GnuPG - защитное преобразование/восстановление файлов

GnuPG позволяет защищать и подписывать данные, предоставляя развитую систему управления ключами, которая включает в себя модули доступа ко всем типам каталогов открытых ключей.

Переменные окружения

Переменная $GNUPGHOME используется GnuPG для определения каталога, в котором хранятся все настройки. По умолчанию $GNUPGHOME не установлена и используется домашний каталог текущего пользователя. Таким образом, после установки появится новый каталог `~/.gnupg`. Можно указать другой каталог для GnuPG, добавив след. строку в `~/.profile`:

```
export GNUPGHOME="///"
```

Ключи

GnuPG ключ состоит из двух частей: закрытый (приватный) ключ и открытый (публичный) ключ:

- Закрытый ключ хранится у владельца, закодирован защитным преобразованием и защищен паролем;
- Открытый ключ - свободно распространяется.

С помощью закрытого ключа можно:

- Подписывать данные;
- Восстанавливать данные, закодированные защитным преобразованием с соответствующим открытым ключем.

Для выполнения всех операций, использующих закрытый ключ, нужно вводить пароль (парольная фраза).

С помощью открытого ключа можно:

- Проверять подпись данных;
- Выполнять защитное преобразование данных.

Управление ключами

Создание ключа

Для создания пары закрытый-открытый ключ используется утилита gnupg:

```
gpg --gen-key
```

Экспорт ключей

Экспорт открытого ключа:

```
gpg --export 12345678 > /home/user/public.key
```

Где 12345678 идентификатор ключа.

Экспорт закрытого ключа:

```
gpg --export-secret-keys 12345678 > /home/user/private.key
```

Где 12345678 идентификатор ключа.

Импорт ключей

Импорт открытого ключа в список открытых ключей:

```
gpg --import public.key
```

Импорт закрытого ключа в список закрытых ключей:

```
gpg --import private.key
```

Отображение ключей

Вывод списка открытых ключей:

```
gpg --list-keys
```

Вывод списка закрытых ключей:

```
gpg --list-secret-keys
```

Защитное преобразование и восстановление данных

Для выполнения защитного преобразования данных необходимо импортировать публичный ключ. Восстановление данных происходит с помощью соответствующего закрытого ключа
Если импортировано несколько ключей, необходимо указать идентификатор нужного ключа. Для этого используйте опцию `-u <_>`, иначе будет использован ключ, выбранный по умолчанию.

Выполнение защитного преобразования данных, находящихся в файле `file.tar`, с сохранением результата в файле `file.tar.gpg` (опция -o), для пользователя <имя_пользователя> (опция -r, открытый ключ этого пользователя предварительно должен быть импортирован):

```
gpg --encrypt -r <_> -o file.tar.gpg file.tar
```

Восстановление данных получателем (обладателем закрытого ключа):

```
gpg --decrypt file.tar.gpg
```