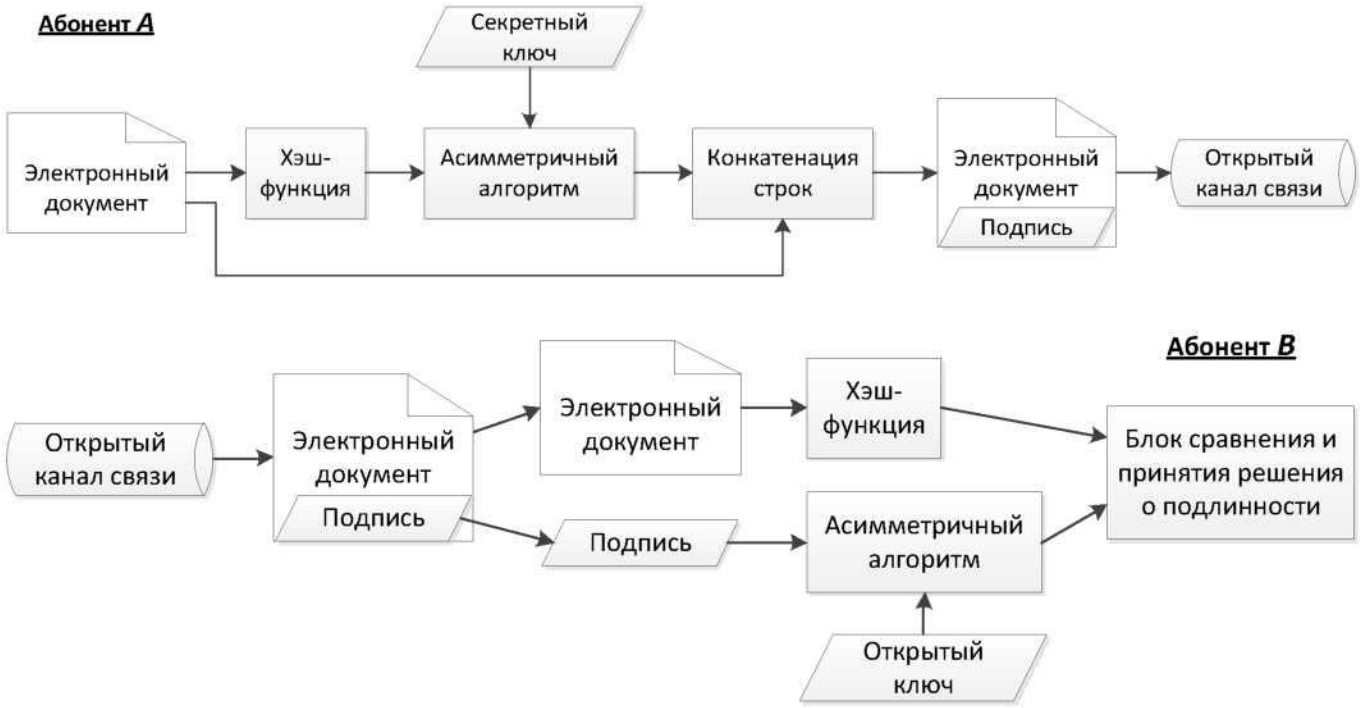
Практическая работа № 5

Тема: Электронная цифровая подпись.

Цель работы: ознакомление студентов с реализацией ассиметричного шифрования данных и формированием электронной цифровой подписи на основе алгоритма RSA и алгоритма Эль-Гамаля. Формирование навыков работы с приложениями, позволяющими осуществлять шифрование данных и формировать электронную подпись.

Теоретическая часть.

Наиболее распространённая схема электронной цифровой подписи (ЭЦП) использует шифрование хэш-функции полученной в результате обработки электронного документа, при помощи асимметричного алгоритма. Структурная схема такого варианта построения ЭЦП представлена на рисунке:



Процесс генерации ЭЦП происходит следующим образом:

Участник А вычисляет хэш-код от электронного документа. Полученный хэш-код проходит процедуру преобразования с использованием секретного ключа участника А. После этого полученное значение (которое и является ЭЦП) вместе с электронным документом отправляется участнику В.

Участник B должен получить электронный документ с ЭЦП и сертифицированный открытый ключ участника A, а затем произвести расшифрование на нём ЭЦП. Электронный документ подвергается операции хэширования, после чего результаты сравниваются, и если они совпадают, то ЭЦП признается истинной, в противном случае - ложной.

В настоящее время применяется несколько алгоритмов цифровой подписи.

- RSA (наиболее популярен);
- Digital Signature Algorithm, DSA (алгоритм цифровой подписи американского правительства, который применяют в стандарте цифровой подписи (Digital Signature Standard, DSS), также используется часто);
- алгоритм Эль-Гамаля (иногда можно встретить);
- алгоритм, который применяют в стандарте ГОСТ Р34.10-94 (в основе лежит DSA и является вариацией подписи Эль-Гамаля);
- так же существуют алгоритмы подписей, в основе которых лежит криптография эллиптических кривых; они похожи на все прочие, но в некоторых ситуациях работают эффективнее.

Электронная подпись RSA

Для осуществления подписи сообщения $M = M_1M_2M_3...M_n$ необходимо вычислить хэш-функцию $m = h(M_1M_2M_3...M_n)$, которая ставит в соответствие сообщению M число m. На следующем шаге достаточно снабдить подписью только число m, и эта подпись будет относиться ко всему сообщению M.

Далее по алгоритму RSA вычисляются ключи (e, n) и (d, n).

Затем вычисляется $s = m^d \bmod n$ (d - секретная степень).

Число s - это и есть цифровая подпись. Она просто добавляется к сообщению и получается подписанное сообщение $\{M, s\}$.

Теперь каждый, кто знает параметры подписавшего сообщение (т.е. числа e и n), может проверить подлинность подписи.

Для этого необходимо проверить выполнение равенства $h(M) = s^e \bmod n$.

Алгоритм Эль-Гамаля

Для генерации пары ключей сначала выбирается большое простое число p, один из его первообразных корней g и случайное число x ($g<p$, $x<p$). Затем вычисляется $y = g^x \bmod p$ [1, 2]. Открытым ключом являются y, g и p. Закрытым ключом является x.

Чтобы подписать m, являющееся хэш-значением некоторого сообщения M, сначала выбирается секретное случайное число k, взаимно простое с p–1. Затем вычисляется $a = g^k \bmod p$.

Из соотношения $m = (x \cdot a + к \cdot b) \bmod (p–1)$ определяется b. Выполнив преобразования, получим $b = k^{-1} \cdot (m – x \cdot a) \bmod (p–1)$, где k^{-1} определяется из соотношения $k^{-1} \cdot k \equiv 1 \pmod{(p–1)}$.

В результате подписью будет пара (a, b). Для проверки подписи нужно убедиться, что $y^a \cdot a^b \bmod p = g^m \bmod p$.

Пример.

Пусть $p = 11$, $g = 2$, $x = 8$. Тогда $y = 2^8 \bmod 11 = 3$. $m = 5$.

Выбираем $k = 9$. Тогда $a = 2^9 \bmod 11 = 6$.

Из соотношения $9 \cdot k^{-1} \equiv 1 \pmod{10}$ находим обратный элемент k^{-1}, применяя расширенный алгоритм Евклида (см. далее): $k^{-1} = 9$.

$$b = k^{-1} \cdot (m – x \cdot a) \bmod (p – 1) = 9 \cdot (–43) \bmod 10 = 3.$$

Подписью хэш-значения $m = 5$ является пара (a, b) = (6, 3).

Проверка: $3^6 \cdot 6^3 \bmod 11 = 2^5 \bmod 11 = 10$.

Нахождение обратного элемента с помощью расширенного алгоритма Евклида:

Пусть нужно найти элемент d^{-1} такой, что $d \cdot d^{-1} \equiv 1 \pmod{f}$.

Пусть $x = (1,0,f)$, $y = (0,1,d)$. В цикле выполняются следующие действия:

1. Если $y_3 = 0$, то не существует элемента, обратного к d по модулю f.
2. Если $y_3 = 1$, то $d^{-1} = y_2$.
3. Иначе выполняются следующие преобразования, после которых выполняется переход на шаг 1

$$q = \left[\frac{x_3}{y_3}\right],$$
$$t = x - q \cdot y, \qquad x = y, \qquad y = t.$$

Пример нахождения обратного элемента:

$$d = 9, \qquad f = 10.$$
$$x = (1,\ 0,\ 10), \qquad y = (0,\ 1,\ 9).$$
$$q = 1.$$
$$t = (1,\ 0,\ 10) - 1 \cdot (0,\ 1,\ 9) = (1, -1,\ 1).$$
$$x = (0,\ 1,\ 9), \qquad y = (1, -1,\ 1).$$
$$y_3 = 1, \ \Rightarrow \ d^{-1} = y_2 = -1 + 1 \cdot 10 = 9.$$

Задание на практическую работу

1. Скачать и установить бесплатный набор инструментов, предназначенных для шифрования файлов и электронных сообщений «Gpg4win». В состав пакета входят следующие компоненты: ядро программы, менеджер сертификатов и ключей шифрования, плагин для почтового клиента Microsoft Outlook 2003/2007, плагин для шифрования файлов, менеджер сертификатов и ключей шифрования Kleopatra, а также небольшой почтовый клиент.

2. Сгенерировать в Kleopatra новую пару ключей (открытый и закрытый) по алгоритму RSA.

3. Экспортировать открытый ключ в файл и передать его партнеру (одногруппнику (-це)) по электронной почте.

4. Получить открытый ключ партнера (файл с расширением .asc) и импортировать его в Kleopatra, заверить своим закрытым ключом.

5. Создать файл формата .doc/.docx/.txt с текстом.

6. Используя открытый ключ партнера, зашифровать для него созданный файл в Kleopatra и передать его по электронной почте.

7. Расшифровать зашифрованный файл (сначала без подписи, затем с подписью) партнера своим закрытым ключом.

8. Созданный в п.5 текстовый документ подписать своей электронной подписью и отправить партнеру два файла: сам документ и файл с подписью (***.sig).

9. Проверить электронную подпись партнера.

10. Изменить содержание документа и проверить электронную подпись повторно.

Загрузка и установка приложения для шифрования и электронной подписи

Для выполнения заданий, предусмотренных данной практической работой необходимо из компонентов программы выбрать приложение Kleopatra (рис. 1). Вы можете ознакомиться с описанием остальных компонентов, и при необходимости их установить дополнительно.

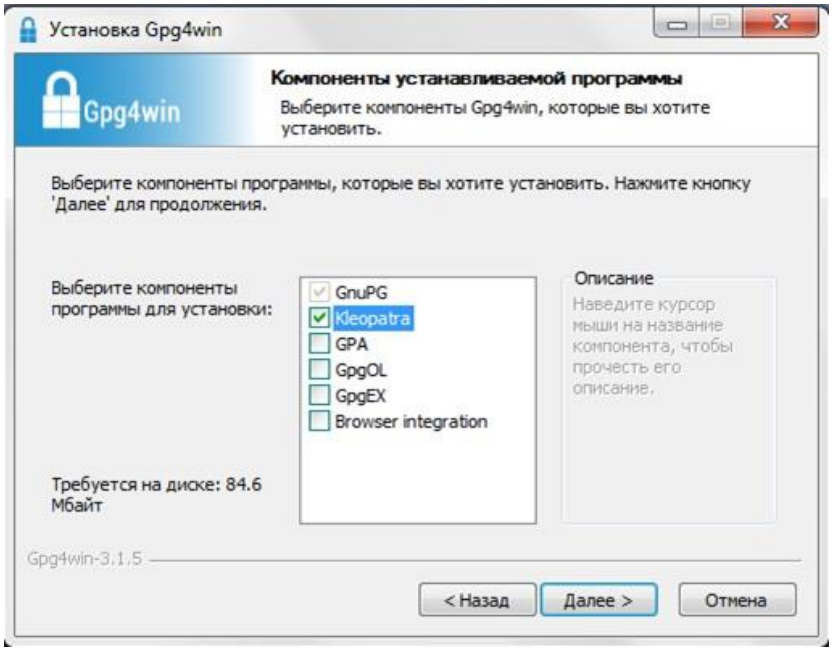


Рис. 1. Выбор компонентов устанавливаемого приложения

Создание пары ключей для шифрования и электронной подписи

1. Запустите приложение Kleopatra (рис. 2)

Рис. 2. Интерфейс приложения Kleopatra

2. Нажмите кнопку «Создать новую пару ключей». Появится окно «мастер создания пары ключей». Введите свои регистрационные данные:

- Фамилия Имя (Отчество - необязательно)
- Адрес электронной почты

3. При нажатии на кнопку «Дополнительные параметры» появиться окно «Дополнительные параметры» (рис. 3) где можно выбрать параметры:

a) алгоритм шифрования (RSA, DSA, ECDSA/EdDSA)

b) длину ключа (2048, 3072, 4096 бит)

c) срок действия сертификата электронной подписи

d) и другие параметры

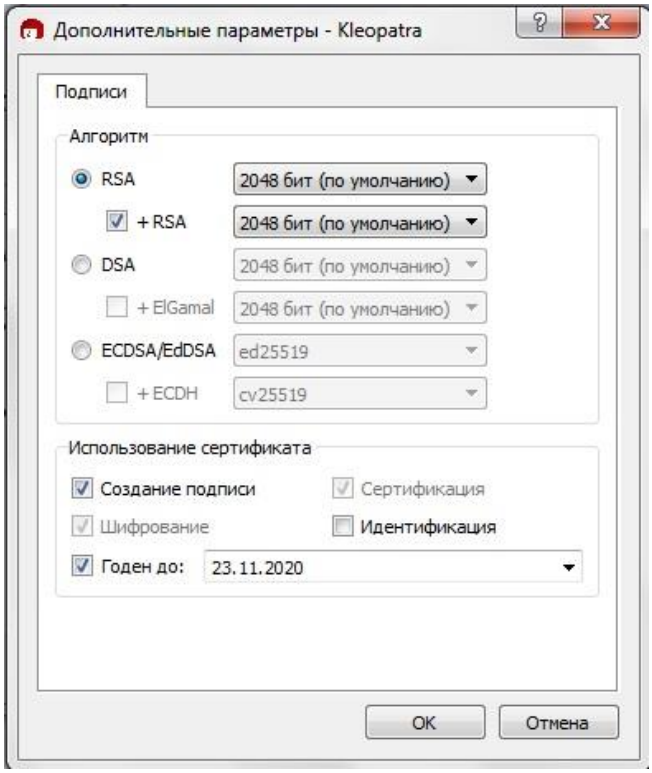


Рис. 3. Дополнительные параметры

4. Не меняя настроек, нажмите кнопку «Отмена» и выйдите из окна «Дополнительные параметры». Нажмите «Далее»

5. Откроется окно «Обзор параметров», в котором можно проверить введенные данные перед созданием пары ключей. Нажмите кнопку «Создать».

6. Программа попросит ввести фразу-пароль для защиты нового ключа. Введите фразу-пароль и подтвердите ее. Нажмите «ОК» (рис. 4).

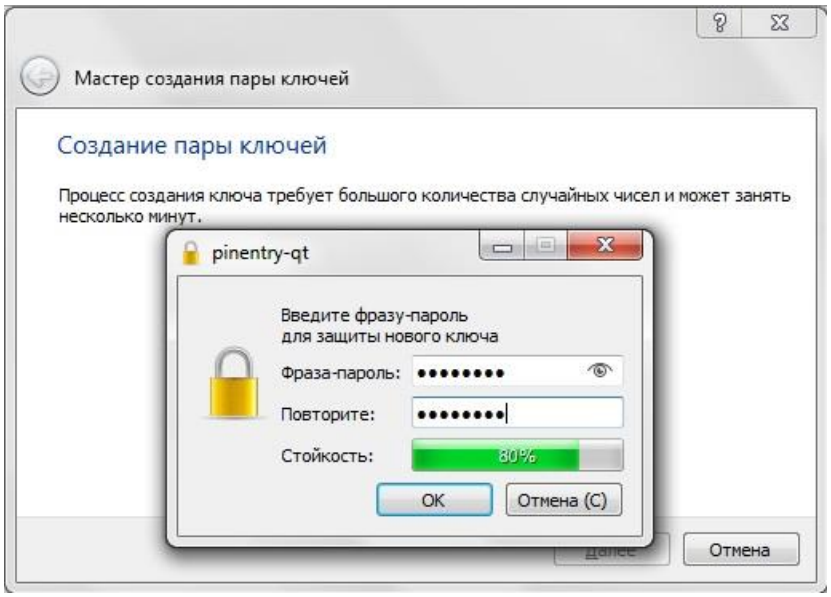


Рис. 4 Ввод фразы-пароля для защиты новых ключей

7. Об успешном создании новой пары ключей программа оповещает следующим окном (рис. 5). Нажмите кнопку «Завершить».

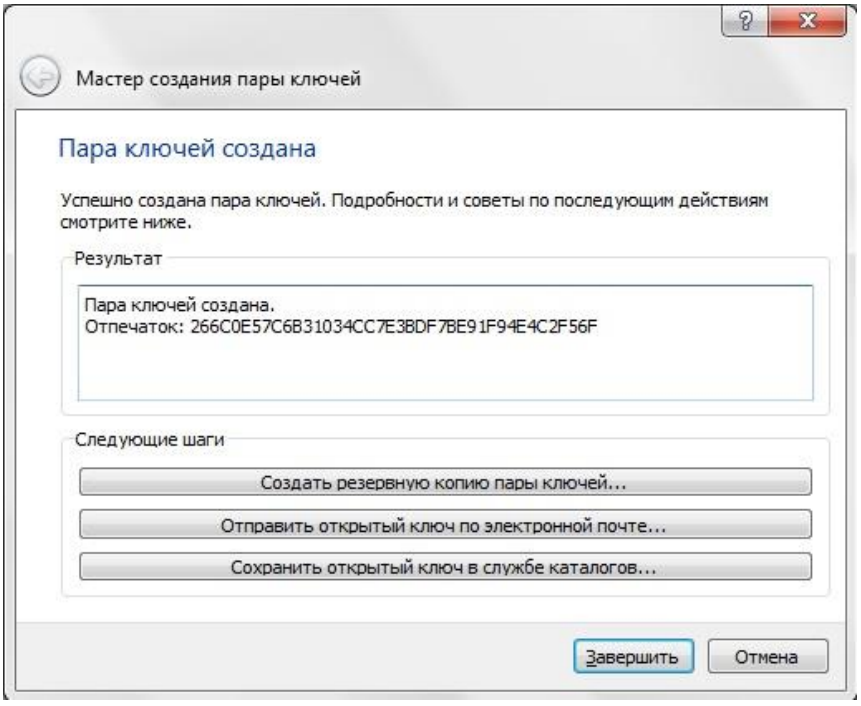


Рис. 5. Окно, оповещающее пользователя о создании новой пары ключей.

8. В списке сертификатов появится строчка, состоящая из имени пользователя, электронной почты, идентификатора пользователя, даты создания и окончания действия сертификата, а также идентификатора ключа

(рис. 6). Полужирное начертание означает наличие пары ключей (открытого и закрытого).

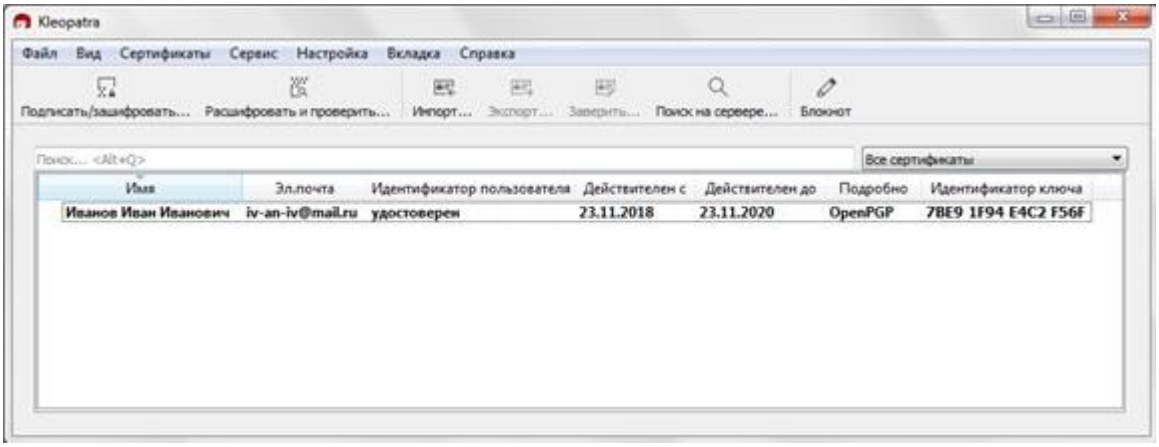


Рис. 6. Отображение сертификата в списке сертификатов

Экспорт открытого ключа в файл.

1. Для того чтобы осуществлять шифрование и подпись файлов для передачи другим лицам, необходимо выполнить процедуру обмена открытыми ключами. Для этого сначала необходимо экспортировать открытый ключ в файл и передать его по какому-либо каналу связи.

2. Выберите сертификат, для которого необходимо выполнить экспорт открытого ключа в файл, нажав на него левой кнопкой мыши.

3. На панели инструментов нажмите кнопку **«Экспорт…»**

4. Выберите директорию, в которой будет располагаться экспортированный файл и нажмите «Сохранить». В данной директории появится файл с расширением .asc

5. Данный файл можно отправить другому лицу для того, чтобы:

- вам могли отправить файл, зашифрованный по вашему открытому ключу;
- получатель имел возможность проверить вашу электронную подпись.

Импорт стороннего открытого ключа (сертификата)

1. Допустим, вы получили по электронной почте файл, содержащий открытый ключ другого лица. Для того чтобы можно было использовать данный открытый ключ для шифрования файлов или проверки электронной подписи, необходимо импортировать сертификат в приложение Kleopatra.

2. Нажмите кнопку **«Импорт…»**

3. Выберите файл, содержащий открытый ключ другого лица и нажмите «Открыть».

4. Появится окно с запросом подтверждение операции, позволяющей заверить импортированный сертификат (открытый ключ), тем самым применяя дополнительную меру защиты, основанную на доверии к сертификатам, отпечаток которых был проверен с помощью информации, полученной по телефонному звонку, из визитки или после проверки на доверенном веб-сайте (рис.7). Нажмите кнопку «Да», чтобы заверить сертификат.

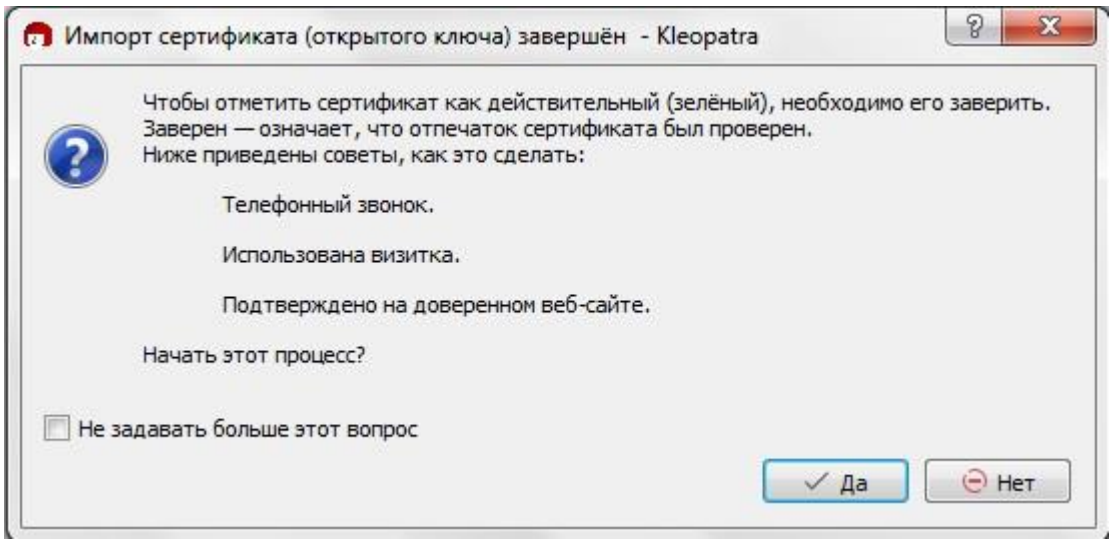


Рис. 7. Окно подтверждения операции, позволяющей заверить импортированный сертификат

5. Выберите сертификат, который будете заверять, поставив рядом с ним галочку. Проверьте контрольную сумму подписываемого сертификата с той, которую вам предоставил лично или другими безопасными способами партнер, сертификат которого вы заверяете (подписываете своим закрытым ключом). Если контрольные суммы совпадают, поставьте галочку рядом с надписью **«Я проверил контрольную сумму»**. Нажмите кнопку **«Далее»**.

6. В рамках выполнения данной практической работы необходимо выбрать способ удостоверения **«Удостоверить только для себя»** (рис. 8). Нажмите кнопку **«Заверить»**

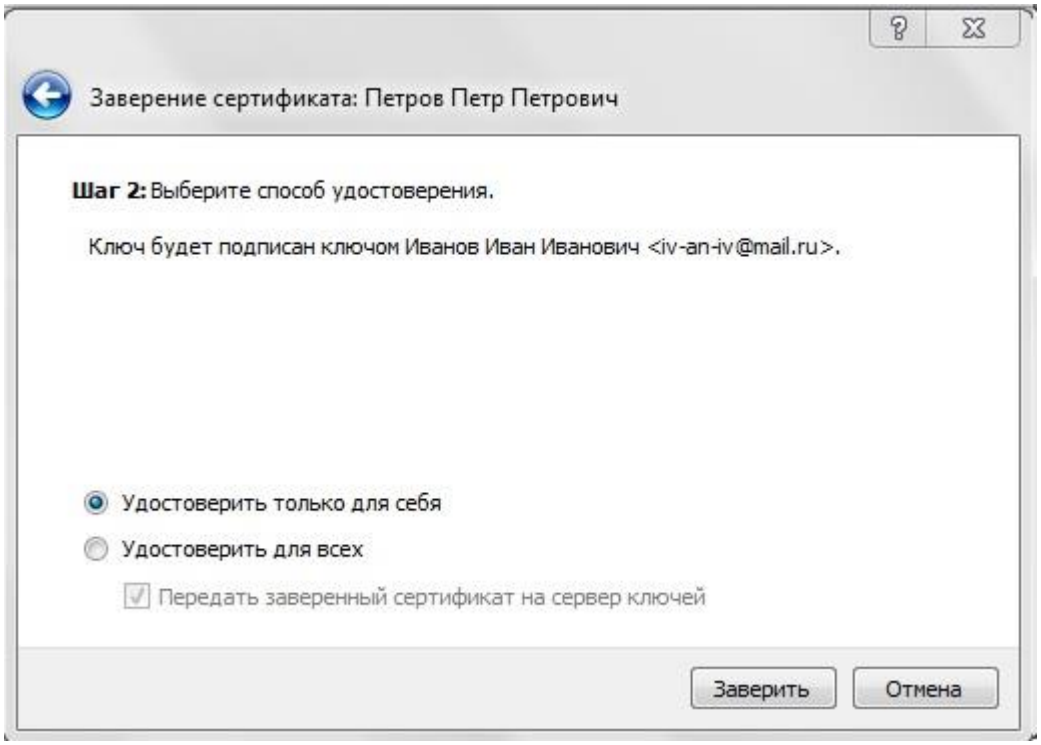


Рис. 8. Выбор способа удостоверения

7. Введите фразу-пароль для разблокировки вашего секретного ключа (которую вы вводили при создании пары ключей), чтобы с его помощью подписать импортированный сертификат (рис. 9). Нажмите **«ОК»**

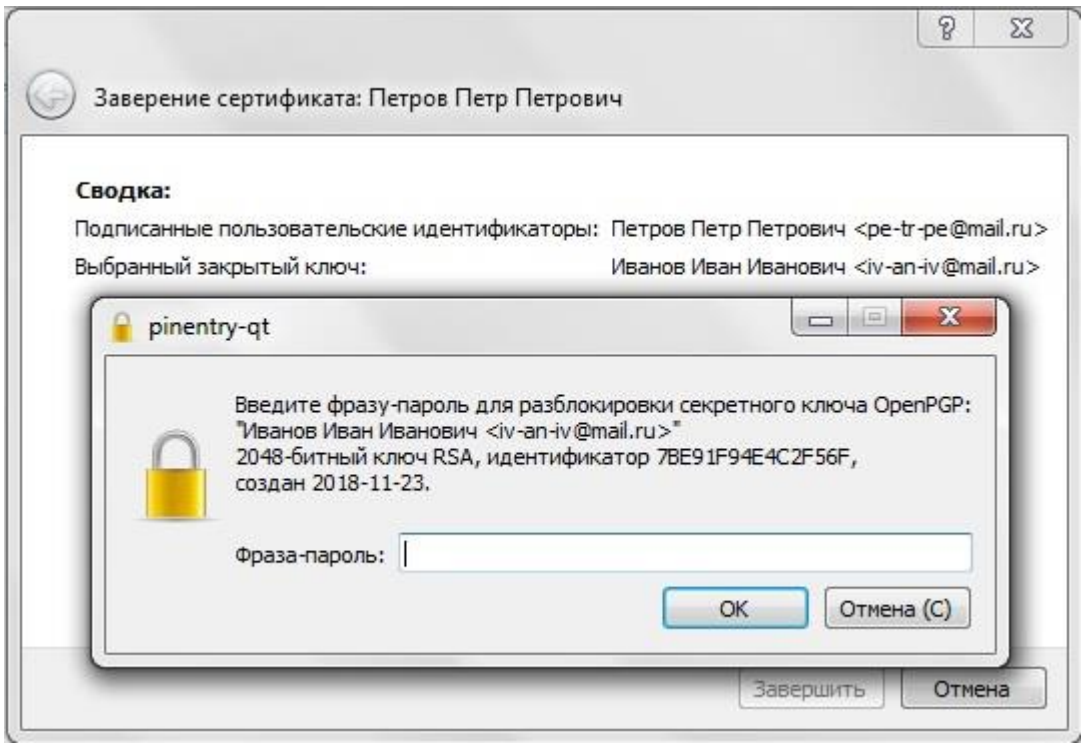


Рис. 9. Ввод фразы-пароля для разблокировки секретного ключа

8. Появится сообщение **«Успешно удостоверено»**. Нажмите **«Завершить»**.

9. В списке сертификатов появится импортированный сертификат (рис. 10). Его начертание будет обычное, так как он содержит только открытый ключ.

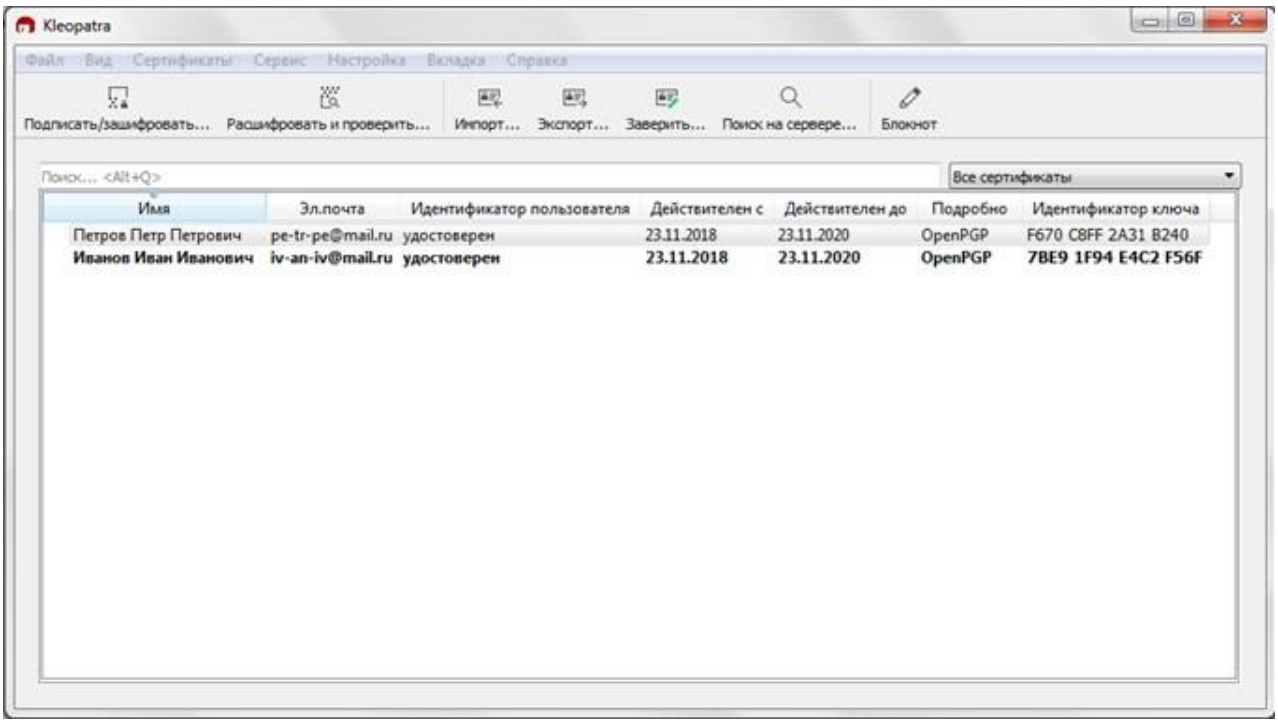


Рис. 10. Список сертификатов

Шифрование и расшифрование файлов без подписи

1. В рамках данной практической работы будет рассмотрено шифрование файлов для передачи электронных документов с конфиденциальной информацией определенному лицу (данная программа также позволяет осуществлять шифрование файлов только для личного пользования). Так как в программе используется ассиметричное шифрование, исходный файл будет зашифрован с помощью открытого ключа (сертификата) получателя. В предыдущих разделах был рассмотрен обмен сертификатами с помощью операций экспорта в файл и импорта из файла. У пользователя имеется пара своих ключей, и открытый ключ его партнера, который затем расшифрует зашифрованный файл своим секретным ключом.

2. Для дальнейшего шифрования необходимо подготовить электронный документ формата .doc/.docx с названием «Секретный документ.docx», содержащий текст «Конфиденциальная информация» (рис. 11).

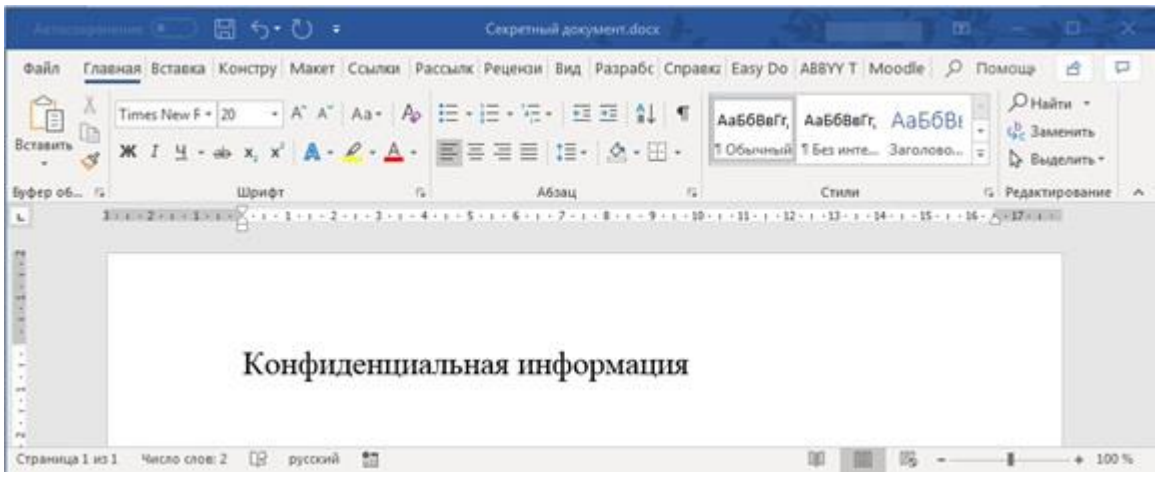


Рис. 11. Подготовленный документ для шифрования

3. В приложении Kleopatra нужно нажать кнопку **«Подписать/Зашифровать…»**

4. Далее необходимо выбрать файл для шифрования и нажать кнопку **«Открыть»**

5. В появившемся окне (рис. 12) выбираем (ставим галочки) в разделе «Шифрование» напротив пунктов **«Зашифровать для других»** и **«Зашифровать для себя»** (на тот случай, если возникнет необходимость расшифровать зашифрованные файлы для собственного пользования)

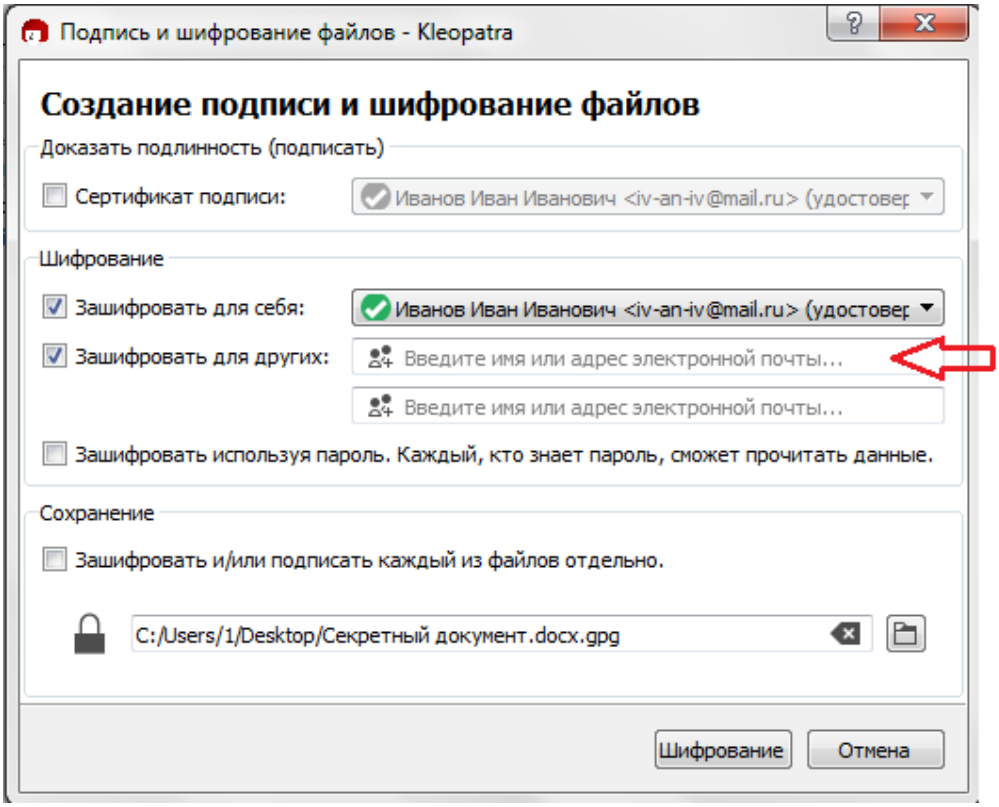
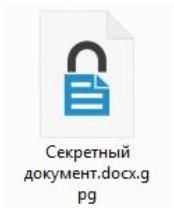


Рис. 12. Шифрование данных

6. Рядом с пунктом **«Зашифровать для других»** имеется поле ввода, где нужно выбрать сертификат партнера, которому будет направлено зашифрованное сообщение.

7. В дополнение к шифрованию с использованием открытых ключей получателя, возможно зашифровать данные, используя пароль. Любой, кто знает пароль, сможет прочесть данные без закрытого ключа. Использование пароля, даже очень сложного менее безопасно, чем использование шифрования на основе двухключевой криптосистемы. В данной работе использование пароля для шифрования файлов не используется, поэтому галочку рядом с пунктом «Зашифровать используя пароль…» ставить не надо.

8. Далее необходимо нажать на кнопку **«Шифрование»**. Если шифрование прошло успешно, будет отображено окно оповещения об успешном шифровании и в назначенной директории появится зашифрованный файл **«Секретный документ.docx.gpg»**



10. Для расшифровки полученного файла необходимо в приложении **Kleopatra** нажать на кнопку **«Расшифровать и проверить…»**

11. Выберите зашифрованный файл, который заканчивается на .gpg и нажмите «Открыть». Появится окно «Расшифровка и проверка файлов», где необходимо ввести фразу-пароль для разблокировки секретного ключа (рис. 13)

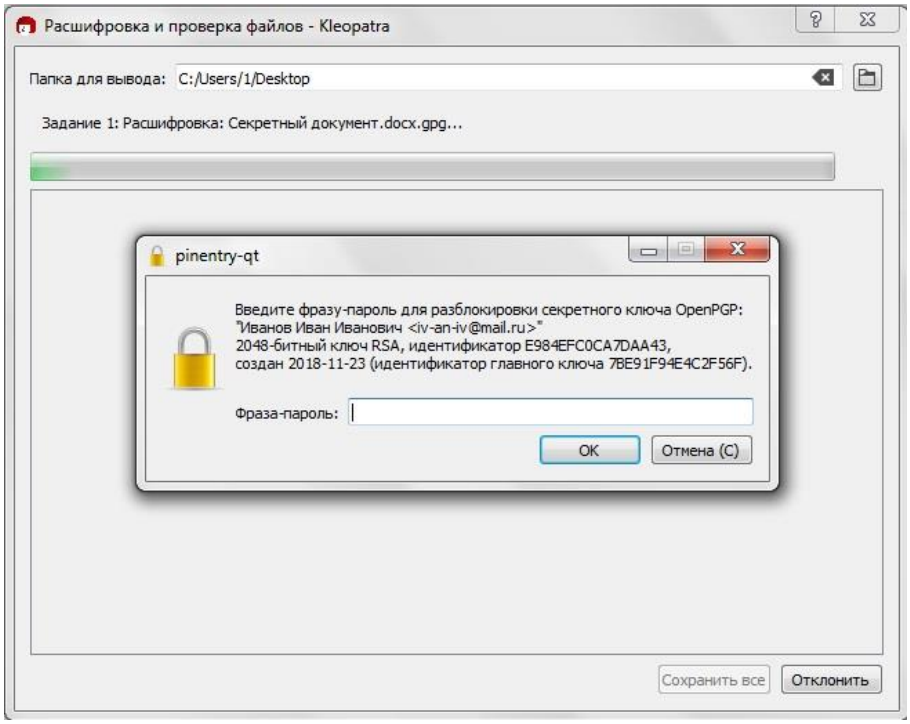


Рис. 13. Расшифровка и проверка файлов

12. После ввода фразы-пароля нажмите **«ОК»**. Приложение расшифрует файл в указанную директорию и сообщит пользователю о завершении процесса расшифровки. Чтобы закрыть окно и сохранить расшифрованный файл нажмите **«Сохранить все»**.

13. Так как шифрование происходило без подписи, то будет отображено примечание, которое имеет следующее содержание: *«Так как отсутствует подпись сообщения, то не удается достоверно установить кем зашифровано это письмо, т.к. подпись отсутствует».*

Шифрование и расширование файлов с подписью

14. Если помимо шифрования необходимо, чтобы получатель мог установить кем был зашифрован файл, то можно дополнительно подписать зашифрованный файл сертификатом отправителя, поставив галочку напротив пункта **«Сертификат подписи»** и выбрать нужный сертификат (см. п. 5 данного раздела, рис. 12). После шифрования приложение оповестит

пользователя, что шифрование и подпись прошли успешно. После этого нужно нажать кнопку **«Завершить».**

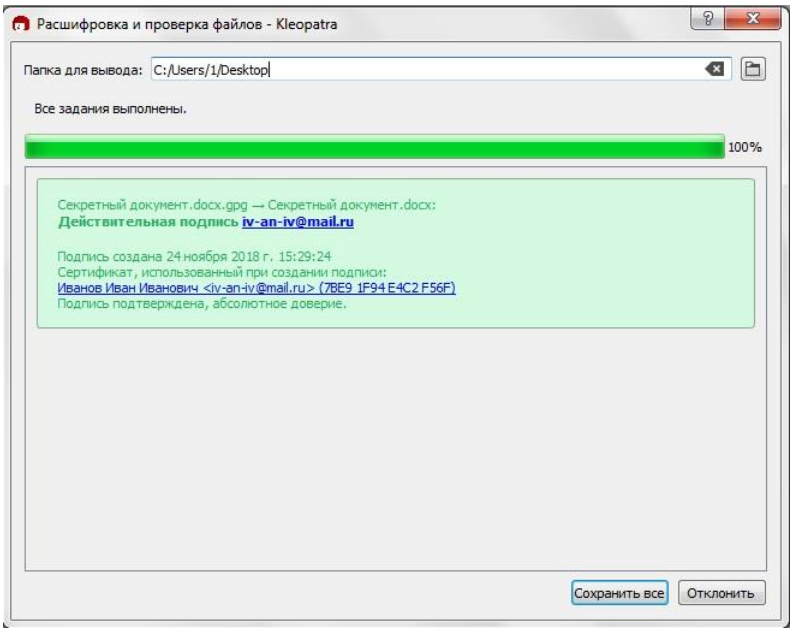


Рис. 14. Расшифровка файла и проверка подписи выполнены.

15. Тогда после расшифровки получатель увидит информацию о том, кем был подписан зашифрованный файл (рис. 14). Для закрытия окна и сохранения расшифрованного файла нажмите **«Сохранить все».**

Электронная подпись для файлов и ее проверка

1. Приложение Kleopatra позволяет формировать электронную подпись для проверки целостности подписываемых электронных документов и установления их авторства на основе сертификатов подписывающих лиц.

2. Для подписывания будет использован подготовленный ранее файл **«Секретный документ.docx»**.

3. В приложении Kleopatra нужно нажать кнопку **«Подписать/Зашифровать…»**

4. Далее необходимо выбрать подписываемый файл и нажать кнопку **«Открыть»**

5. В появившемся окне поставьте галочку рядом с пунктом **«Сертификат подписи»**. Выберите необходимый сертификат и нажмите кнопку **«Подписать»** (рис. 15).

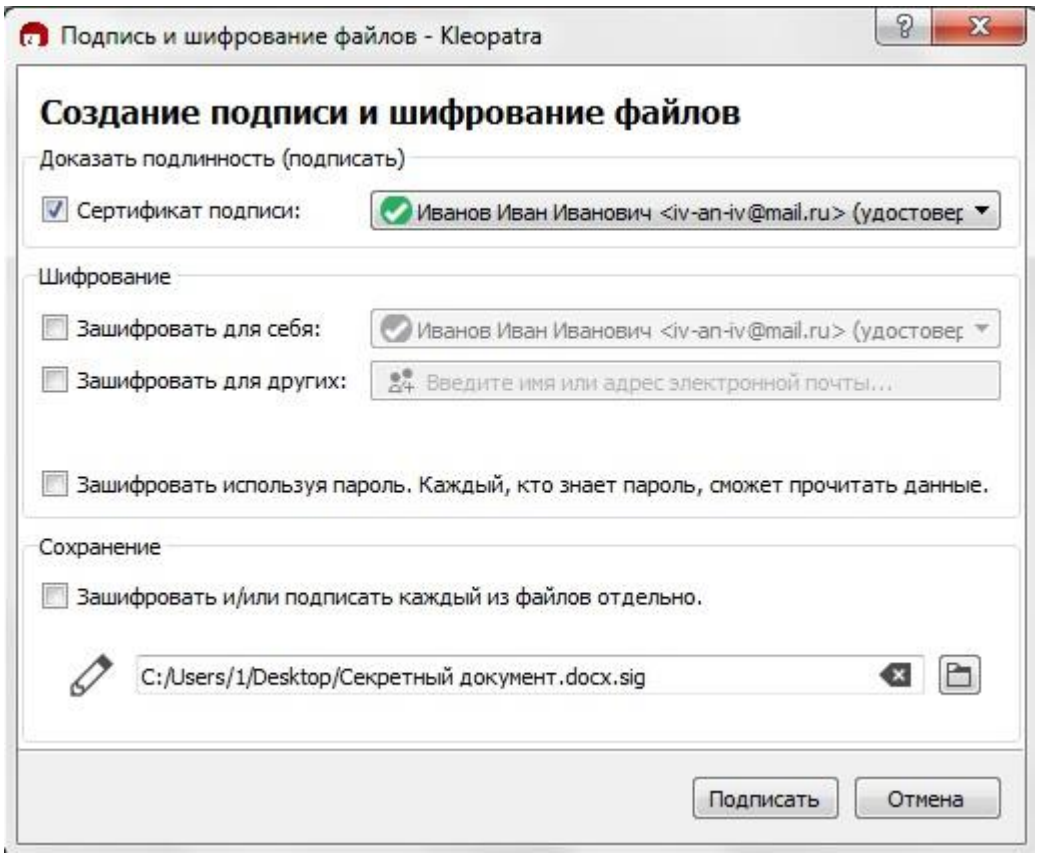


Рис. 15 Создание подписи

6. Введите фразу-пароль для разблокировки секретного ключа (рис. 16)

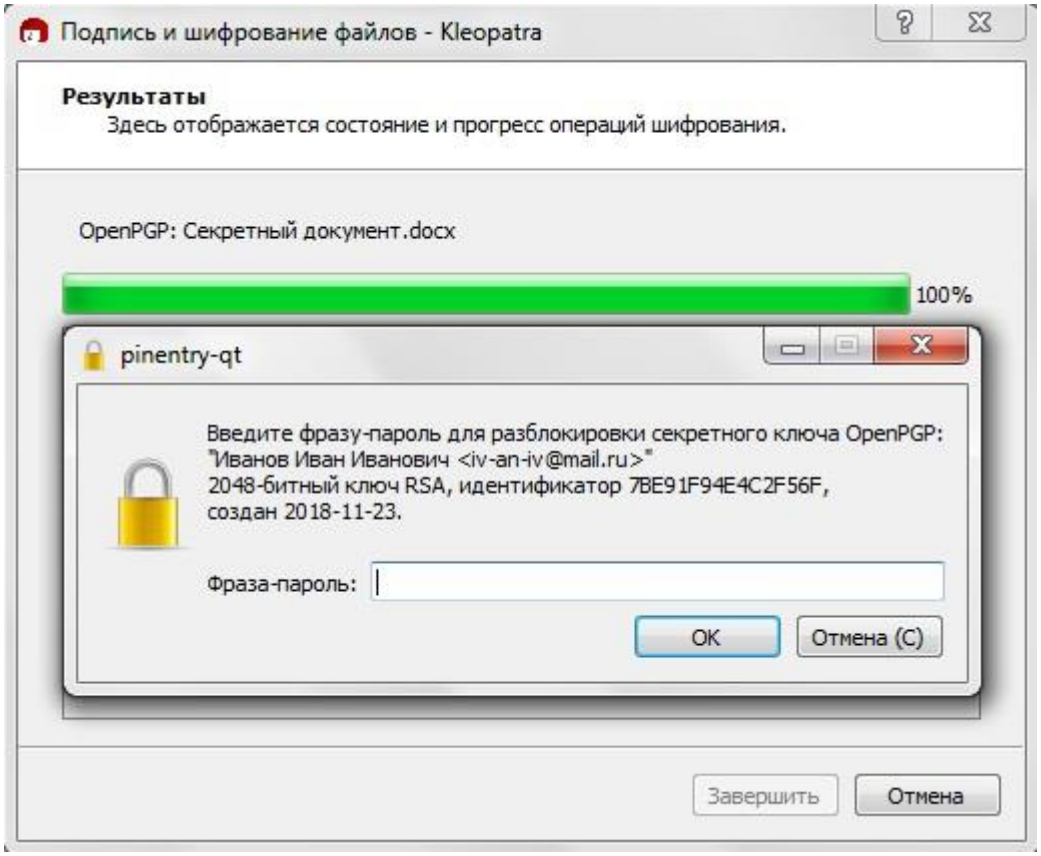


Рис. 16. Ввод фразы-пароля для подписи файла

7. Приложение оповестит пользователя о том, что файл успешно подписан (рис. 17). Необходимо нажать кнопку **«Завершить».**

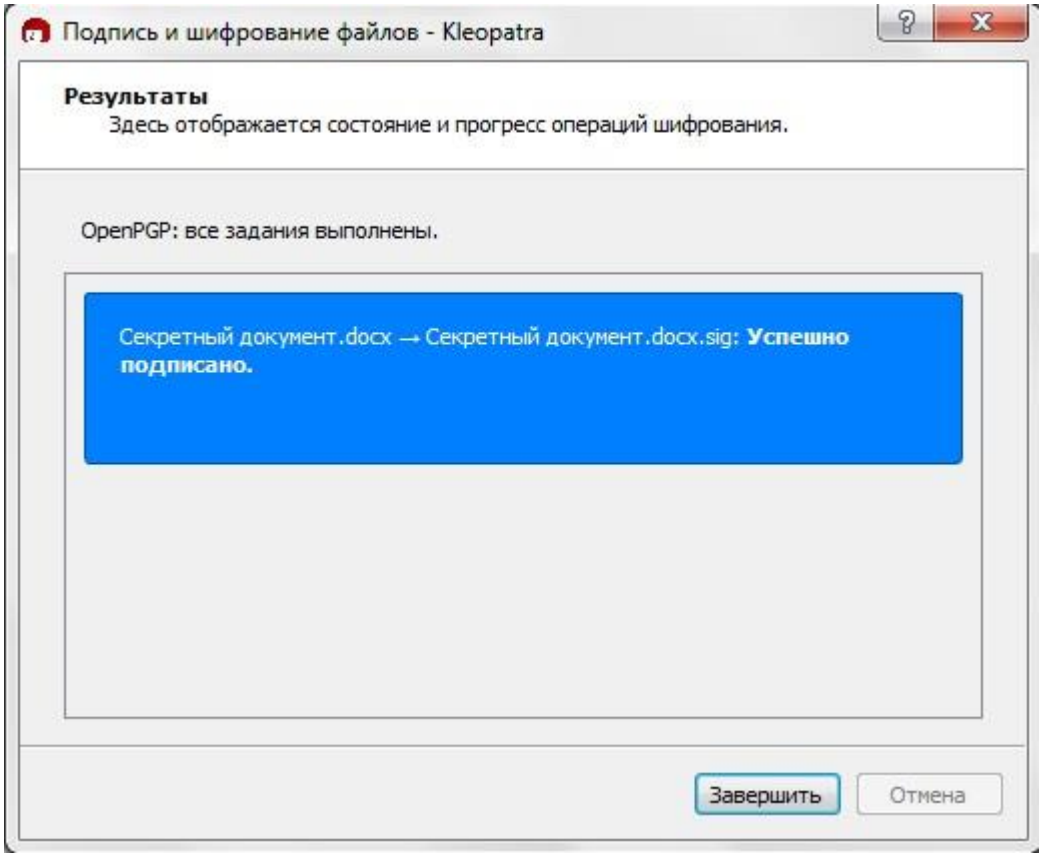
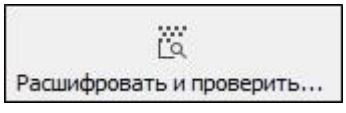


Рис. 17. Файл успешно подписан

8. В директории, где расположен подписываемый файл, появится отдельный файл подписи **«Секретный документ.docx.sig»**. Данный файл отправляется вместе с подписываемым файлом.

9. Для проверки подписи необходимо в приложении Kleopatra нажать на кнопку **«Расшифровать и проверить…»**



10. Далее выберите файл подписи, который должен заканчиваться на .sig и нажмите **«Открыть».**

Примечание. Файл подписанного документа и файл подписи должны находиться в одной папке, иначе проверка подписи пройдет некорректно.

11. Если проверка подписи прошла успешно, приложение оповестит пользователя, что подпись действительна и покажет информацию о том, кем она была произведена (рис. 18).

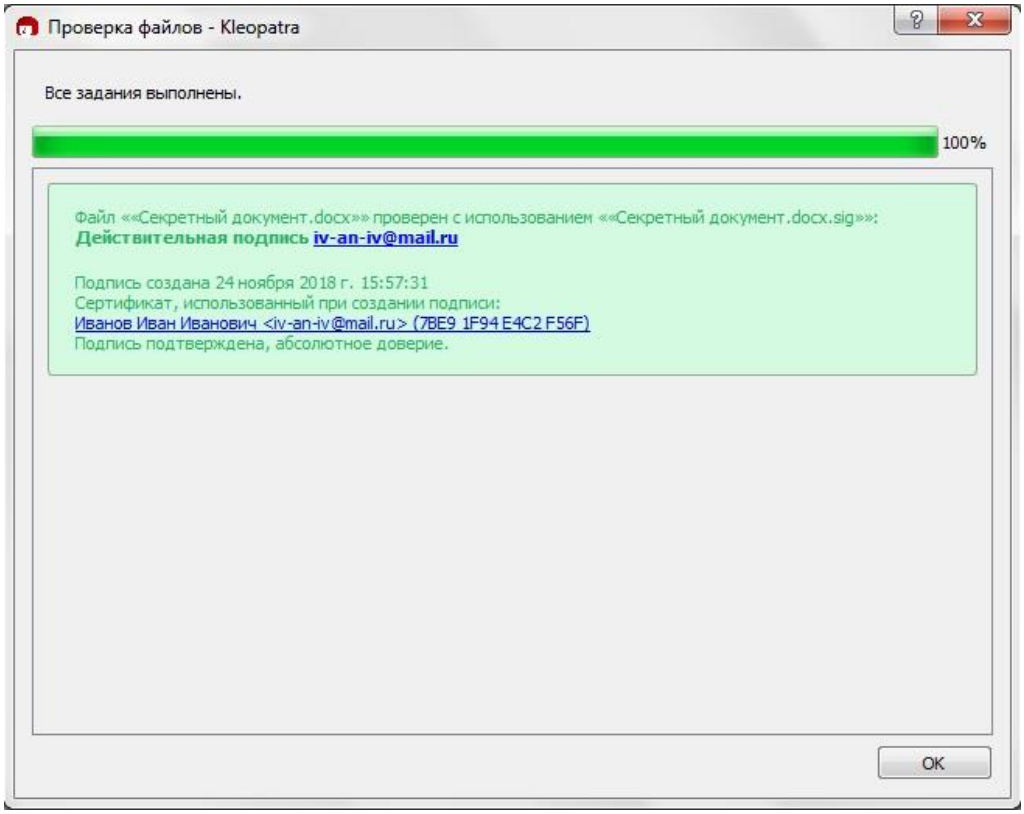


Рис. 18. Подтверждение подписи

12. Как известно, электронная подпись позволяет не только определить лицо, подписавшее электронный документ, но и обнаружить факт внесения изменений в электронный документ после момента его подписания. Для проверки данной полезной функции внесите изменения в уже подписанный документ **«Секретный документ.docx»** (например, поставьте в конце одну запятую) и сохраните его (рис. 19)

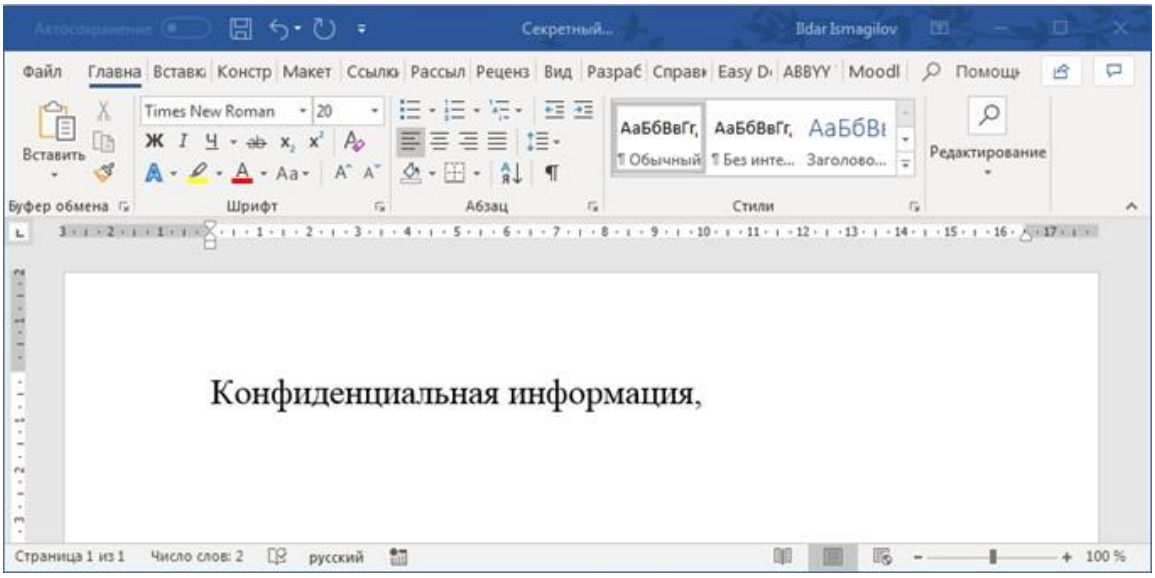


Рис. 19. Внесение изменений в подписанный документ.

13. Повторите действия, описанные в п.п. 9-11 данного раздела. Приложение оповестит пользователя о том, что подпись неверна (рис. 20).

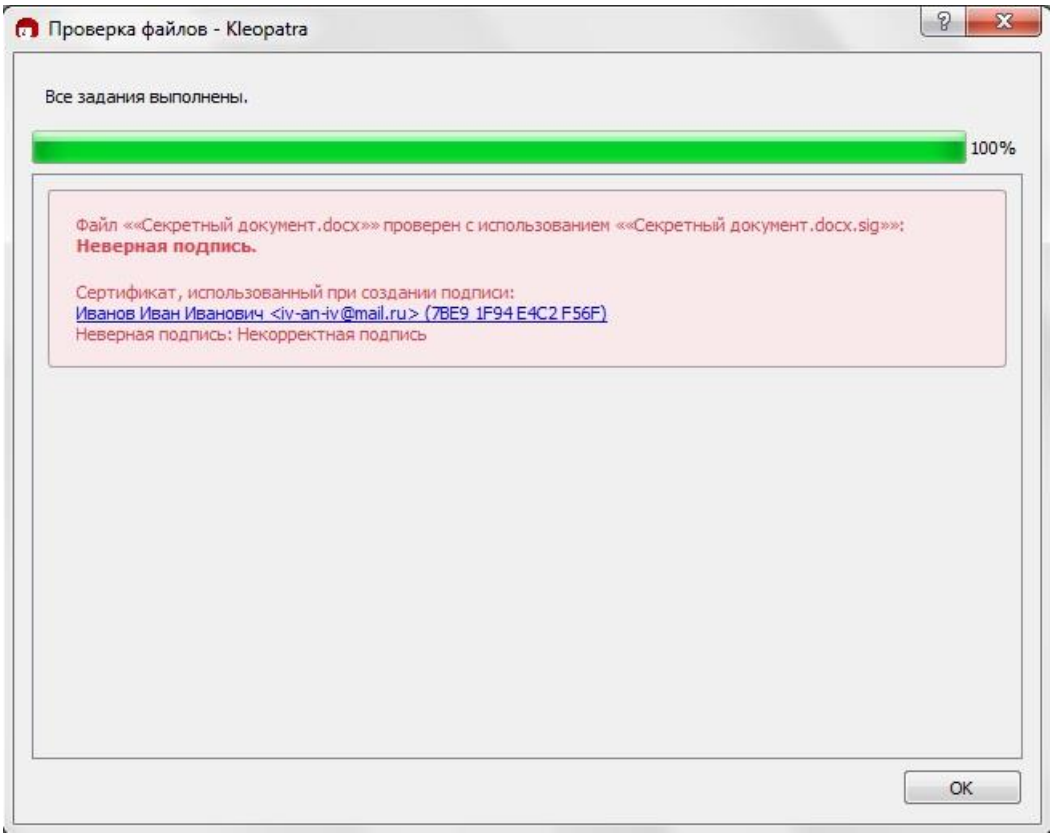


Рис. 20. Оповещение пользователя о неверной подписи.