 1: если Daemon был запущен из командной строки, вам нужно:

1. остановить почтовую систему;
2. удалить все запущенные процессы-демоны:  
**/kavdaemon -ka**
3. выполнить настройку программы Кеерг посредством Web-Tuner или утилиты *kldbedit* (подробнее см. соответствующие Руководства пользователя "Антивирус Касперского для Linux/Sun Solaris/xBSD Mail Server");
4. запустить программу Daemon с опцией лечения:  
**/kavdaemon -I2**
5. запустить программу Кеерг;
6. запустить почтовую систему.

Вариант 2: если Демон был запущен с помощью скрипта `/etc/rc.d/init.d/kavd` при старте системы, необходимо:

1. в файле `/etc/rc.d/init.d/kavd` внести следующие изменения:  
**DPARMS="-I2"**
2. выполнить настройку программы Кеерг посредством Web-Tuner или утилиты `kidbedit` (подробнее см. Руководства пользователя "Антивирус Касперского для Linux/Sun Solaris/xBSD Mail Server");
3. перезапустить операционную систему.