

# Сравнение ПО для создания ЭЦП

Программы для создания и проверки ЭП различаются возможностями, стоимостью, принципом работы. Преимущества и недостатки сервисов удобно оценить в специальной таблице сравнения ПО.

	КриптоАРМ	Онлайн-сервис Контур.Крипто
Стоимость	Бесплатная только стартовая версия	Бесплатно
Пакетная подпись	Есть	Есть
Форматы	Все	Все
Объем файла	Без ограничений	До 100 Мб
Формирование усовершенствованной ЭП	В версии стандарт и базовая	Есть
Тип ЭП	Отсоединенная/ присоединенная	Только отсоединенная
Дополнительные функции шифрования, проверки, расшифрования	В версии стандарт и базовая	Есть

С электронной цифровой подписью могут работать как физические, так и юридические лица. Ее использование наделяет ЭД юридической силой и приравнивает его к бумажному.

Для работы с ЭП необходимо иметь криптопровайдер и средства ЭЦП. К ним относят закрытый и открытый ключ и специальное ПО.

Подписание документов возможно через отдельные плагины для MS Office и Adobe Systems, а также через отдельные программы (КриптоАрм или CryptoFile) или через онлайн-сервисы.

Формирование ЭП и получение заверенного файла происходит в несколько простых шагов вне зависимости от выбранного вида средств ЭЦП.

Однако наличие определенных функций, поддерживаемые форматы и даже допустимый объем заверяемого документа уже зависят от типа и версии ПО.

# Как подписать документ электронной цифровой подписью

Использование электронной цифровой подписи позволяет заверять любой тип документов. Ее удобство в том, что ЭЦП гарантирует неизменность подписанной информации, устанавливает авторство и защищает содержимое ЭД от несанкционированного доступа третьих лиц. Заверить документ с помощью ЭЦП можно в КриптоПро, специальных приложениях для подписания файлов или через онлайн-сервисы. От выбранного способа будет зависеть доступность дополнительных функций, возможность формирования усовершенствованной подписи или создание отсоединенной ЭЦП.

## Алгоритм работы ЭЦП

Надежность квалифицированной электронной подписи объясняют криптографические процессы и функции хэширования. В процессе подписания и проверки используются сложные личные и открытые ключи, а также сертификаты открытого ключа.

Личный или закрытый ключ формируется через датчик случайных чисел и используется для подписания документов. А открытый — вычисляется из закрытого и применяется для проверки принадлежности подписи владельцу. Закрытый ключ работает только в паре с открытым, а хранить его необходимо в тайне от третьих лиц.

Если личный ключ был скомпрометирован, то необходимо обратиться в УЦ, написать заявку о признании сертификата недействительным и о перевыпуске ЭЦП. Иначе ключ может быть использован для причинения материального или иного ущерба владельцу ЭП и контрагентам.

Подписание документов ЭЦП не изменяет содержимое файла, но добавляет новый блок данных. Этот блок и является электронной подписью. Сложность процесса гарантирует неизменность информации: если после подписания документ был изменен, то исправления будут видны и в отпечатке, что отразится на проверке ЭЦП.

После того, как сформирована ЭЦП, редактирование файла подписанного документа невозможно. Если попытаться отредактировать текст или внести изменения в заверенный архив, то все ЭП удалятся, а при проверке будет выходить ошибка.

## Что необходимо для работы с ЭЦП

Чтобы подписать документ электронной подписью пользователь должен иметь:

- сформированный и проверенный файл, который необходимо заверить;
- сертификат электронной подписи с неистекшим сроком годности;

- средства ЭП (комплекс программных средств, настроенный криптопровайдер и браузер);
- средства для создания электронной подписи.

К программам для создания ЭП относят плагины для MS Office и PDF, отдельные программы (КриптоАрт) или онлайн-сервисы. Часть из них дает возможность подписать документа бесплатно, часть имеет ограниченный бесплатный функционал, а некоторые доступны только после покупки.

# Подписание при помощи специального ПО

Документы можно подписывать также через специальное программное обеспечение — КриптоАрт.

## КриптоАрт

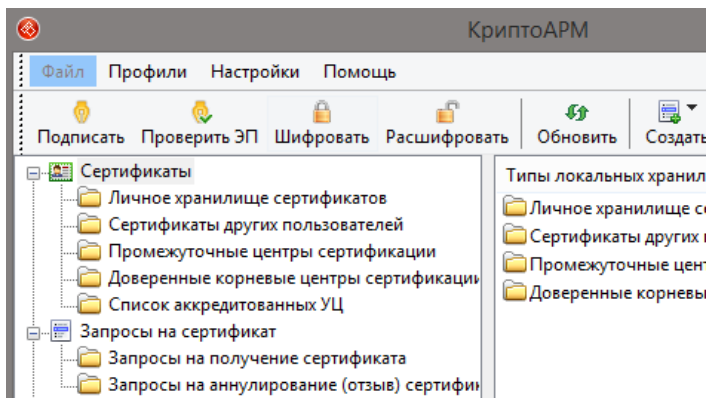
Продукт КриптоАрт создан для проверки электронных ключей, шифрования и расшифрования данных, для работы с криптопровайдерами с использованием криптоалгоритмов, отвечающих требованиям ФСБ РФ. Бесплатно пользователь может получить только стартовую версию, которая может ставить или проверять подписи на документах в формате pdf, Word, Excel и т.д.

Базовая и стандартная версии программы приобретаются за дополнительную плату, и обладают такими функциями, как:

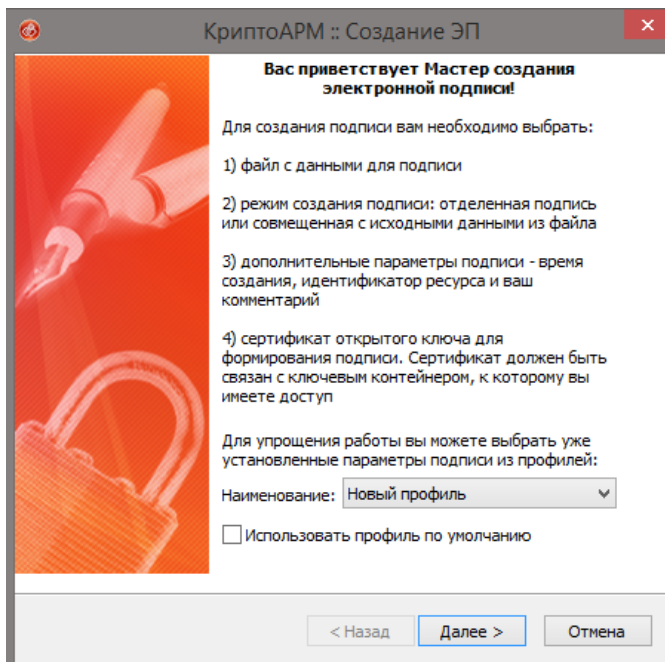
- создание и проверка корректности ЭП;
- расшифрование и шифрование файлов произвольного формата;
- поддержка модуля усовершенствованной подписи и т.д.

Как ставить подпись в электронном документе при помощи КриптоАрт:

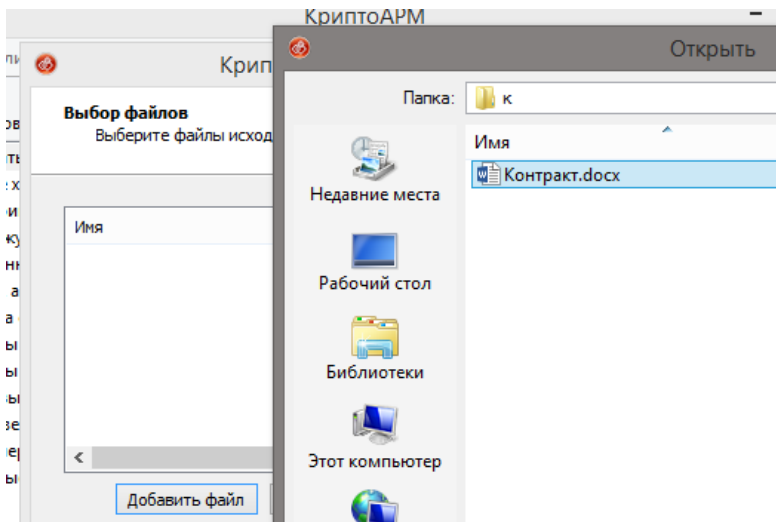
- открыть программу и выбрать «Подписать»;



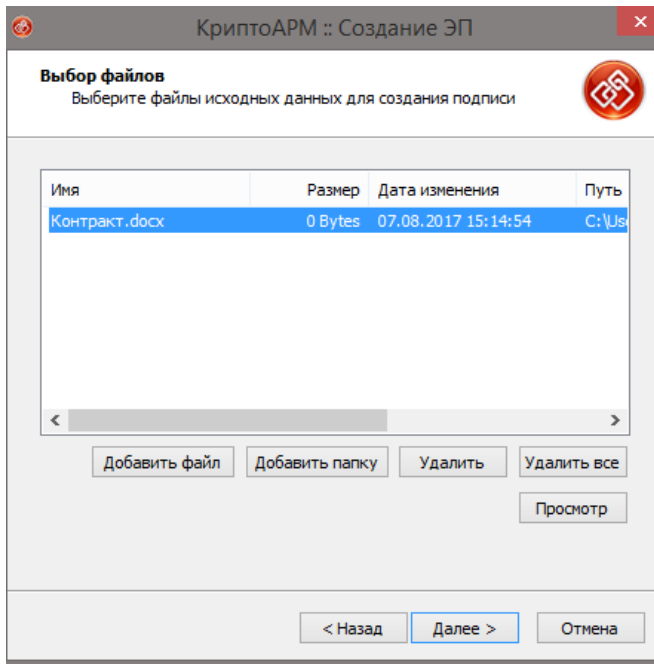
- после ознакомления с инструкцией нажать «Далее»;



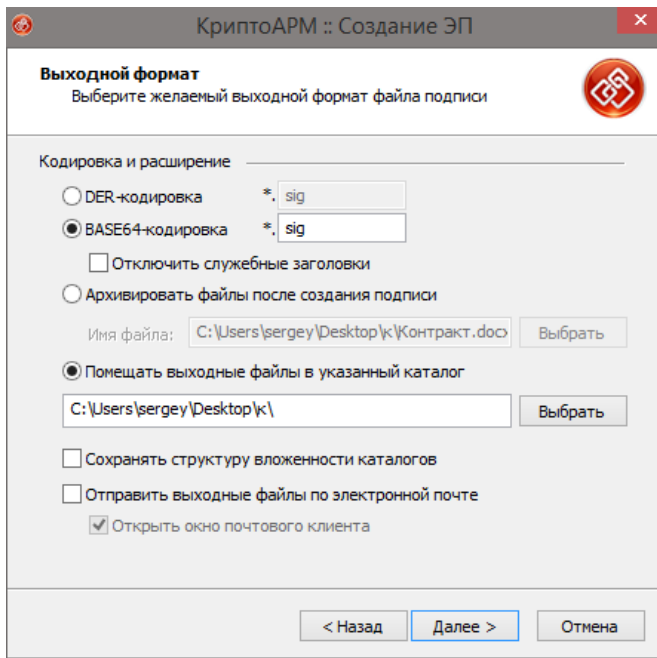
- затем нажать «Выбор файла» и «Далее»;



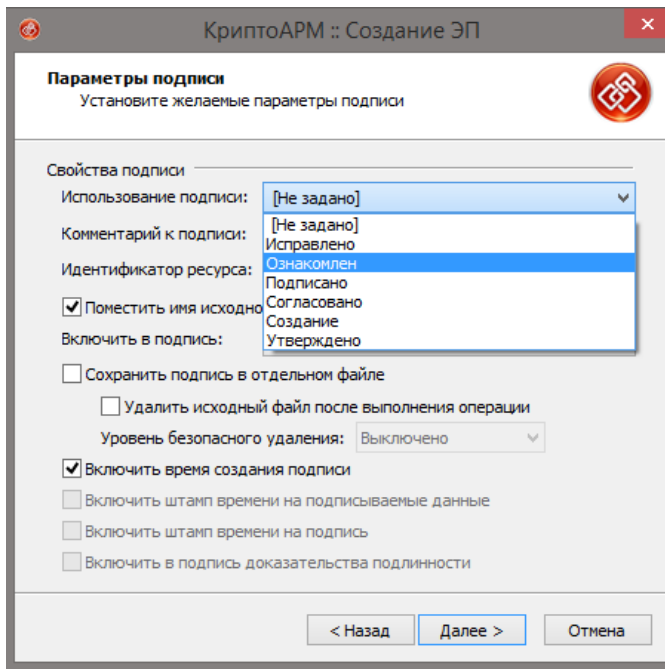
- после выбора электронного документа нужно еще раз нажать «Далее»;



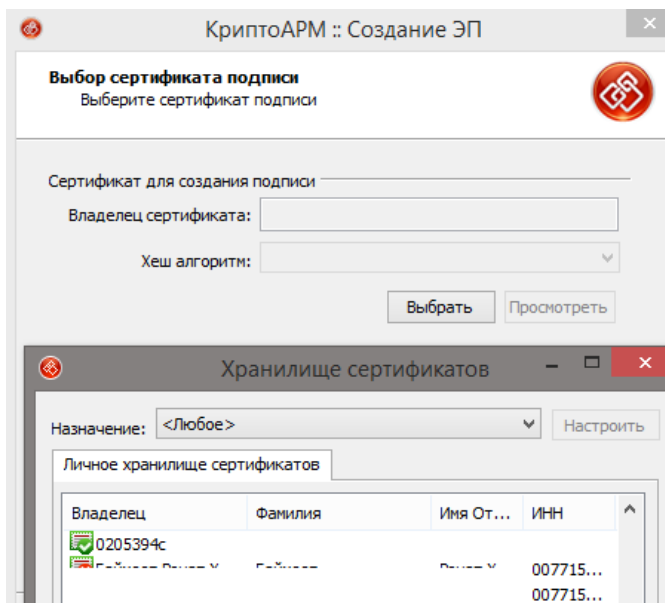
- в новом окне «Выходной формат» можно оставить кодировку в исходном значении, а можно поменять под нужные требования. Программа для подписи может сохранить файл в любом удобном формате;



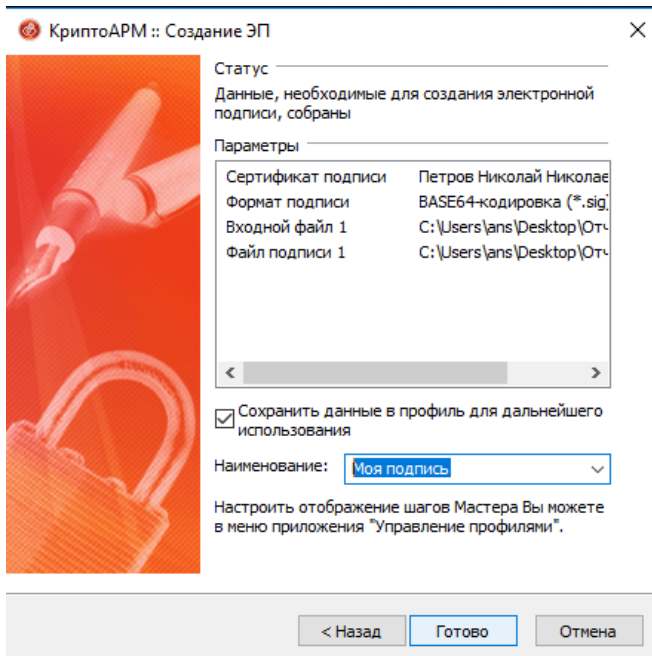
- в «Параметрах» пользователь может выбрать отсоединенную или присоединенную ЭП, добавить комментарий или свойство. Затем нажать «Далее»;



- следующий шаг — выбор нужного сертификата;



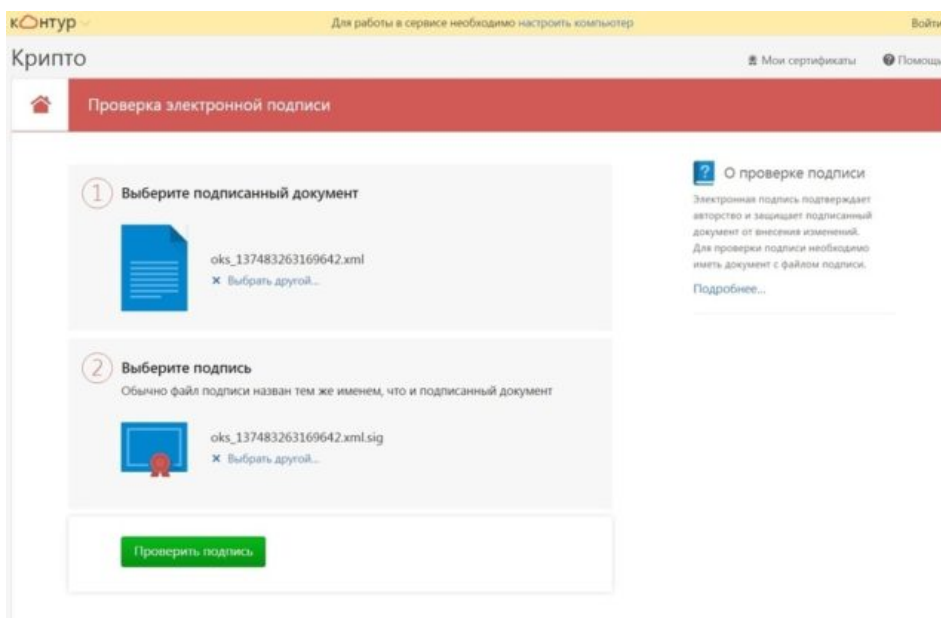
- в завершение открывается окно с описанием данных. Профиль лучше сохранить, если по шаблону будет подписано несколько документов.



Нажать «Готово». Система выдаст сообщение об успешном подписании файла.

## Использование веб-сервисов

Для того чтобы подписать ЭД необязательно приобретать программное обеспечение или плагины. Можно воспользоваться одним из онлайн-сервисов. Например, Крипто Контур (<https://crypto.kontur.ru/>). Сервис бесплатный, и позволяет проверить и создать ЭП. Контур от КриптоПро также может расшифровать и зашифровать электронный файл. Еще один плюс работы — возможность подписать договор в любом формате, пакет файлов или целый архив.



Сервис становится доступным для работы после простой регистрации и автоматической установки на ПК для выполнения криптографических преобразований. Сервис имеет понятный и удобный интерфейс, а чтобы подписать файл нужно:

- загрузить документ, который необходимо заверить ЭП;
- выбрать один из доступных сертификатов;
- создать файл ЭП;
- нажать «Подписать». Сервис автоматически создаст папку с оригинальным и подписанным файлом (расширение .sig);
- при необходимости скачать с сервера папку с ЭД

Отправка подписанного ЭД возможна также напрямую с сервера. В этом случае адресат получается ссылкой на папку, сохраненную в Крипто Контур. Скачанную папку (оригинал ЭД, файл с подписью, сертификат ЭП и инструкция по проверке ЭЦП) можно отправить через любую почтовую систему.