**Раздел:** Жизненный цикл ИБ

**Модуль:** Средства защиты информации

**Выполнил:** Василий Костюков

**Условия задачи**

Установите GnuPG и создайте две пары ключей. Зашифруйте тестовый файл ключом из первой пары на открытом ключе второй пары, а потом расшифруйте файл.

**Что нужно сделать**

1. Установить GnuPG в разных системах.
2. Создать пару ключей № 1.
3. Создать пару ключей № 2 с указанием другой электронной почты.
4. Зашифровать любой файл с помощью закрытого ключа № 1 на открытом ключе № 2.
5. Расшифровать файл с помощью закрытого ключа № 2.

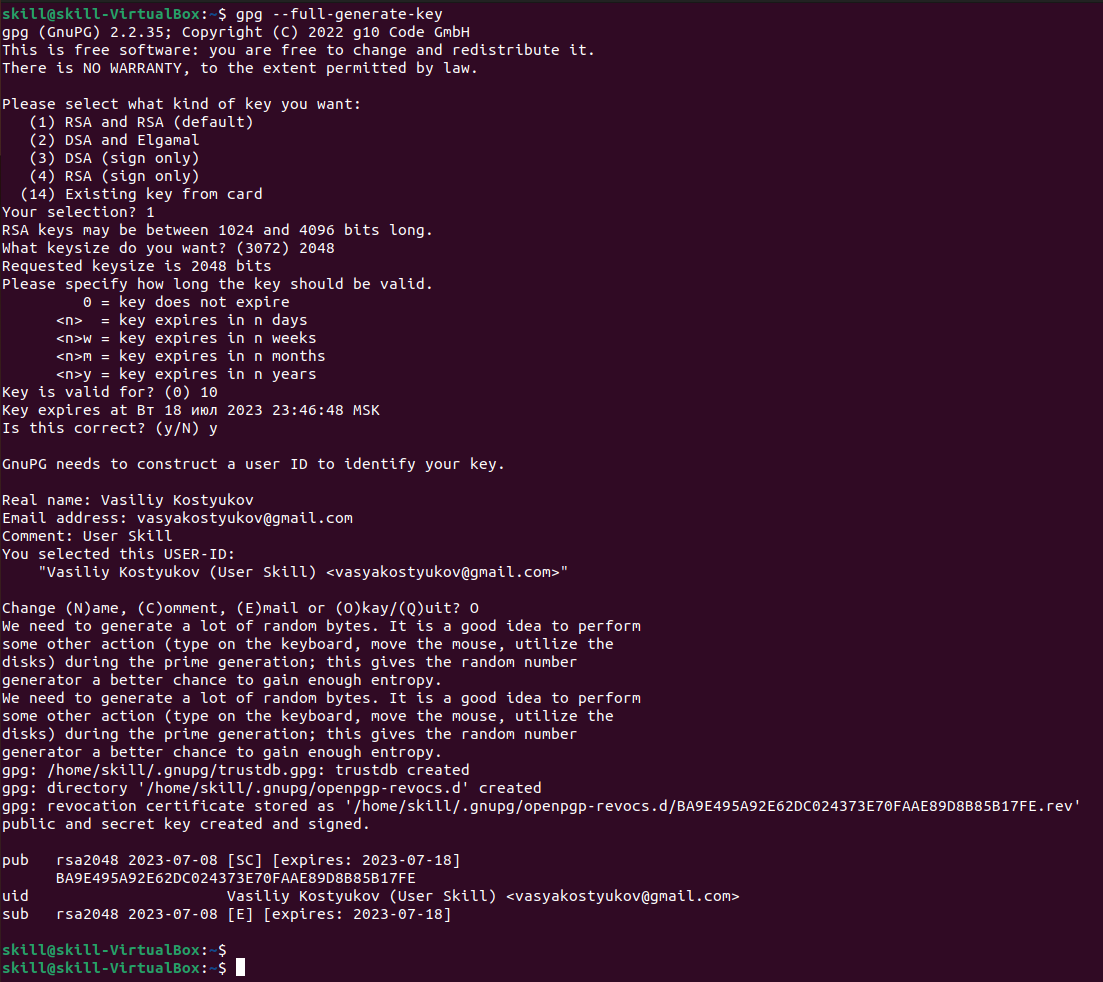
**Условия реализации**

Пришлите в формате Word или PDF или в виде скриншотов содержимое терминала с командами и результатами их выполнения, которые были использованы в рамках практической работы.

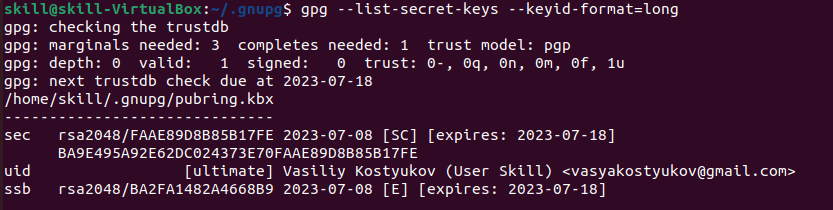
Одним из вариантов решения задачи может быть установка GnuPG в двух разных системах (на двух разных виртуальных машинах) с полноценным обменом открытыми ключами и зашифрованным файлом между ними.

**Шаг1:** Устанавливаем GnuPG командой **sudo apt install gnupg**.

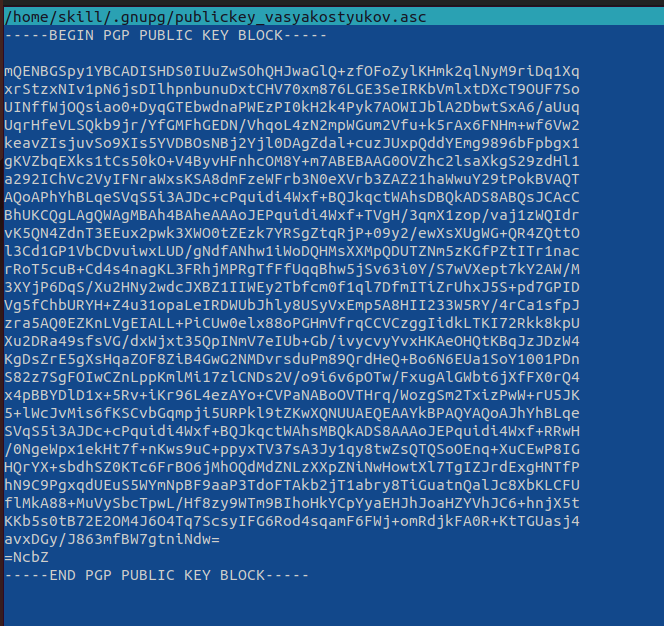
**Шаг2:** Создаём пару ключей на витруальной машине с пользователем **skill**.



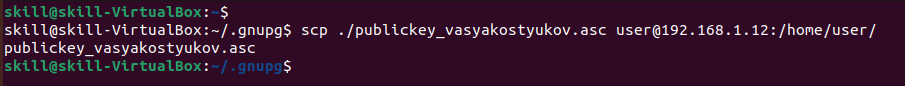
**Шаг3:** Проверяем наличие ключей с системе.



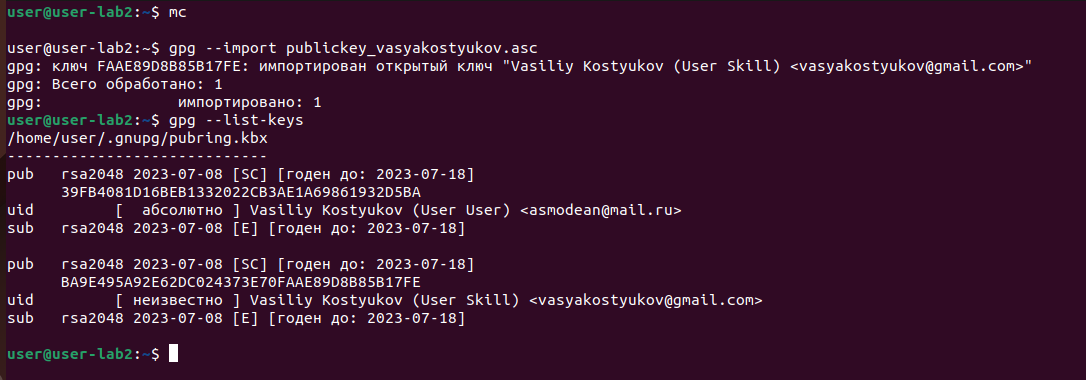
**Шаг4:** Экспортируем публичный ключ в файл **publickey\_vasyakostyukov.asc** с помощью команды **gpg --export --armor** [**vasyakostyukov@gmail.com**](mailto:vasyakostyukov@gmail.com) **> publickey\_vasyakostyukov.asc** .



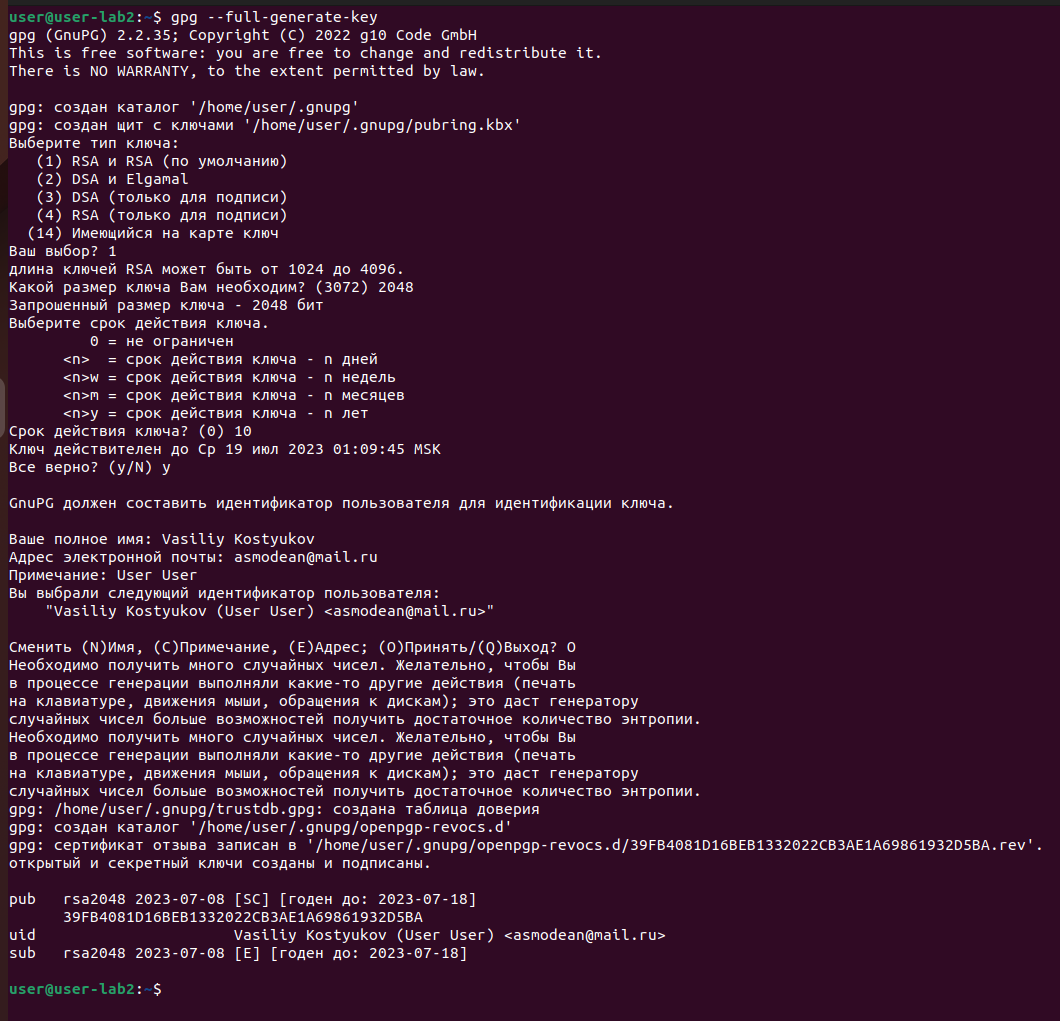
**Шаг5:** Копируем полученный файл на вторую виртуальную машину с пользователем **user**.



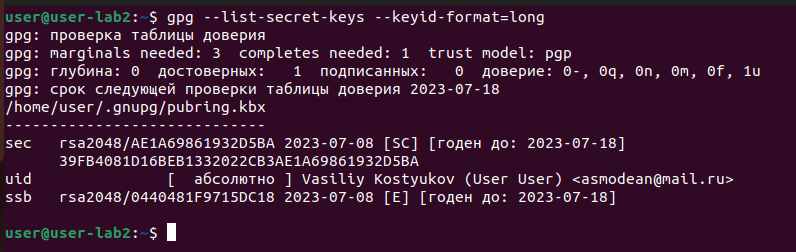
**Шаг6:** На второй виртульной машине импортируем в систему файл с ключом.



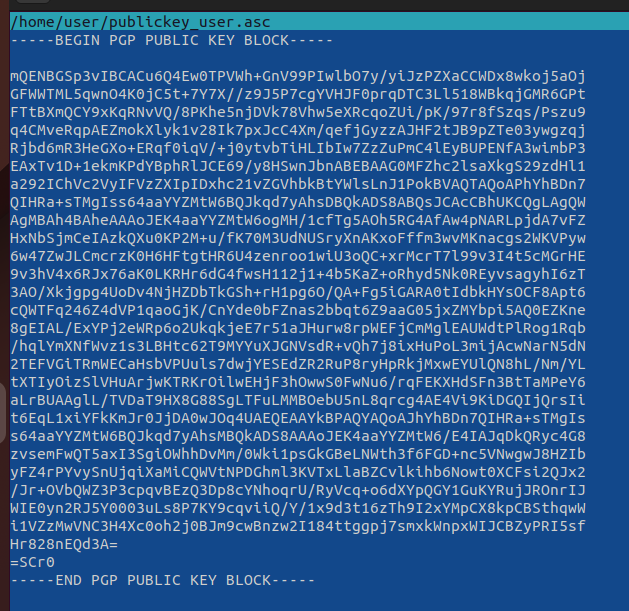
**Шаг7**: Теперь создаём пару ключей на виртуальной машине с пользователем **user**.



**Шаг8**: Проверяем наличие ключей в системе.

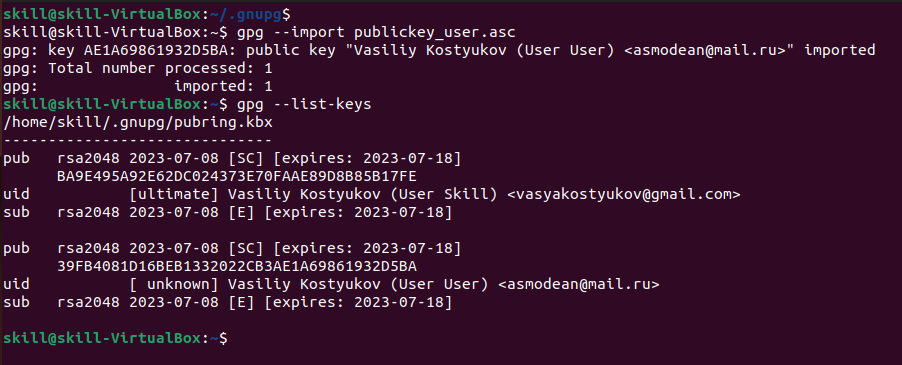


**Шаг9**: И экспортируем публичный ключ в файл **public\_user.asc** c помощью команды **gpg --export --armor** [**asmodean@mail.ru**](mailto:asmodean@mail.ru) **> publickey\_ user.asc** .

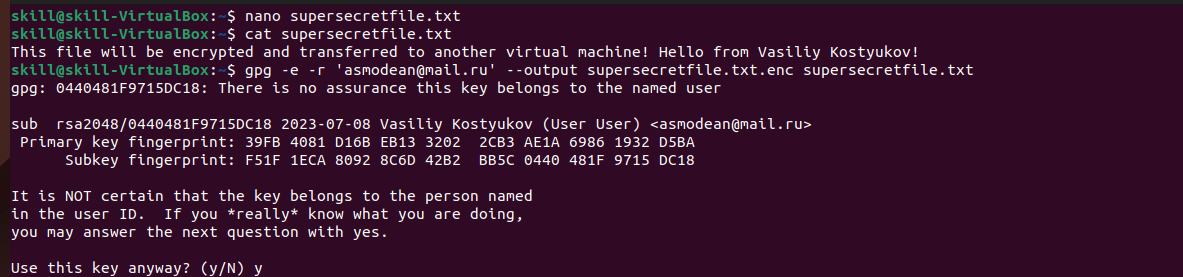


**Шаг:10** Копируем полученный файл на виртуальную машину с пользователем skill. Ssh соединение, с машины пользователя user к пользователю skill, я не настраивал. Так что просто скопировал файл с помощью usb-накопителя.

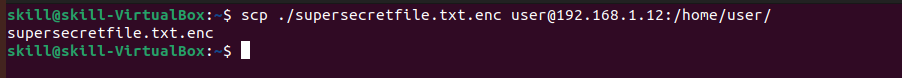
**Шаг:11** Импортируем в систему файл с ключом на первой витруальной машине.



**Шаг12:** На первой виртуальной машине создаем текстовый файл и зашифровываем его.



**Шаг13:** Копируем зашифрованный файл на вторую виртуальную машину.



**Шаг14:** Расшифровываем файл на второй виртуальной машине.

