

**Тема:** Применение криптографии и электронной цифровой подписи.

**Цель:** Знакомство с средствами криптографической защиты и электронной цифровой подписи, приобретение практических навыков использования на примере системы GnuPG.

**Варианты заданий:**

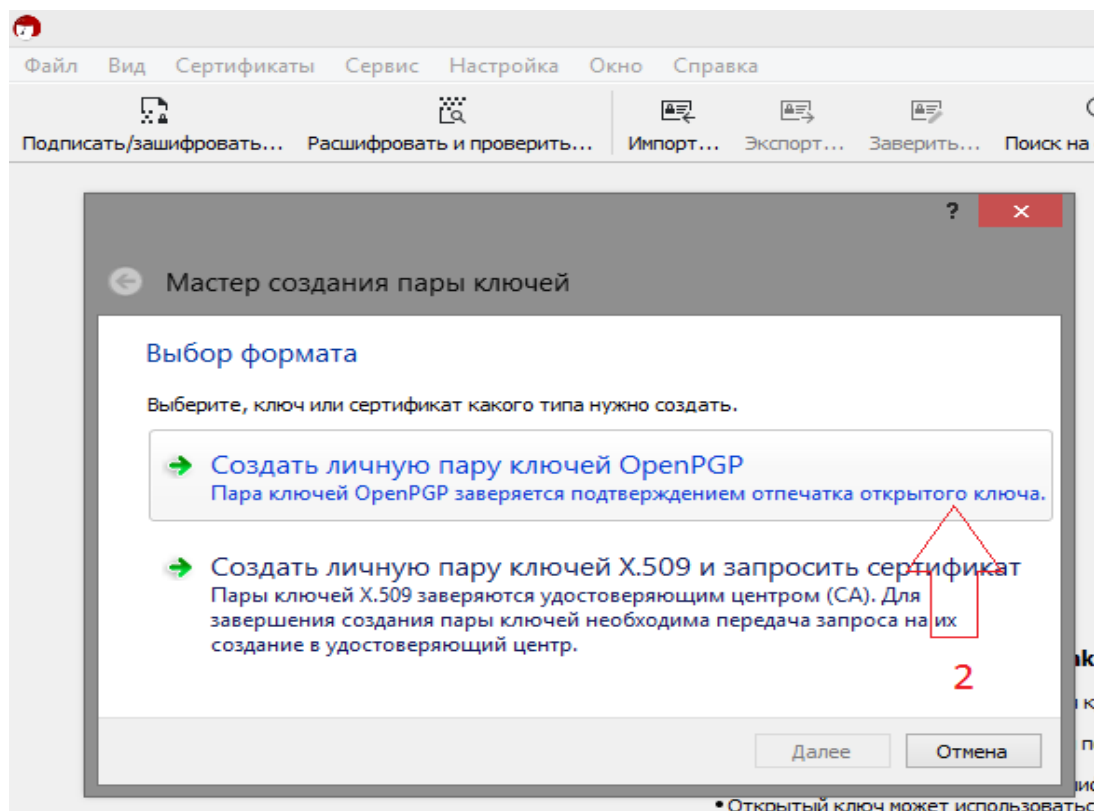
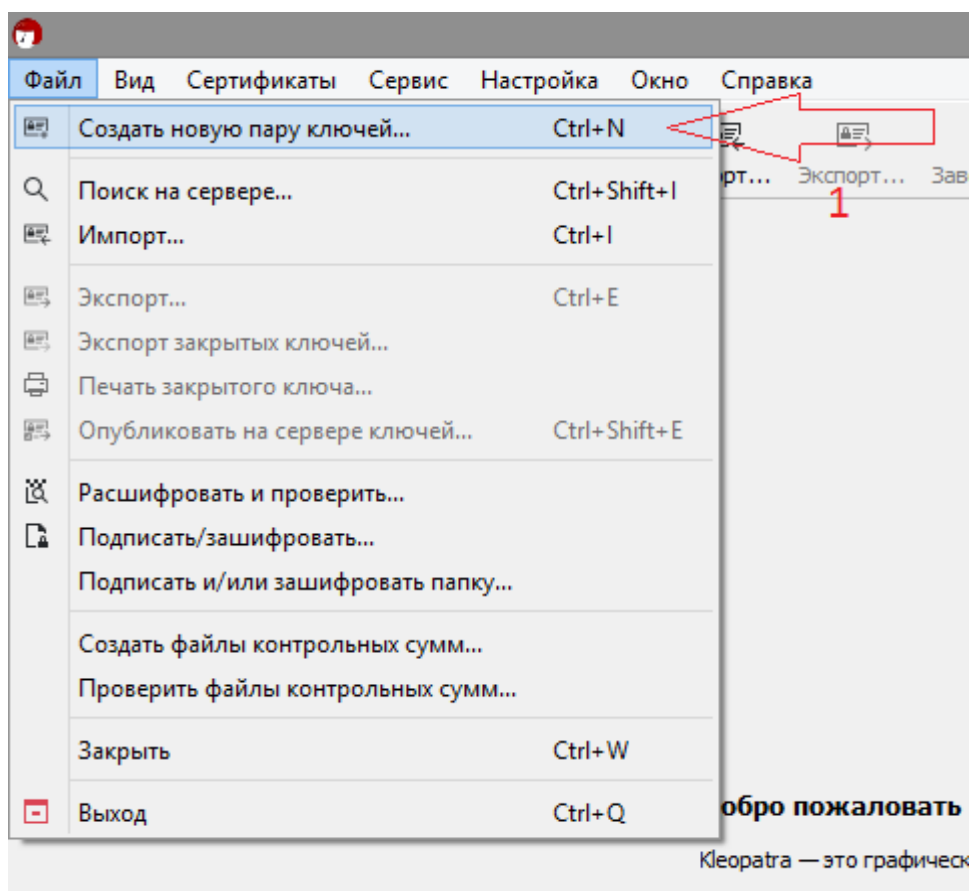
Вариант	Характеристика пары ключей			Хэш алгоритм	Содержание текста для шифрования
	RSA	RSA+	Действителен		
1	2048	2048	1 месяц	sha256	Вариант_1_sha256_RSA+
2	2048	3072	2 месяца	sha1	Вариант_2_sha1_RSA+
3	2048	4096	3 месяца	md5	Вариант_3_md5_RSA+
4	3072	-	4 месяца	sha256	Вариант_4_sha256_RSA
5	3072	3072	5 месяцев	sha1	Вариант_5_sha1_RSA+
6	3072	4096	6 месяцев	md5	Вариант_6_md5_RSA+
7	4096	2048	7 месяцев	sha256	Вариант_7_sha256_RSA+
8	4096	-	8 месяцев	sha1	Вариант_8_sha1_RSA
9	4096	4096	9 месяцев	md5	Вариант_9_md5_RSA+
10	2048	-	10 месяцев	sha256	Вариант_10_sha256_RSA
11	3072	2048	11 месяцев	sha1	Вариант_11_sha1_RSA+
12	4096	-	1 год	md5	Вариант_12_md5_RSA
13	2048	3072	1 год 4 месяца	sha256	Вариант_13_sha256_RSA+
14	3072	3072	10 дней	sha1	Вариант_14_sha1_RSA+
15	4096	3072	15 дней	md5	Вариант_15_md5_RSA+
16	2048	4096	25 дней	sha256	Вариант_16_sha256_RSA+
17	3072	-	1 год 3 месяца	sha1	Вариант_17_sha1_RSA
18	4096	4096	2 года	md5	Вариант_18_md5_RSA+
19	4096	3072	5 месяцев	sha256	Вариант_19_sha256_RSA+
20	4096	4096	6 месяцев	sha1	Вариант_20_sha1_RSA+
21	2048	2048	7 месяцев	md5	Вариант_21_md5_RSA+
22	3072	-	2 месяца	sha256	Вариант_22_sha256_RSA
23	4096	2048	3 месяца	sha1	Вариант_23_sha1_RSA+
24	2048	3072	4 месяца	md5	Вариант_24_md5_RSA+
25	3072	3072	3 года	sha256	Вариант_25_sha256_RSA+

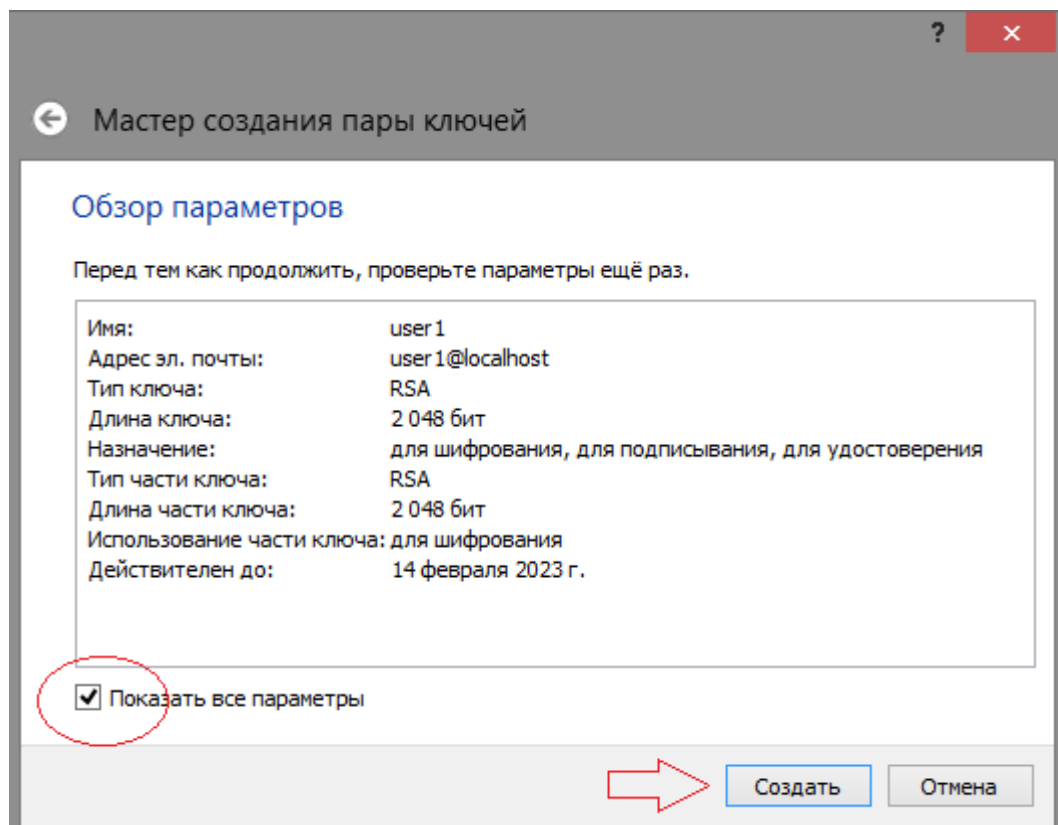
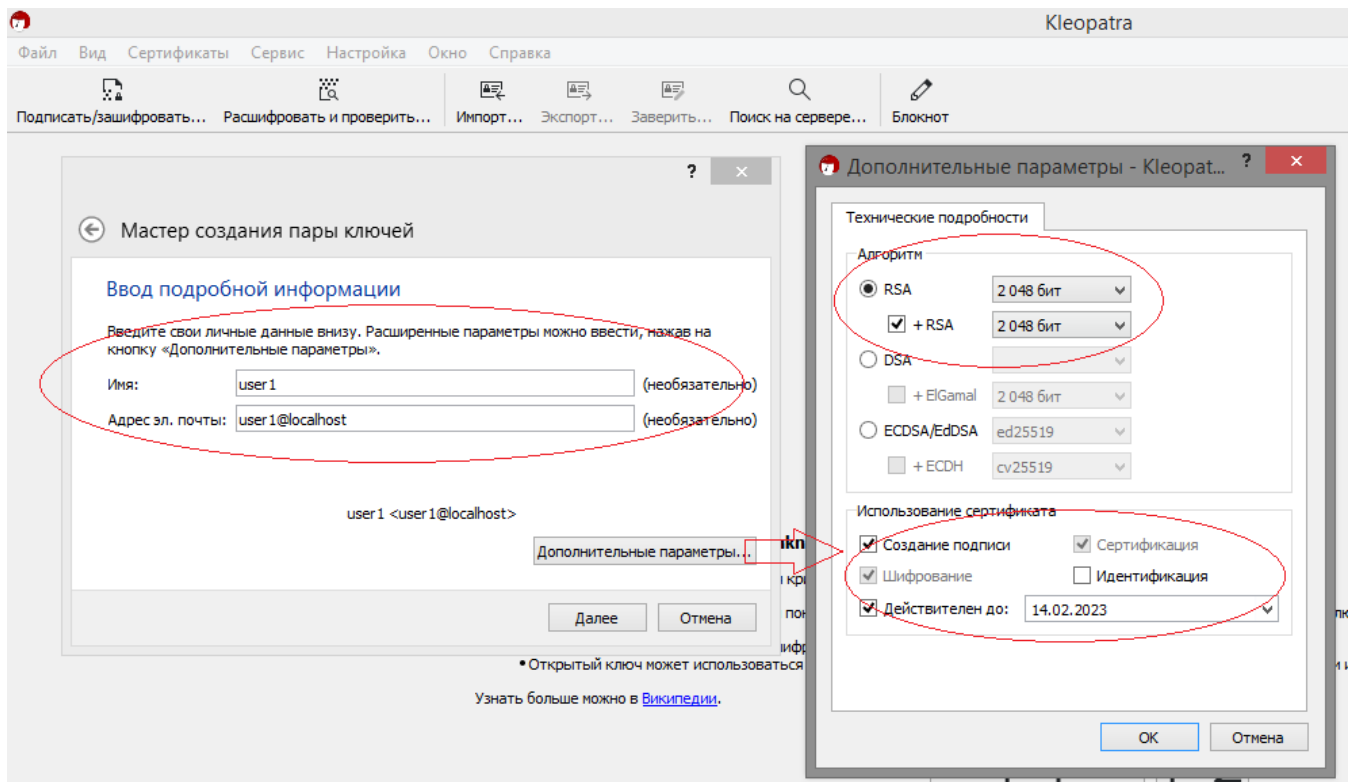
**Примечание:**

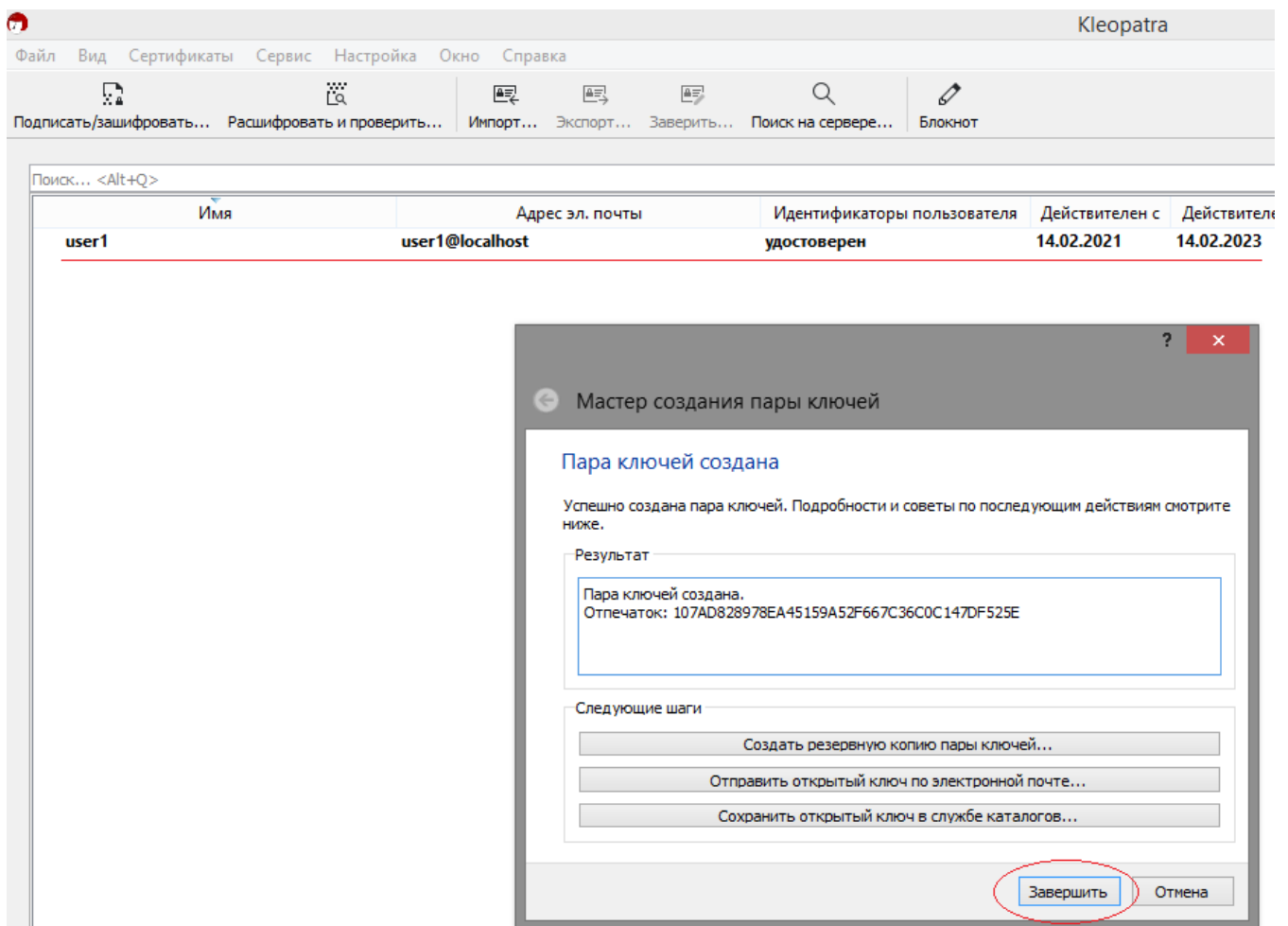
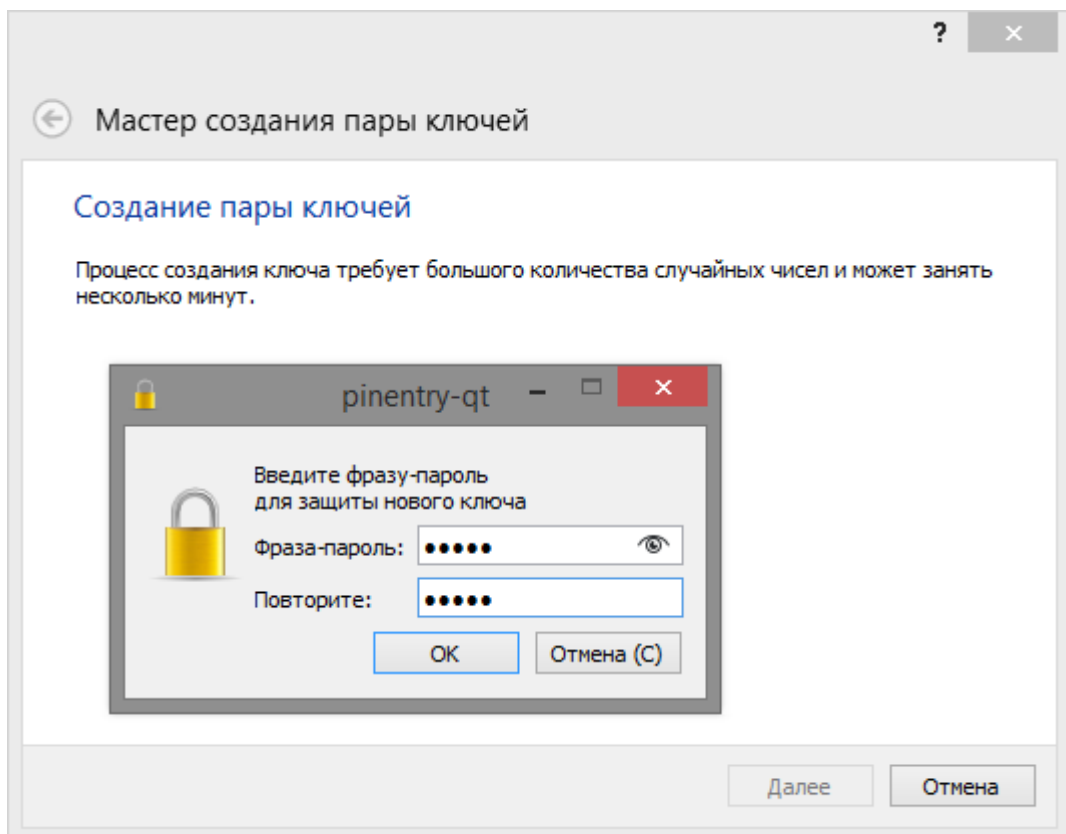
Если в варианте отсутствует внутренний (вложенный) ключ шифрования RSA+, то шифрование должно осуществляться при помощи основного ключа RSA.

## Порядок выполнения лабораторной работы:

1. Создать пару ключей в менеджере ключей Kleopatra (в соответствии с вариантом задания).





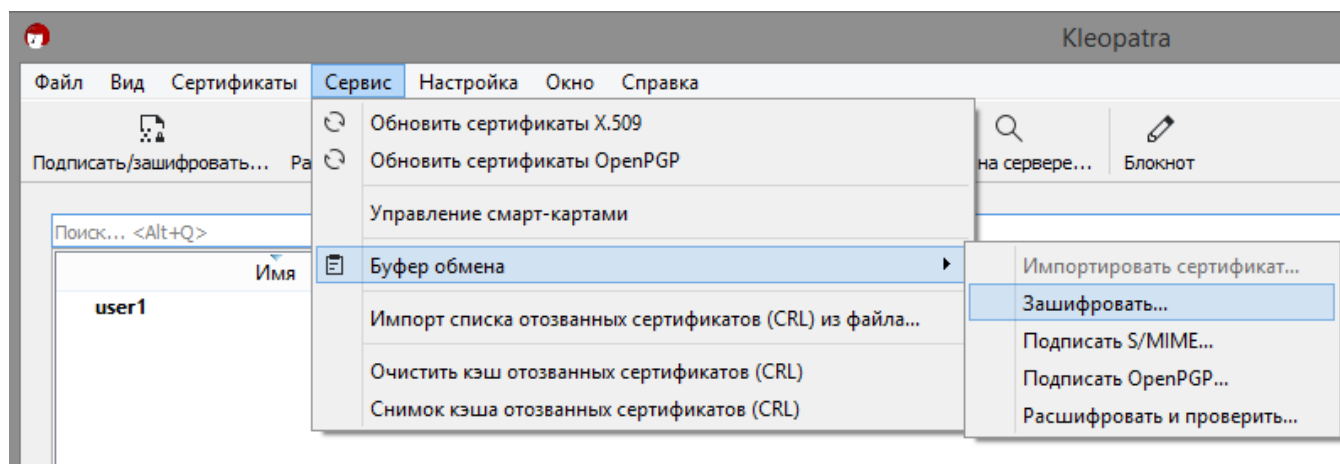
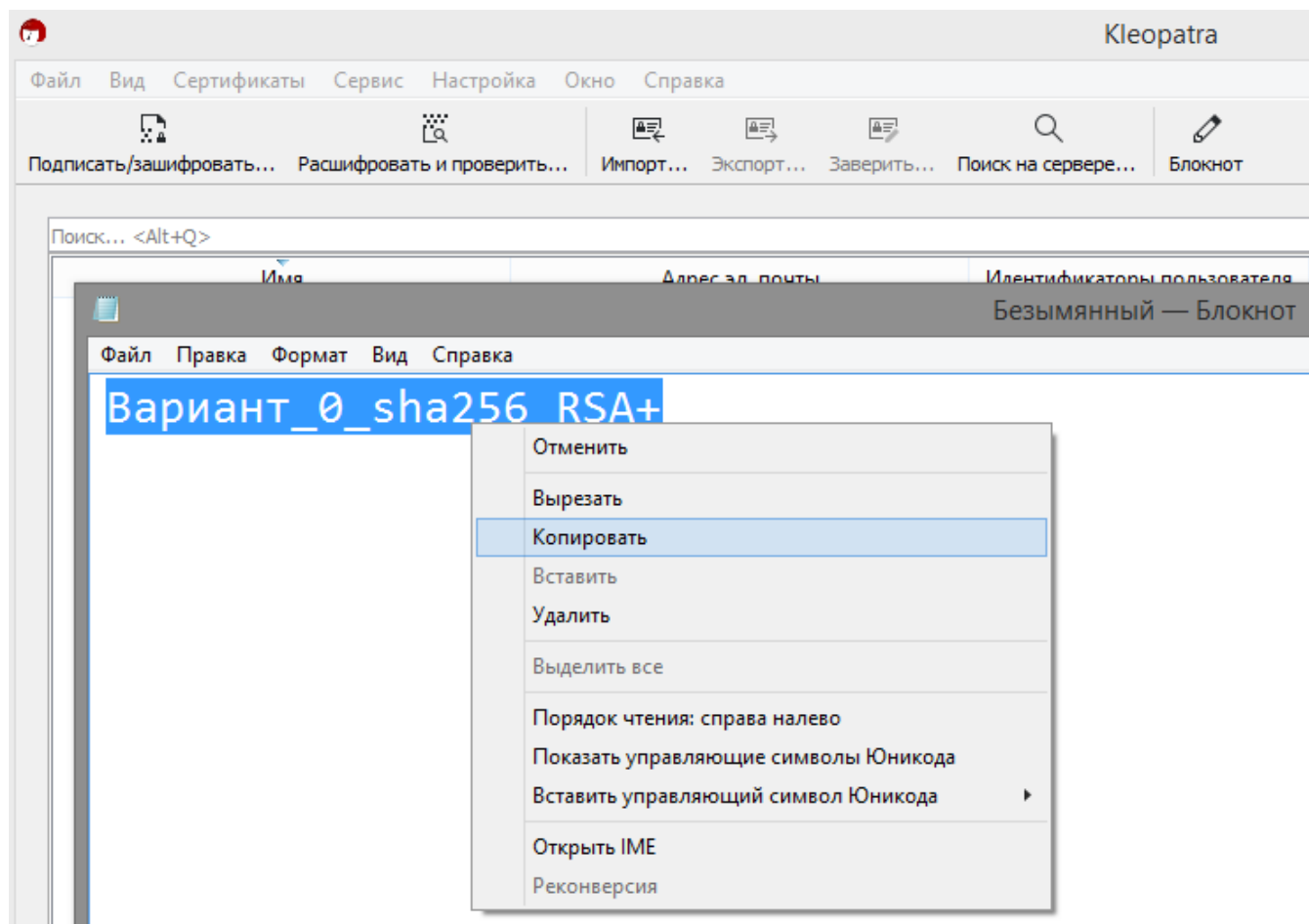


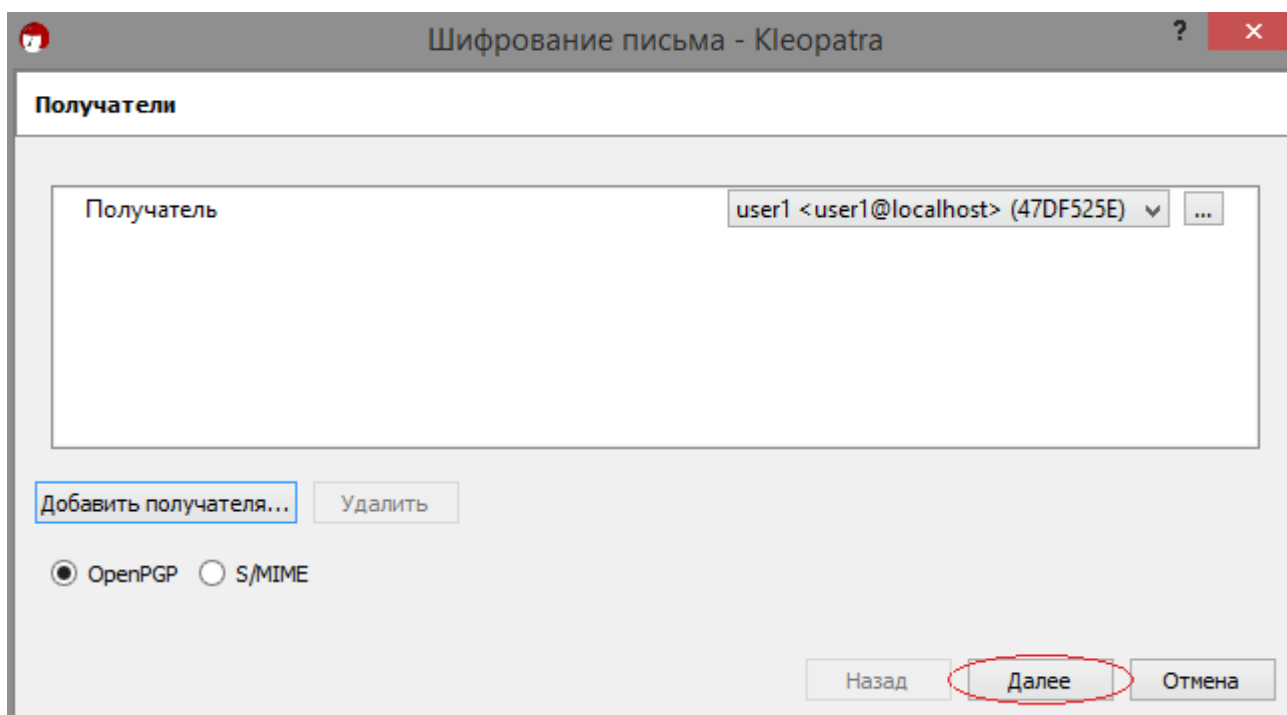
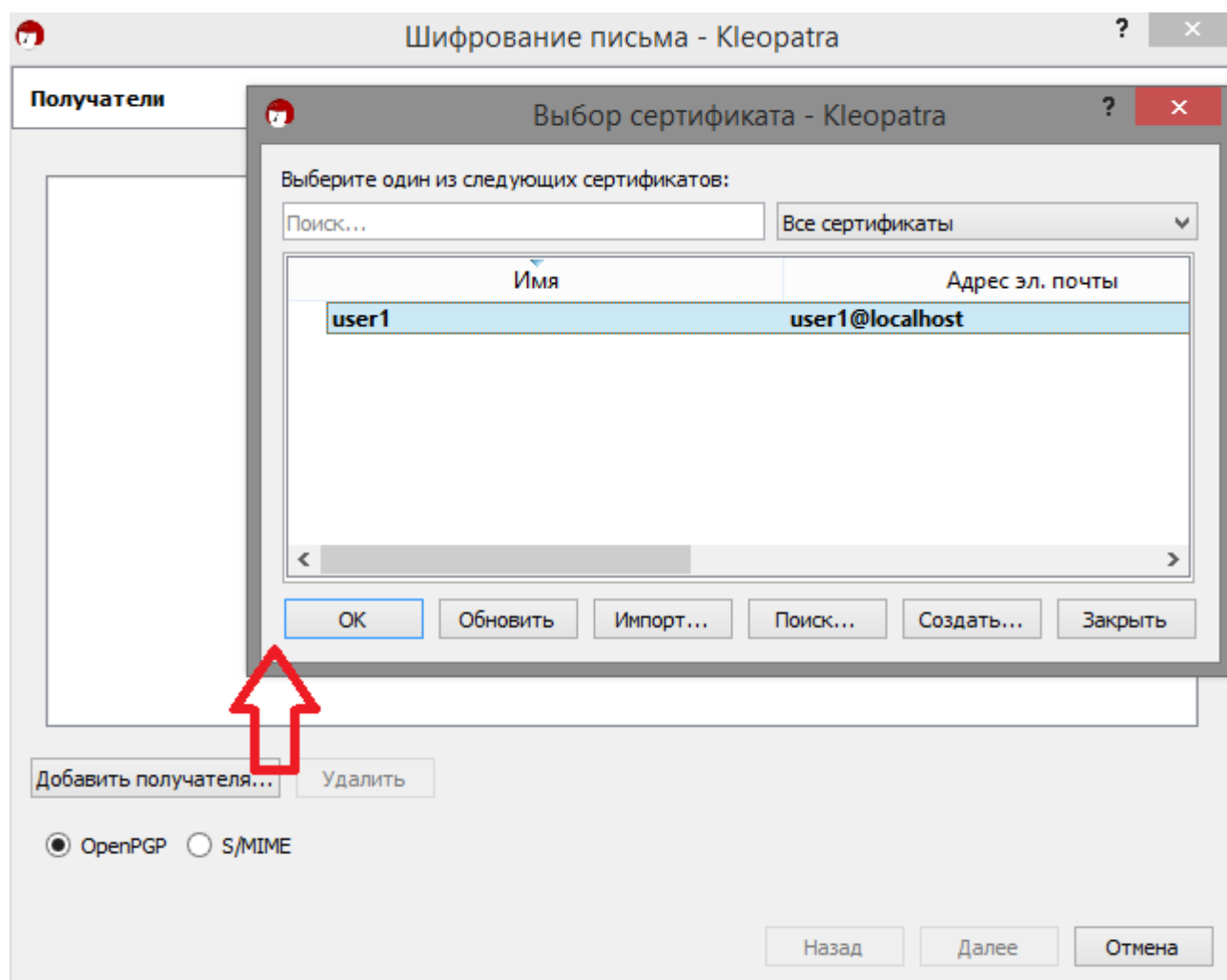
2. Протестировать процесс оперативного шифрования.

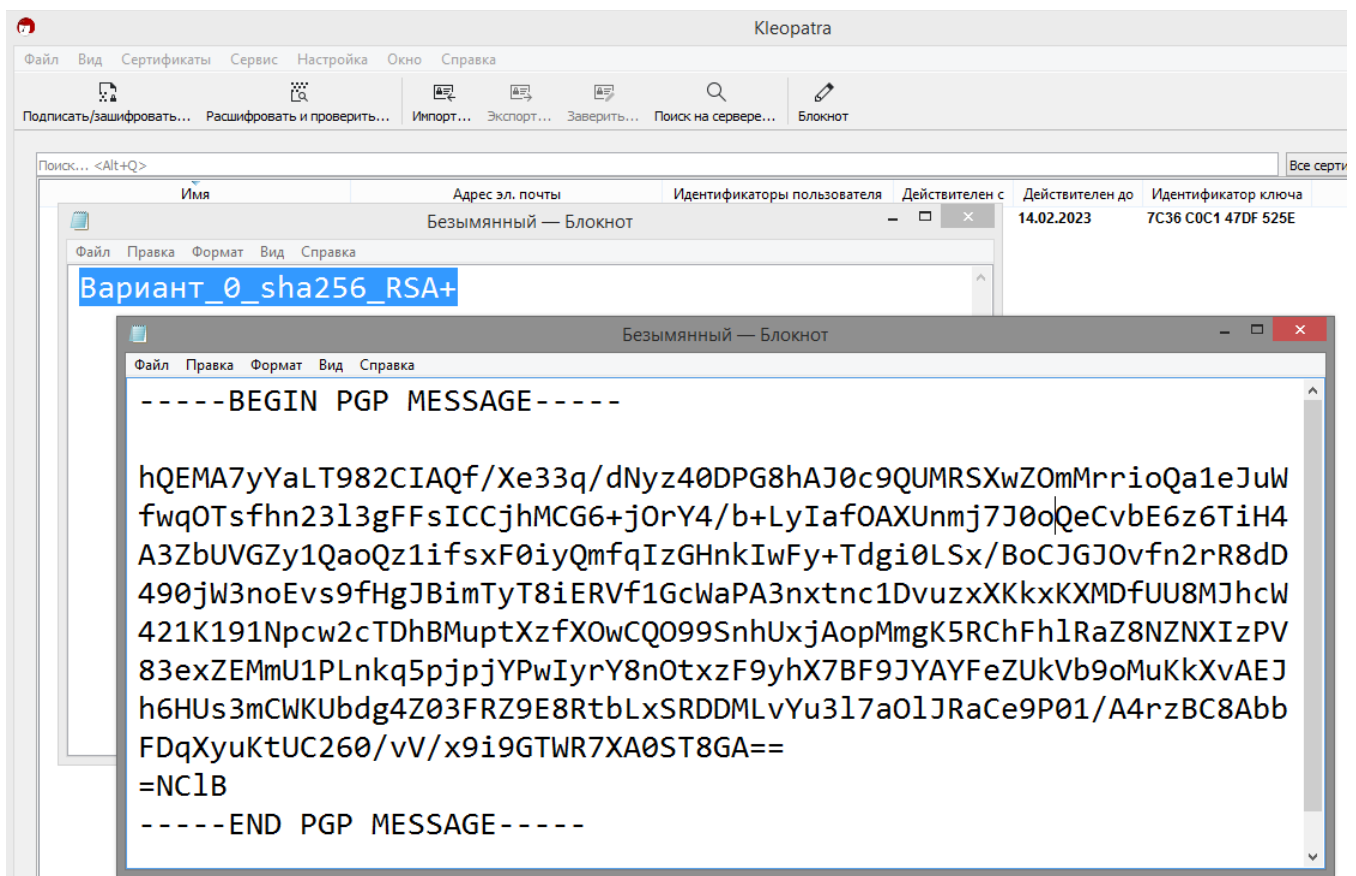
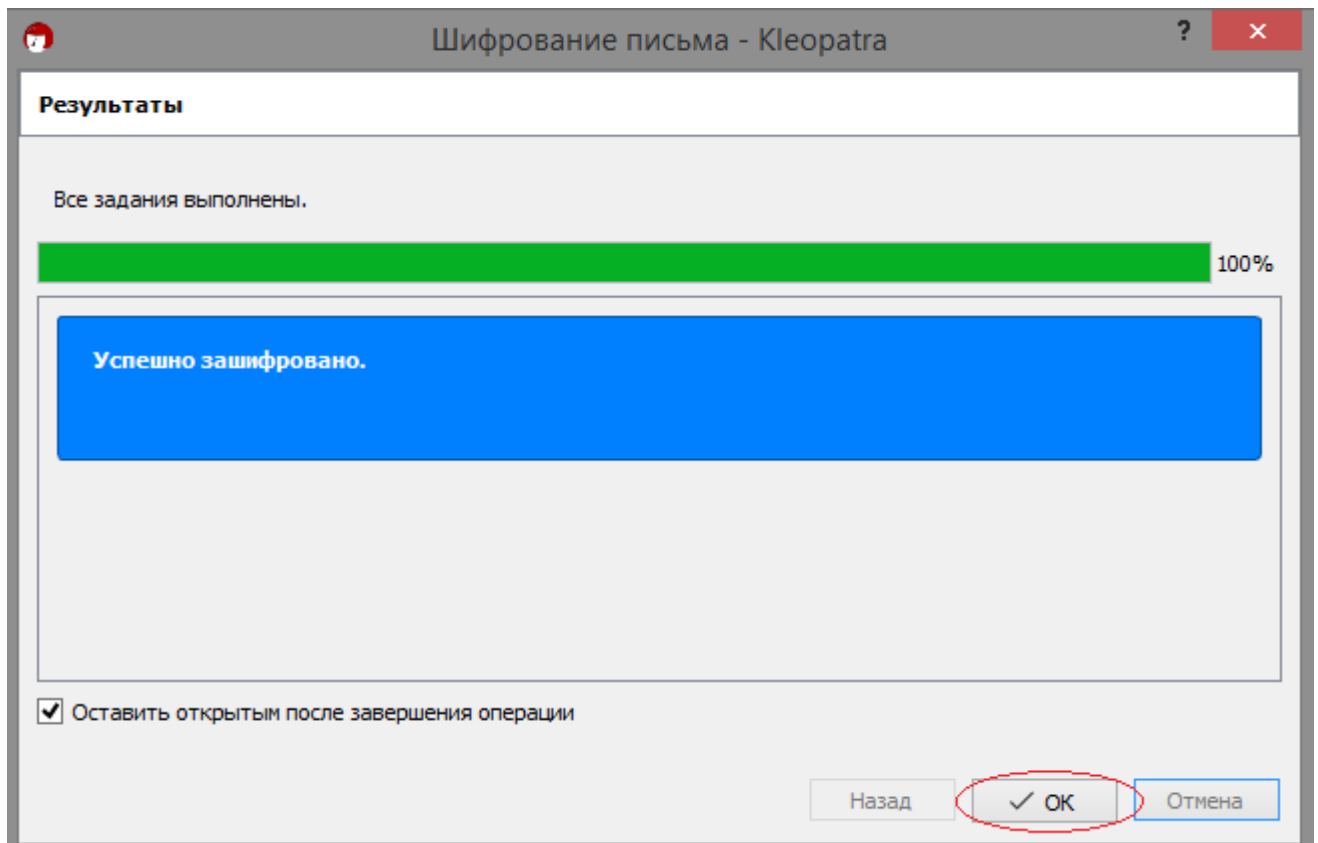
2.1. Скопировать текст для шифрования (в соответствии с вариантом) в буфер обмена и зашифровать его содержимое с помощью созданного открытого ключа. Вставить содержимое буфера обмена в текстовый редактор "Блокнот" и убедиться, что текст зашифрован.

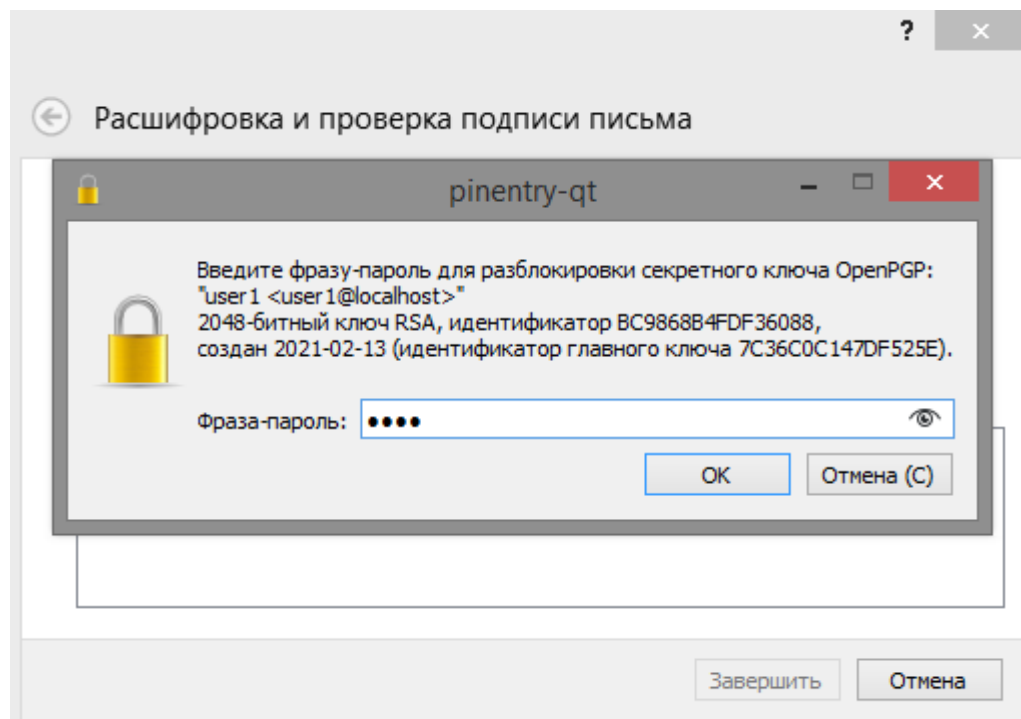
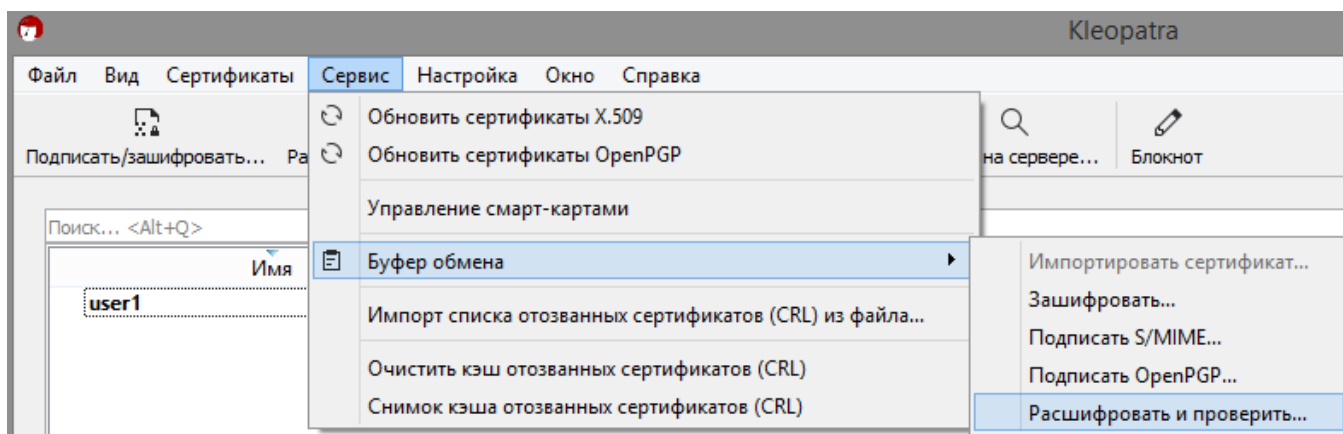
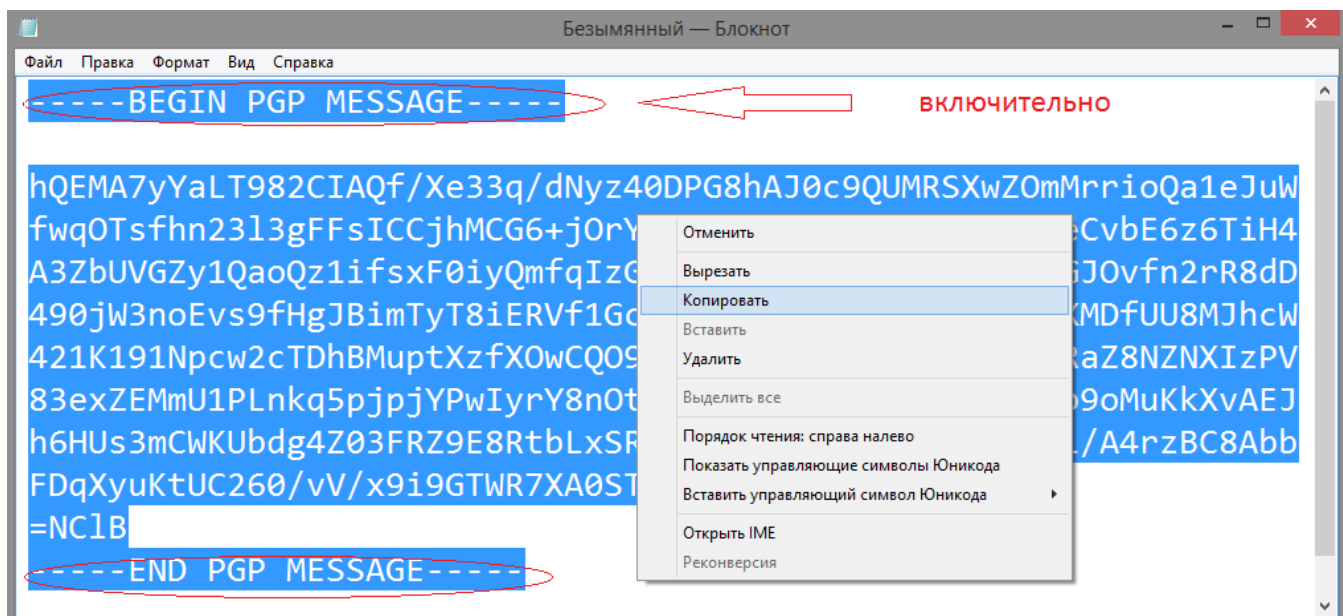
2.2. Провести действия по расшифровке содержимого буфера обмена (аналогично п. 2.2).

2.3. Повторить действия п.п. 2.1, 2.2 с помощью встроенного сервиса менеджера ключей Kleopatra "Блокнот".

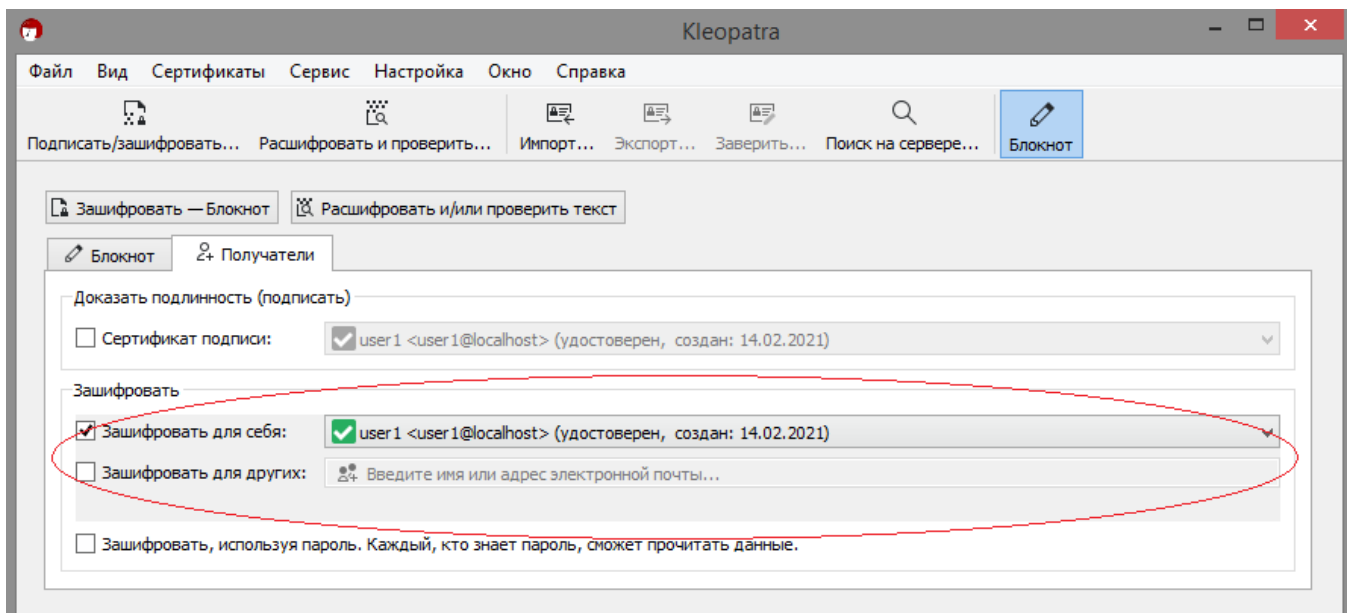
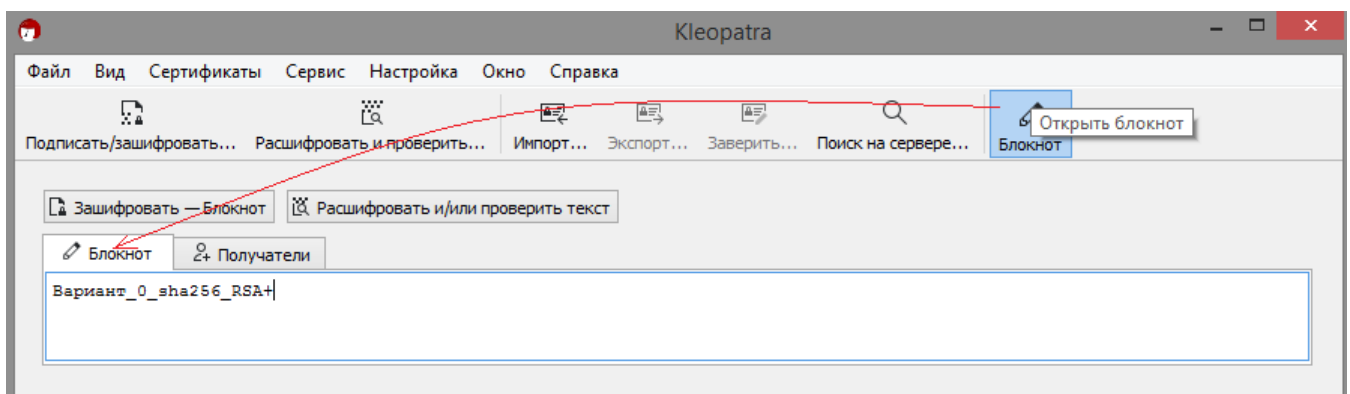
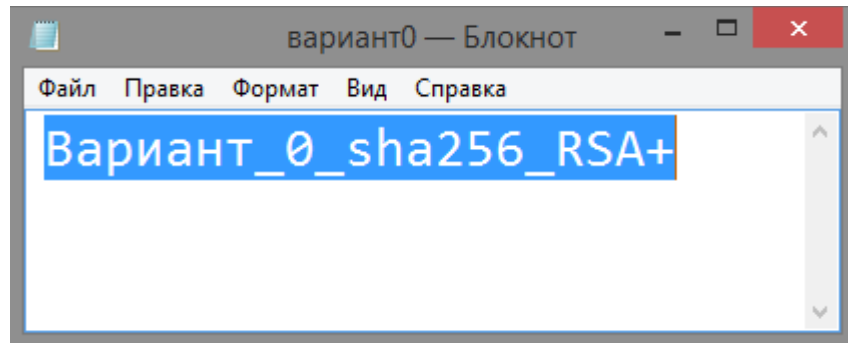


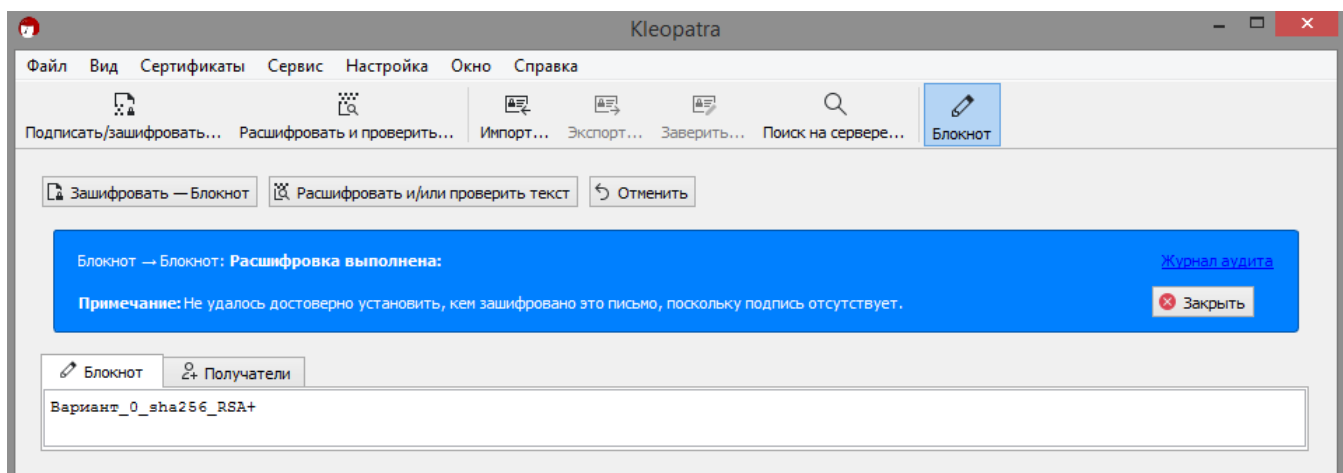
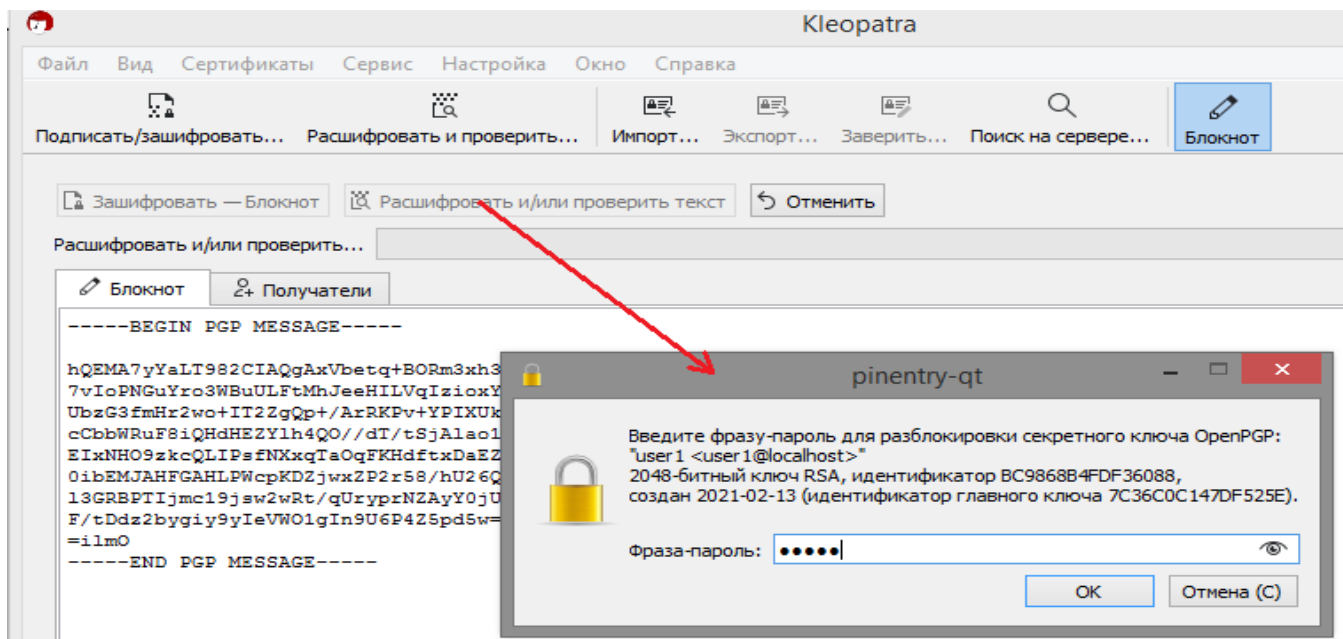
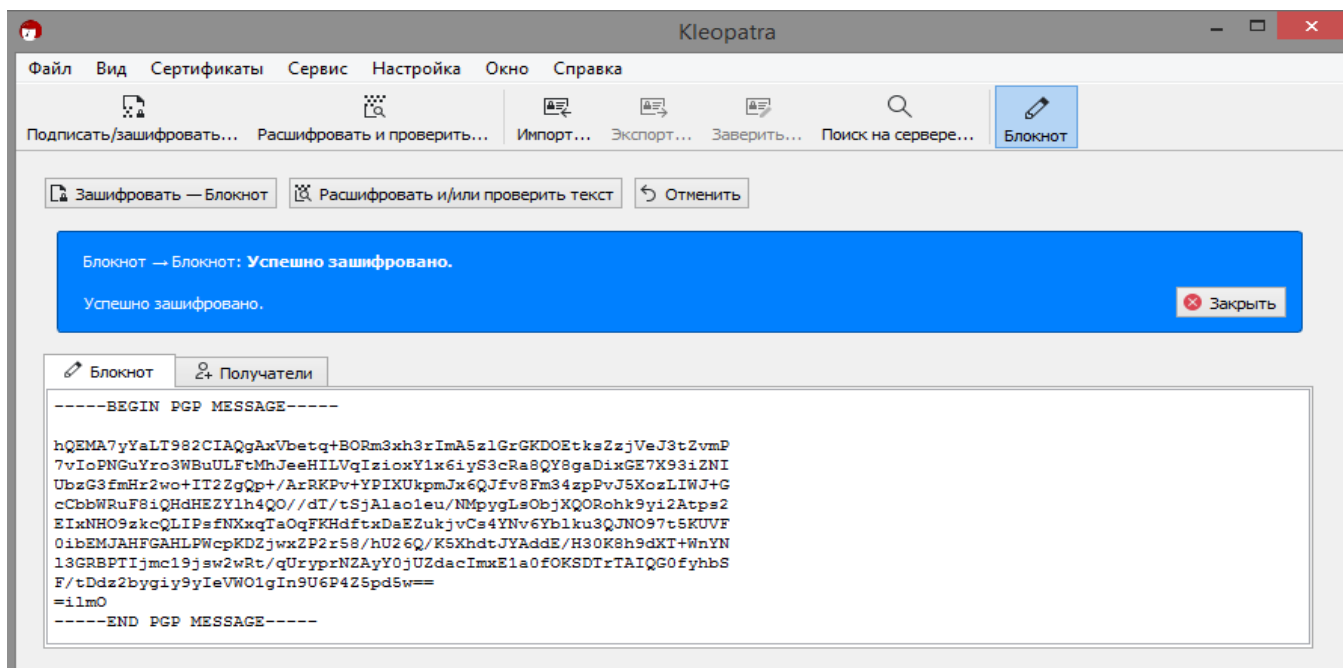










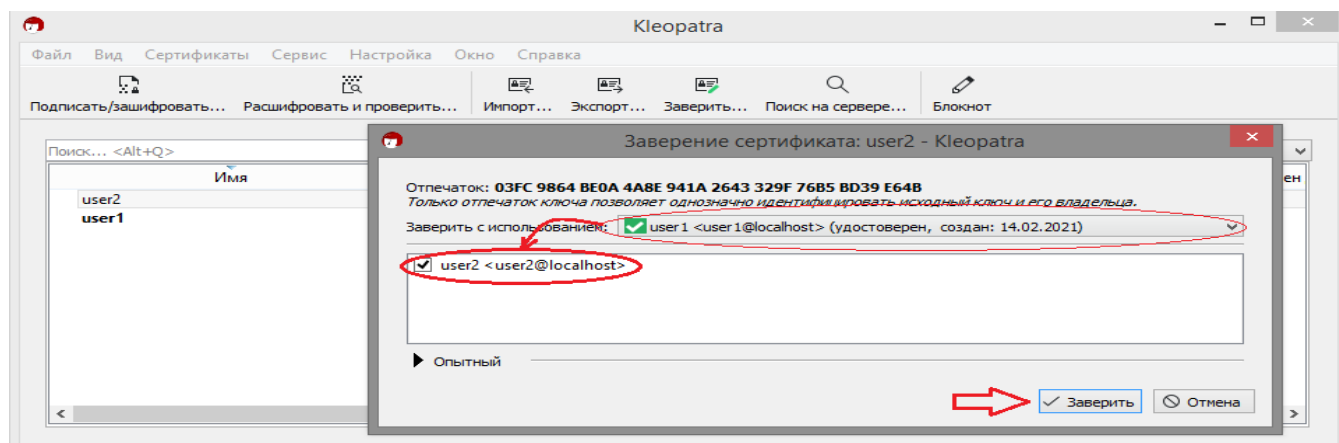
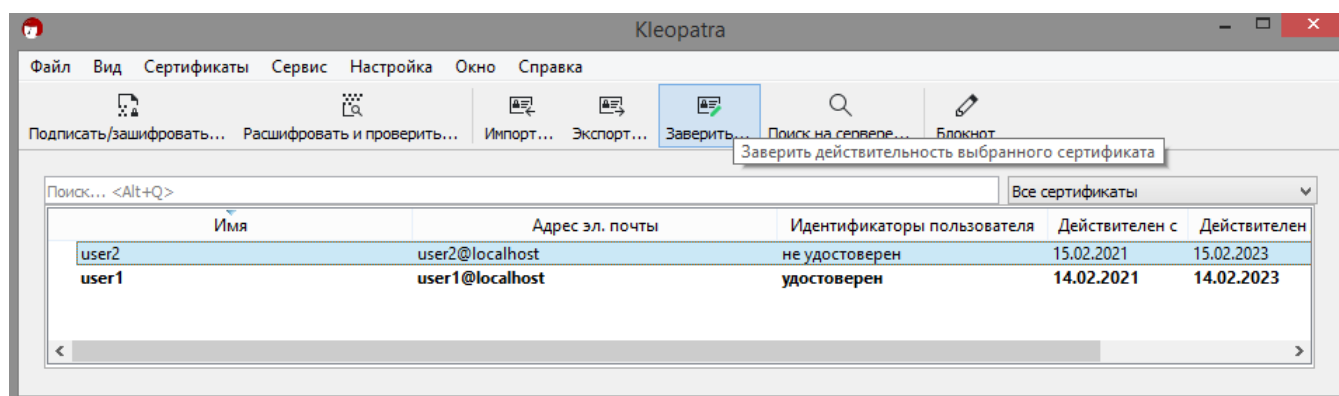
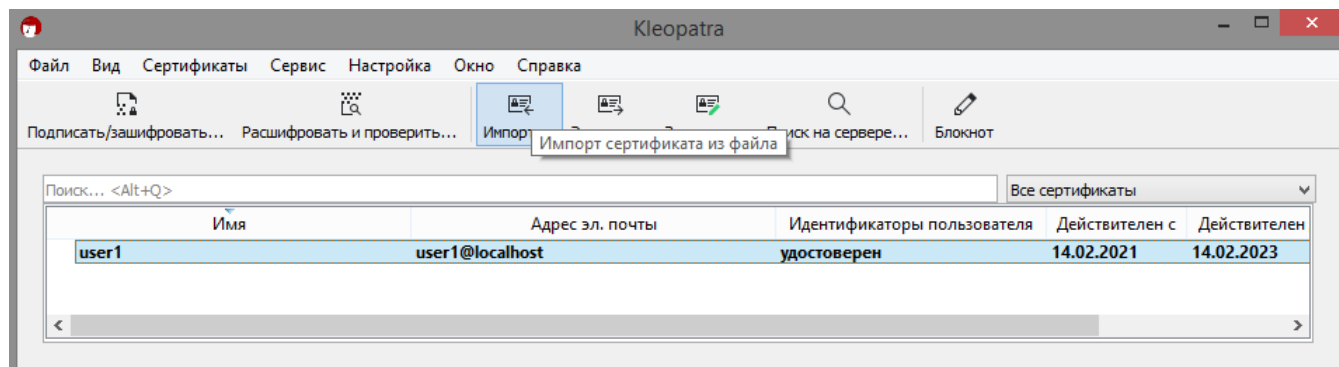
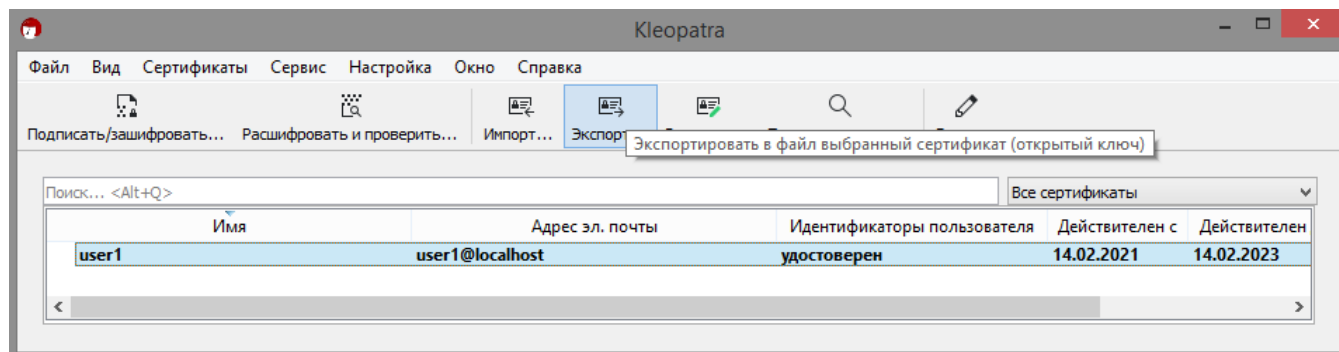


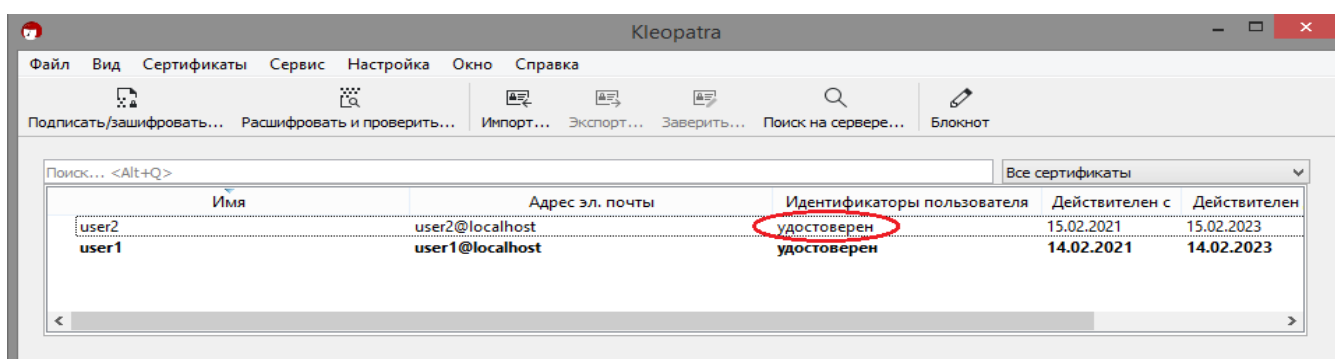
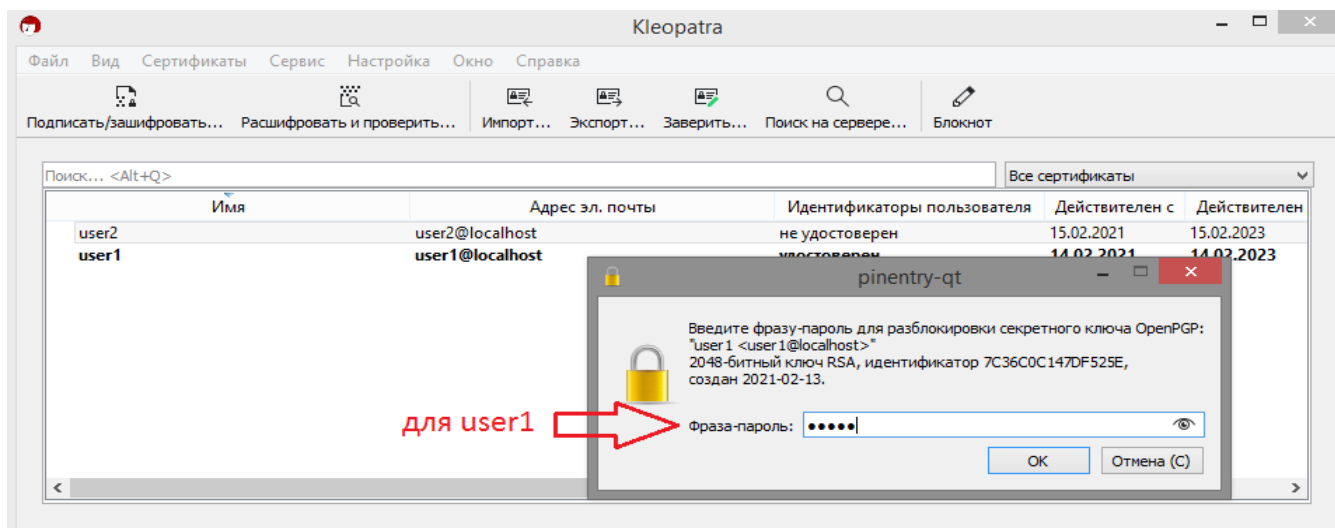
### 3. Протестировать процесс обмена ключами.

3.1. Экспортировать сертификат открытого ключа из пары созданных ключей в файл и переслать его напарнику (по электронной почте, через файловый обменник, на сменном носителе и т.п.).

3.2. Получив сертификат открытого ключа от напарника, импортировать полученный открытый ключ его в свой менеджер ключей и установите для импортированного ключа полное доверие.

3.3. Заверить полученный от напарника сертификат.



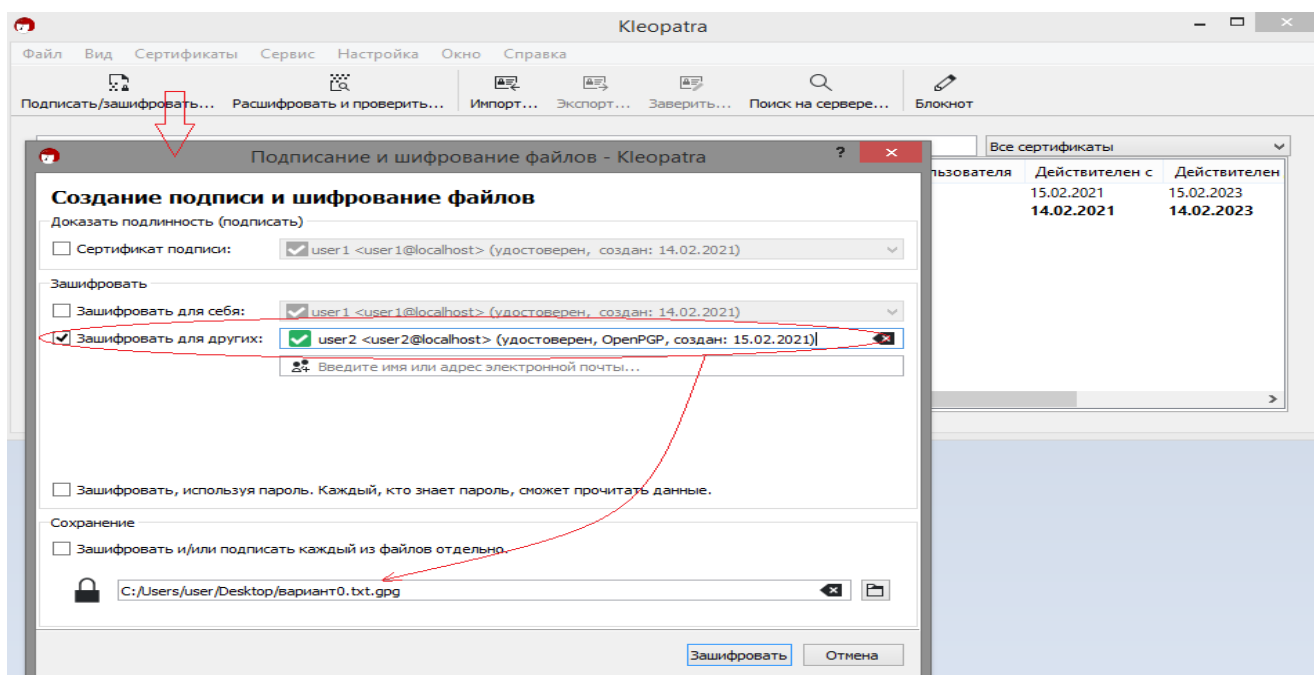


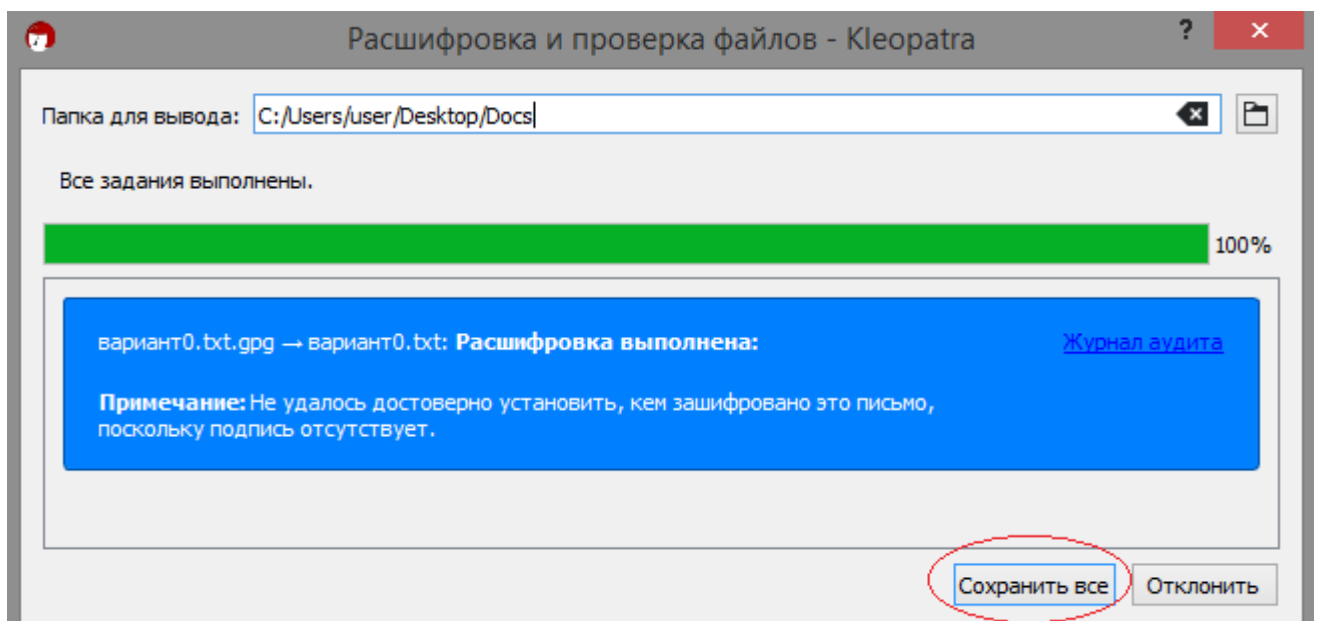
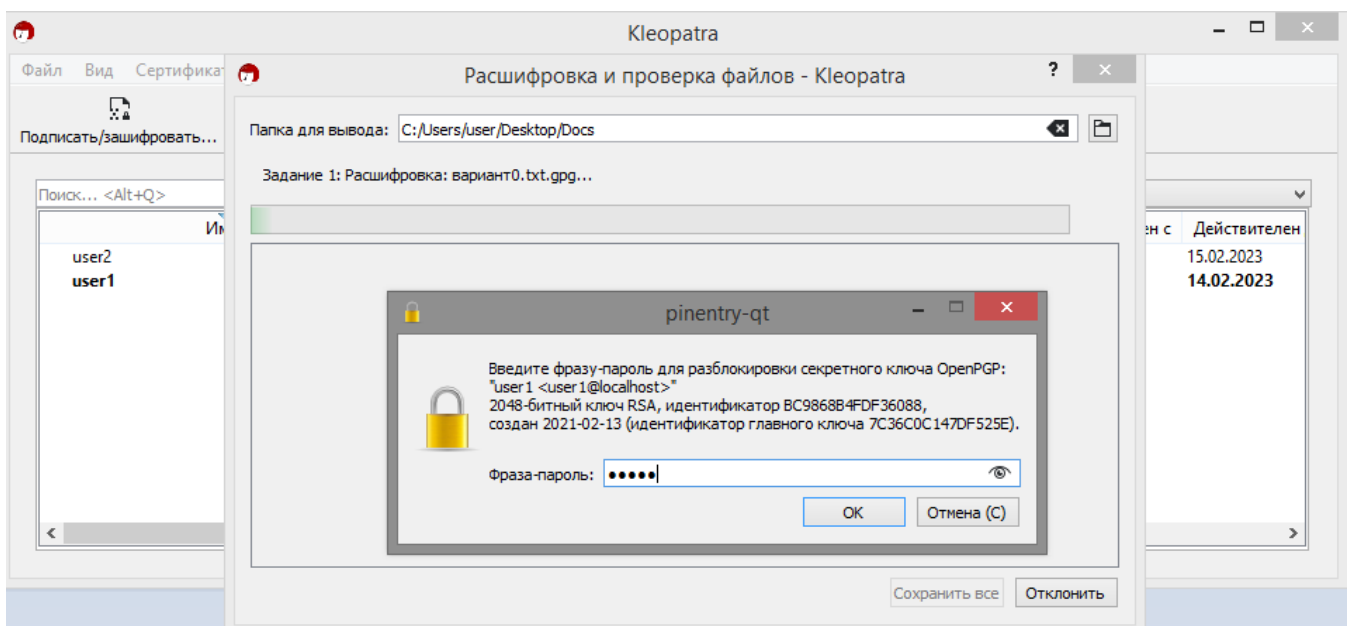
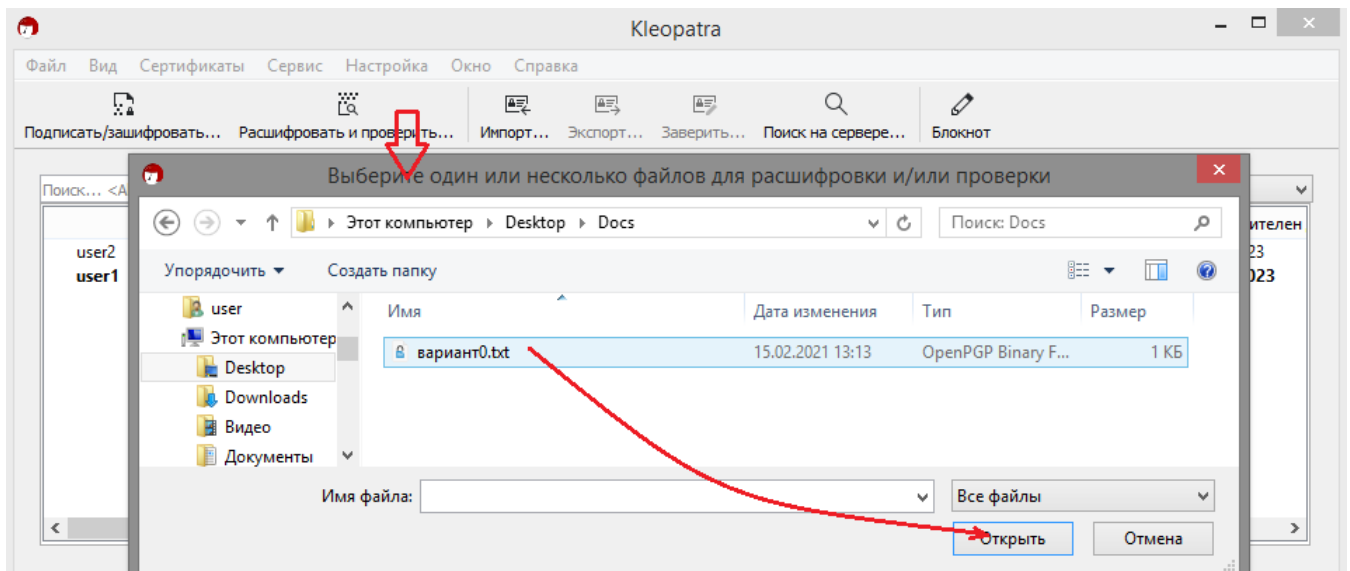
#### 4. Протестировать процесс асимметричного шифрования.

4.1. Создать с помощью тестового редактора "Блокнот" текстовый файл (.txt), содержащий текст в соответствии с вариантом задания.

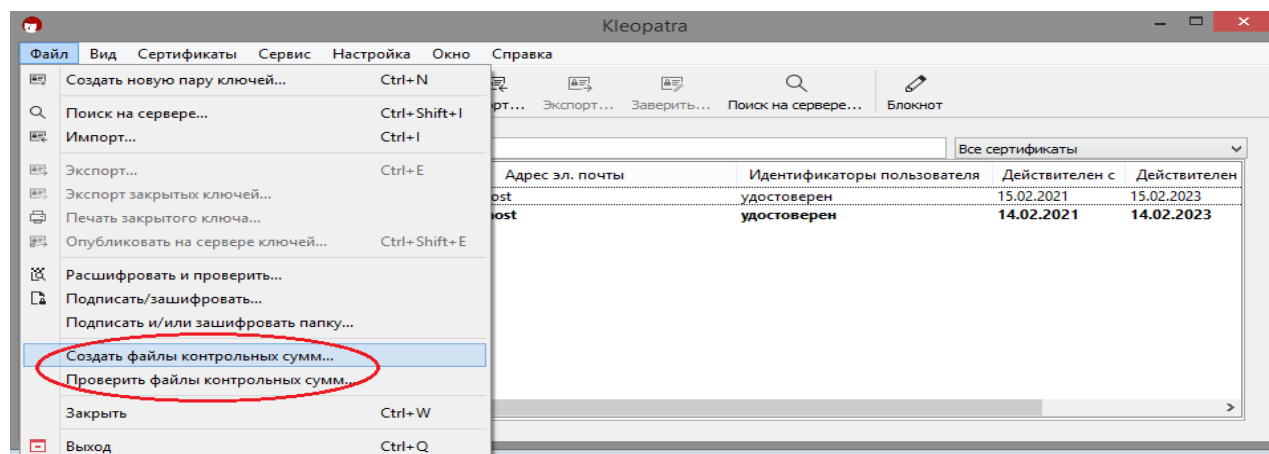
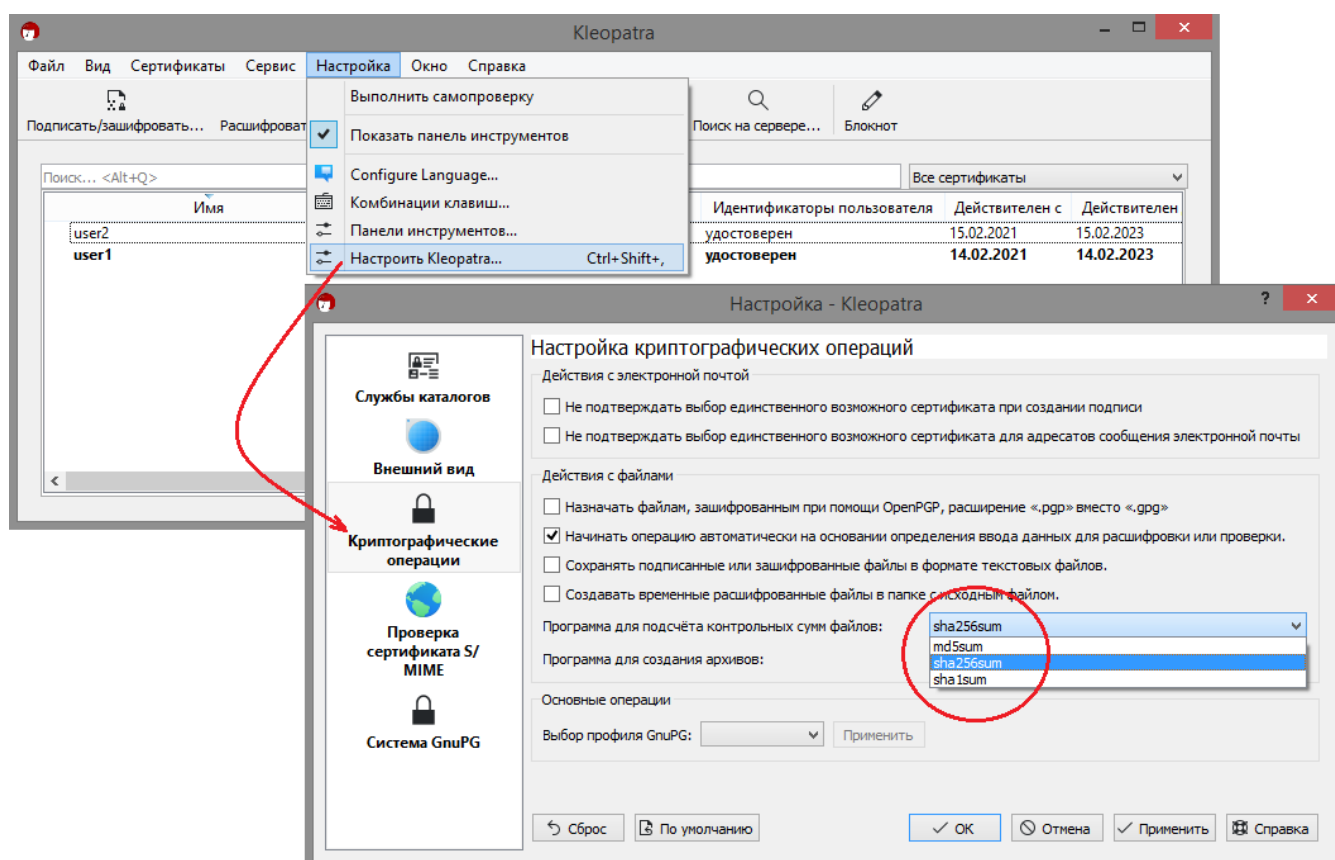
4.2. Зашифровать с использованием импортированного ключа напарника созданный текстовый файл и передать его шифровку напарнику.

4.3. Получив зашифрованный файл от напарника, дешифровать его и убедиться, что файл был успешно дешифрован (указать номер варианта задания напарника).





5. Протестировать процесс электронной подписи (инструменты аналогичны п. 4).
- 5.1. Подписать созданный текстовый документ, содержащий текст в соответствии с вариантом задания, используя свой закрытый ключ. Передать документ и подпись напарнику.
- 5.2. Получить от напарника документ с подписью и убедиться, что подпись верна.
- 5.3. Изменить полученный подписанный документ и проверить, что подпись стала неверна.
6. Протестировать одновременное шифрование и подписание документа.
7. Работа с контрольными суммами.
- 7.1. Создать папку и скопировать в нее файлы, созданные в п.п. 4 и 5 (например, текстовый файл и его шифровка).
- 7.2. Сформировать для этих файлов контрольные суммы (алгоритм формирования контрольных сумм определяется вариантом задания).
- 7.3. Внести изменения в один из файлов и проверить его на целостность. Убедиться, что система обнаружит наличие искажения в файле при сравнении контрольных сумм.



7. Протестировать процесс симметричного шифрования по паролю.
- 7.1. Зашифровать папку, созданную в п. 6.1., симметричным шифрованием с паролем в качестве ключа (ключом должен являться вариант задания, например, "variant15").
- 7.2. Передать зашифрованный файл напарнику.
- 7.3. Расшифровать полученный от напарника файл, зная его вариант (см. п. 4.3.).

Подписание и шифрование файлов - Kleopatra

### Создание подписи и шифрование файлов

Доказать подлинность (подписать)

☐ Сертификат подписи: user1 <user1@localhost> (удостоверен, создан: 14.02.2021)

Зашифровать




☐ Зашифровать для себя: user1 <user1@localhost> (удостоверен, создан: 14.02.2021)

☐ Зашифровать для других: Введите имя или адрес электронной почты...

☒ Зашифровать, используя пароль. Каждый, кто знает пароль, сможет прочитать данные.

Сохранение

☐ Зашифровать и/или подписать каждый из файлов отдельно.



Зашифровать Отмена

Подписание и шифрование файлов - Kleopatra


### Результаты

Здесь отображаются состояние и ход выполнения операций шифрования.

OpenPGP: вариант0.txt

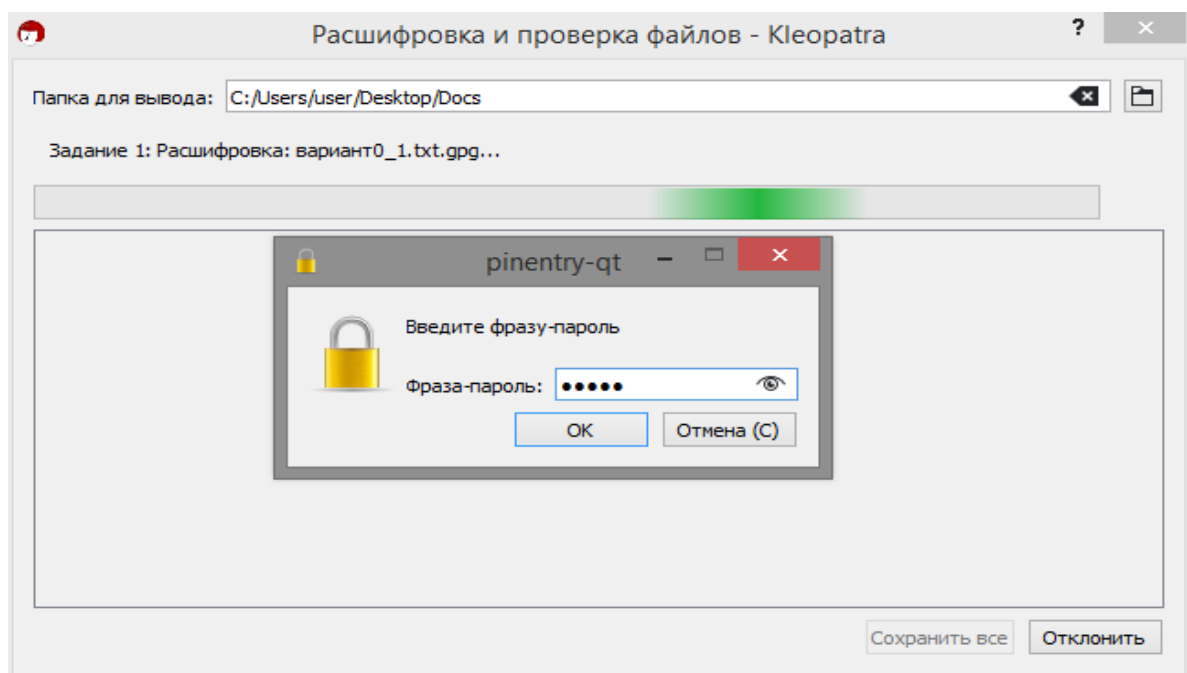
Введите фразу-пароль

Фраза-пароль:  

Повторите:

OK Отмена (C)

Завершить Отмена



Дополнительные источники информации:

1. GnuPG (GNU Privacy Guard). <https://www.gnupg.org/index.html>
2. Gpg4win (<https://gpg4win.org/download.html>, <https://www.gpg4win.org/documentation.html>).
3. Kleopatra. <https://docs.kde.org/stable5/en/pim/kleopatra/index.html>

### **Требования к оформлению отчета**

Отчет должен быть выполнен согласно установленным на кафедре требованиям к оформлению отчетов практических и лабораторных работ.

Описание каждого этапа выполнения лабораторной работы должно быть сопровождено скриншотами и описанием выполненных конфигураций.

Структурными элементами отчета являются:

- титульный лист;
- содержание;
- основная часть;
- заключение;
- список использованных источников.

Содержание основной части:

- цель работы;
- поставленная задача;
- ход работы, содержащий описание выполненных действий, проделанных в процессе выполнения работы.

Заключение должно содержать:

- краткие выводы по результатам работы;
- оценку полноты выполнения поставленной задачи.

Электронный документ, содержащий текст отчета, должен быть предоставлен в формате PDF.