



УТВЕРЖДАЮ

Руководитель  
Федеральной службы  
по аккредитации

 Н.В. Скрыпник

«30» декабря 2020 г.


## СМ № 02.1-3.0002

Версия 01. Декабрь 2020 г.

---

## ИНСТРУКЦИЯ

по подписанию документов электронной подписью

 <b>росаккредитация</b> Федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 2 из 32
	<b>СМ № 02.1-3.0002</b>	вер. 01    утв.: <b>30 ДЕК 2020</b>	

## ПРЕДИСЛОВИЕ

Настоящая инструкция разработана Федеральной службой по аккредитации в целях разъяснения порядка подписания документов электронной подписью при проведении выездной оценки соответствия заявителя, аккредитованного лица критериям аккредитации в форме удаленной оценки и вводится впервые. Настоящая инструкция вводится в действие по истечении трех рабочих дней со дня ее утверждения.

## СОДЕРЖАНИЕ

1. Область применения .....	3
2. Нормативные ссылки .....	3
3. Термины и определения .....	3
4. Справочная информация .....	4
5. Проверка наличия сертификатов .....	5
6. Работа с Контур.Крипто .....	6
7. Работа с КриптоАРМ .....	22
8. Дополнительная информация .....	31
Лист регистрации изменений .....	32



## 1. Область применения

1.1. Настоящая инструкция устанавливает порядок подписания документов электронной подписью при проведении выездной оценки соответствия заявителя, аккредитованного лица критериям аккредитации в форме удаленной оценки.

1.2. Настоящая инструкция предназначена для участников национальной системы аккредитации, в том числе аккредитованных лиц, экспертов по аккредитации и технических экспертов.

## 2. Нормативные ссылки

2.1. В настоящей инструкции использованы ссылки на следующие документы:


**Федеральный закон №63-ФЗ**      Федеральный закон от 06.04.2020 №63-ФЗ  
«Об электронной подписи»

2.2. При пользовании настоящей инструкцией следует проверять действие ссылочных документов. Если ссылочный документ заменен, то при пользовании настоящей инструкции следует руководствоваться замененным (измененным) документом.

## 3. Термины и определения

3.1. В настоящей инструкции применяются следующие термины:

- электронная подпись (ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию
- простая электронная подпись** – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом
- удостоверяющий центр** – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции
- усиленная квалифицированная электронная подпись** – электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, имеющие

 <b>росаккредитация</b> федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 4 из 32
	<b>СМ № 02.1-3.0002</b>	<b>вер. 01</b> <b>утв.: 30 ДЕК 2020</b>	

подтверждение соответствия требованиям, установленным в соответствии Федеральным законом № 63.

**усиленная  
неквалифицированная  
электронная подпись**

- электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи.

#### **4. Справочная информация**

4.1. Для корректной работы программ необходимо заранее установить сертификаты электронной подписи в личное хранилище сертификатов.

4.2. Для выполнения *пункта 4.1 настоящей инструкции* необходимо воспользоваться следующим программным обеспечением:

- VipNet CSP;
- КриптоПРО CSP.

4.3. Для получения дополнительных консультаций по вопросам работы с электронной подписью необходимо обращаться в удостоверяющий центр, выдавший электронную подпись.

4.4. Для проверки наличия сертификатов в личном хранилище необходимо следовать *разделу 5*.

4.5. Загруженные файлы документов необходимо подписывать квалифицированной электронной подписью, сформированной в виде отдельного файла от исходных данных с помощью программного обеспечения электронной подписи.

4.6. Для подписания файлов документов необходимо воспользоваться соответствующим программным обеспечением и следовать его инструкции по подписанию документов.

4.7. По завершении процесса подписания к документам (прошедшим процесс подписания) необходимо приложить файл отсоединенной электронной подписи с расширением «\*.sig».


4.8. Для проверки подлинности электронной подписи необходимо следовать *пунктам 6.3 и 7.3 настоящей инструкции* в зависимости от выбранного программного обеспечения.

4.9. Согласно *Федеральному закону №63-ФЗ «Об электронной подписи»*, имеет место деление на:

- простую электронную подпись;
- усиленную неквалифицированную электронную подпись;
- усиленную квалифицированную электронную подпись.

4.9.1. Простая электронная подпись посредством использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

4.9.2. Усиленную неквалифицированную электронную подпись получают

 <b>росаккредитация</b> федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 5 из 32
	<b>СМ № 02.1-3.0002</b>	<b>вер. 01 утв.: 30 ДЕК 2020</b>	

в результате криптографического преобразования информации с использованием закрытого ключа подписи. Данная ЭП позволяет определить лицо, подписавшее электронный документ, и обнаружить факт внесения изменений после подписания электронных документов.

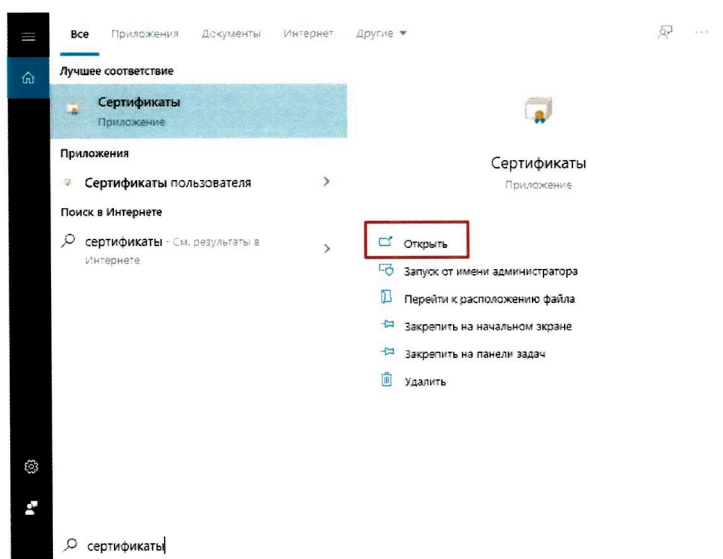
4.9.3. Усиленная квалифицированная электронная подпись соответствует всем признакам неквалифицированной электронной подписи, но для создания и проверки ЭП используются средства криптозащиты, которые сертифицированы ФСБ РФ. Кроме того, сертификаты квалифицированной ЭП выдаются исключительно аккредитованными удостоверяющими центрами.

4.9.4. Участники национальной системы по аккредитации для подписания документов используют усиленную квалифицированную подпись.

Подписанные документы в машиночитаемом виде в формате «.pdf» направляются в Росаккредитацию вместе с файлами отсоединенных электронных подписей с расширением «\*.sig» всех подписантов.

## 5. Проверка наличия сертификатов

5.1. В поисковой строке Windows необходимо ввести текст «Сертификаты» и нажать пункт «Открыть» (в соответствии с *рисунком 1*)



*Рисунок 1*

5.2. В открывшемся окне необходимо нажать «Да» (в соответствии с *рисунком 2*)

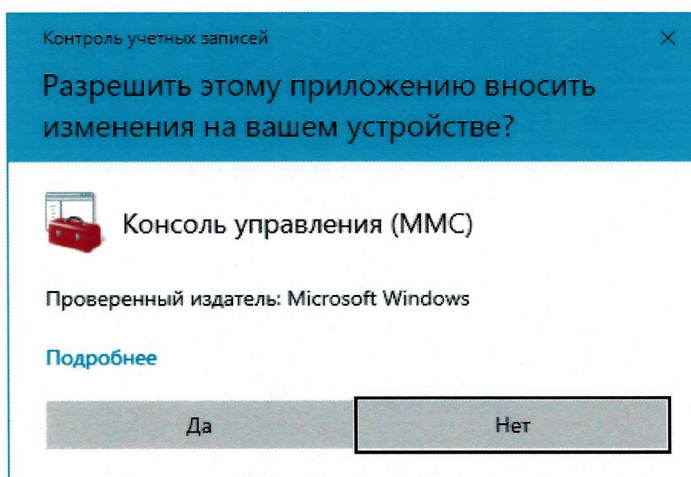


Рисунок 2

5.2. В открывшемся окне в левом меню необходимо развернуть пункт «Сертификат – текущий пользователь», затем – «Личное» и «Сертификаты» (в соответствии с рисунком 3)

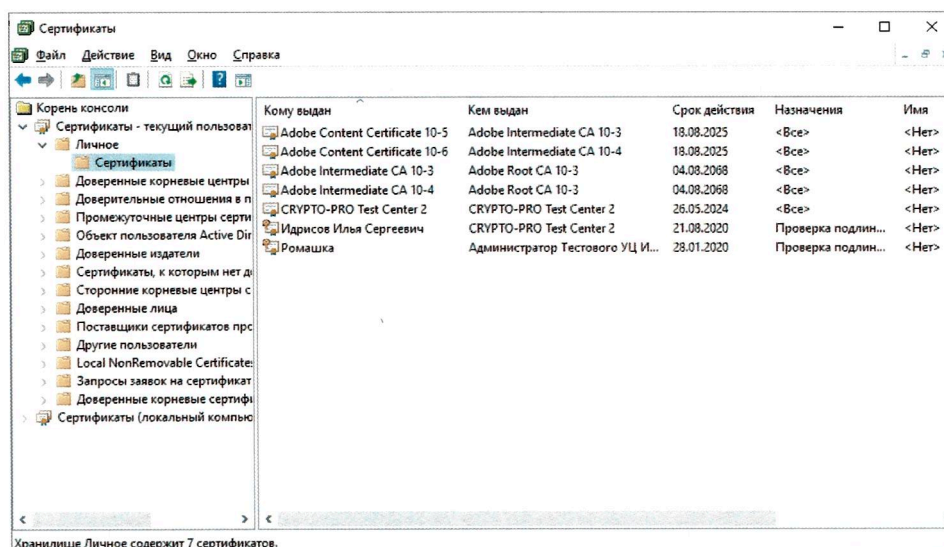


Рисунок 3


5.3. В открывшемся правом меню откроется список установленных на компьютере сертификатов (в соответствии с рисунком 3).

5.4. В случае отсутствия ФИО подписанта документа необходимо установить сертификат электронной подписи в соответствии с инструкциями удостоверяющего центра.

## 6. Работа с Контур.Крипто

### 6.1. Установка Контур.Крипто:

- 1) В браузере необходимо открыть сайт: <https://crypto.kontur.ru>.
- 2) В открывшемся окне необходимо нажать «Войти» (в соответствии с рисунком 4).

 <b>РОСАККРЕДИТАЦИЯ</b> федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 7 из 32
	<b>СМ № 02.1-3.0002</b>	<b>вер. 01</b> утв.: <b>30 ДЕК 2020</b>	

контур.крипто

Войти

Подписание, хранение и отправка  
документов с электронной подписью

Начать пользоваться



Рисунок 4

3) В открывшемся окне необходимо переключиться на вкладку «По сертификату» и нажать на ссылку «Контур.Плагин» (в соответствии с *рисунком 5*).

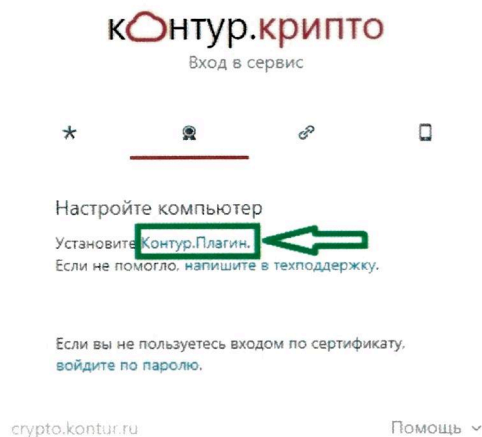



Рисунок 5

4) В открывшемся окне необходимо нажать на кнопку «Установить» (в соответствии с *рисунком 6*).

 <b>росаккредитация</b> Федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 8 из 32
	<b>СМ № 02.1-3.0002</b>	<b>вер. 01</b> <b>утв.: 30 ДЕК 2020</b>	

контур

Для работы в сервисе Кристо вам нужны:

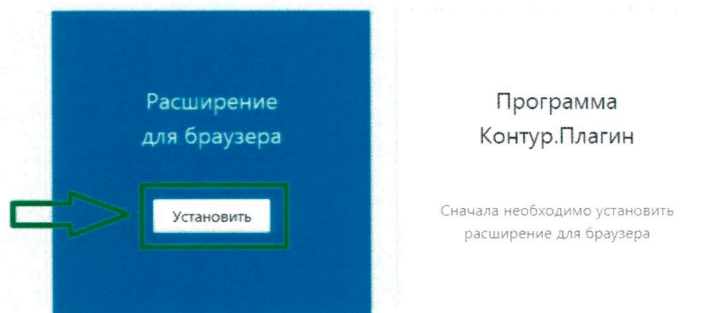


Рисунок 6

5) В открывшемся окне необходимо нажать на кнопку «Установить» (в соответствии с *рисунком 7*).

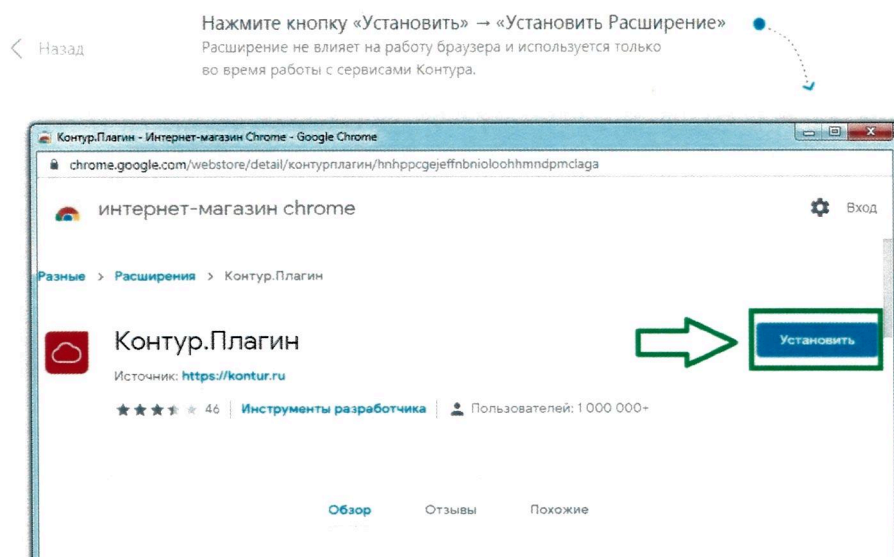


Рисунок 7

6) В открывшемся окне сверху необходимо нажать на кнопку «Установить расширение» (в соответствии с *рисунком 8*).

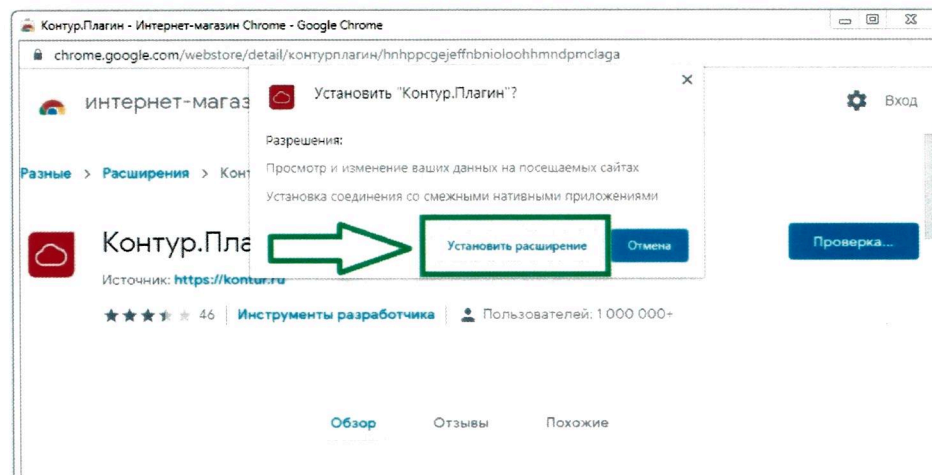




< Назад

Нажмите кнопку «Установить» → «Установить Расширение»

Расширение не влияет на работу браузера и используется только во время работы с сервисами Контур.



*Рисунок 8*

7) В открывшемся окне необходимо нажать на кнопку «Установить» (в соответствии с *рисунком 9*).



Для работы в сервисе Кripto вам нужны:



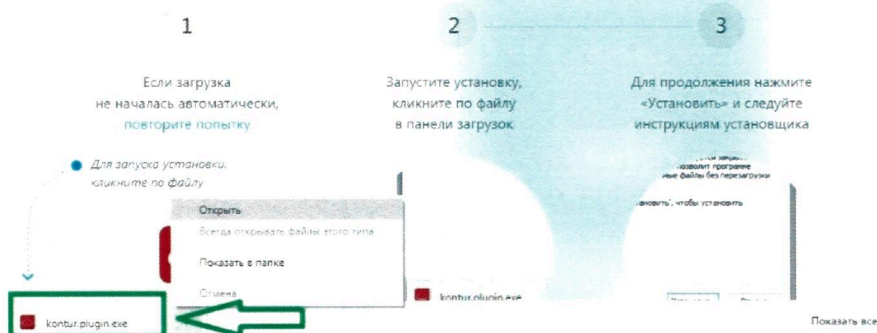
*Рисунок 9*

8) Далее необходимо открыть загруженный файл (в соответствии с *рисунком 10*).

← Назад

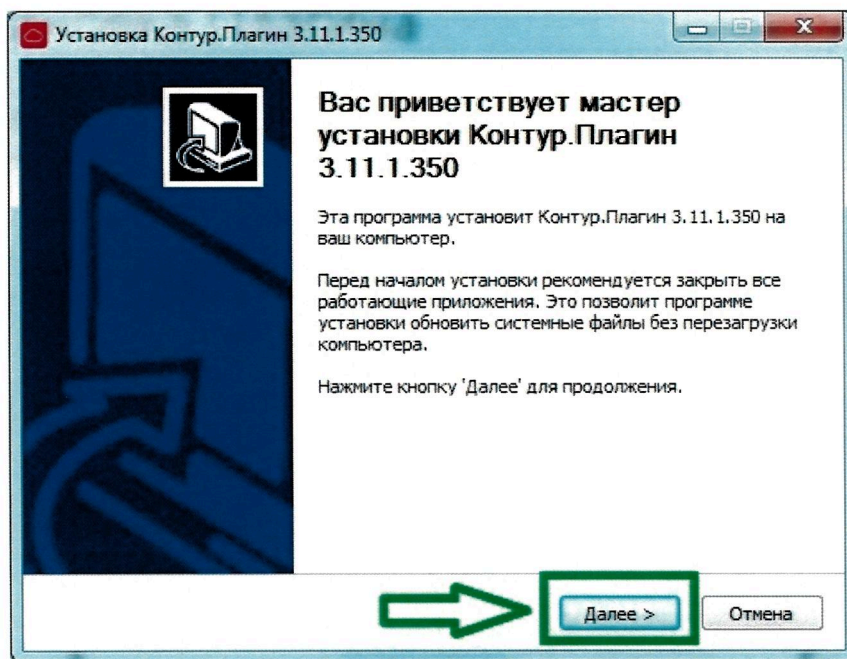
## Установка Плагина

Плагин отвечает за работу с сертификатами электронной подписи  
и обеспечивает шифрование документов



*Рисунок 10*

9) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с *рисунком 11*).



*Рисунок 11*

10) В открывшемся окне после завершения установки необходимо нажать кнопку «Готово» (в соответствии с *рисунком 12*).

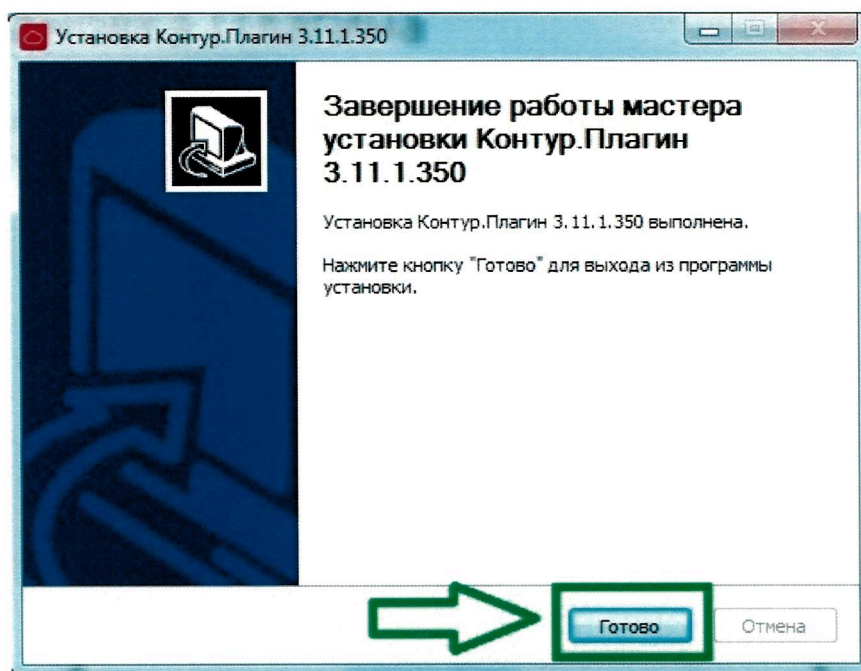


Рисунок 12

11) На сайте появится сообщение об успешной установке, после чего необходимо нажать на ссылку «Вернуться в сервис Крипто» (в соответствии с *рисунком 13*).

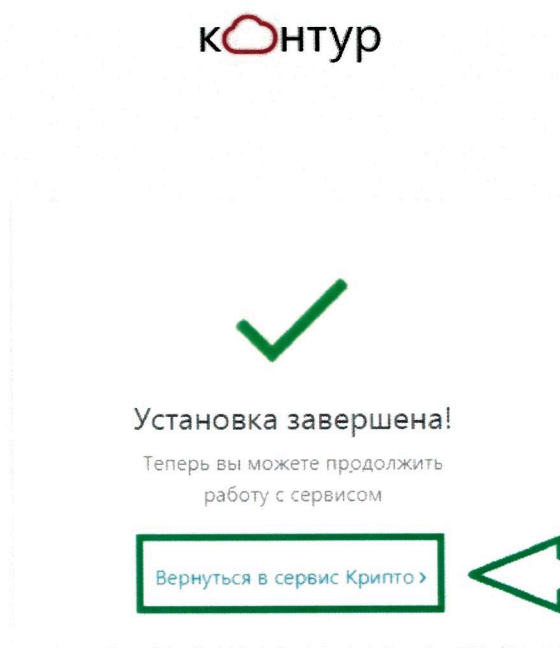

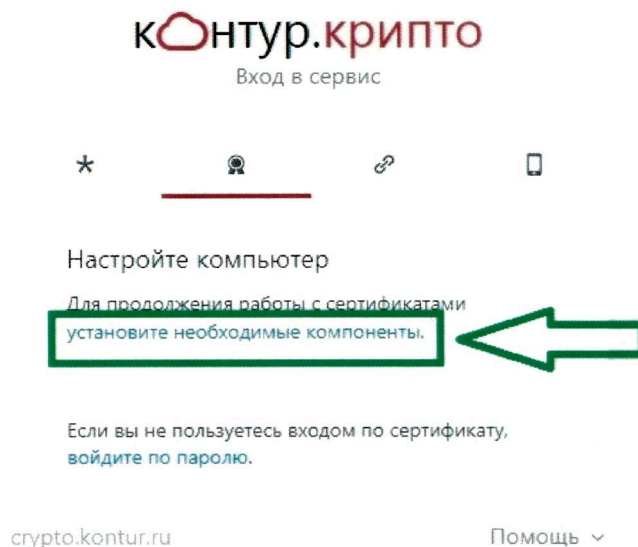


Рисунок 13

12) В открывшемся окне необходимо нажать на ссылку «Установите необходимые компоненты» (в соответствии с *рисунком 14*).

 <b>росаккредитация</b> федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 12 из 32
	<b>СМ № 02.1-3.0002</b>	<b>вер. 01</b> <b>утв.: 30 ДЕК 2020</b>	



*Рисунок 14*

13) В открывшемся окне необходимо нажать на кнопку «Скачать расширение» (в соответствии с *рисунком 15*).



*Рисунок 15*

14) В открывшемся окне необходимо нажать на кнопку «Установить» (в соответствии с *рисунком 16*).

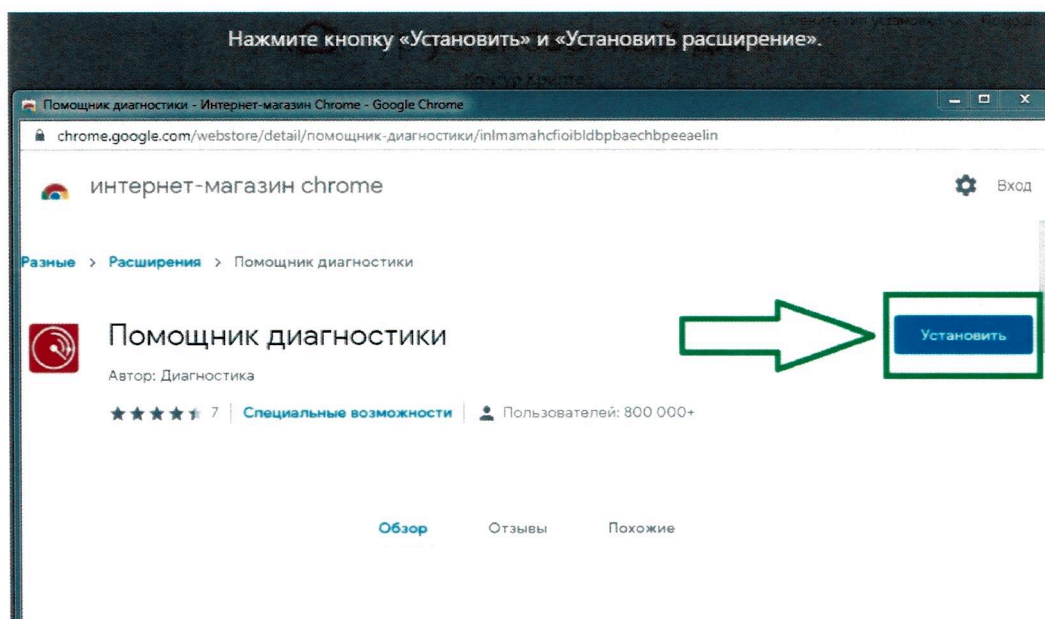


Рисунок 16

15) В открывшемся окне сверху необходимо нажать на кнопку «Установить расширение» (в соответствии с *рисунком 17*).

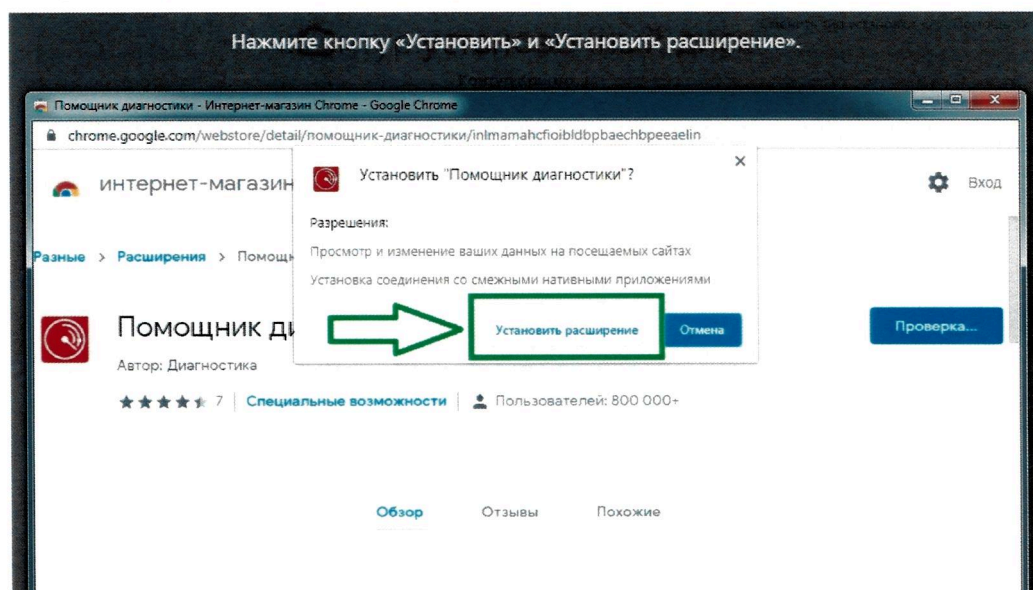


Рисунок 17

16) В открывшемся окне необходимо нажать на кнопку «Скачать Диаг.Плагин» (в соответствии с *рисунком 18*).



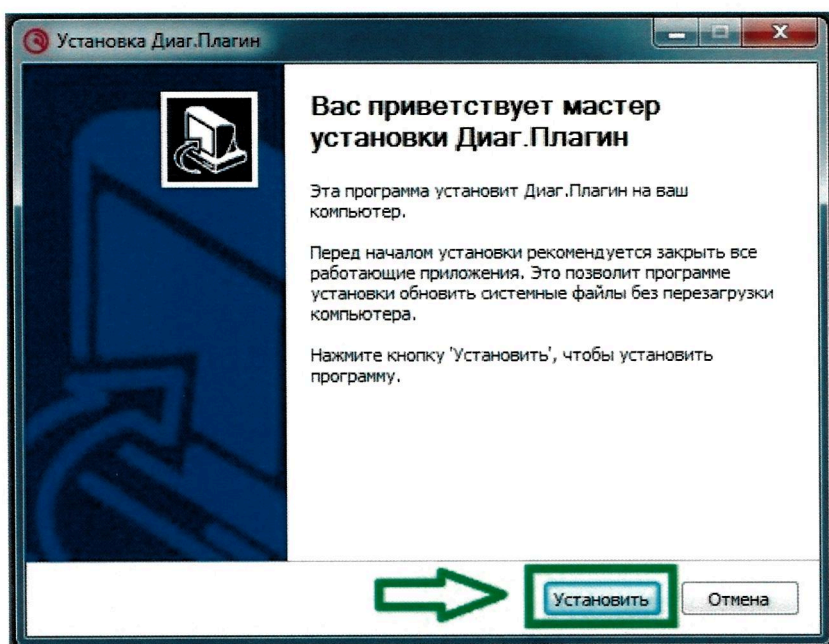


Рисунок 20

19) На сайте необходимо нажать на кнопку «Установить» (в соответствии с рисунком 21).



Рисунок 21

20) По завершении установки в открывшемся окне необходимо нажать на кнопку «Перезагрузить сейчас», а затем – «Подтвердить перезагрузку» (в соответствии с рисунком 22, 23).



### Настройка и установка компонентов

- ✓ 3. Отключение конфликтных служб (MoviesToolbar, GuardMailRu, CipGuard) ★
- ✓ 4. Настройка зоны "Надежные узлы" (129 КБ) ★ ⬇
- ✓ 5. Отключение конфликтных надстроек IE (ICQ Toolbar и прочих) ★
- ✓ 8. Установка сертификатов УЦ (503 КБ) ★ ⬇
- ✓ 9. Установка КриптоПро CSP 4.0 R4 (5.58 МБ) ★ ⬇
- ✓ 10. Добавление программ в исключения КриптоПро CSP ★
- ✓ 12. Установка компонента диагностики Рутокен (558 КБ) ★ ⬇
- ✓ 13. Регистрация OID сертификатов для УЦ (114 КБ) ★ ⬇
- ✓ 15. Создание ярлыка "Контур.Крипто" на рабочем столе ★

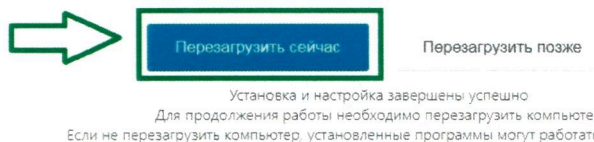


Рисунок 22

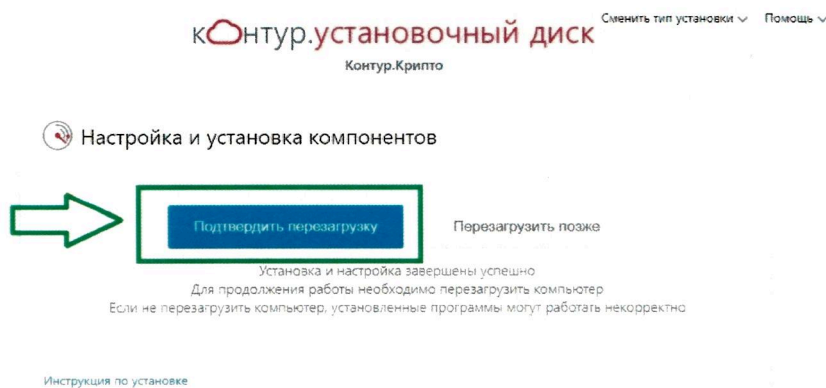


Рисунок 23

21) По завершении перезагрузки компьютера откроется страница сайта с сообщением об успешном открытии сервиса (в соответствии с *рисунком 24*).

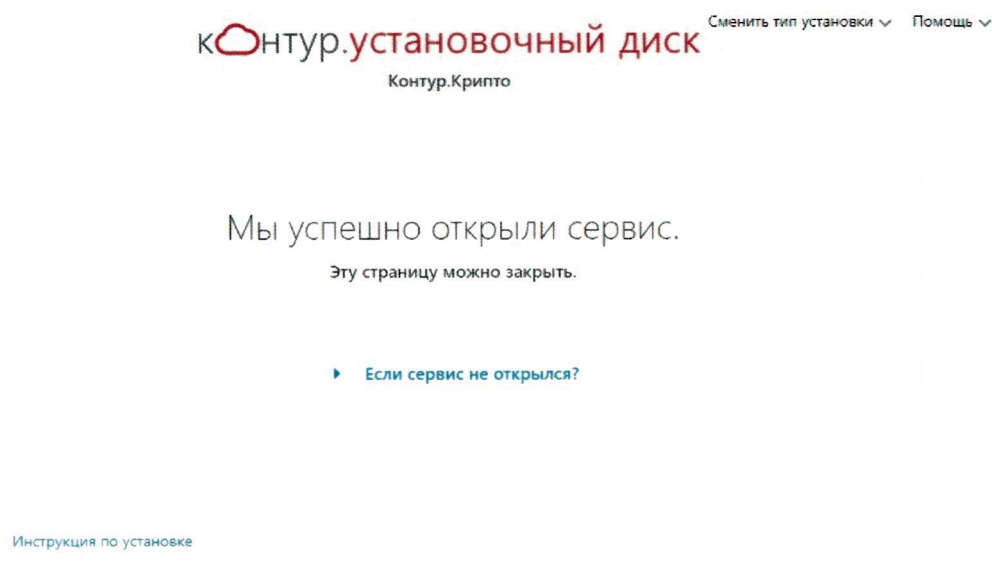



Рисунок 24



 <b>росаккредитация</b> федеральная служба по аккредитации	<b>ИНСТРУКЦИЯ</b> <i>по подписанию документов электронной подписью</i>		стр. 17 из 32
	<b>СМ № 02.1-3.0002</b>	вер. 01    утв.: <b>30 ДЕК 2020</b>	

## 6.2. Подписание документов:

1) В браузере необходимо открыть сайт <https://crypto.kontur.ru> и нажать на кнопку «Войти» (в соответствии с *рисунком 25*).

контур.крипто



Подписание, хранение и отправка  
документов с электронной подписью

Начать пользоваться

Для подписания документов нужен сертификат. Купить >

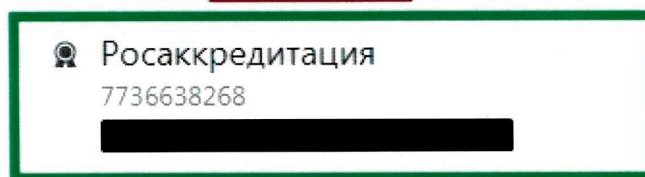


*Рисунок 25*

2) В открывшемся окне необходимо выбрать сертификат (в соответствии с *рисунком 26*).

контур.крипто

Вход в сервис



crypto.kontur.ru

Помощь ▾

*Рисунок 26*

3) В открывшемся окне необходимо ввести пин-код от электронной подписи и нажать на кнопку «ОК» (в соответствии с *рисунком 27*).



контур.крипто

Вход в сервис

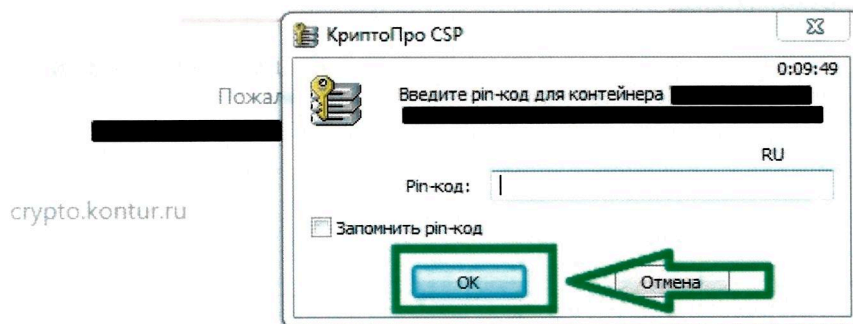


Рисунок 27

4) Для подписания документа в левом столбце открывшегося окна необходимо выбрать раздел «Подписать» и нажать на кнопку «Выбрать файлы...» (в соответствии с рисунком 28).

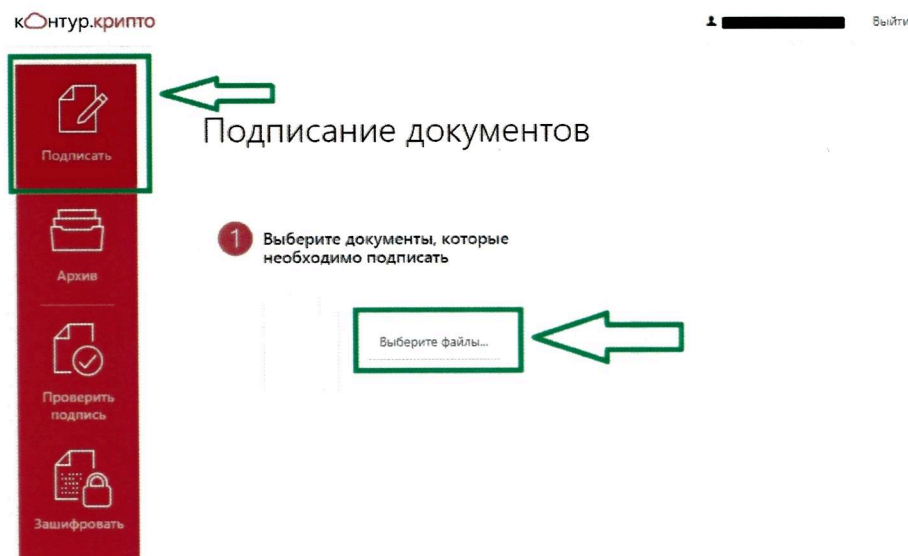


Рисунок 28

5) В открывшемся окне необходимо выбрать файл, который нужно подписать, и нажать на кнопку «ОК».

6) Далее необходимо выбрать сертификат, которым требуется подписать файл. По умолчанию выбран сертификат, с помощью которого происходила авторизация в сервисе. Необходимо нажать на кнопку «Подписать» (в соответствии с рисунком 29).



## Подписание документов

1) Выберите документы, которые необходимо подписать



2) Выберите сертификат

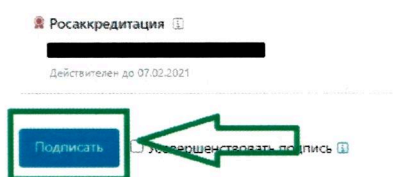


Рисунок 29

7) Далее необходимо ввести пин-код и нажать на кнопку «ОК» (в соответствии с рисунком 30).

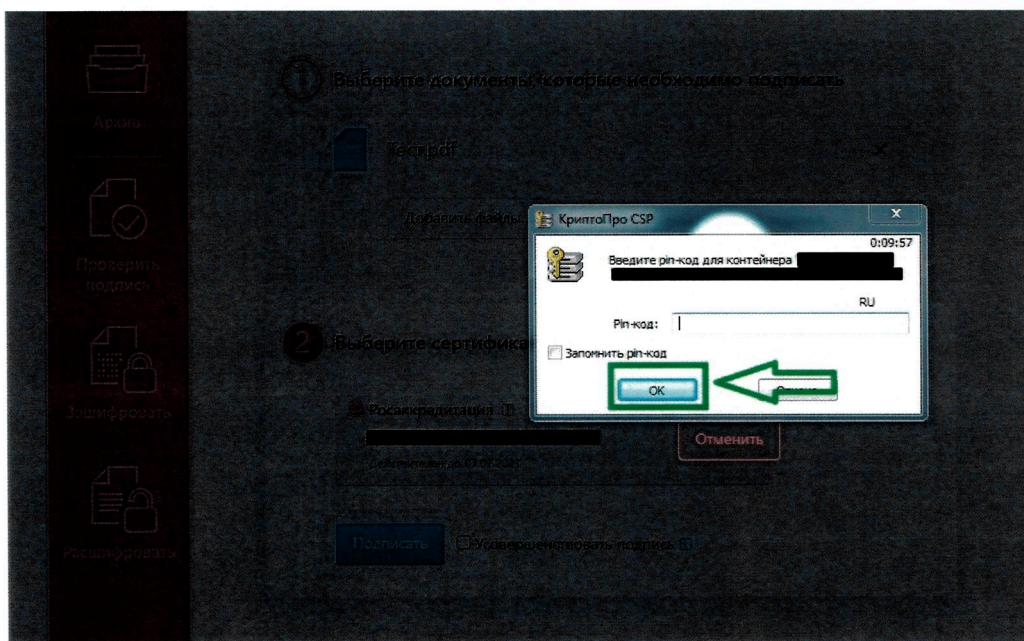


Рисунок 30

8) Необходимо нажать на кнопку «Скачать все». Загруженный архив будет содержать документ, файл подписи и открытый сертификат (в соответствии с рисунком 31).

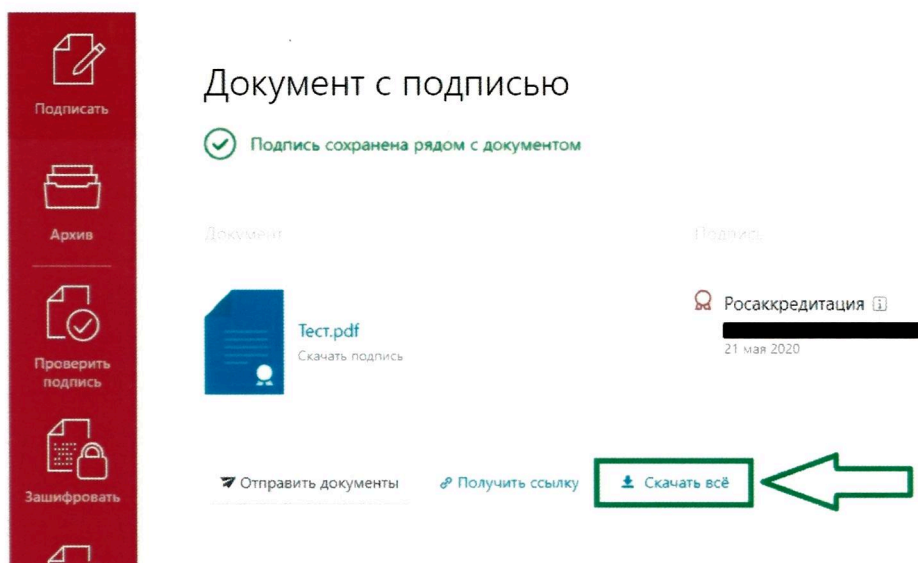


Рисунок 31

### 6.3. Проверка электронной подписи:

1) Для проверки электронной подписи в левом столбце необходимо выбрать раздел «Проверить подпись» и нажать на кнопку «Выбрать...» (в соответствии с рисунком 32).



Рисунок 32

2) Необходимо выбрать документ, электронную подпись которого требуется проверить, нажать на кнопку «ОК».

3) Далее необходимо нажать на кнопку «Выбрать...» для выбора файла подписи (в соответствии с рисунком 33).



## Проверка электронной подписи

1 Выберите подписанный документ



2 Выберите подпись

Обычно файл подписи назван тем же именем, что и подписанный документ



Рисунок 33

4) Необходимо выбрать файл подписи с расширением «\*.sig» и нажать на кнопку «ОК».

5) Далее необходимо нажать на кнопку «Проверить подпись» (в соответствии с рисунком 34).



## Проверка электронной подписи

1 Выберите подписанный документ



2 Выберите подпись

Обычно файл подписи назван тем же именем, что и подписанный документ



Рисунок 34

5) По завершении процедуры проверки появится окно с подтверждением подписи (в соответствии с рисунком 35).

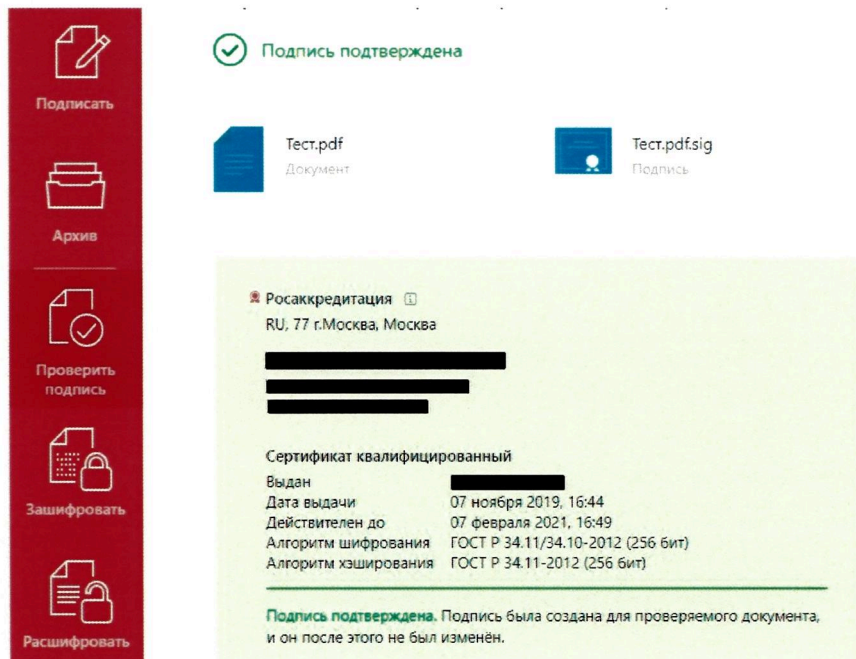


Рисунок 35

## 7. Работа с КриптоАРМ

### 7.1. Установка КриптоАРМ:

1) В браузере необходимо открыть сайт <https://cryptoarm.ru/kak-skachat-programmu-cryptoarm> и нажать на кнопку «Скачать». При первой установке на рабочем месте активируется бесплатный период сроком на 14 дней. После истечения этого срока программа перейдет в режим «Старт», что заметно снизит ее возможности (в соответствии с *рисунком 36*).

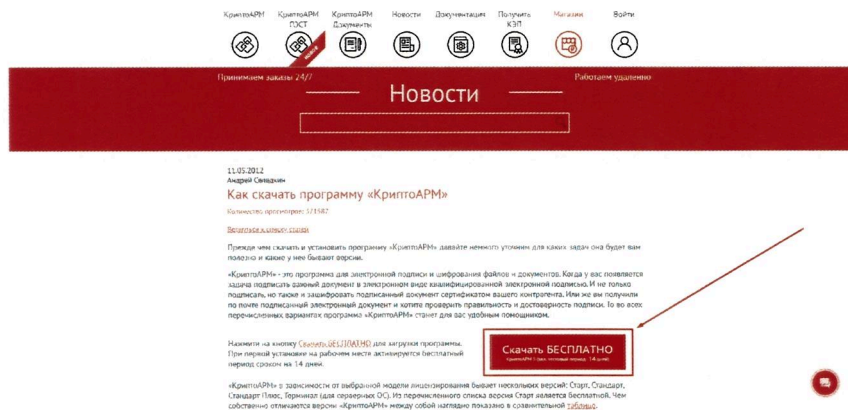


Рисунок 36

2) Далее необходимо запустить скачанный файл, выбрать пункт «Быстрая установка» и нажать на кнопку «Далее» (в соответствии с *рисунком 37*).

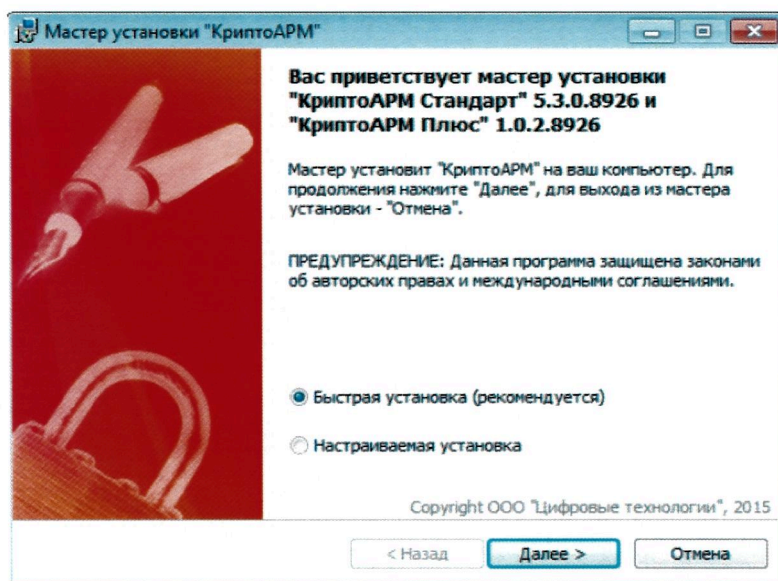


Рисунок 37

3) Далее необходимо принять условия лицензионного соглашения и нажать на кнопку «Начать» (в соответствии с *рисунком 38*).

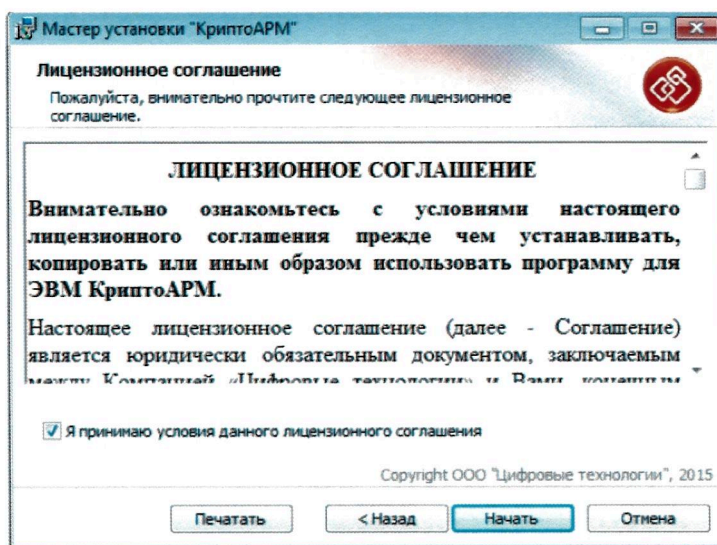


Рисунок 38

4) По завершении процесса установки программного обеспечения необходимо произвести перезагрузку персонального компьютера.

## 7.2. Подписание документов:

1) Для подписания документов необходимо правой кнопкой мыши щелкнуть на документ, в открывшемся меню выбрать пункт «КриптоАРМ», далее нажать на пункт «Подписать...» (в соответствии с *рисунком 39*).

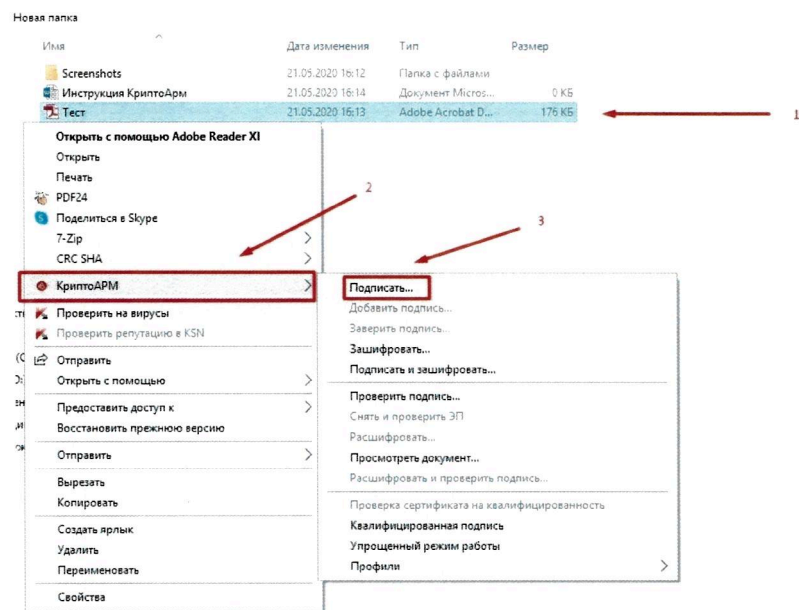


Рисунок 39

2) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с рисунком 40).

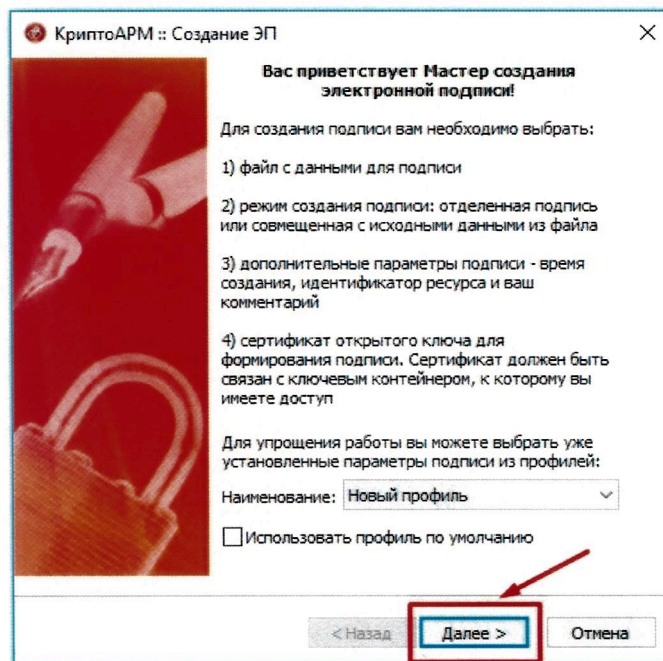


Рисунок 40

3) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с рисунком 41).



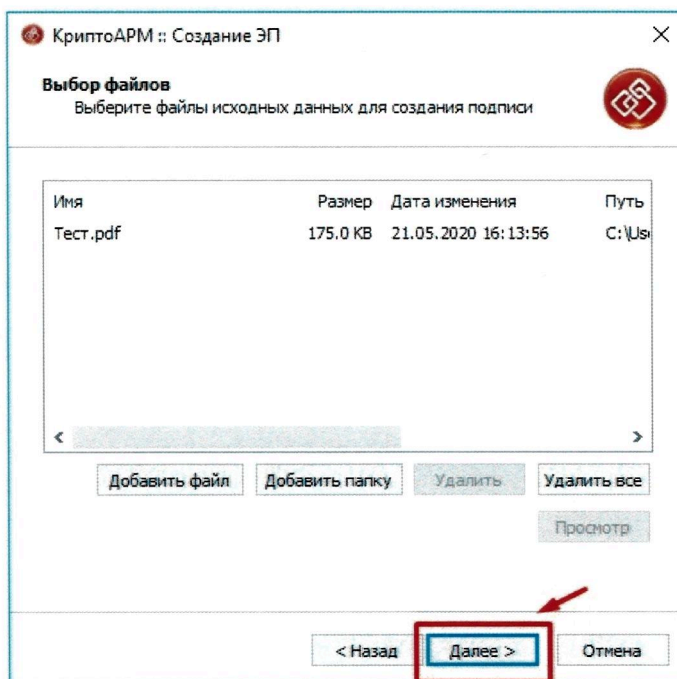


Рисунок 41

4) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с рисунком 42).

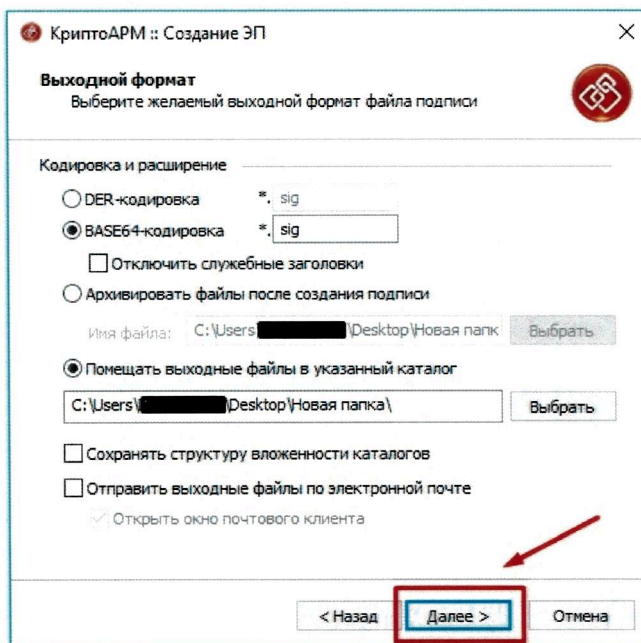


Рисунок 42

5) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с рисунком 43).

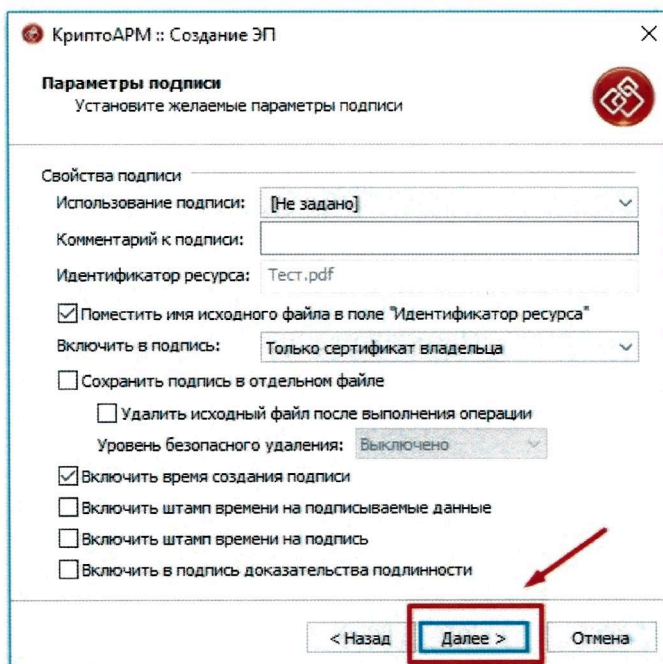


Рисунок 43

6) В открывшемся окне необходимо нажать на кнопку «Выбрать» (в соответствии с *рисунком 44*).

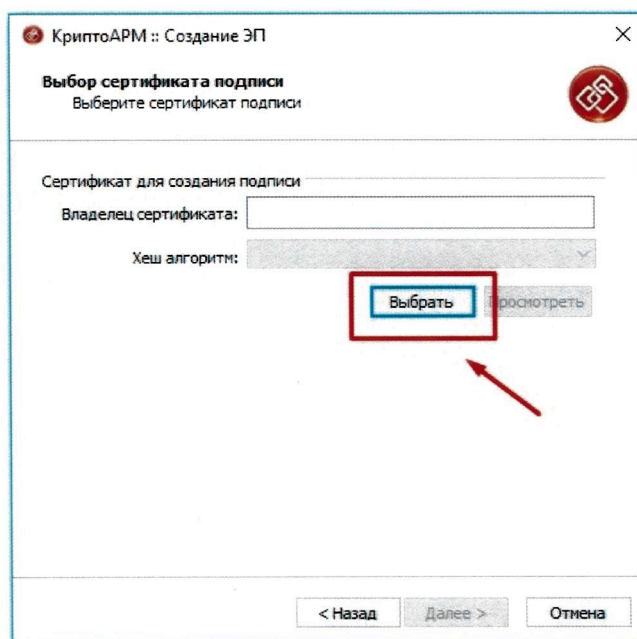


Рисунок 44

7) В открывшемся окне необходимо выбрать требующийся сертификат и нажать на кнопку «ОК» (в соответствии с *рисунком 45*).

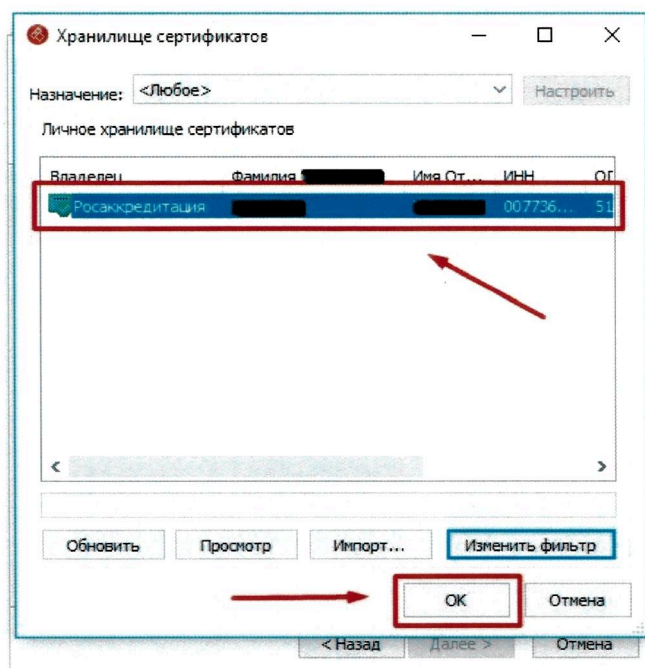


Рисунок 45

8) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с рисунком 46).

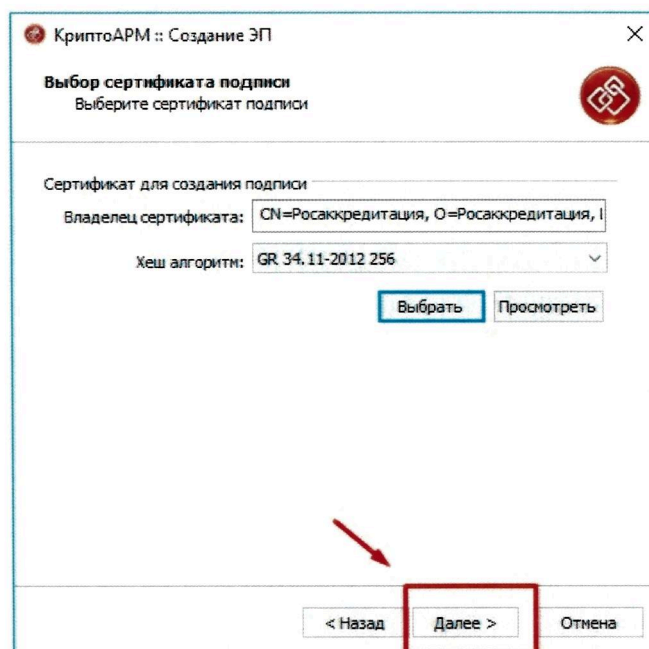


Рисунок 46

9) В открывшемся окне необходимо нажать на кнопку «Готово» (в соответствии с рисунком 47).

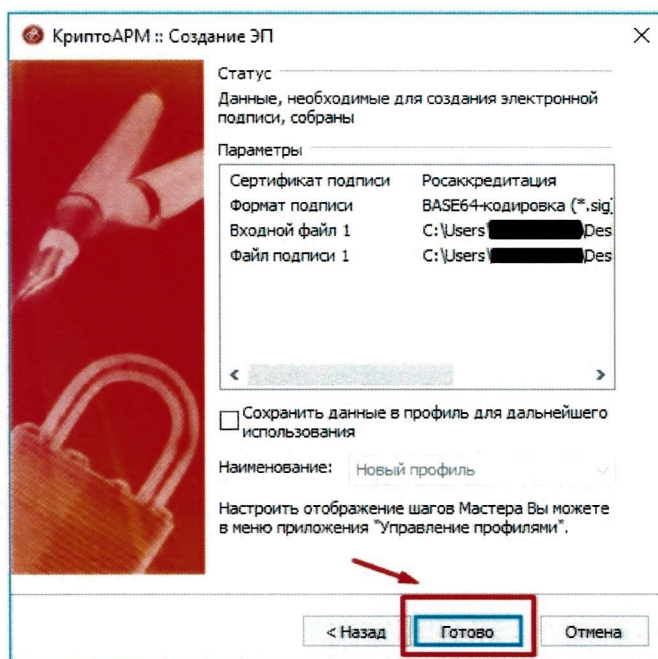


Рисунок 47

10) В открывшемся окне необходимо ввести пин-код от электронной подписи и нажать на кнопку «ОК» (в соответствии с *рисунком 48*).

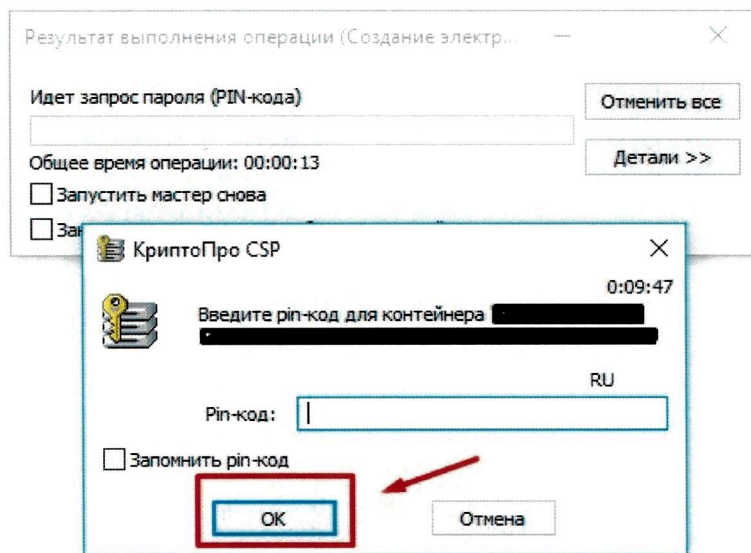


Рисунок 48

11) При успешном завершении подписания документа в той же папке появится подписанный файл (в соответствии с *рисунком 49*).


Имя	Дата изменения	Тип	Размер
Screenshots	21.05.2020 16:53	Папка с файлами	
Инструкция КристоАрм	21.05.2020 16:14	Документ Micros...	0 КБ
Тест	21.05.2020 16:13	Adobe Acrobat D...	176 КБ
 Тест.pdf	21.05.2020 16:54	Подпись PKCS #7	246 КБ



Рисунок 49

### 7.3. Проверка электронной подписи.

1) Для проверки электронной подписи необходимо щелкнуть правой кнопкой мыши на документ (подписанный), в открывшемся меню выбрать пункт «КристоАРМ», затем – пункт «Проверить подпись...» (в соответствии с *рисунком 50*).

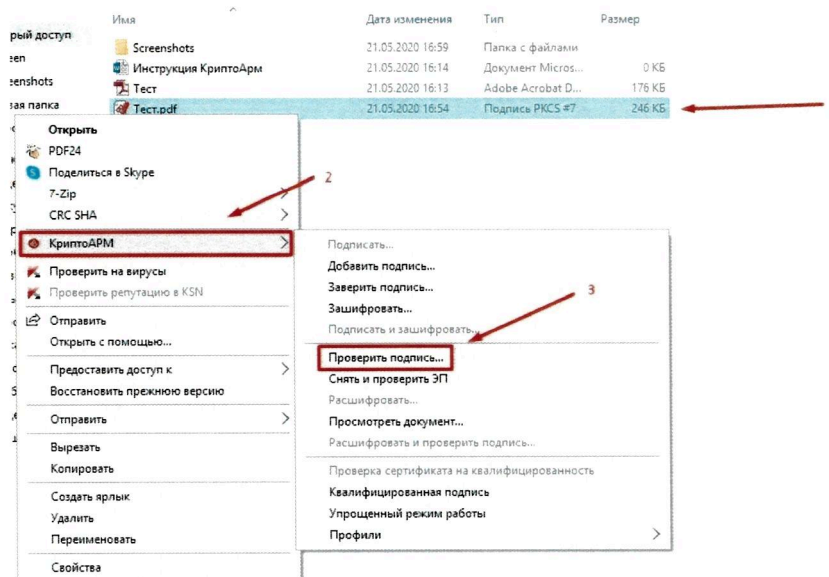


Рисунок 50

2) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с *рисунком 51*).

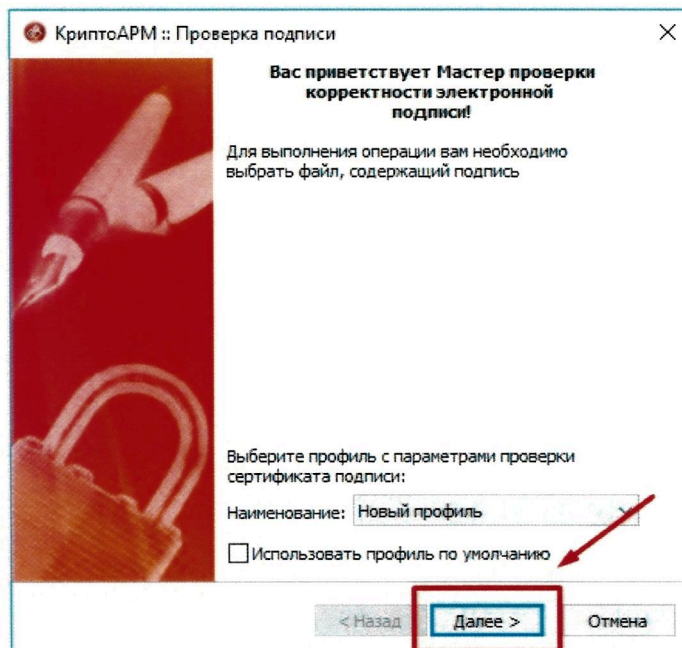


Рисунок 51

3) В открывшемся окне необходимо нажать на кнопку «Далее» (в соответствии с рисунком 52).

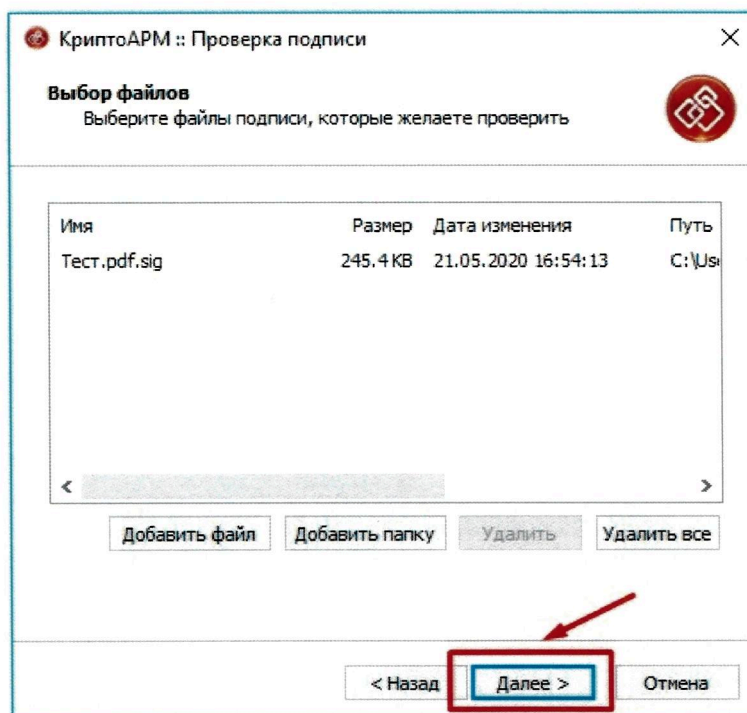


Рисунок 52

4) В открывшемся окне необходимо нажать на кнопку «Готово» (в соответствии с рисунком 53).

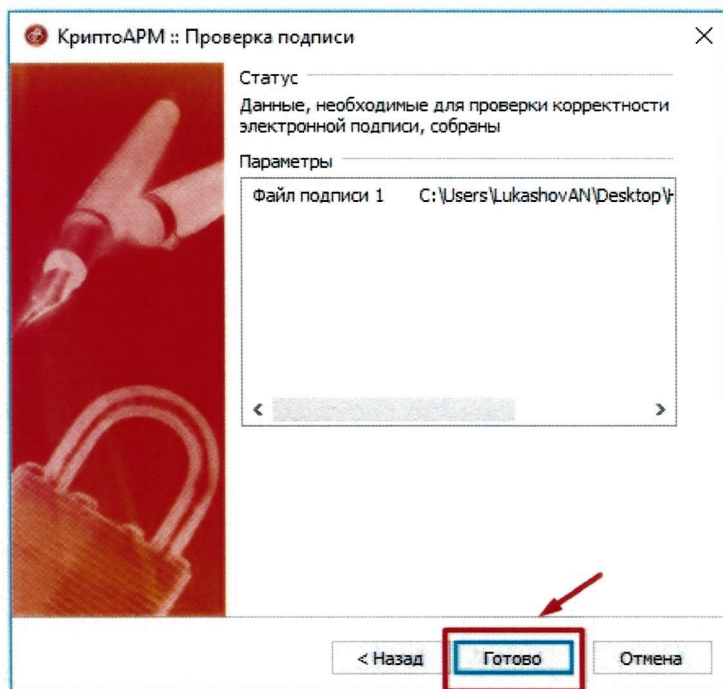


Рисунок 53

5) При успешном завершении проверки появится соответствующее окно (предупреждение об отсутствии доверия к сертификату допустимо) (в соответствии с рисунком 54).

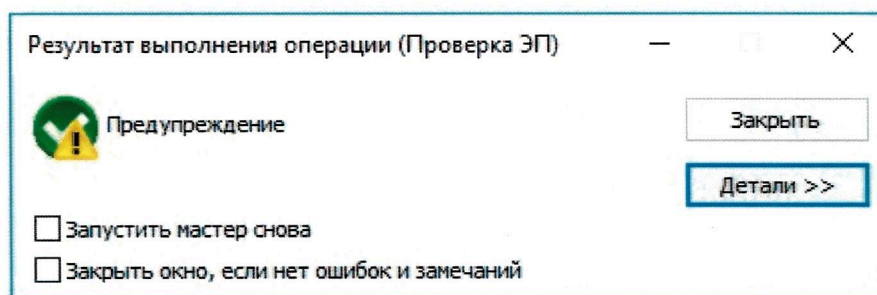


Рисунок 54

## 8. Дополнительная информация

8.1. Руководство по эксплуатации Контур.Крипто: <https://crypto.kontur.ru/help>.

8.2. Руководство по эксплуатации КриптоАРМ: [https://cryptoarm.ru/upload/docs/user\\_guide.pdf](https://cryptoarm.ru/upload/docs/user_guide.pdf).

