

# Отчет по лабораторной работе 1:

## L<sup>A</sup>T<sub>E</sub>X Git GPG

Семён Мартынов

<semen.martynov@gmail.com>

2 марта 2015 г.

## Содержание

<b>1</b>	<b>Система верстки T<sub>E</sub>X и расширения L<sup>A</sup>T<sub>E</sub>X</b>	<b>2</b>
1.1	Цель работы . . . . .	2
1.2	Ход работы . . . . .	2
1.2.1	Компиляция в командной строке . . . . .	2
1.2.2	Оболочка TexMaker . . . . .	2
1.2.3	Классы документов . . . . .	4
1.2.4	Подключаемые пакеты . . . . .	4
1.2.5	Вёрстка формул . . . . .	5
1.3	Выводы . . . . .	5
<b>2</b>	<b>Система контроля версий Git</b>	<b>6</b>
2.1	Цель работы . . . . .	6
2.2	Ход работы . . . . .	6
2.3	Выводы . . . . .	7
<b>3</b>	<b>Создание электронных цифровых подписей с PGP</b>	<b>8</b>
3.1	Цель работы . . . . .	8
3.2	Ход работы . . . . .	8
3.2.1	Знакомство с пакетом Kleopatra . . . . .	8
3.2.2	Использовании gpg через интерфейс командной строки . . . . .	10
3.3	Выводы . . . . .	11

# 1 Система верстки $\text{T}_{\text{E}}\text{X}$ и расширения $\text{L}_{\text{A}}\text{T}_{\text{E}}\text{X}$

## 1.1 Цель работы

Изучение принципов верстки  $\text{T}_{\text{E}}\text{X}$ , создание первого отчёта.

## 1.2 Ход работы

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

### 1.2.1 Компиляция в командной строке

- `latex` генерирует файл в формате DVI (**DeVice Independent** — аппаратно независимый) не предназначенный для чтения человеком, но содержит двоичные данные, описывающие визуальное представление документа способом, не ориентированным на какой-либо формат изображения, монитор или принтер. Файлы DVI обычно подаются на вход другой программы (называемой DVI-драйвером), которая преобразует их в графические данные.

```
latex report.tex
```

- `xdvi` одна из программ DVI-драйверов, позволяющих отображать данные в формате DVI в X Window системах

```
xdvi report.dvi
```

Результат показан на рисунке 1.

- `pdflatex` позволяет сразу сгенерировать pdf файл. Главное различие между  $\text{TeX}$  и `pdfLaTeX` состоит в том, что  $\text{TeX}$  после трансляции выдаёт DVI-файлы, а `pdfTeX` — PDF-файлы, минуя цепочку преобразований DVI  $\rightarrow$  PS  $\rightarrow$  PDF.

```
pdflatex report.tex
```

### 1.2.2 Оболочка `TexMaker`

`Texmaker` является мощным редактором текста и исходного кода, работающий с языком разметки  $\text{LaTeX}$ . Он позволяет форматировать текст и готовить многостраничные документы к печати. Редактор предоставляет возможность работы с библиографическими списками, оглавлением и другими атрибутами профессионального оформления. В `Texmaker` есть так

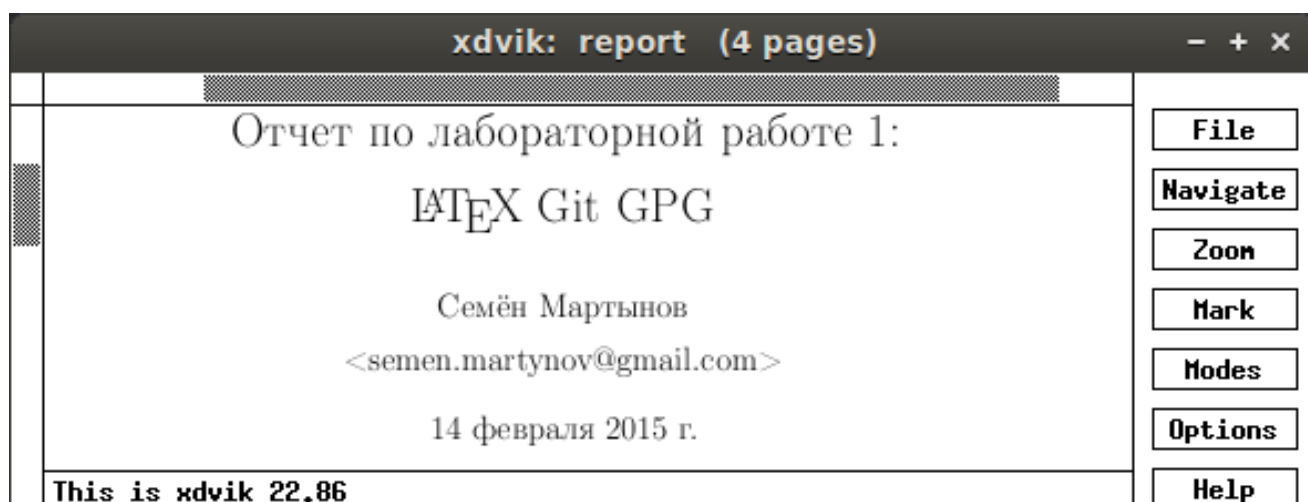


Рис. 1: Запуск xdvik

же возможность конвертирования документов в различные форматы, функции сворачивания блоков кода и автозавершения кода, встроенный просмотрщик PDF документов и многое другое. Внешний вид редактора представлен на рисунке 2.

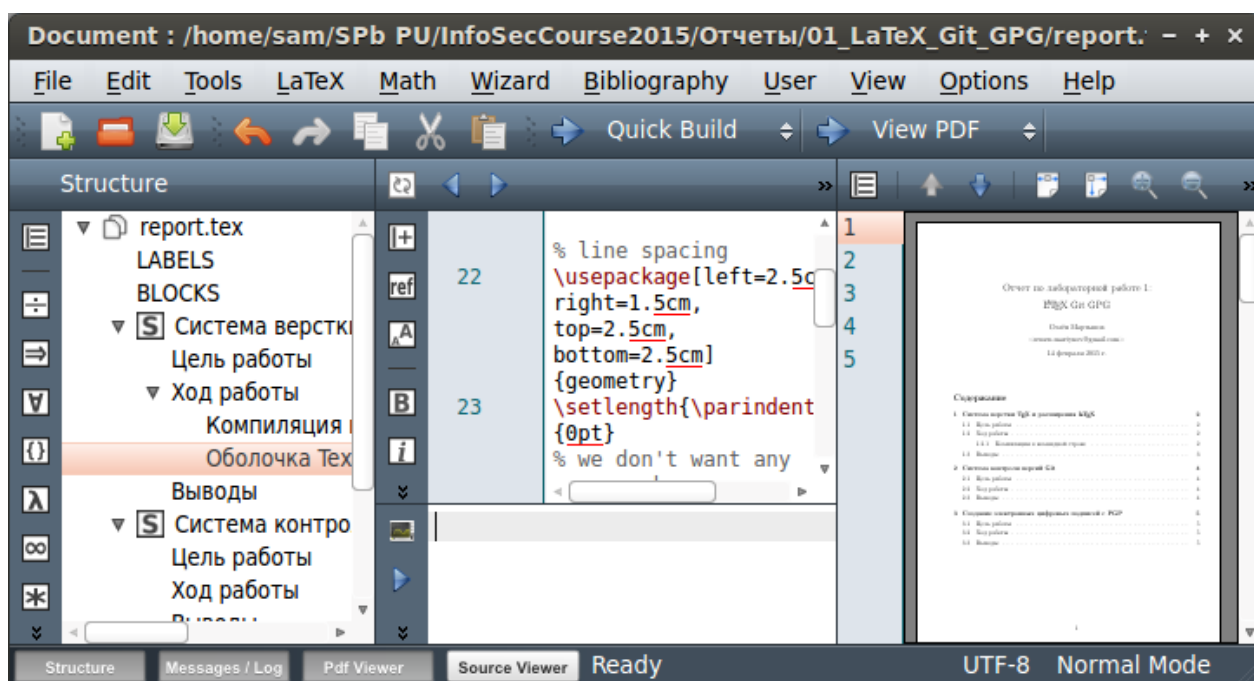


Рис. 2: Редактор TexMaker

Texmaker обладает двумя интересными возможностями: быстрый старт и быстрая сборка. Быстрый старт (рисунок 2) позволяет задать преамбулу (главные особенности - класс, размер бумаги, кодировку...) документа. Имеется возможность создать собственную модель преамбулы в редакторе.

Самый простой способ скомпилировать документ это использовать команду "Быстрая

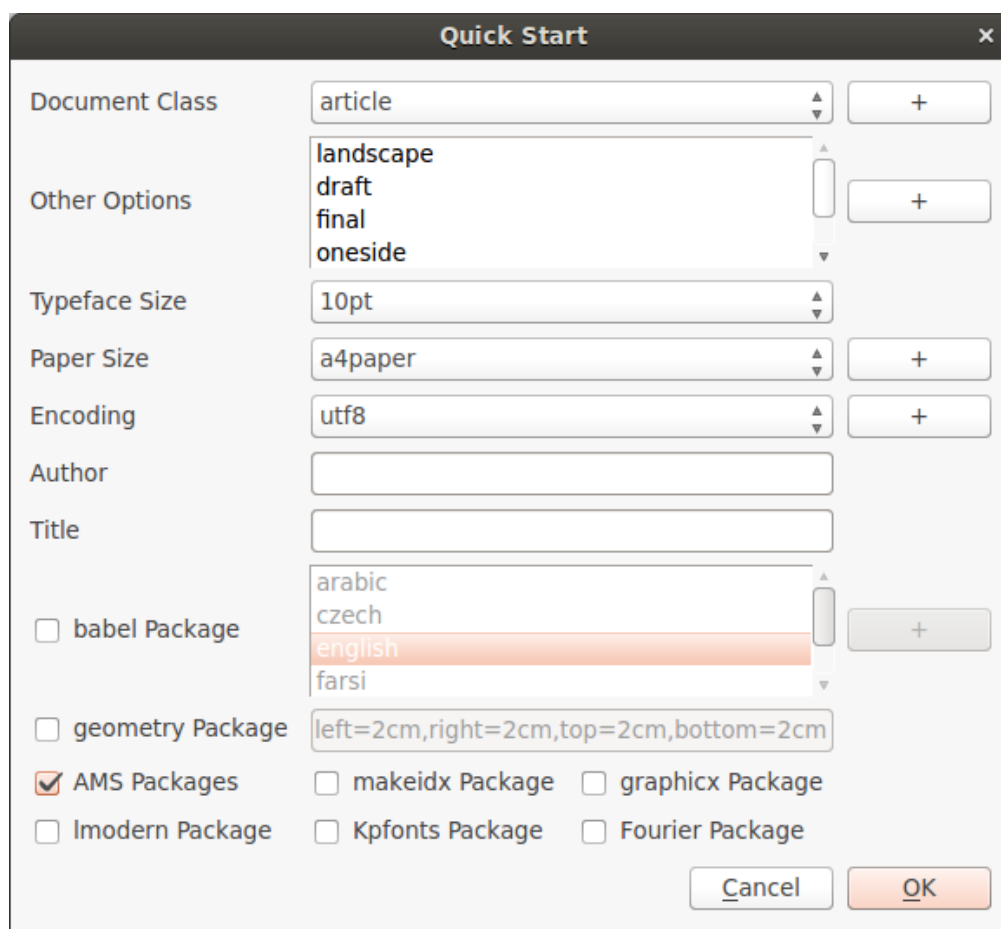


Рис. 3: Редактор TexMaker

сборка". Задать последовательность команд используемых быстрой сборкой можно в диалоге "Настроить Texmaker". Если в коде документа содержатся ошибки, Texmaker напишет об этом в окне сообщений.

### 1.2.3 Классы документов

Каждый созданный файл в  $\text{\LaTeX}$  начинается с команды `\documentclass[...]{...}`, в фигурных скобках которой задаются параметры оформления стиля документа, а в квадратных — список классовых опций.

Всего же в  $\text{\LaTeX}$  5 основных классов документов: `article` (для статей), `report` (для верстки небольших книг, статей, разбитых на главы), `book` (для верстки книг), `proc` (возможно использовать для докладов) и `letter` (для оформления деловых писем). Помимо этих основных, есть ещё множество дополнительных классов, таких как `beamer`.

### 1.2.4 Подключаемые пакеты

В  $\text{\LaTeX}$  можно применять специфические, отличные от изначальных, настройки (поля, списки и таблицы, библиографические ссылки и прочее). Для этого используются пакеты

расширений, подключаемые в "шапке" документа.

Пример:

```
\usepackage[russian]{babel} % Пакет поддержки русского языка
```

### 1.2.5 Вёрстка формул

Вёрстка формул не представляет никакой сложности.

Система дифференциальных уравнений Рёсслера

$$\begin{cases} \frac{dx}{dt} = -y - z \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = b + z(x - c) \end{cases};$$

Массив связанных осцилляторов Рёсслера:

$$\begin{aligned} \dot{x}_i &= -\omega_i y_i - z_i + k(2x_i - x_{i-1} - x_{i+1}), \\ \dot{y}_i &= \omega_i x_i - a y_i, \\ \dot{z}_i &= b + z_i(x_i - c), \end{aligned}$$

## 1.3 Выводы

Л<sup>A</sup>T<sub>E</sub>X наиболее популярный набор макрорасширений (или макропакет) системы компьютерной вёрстки T<sub>E</sub>X, который облегчает набор сложных документов.

Пакет позволяет автоматизировать многие задачи набора текста и подготовки статей, включая набор текста на нескольких языках, нумерацию разделов и формул, перекрёстные ссылки, размещение иллюстраций и таблиц на странице, ведение библиографии и др. Кроме базового набора существует множество пакетов расширения Л<sup>A</sup>T<sub>E</sub>X.

Термин Л<sup>A</sup>T<sub>E</sub>X относится только к языку разметки, он не является текстовым редактором. Для того, чтобы создать документ с его помощью, надо набрать .tex-файл с помощью какого-нибудь текстового редактора. В принципе, подойдёт любой редактор, но большая часть людей предпочитает использовать специализированные, которые так или иначе облегчают работу по набору текста Л<sup>A</sup>T<sub>E</sub>X-разметки.

Будучи распространяемым под лицензией LaTeX Project Public License, Л<sup>A</sup>T<sub>E</sub>X относится к свободному программному обеспечению.

## 2 Система контроля версий Git

### 2.1 Цель работы

Изучить систему контроля версий Git, освоить основные приёмы работы с ней.

### 2.2 Ход работы

- Получить содержимое репозитория

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

- Добавить новую папку и первого файла под контроль версий

```
cd InfoSecCourse2015/  
mkdir tmp  
cd tmp  
echo 1 >> file  
git add --all
```

- Зафиксировать изменения в локальном репозитории

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

- Внести изменения в файл и просмотреть различия

```
echo 2 >> file  
git diff master:./file ./file
```

- Отменить локальные изменения

```
git reset HEAD ./file  
git checkout ./file
```

- Внести изменения в файл и просмотреть различия

```
echo 3 >> file  
git diff master:./file ./file
```

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

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

- Получить изменения из центрального репозитория

```
git pull
```

- Поэкспериментировать с ветками

```
git branch -v
git checkout -b temp
git checkout master
git merge temp
git branch
git branch -D temp
git branch
```

## 2.3 Выводы

Git распределённая система управления версиями файлов. Git используется многими продуктами с открытым исходным кодом, такими как ядро Linux, Android, GNU Core Utilities, Mesa, Wine, Chromium и т.д. Программа является свободной и выпущена под лицензией GNU GPL версии 2.

Преимущества и недостатки git по сравнению с централизованными системами управления версиями (такими как, например, Subversion) типичны для любой распределённой системы. Если же сравнивать git с «родственными» ей распределёнными системами, можно отметить, что git изначально идеологически ориентирован на работу с изменениями, а не с файлами, «единицей обработки» для него является набор изменений, или патч. Эта особенность прослеживается как в структуре самой системы (в частности — в структуре репозитория), так и в принципах построения команд; она отражается на производительности системы в различных вариантах её использования и на достоинствах и недостатках git по сравнению с другими DVCS.

## 3 Создание электронных цифровых подписей с PGP

### 3.1 Цель работы

Научиться создавать сертификаты, шифровать файлы и ставить ЭЦП.

### 3.2 Ход работы

#### 3.2.1 Знакомство с пакетом Kleopatra

Kleopatra это графический интерфейс к GnuPG и предназначенных для работы под окружением KDE и портированный на MS Windows (доступные в составе пакета Gpg4win). Внешний вид пакета представлен на рисунке 4.

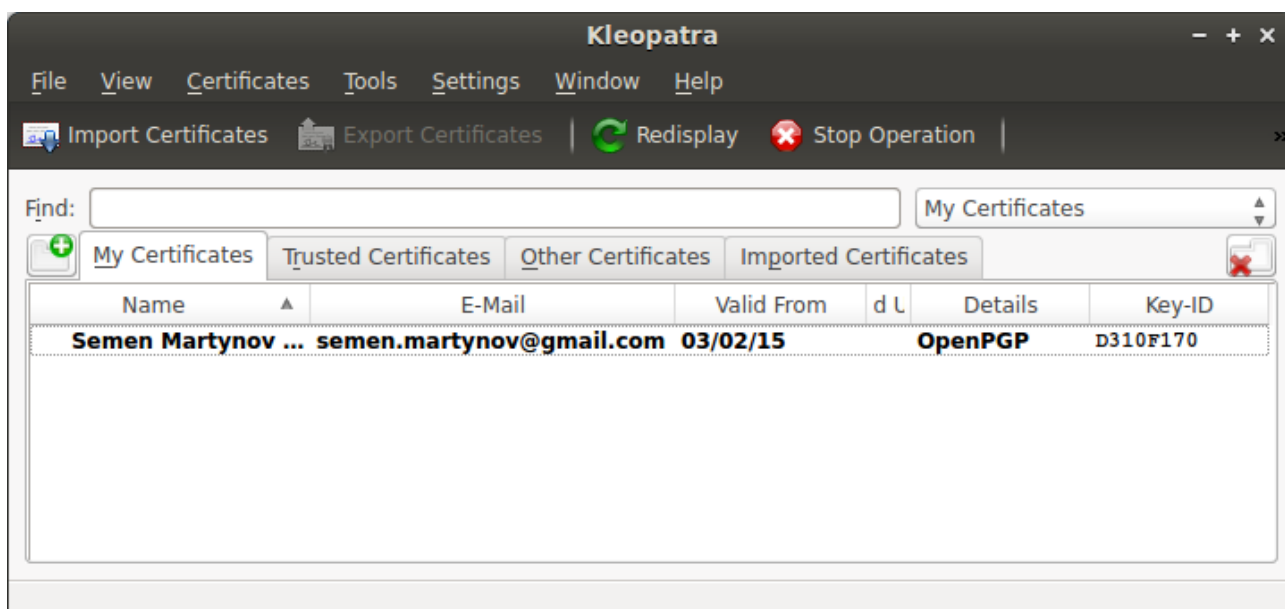


Рис. 4: Графический интерфейс Kleopatra

При помощи мастера, графический интерфейс позволяет создать сертификат. Его текстовый вид представлен в листинге 1.

Листинг 1: Сертификат в формате asc (ASCII Armored file)

```
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2 Version: GnuPG v2.0.22 (GNU/Linux)
3
4 mQENBFTzldMBCAD9K7AQha/SmP+XAtzh1qduhWGsVFewYrebHpuRev/GuLPZetYp
5 Ia6iH1a5Pm8Fc0/vWmP3hxWX+3RR4izWJ/JbdukLBME43bnE5FJc8f0o8PukAeop
6 CE1iJeWvGvEi6bbGkFSBxPzAMnjWAoQC60F0/a+A9Y91AzVTMwzKkrEey9U4zu2I
7 vkYVXJ1jdLt7xfDckah9BBGUwUDai0bq9noI2koThzRskKN0/BCKXbbLlBeAz82/
8 RGY1SSB5xi0e00Vejq9hJI0Nurnu/YyuLcw1rlQclKu8gosXTz4K2y5IYEdjhfdY
9 ZiG8X/lw9inB5rdJ1LMf3GaVE0vykgUMiYdNABEBAAGOPVNlbWVuIE1hcnR5bm92
```



```

10 IChJbmZvU2VjQ291cnNlMjAxNSkgPHNlbWVuLm1hcnR5bm92QGdtYWlsLmNvbT6J
11 ATkEEwECACMFA1TzldMCGw8HCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCK
12 aJF90xDxcAYtCACy0qh1ZsLWMnsMJedLEva8BqHd6YXsGho0B81lXDcL9DZaQ4eX
13 9IzNS38MgD7+GiRe1SoANi3niXg3fREx2eaHK+7dZQIOBB93HYveOC0brW2fB1CE
14 D4jFHGXd2KPZMk+LOXaXqZhabd/Bqs/WbhiIt5Ah4rKSVhxbAV4TWqmq10FtKOSf
15 PtzyQPkbpVShFoYsIwY4eoLFoR8kiK7/zQnN6/J+lm7TlVuHpoM1qrGNPsAJyIjJ
16 ELPeogdY421SG1RGc2UuoZT3egdY0YCUaCNk0E40tGo/qR07mEPpn1L0iTV77Nm
17 ZETTWQpsopJupOczGDgeVDzGB4vPHyZCoybM
18 =19tG
19 -----END PGP PUBLIC KEY BLOCK-----

```

Имея свой сертификат, можно подписать любой имеющийся документ. Цифровая подпись сохраняется в отдельный файл с расширением sig. Если зашифровать файл *rfc7169.txt*, то подпись будет сохранена в файле *rfc7169.txt.sig* (см. рис. 5).

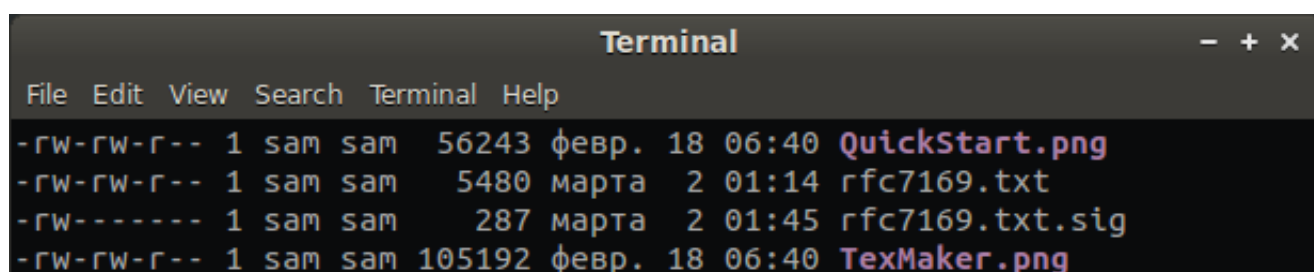


Рис. 5: Файл RFC7169 с подписью

Программа позволяет импортировать чужие сертификаты, и проверять подписи. На рисунке 6 показан итог импорта чужого файла.

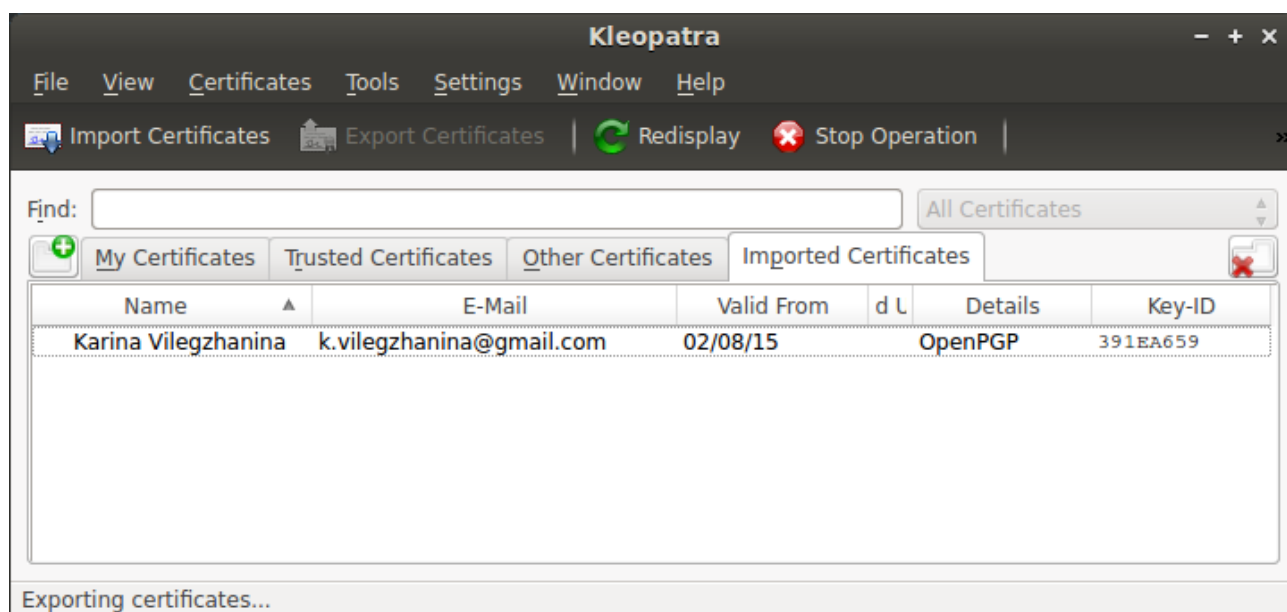


Рис. 6: Импорт чужого ключа в Kleopatra

Если подтвердить достоверность импортированного ключа, то его можно использовать для проверки чужой подписи. На рисунке 7 показана проверка файла *myfirst.pdf*.

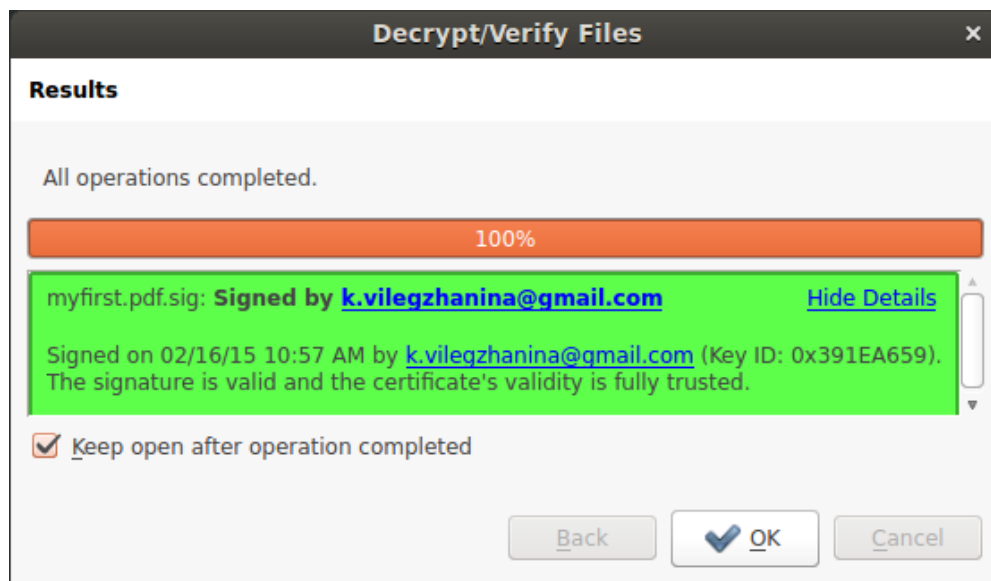


Рис. 7: Результат проверки файла *myfirst.pdf*

### 3.2.2 Использование `gpg` через интерфейс командной строки

Результат, полученный при помощи Kleopatra легко повторить используя терминал. Генерация ключа происходит в диалоговом режиме после ввода команды

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

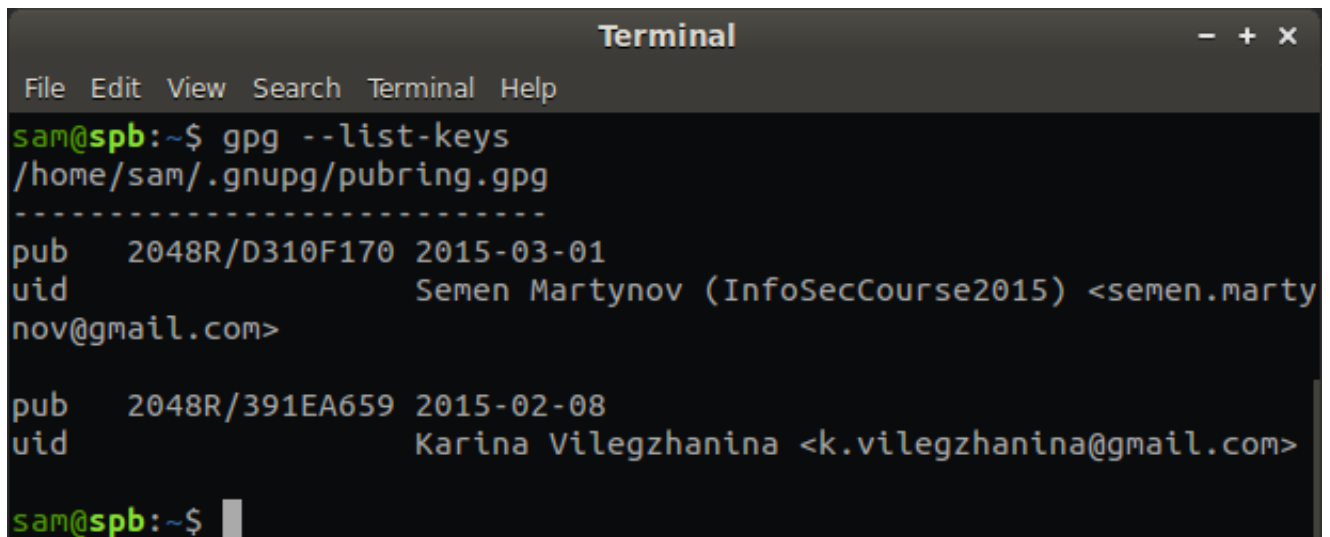
В процессе работы, мастер создания ключа запросит следующую информацию:

- Тип ключа (по умолчанию это DSA и ElGamal).
- Размер ключа (с DSA/ElGamal ключами не использую длину больше чем 2048).
- "срок годности" ключа.
- Информацию о пользователе (имя, электронный адрес).
- Пароль для ключа (если нужен).

В процессе генерации ключа, GnuPG использует энтропию. Для способствования её сбору рекомендуется активно двигать мышкой или запустить `mp3` в фоновом режиме.

Просмотреть доступные в системе ключи позволяет команда

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



```
Terminal
File Edit View Search Terminal Help
sam@spb:~$ gpg --list-keys
/home/sam/.gnupg/pubring.gpg
-----
pub      2048R/D310F170 2015-03-01
uid                               Semen Martynov (InfoSecCourse2015) <semen.marty
nov@gmail.com>

pub      2048R/391EA659 2015-02-08
uid                               Karina Vilegzhanina <k.vilegzhanina@gmail.com>

sam@spb:~$
```

Рис. 8: Список ключей в системе.

Её вывод показан на рисунке 7.

Для экспорта можно использовать команду (ключ определяется по электронному адресу)

```
gpg --armor --output john.asc --export john@mail.ru
```

Для импорта используется

```
gpg --import tomas.asc
```

### 3.3 Выводы

Пакет Kleopatra имеет большое количество зависимостей, среди которых akonadi-backend-mysql, akonadi-server, dirmngr, docbook-xml, docbook-xsl, gnupg-agent, gnupg2, gpgsm, icoutils, kate-data, katepart, kde-runtime, kde-runtime-data, kdelibs-bin, kdelibs5-data, kdelibs5-plugins, kdepim-runtime, kdepimlibs-kio-plugins, kdoctools, kleopatra, kubuntu-debug-installer, libaccounts-qt1, libakonadi-calendar4, libakonadi-contact4, libakonadi-kabc4, libakonadi-kcal4, libakonadi-kde4, libakonadi-kmime4, libakonadi-notes4, libakonadi-socialutils4, libakonadi-protocolinternals1, libattica0.4, libbaloo-core4, libbaloo-files4, libbaloo-pim4, libbaloo-xapian4, libboost-program-options1.54.0, libcalendarsupport4, libdirdirectories1, libdmtx0a, libepub0, libgpgme++2, libgrantlee-core0, libgrantlee-gui0, libincidenceeditorsng4, libkabc4, libkactivities-bin, libkactivities-models1, libkactivities6, libkalarmcal2, libkatepartinterfaces4, libkcal4, libkcal-core4, libkcalutils4, libkcmutils4, libkde3support4, libkdeclarative5, libkdecore5, libkdepim4, libkdepimdbusinterfaces4, libkdesu5, libkdeui5, libkdewebkit5, libkdgantt2-0, libkdnssd4, libkemoticons4, libkfbapi1, libkfile4, libkgapi2-2, libkholdd4, libkhtml5, libkidletime4, libkimap4, libkio5, libkjsapi4, libkjsembed4, libkldap4, libkleo4, libkmbox4, libkmediaplayer4, libkmime4, libknewstuff3-4, libknotifyconfig4, libkntlm4, libkolab0, libkolabxml1, libkparts4, libkpgp4, libkpimidentities4, libkpimtextedit4, libkpimutils4,

libkprintutils4, libkpty4, libkresources4, libkrosscore4, libksba8, libktexteditor4, libktnef4, libkubuntu0, libkxmlrpcclient4, libmailcommon4, libmailimporter4, libmailtransport4, libmessagecomposer4, libmessagecore4, libmessageviewer4, libmicroblog4, libmysqlclient18, libnepomuk4, libnepomukcleaner4, libnepomukcore4abi1, libnepomukquery4a, libnepomukutils4, libntrack-qt4-1, libntrack0, libphonon4, libpimcommon4, libplasma3, libpolkit-qt-1-1, libprison0, libpth20, libqapt2, libqapt2-runtime, libqca2, libqgpgme1, libqjson0, libqmobipocket1, libqrencode3, libqt4-qt3support, libqt4-sql-mysql, libsendlater4, libsignon-qt1, libsolid4, libsoprano4, libstreamanalyzer0, libstreams0, libtemplateparser4, libthreadweaver4, libvirtodbc0, libxerces-c3.1, libxml2-utils, libzip2, mysql-client-core-5.5, mysql-server-core-5.5, nepomuk-core-data, nepomuk-core-runtime, ntrack-module-libnl-0, odbcinst, odbcinst1debian2, oxygen-icon-theme, phonon, phonon-backend-gstreamer, phonon-backend-gstreamer-common, phonon-backend-gstreamer1.0, pinentry-gtk2, pinentry-qt4, plasma-scriptengine-javascript, qapt-batch, sddaemon, sgml-data, shared-desktop-ontologies, soprano-daemon, ttf-dejavu-core, virtuoso-minimal, virtuoso-opensource-6.1-bin, virtuoso-opensource-6.1-common. В общей сложности, эти пакеты требуют порядка 300 мегабайт, что делает использование интерфейса командной строки более предпочтительным вариантом.