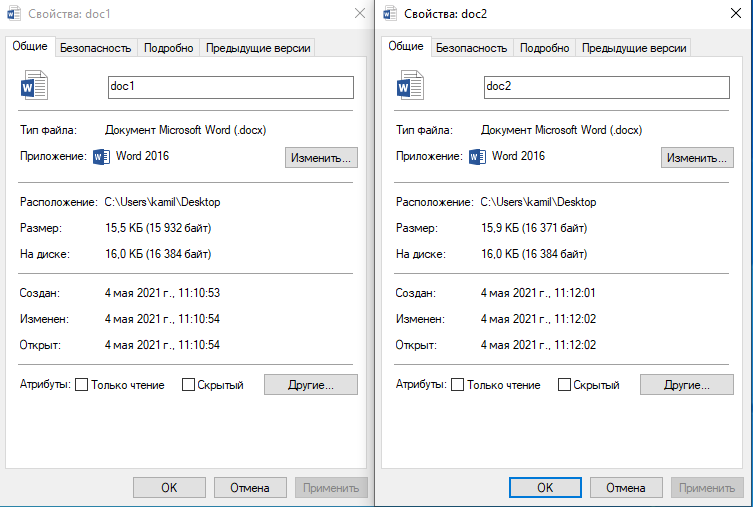
\*\*\*ТИТУЛЬНЫЙ ЛИСТ\*\*\*

1. Подготовим два файла формата .docx и запишем в них некоторый текст. Размеры документов представлены на рис. 1:



*Рисунок 1. Размер файлов doc1 и doc2*

2. Для того чтобы подписать цифровой подписью первый документ, выберем место, где будет располагаться подпись, последовательно зайдём: Вставка->Строка подписи->Строка подписи Microsoft Office. В диалогом окне “Настройка подписи” введём сведения, которые будут отображены под строкой подписи. В файле появится место подписи. Кликнув по нему ПКМ и выбрав меню “Подписать…”, выберем “Создать своё цифровое удостоверение”. В окне подписи в поле рядом со значком X введём свою фамилию, чтобы добавить печатную версию подписи. Нажмём кнопку “Подписать” и получим уведомление о том, что подпись сохранена и необходимо подтвердить действие (рис. 2). Размер документа после пройденных действий можно увидеть на рис. 3. Он увеличился, потому что подпись, которую мы поставили, а следовательно, и ключи шифрования и т.д. – занимают определённое место.

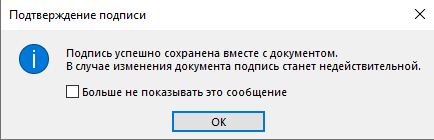


Рисунок . Подтверждение подписи

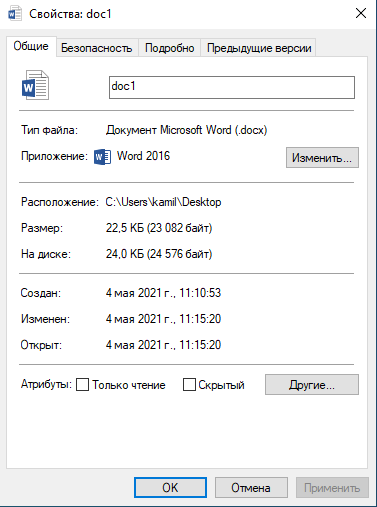


Рисунок . Размер документа doc1 после подписи

3. Чтобы создать подпись с электронным изображением своей реальной подписи, распишемся на листе бумаги, сфотографируем и загрузим в ПК. Пользуясь фоторедакторами, проследим, чтобы размер картинки был не более 2 см. Сохраним картинку в формате jpeg/png.

4. В качестве подписи второго документа doc2 будем использовать изображение рукописной подписи, результат приведён на рис. 4. Также проверим занимаемый файлом объём памяти (рис. 5).

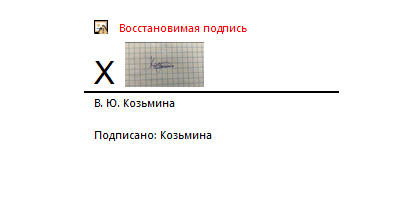


Рисунок . Подпись с рукописным форматом

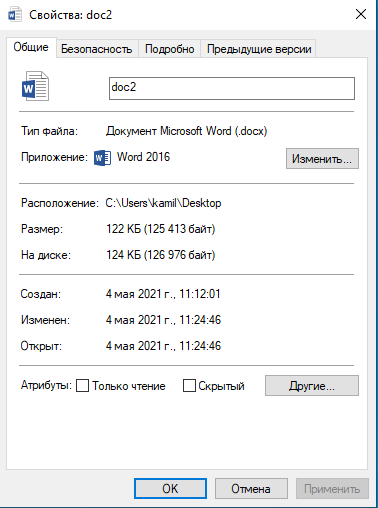


Рисунок . Размер документа doc2 после подписи рукописного формата

5. Изучим важные моменты состава подписи второго документа (рис. 6):

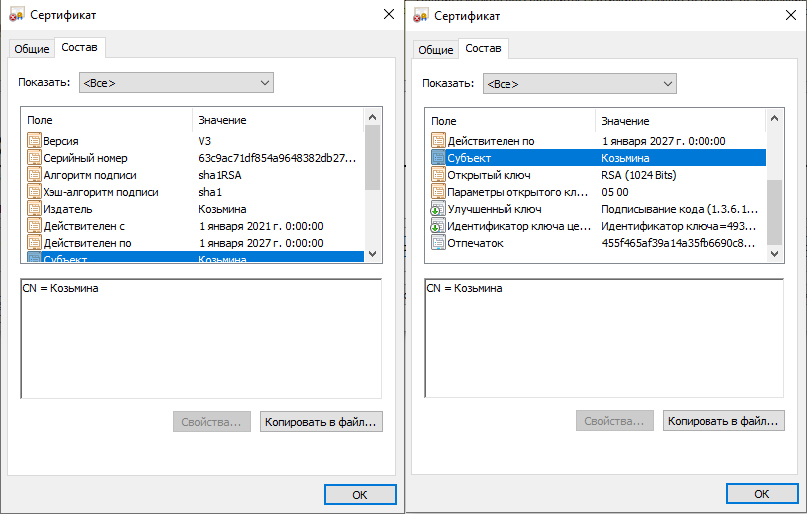


Рисунок . Состав подписи второго документа

– Серийный номер

По аналогии с серией и номером паспорта, серийный номер – уникальный для издателя код сертификата.

– Алгоритм подписи (DSA)

Криптографический алгоритм с использованием закрытого ключа для создания электронной подписи, но не для шифрования.

– Хэш-алгоритм подписи

Это функция, которая с помощью хеширования конвертирует ввод информации в числовую последовательность фиксированной длины. Он часто используется в алгоритмах электронно-цифровой подписи, где шифруется не само сообщение, а его хеш-код, что уменьшает время вычисления. Также в большинстве случаев вместо паролей хранятся значения их хеш-кодов.

– Издатель

Название удостоверяющего центра, выдавшего сертификат.

– Открытый ключ

Известен всем пользователям системы и необходим для проверки электронной подписи. С его помощью получатель документа устанавливат авторство документа и неизменность документа после подписания. RSA – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

– Отпечаток

Уникальный во всём мире код сертификата. Отпечаток однозначно идентифицирует конкретный сертификат.

6. Запишем сертификат в отдельный файл, нажав кнопку “Копировать в файл”. В качестве кодировки будем использовать DER. Это нужно, чтобы подтвердить принадлежность электронной подписи владельцу и содержит:

– закрытый ключ для генерации электронных подписей

– открытый ключ для проверки подлинности подписи получателем

– сведения о владельце для проверки получателем информации об авторе документа

7. Есть немало способов проверить подлинность и целостность файла. Один из способов – использование портала “Госулуги”. Для этого достаточно загрузить нужный файл в систему, ввести защитную капчу и нажать «Проверить». Если ЭЦП расположена в отдельном файле, то дополнительно нужно на портал загрузить и ее.

Результат проверки подписи будет представлен на отдельной странице — показан статус сертификата подписи, кто владелец подписи и в каком удостоверяющем центре она была выдана, а также её срок действия. Пример результата можно увидеть ниже, на рис. 7:

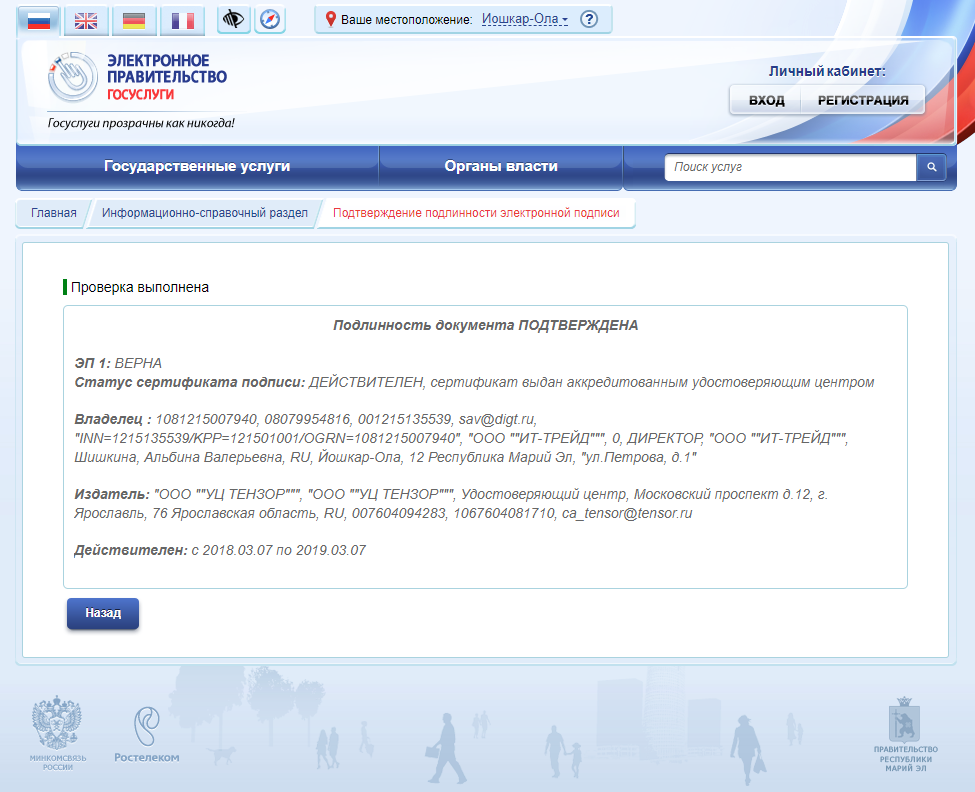


Рисунок . Проверка документа через портал "Госуслуги"

8. Чтобы удалить цифровую подпись из первого документа, зайдём в Файл->Сведения->Просмотр подписей. Произойдёт возврат к представлению документа, и появится панель “Подписи”. Необходимо щёлкнуть стрелку рядом с подписью и нажать на кнопку “Удалить подпись” (рис. 8).

9. Чтобы установить скрыту цифровую подпись, зайдём в Файлы->Сведения, нажать кнопку “Защита документа”, затем на кнопку “Добавить цифровую подпись” (рис. 9). В диалоговом окне “Подпись” в поле “Цель подписания документа” укажем цель подписания документа и щёлкнем элемент “Подпись”. Размер файла после указанных выше действий изображён на рис. 10.

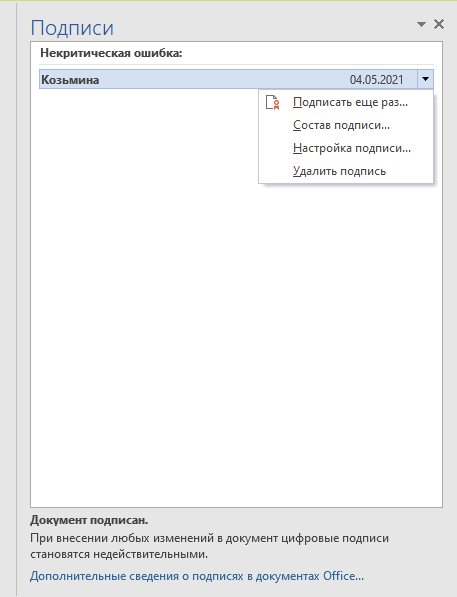


Рисунок . Удаление подписи

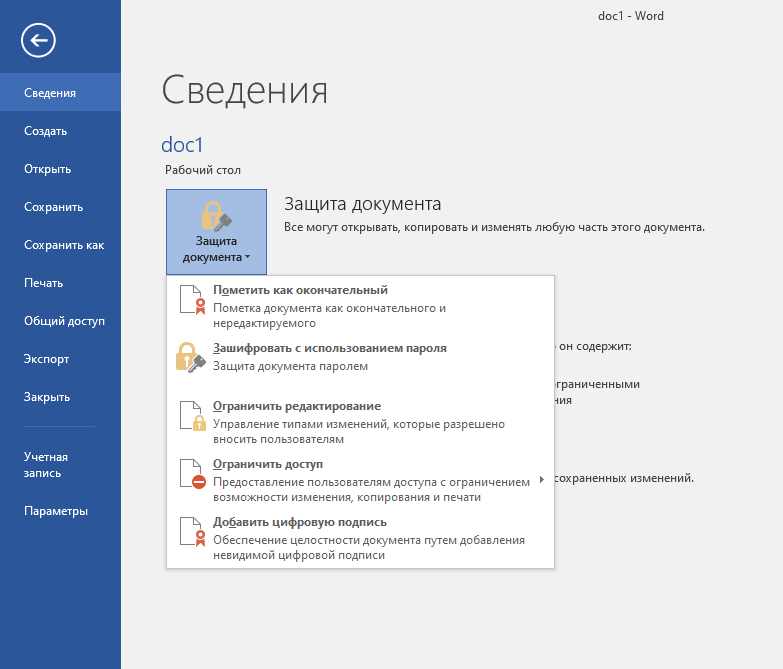


Рисунок . Добавление невидимой цифровой подписи

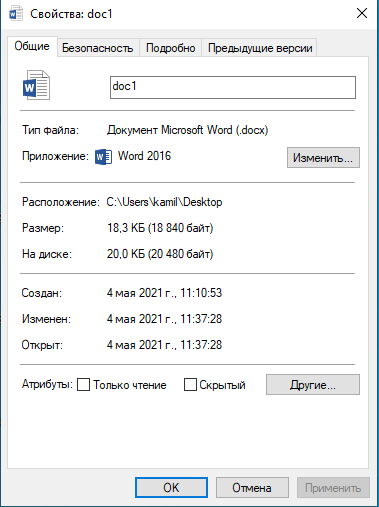


Рисунок . Размер файла doc1 после невидимой цифровой подписи

10. Определим параметры цифровой подписи первого документа, изображённых на рис. 11:

Версия: V3

Серийный номер: 63c9ac71df854a9648382db2789c5bf7

Алгоритм подписи: sha1RSA

Хэш-алгоритм подписи: sha1

Издатель: Козьмина

Действителен с: 1 января 2021 г. 0:00:00

Действителен до: 1 января 2027 г. 0:00:00

Субъект: Козьмина

Открытый ключ: RSA (1024 Bits)

Параметры открытого ключа: 05 00

Улучшенный ключ: Подписывание кода (1.3.6. 1.5.5.7.3.3)

Отпечаток: 455f465af39a14a35fb6690c8c43e91be5cff00c

Параметры данной подписи совпадают с параметрами подписи на втором документе, что означает, что данные признаются целостными и достоверными.

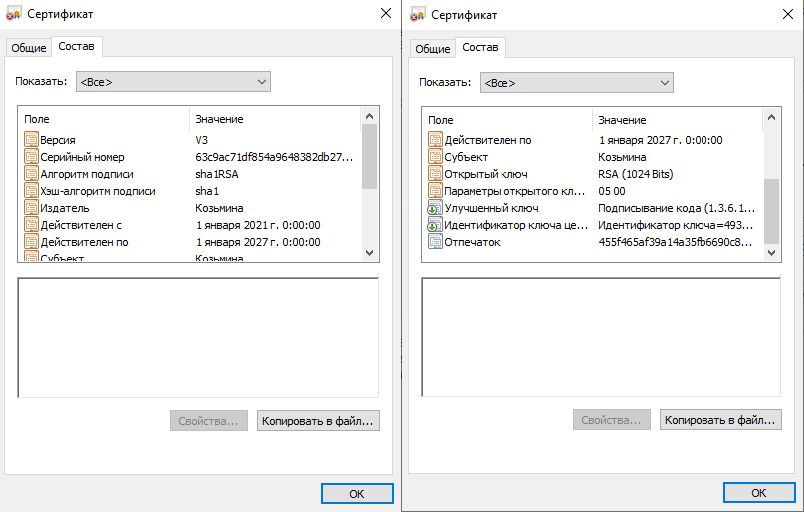


Рисунок . Параметры сертификата подписи документа doc1