

КриптоПро Office Signature

КРИПТОПРО OFFICE SIGNATURE

Руководство пользователя

АННОТАЦИЯ

Настоящий документ содержит описание процесса установки и эксплуатации программного обеспечения «КриптоПро Office Signature» (далее - Office Signature), для обеспечения возможности создания и проверки электронной подписи (ЭП) в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 для документов Word и Excel из состава Microsoft Office 2007/2010/2013/2016.

ЭП подписываются документы, редактирование которых завершено, для обеспечения гарантии подлинности, неизменности и авторства документа.

Документ предназначен для администраторов и пользователей как руководство по установке и эксплуатации «КриптоПро Office Signature».

Информация о разработчике ПК «КриптоПро Office Signature»:

127 018, Москва, Сушевский Вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

<http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

| | |
|--|-----------|
| 1. Установка Office Signature | 3 |
| 1.1. Требования к аппаратному и программному обеспечению..... | 3 |
| 1.2. Установка в интерактивном режиме | 3 |
| 1.3. Ввод серийного номера | 3 |
| 2. Неотображаемая электронная подпись..... | 5 |
| 2.1. Создание и проверка электронной подписи..... | 5 |
| 2.2. Подписание документа, содержащего цифровую подпись | 11 |
| 3. Строка подписи..... | 13 |
| 3.1. Добавление строки подписи..... | 13 |
| 3.2. Добавление электронной подписи в строку подписания..... | 14 |
| 3.3. Просмотр свойств электронной подписи | 19 |
| 4. Настройка Office Signature | 23 |
| 4.1. Алгоритм хеширования содержимого контейнера документа | 23 |
| 5. Программное создание и проверка ЭП в документах MS Office..... | 24 |
| 5.1. Средства автоматизации MS Office | 24 |
| 5.2. КриптоПро .NET | 24 |
| 6. Перечень сокращений..... | 25 |

1. Установка Office Signature

1.1. Требования к аппаратному и программному обеспечению

КриптоПро Office Signature реализован как надстройка для Microsoft Office и функционирует во всех операционных системах Microsoft Windows, поддерживаемых Microsoft Office 2007/2010/2013/2016 (для процессоров x86/x64).

Требования к аппаратному обеспечению определяются требованиями ОС, на которой планируется эксплуатировать Office Signature.

Для выполнения криптографических операций необходим установленный КриптоПро CSP 3.6 и выше.

1.2. Установка в интерактивном режиме

Установка Office Signature осуществляется в следующем порядке:

1. Запустите с компакт-диска универсальный установщик

- **CryptoProOfficeSignature.exe**

или запустите установку пакета в соответствии с версией Microsoft Office:

- Для **32-разрядных** версий Microsoft Office – **xmlsigaddin-win32.msi**.
- Для **64-разрядных** версий Microsoft Office – **xmlsigaddin-x64.msi**.

После коротких подготовительных процедур на экране появится окно мастера установки. Следуйте подсказкам мастера.

2. Перезапустите офисные приложения.

1.3. Ввод серийного номера

Дистрибутив КриптоПро Office Signature поставляется с демонстрационной лицензией на 90 дней, по истечении этого срока при использовании плагина для подписи выводится сообщение об отсутствии действующей лицензии (см. Рисунок 1)

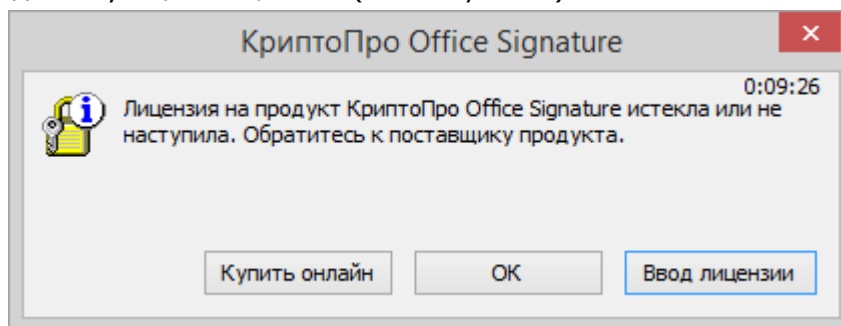


Рисунок 1. Предупреждение о необходимости лицензии

Для продолжения использования функционала надстройки необходимо приобрести и ввести серийный номер лицензии.

Также ввести серийный номер можно при установке в диалоге указания информации о пользователе (см. Рисунок 2)

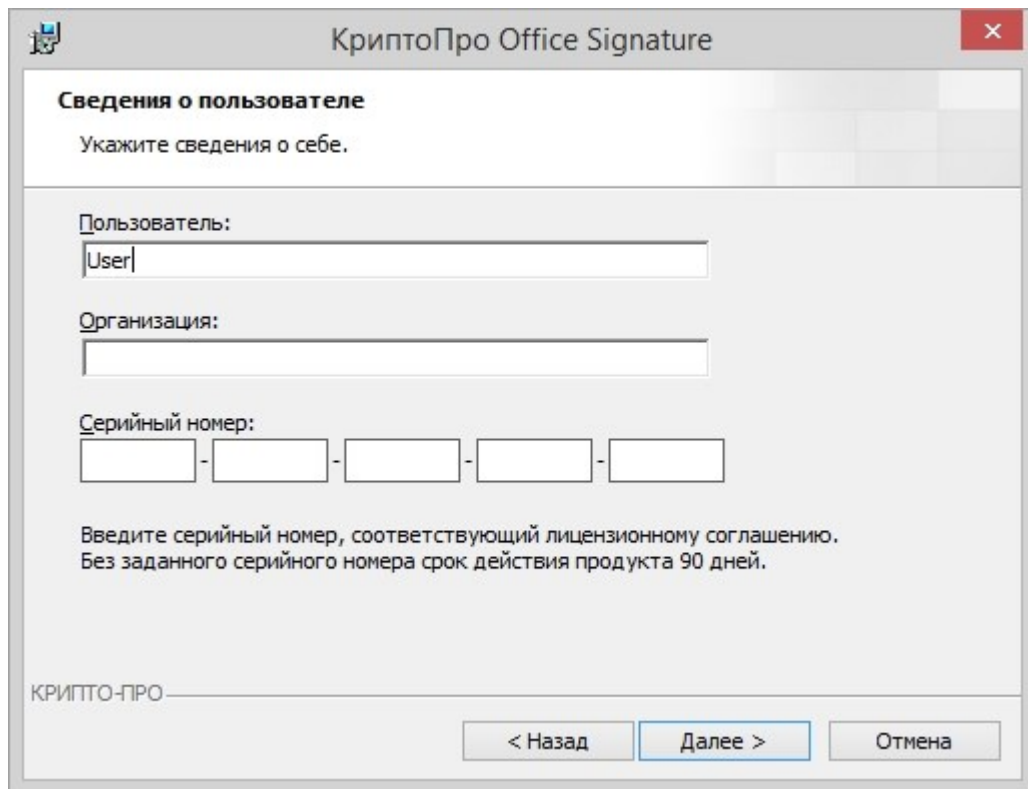


Рисунок 2. Сведения о пользователе

В любое время после установки серийный номер указывается через оснастку **Управление лицензиями КриптоПро РКІ** (доступна в меню **Пуск->КРИПТО-ПРО**, см. Рисунок 3)

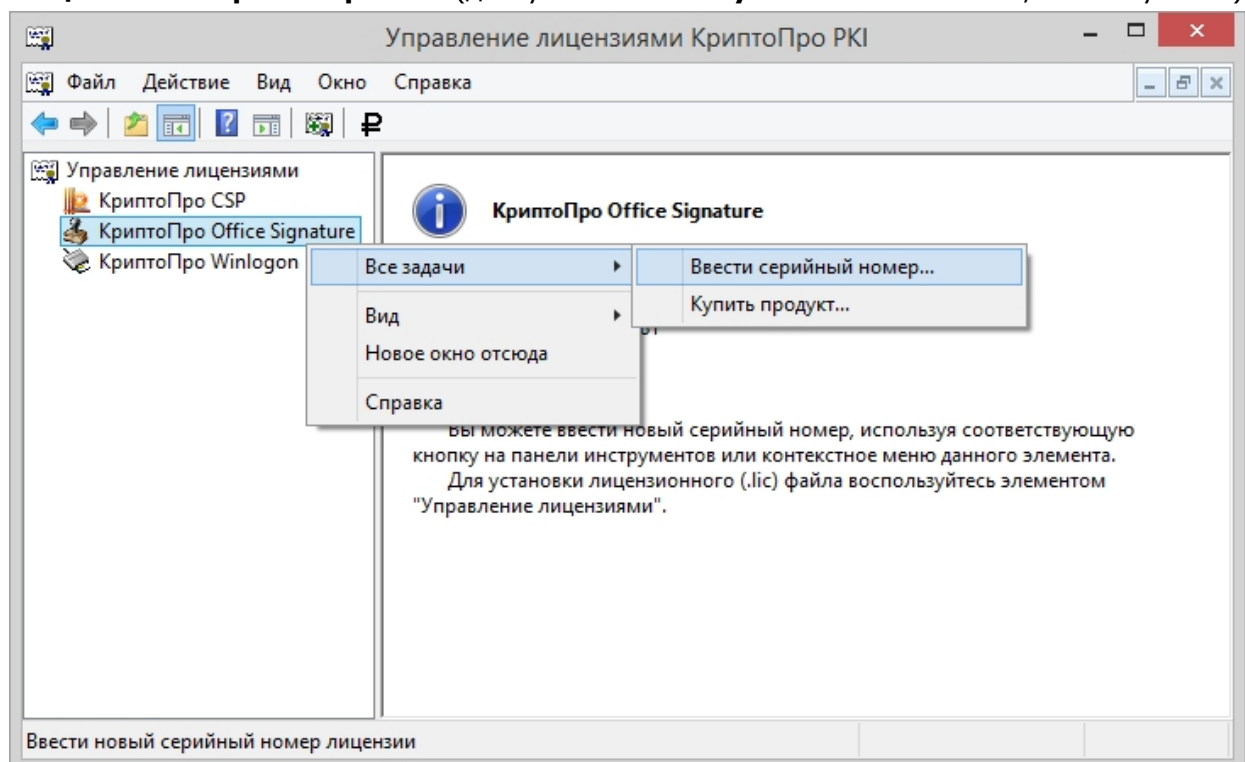


Рисунок 3. Управление лицензиями КриптоПро РКІ

2. Неотображаемая электронная подпись

2.1. Создание и проверка электронной подписи

После завершения редактирования и сохранения документа можно добавить электронную подпись к документу. Подписанный документ будет доступен только для чтения. Если в подписанный документ нужно внести изменения, то все созданные ЭП следует удалить из документа, поскольку они станут недействительными.

Ниже описывается работа с русскими версиями Microsoft Office.

Для создания неотображаемой электронной подписи в **Microsoft Office Word 2007** или **Excel 2007** в главном меню выберите пункт **Подготовить**, затем **Добавить электронную подпись (КРИПТО-ПРО)** (см. Рисунок 4)

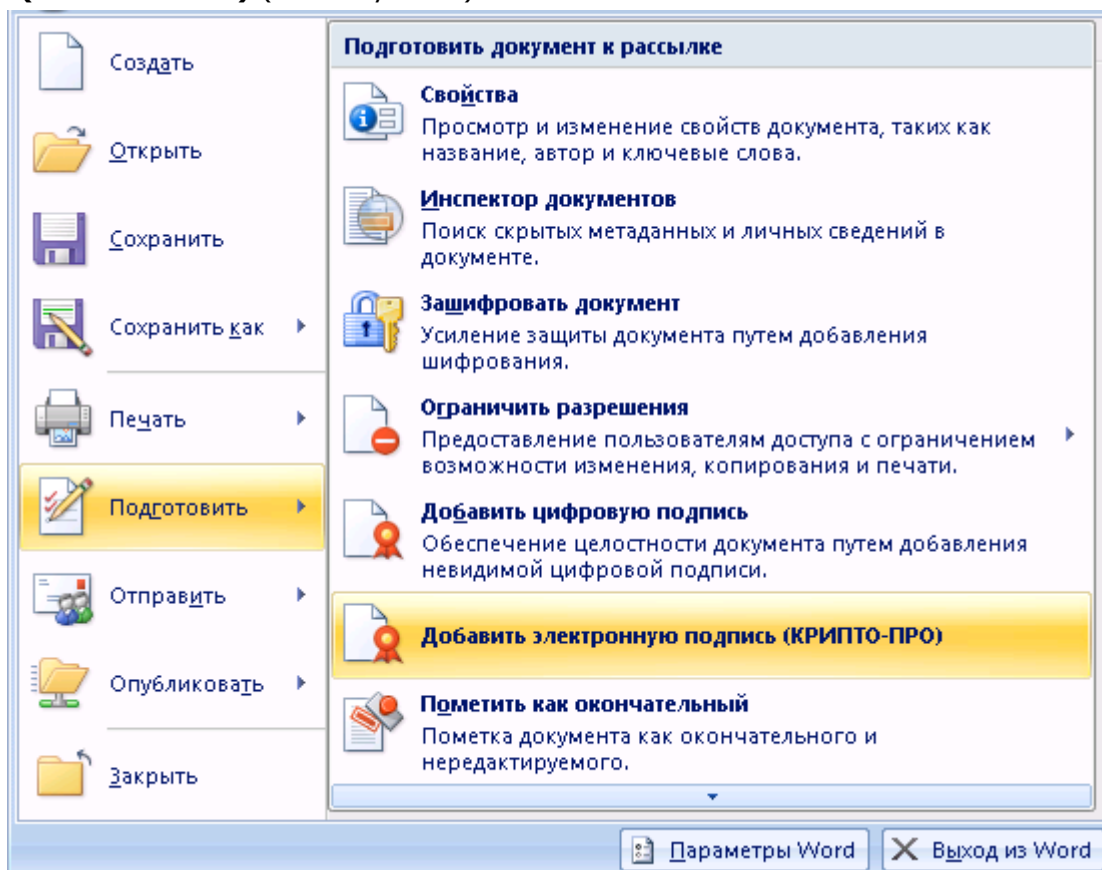


Рисунок 4. Добавление электронной подписи в Microsoft Word 2007

Для создания неотображаемой электронной подписи в **Microsoft Office Word 2010/2013/2016** или **Excel 2010/2013/2016** на вкладке **Файл** в разделе **Сведения** нажмите кнопку **Добавить электронную подпись (КРИПТО-ПРО)** (см. Рисунок 5)

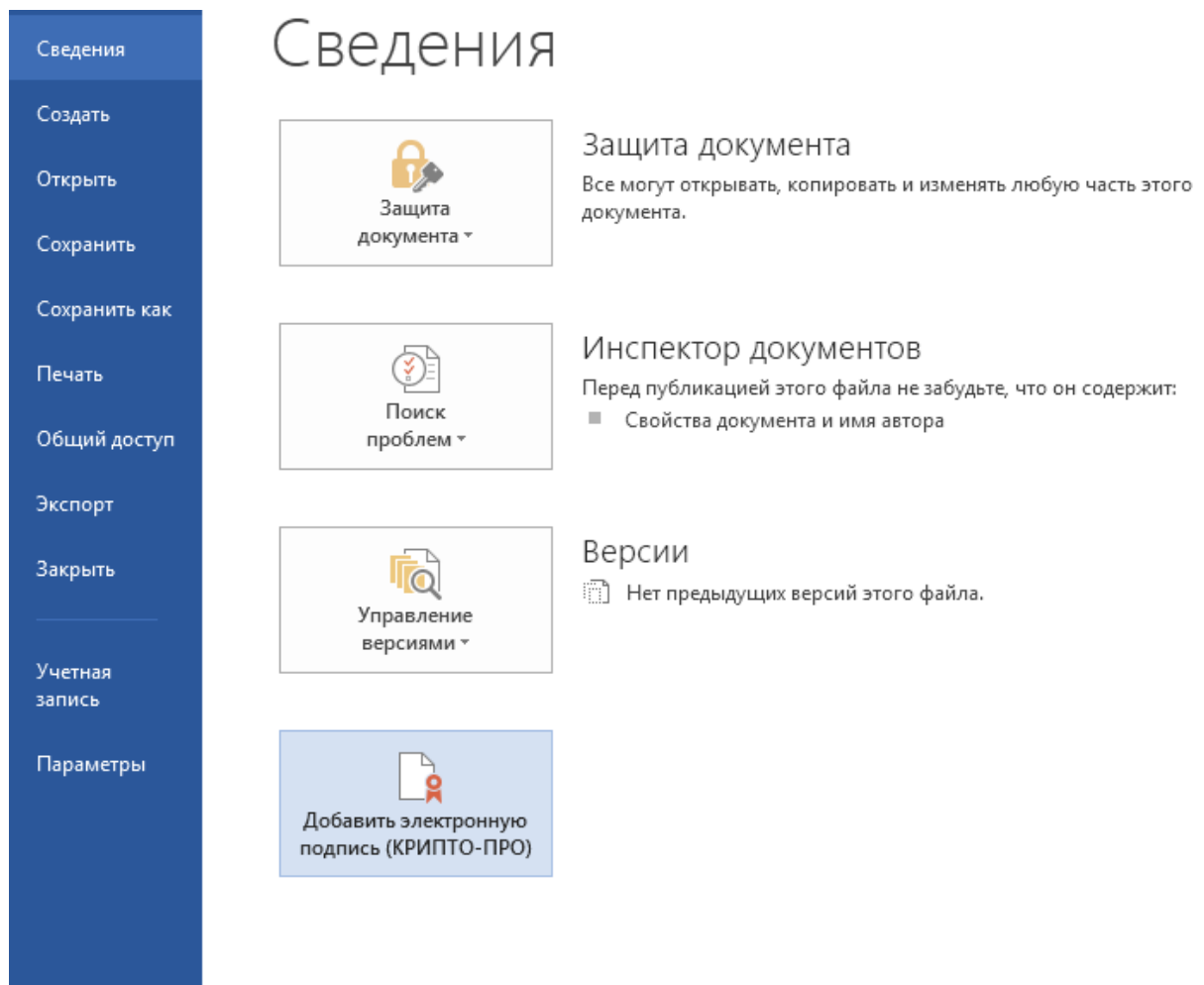


Рисунок 5. Добавление электронной подписи в Microsoft Office 2010/2013/2016

После этого появится диалог подписи документа, в котором нажатием кнопки **Изменить** можно выбрать личный сертификат подписи. После выбора сертификата нажмите **Подписать** (см. Рисунок 6).

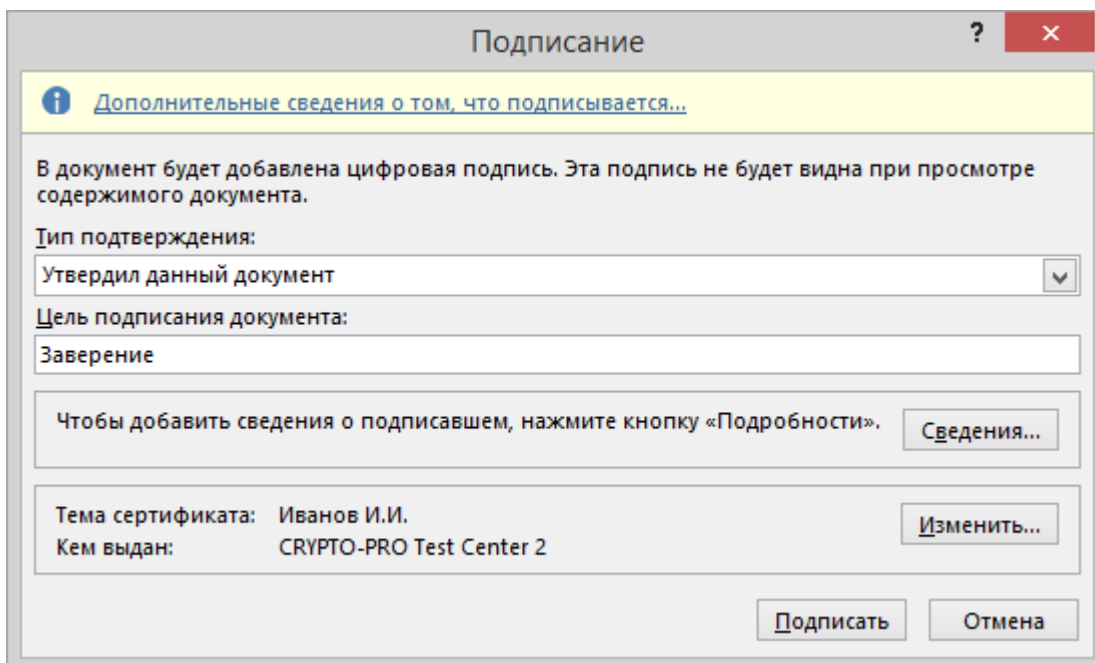


Рисунок 6. Подписание документа

Если для доступа к ключевому контейнеру требуется задать пароль - появится окно ввода пароля (см. Рисунок 7).

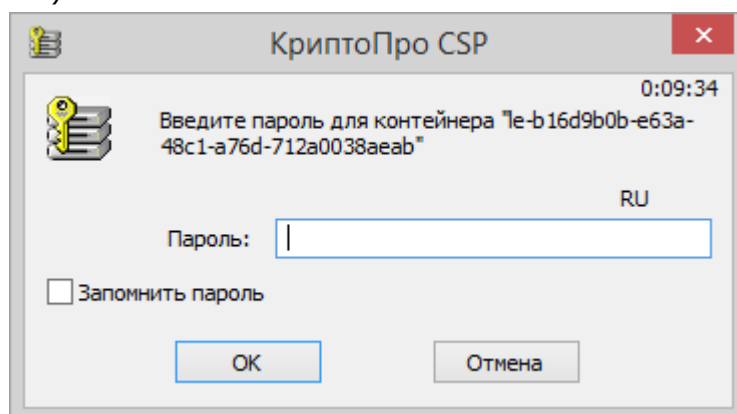


Рисунок 7. Ввод пароля для контейнера

Если пароль введен неверно, повторите попытку. При успешном вводе пароля появится сообщение о статусе подписания документа (см. Рисунок 8).

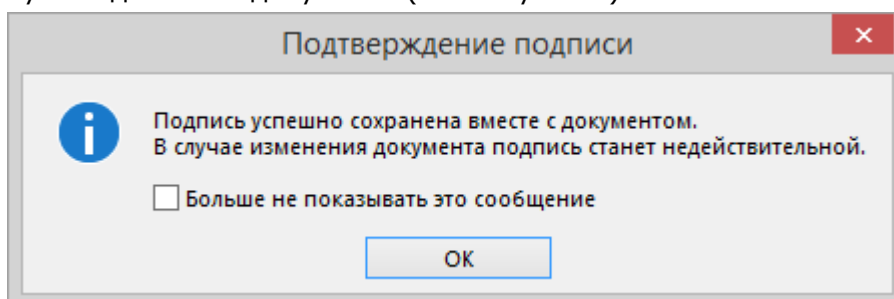


Рисунок 8. Сообщение о подтверждении подписи

После подписи документа в меню Файл, разделе Сведения выводится информация о том, что документ подписан и редактирование запрещено (Рисунок 9)

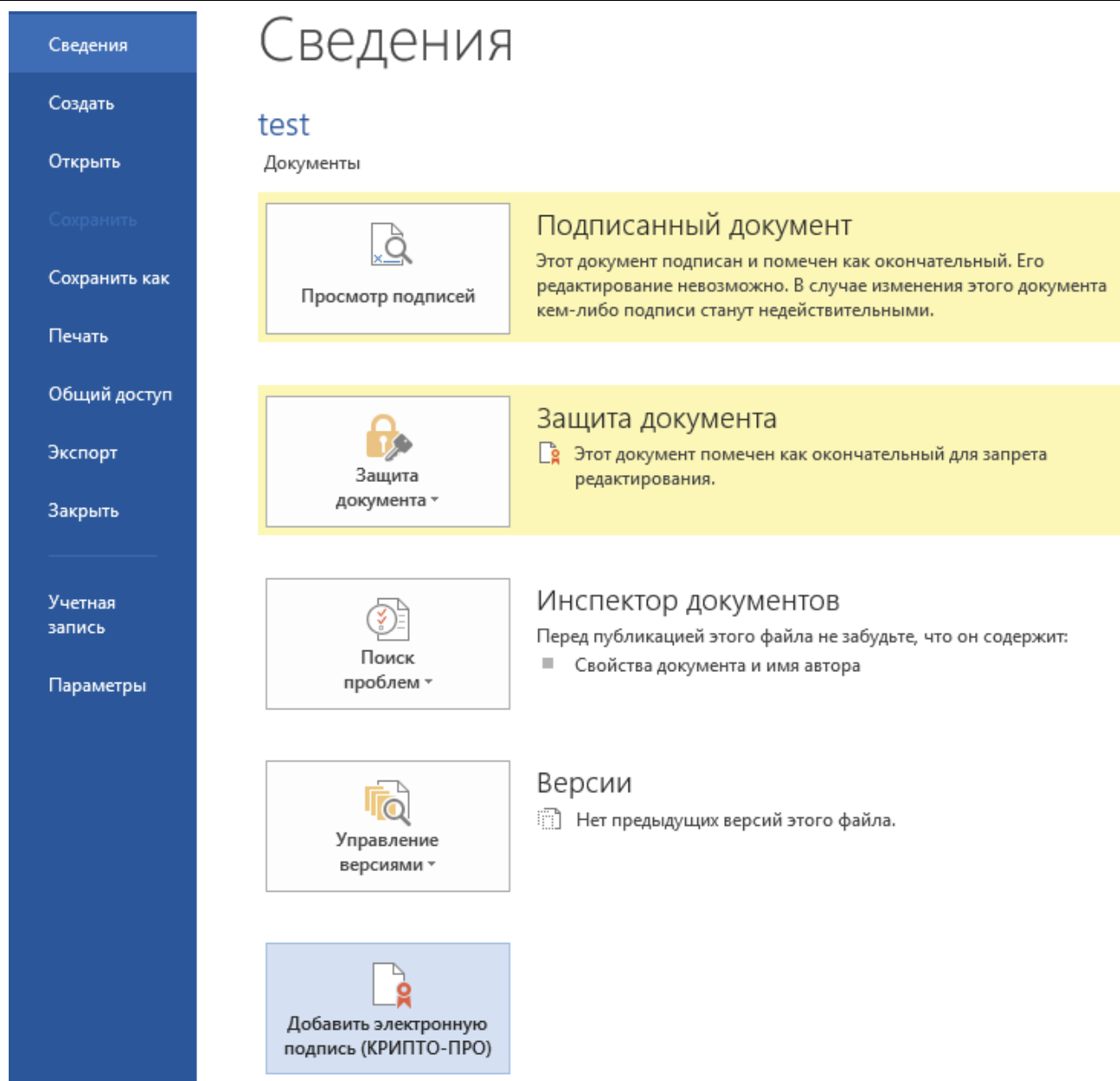


Рисунок 9. Сведения о подписанном документе

В строке состояния окна документа появится значок, свидетельствующий о том, что данный документ имеет электронную подпись (см. Рисунок 10).

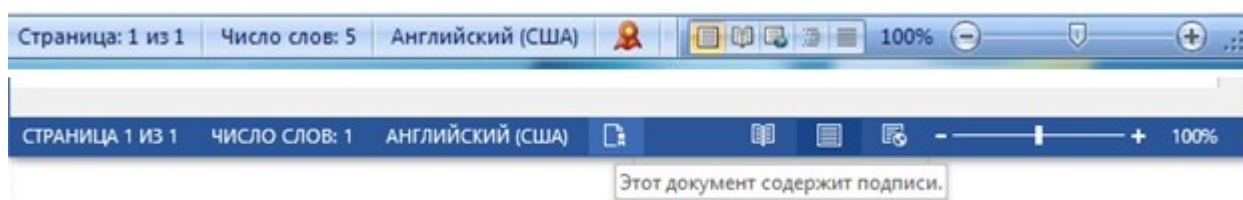


Рисунок 10. Строка состояния Microsoft Word 2007/2013/2016

Для проверки статуса подписи, нажмите на этот значок, и справа появится вкладка **Подписи**, в которой указан статус подписи (см. Рисунок 11).

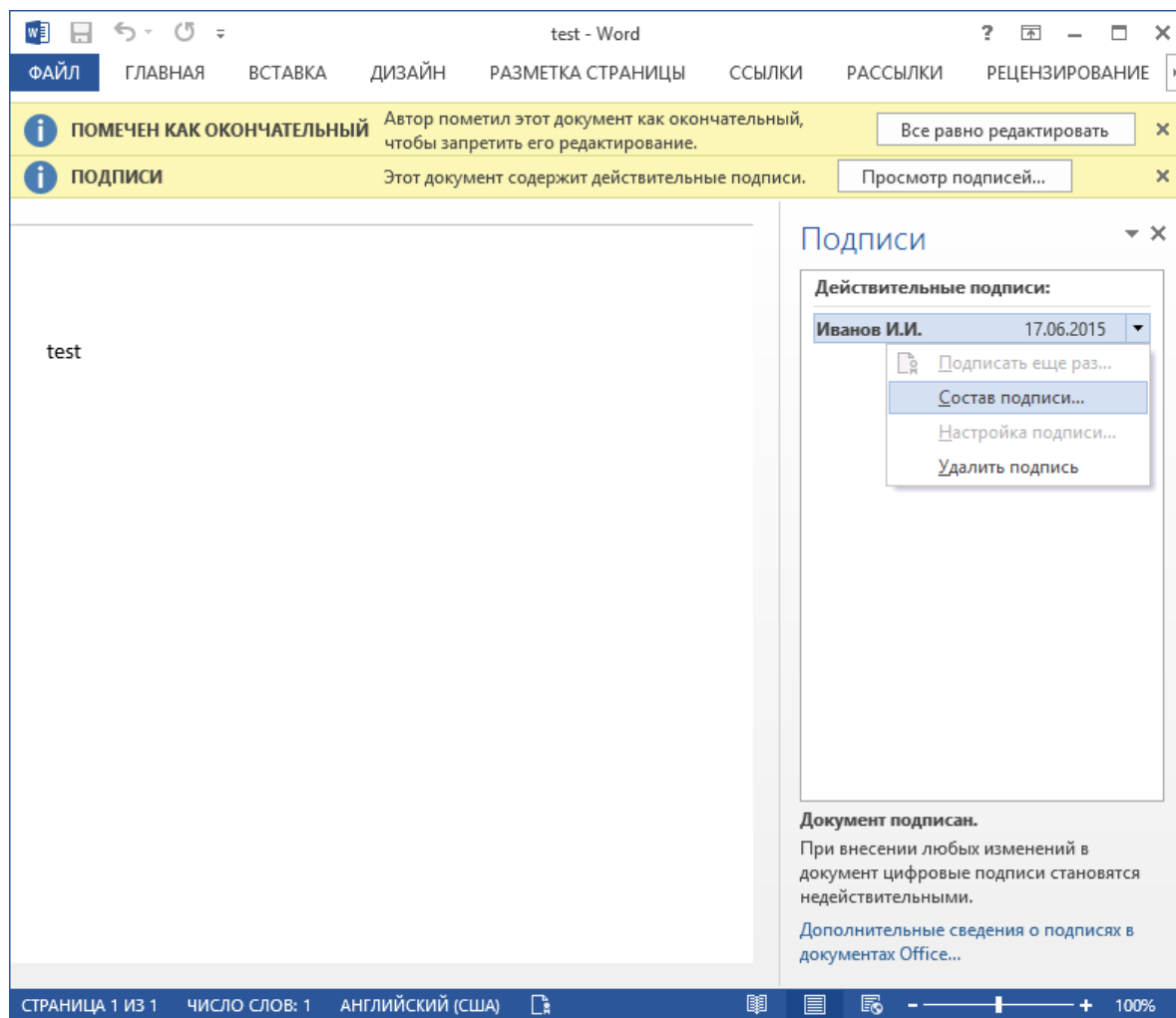


Рисунок 11. Статус подписи

Для просмотра состава подписи, щелкните правой кнопкой мыши на строке подписи и выберите пункт **Состав подписи**. Появится детальное сообщение о составе подписи (см. Рисунок 12).

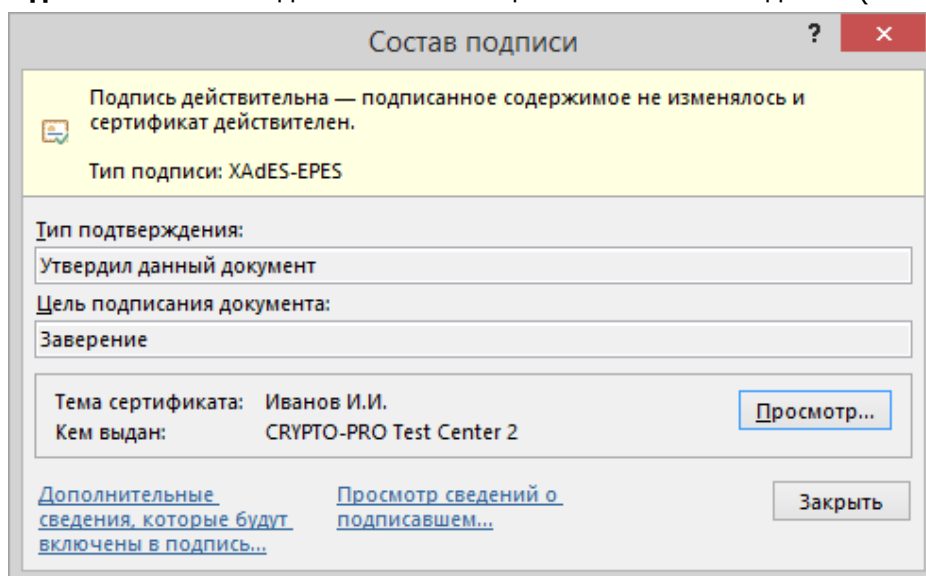


Рисунок 12. Состав подписи

Если открыть документ для редактирования, все подписи удаляются, об этом выводится предупреждение.

При открытии измененного документа, содержащего недействительную ЭП, появится сообщение (см. Рисунок 13).

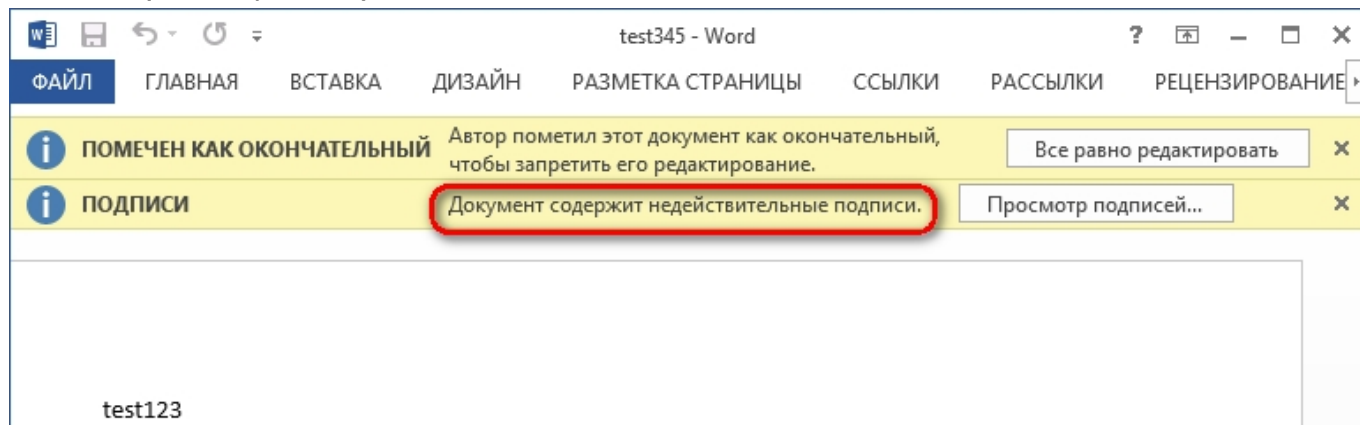


Рисунок 13. Документ с недействительной подписью

Для более детального просмотра статуса, нажмите на значок ЭП в строке состояния. В результате справа появится окно, содержащее недействительный статус подписи. Состав подписи можно посмотреть нажатием правой кнопки мыши и выбором пункта **Состав подписи** в выпадающем меню (см. Рисунок 14)

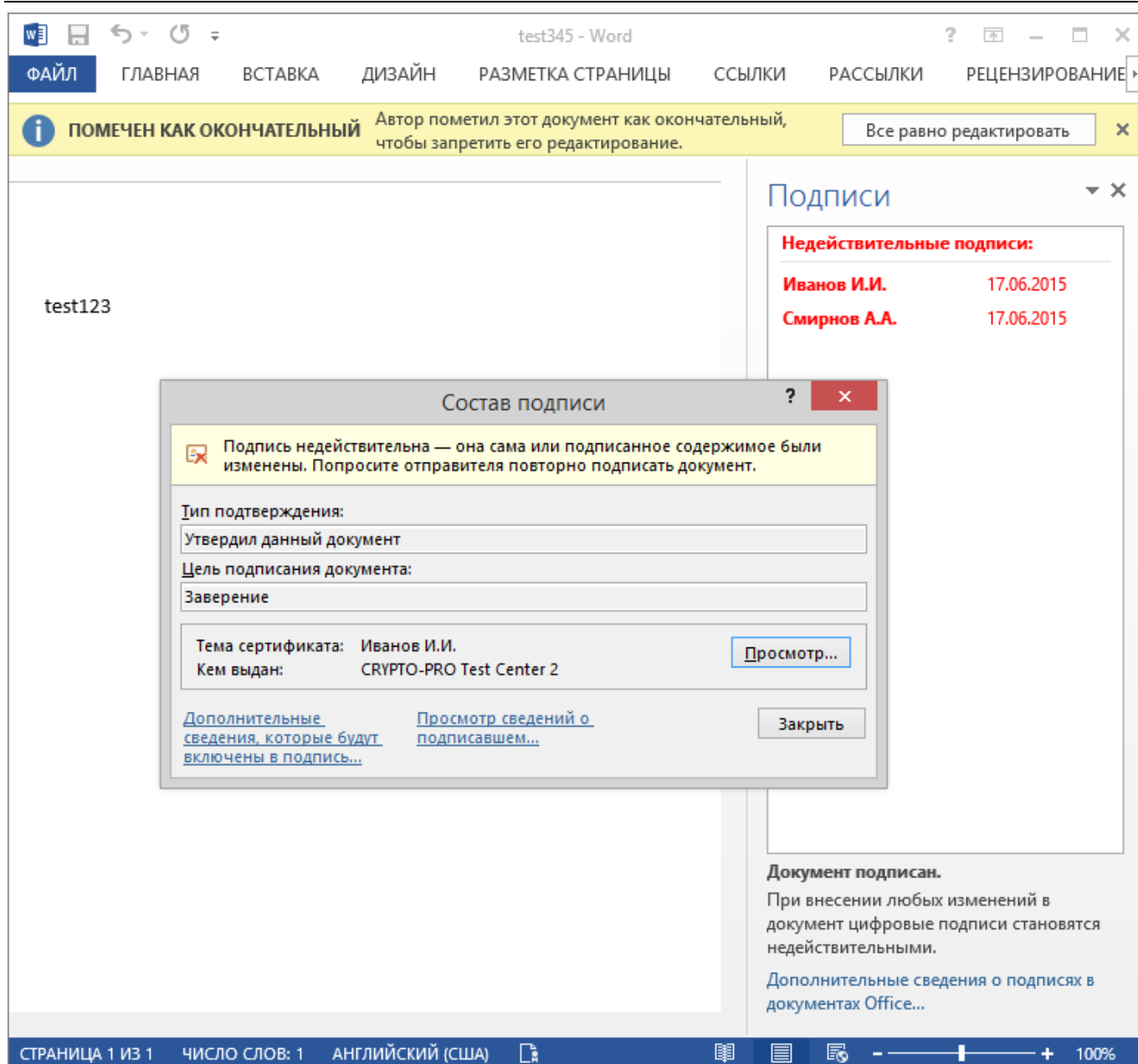


Рисунок 14. Состав недействительной подписи

2.2. Подписание документа, содержащего цифровую подпись

Если документ уже содержит электронную подпись, его можно подписать еще раз.

Для добавления новой ЭП в **Microsoft Office Word 2007** или **Excel 2007** в главном меню выберите пункт **Подготовить**, затем **Добавить электронную подпись (КРИПТО-ПРО)**.

Для добавления новой ЭП в **Microsoft Office Word 2010/2013/2016** или **Excel 2010/2013/2016** на вкладке **Файл** в разделе **Сведения** нажмите кнопку **Добавить электронную подпись (КРИПТО-ПРО)**.

Дальнейшие действия аналогичны созданию первой подписи.

В результате на вкладке **Подписи** появится еще одна действительная подпись (см. Рисунок 15).

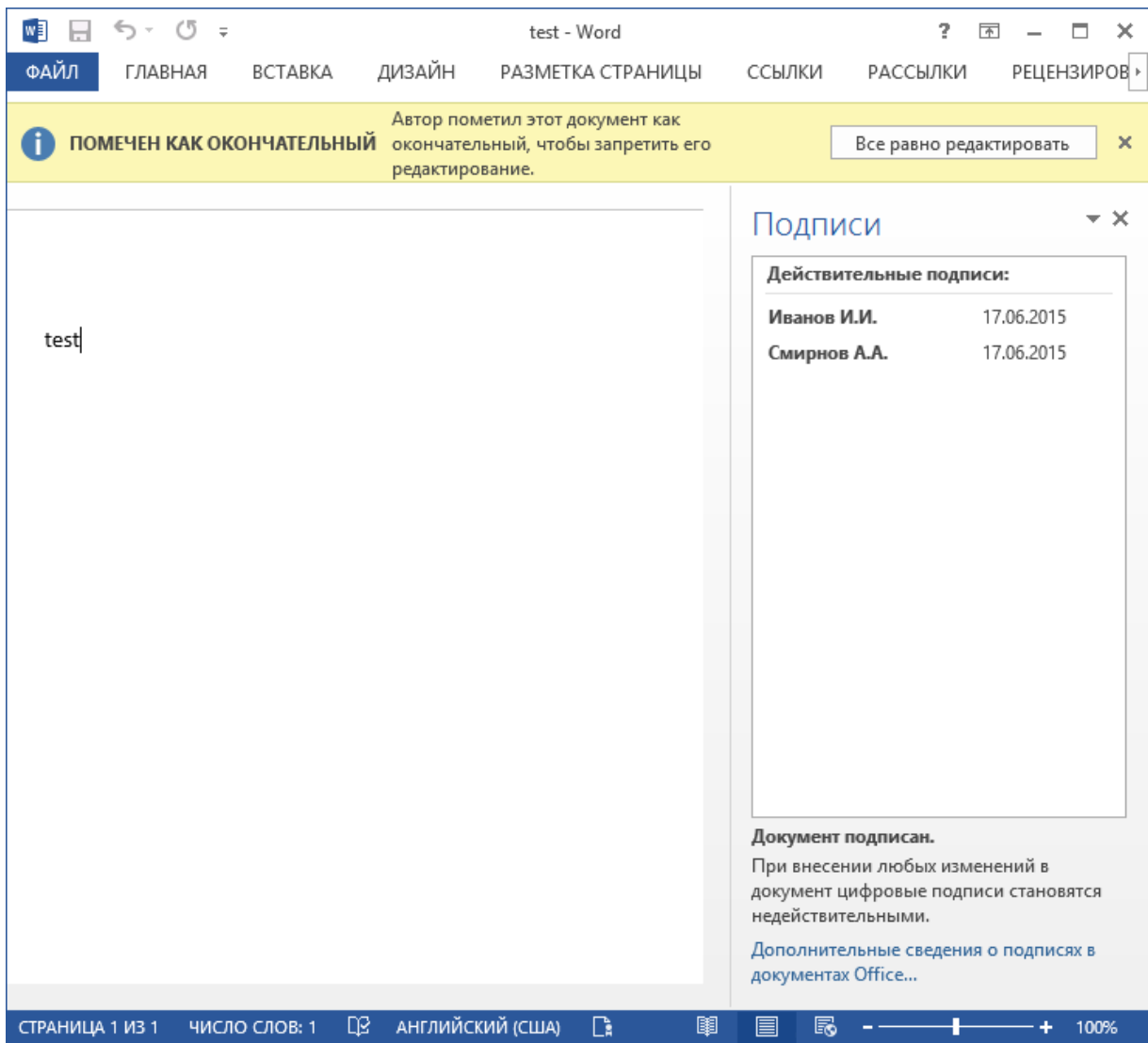


Рисунок 15. Несколько подписей в документе

3. Строка подписи

3.1. Добавление строки подписи

На вкладке **Вставка** в группе **Текст** нажмите на стрелку рядом с кнопкой **Строка подписи** и в появившемся меню выберите **Строка электронной подписи (КРИПТО-ПРО)** (см.Рисунок 16).

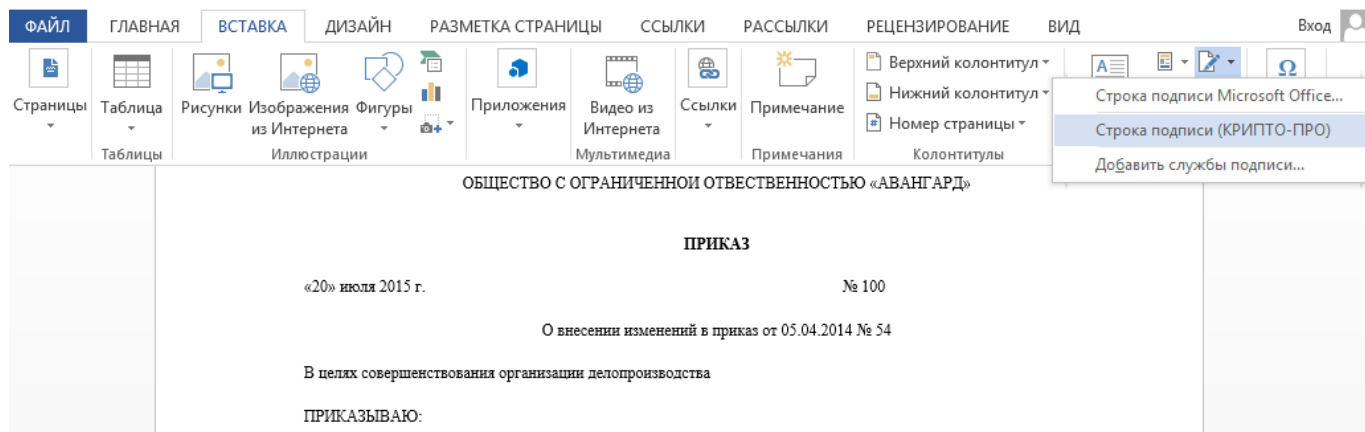


Рисунок 16. Строка электронной подписи (КРИПТО-ПРО)

Появится диалоговое окно **Настройка подписи** (см. Рисунок 17).

Рисунок 17. Настройка подписи

В нём можно ввести информацию о лице, которое будет добавлять подпись. Эти сведения будут отображены в строке подписи в документе. Заполнять все пункты не обязательно.

- в поле **Предложенный подписывающий** вводится ФИО подписывающего;
- в поле **Должность предложенного подписывающего** - название должности подписывающего;
- в поле **Адрес электронной почты** предложенного подписывающего - адрес электронной почты подписывающего;
- в поле **Инструкции для подписывающего** можно ввести рекомендации или требования для подписывающего. Эти инструкции отображаются в диалоговом окне Подпись, в котором подписывающий будет ставить подпись;

- для разрешения самому подписывающему добавления комментариев в процессе создания подписи установите флажок **Разрешить подписывающему добавлять примечания в окне подписи**;
- для отображения даты подписания документа, установите флажок **Показывать дату подписи в строке подписи**.

Нажмите кнопку **ОК**. Созданная строка подписи представляет собой графический объект, который можно переместить на любое место в тексте документа (см. Рисунок 18).

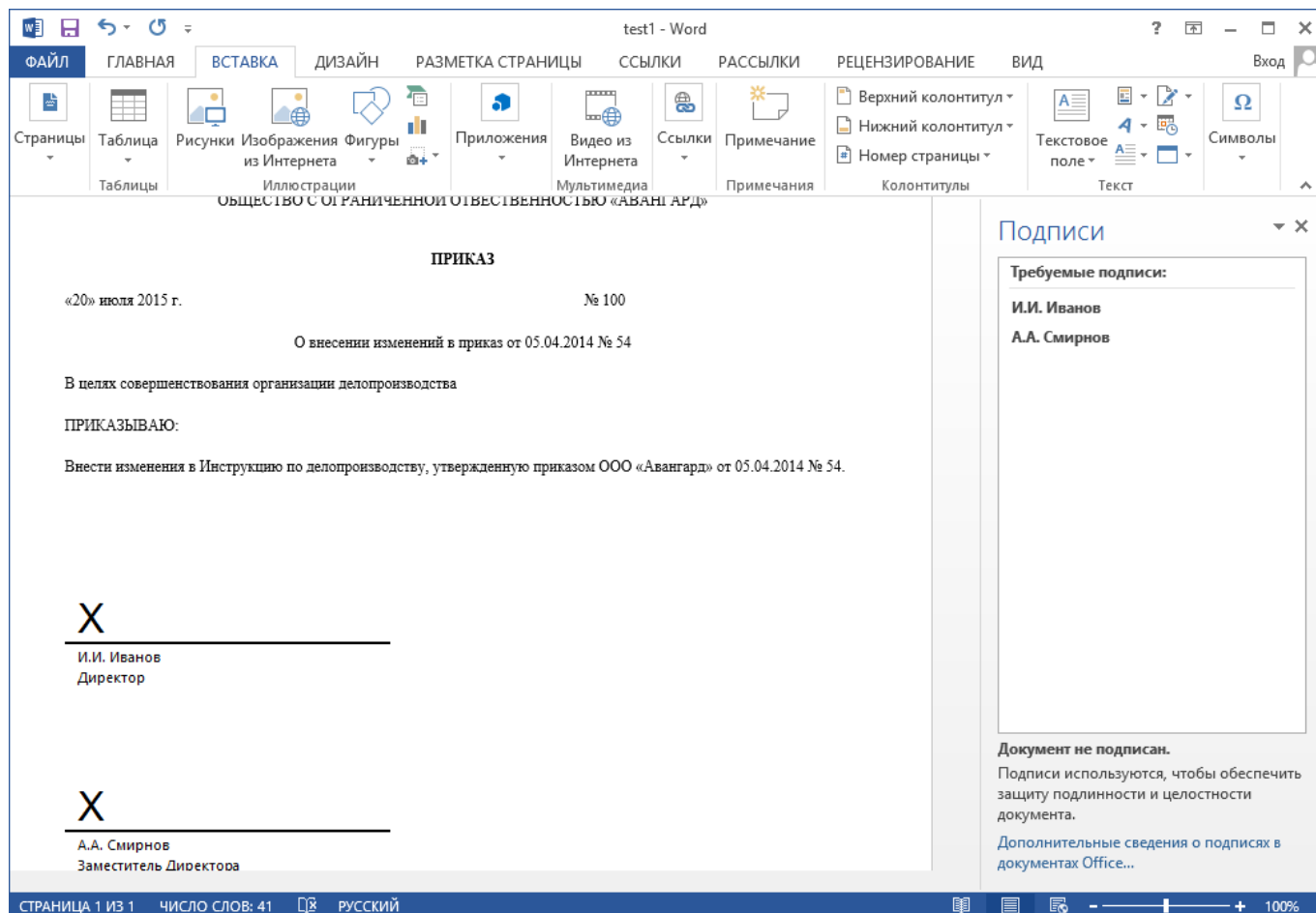


Рисунок 18. Строка подписи

При необходимости можно повторить добавление видимой строки подписи, например, если документ подписывается разными людьми. Добавление второй и следующих видимых подписей должно происходить до того, как будет добавлена первая электронная подпись, так как в этот момент содержимое документа становится защищенным от редактирования.

3.2. Добавление электронной подписи в строку подписания

Дважды щелкните мышью в документе по строке подписи, в которую требуется поместить электронную подпись, или выберите **Подписать** в контекстном меню, щелкнув правой кнопкой мыши по элементу подписи. Появится диалоговое окно **Подписание** (см. Рисунок 19).

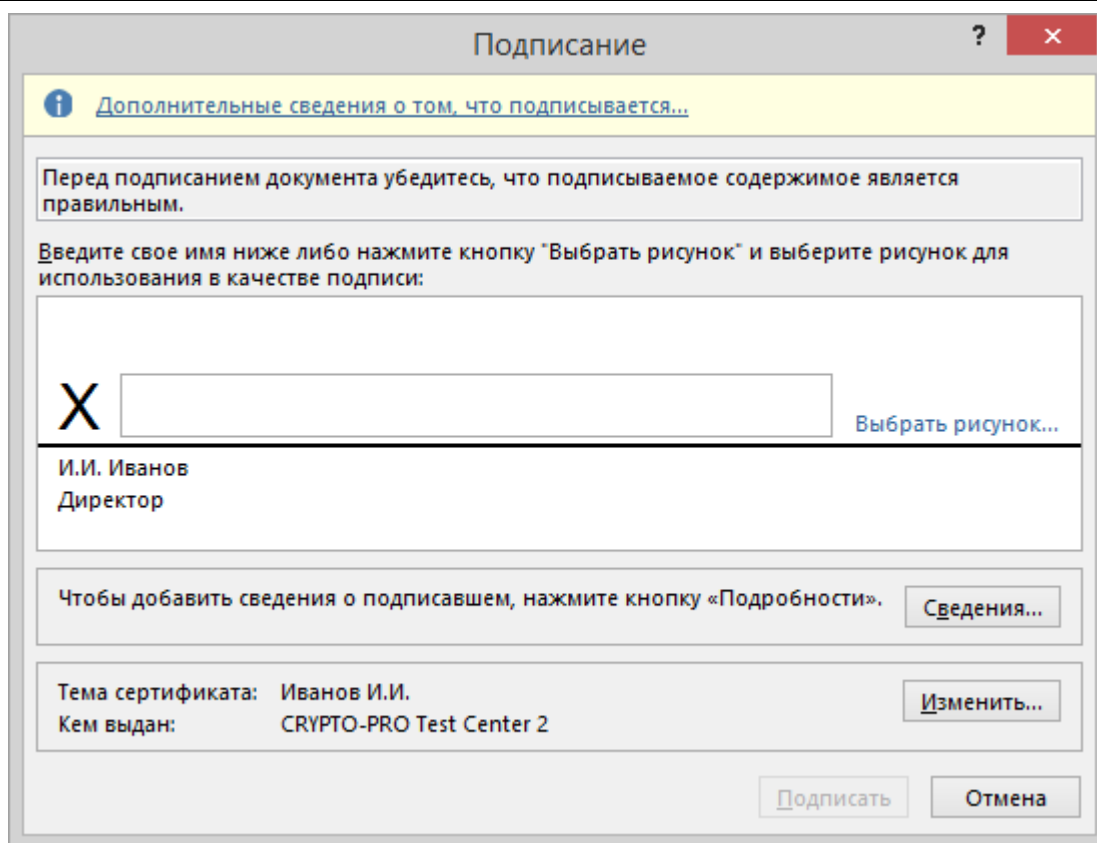


Рисунок 19. Выбор параметров электронной подписи

В верхней части окна можно просмотреть дополнительные сведения о создаваемой подписи нажав ссылку **Дополнительные сведения о том, что подписывается...**

При нажатии ссылки **Выбрать рисунок** можно добавить изображение, например, своей рукописной подписи.

Один из имеющихся на компьютере сертификатов будет выбран автоматически. Для выбора другого цифрового сертификата для подписи нажмите кнопку **Изменить** и в окне **Выбор сертификата** выберите необходимый сертификат.

В окне **Подписание** нажмите кнопку **Подписать**. Выводится окно, в которое нужно ввести пароль к контейнеру закрытого ключа (см.Рисунок 7), после ввода правильного пароля появится информационное окно подтверждения подписи (см.Рисунок 20), в этом окне нажмите кнопку **ОК**. Для удобства работы можно установить флажок **Больше не показывать это сообщение**.

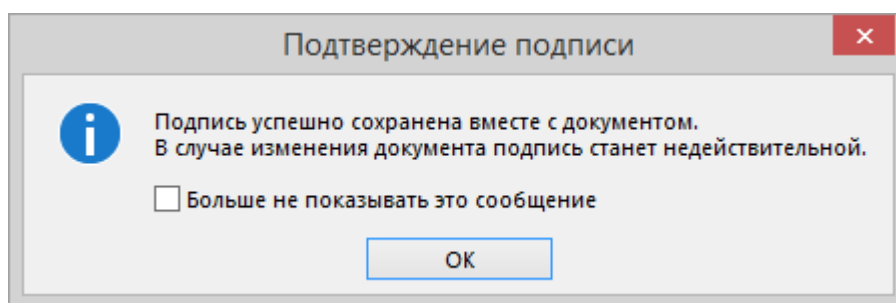


Рисунок 20. Подтверждение подписи

Созданная подпись будет отображена в документе. Одновременно будет отображена вкладка **Подписи**, в которой приведен список подписей в документе. Созданная подпись будет находиться в разделе **Действительные подписи**. Незаполненная подпись - в разделе **Требуемые подписи** (см. Рисунок 21).

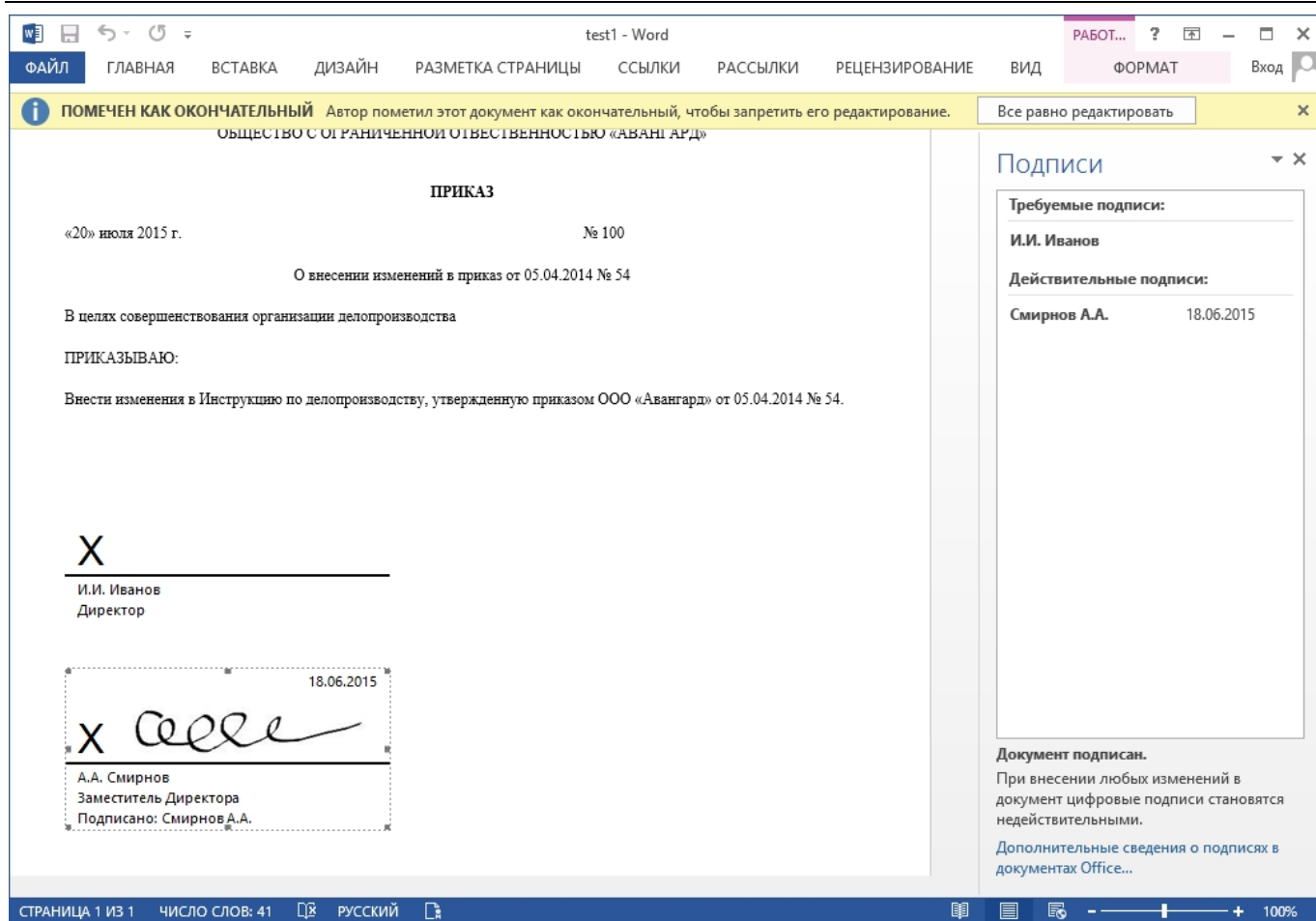


Рисунок 21. Требуемые подписи

После того, как в документе появилась первая (или единственная) цифровая подпись, он автоматически помечается как окончательный и доступен только для чтения.

Если документ содержит единственную подпись, то на этом работа с ним заканчивается.

Если документ содержит несколько строк подписей для нескольких лиц, документ следует передать этим лицам для подписания.

При открытии документа, содержащего незаполненные строки подписи, появляется панель сообщений (см. Рисунок 22).

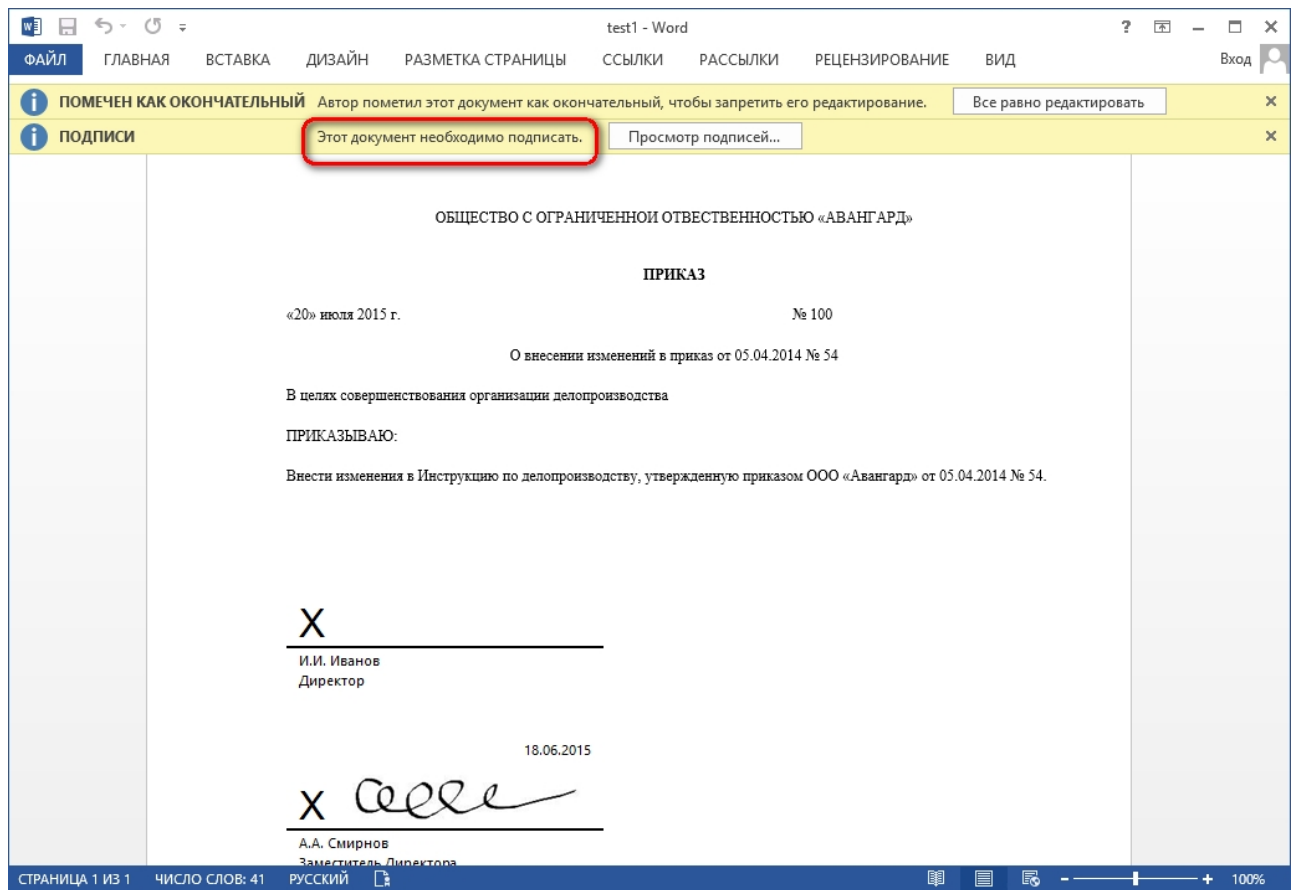


Рисунок 22. Документ с несколькими подписями

Щелкните по кнопке **Просмотр подписей**, после чего на вкладке **Подписи** будет отображен список подписей в документе (см. Рисунок 23).

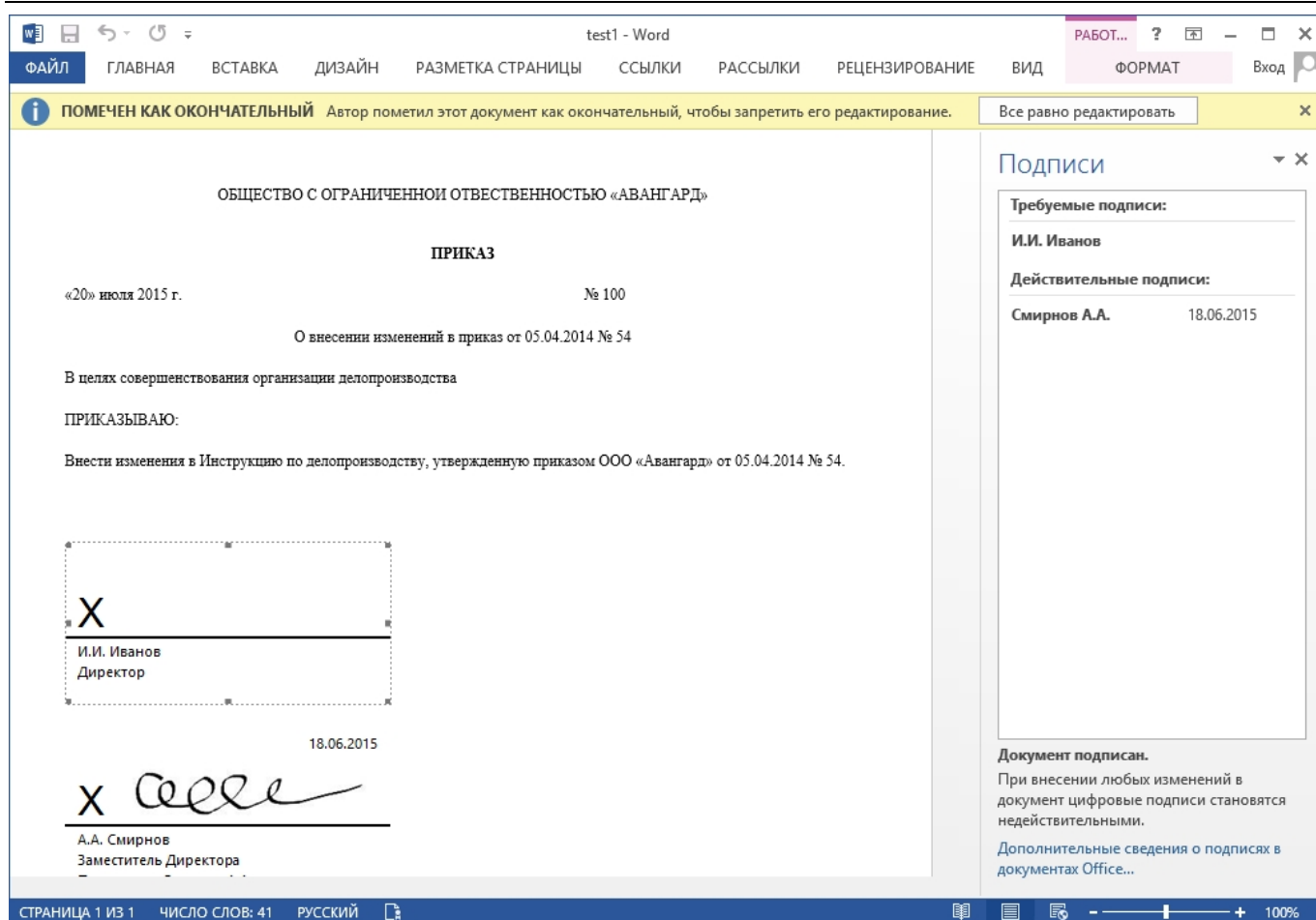


Рисунок 23. Список подписей на документе

Для добавления подписи в строку подписи дважды щелкните по строке подписи в тексте документа, либо выберите действие **Подписать** в контекстном меню элемента, либо в панели **Подписи** нажмите правой кнопкой мыши на нужной строке подписи и выберите команду **Подписать** (см. Рисунок 24).

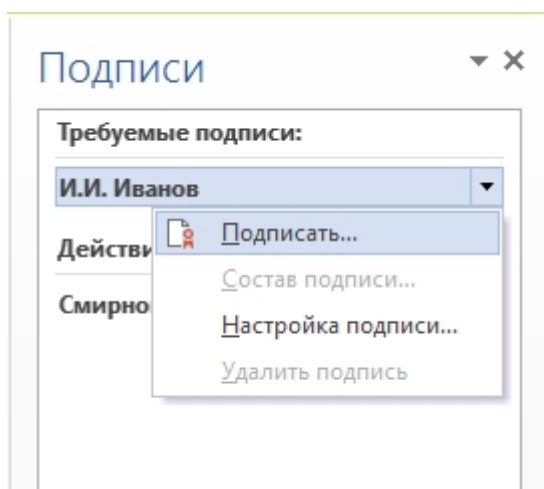


Рисунок 24. Добавление подписи

В окне **Подписание** введите необходимую информацию и нажмите кнопку **Подписать**.

После создания последней подписи в документе в панели **Подписи** все подписи будут находиться в разделе **Действительные подписи** (см. Рисунок 25).

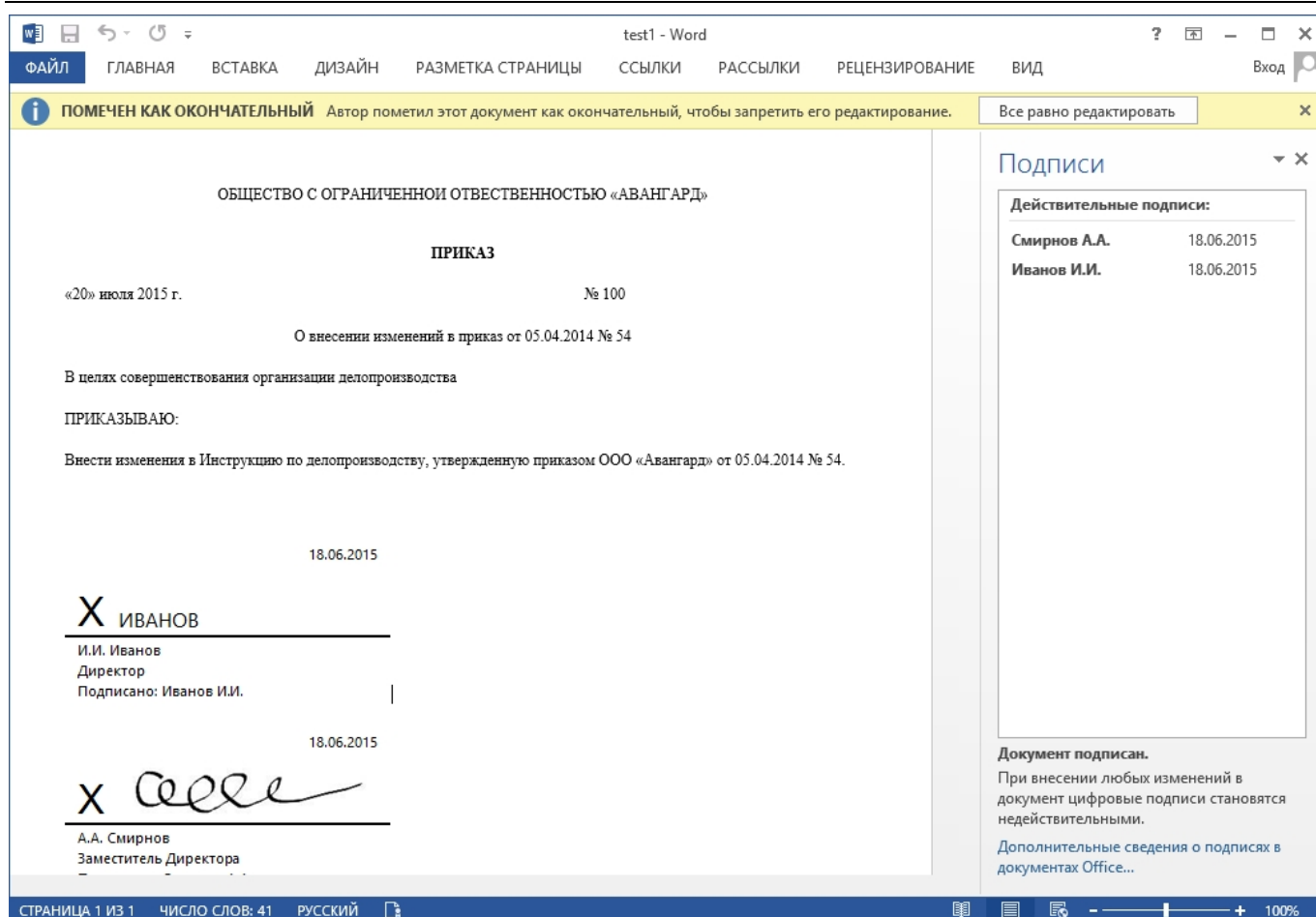


Рисунок 25. Документ с несколькими подписями

3.3. Просмотр свойств электронной подписи

В окне документа в панели **Подписи** щелкните по стрелке требуемой подписи и выберите команду **Состав подписи** (см. Рисунок 26). Можно также дважды щелкнуть мышью по строке подписи в тексте документа.

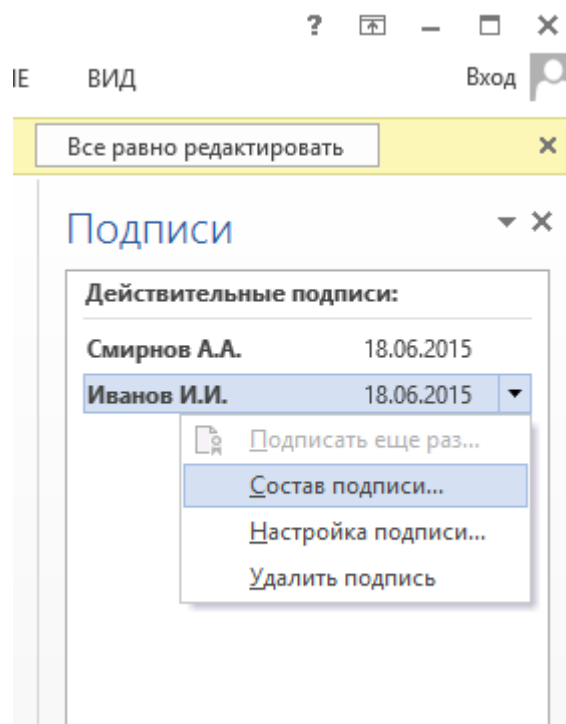


Рисунок 26. Меню свойств подписи

Свойства подписи будут отображены в соответствующем окне (см. Рисунок 27).

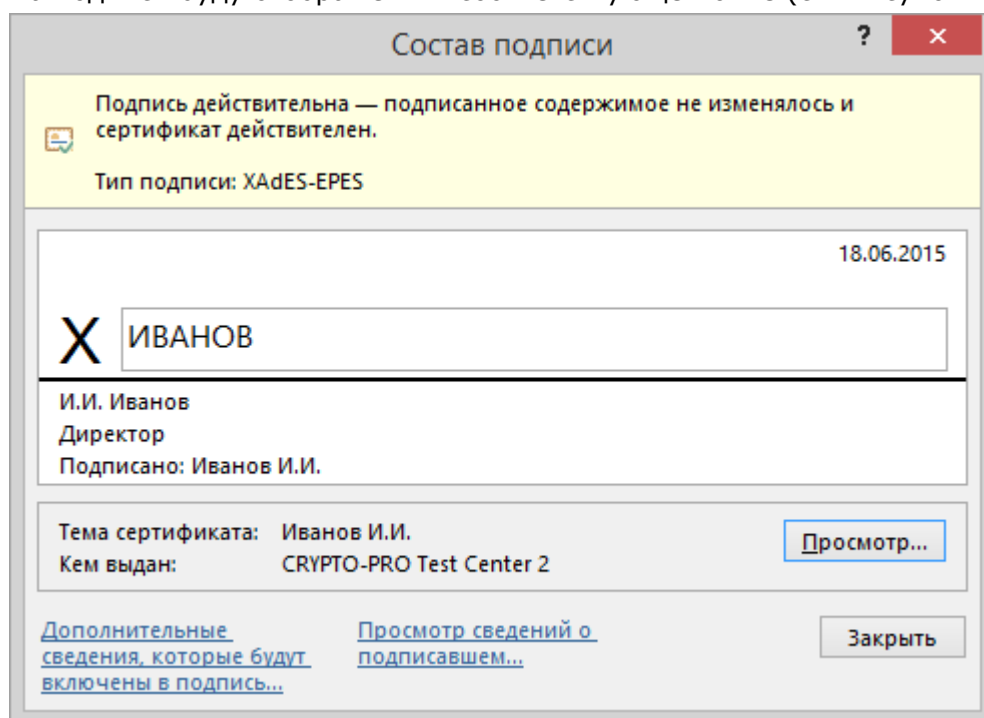


Рисунок 27. Просмотр состава подписи

Для просмотра сертификата, использовавшегося при создании подписи, нажмите кнопку **Просмотр** (см. Рисунок 28).

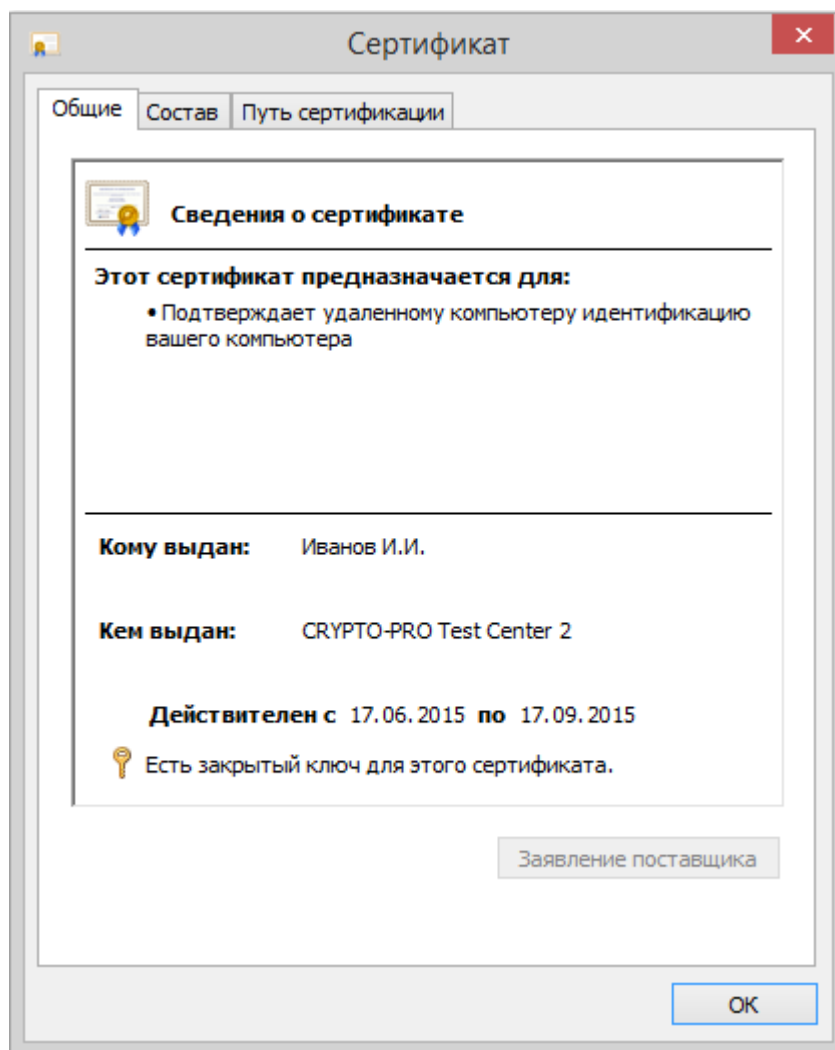


Рисунок 28. Сведения о сертификате

Подписанный документ можно просматривать, печатать, выделять фрагменты и копировать их в буфер обмена. Можно скопировать и строку подписи в другой документ, но эта строка подписи вставляется без цифровой подписи. Необходимо добавление подписи в строку подписи в новом документе.

При попытке сохранить подписанный документ под другим именем, появляется информационное окно (см. Рисунок 29).

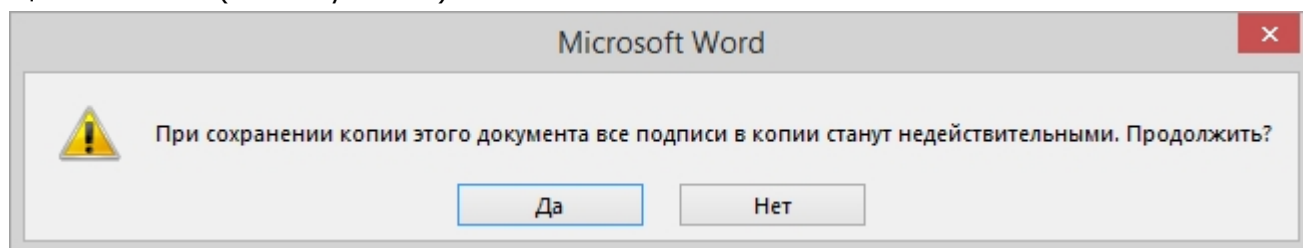


Рисунок 29. Сохранение подписанного документа

Если нажать кнопку **Да**, все подписи в документе станут недействительными.

Документ, содержащий цифровые подписи, автоматически помечается как окончательный. При попытке снятия этой отметки появляется информационное окно (см. Рисунок 30).

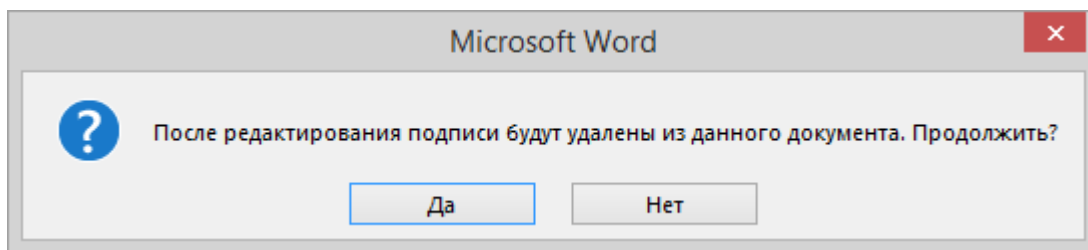


Рисунок 30. Сообщение при попытке редактирования документа

Если нажать кнопку **Да**, то любое действие по редактированию документа приведёт к тому, что все подписи из документа будут удалены (см. Рисунок 31).

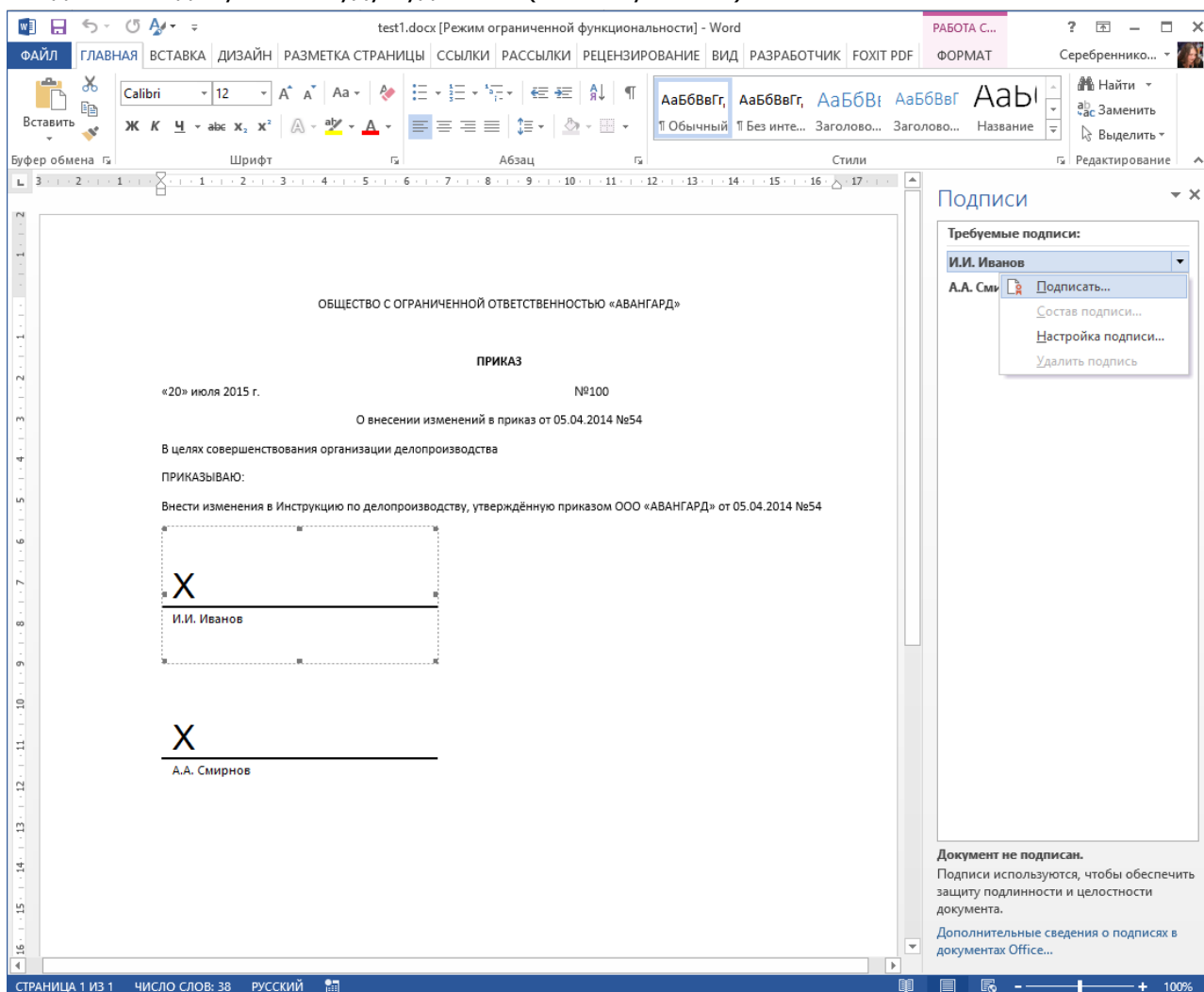


Рисунок 31. Документ с подписями, удалёнными в результате редактирования

Документ можно подписать повторно, для этого на вкладке **Подписи** щелкните по требуемой подписи и выберите команду **Подписать...** Можно также щелкнуть правой кнопкой мыши по строке подписи в тексте документа и в контекстном меню выбрать команду **Подписать...** Заново заполните окно **Подписание** и нажмите кнопку **Подписать**.

4. Настройка Office Signature

4.1. Алгоритм хэширования содержимого контейнера документа

Microsoft Office при создании электронной подписи по умолчанию использует для хэширования содержимого контейнера алгоритм sha-1.

Настроить использование ГОСТ 34.11-94/ГОСТ 34.11-2012 можно с помощью групповой политики или через профиль пользователя.

Расположение настроек групповой политики:

```
HCU\Software\Policies\Microsoft\Office\[Версия]\Common\Signatures:  
"SignatureHashAlg"="GOST R 34.11-94[GR 34.11-2012 256][GR 34.11-2012 512]"
```

Расположение в профиле пользователя:

```
HCU\Software\Microsoft\Office\[Версия]\Common\Signatures:  
"SignatureHashAlg"="GOST R 34.11-94[GR 34.11-2012 256][GR 34.11-2012 512]"
```

Где [Версия]:

- **12.0** для MS Office 2007
- **14.0** для MS Office 2010
- **15.0** для MS Office 2013
- **16.0** для MS Office 2016

Если раздел реестра или параметр отсутствуют, их нужно создать, при этом тип параметра SignatureHashAlg должен быть строковым (REG_SZ).

5. Программное создание и проверка ЭП в документах MS Office

5.1. Средства автоматизации MS Office

Самый простой способ программно добавить подписи в документы, это воспользоваться методом `signatureSet->AddNonVisibleSignature (sigprov, &signature)` объекта `SignatureSet` доступного из документов с помощью `get_Signatures`.

Идентификатор плагина КриптоПро Office Signature:

`{F5AC7D23-DA04-45F5-ABCB-38CE7A982553}`.

5.2. КриптоПро .NET

Электронные подписи, совместимые с КриптоПро Office Signature, могут быть созданы и проверены программно на платформе Microsoft .NET 3.5 и выше с использованием КриптоПро .NET при помощи `System.IO.Packaging.PackageDigitalSignatureManager`. Примеры создания и проверки `Simple35.Office.Sign/Verify` входят в комплект КриптоПро .NET SDK.

Скачать актуальные версии КриптоПро .NET и КриптоПро .NET SDK можно по адресу <http://cryptopro.net>.

6. Перечень сокращений

| | |
|-----|--|
| PKI | Инфраструктура открытых ключей (Public Key Infrastructure) набор средств, распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей |
| ЭП | Электронная подпись |