Методические указания к практической работе «Защита информации в электронных документах путем шифрования и формирования электронной подписи" (для пользователей MacOS)

1. Загрузка и установка приложения для шифрования и электронной подписи

1. Необходимо зайти на интернет-сайт GPG Suite по ссылке
2. С помощью ссылки GPG Suite зайдите на страницу загрузки приложения GPG Suite (рис .1).

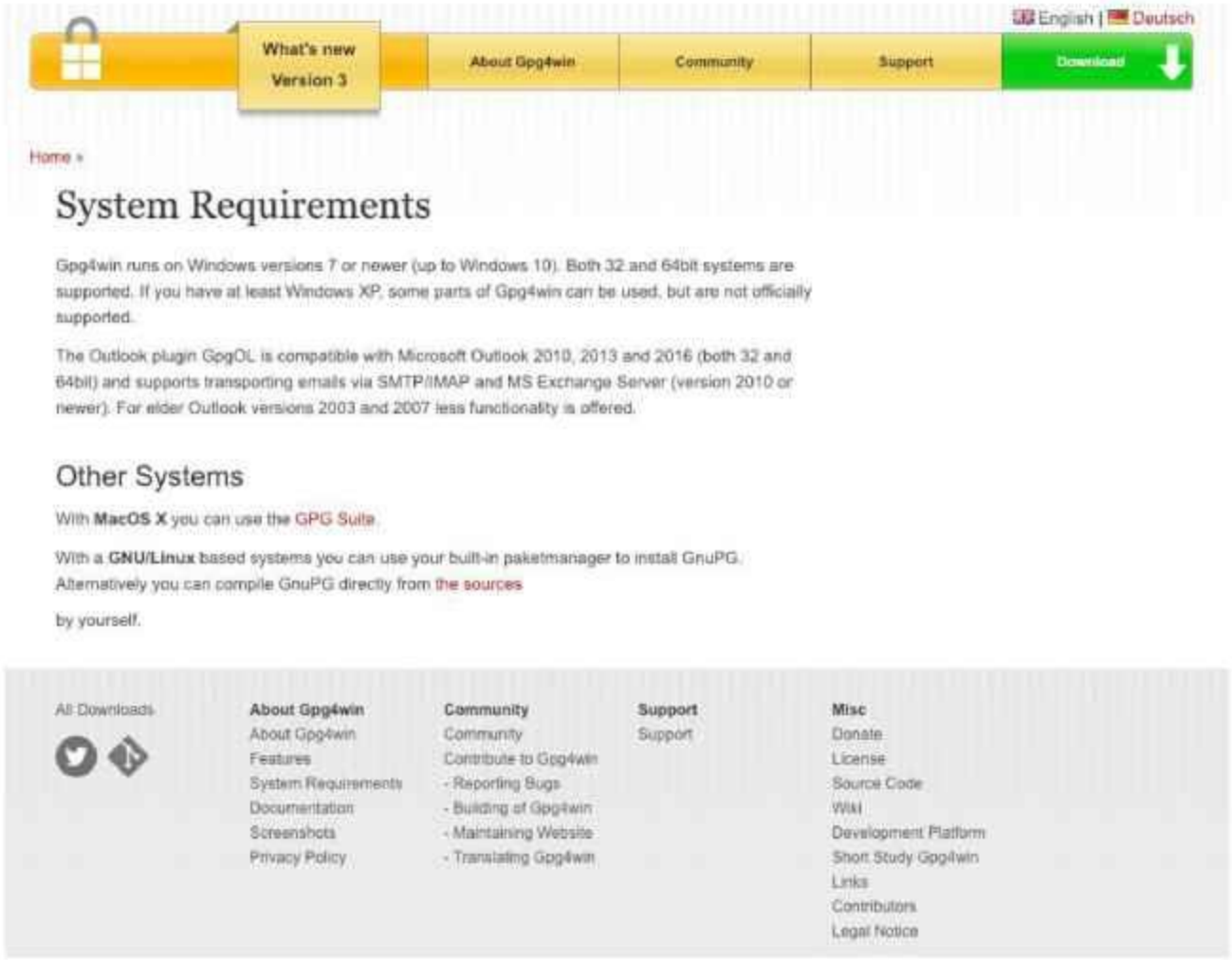
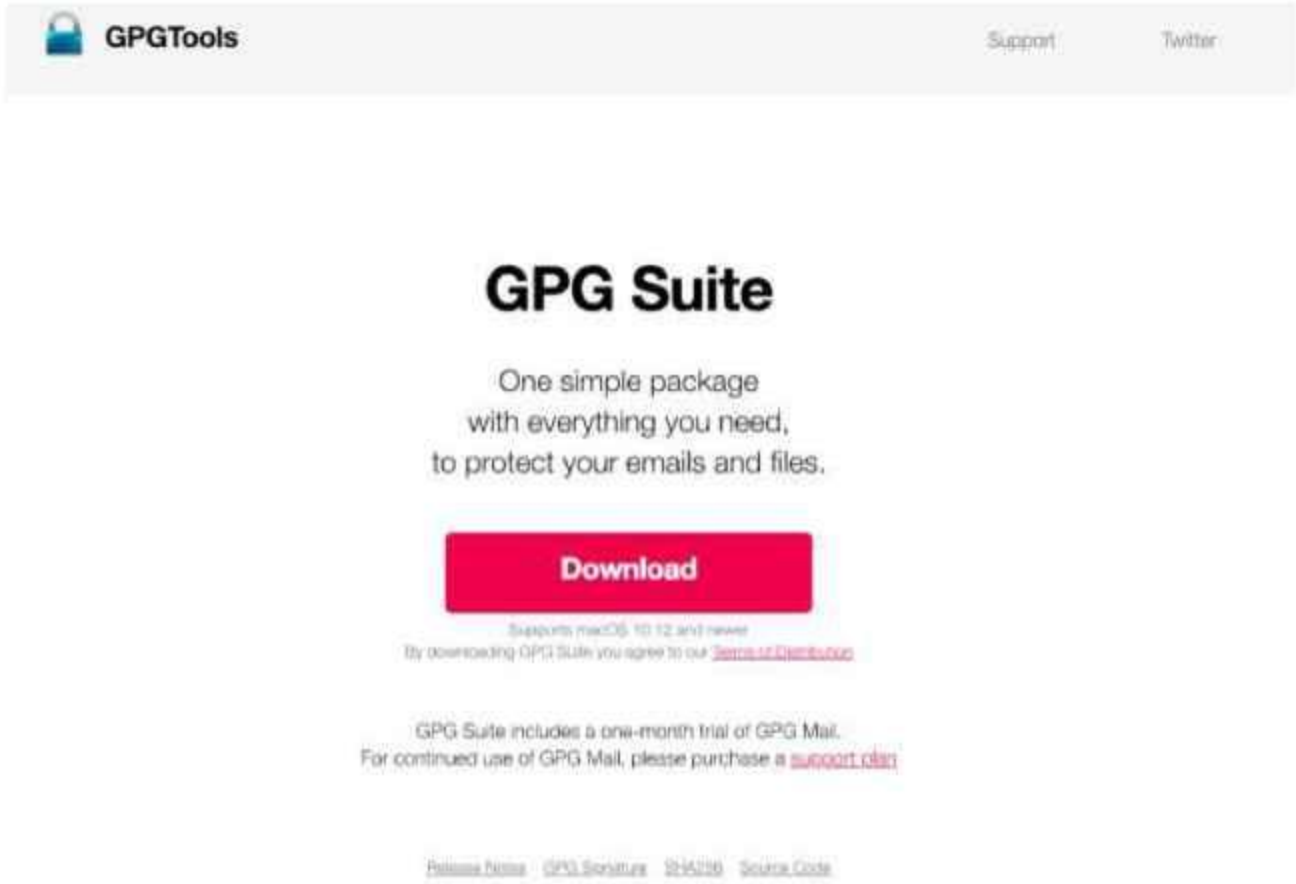


Рис. 1. Страница загрузки приложения GPG Suite

3. Откроется страница для загрузки приложения. Нажмите на кнопку **Download** для загрузки установочного файла приложения на компьютер.



4. Запустите установочный файл GPG_Suite-2018.5.dmg. Два раза нажимает по иконке коробки. (рис. 3).

Рис. 3. Установка приложения GPG Suite

5. Проходим все этапы установки

Рис. 4. Компоненты устанавливаемого приложения

6. Принимаем условия лицензионного соглашения GPG Suite (рис.5)

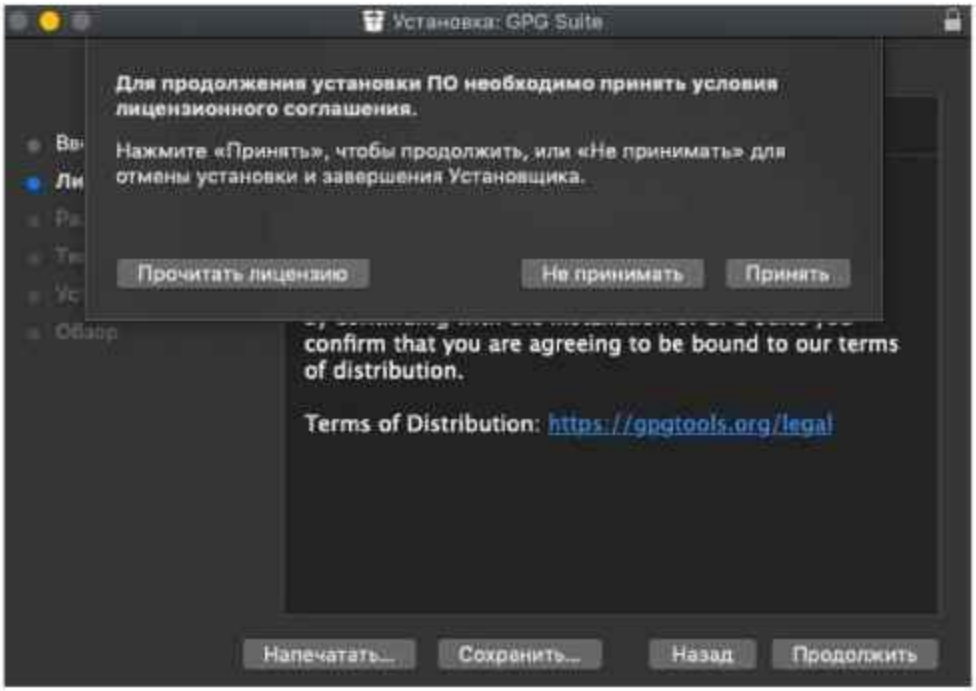


Рис. 5. Принимаем условия лицензионного соглашения GPG Suite

7. Нажмите кнопку «Установить». (рис. 6).

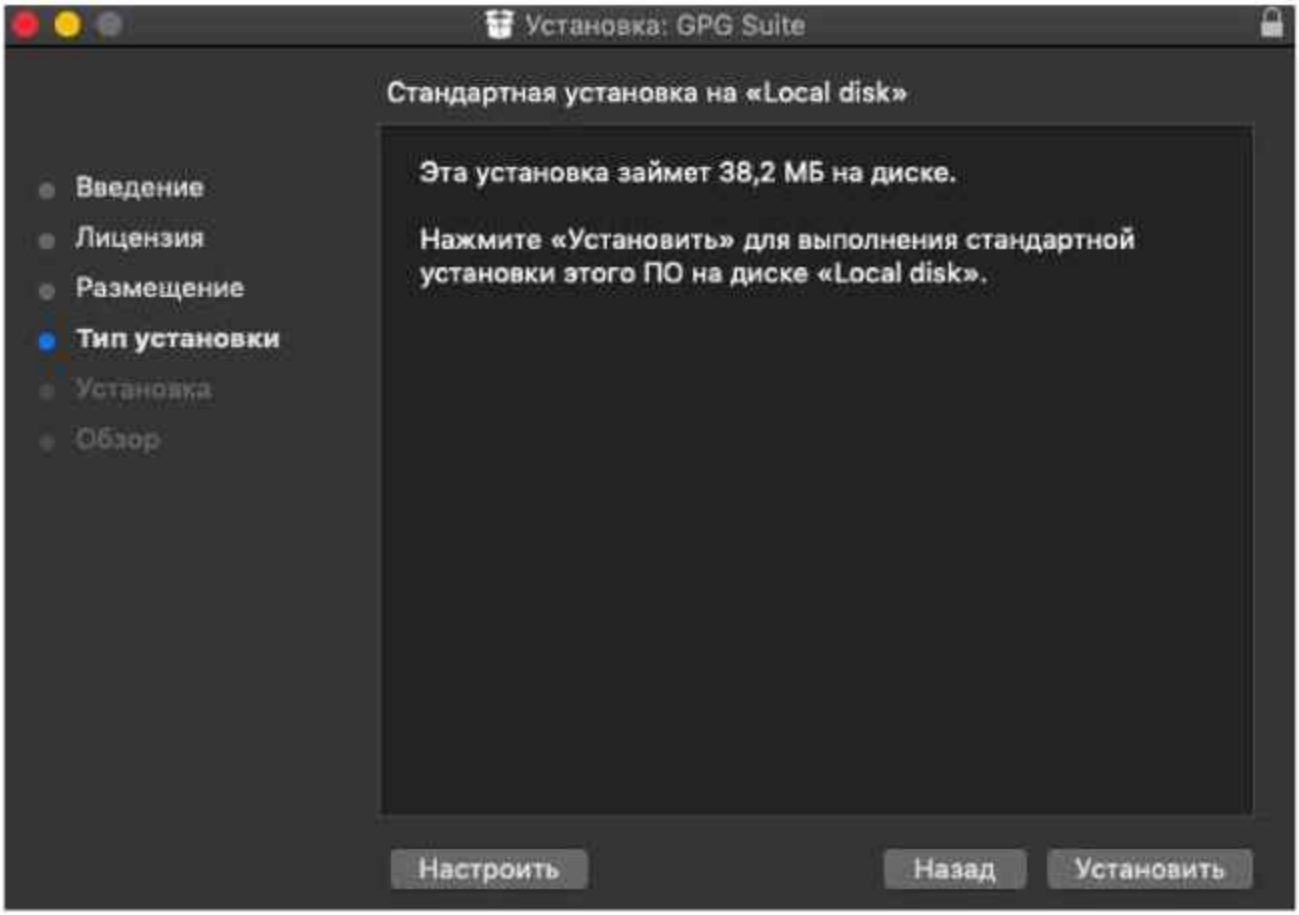


Рис. 6. Завершение установки приложения GPG Suite.

2 Создание пары ключей для шифрования и электронной подписи

1. Запустите приложение GPG Keychain (рис. 7)

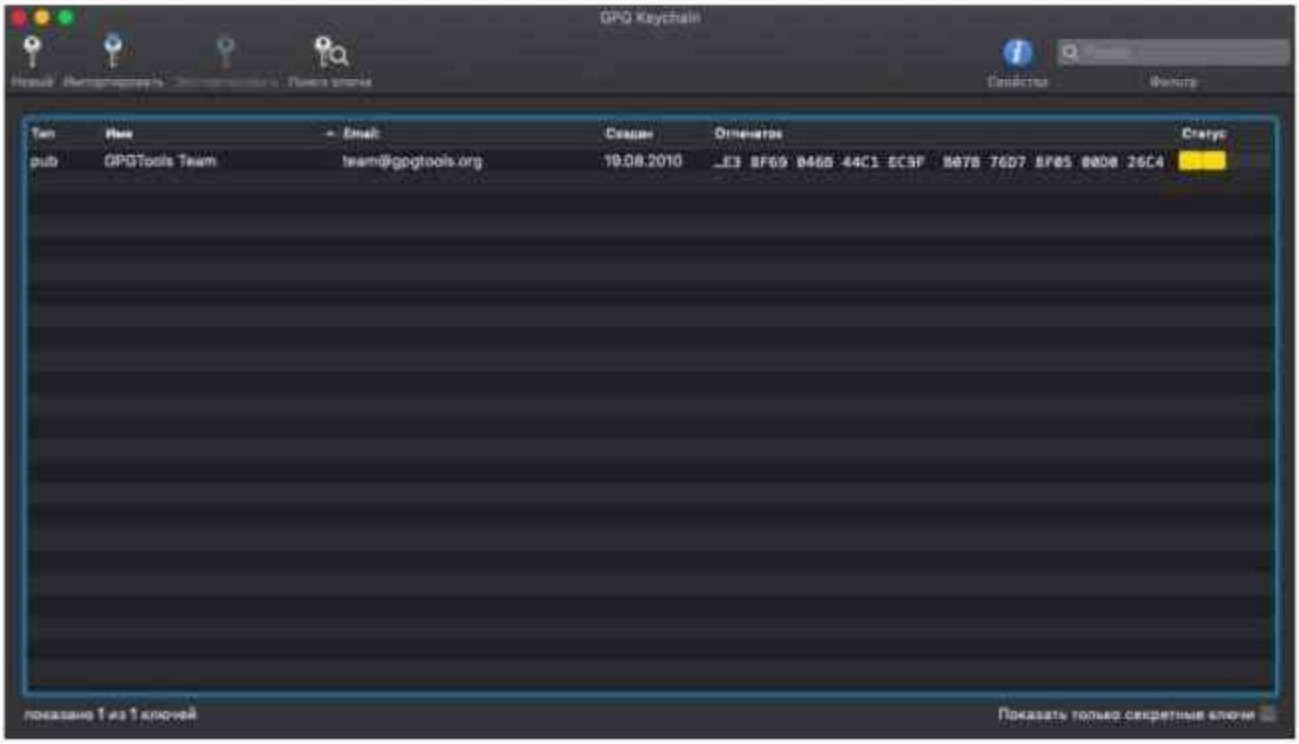


Рис. 7. Интерфейс приложения GPG Keychain

2. Нажмите кнопку «Новый». Появится окно «Сгенерировать новую пару ключей» (рис. 8). Введите свои регистрационные данные:

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

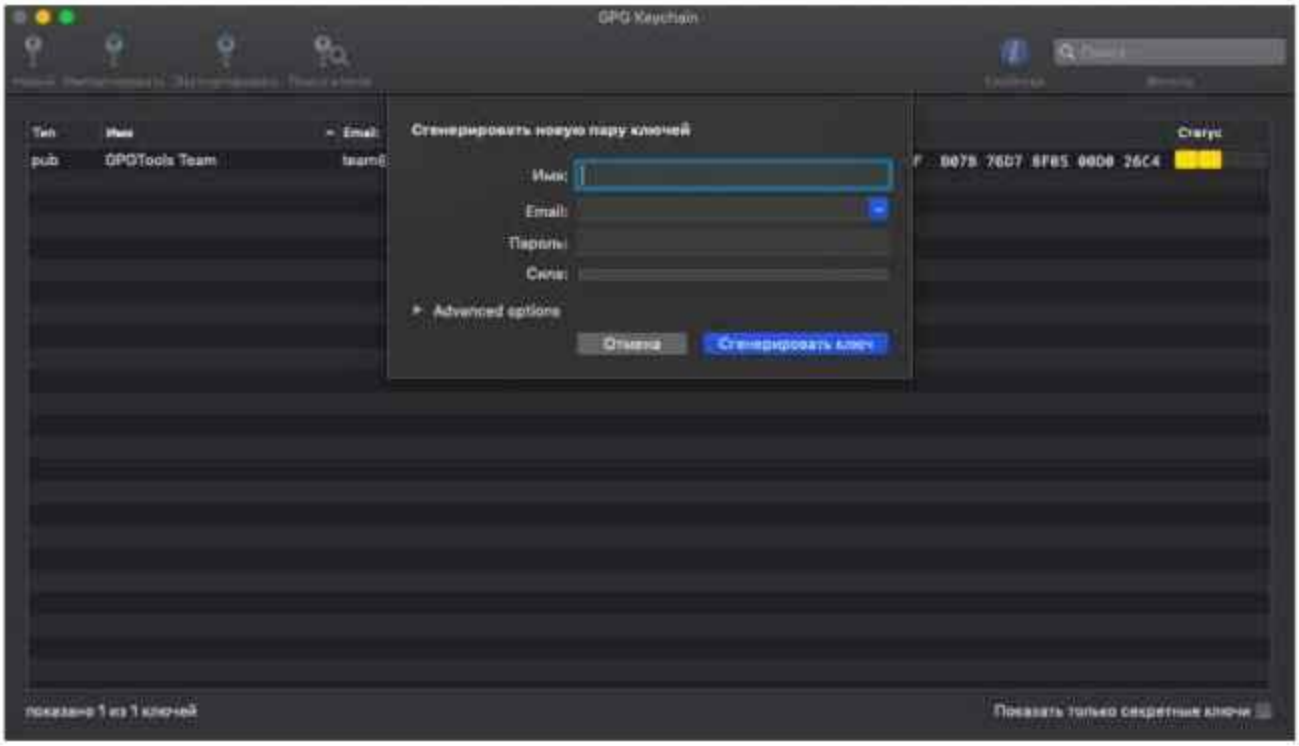


Рис. 8. Мастер создания пары ключей

3. Нажав кнопку «Advanced options» выйдет окно (рис. 9), с помощью которого имеется возможность выбрать:

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

b) длину ключа (2048, 3072, 4096 бит)

c) срок действия сертификата электронной подписи

d) и другие параметры

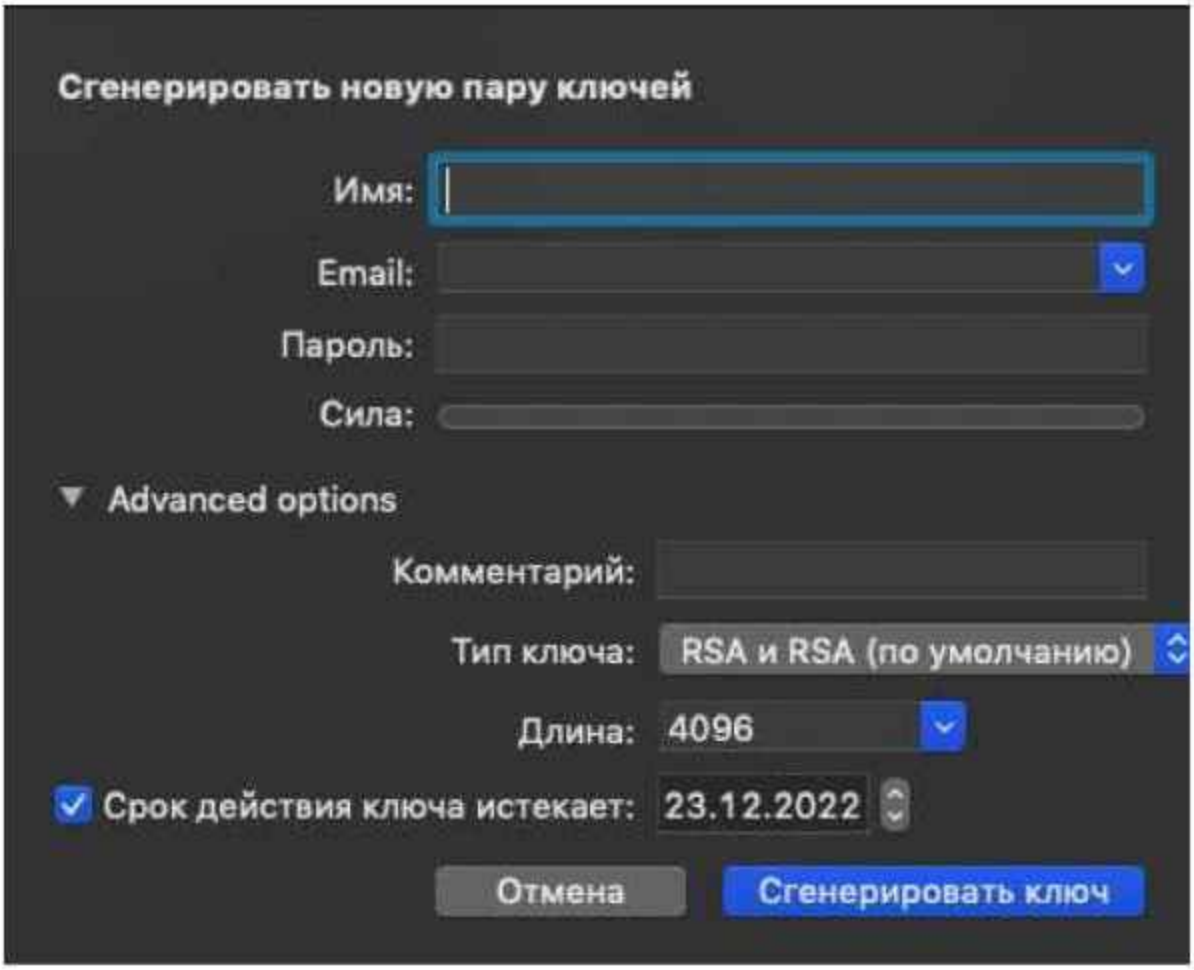


Рис. 9. Дополнительные параметры

4. Не изменяя настроек нажмите кнопку «Сгенерировать ключ».

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

идентификатора ключа (рис. 10). Полужирное начертание означает наличие пары ключей (открытого и закрытого).

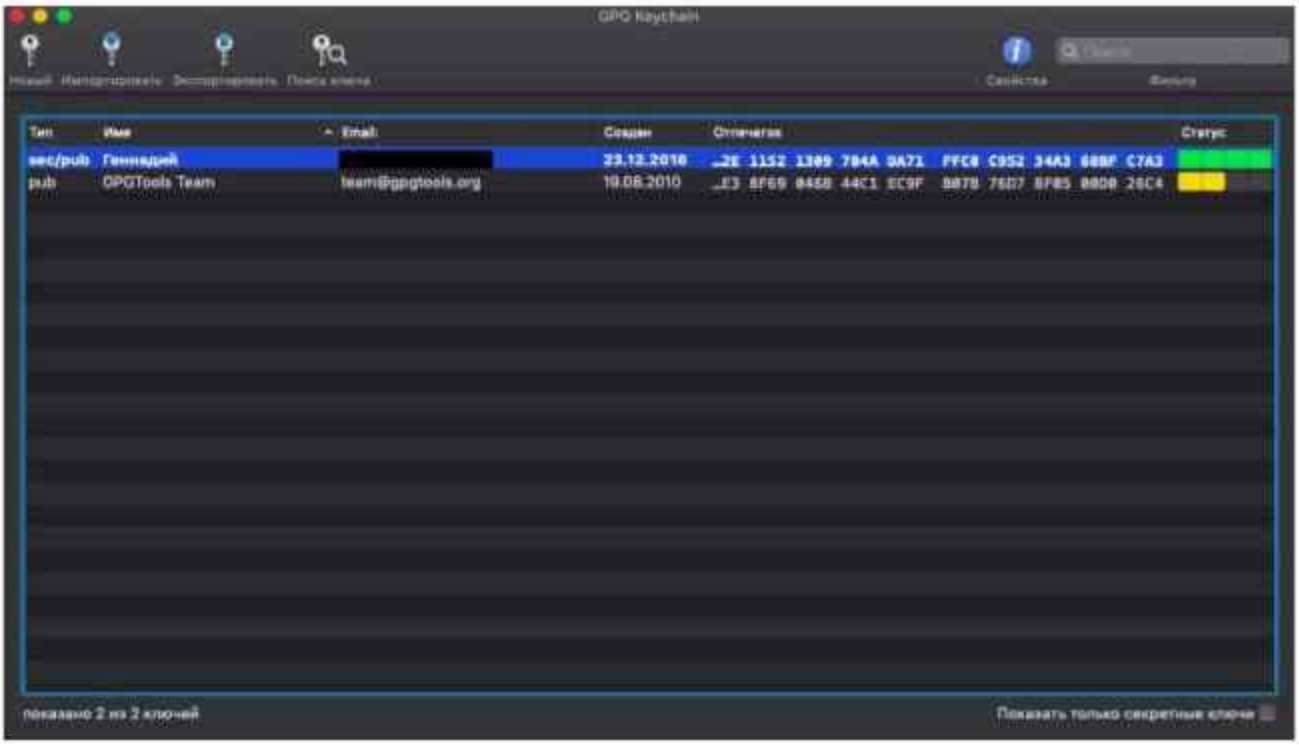


Рис. 10. Отображение сертификата в списке сертификатов после создания новой пары ключей

3 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 **«Экспортировать»**

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

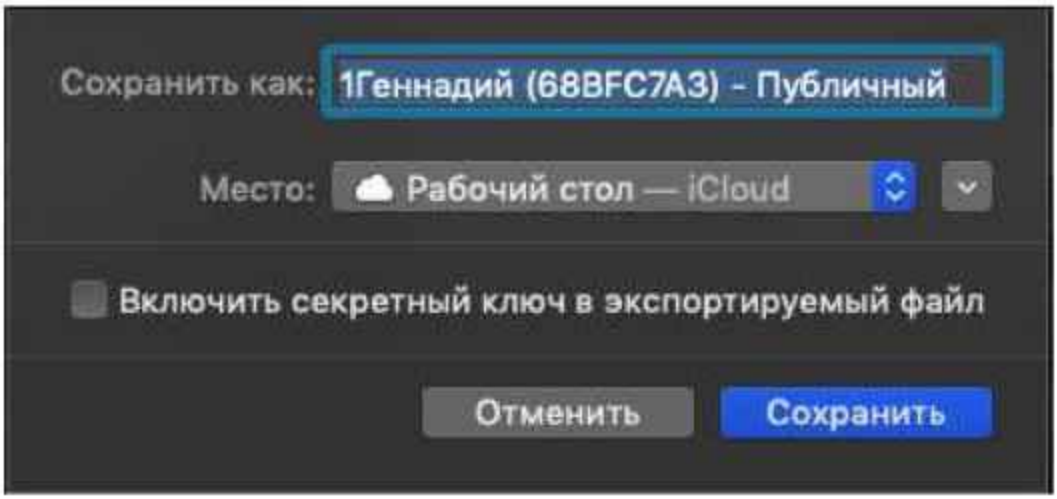


Рис. 11. Экспорт открытого ключа в файл

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

4 Импорт стороннего открытого ключа (сертификата)

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

2. Нажмите кнопку **«Импортировать»**

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

8. Появится сообщение **«Импортирование успешно»**. Нажмите **«Ок»**.

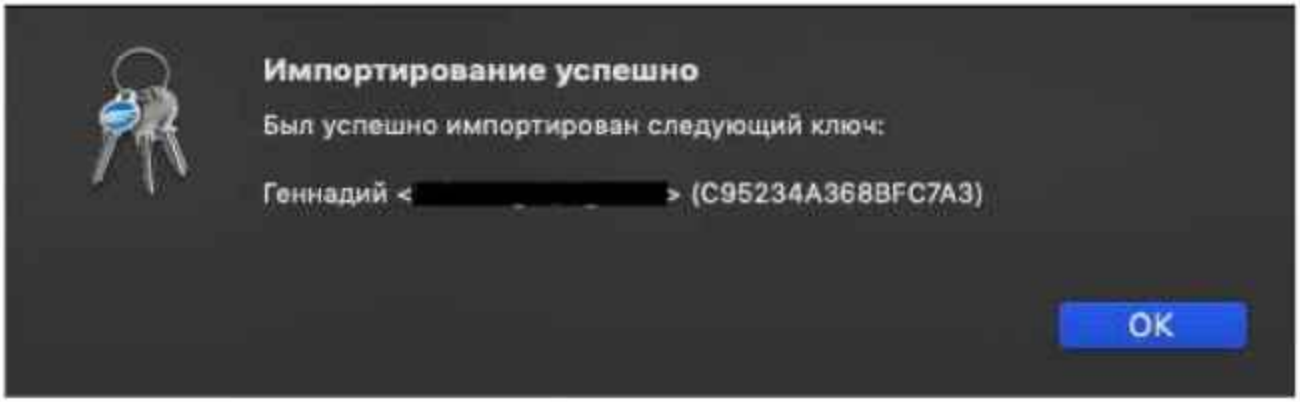


Рис. 12. Завершение процесса импортирования сертификата.

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

5 Шифрование и расшифрование файлов

В данной главе рассматривается шифрование и расшифрование файлов с помощью приложения GPG Suite с электронной подписью и без электронной подписи.

5 Шифрование и расшифрование файлов

5.1 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 GPG Suite используется ассиметричное шифрование, исходный файл будет зашифрован с помощью открытого ключа (сертификата) получателя. В предыдущих разделах был рассмотрен обмен сертификатами с помощью операций экпорта 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».

3. После создания файла нужно нажать правой кнопкой мыши на файл и в пункте «Службы» выбрать кнопку **«OpenPGP: Encrypt File»**

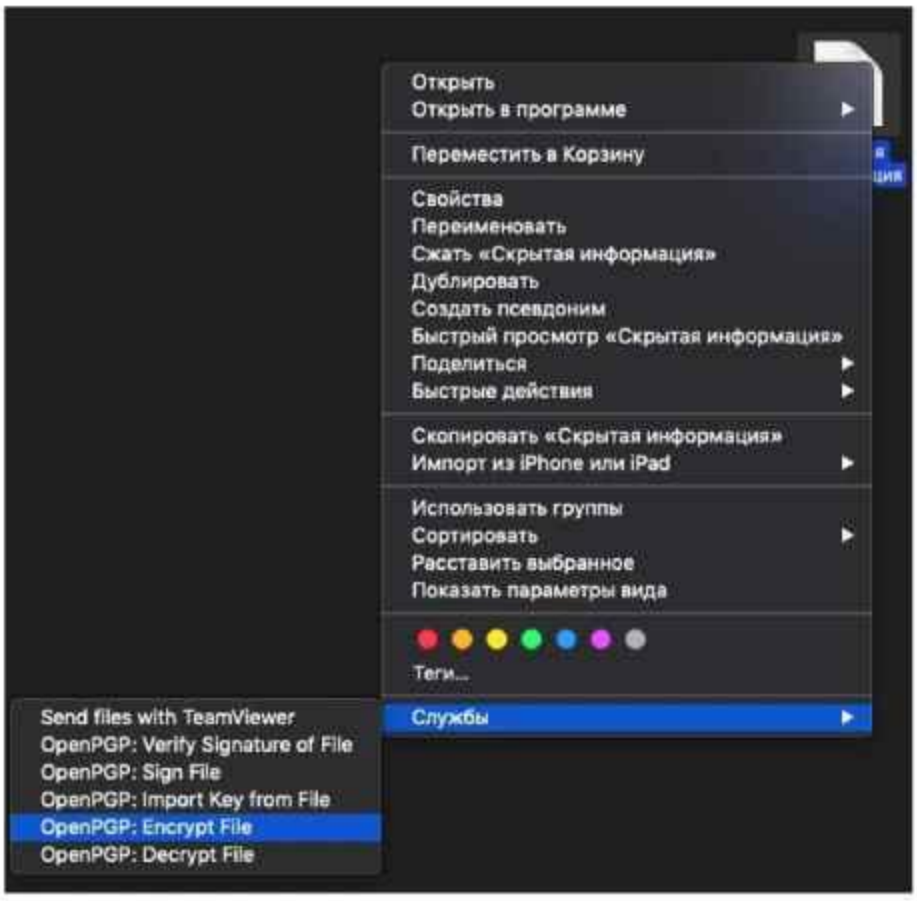


Рис. 13. Выбор операции шифрования файла

4. В появившемся окне выбираем (ставим галочки) в разделе Шифрование напротив пунктов **«Sign»** (на тот случай, если возникнет необходимость расшифровать зашифрованные файлы для собственного пользования)

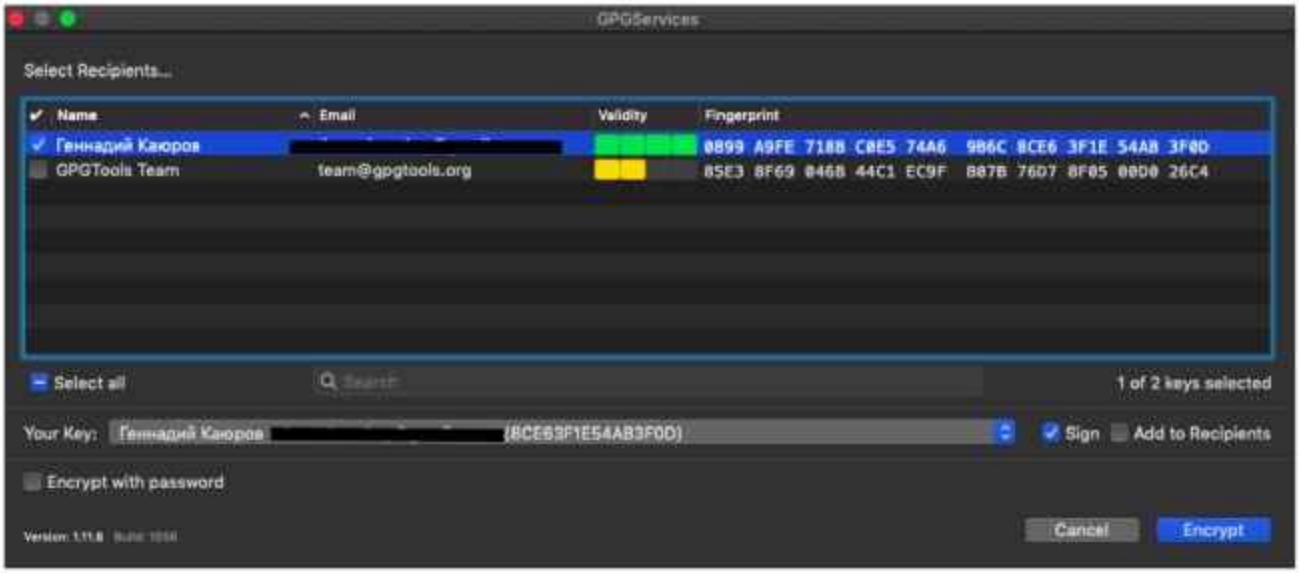


Рис. 14. Шифрование файла

5. 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 «Encrypt with password ставить не надо.

6. Далее необходимо нажать на кнопку **«Encrypt»**. Если шифрование произошло успешно, будет отображено следующее окно

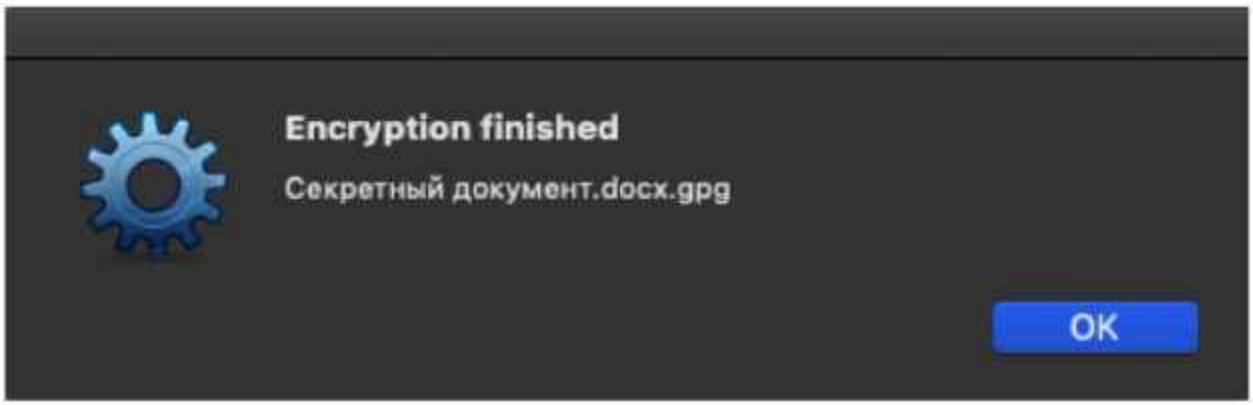


Рис. 15. Завершение шифрования файлов

7. После шифрования в назначенной директории появится зашифрованный файл **«Секретный документ.docx.gpg»**

8. Для расшифровки полученного файла необходимо в службах зашифрованного файла нажать на кнопку **«OpenPGP: Decrypt File»**

9. После ввода фразы-пароля нажмите **«ОК»**. Приложение расшифрует файл в текущую дерикторию.

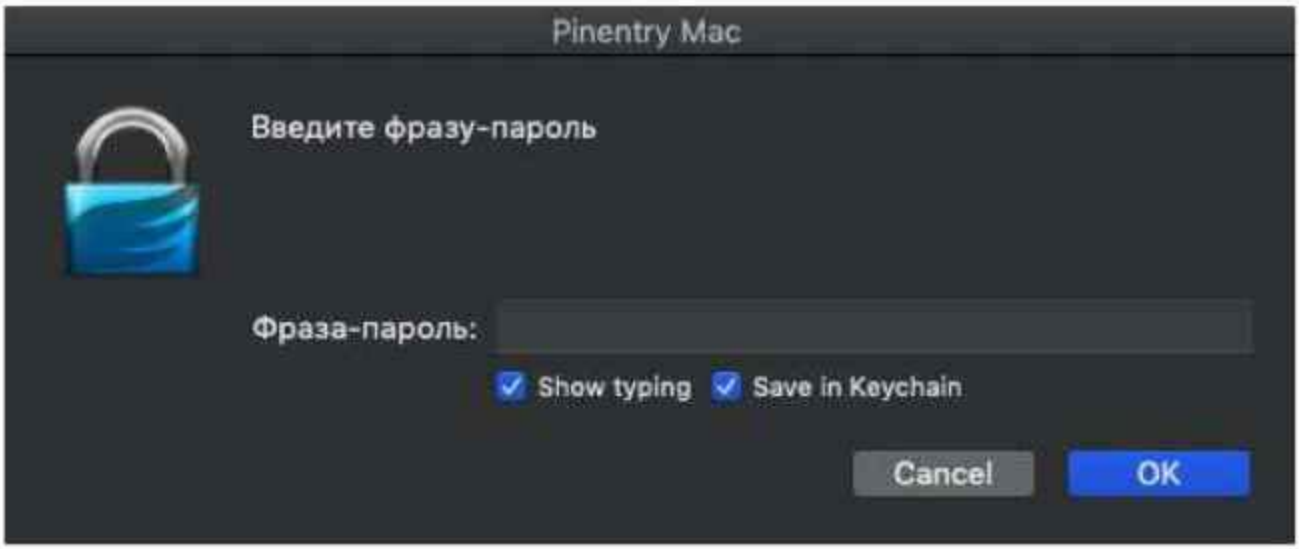


Рис. 16. Ввод фразы-пароля.

10. 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».*

5.2 Шифрование и расширование файлов с подписью

11. Если помимо шифрования необходимо, чтобы получатель мог установить кем был зашифрован файл, то можно дополнительно подписать зашифрованный файл сертификатом отправителя, поставив галочку напротив пункта **«Add to Recipients»** и выбрать нужный сертификат (см. п. 5 данного раздела). После шифрования приложение оповестит пользователя, что шифрование и подпись прошли успешно После этого нужно нажать кнопку **«Encrypt».**

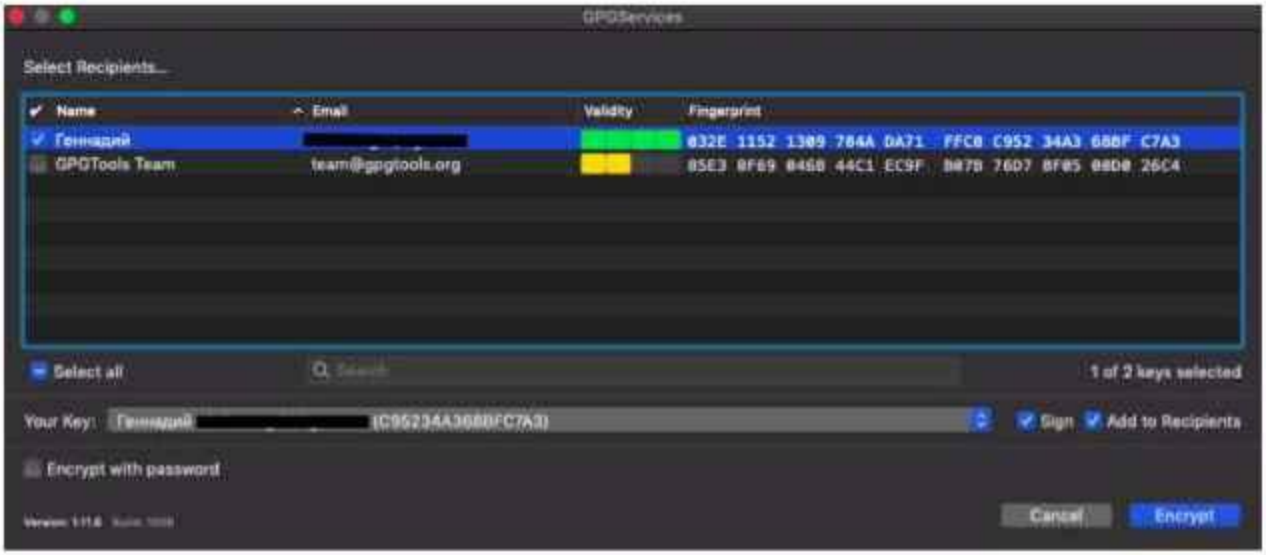


Рис. 17. Шифрование файла с подписью.

12. Тогда после расшифровки получатель увидит информацию о том, кем был подписан зашифрованный файл. Для закрытия окна и сохранения расшифрованного файла нажмите **«ОК».**

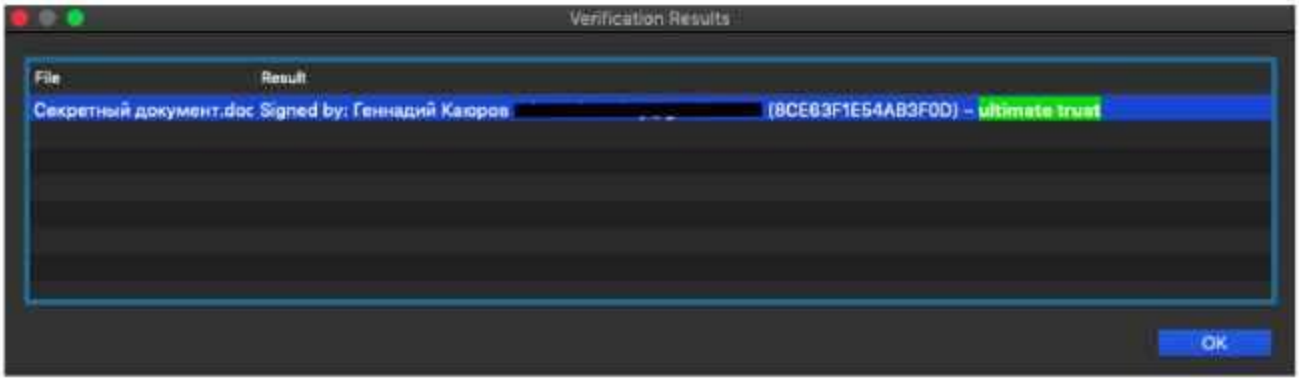


Рис. 18. Расшифровка файла и проверка подписи выполнены.

6 Электронная подпись для файлов и ее проверка

1. Приложение GPG Suite 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»** (п.2 предыдущего раздела).

3. Нажимаем правой кнопкой мыши на файл и в пункте «службы» выбрать кнопку **«OpenPGP: Encrypt File»**

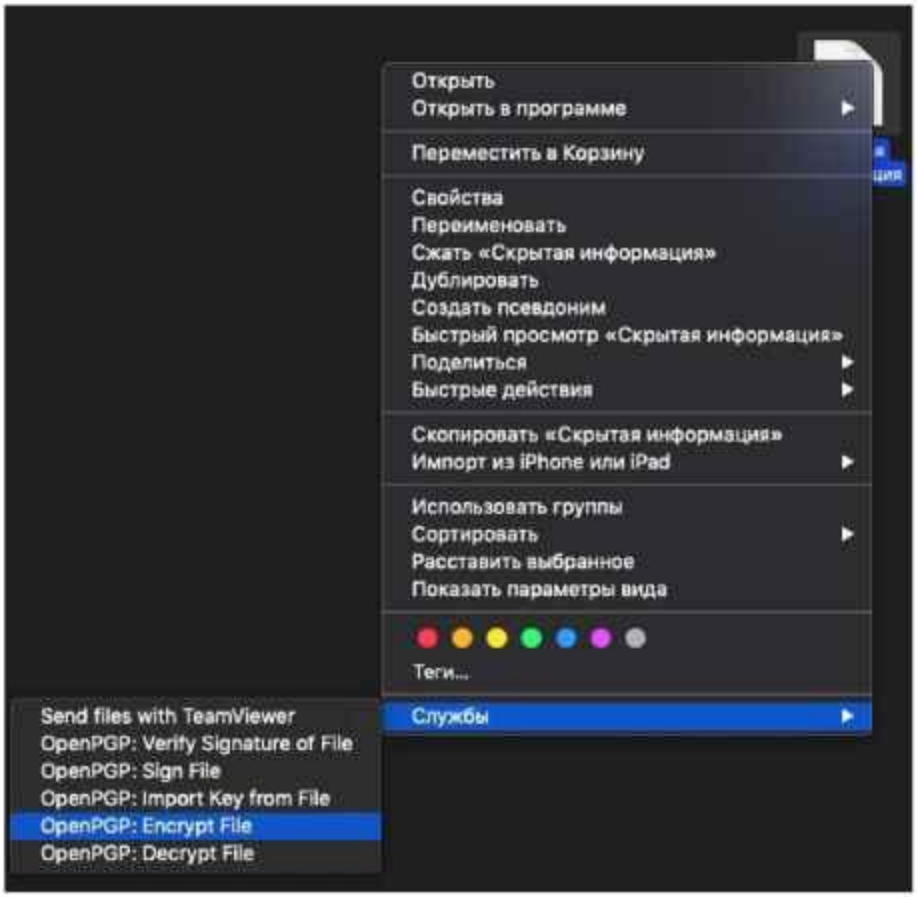


Рис. 19. Выбор операции формирования электронной подписи

4. В появившемся окне указываем **«Your Key»**. Выберите необходимый сертификат и нажмите кнопку **«Encrypt»**.

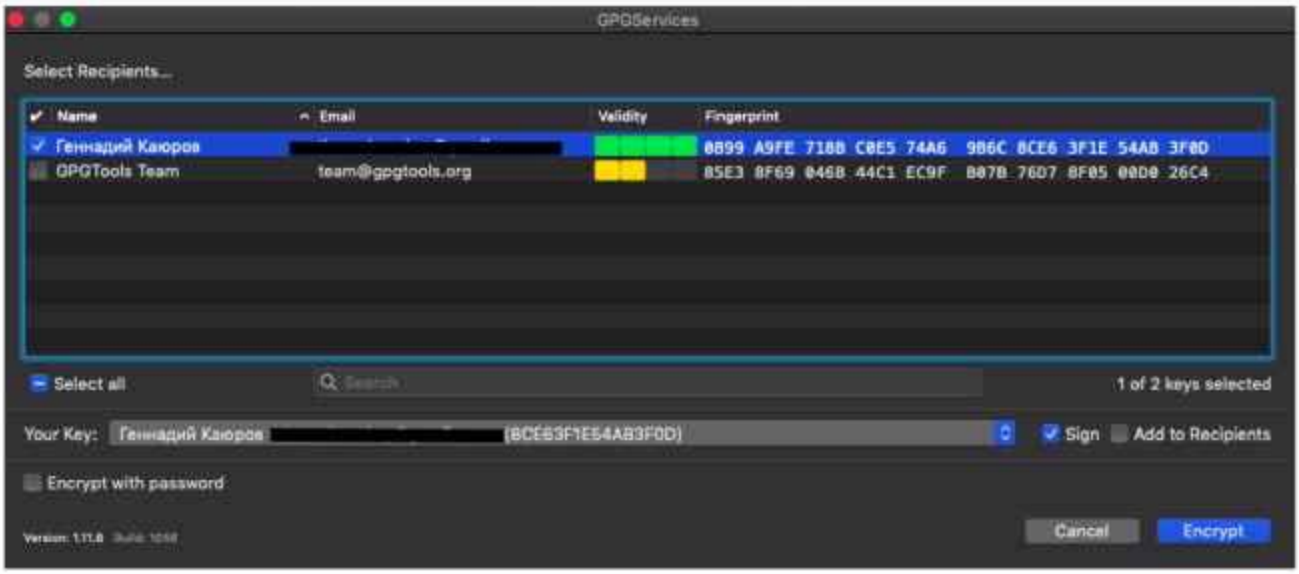


Рис. 20. Создание подписи

5. Введите фразу-пароль для разблокировки секретного ключа

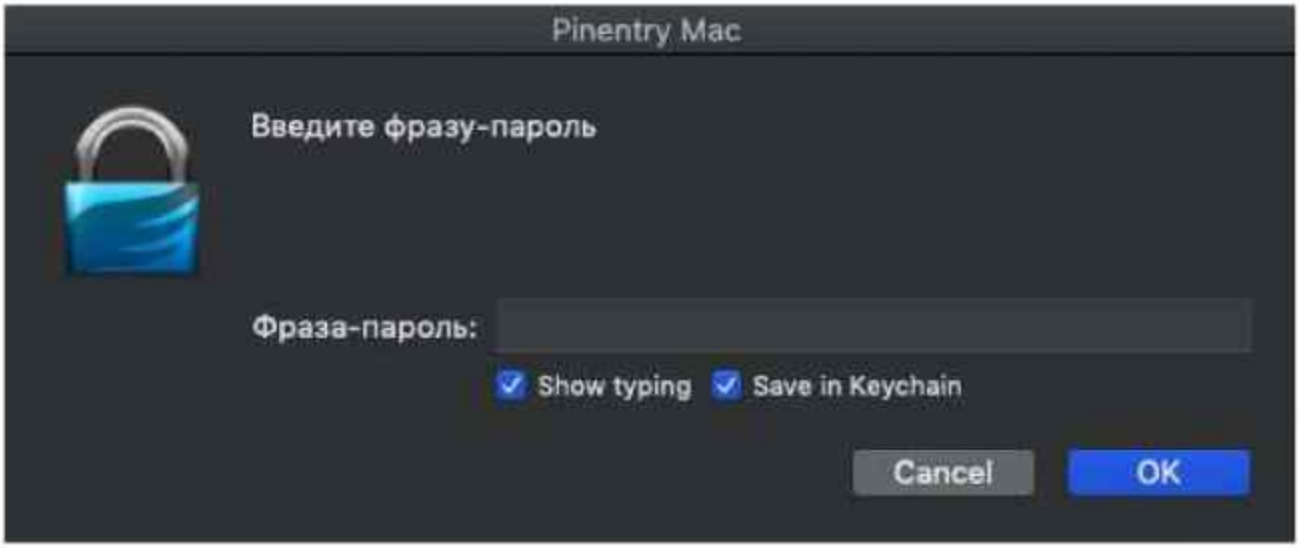


Рис. 21. Ввод фразы-пароля для подписи файла

6. Приложение оповестит пользователя о том, что файл успешно подписан. Необходимо нажать кнопку **«OK».**

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

8. Для расшифровки полученного файла необходимо в службах зашифрованного файла нажать на кнопку **«OpenPGP: Decrypt File»**

9. 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.

10. Если проверка подписи прошла успешно, приложение оповестит пользователя, что подпись действительна и покажет информацию о том, кем она была произведена.

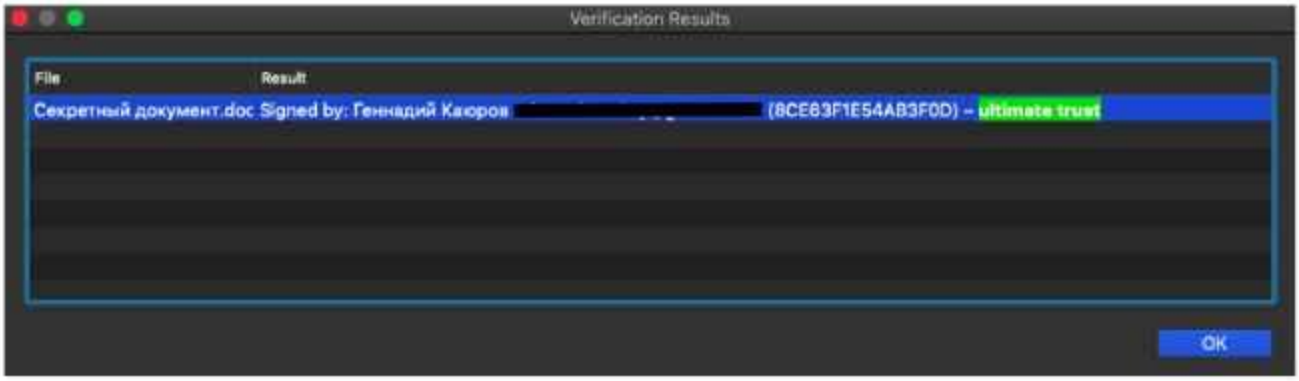


Рис. 22. Подтверждение подписи

11. 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

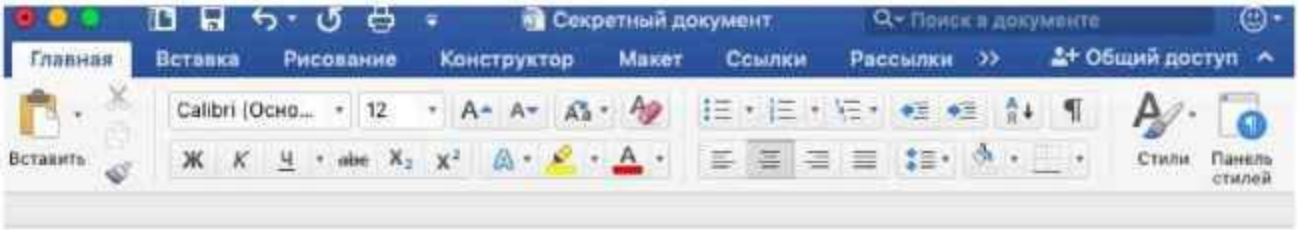


Рис. 23. Внесение изменений в подписанный документ.

13. Повторите действия, описанные в п.п. 8-10 данного раздела. Приложение оповестит пользователя о том, что подпись неверна.

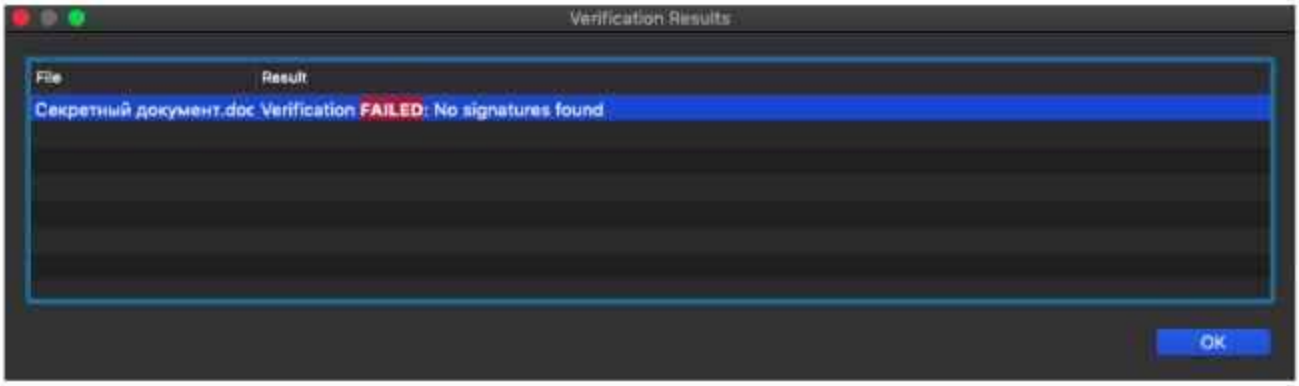


Рис. 24. Оповещение пользователя о неверной подписи.