

Лабораторная работа №3
Курс: Защита информации

Патраков Николай

25 сентября 2015 г.

Содержание

1	Создать ключевую пару OpenGr	3
2	Поставить ЭЦП на файл	5
3	Получить чужой сертификат,импортировать его, проверить подпись	5
4	Работа с консолью	7

Программа для шифрования и подписи GPG, пакет Gpg4win

1 Создать ключевую пару OpenGr

Клеопатра это графический интерфейс к GnuPG и предназначенных для работы под окружением KDE, портированный на MS Windows(Рис. 1).

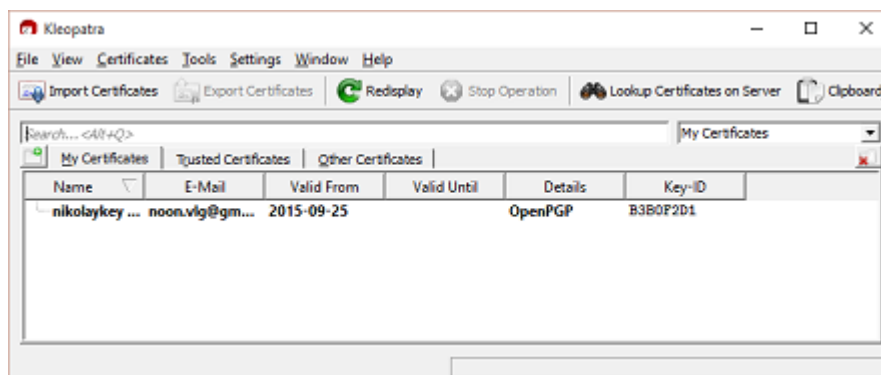


Рис. 1: Новая ключевая пара

Выглядит ключ следующим образом(Рис. 2).

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFYEOMIBCADxJVuWXB82KbunexOQXIbXVfJnRtnN7JyZelcVp+ttFLXD6/8Vp
otLZgb8z0z7/gSIF+5Y8jv9cPlHBICuax3Y9Dz7MzbdKATW3KYdLQu9kuM41CT8z
6g0XYAKSF+bk8q+WmQ1lbJttGgX8jDAs5osVNQaa9z23f44fRGtqzotaOsHUB11/
A3IZLxkGCPJCBDdBdgU3+QXMyhEQIn18uDwb0ehB11b8NE466jhbIc4wWm5DilW3
7G7pvirSZ3ONt2PrMroKQMGQ5RzvxQgsQDNwa/jtWbug82k5gAuB+/h1Ydw5uPU9
V/57TBW5Y++h/RMqK1kK0aSxy11ASinssHRnABEBAAQJW5pa29sYX1rZXkgKHh1
eCkgPG5vb24udmxnQGdtYWlsLmNvbT6JATkEEwEIACMFAlYEOMICGwMHCwkIBwMC
AQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCMuqQes7Dy0RV5CAGCo6YUNP9WUESZbwLOX
wA/YFijD32ys4rj/AWiIJVSLtaoDWXia8KoWXGZJKZPsJ49dD8dgwY5Y2a1T4eNF
zXWNJzcWRgv07h54/Ci+NvxDU9+05bMcfcQ3WyoMSApBc+baAfYJyINIZMeDP9i
3D9jxykE4zjH0w51voRub9kAHzvEhZJzmEJomKxmQeyRRZFNWdoIYjUSP9k9xDWvt
Pk33FYvzzreZUY7XptJwWoc5vJ+1CzcGDDtqE707yYDsfQq3UOXcAGb8Kert4SMX
KXqnHv/o14VnS5ycu2BK9IMNJRoVn7vvFKgZ56kUknI1Iy9LB4IcNmMAB33Wnzsj
n2mDuQENBFYEOMIBCADXheaJDbYLxjNwHZ12kOmGNjO1XO8Wm978kVwV442NmVzw
cSYqgI7f/5xSBtaQnxRQC5X5usEbpilXfxBRBDB5Edj9jPT1B9Si0IMcKhgcX48u
MqRuUgDAJYsLG45HBDB4sKmkVGgkieHMXMgYyDZpgKGQ6PLc+8EDGco0TX/D/2P/
xKkorCr++MT15YLKfr/m52rMDQz4c3UXD7KGexVEdNrqOvQ6M1Zccg8HE2aCjJKR
m3JStPSRCnwedMaxEWGq7kE4a+2Tgjc+v6IHtBRyGO74CwgF4YGQBn4oaFPjJA6t
DecGee6qNgIOyysv0+4b/6e0iH0mlAPjgmmN4OKhABEBAAQJAR8EGAEIAAKFAlYE
OMICGwwACgkQjLqkHrOw8tFVLAgAq0kFtJVkmsXL4qXSgHiDi3GUaCCKr/4qKLjJ
WgfSCEc5OtWOMUaUT9vhy6sHKY+SaHKQ2iyNk7KFzT6AJF/flsLOpD74PyadJMoM
UengoJBrtvgyygFszrmMoZUVy9XStWew8CPTNynwuZ3Cf5cUdvUCZUbnRWRICte
xzHeWD28rulzRCFu54DUgAqBK//6R8DY1FAH4006s/+ag+J7QwB4UgljW3IaOylm
HF+VvkqwsCvNGuOPxtughHYoIT0msUwC/olWYBQR8DqX3HBjczspFKQaIdwvm+IX
VoJaek+NHvXJ5zPTnVm9MwxHi+0vrz6LjwNmGq9oiEj4vsgBvg==
=eBtU
-----END PGP PUBLIC KEY BLOCK-----
```

Рис. 2: Ключ

2 Поставить ЭЦП на файл

После подписания файла создается его копия, но с измененным форматом. В конце приписывается .sig(Рис. 3).

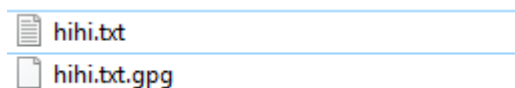


Рис. 3: Файл hihi.txt с подписью

3 Получить чужой сертификат,импортировать его, проверить подпись

Получив чужой сертификат(Рис. 4), можно расшифровывать подписанные этим пользователем файлы (Рис. 5).

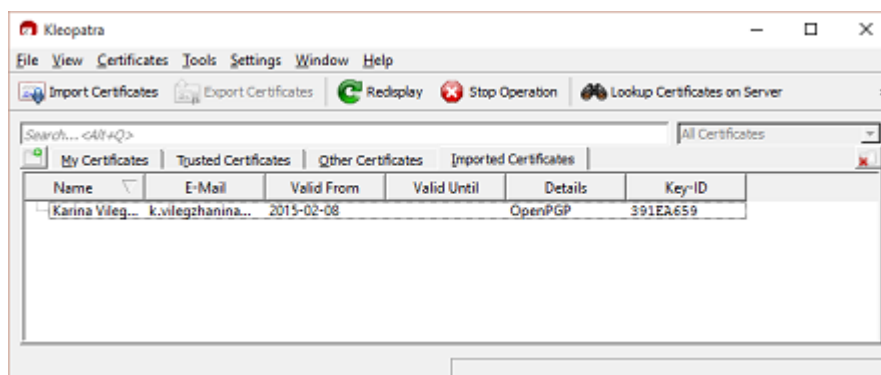


Рис. 4: Полученный сертификат

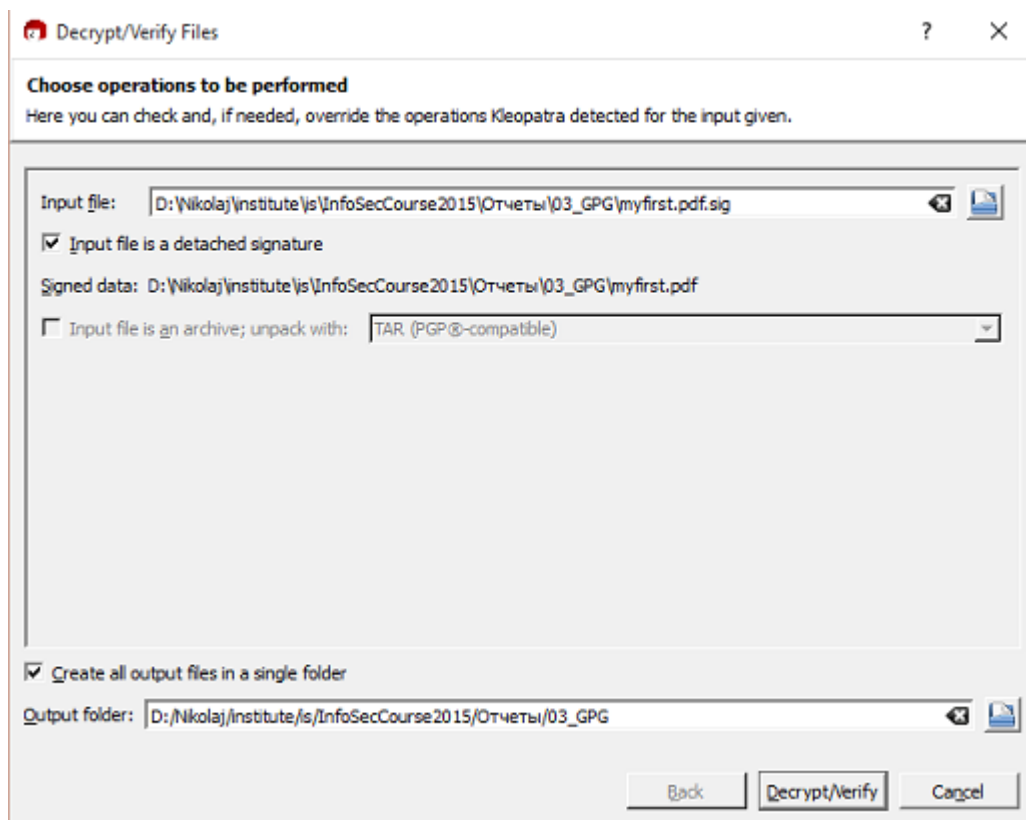


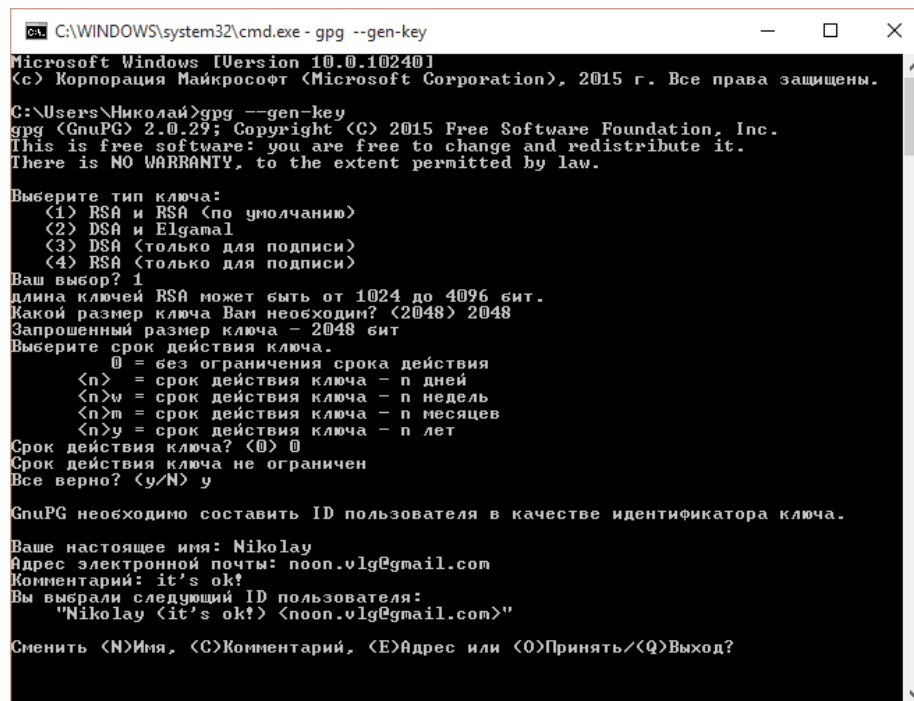
Рис. 5: Расшифровка файла с помощью импортированного сертификата

4 Работа с консолью

Все эти операции можно повторить в консоли. Например, создание ключа осуществляется командой:

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

При создании нас просят ввести дополнительные параметры. Выглядит это примерно так (Рис. 6).



```
C:\WINDOWS\system32\cmd.exe - gpg --gen-key
Microsoft Windows [Version 10.0.10240]
(c) Корпорация Майкрософт (Microsoft Corporation), 2015 г. Все права защищены.

C:\Users\Николай>gpg --gen-key
gpg (GnuPG) 2.0.29; Copyright (C) 2015 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.

Выберите тип ключа:
  (1) RSA и RSA (по умолчанию)
  (2) DSA и Elgamal
  (3) DSA (только для подписи)
  (4) RSA (только для подписи)
Ваш выбор? 1
длина ключей RSA может быть от 1024 до 4096 бит.
Какой размер ключа Вам необходим? (2048) 2048
Запрошенный размер ключа - 2048 бит
Выберите срок действия ключа.
  0 = без ограничения срока действия
  <n> = срок действия ключа - n дней
  <n>w = срок действия ключа - n недель
  <n>m = срок действия ключа - n месяцев
  <n>y = срок действия ключа - n лет
Срок действия ключа? (0) 0
Срок действия ключа не ограничен
Все верно? (y/N) y

GnuPG необходимо составить ID пользователя в качестве идентификатора ключа.
Ваше настоящее имя: Nikolay
Адрес электронной почты: noon.vlg@gmail.com
Комментарий: it's ok!
Вы выбрали следующий ID пользователя:
"Nikolay (it's ok!) (noon.vlg@gmail.com)"

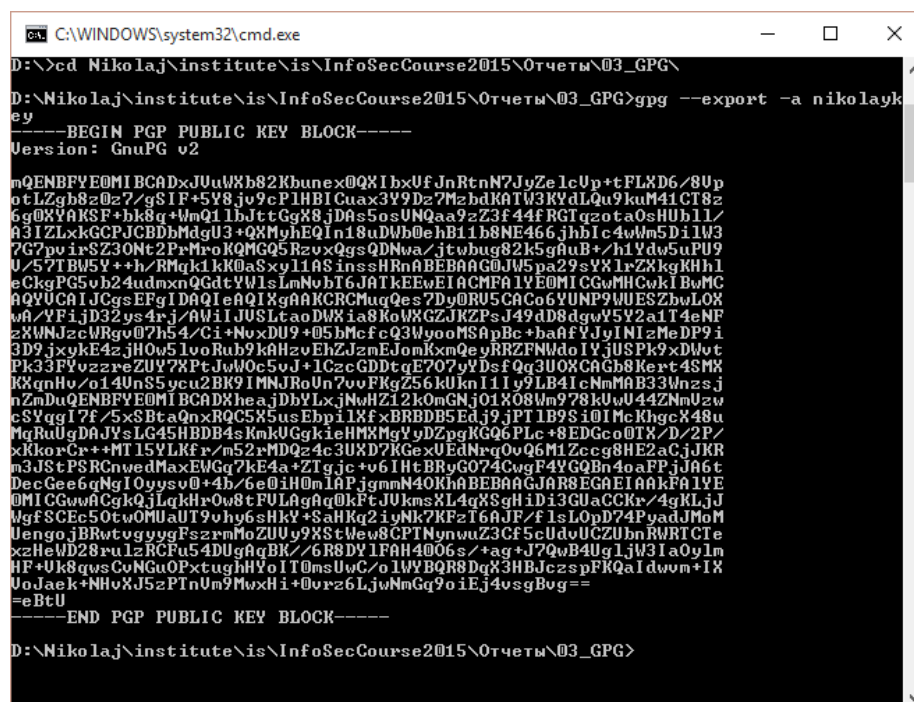
Сменить (N)Имя, (C)Комментарий, (E)Адрес или (O)Принять/(Q)Выход?
```

Рис. 6: Создание ключа в консоли

Мы можем убедиться, что он создан с помощью команды `gpg --list-keys`

Для импорта и экспорта используются команды `import` и `export` соответственно.

Шифрование. Для того, чтобы можно было в последующем на другой машине расшифровать/верифицировать наши файлы необходимо экспортировать ключ. Воспользуемся для этого ключом `export`. Пример команды:



```
C:\WINDOWS\system32\cmd.exe
D:\>cd Nikolaj\institute\is\InfoSecCourse2015\0тчеты\03_GPG\
D:\Nikolaj\institute\is\InfoSecCourse2015\0тчеты\03_GPG>gpg --export -a nikolayk
ey
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFYEOmIBCADxJUuWxb82Kbunex@QX1bxUfJnRtnN7JyZe1cUp+tfLKD6/8Up
otLZgb8z0z7/gSIF+5Y8jv9cP1HB1Cuax3Y9Dz7MzbdKAIW3KYdLQu9kuM41CT8z
6g0XYAKSF+bk8q+WmQ11bJttGgX8jDAs5osUNQaa9zZ3f44fRG1qzota0sHUb11/
A31ZLxkGCPJCBDhMdGU3+QXMyhEQIn18uDWb0ehB11b8NE466jhb1c4wWm5Di1W3
7G7puirSZ3ONc2PrMroKQMGQ5RzvxQgsQDNwa/jtwbug82k5gAuB+/h1Ydw5uPU9
U/57TBW5Y++h/RMqk1kk0aSy11ASinssHRnABEBAGQJW5pa29sYX1rZXkgKHh1
eCkgPG5vb24udmxnQGdtYW1sLnNvbT6JATkEEwE1ACMFAYEOmIBGwMHcWkiBwMC
AQYUCAlJCgsEFgIDAQIeAQIXgAAKCRCMuqQes7Dy@RU5CaCo6YUNP9WUESZhwLOX
wA/YFijD32ys4rj/AWi1JUSLtaoDWXia8KoWKGZJKZPsJ49dD8dgvY5V2a1T4eNF
zXVnJzcWRgv07h54/Ci+NvxDU9+05bMcfcQ3Wyo0MSApBc+baafVjyINIzMeDP9i
3D9jxykE4zjH0w5lvoRub9kAHzvEhZJzmEJomKxmQeyRRZFNUdoIYjUSPk9xDWvt
Pk33FVuzzzeZUY7XPtJwW0c5vJ+1CzcGDDtgE7O7yYDsfQq3U0XCAgB8Kert4SMX
KXgnHu/o14UnS5ycu2BK9IMNJR0Un7v0FKgZ56kUkn11Iy9LB41cNmMAB33Wnzsj
nZmDuQENBFYEOmIBCADxheajDbYLxjNwHZ12kOmGNj01X08Wm978kUuU44ZnmUzw
cSYggI7f/5xSBtaQnxRQC5X5usEbp1lXfxBRBDB5Edj9jPT1B9Si0IMcKhgcX48u
MqRuUgDAJySLG45HDBB4sKmkUGgkieHMMgYyDZpgKGQ6PLc+8EDGco0TK/D/2P/
xKkorCk++MT15VYLkfr/m52+MDQz4c3UXD7KGeXUEdNqOvQ6M1Zccg8HE2aCjJKR
m3JStPSRCnwdMxEMGq7kE4a+ZTgjc+u6IHtBRyG0724Cuf4YQGQbn4oaFPjJA6t
DecGee6gNg1Oyysv0+4b/6e0ih0m1APjgmmN40KhaBEBAGJAR8EGAEIAAkFA1YE
0MI CGwA CgkQJlqkHr0w8tFULAgA0kFtJUlmsX14qXSGhiDi3GUaCCk+/4gKLjJ
MgFSCEc50tW0MuAU79vhy6sHkY+SAHkq2iyNk7KFZT6AJF/FlsLopD74PyadJMoM
UengoJBRwtvgyygFszzmMoZUUY9XStWew8CPTMynwuZ3Cf5cUdvUCZUbnRWRICTe
xzHeWJ28ru1zRCFu54DUgAgBK//6R8DY1FAH4006s/+ag+J7QwB4Ug1JW31a0y1m
HF+Uk8qwsCvNGuOPxtughHYoIT0msUwC/o1WYBQR8DqX3HBjczspFKQaldwum+IX
UoJek+NhvxJ5zPTnUm9MwxHi+0vz26LjwNmGq9oIEj4vsgBug==
-----END PGP PUBLIC KEY BLOCK-----
D:\Nikolaj\institute\is\InfoSecCourse2015\0тчеты\03_GPG>
```

Рис. 7: Экспорт ключа

Сделаем вывод в файл, чтобы потом отправить его на удаленную машину. Теперь перейдем к шифрованию: зашифруем файл на удаленной машине, после чего скинем его на основную и расшифруем.

Как видно, появился файл `hihi.txt.asc`, теперь его можно передать на клиентскую машину для расшифровки. Расшифровать можно с помощью команды:

```
gpg -d hihi.txt.asc >hihi.txt
```



```
C:\WINDOWS\system32\cmd.exe

D:\Nikolaj\institute\is\InfoSecCourse2015\Отчеты\03_GPG>gpg -ea -r nikolaykey hi
hi.txt

D:\Nikolaj\institute\is\InfoSecCourse2015\Отчеты\03_GPG>dir
Том в устройстве D имеет метку Локальный диск
Серийный номер тома: 322D-BB82

Содержимое папки D:\Nikolaj\institute\is\InfoSecCourse2015\Отчеты\03_GPG
25.09.2015 08:19 <DIR> .
25.09.2015 08:19 <DIR> ..
25.09.2015 07:47 21 hihi.txt
25.09.2015 08:19 584 hihi.txt.asc
25.09.2015 07:49 659 hihi.txt.gpg
24.09.2015 18:33 1 349 karina.asc
24.09.2015 18:33 110 397 myfirst.pdf
24.09.2015 18:33 287 myfirst.pdf.sig
25.09.2015 07:44 1 740 nikolaykey.asc
7 файлов 115 037 байт
2 папок 135 941 853 184 байт свободно
D:\Nikolaj\institute\is\InfoSecCourse2015\Отчеты\03_GPG>_
```

Рис. 8: Шифрование файла