

Лабораторные работы №1-3
Курс: Защита информации

Воробьев Олег

7 июня 2015 г.

Часть I

Система верстки TEX и расширения LATEX

Файл .tex представляет из себя обычный текстовый файл содержащий макрокоманды текстовой разметки.

1 Создание минимального файла .tex в простом текстовом редакторе преамбула, тело документа

Создаем в блокноте простой файл, включающий в себя минимум строк (Рис 1).

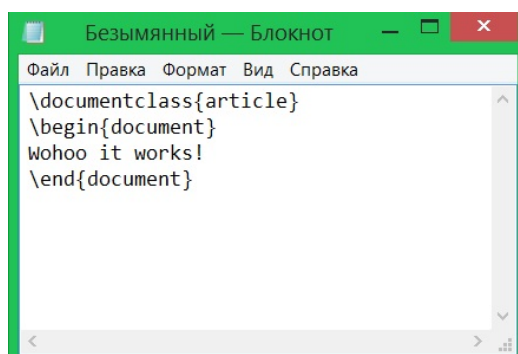


Рис. 1: Простейший tex документ.

Здесь указывается тип документа, а так же выводится одна простая строка.

2 Компиляция в командной строке – latex, xdv, pdflatex

Файлы latex оегко могут быть скомпилированы прямо из командной строки. В системе эти файлы хранятся в формате, не предназначенном для чтения, поэтому требуется преобразовать их в читаемый вид. Так компилируется latex файл (Рис 2).

```

D:\Учеба\10 семестр\защита информации>latex test.tex
This is pdfTeX, Version 3.1415926-2.5-1.40.14 (MiKTeX 2.9 64-bit)
entering extended mode
("D:\Учеба\10 семестр\защита информации\test.tex"
LaTeX2e <2011/06/27>
Babel <v3.8m> and hyphenation patterns for english, afrikaans, ancientgreek, ar
abic, armenian, assamese, basque, bengali, bokmal, bulgarian, catalan, coptic,
croatian, czech, danish, dutch, esperanto, estonian, farsi, finnish, french, ga
lician, german, german-x-2013-05-26, greek, gujarati, hindi, hungarian, iceland
ic, indonesian, interlingua, irish, italian, kannada, kurmanji, latin, latvian,
lithuanian, malayalam, marathi, mongolian, mongolianlmc, monogreek, ngerman, n
german-x-2013-05-26, nynorsk, oriya, panjabi, pinyin, polish, portuguese, roman
ian, russian, sanskrit, serbian, slovak, slovenian, spanish, swedish, swissgerm
an, tamil, telugu, turkish, turkmen, ukenglish, ukrainian, uppersorbian, usengl
ishmax, welsh, loaded.
("C:\Program Files\MiKTeX 2.9\tex\latex\base\article.cls"
Document Class: article 2007/10/19 v1.4h Standard LaTeX document class
("C:\Program Files\MiKTeX 2.9\tex\latex\base\size10.clo"))
("D:\Учеба\10 семестр\защита информации\test.aux")
[1] ("D:\Учеба\10 семестр\защита информации\test.aux")
Output written on test.dvi (1 page, 240 bytes).
Transcript written on test.log.

```

Рис. 2: Компиляция в консоли.

Так же tex файла можно преобразовать в PDF файлы с помощью ко-манды PDFLATEX(Рис 3).

3 Оболочка TexMaker, Быстрый старт, Быст- рая сборка

Вместо texmaker был установлен не менее удобный редактор texstudio. Texstudio - это редактор текста поддерживающий язык разметки Latex. Он реализует всю функциональность, требующуюся для работы с мно-гостраничными документами. Внешний вид редактора выглядит следу-ющим образом(Рис 4).

В редакторе так же реализованы две функции: быстрый старт и быст-рая сборка. Первая - позволяет быстро создать шаблон документа(Рис 5).

Вторая скомпилировать его и преобразовать в читаемый вид. Процесс схож с компиляцией программы. Имеется возможность задания после-довательности действий при быстрой сборке.

```

D:\Учеба\10 семестр\защита информации>pdflatex test.tex
This is pdfTeX, Version 3.1415926-2.5-1.40.14 (MiKTeX 2.9 64-bit)
entering extended mode
("D:\Учеба\10 семестр\защита информации\test.tex"
LaTeX2e <2011/06/27>
Babel <v3.8m> and hyphenation patterns for english, afrikaans, ancientgreek, ar
abic, armenian, assamese, basque, bengali, bokmal, bulgarian, catalan, coptic,
croatian, czech, danish, dutch, esperanto, estonian, farsi, finnish, french, ga
lician, german, german-x-2013-05-26, greek, gujarati, hindi, hungarian, iceland
ic, indonesian, interlingua, irish, italian, kannada, kurmanji, latin, latvian,
lithuanian, malayalam, marathi, mongolian, mongolianlmc, monogreek, ngerman, n
german-x-2013-05-26, nynorsk, oriya, panjabi, pinyin, polish, portuguese, roman
ian, russian, sanskrit, serbian, slovak, slovenian, spanish, swedish, swissgerm
an, tamil, telugu, turkish, turkmen, ukenglish, ukrainian, uppersorbian, usengl
ishmax, welsh, loaded.
("C:\Program Files\MiKTeX 2.9\tex\latex\base\article.cls"
Document Class: article 2007/10/19 v1.4h Standard LaTeX document class
("C:\Program Files\MiKTeX 2.9\tex\latex\base\size10.clo"))
("D:\Учеба\10 семестр\защита информации\test.aux")
[1{C:/ProgramData/MiKTeX/2.9/pdftex/config/pdftex.map}]
("D:\Учеба\10 семестр\защита информации\test.aux")
)<C:/Program Files/MiKTeX 2.9/fonts/type1/public/amsfonts/cm/cmri10.pfb>
Output written on test.pdf (1 page, 13012 bytes).
Transcript written on test.log.

```

Рис. 3: Компиляция pdf в консоли.

4 Создание титульного листа, нескольких раз- делов, списка, несложной формулы

Содание титульного листа в самом простом варианте осуществляется следующим образом. В преамбуле документа нужно указать название документа и автора.

```

\title{Лабораторные работы №1-3 \Курс: Защита информации}
\author{Воробьев Олег}

```

Затем, сам заголовок создается командой

```

\maketitle

```

В итоге получаем титульный лист (Рис 6).

Новый раздел создается командой part

```

part[1]{Раздел 1}
part[2]{Раздел 2}
part[3]{Раздел 3}

```

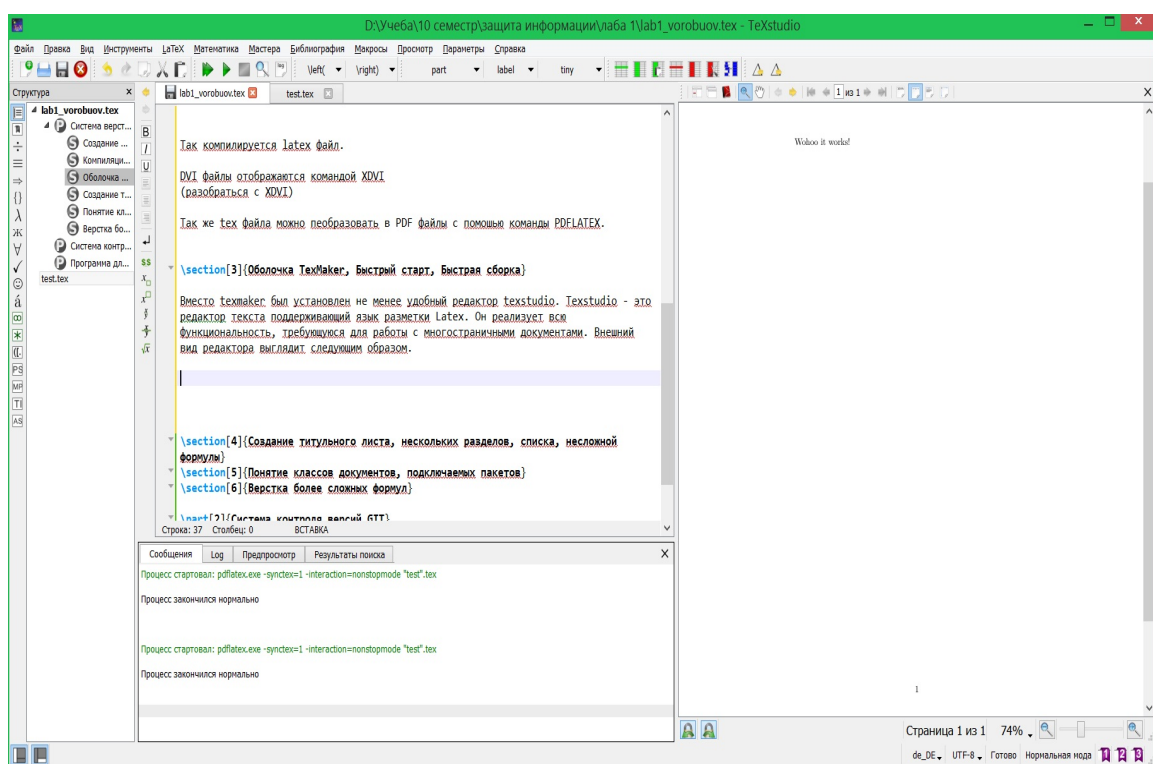


Рис. 4: Вид texstudio.

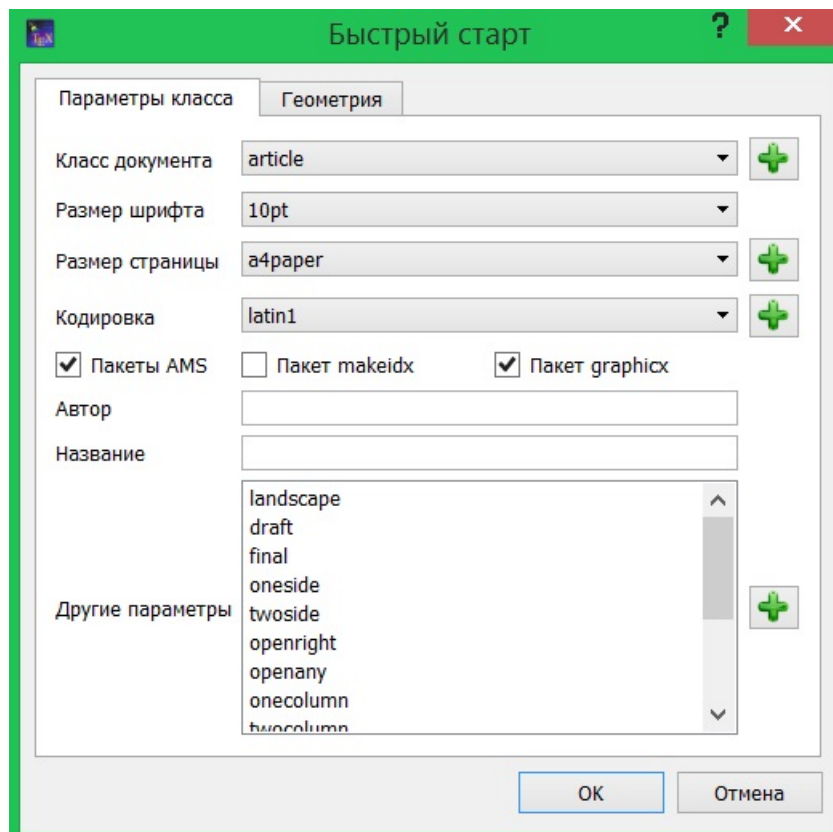


Рис. 5: Создание шаблона документа.

Лабораторные работы №1-3

Курс: Защита информации

Воробьев Олег

3 марта 2015 г.

Рис. 6: Титульный лист.

Part I
1

Part II
2

Part III
3

Рис. 7: Разделы.

- one
- two
- three

Рис. 8: Списки.

В документе это выглядит следующим образом (Рис 7). Списки в LATEX создаются автоматически с помощью нескольких команд. Перед каждым элементом всегда должна идти команда ITEM, внутри блока begin-end реализуется сам список (Рис 8). Процесс написания формул схож таковым в MATLAB. Выглядит это примерно так:

`f\{x,y}\=\frac{x^2+y^2}{\sqrt{x^3+y^3}}`

$$f(x, y) = \frac{x^2 + y^2}{\sqrt{x^3 + y^3}}$$

5 Понятие классов документов, подключаемых пакетов

Каждый файл в LATEX начинается с команды `documentclass[...]`, в фигурных скобках которой задаются параметры оформления стиля документа, а в квадратных — список классовых опций. Всего в LATEX 5 основных классов документов:

- article для статей

- report для книг и статей
- book для книг
- proc для докладов
- letter для оформления деловых писем .

Помимо этих основных, есть ещё множество дополнительных.

В LATEX помимо стандартных настроек существует возможность подключения сторонних пакетов со специфическими настройками. Такие пакеты расширений подключаются в шапке документа.

`usepackage{listings}` предоставляет возможности цитирования кода в тексте с сох.

6 Верстка более сложных формул

Рассмотрим формулу проведения консолидированного платежа.

$$\frac{P_0}{1+n_0*r} = \sum_{k=1}^m \frac{P_k}{1+n_k*r}$$

7 Вывод

LATEX наиболее популярный набор макросов системы компьютерной вёрстки TEX, который облегчает набор сложных документов. Упрощается и автоматизируется процесс написания текста и подготовки статей. Существует множество пакетов расширения LATEX, позволяющих удобно настраивать документ. Для работы с latex чаще всего используются специализированные среды, поддерживающие разметку и выделение кода, позволяющие автоматически компилировать документы, предпросматривать конечный результат и тд.

Часть II

Система контроля версий GIT

8 Получить содержимое репозитория

Содержимое репозитория можно получить простой командой.

`git clone git@github.com:Vorobjov101/InfoSecCourse2015.git`

9 Добавить папку и файл в систему

Создание папки в репозитории и добавление файла в нее.

```
mkdir test
cd test
echo 11001 >> var
git add --all
```

10 Зафиксировать изменения в локальном репозитории

```
git commit -a -m "file added"
```

11 Внести изменения в файл и посмотреть различия

```
echo 11111 >> var
git diff master:./var ./var
```

12 Отменить локальные изменения

```
git reset HEAD ./var
git checkout ./var
```

13 Внести изменения в файл и посмотреть различия

```
echo 00010101 >> var
git diff master:./file ./file
```

14 Зафиксировать изменения в локальном репозитории, зафиксировать изменения в центральном репозитории

```
git commit -a -m "file changed"
```

`git_push`

15 Получить изменения из центрального репозитория

`git_pull`

16 Поэкспериментировать с ветками

`git_branch -n`
`git_checkout master`
`git_merge temp`
`git_branch`

17 Вывод

Git система предоставляющая возможность управления версиями файлов и их распределенное хранение. Git используется во множестве проектов для обеспечения совместной работы над проектом.

Часть III

Программа для шифрования и подписи GPG, пакет Gpg4win

18 Создать ключевую пару OpenGr

Kleopatra это графический интерфейс к GnuPG и предназначенных для работы под окружением KDE, портированный на MS Windows(Рис 9). Выглядит ключ следующим образом(Рис 10).

19 Поставить ЭЦП на файл

После подписания файла создается го копия, но с измененным форматом. В конце приписывается .sig(Рис 11).

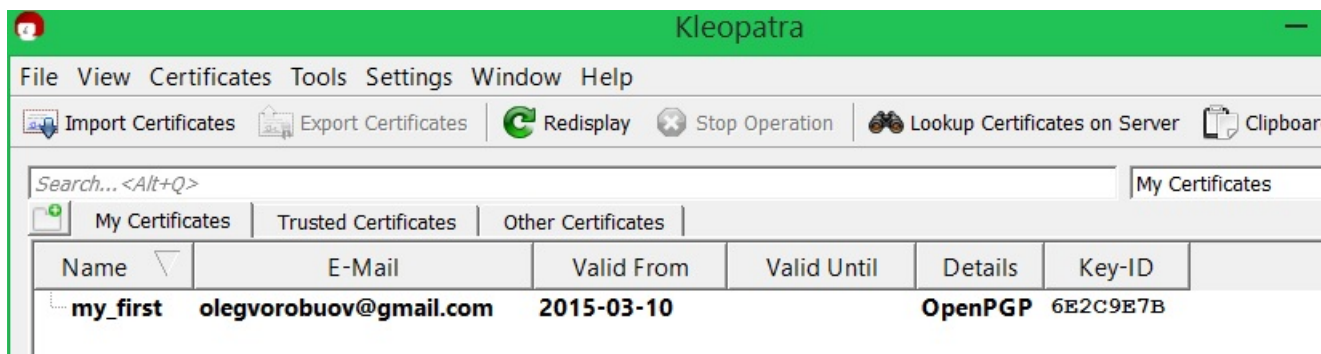


Рис. 9: Новая ключевая пара.

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

mQENBFT+H0kBCACV0+DmQXr2nE53P1BBdIKO/M402NtDiurQh6tc2fp0EX9dg/w5
tD2+to7CPTqLPV1H5v3h3J0d0MF23U9cmIlw1fzIulrPSnja4cwrz6nTrfbEYdzQ
IHAgnv0sSBnLdHcjlq/HptDAVHiil8AYV1lB1BAKMsRjPC8ctMSn4B8FypxMxLgm
hrTUZb8w7Ye5ZJwpMp3hKb5Na80kLE0+i4akpQ9Gx9cG2S1rkFEdaG332L0o3HTt
e3L4GWQyrBrcotCykLQJ8xq3LXBsFZguni9mHKTlCdnm+E4H0+gZtJxQUpEvt1GI
4xBOnz5m2qId6HmTH782Xz3NROK6kMAFSB2zABEBAAG0IW15X2ZpcnN0IDxvbGVn
dm9yb2J1b3ZAZ21haWwY29tPokBOQQTAAQIAIwUCVP4c6QIbDwcLCQgHAwIBBhUI
AgkKCwQWAgMBAh4BAheAAoJEFJZBupuLJ57X3cH/R6wAg2WwBU0DvrFFfkFscCg
KCvm3d2nVT5zH0CW8VtkY8kHQyg2zdn6t75RLr05dDp6C+B6jxfiRY8s95i2JtQn
kAjQKG274nxU9/8TF9hvygxN8qnZ3MKkKSjjQT4uSrEvrIfyqbHm4WPI6fb81xyY
NEUb5JXdQ7MBbB4/OCISdqNl64CwlpNderhUrjJyXKYBA90tTjuu2bfsbfE2/el1
g+gqym8+QSydVHFTdTnqKZx15gQ7NRAev+3Iq4DuR2+XeLeqqfZxxWchS1L2jEAR
8RQYi09fhc7VnN8yfp1MLI1S8p0AUPrJTs5dnGMlUk3Xzi1AIBdCwlffnxii29s=
=oZlZ
-----END PGP PUBLIC KEY BLOCK-----
```

Рис. 10: Ключ.

```
lec2_vorobuov.aux
lec2_vorobuov.log
lec2_vorobuov.pdf
lec2_vorobuov.tex
lec2_vorobuov.log.sig
lec2_vorobuov.synctex.gz
```

Рис. 11: Файл lec2 vorobuov с подписью

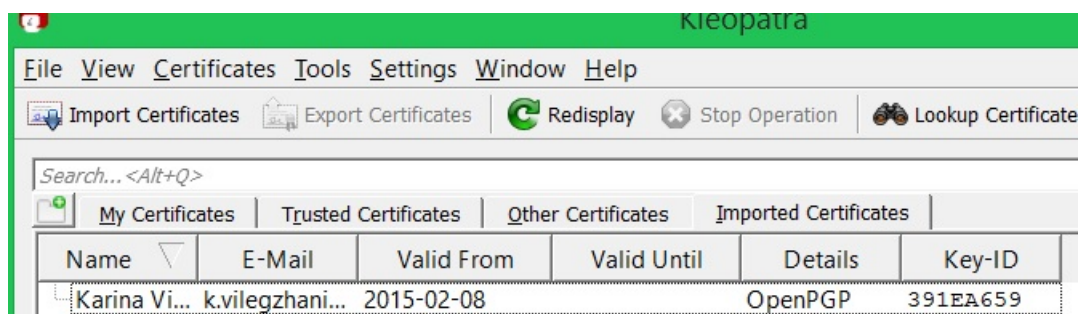


Рис. 12: Полученный сертификат.

20 Получить чужой сертификат,импортировать его, проверить подпись

Получив чужой сертификат(Рис 12), можно расшифровывать подписанные этим пользователем файлы(Рис 13).

21 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 14). Мы можем уедиться, что он создан с помощью команды(Рис 15).

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

Для импорта и экспорта используются команды `-import` и `-armor` соответственно.

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

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.

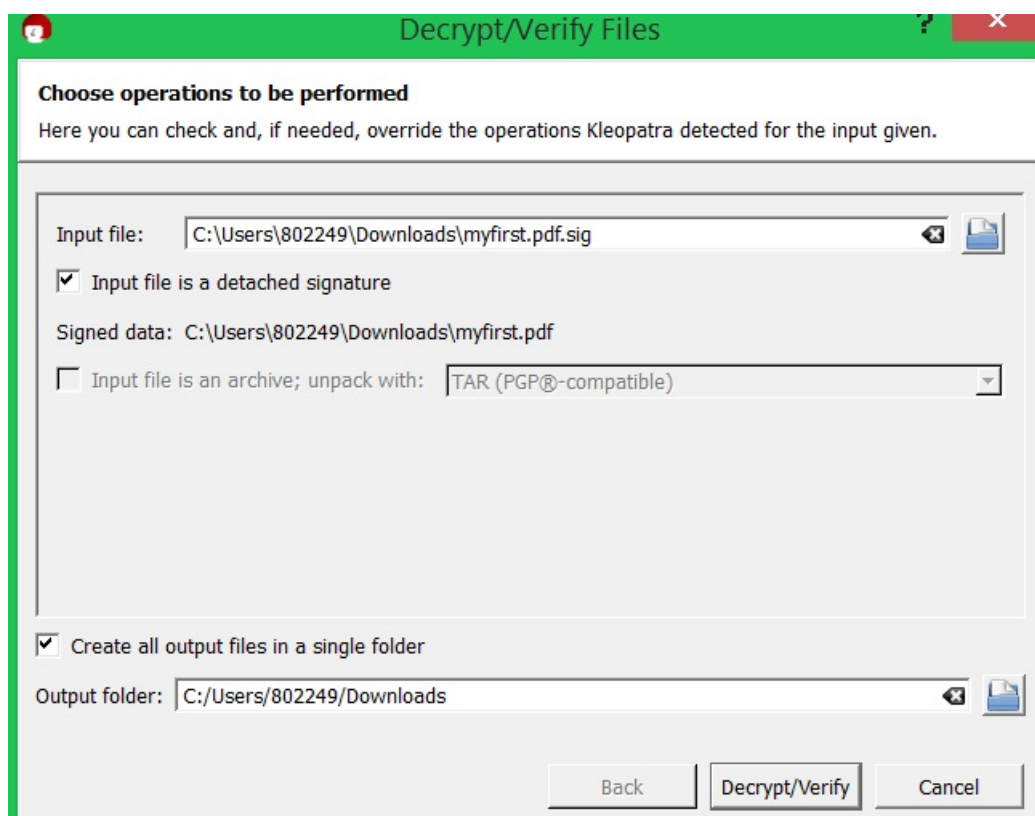


Рис. 13: Расшифровка файла с помощью импортированного сертификата.

```

C:\Users\802249>gpg --gen-key
gpg (GnuPG) 2.0.26; Copyright (C) 2013 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 требуемый тип ключа:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (только для подписи)
  (4) RSA (только для подписи)
Ваш выбор (?-подробнее)? 1
Ключи RSA могут иметь длину от 1024 до 4096 бит.
Какой размер ключа необходим? (2048)
Запрашиваемый размер ключа 2048 бит
Выберите срок действия ключа.
    0 = без ограничения срока действительности
    <n> = срок действительности n дней
    <n>w = срок действительности n недель
    <n>m = срок действительности n месяцев
    <n>y = срок действительности n лет
Ключ действителен до? (0) 11.03.2015
недопустимое значение
Ключ действителен до? (0) 2
Ключ действителен до: 03/12/15 01:57:36 RTZ 2 (чшър)
Все верно? (y/N) y

GnuPG необходимо составить UserID в качестве идентификатора ключа.

Ваше настоящее имя: oleg
Имя не должно быть короче 5 символов
Ваше настоящее имя: olegvorobuov
Email-адрес: olegvorobuov@gmail.com
Комментарий:
Вы выбрали следующий User ID:
    "olegvorobuov <olegvorobuov@gmail.com>"

Сменить (N)Имя, (C)Комментарий, (E)email-адрес или (O)Принять/(Q)Выход? o
Для защиты секретного ключа необходима фраза-пароль.

```

Рис. 14: Создание ключа в консоли.

```

pub      2048R/61F0ED62 2015-03-09 [просрочен с: 2015-03-11]
uid      [просрочен] olegvorobuov <olegvorobuov@gmail.com>

D:\Учеба\10 семестр\защита информации\паба 1>gpg --export -a my_first
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFT+H0kBCACU0+DmQXr2nE53P1BBdIK0/M402NtDiurQh6tc2fp0EX9dg/w5
tD2+to7CPTqLPU1H5v3h3J0d0MF23U9cmIlw1fzIulrPSnja4cwrz6nTrfbEYdzQ
IHAgvu0sSBnLdHcj1q/HptDAUHii18AYU11B1BAKMsRjPC8ctMSn4B8FypxMxLgm
hrTUZb8w7Ye5ZJwpMp3hKb5Na80kLE0+i4akpQ9Gx9cG2S1rkFEdaG332L0o3HTt
e3L4GwQyrBrcotCykLQJ8xq3LXBsFZguni9mHKT1Cdnm+E4H0+gZtJxQUpEvt1GI
4xB0nz5m2qId6HmTH782Xz3NR0K6kMAfSB2zABEBAAG0IW15X2ZpcnN0IDxubGVu
dm9yb2J1b3ZAZ21haWwvY29tPokB0QQTAAIAIwUCUP4c6QIbDwcLCQgHAWIBBhUI
AgkKCwQWAgMBAh4BAheAAAOJEFJZBupuLJ57X3cH/R6wAg2WwBU0DurFFfkFscCg
KCum3d2nUT5zH0CW8UtkY8kHQyg2zdn6t75RLr05dDp6C+B6jxfiRY8s95i2JtQn
kAjQKG274nxU9/8TF9huygxN8qnZ3MKkKSjjQT4uSrEvrIfyqbHm4WPI6fb81xyY
NEUb5JXdQ7MBbB4/OCISdqN164CwlpNderhUrjJyXKYBA90tTjuu2bfsbfE2/e11
g+gqym8+QSydUHFTdTnqKZx15gQ7NRAev+3Iq4DuR2+Xe1eqqfZxxWchS1L2jEAR
8RQYi09fhc7UnN8yfp1MLI1S8p0AUPrJTs5dnGM1Uk3Xzi1AIBdCw1ffnxii29s=
=oZ1Z
-----END PGP PUBLIC KEY BLOCK-----

D:\Учеба\10 семестр\защита информации\паба 1>_

```

Рис. 15: Отображение всех зарегистрированных в система ключей.

```
pub      2048R/61F0ED62 2015-03-09 [просрочен с: 2015-03-11]
uid      [просрочен] olegvorobuov <olegvorobuov@gmail.com>

D:\Учеба\10 семестр\защита информации\лаба 1>gpg --export -a my_first
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFT+H0kBCACU0+DmQXr2nE53P1BBdIK0/M402NtDiurQh6tc2fp0EX9dg/w5
tD2+to7CPTQLPU1H5v3h3J0d0MF23U9cmI1w1fzIu1rPSnja4cwrz6nTrfbEYdzQ
IHAgnu0sSBnLdHcjlq/HptDAVHiil8AYU11B1BAKMsRjPC8ctMSn4B8FypxMxLgm
hrTUZb8w7Ye5ZJwpMp3hKb5Na80kLE0+i4akpQ9Gx9cG2S1rkFEdaG332L0o3HTt
e3L4GwQyrBrcotCykLQJ8xq3LXBsFZguni9mHKT1Cdnm+E4H0+gZtJxQUUpEvt1GI
4xB0nz5m2qId6HmTH782Xz3NR0K6kMAfSB2zABEBAAG0IW15X2ZpcnN0IDxubGVn
dm9yb2J1b3ZAZ21haWwuyY29tPokB0QQTAAQIAIwUCVP4c6QIbDwcLCQgHAwIBBhUI
AgkKCwQWAgMBAh4BAheAAoJEFJZBupuLJ57X3cH/R6wAg2WwBU0DurFFfkFscCg
KCum3d2nUT5zH0CW8UtkY8kHQyg2zdn6t75RLr05dDp6C+B6jxfiRY8s95i2JtQn
kAjQKG274nxU9/8TF9hvygxn8qnZ3MKkK$jjQT4uSrEurIfyqbHm4WPI6fb81xyY
NEUb5JXdQ7MBbB4/OCISdqN164CwlpNderhUrjJyXKYBA90tTjuu2bfsbfE2/e11
g+gqym8+QSydUHFTdTnqKZx15gQ7NRAev+3Iq4DuR2+Xe1eqqfZxxWchS1L2jEAR
8RQYi09fhc7UnN8yfp1MLI1S8p0AUPrJT55dnGM1Uk3Xzi1AIBdCw1ffnxii29s=
=oZ1Z
-----END PGP PUBLIC KEY BLOCK-----

D:\Учеба\10 семестр\защита информации\лаба 1>_
```

Рис. 16: Экспорт ключа.

```
D:\Учеба\10 семестр\защита информации\лаба 1>gpg --export -a my_first > my_first
.asc
```

Рис. 17: Экспорт ключа в файл.

Как видно, появился файл lab1_vorobuov.pdf.asc, теперь его можно передать на клиентскую машину для расшифровки. Расшифровать можно с помощью команды:

```
gpg -d lab1_vorobuov.pdf.asc >lab1_vorobuov.pdf
```



```
D:\Учеба\10 семестр\защита информации\паба 1>gpg -ea -r my_first lab1_vorobuov.pdf
D:\Учеба\10 семестр\защита информации\паба 1>dir
Том в устройстве D имеет метку Data
Серийный номер тома: 18D1-3E7C

Содержимое папки D:\Учеба\10 семестр\защита информации\паба 1
07.06.2015  23:27    <DIR>          .
07.06.2015  23:27    <DIR>          ..
10.03.2015  01:24                960 2BBF6A7B4639C72EC2E31D2A525906EA6E2C9E7B.asc

09.03.2015  22:55                0 document.tex
07.06.2015  22:20             6a708 lab1_vorobuov.aux
07.06.2015  22:20             34a110 lab1_vorobuov.log
07.06.2015  22:20             1a755a876 lab1_vorobuov.pdf
07.06.2015  23:27             1a983a764 lab1_vorobuov.pdf.asc
07.06.2015  22:20             25a668 lab1_vorobuov.synctex.gz
07.06.2015  23:20             14a001 lab1_vorobuov.tex
26.04.2015  20:20             1a154 lab1_vorobuov.toc
07.06.2015  23:22             960 my_first.asc
```

Рис. 18: Шифрование файла.