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, включкющий в себя минимум строк(Рис 1).

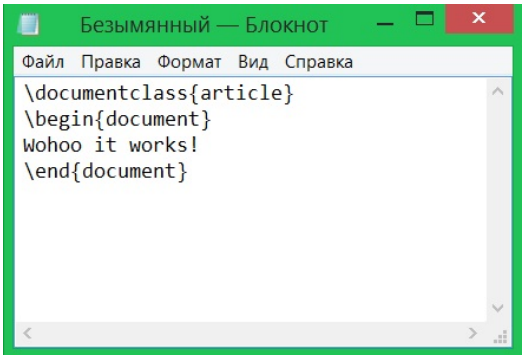

Рис. 1: Простейший tex документ.

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

2 Компиляция в командной строке – latex, xdvi, 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).

Рис. 2: Компиляция в консоли.

Так же tex файла можно преобразовать в PDF файлы с помошью команды PDFLATEX(Рис 3).

3 Оболочка TexMaker, Быстрый старт, Быстрая 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 многостраничными документами. Внешний вид редактора выглядит следующим образом(Рис 4).

В редакторе так же реализованы две функции: быстрый старт и быстрая 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 последовательности действий при быстрой сборке.

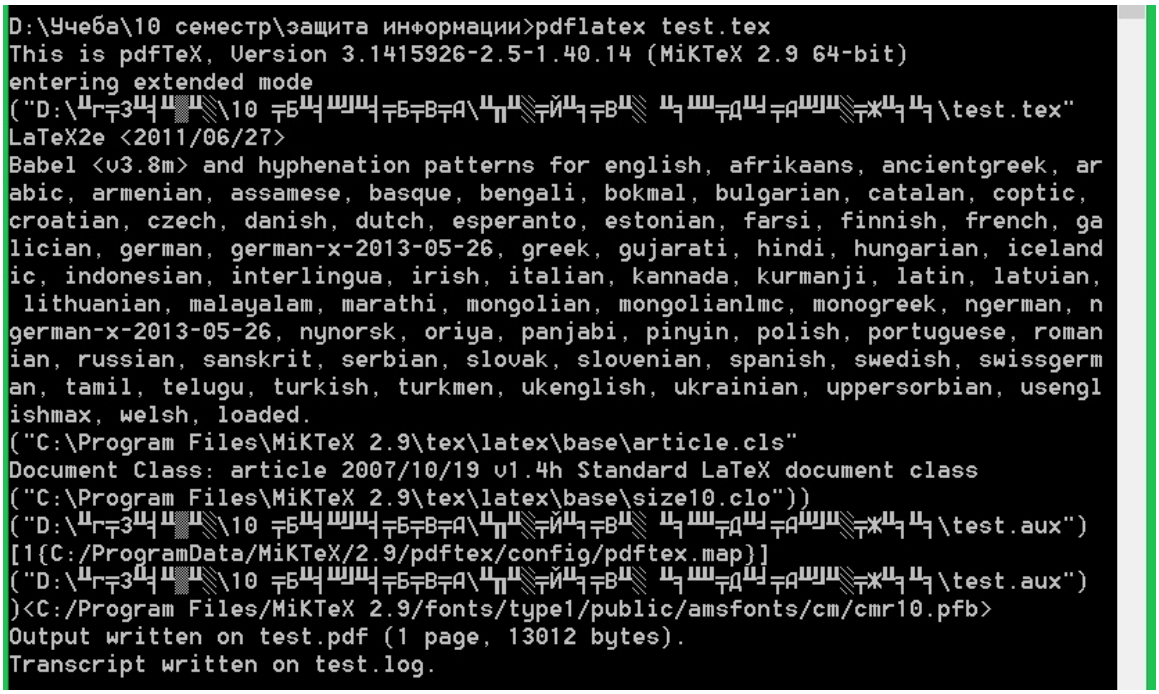

Рис. 3: Компиляция pdf в консоли.

4 Создание титульного листа, нескольких разделов, 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}
```

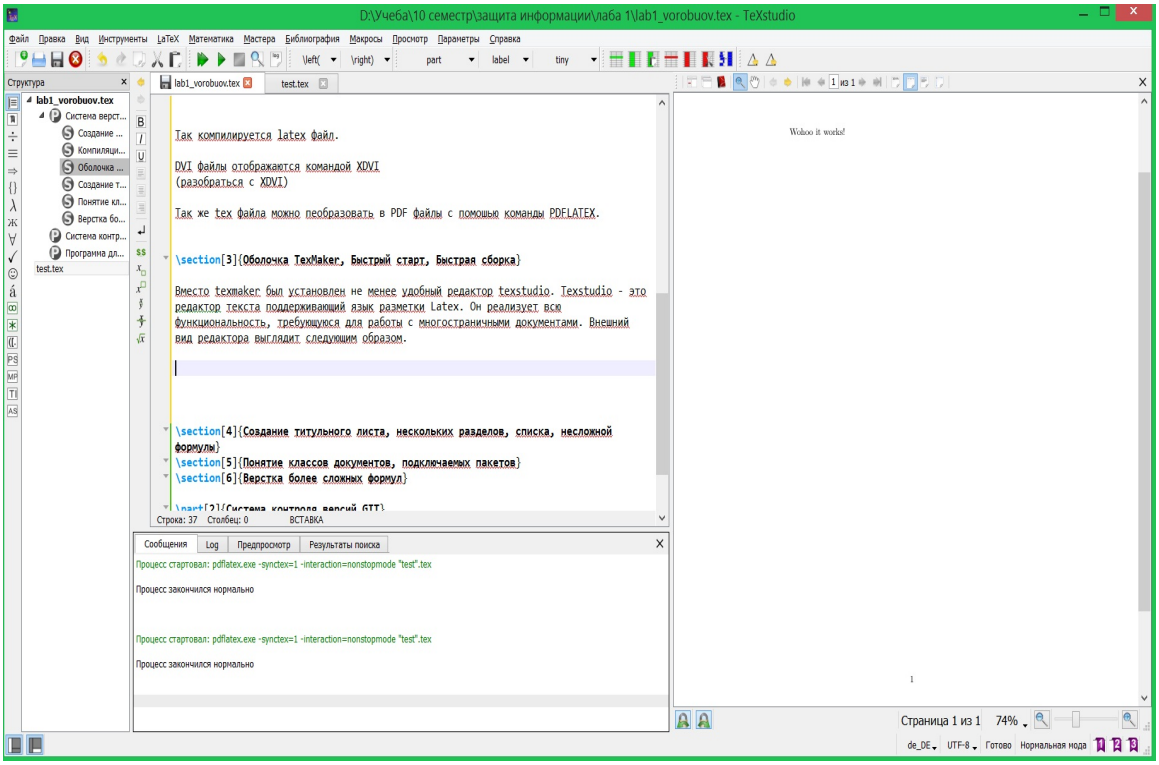

Рис. 4: Вид texstudio.

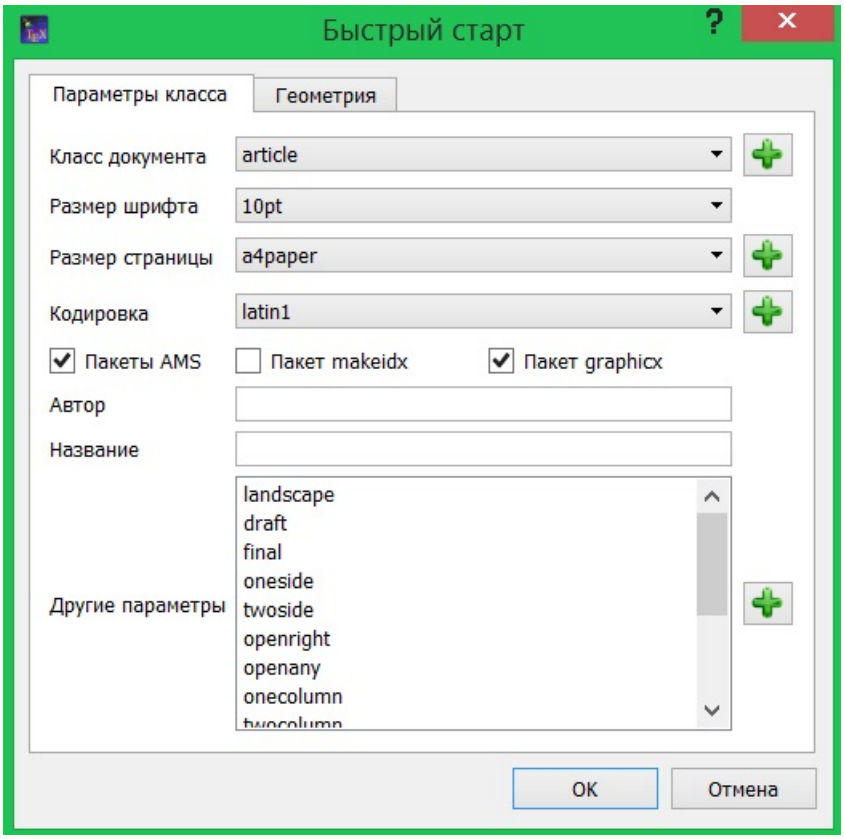

Рис. 5: Создание шаблона документа.

Лабораторные работы №1-3
Курс: Защита информации

Воробьев Олег

3 марта 2015 г.

Рис. 6: Титульный лист.

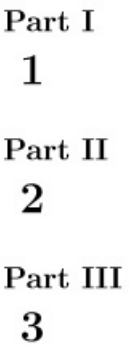

Рис. 7: Разделы.

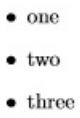

Рис. 8: Списки.

В документе это выглядит следующим образом(Рис 7). Списки в LATEX создаются автоматически с помошью нескольких команд. Перед каждым элементом вседа должна идти команда ITEM,внутри блока begin-end реализуется сам список(Рис 8). Процесс написания формул схож таковым в MATLAB. Вышлядит 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 раширений 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}
```

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

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 специализированняе среды, поддерживающие разметку и выделение кода, поволяющие 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 распределеное 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 OpenGp

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).

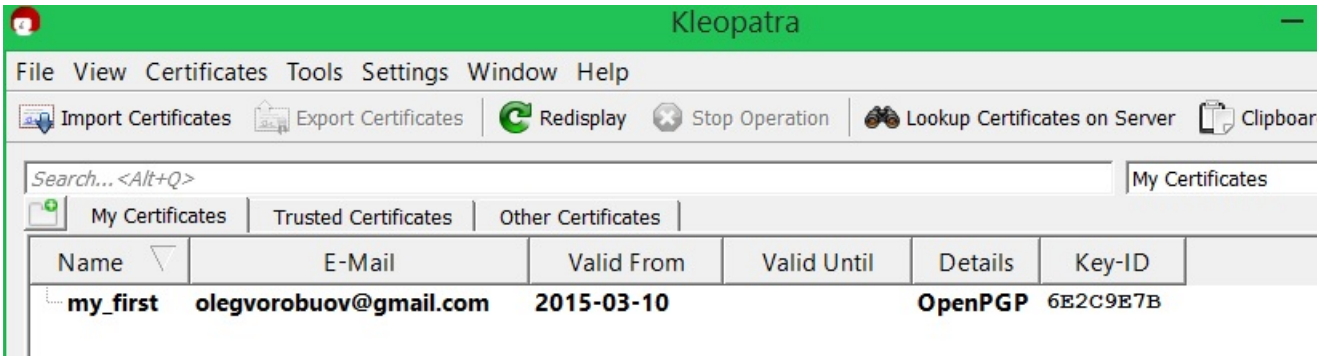

Рис. 9: Новая ключевая пара.

Рис. 10: Ключ.

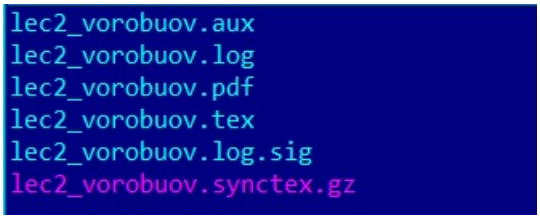

Рис. 11: Файл lec2 vorobuov с подписью

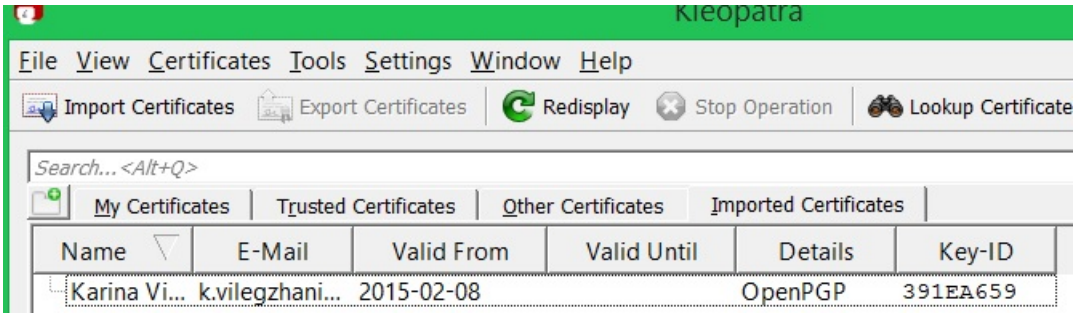

Рис. 12: Полученный сертификат.

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 помошью 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.

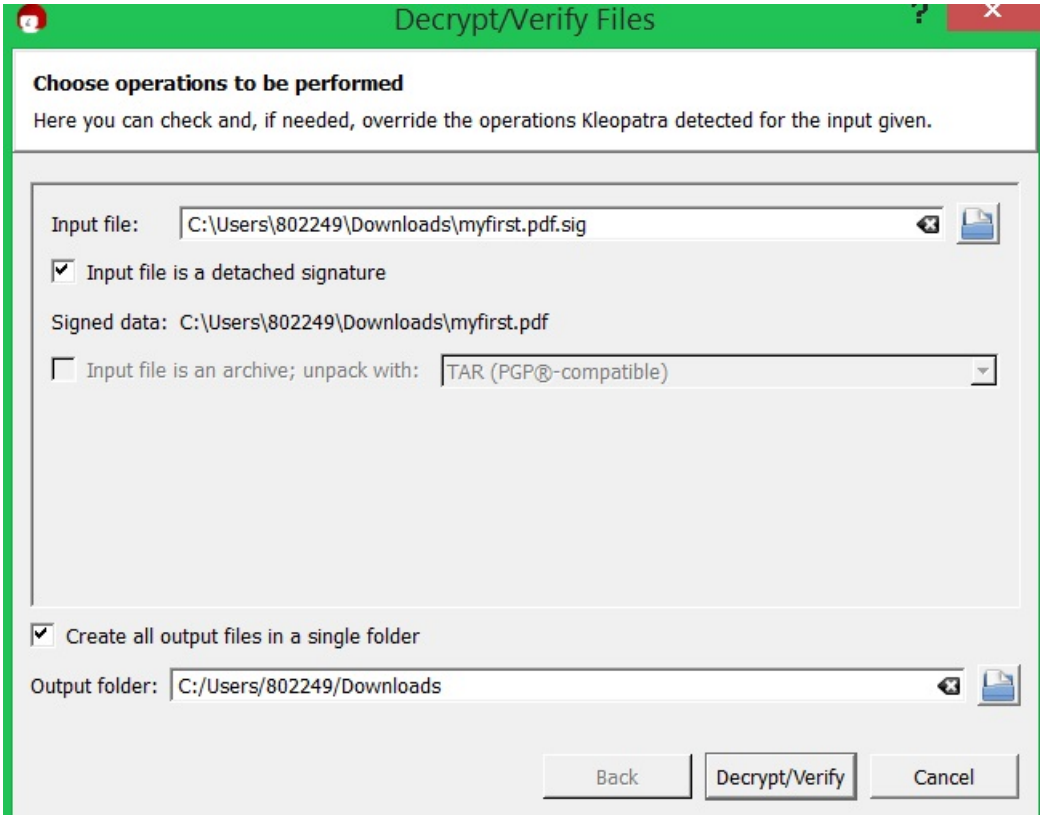

Рис. 13: Расшифровка файла с помощью импортированного сертификата.

```
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 (чшьр)
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.
```
cc

Рис. 14: Создание ключа в консоли.

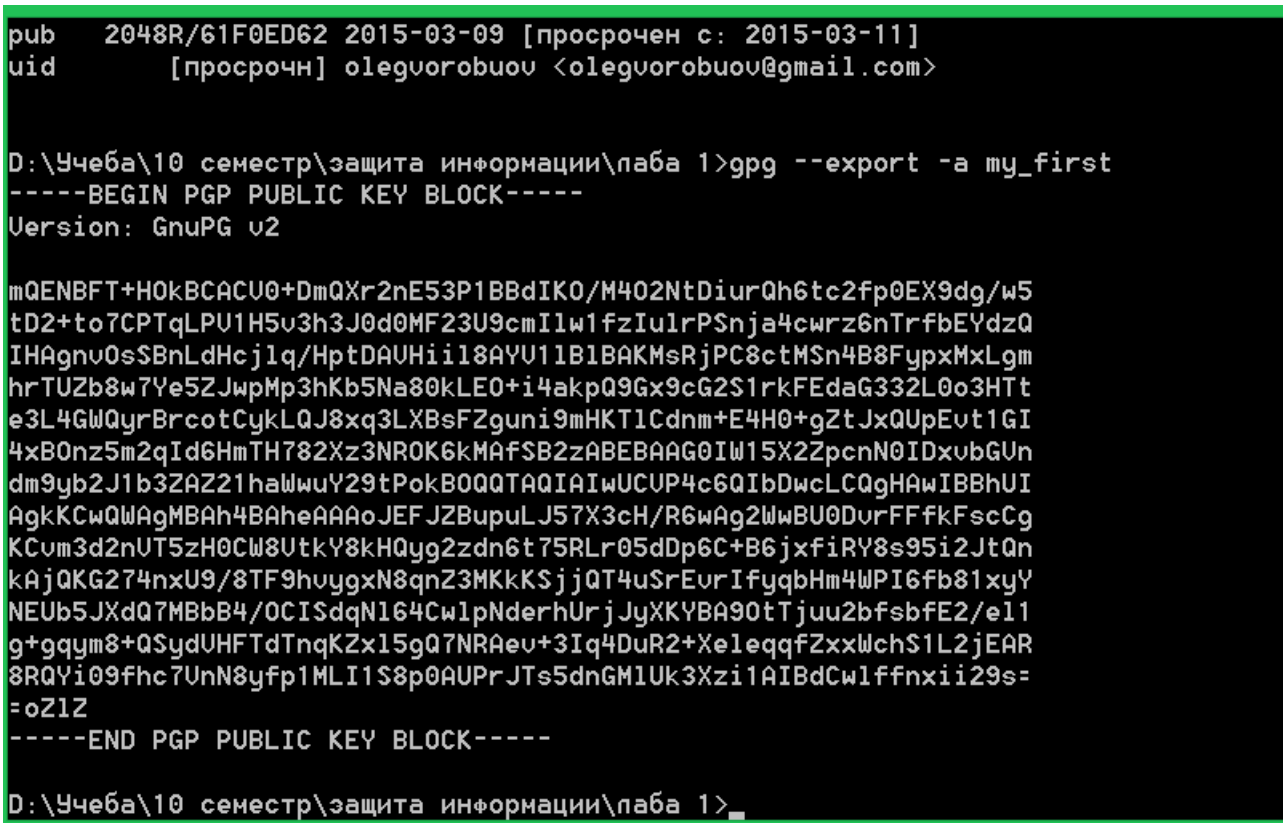

Рис. 15: Отображение всех зарегестрированных в система ключей.

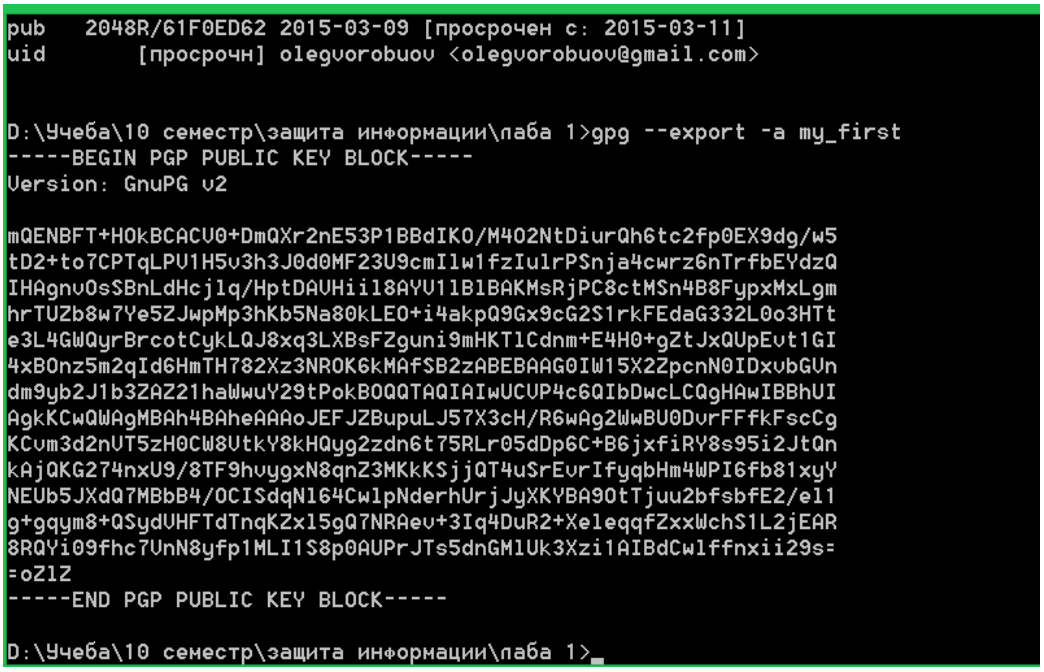

Рис. 16: Экспорт ключа.

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 помошью команды:

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

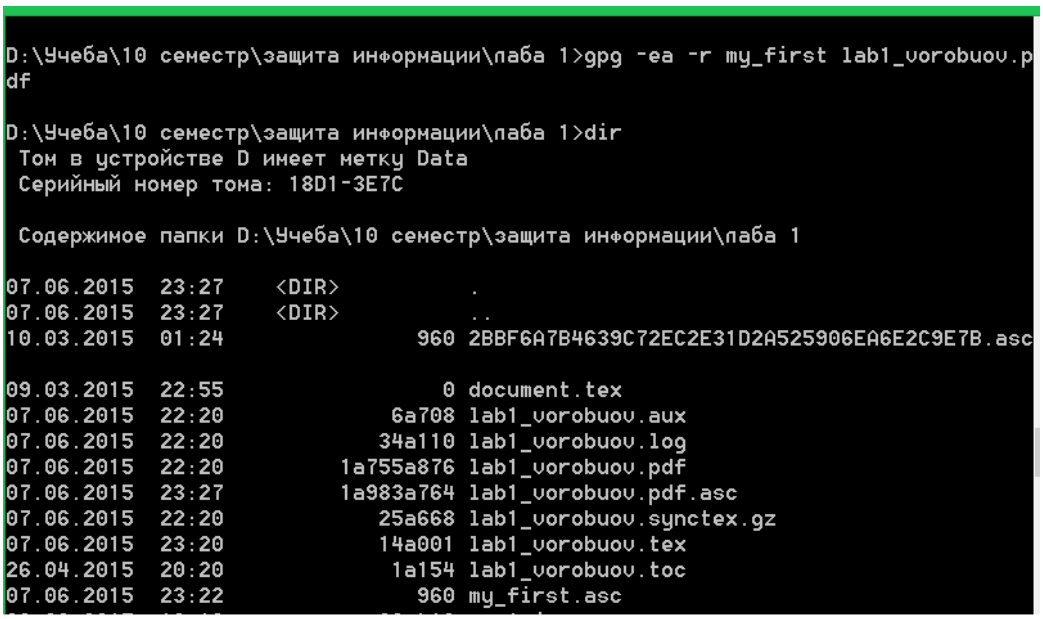

Рис. 18: Шифорвание файла.