Запуск Skype в изолированном окружении Apparmor

Для защиты от потенциального доступа закрытого приложения Skype к данным других программ можно организовать выполнение Skype в изолированном окружении.

Создаём профиль Apparmor на основе тестового запуска приложения:

```
sudo genprof /usr/bin/skype
```

После этого будет создан профиль для сбора информации о работе приложения. В другой консоли запускаем Skype, делаем тестовый вызов и выходим из Skype.

Повторно запускаем:

```
sudo genprof /usr/bin/skype
```

и инициируем сканирование накопленных событий, выбрав "S". В процессе вывода результатов выбираем что можно процессу, а что нет. В завершении жмём "S" для сохранения профиля и "F" для выхода.

Профиль будет создан в файле **/etc/apparmor.d/usr.bin.skype**
Если нет желания разбираться с составлением правил вручную можно использовать готовый профиль:

```
#include <tunables/global>
  /usr/bin/skype {
      #include <abstractions/audio>
      #include <abstractions/base>
      #include <abstractions/fonts>
      #include <abstractions/nameservice>
      #include <abstractions/nvidia>
      /etc/gai.conf r,
      /home/*/.ICEauthority r,
      /home/*/.Skype/** krw,
      /home/*/.Xauthority r,
      /home/*/.config/* kr,
      /home/*/.kde/share/config/kioslaverc r,
      /proc/*/cmdline r,
      /tmp/.ICE-unix/* w,
      /tmp/.X11-unix/* w,
      /usr/bin/skype mr,
      /usr/share/X11/* r,
      /usr/share/icons/** r,
      /usr/share/skype/** kr,
    }
```

Перезапускаем AppArmor:

```
sudo /etc/init.d/apparmor restart
```

Активируем работу Skype в sandbox-окружении Apparmor:

```
sudo aa-enforce skype
```

Проверяем результат:

```
sudo sudo apparmor_status
```