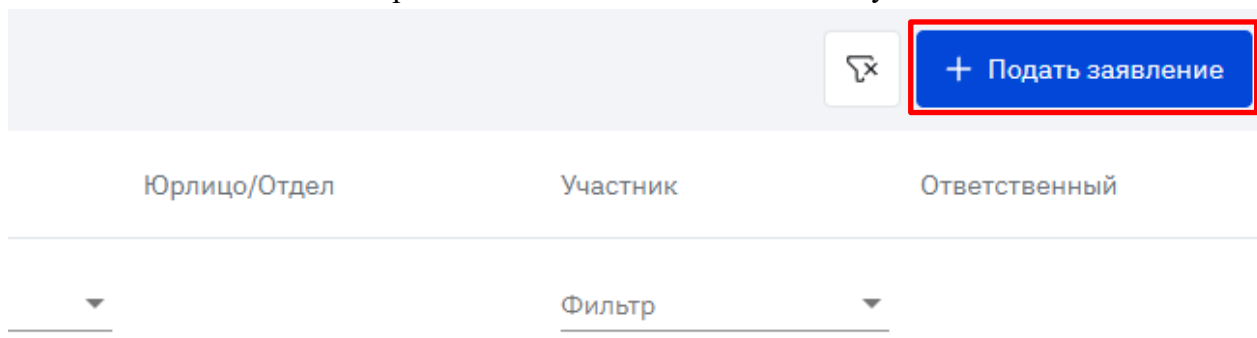


Оглавление

Подписание произвольного файла УНЭП в HRLink:	2
Проверка подписанного в HRLink файла с помощью портала Госуслуг	5
Проверка подписанного в HRLink файла с помощью КриптоПро CSP/КриптоАРМ ГОСТ.7	
Подготовительные действия	7
Процесс проверки подписанного файла с помощью КриптоПро CSP	13
Процесс проверки подписанного файла с помощью КриптоАРМ ГОСТ	15

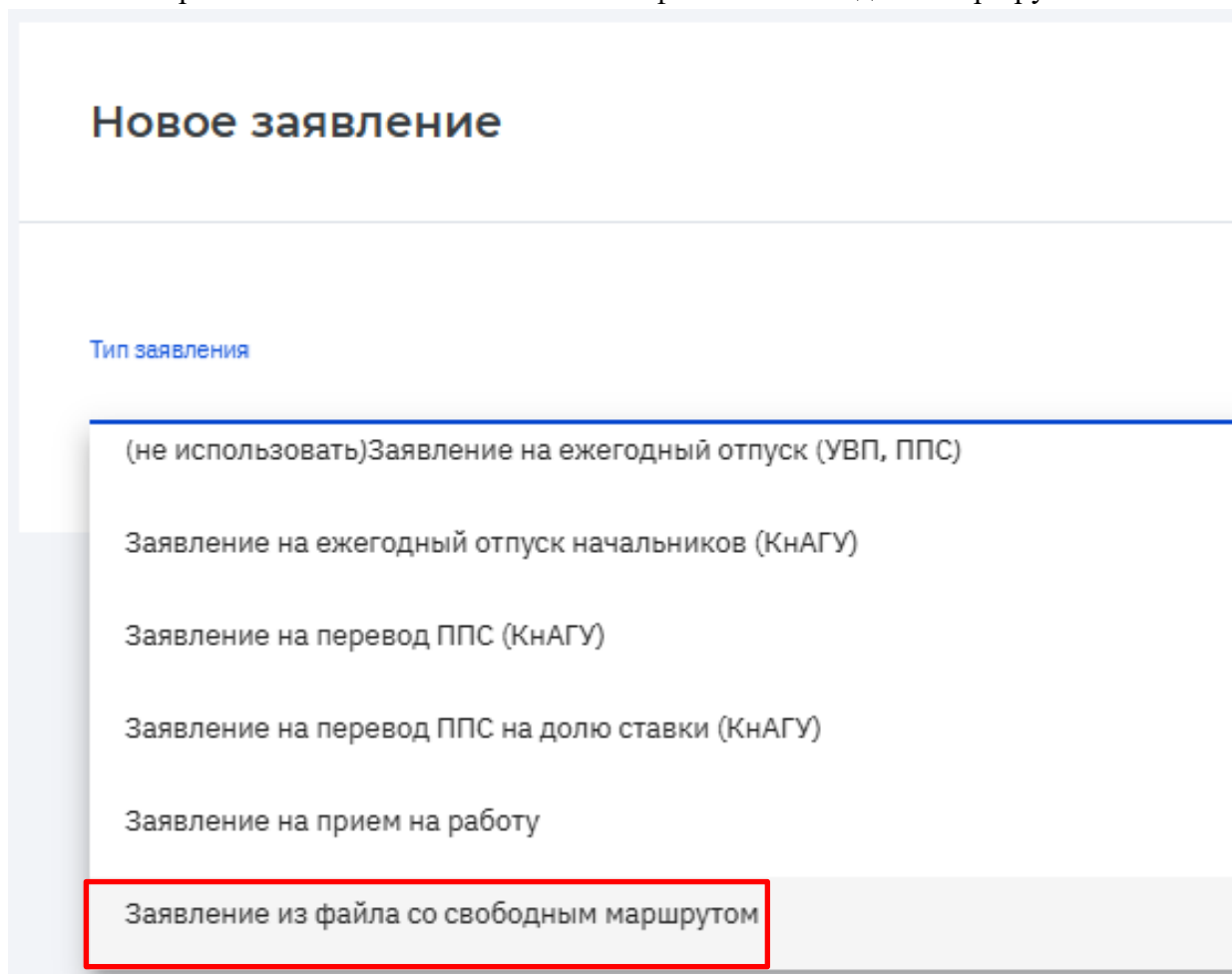
Подписание произвольного файла УНЭП в HRLink:

1. В системе HRLink в разделе заявления нажимает кнопку «Подать заявления»



The screenshot shows the top part of the HRLink interface. At the top right, there is a blue button with a white plus sign and the text «Подать заявление», which is highlighted with a red rectangular box. Below this, there are three columns with headers: «Юрлицо/Отдел», «Участник», and «Ответственный». At the bottom of this section, there is a «Фильтр» button with a dropdown arrow on its right side.

2. Выбираем тип заявления «Заявление из файла со свободным маршрутом»



The screenshot shows the 'Новое заявление' (New Statement) form. The title 'Новое заявление' is at the top. Below it, there is a section titled 'Тип заявления' (Statement Type). A dropdown menu is open, showing several options. The option 'Заявление из файла со свободным маршрутом' (Statement from file with free route) is highlighted with a red rectangular box. The other options in the list are: '(не использовать)Заявление на ежегодный отпуск (УВП, ППС)', 'Заявление на ежегодный отпуск начальников (КНАГУ)', 'Заявление на перевод ППС (КНАГУ)', 'Заявление на перевод ППС на долю ставки (КНАГУ)', and 'Заявление на прием на работу'.

3. В качестве согласующего никого не выбираем и в разделе «Файл заявления» нажимаем на кнопку «Выберите файл».

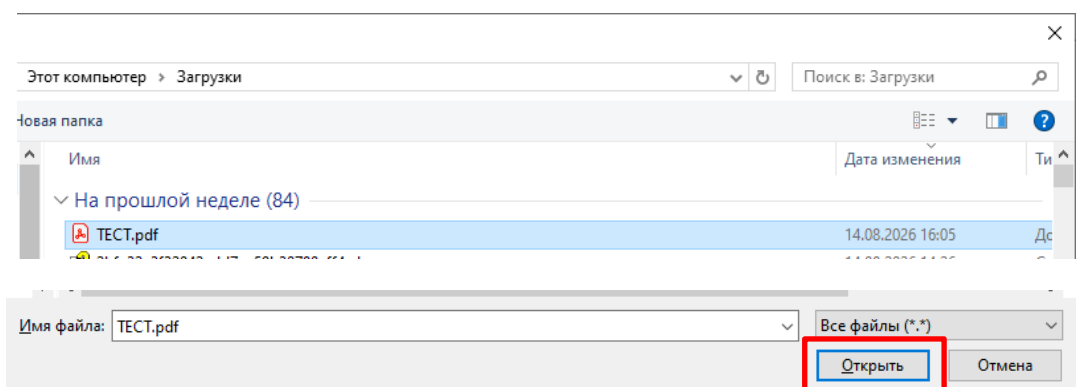
Согласующий

Файл заявления

- Поддерживаемые форматы файлов: .pdf, .doc, .docx, .xls, .xlsx, .rtf, .jpeg, .jpg, .bmp, .png, .tiff
- Максимальный размер файла - 100 МБ

Выберите файл

4. В окне выбора файла указываем требуемый файл и нажимаем «Открыть»



5. Нажимаем кнопку «Перейти к подписанию»

Файл заявления

- Поддерживаемые форматы файлов: .pdf, .doc, .docx, .xls, .xlsx, .rtf, .jpeg, .jpg, .bmp, .png, .tiff
- Максимальный размер файла - 100 МБ

ТЕСТ.pdf

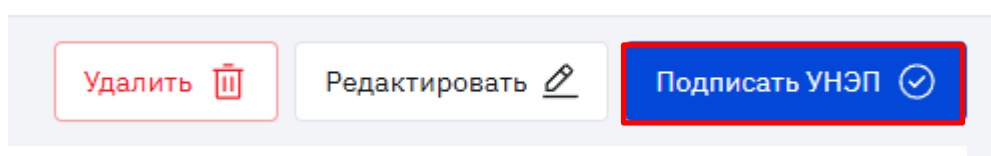
Вложения

- Поддерживаемые форматы файлов: .pdf, .doc, .docx, .xls, .xlsx, .rtf, .jpeg, .jpg, .bmp, .png, .tiff, .zip, .sig, .sgn, .xml
- Максимальный суммарный размер загружаемых файлов - 100 МБ

Выберите файлы

Перейти к подписанию

6. В следующем окне необходимо дождаться формирования заявления (время зависит от размера подгружаемого файла) и после нажать на кнопку «Подписать УНЭП»



7. Для подписания файла необходимо ввести код который придет либо в мобильное приложение либо на электронную почту. После ввода кода нажимаем кнопку «Подписать»

Подписание заявления



Отправили код подписания в **пуш-уведомления HRlink**.

Код подписания

Введите 6 цифр кода

Отмена

Подписать

8. После завершения подписания для получения подписанного открепленной

подписью файла необходимо нажать на кнопку



9. В результате на компьютер будет загружен архив с тремя файлами:

- Исходный файл
- Печатная форма исходного файла (исходный файл со штампом подписи)
- Информационный файл о подписании с расширением xml
- **Открепленная электронная подпись (файл с расширением sig).**

Файл с расширением sig является файлом открепленной подписи, которая удостоверяет авторство документа и по которому можно проверить истинность электронной подписи.

Проверка подписанного в HRLink файла с помощью портала Госуслуг

1. Из скаченного после подписания в системе HRLink архива с подписью извлекаем исходный файл и файл электронной подписи (файл с расширением sig)
2. Переходим в браузере по ссылке <https://e-trust.gosuslugi.ru/check/sign-unep>

Проверка ЭП ▾ Проверка МЧД ▾ Реестры ▾ Мониторинг АУЦ

Проверка квалифицированной ЭП Проверка УНЭП Проверка сертификата

Проверка неквалифицированной электронной подписи

Проверка отсоединенной неквалифицированной электронной подписи

Данный сервис позволяет проверить усиленную неквалифицированную электронную подпись, созданную в соответствии с «Правилами создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утвержденными постановлением Правительства РФ от 1 декабря 2021 г. № 2152

Загрузите подписанный документ для проверки

Перетащите файл или выберите на компьютере

[Выбрать файл](#)

Можно выбрать файл на 100 Мб

Загрузите файл отсоединенной электронной подписи для проверки

Перетащите файл или выберите на компьютере

[Выбрать файл](#)

Допустимые форматы файла: p7s, sign, sig, sgn

Можно выбрать файл на 1 Мб

[Проверить](#)

3. Указываем исходный файл, файл открепленной электронной подписи и нажимаем кнопку «Проверить». В отчете смотрим статус ЭП.

Отчет о проверке неквалифицированной электронной подписи

Подпись НЕДЕЙСТВИТЕЛЬНА

Подпись 1

Статус ЭП

Электронная подпись верна

Статус сертификата ЭП

Сертификат был выдан недоверенным УЦ

Владелец сертификата

[Redacted]

Издатель сертификата

ООО \"АСТРАЛ-СОФТ\"

Серийный номер

[Redacted]

Отпечаток

[Redacted]

Действует

[Redacted]

[Загрузить сертификат](#)

Важно: Информация о том, что подпись недействительна связана с тем, что сертификат выдан недоверенным удостоверяющим центром, что в случае неквалифицированной ЭП допускается, на этот статус внимание не обращаем.

Важно: Для проверки электронной подписи данным способом на АРМ пользователя **не требуется** наличие установленных средств электронной подписи.

Проверка подписанного в HRLink файла с помощью КриптоПро CSP/КриптоАРМ ГОСТ

Подготовительные действия

Указанные ниже действия производятся единожды и не требуют повторения при каждой проверке.

1. Система HRLink не позволяет выгрузить сертификат электронной подписи, который требуется при локальной проверке подписи. Для получения сертификата электронной подписи необходимо единожды воспользоваться проверкой с помощью портала Госуслуг (см. предыдущий раздел) и нажать на кнопку «Загрузить сертификат».

Отчет о проверке неквалифицированной электронной подписи

Подпись НЕДЕЙСТВИТЕЛЬНА

Подпись 1

Статус ЭП

Электронная подпись верна

Статус сертификата ЭП

Сертификат был выдан недоверенным УЦ

Владелец сертификата

Магола Дмитрий Степанович

Издатель сертификата

ООО \"АСТРАЛ-СОФТ\"

Серийный номер

050B788300A6B47093408D234345798817

Отпечаток

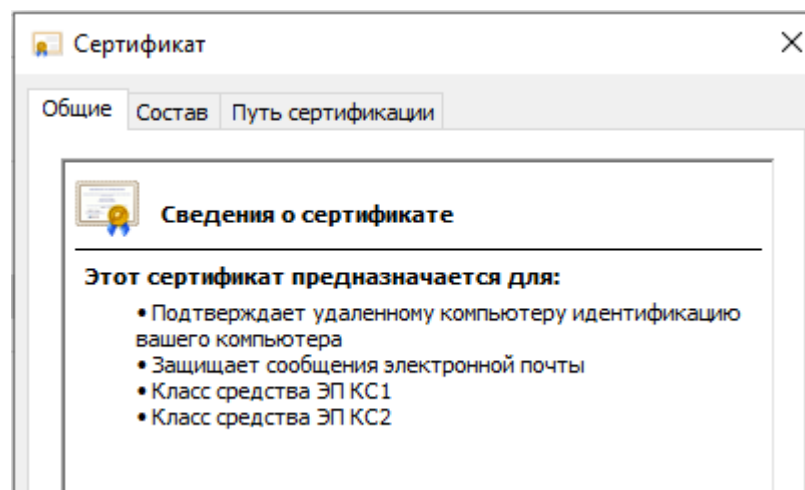
8D84E8CBD1F867D63A70F109EF83322CC532D8B0

Действует

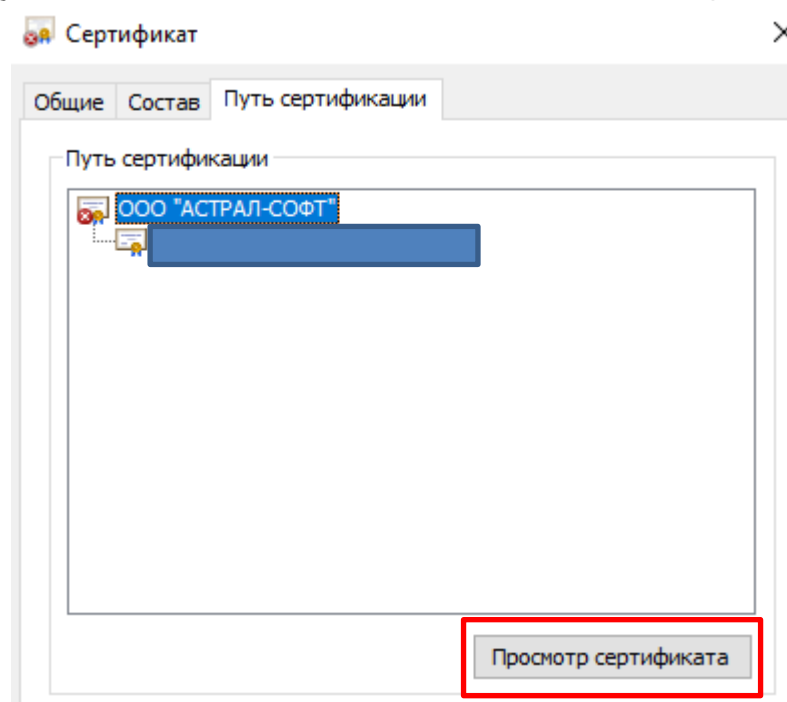
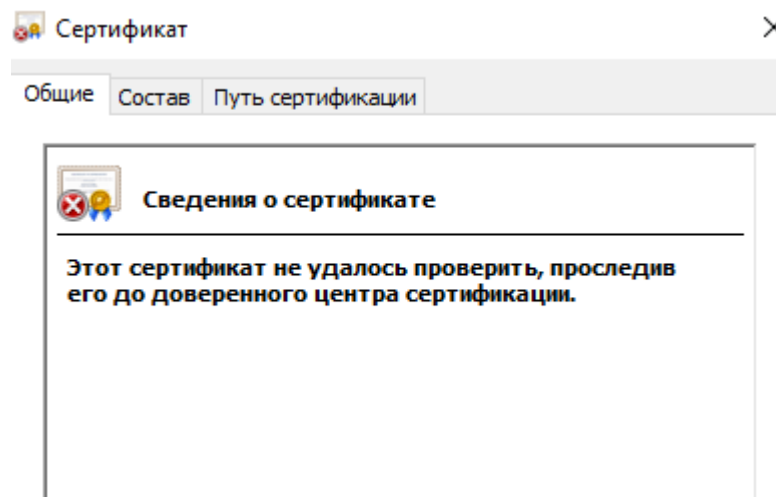
с 14.08.2026 по 14.08.2027

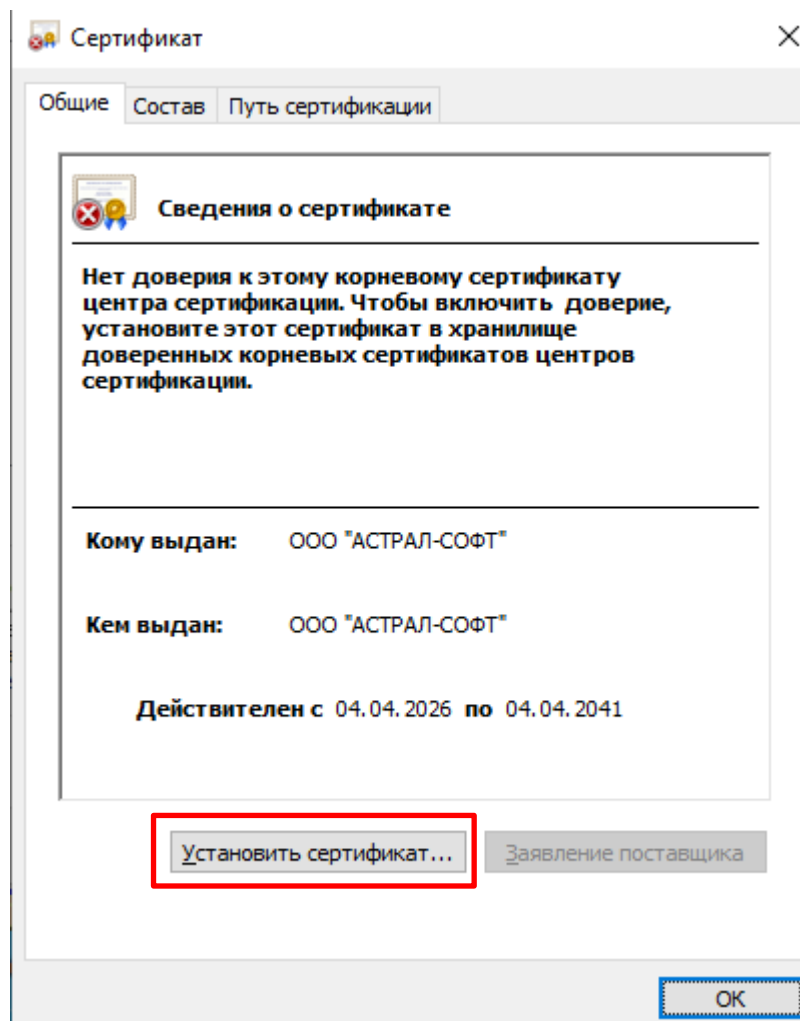
Загрузить сертификат

2. Загруженный сертификат (файл с расширением cer) запустить двойным щелчком и убедиться, что сертификат действительный. Если сертификат действительный, то переходим на шаг 8.

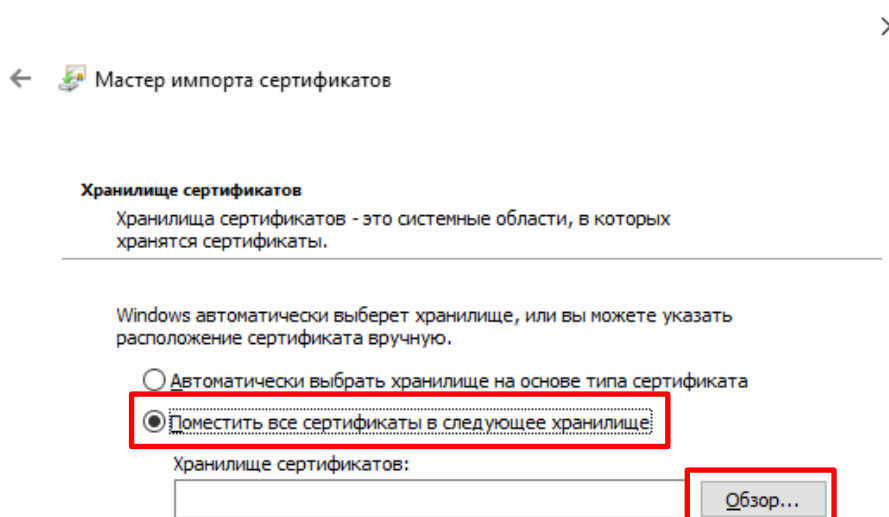


3. Если при проверке отражена информация, что сертификат не удалось проверить, то необходимо установить корневой сертификат УЦ. Для этого в окне сертификата необходимо перейти на вкладку «Путь сертификации», выбрать сертификат Астрал-Софт и нажать на кнопку «Просмотр сертификата»

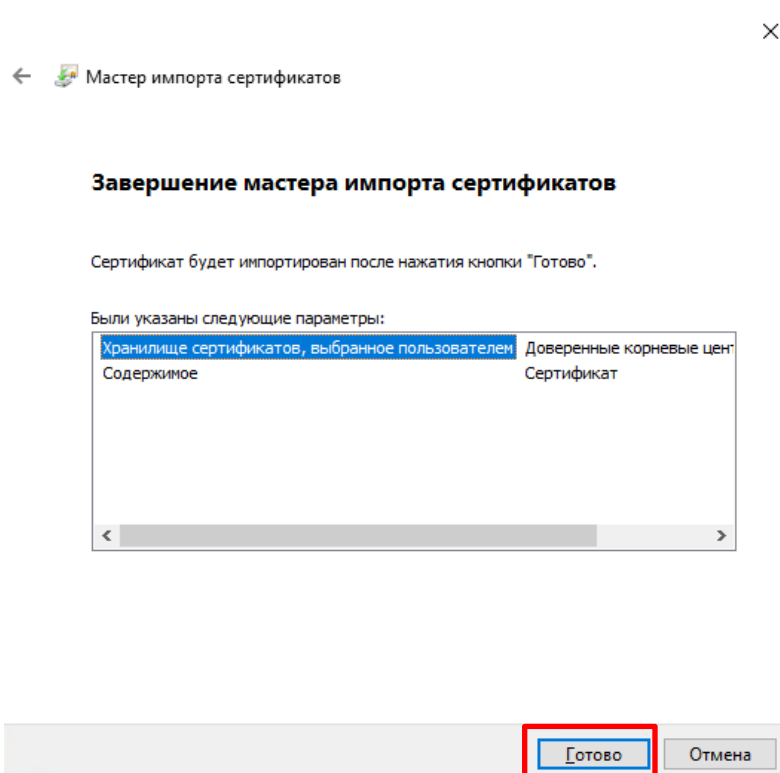
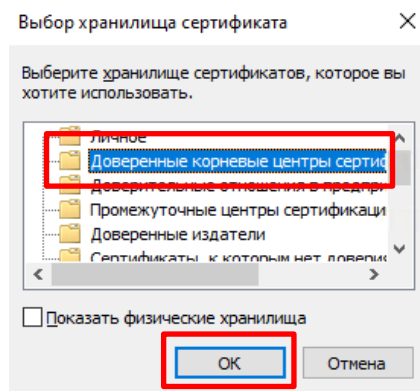




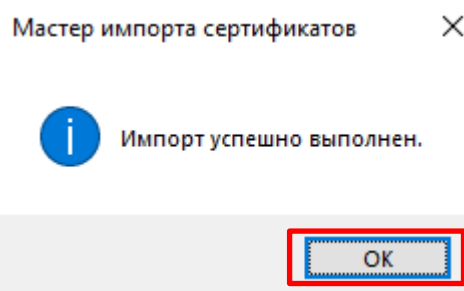
4. Нажимаем «Установить сертификат», выбираем «Поместить все сертификаты в следующее хранилище» и нажимаем «Обзор»



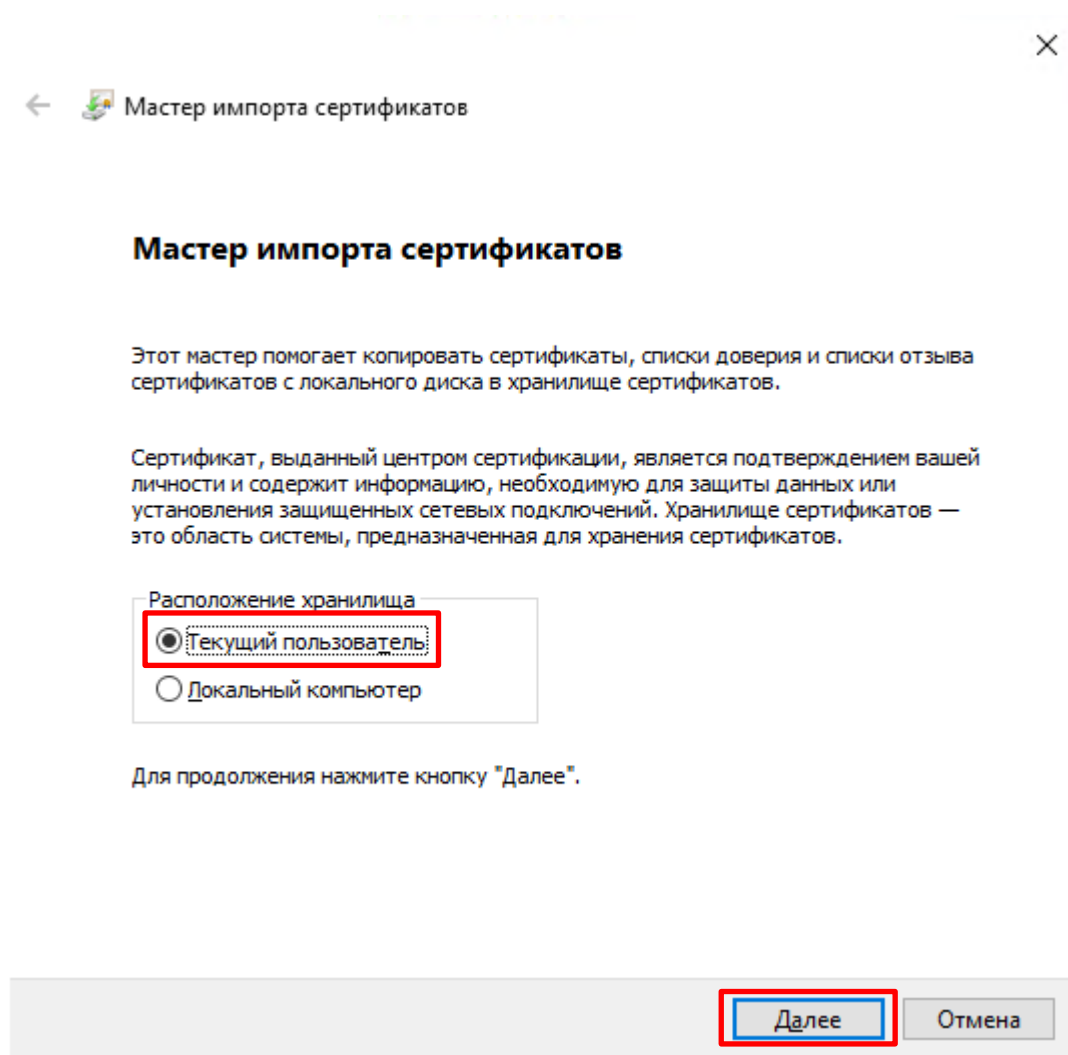
5. Выбираем «Доверенные корневые центры сертификации» и нажимаем «Ок», затем нажимаем «Далее» и «Готово»



6. В появившемся сообщении нажимаем «Да», а после «Ок»



7. Повторно запускаем двойным щелчком мыши сертификат пользователя (см. п.2) и проверяем, что сертификат действительный.
8. Нажимаем на кнопку «Установить сертификат», выбираем «Текущий пользователь» и нажимаем «Далее»



9. Нажимаем «Далее», затем «Готово», затем «Ок».



Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

☒ Автоматически выбрать хранилище на основе типа сертификата

☐ Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Обзор...

Далее

Отмена

Мастер импорта сертификатов

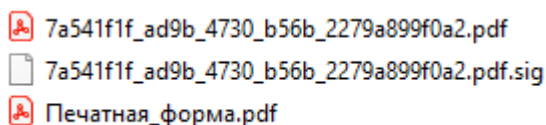


Импорт успешно выполнен.

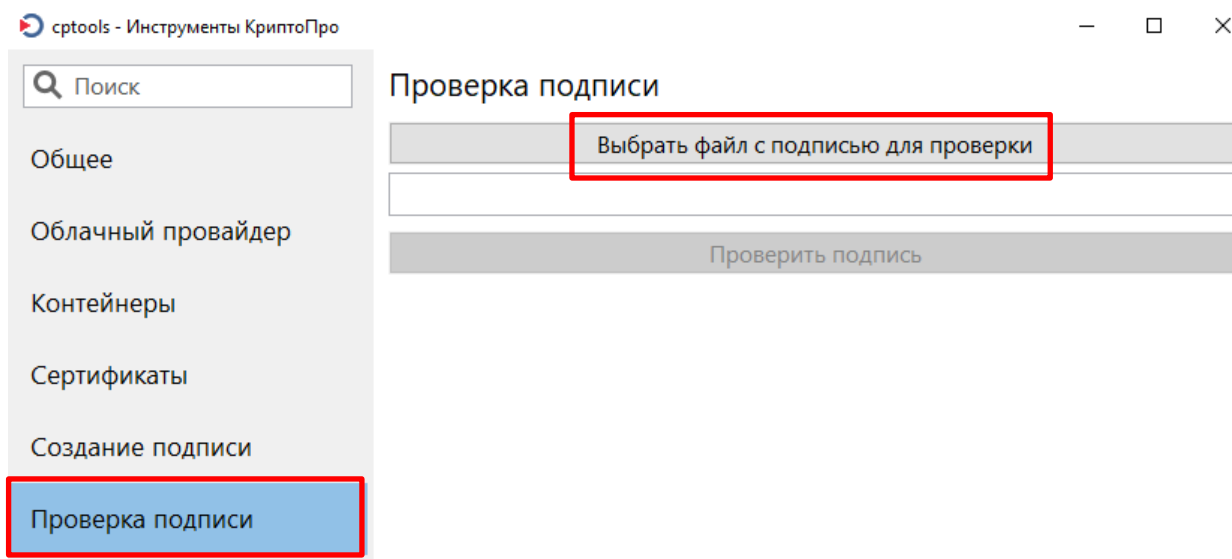
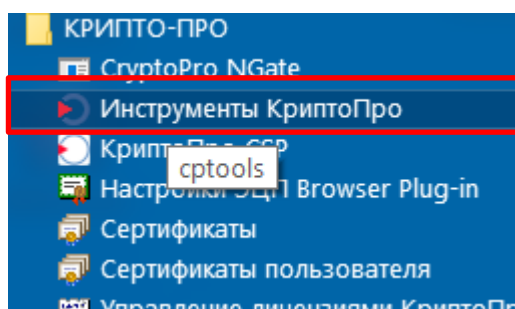
ОК

Процесс проверки подписанного файла с помощью КриптоПро CSP

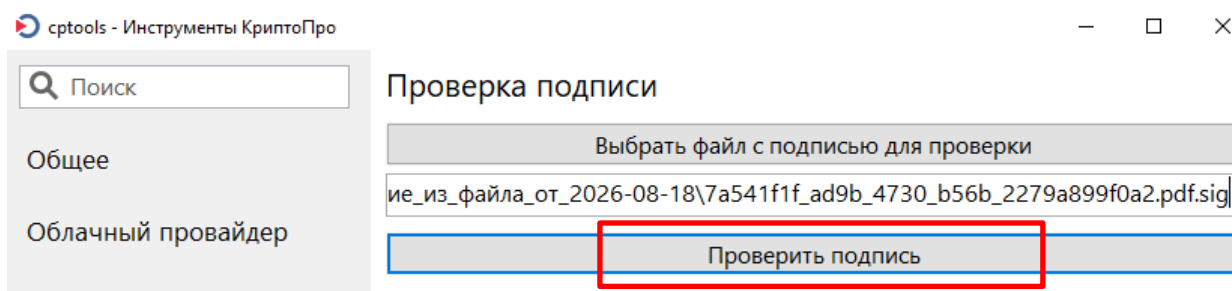
1. По умолчанию выгруженный архив с системы HR link включает файлы с разными именами. Для СКЗИ «КриптоПро CSP» и «КриптоАРМ ГОСТ» важно чтобы имя файла открепленной подписи отличалось от имени исходного файла только добавлением расширения «sig», поэтому **обязательно** переименуйте исходный файл и файл подписи, чтобы они имели одинаковые имена за исключением добавления в имя файла подписи расширения «.sig». Например, если исходный файл называется «123456.pdf», то файл подписи должен называться «123456.pdf.sig».



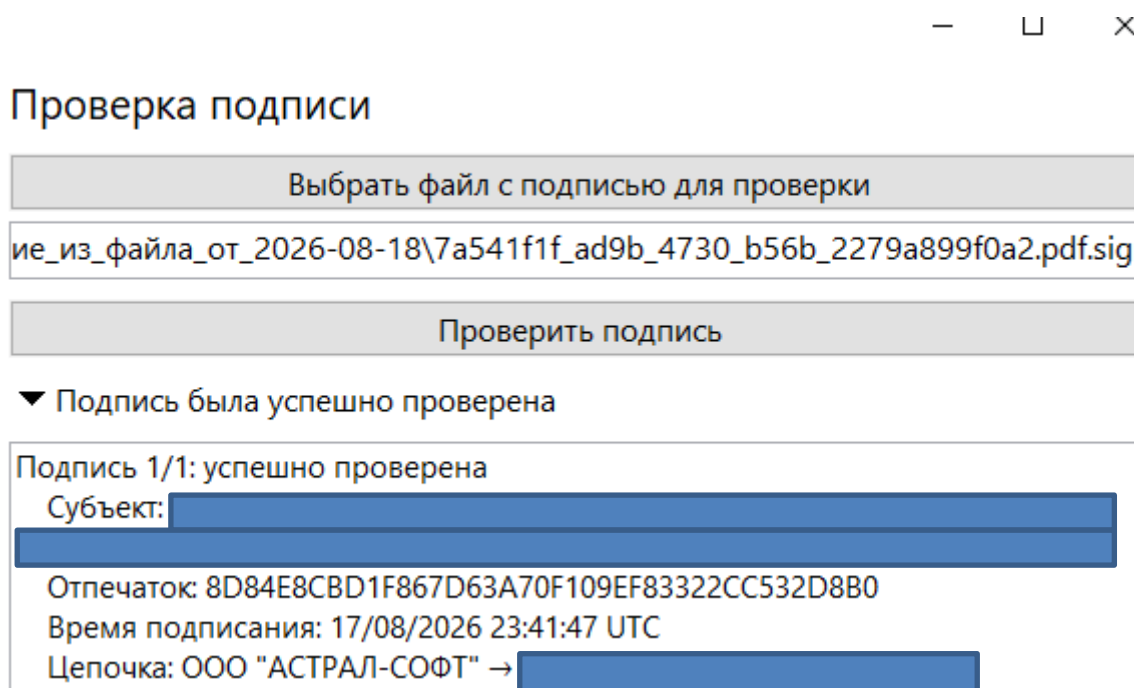
2. Откройте «Инструменты КриптоПро», перейдите в раздел «Проверка подписи»



3. Нажмите на кнопку выбора файла подписи и укажите соответствующий файл



4. Нажмите на кнопку «Проверить подпись» и раскройте результат проверки



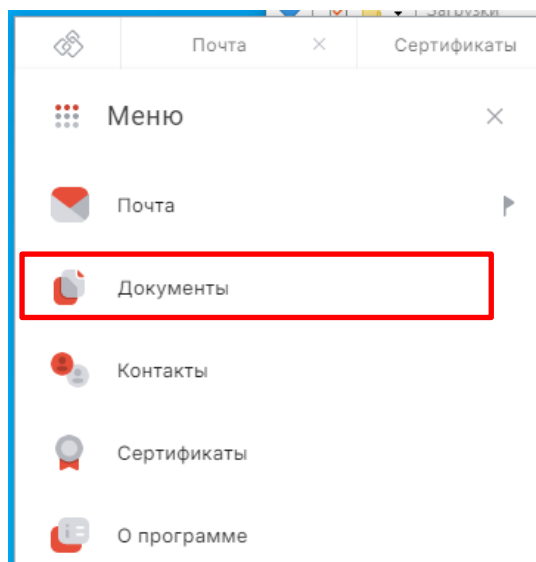
Важно: Для проверки электронной подписи данным способом на АРМ пользователя **требуется** наличие установленного СКЗИ «КриптоПро CSP 5.0» с наличием лицензии на использование ПО (демонстрационная лицензия действует 90 календарных дней)

Процесс проверки подписанного файла с помощью КриптоАРМ ГОСТ

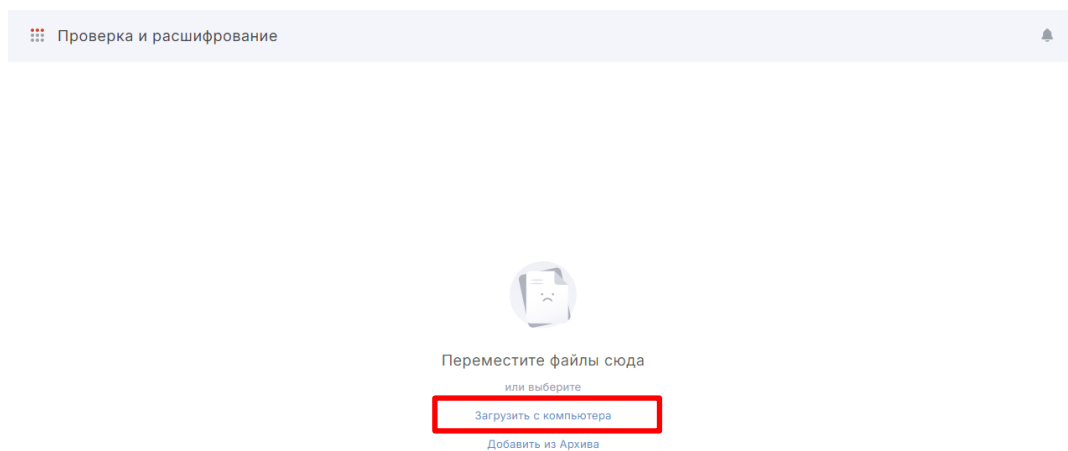
1. По умолчанию выгруженный архив с системы HR link включает файлы с разными именами. Для СКЗИ «КриптоПро CSP» и «КриптоАРМ ГОСТ» важно чтобы имя файла отсоединенной подписи отличалось от имени исходного файла только добавлением расширения «sig», поэтому обязательно переименуйте исходный файл и файл подписи, чтобы они имели одинаковые имена за исключением добавления в имя файла подписи расширения «.sig». Например, если исходный файл называется «123456.pdf», то файл подписи должен называться «123456.pdf.sig»

 7a541f1f_ad9b_4730_b56b_2279a899f0a2.pdf
 7a541f1f_ad9b_4730_b56b_2279a899f0a2.pdf.sig
 Печатная_форма.pdf

2. Откройте «КриптоАРМ ГОСТ», перейдите в раздел «Документы»

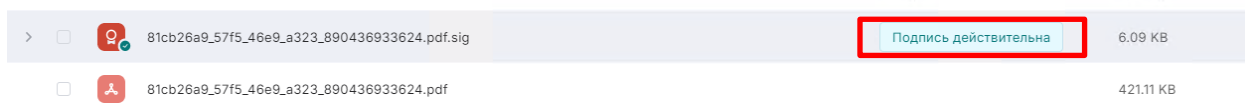


3. Выберите «Проверка и расшифрование»



4. Перетащите на область «КриптоАРМ» исходный файл и файл электронной подписи или с помощью кнопки «Загрузить с компьютера» укажите их

5. Результат проверки отобразится на экране



6. При необходимости можно нажать на кнопку «Подробнее»



 81cb26a9_57f5_46e9_a323_89043693...  

О подписи

О документе

ПРОВЕРЯЕМЫЕ ФАЙЛЫ

Документ	81cb26a9_57f5_46e9_a323_8904369336...	
Файл подписи	81cb26a9_57f5_46e9_a323_890436933624.p...	

ОБЩИЙ СТАТУС

 Подпись документа действительна
Проверено 18 августа 2026 г., 10:40

ПОДПИСИ ДОКУМЕНТА (1)

 
Действительна

СВОЙСТВА ПОДПИСИ

Поставлена	17 августа 2026 г., 11:33
Математическая корректность	Верна
Стандарт	CAdES-T

ТИП ШТАМПА ВРЕМЕНИ

 Штамп времени на подпись
Действителен

ПОДПИСЧИК

Общее имя	
Email	

Важно: Для проверки электронной подписи данным способом на АРМ пользователя **требуется** наличие установленного СКЗИ «КриптоПро CSP 5.0» с наличием лицензии на использование ПО (демонстрационная лицензия действует 90 календарных дней) и установленного ПО «КриптоАРМ ГОСТ» с наличием лицензии на использование ПО (демонстрационная лицензия действует 30 календарных дней)