

1. Установка GnuPG на двух Линукс системах командой `sudo apt install gnupg`. (утилиты уже были установлены ранее)

2. Проверка версий

```
nn@nn-HP: ~  
Файл Правка Вид Поиск Терминал Помощь  
nn@nn-HP:~$ gpg --version  
gpg (GnuPG) 2.2.27  
libgcrypt 1.9.4  
Copyright (C) 2021 Free Software Foundation, Inc.  
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Home: /home/nn/.gnupg  
Supported algorithms:  
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA  
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,  
CAMELLIA128, CAMELLIA192, CAMELLIA256  
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224  
Compression: Uncompressed, ZIP, ZLIB, BZIP2  
nn@nn-HP:~$  
  
Терминал Пт, 2 августа 12:38  
ak@ak-VirtualBox: ~  
ak@ak-VirtualBox:~$ gpg --version  
gpg (GnuPG) 2.2.27  
libgcrypt 1.9.4  
Copyright (C) 2021 Free Software Foundation, Inc.  
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Home: /home/ak/.gnupg  
Поддерживаются следующие алгоритмы:  
С открытым ключом: RSA, ELG, DSA, ECDH, ECDSA, EDDSA  
Симметричные шифры: IDEA, 3DES, CAST5, BLOWFISH,  
AES, AES192, AES256, TWOFISH, CAMELLIA128,  
CAMELLIA192, CAMELLIA256  
Хеш-функции: SHA1, RIPEMD160, SHA256, SHA384, SHA512,  
SHA224  
Алгоритмы сжатия: Без сжатия, ZIP, ZLIB,  
BZIP2  
ak@ak-VirtualBox:~$
```

3. Создание пары ключей на хосте 1 (linux mint NN) с именем nn-ak

```
nn@nn-HP: ~  
Файл Правка Вид Поиск Терминал Помощь  
nn@nn-HP:~$ gpg --gen-key  
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.  
  
GnuPG needs to construct a user ID to identify your key.  
  
Real name: nn-ak  
Email address: yamediaconstantin@yandex.ru  
You selected this USER-ID:  
"nn-ak <yamediaconstantin@yandex.ru>"  
  
Change (N)ame, (E)mail, or (O)kay/(Q)uit? O  
We need to generate a lot of random bytes. It is a good idea to perform  
some other action (type on the keyboard, move the mouse, utilize the  
disks) during the prime generation; this gives the random number  
generator a better chance to gain enough entropy.  
We need to generate a lot of random bytes. It is a good idea to perform  
some other action (type on the keyboard, move the mouse, utilize the  
disks) during the prime generation; this gives the random number  
generator a better chance to gain enough entropy.  
gpg: /home/nn/.gnupg/trustdb.gpg: trustdb created  
gpg: key 7A46C419E054CC7C marked as ultimately trusted  
gpg: directory '/home/nn/.gnupg/openpgp-revocs.d' created  
gpg: revocation certificate stored as '/home/nn/.gnupg/openpgp-revocs.d/2F79E3453FE7BB2AC6E1D7F67A46C419E054CC7C.rev'  
public and secret key created and signed.  
  
pub   rsa3072 2024-08-02 [SC] [expires: 2026-08-02]  
      2F79E3453FE7BB2AC6E1D7F67A46C419E054CC7C  
uid           nn-ak <yamediaconstantin@yandex.ru>  
sub   rsa3072 2024-08-02 [E] [expires: 2026-08-02]  
nn@nn-HP:~$
```

4. Проверил список ключей

```
nn@nn-HP:~$ gpg --list-secret-keys --keyid-format=long
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2026-08-02
/home/nn/.gnupg/pubring.kbx
-----
sec   rsa3072/7A46C419E054CC7C 2024-08-02 [SC] [expires: 2026-08-02]
      2F79E3453FE7BB2AC6E1D7F67A46C419E054CC7C
uid    [ultimate] nn-ak <yamediakonstantin@yandex.ru>
ssb    rsa3072/D140B3D68C51A297 2024-08-02 [E] [expires: 2026-08-02]

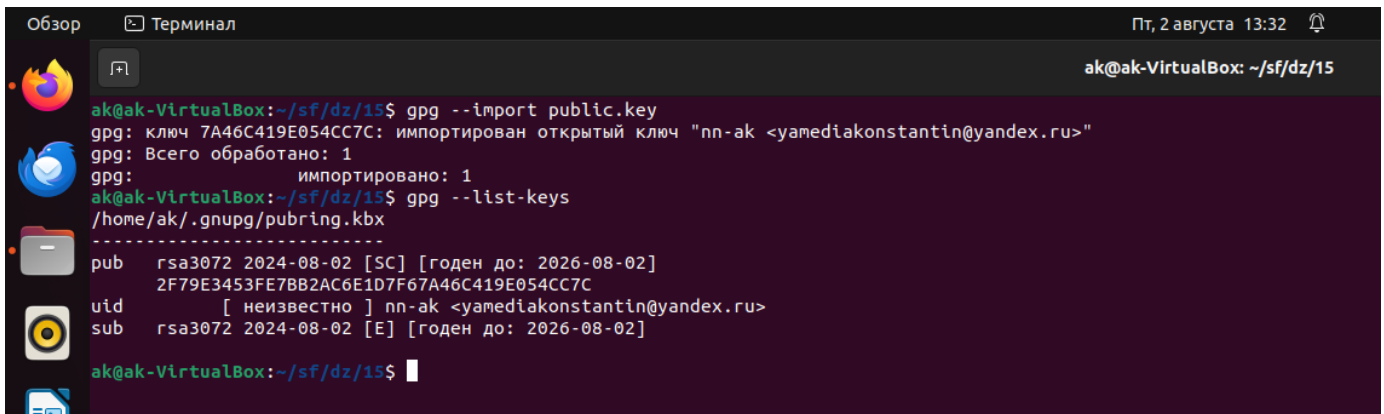
nn@nn-HP:~$
```

5. Экспортировал открытый ключ gpg --armor --export <почта> и отправил его по почте на хост 2 (Linux Ubuntu AK)

```
Файл  Правка  Вид  Поиск  Терминал  Помощь
nn@nn-HP:~/sf/dz/15$ gpg --armor --export yamediakonstantin@yandex.ru
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGasr8QBDAC9WkiHECSiEiMHAFKS9oQFjc0X2wllVqelr/FPDLsy3yY8rLdde
t57P5JM/q5VS46P6H5GG9LtgH+wQyx8USpHErLuF4zL8MWQ9E64I0eJ68gdTIA4P
Hi5gdgrFvt10+Vfj3yByryXwdH//ZRZjuebAYD0yqAN+Ev6g85pp/RF/YPPRD1ey
Alf27L7A39wfvrrZR8iHC12kd79c+VN0cKgCZu2y7joh0QrDXcnGd2uLwqZ9eVcN
Ue/Q5WIIU9xptvoZvmwXWfYsHr4nqzQ6eHE5Is7mQL9Y3ZSa6KmT/tGctVQAYxKw
c3YA3ZVZY8HEcdzmRfmnPQ/M4DdUZA42VImR84IIZtwrZnxDK12Yyfd4VGx1E1
m9JIEvD6RdIq6j/LMR5b3hA2nuWZiJl0AuansSLrw3QF+PBbELoKqbjdBAWpN1b
bUDTunt6kvPAmJWMS5U1lm8rH7Y3KnJHC8MddFjbLUMMDdsi8iEabJqvSoAjrIW
r3YzCwUqc8qpbh0AEQEAAAbjbm4tYwsgPHlhbwVkaWFrB25zdGudGluQhLhbmRl
eC5ydT6JAdQEEwEKAD4WIIQveeNFP+e7Ksbh1/Z6RsQZ4FTMFaucZqyvxAIbAwUJ
e8JnAAULCQgHAgYCGkICwIEFgIDAQIEAQIXgAAKCRB6RsQZ4FTMfLHEDAC2IWIg
1Lhv2QhmK20i+hxlozrSYAo5zH0xcF01iVes+r8UQta+qytyS+pS/3M1lp+cu9MT
9MrsXYL4K4HN/prkBLx1mLSZPzityzgXmbFyc8gAHBH1vJHBH3XDMgkcFpLHnB2
IztkYdyjDo1VSS2taiRME1mfeVo0DTgt+JhXJ0p8y6mUIDrC6SHDM3hDF34K98w
60Jza4i/gstiFcP9ura0jC2BSDR4h2xerFKYB6J7x2DfEC6En0MSn5FqEJIg86zF
ql5sjBa9aStXWIKoYtPmXbsCIpeSuZijQehyxlJTigumfavS8h4ayJJ9Hz2Wt+M
kkh4usxm56DH/dssiLK28cnA4Gugik26AnvcPb5FsozhUAXnW084QYA13qT9Y09
brp9MvjQIB2A3FisBjgET2HqRNPuCSgHuwlAdwVwhiHztZCT3KFiNcIzZ4sSMXta
MuiLyhBNcp9gJwECjFRtMZhGVvhVCAWEbEAPLcFWI70jAKB004ME0P13KMu5AY0E
ZqyvxAEAM2Cosd9JIHda4xTJ5hILBmxrHXx1EM2aIrodjCSTT1F8PPUgiTftB4H
/NjEXz94rAxgmSeV+LzSrQyPuphklino6puMrdjd15/ye+GtjvvnX8kkwDyWA5SY
WsTojG36oFL5kGh4v0LCgRFukG62EfqpLdyLbL8vhNewXFwNS2zq5eiA5viDxEfm
qFg3WmfGtj9PBIFSRqYTNT03uB6BiJx0wacTsafllmBTMQdDvKmgwBUyiZJqSef/
Sz29WzV8f00F+UGTxr48buXLrptfTgJhB+B1bgA0v9H6vBQAx8a2L6QVMraEajLL
49CVf6ueJmEke+k/3WFnRMK7o0B0DncDQ8D3nFWx0JfcESsz2+ivWIGKx8Wv/YSJ
KwQv4GoJTPH5q8Q71TbjGqMMstP0960HiuACILM/teZhsryMpyrZ0FLJGh/tfSUL
IZ9VuW148UheAe42l5if2w2H+IuLZ+hWTwvm1Ixt03ilz9jGgQ5dsNfAsJeg80gc
C4qP59aSJQARAQAABiOG8BBgBCgAmFiEEL3njRT/nuyrG4df2ekbEGeBUzHwFamas
r8QCGwWFCQPCZwAACGkQekbEGeBUzHx0dwv7BvRwGE9fwjVaidYeIn7/QWXsdY4d
7GgdzQD5ChYgjmG2VD4miCUxy6bK3aT32/i/Wr+cVIMU7k68JuujG04kYLbSinxn
QhSeQGRtVGC1K96Ah8E/50AnuAq6oq5SLL3QXgw7+V49pzqI20W6v7/LAXSutdeu
lFe1t07p6MtW6XsSjx3N2IrXLghQ14PyDDqJuc4QjRq258Y8JTktnQEBmtnyDanl
n1zQAwdf9uXEQn+1X0koehGmhK0bXNT5lmpNY0/qq0SMGCDmHTI5Zhn483f9gxyw
iQHAMf+ZRinvcQertSwJ0t9Hv3VpI+APPNTLnsNaXEyBQDCPk2vMy4k0b3otAgge
qaJxVSRGFIpBmV207Bj32oxeqtJ/ogjE0VXffrwtfvCHbUAza0tGgo79nHivmvg
iTq70NM9JnVgzbgIhr/0toHgl2vLdu3dGp0qJkGtAjK0iMbnB+Oop00hhRW5imsN
XDp87hQsd7g0W0Vh6qM9CzI9DwJUulbtLLUS
==hPf
-----END PGP PUBLIC KEY BLOCK-----
```

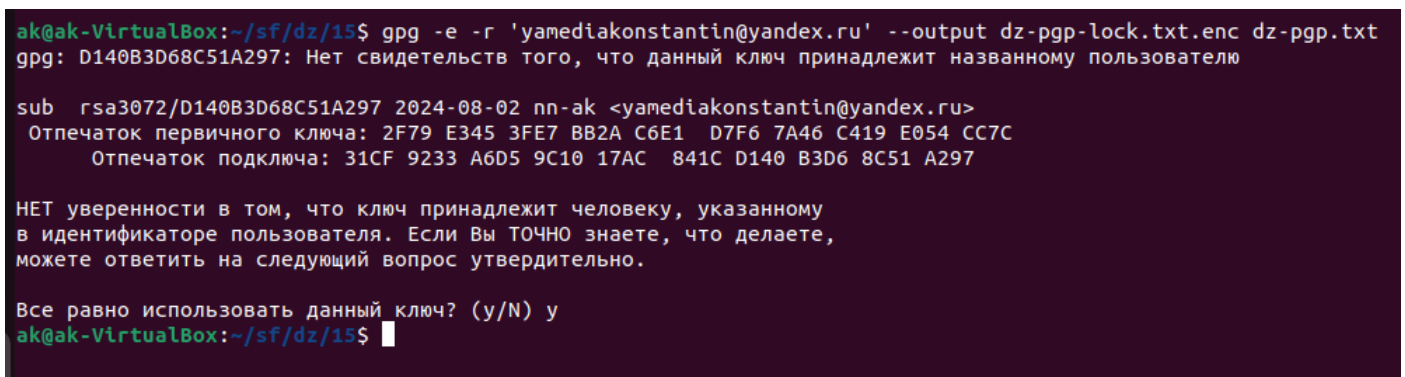
6. Импортировал на хосте 2 открытый ключ gpg --import public.key и сразу проверил список ключей.



```
ak@ak-VirtualBox:~/sf/dz/15$ gpg --import public.key
gpg: ключ 7A46C419E054CC7C: импортирован открытый ключ "nn-ak <yamediaconstantin@yandex.ru>"
gpg: Всего обработано: 1
gpg: импортировано: 1
ak@ak-VirtualBox:~/sf/dz/15$ gpg --list-keys
/home/ak/.gnupg/pubring.kbx
-----
pub   rsa3072 2024-08-02 [SC] [годен до: 2026-08-02]
      2F79E3453FE7BB2AC6E1D7F67A46C419E054CC7C
uid   [ неизвестно ] nn-ak <yamediaconstantin@yandex.ru>
sub   rsa3072 2024-08-02 [E] [годен до: 2026-08-02]

ak@ak-VirtualBox:~/sf/dz/15$
```

7. Зашифровал текстовый файл dz-pgp на хосте 2 с именем dz-pgp-lock и отправил его по почте на хост1.



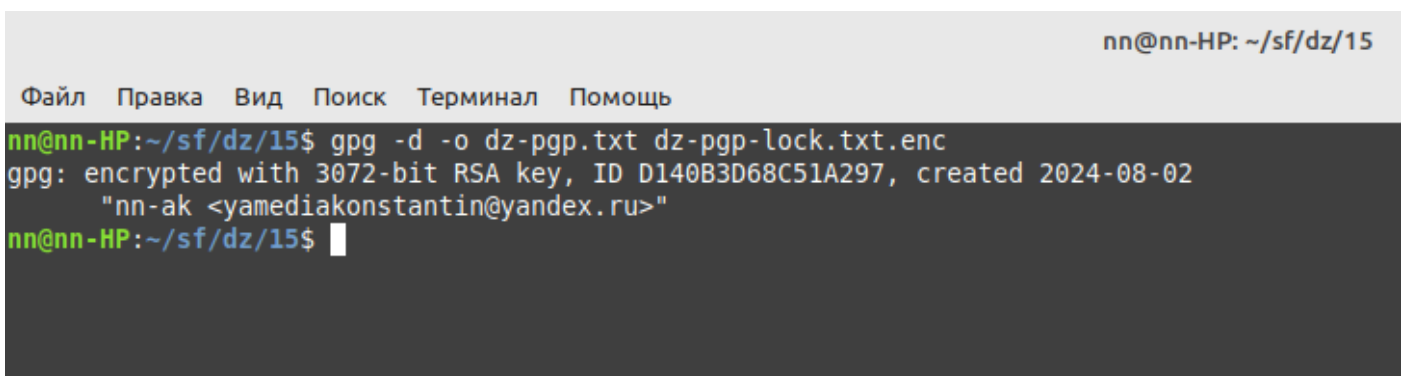
```
ak@ak-VirtualBox:~/sf/dz/15$ gpg -e -r 'yamediaconstantin@yandex.ru' --output dz-pgp-lock.txt.enc dz-pgp.txt
gpg: D140B3D68C51A297: Нет свидетельств того, что данный ключ принадлежит названному пользователю

sub   rsa3072/D140B3D68C51A297 2024-08-02 nn-ak <yamediaconstantin@yandex.ru>
Отпечаток первичного ключа: 2F79 E345 3FE7 BB2A C6E1 D7F6 7A46 C419 E054 CC7C
Отпечаток подключа: 31CF 9233 A6D5 9C10 17AC 841C D140 B3D6 8C51 A297

НЕТ уверенности в том, что ключ принадлежит человеку, указанному
в идентификаторе пользователя. Если Вы ТОЧНО знаете, что делаете,
можете ответить на следующий вопрос утвердительно.

Все равно использовать данный ключ? (у/Н) у
ak@ak-VirtualBox:~/sf/dz/15$
```

8. На хосте 1 расшифровал файл командой gpg -d -o dz-pgp.txt dz-pgp-lock.txt.enc.



```
nn@nn-HP: ~/sf/dz/15

Файл  Правка  Вид  Поиск  Терминал  Помощь

nn@nn-HP:~/sf/dz/15$ gpg -d -o dz-pgp.txt dz-pgp-lock.txt.enc
gpg: encrypted with 3072-bit RSA key, ID D140B3D68C51A297, created 2024-08-02
      "nn-ak <yamediaconstantin@yandex.ru>"
nn@nn-HP:~/sf/dz/15$
```

9. Расшифрованный доступный файл появился в директории.