

Инструкция по проверке подписи файлов

Упрощенная инструкция

1. Скачайте ключ подписи `FSTEC-GPG-KEY-MSVSphere` с сайта продукта <https://msvsphereos.ru/> на свой компьютер.
2. Откройте терминал в вашей ОС и перейдите в папку с ключом, выполнив команду:

```
$ cd /<Адрес до папки с ключом>
```

3. Импортируйте публичный PGP ключ MSVCфера в локальный GPG keyring, выполнив команду:

```
$ gpg --import FSTEC-GPG-KEY-MSVSphere
```

4. Проверьте валидность подписи файла, выполнив команду:

```
$ gpg --verify --trust-model always <Путь до файла подписи с  
  , расширение *.sig> <Путь до исходного файла, подпись к  
  , которому проверяется>
```

В результате выполнения перечисленных шагов на экране отобразится примерно следующий результат, означающий, что проверка подписи завершилась успешно и подпись валидная:

```
gpg: Подпись сделана Ср 01 окт 2025 16:11:16 MSK  
gpg:          ключом RSA с идентификатором 9E646525FB3BC8455EFBB00A604436920681221A  
gpg: Действительная подпись пользователя "MSVSphere Certified <packager@msvsphere-os.ru>" [неизвестно]  
gpg: Внимание: Использование недоверенного ключа!
```

Примечание

Запись «Внимание: Использование недоверенного ключа!» является нормальной в условиях использования быстрого метода проверки. Для того, чтобы данная запись не появлялась, необходимо сделать ключ доверенным в вашем PGP keyring. Для этого воспользуйтесь расширенной инструкцией.

Расширенная инструкция

1. Скачайте ключ подписи FSTEC-GPG-KEY-MSVSphere с сайта продукта <https://msvsphereos.ru/> на свой компьютер.
2. Откройте терминал в вашей ОС и перейдите в папку с ключом, выполнив команду:

```
$ cd /<Адрес до папки с ключом>
```

3. Импортируйте публичный PGP ключ MCBCСфера в локальный GPG keyring, выполнив команду:

```
$ gpg --import FSTEC-GPG-KEY-MSVSphere
```

4. Откройте интерактивное меню для управления ключами GPG, указав последние 8 знаков ID скачанного с сайта ключа, выполнив команду:

```
$ gpg --edit-key 0681221A
```

5. В открывшемся интерактивном меню GPG введите «trust» и нажмите Enter.
6. В интерактивном окне GPG выведется предложение выбрать степень доверия пользователю, который выпустил ключ. Укажите в ответ цифру, соответствующую степени доверия пользователя. Рекомендуется указать цифру «4» или «5». После этого нажмите Enter.
7. В интерактивном окне GPG выведется вопрос «Вы действительно хотите сделать этот ключ <степень доверия, выбранная пользователем>? (y/N)». Введите «y» и нажмите Enter.
4. После этого должна появиться запись примерно со следующим содержанием:

```
pub  rsa4096/604436920681221A
      создан: 2025-03-26      годен до: никогда      назначение: SC
      доверие: абсолютное достоверность: неизвестно
[ неизвестно ] (1). MSVSphere Certified <packager@msvsphere-os.ru>
Учтите, что показанная достоверность ключа может быть неверной,
пока Вы не перезапустите программу.
```

5. В интерактивном окне GPG введите «quit» и нажмите Enter.
6. Проверьте валидность подписи файла, выполнив команду:

```
$ gpg --verify --trust-model always <Путь до файла подписи  
с расширением *.sig> <Путь до исходного файла, подпись к  
которому проверяется>
```

В результате выполнения перечисленных шагов на экране отобразится примерно следующий результат, означающий, что проверка подписи завершилась успешно и подпись валидная:

```
gpg: Подпись сделана Ср 01 окт 2025 16:11:16 MSK  
gpg: ключом RSA с идентификатором 9E646525FB3BC8455EFBB00A604436920681221A  
gpg: проверка таблицы доверия  
gpg: marginals needed: 3 completes needed: 1 trust model: pgp  
gpg: глубина: 0 достоверных: 1 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 1u  
gpg: Действительная подпись пользователя "MSVSphere Certified <packager@msvsphere-os.ru>" [абсолютное]
```