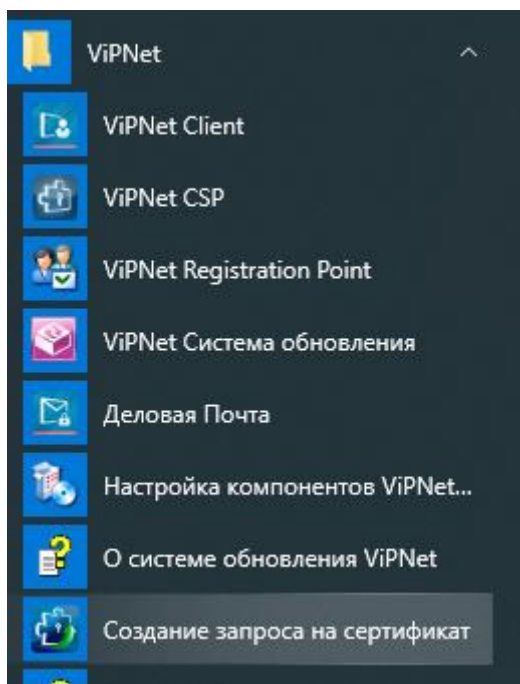
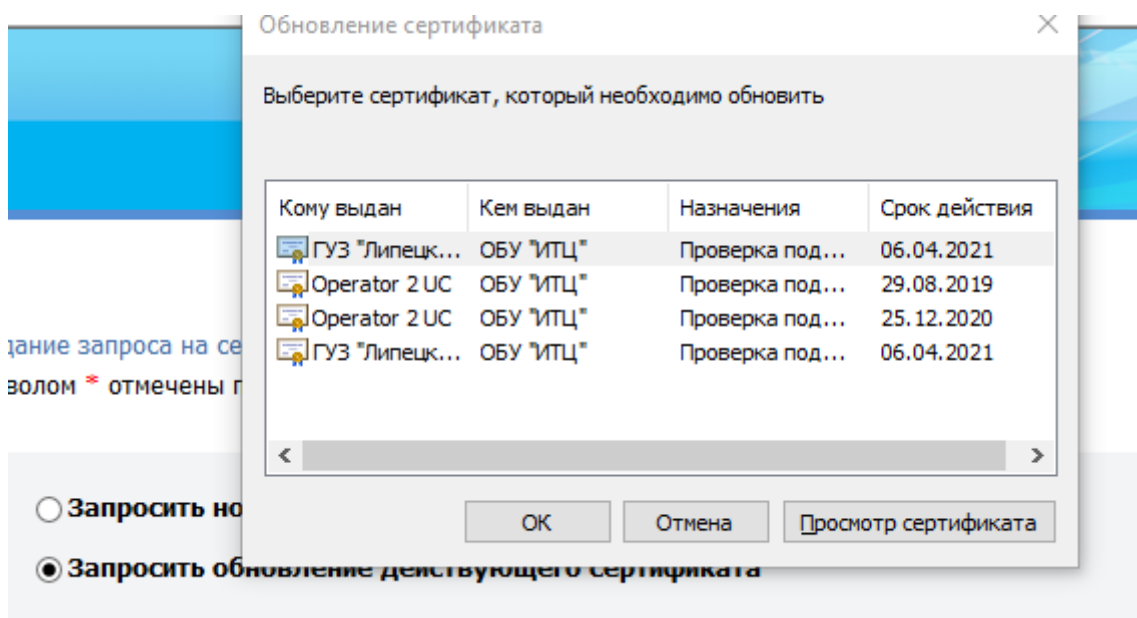


Формирование запроса на сертификат средствами ViPNet

Запустите программу Создание запроса на сертификат.



Запросите обновление действующего сертификата и из окна с сертификатами выберите сертификат, который необходимо обновить.



Нажмите **ОК**. Это поможет заполнить поля в данных о владельце сертификата.

Данные о владельце сертификата:

Для физ. лиц: имя (ФИО); для юр. лиц: наименование организации *	ГУЗ "Липецкая ГБ СМП № 1"
Имя и отчество владельца сертификата *	
Фамилия владельца сертификата *	
Адрес электронной почты	eg@lipbsmp1.ru
Организация	ГУЗ "Липецкая ГБ СМП № 1"
Подразделение	
Должность	Врач
Название улицы, номер дома	улица Космонавтов, д. 39
Населенный пункт	город Липецк
Область (Номер области - Название области)	48 Липецкая область
Страна	RU
ОГРНИП	

После этого снова выберете кнопку **Запросить новый сертификат**.

Запросить новый сертификат

Запросить обновление действующего сертификата

Параметры сертификата

Криптопровайдер:	Infotecs GOST 2012/512 Cryptographic Service Provider
Алгоритм хэширования:	GOST 34.11-2012 256
Назначение:	Подпись и шифрование
Шаблон сертификата:	Квалифицированный ViPNet CSP
Параметры ключа:	<input checked="" type="checkbox"/> Экспортируемый <input type="checkbox"/> Системный

Из выпадающего окна выберете криптопровайдер. Заполните или отредактируйте данные о владельце сертификата. Поле ИНН должно содержать 12 символов, поэтому для ИНН юридического лица впереди добавляются 00.

Выберите место для сохранения запроса на сертификат.

Сохранение запроса в файл

Имя файла: * C:\ProgramData\InfoTeCS\Requests\CertReq.p10 Обзор...

Кодировка: DER MIME (Base 64)

[Скрыть поля](#)

Сформировать запрос

Нажмите на кнопку **Сформировать запрос**. Появится окно с выбором места для хранения ключевого контейнера. Можно изменить имя контейнера, выбрать место и нажать **ОК**.

ViPNet CSP - инициализация контейнера ключей

Укажите место хранения контейнера ключей.

Имя контейнера: rnd-F-CC73-433A-3DD5-0873-388D-072E-3A47

Папка на диске: C:\Users\Администратор\AppData\ Обзор...

Выберите устройство: eToken GOST/JaCarta GOST(00000000009)

Введите ПИН-код: *****

Сохранить ПИН-код

OK Отмена

В результате появится сообщение

Служба сертификации

Сертификационный запрос создан успешно. Файл с запросом - C:\ProgramData\InfoTeCS\Requests\CertReq.p10

OK

В результате создались закрытый ключ ЭП и Запрос на сертификат ЭП.

Далее этот запрос необходимо подписать действующим сертификатом специалиста, на которого выпускается новая ЭП, и передать в Удостоверяющий центр.

Подписать запрос можно в программе КристоАрм.

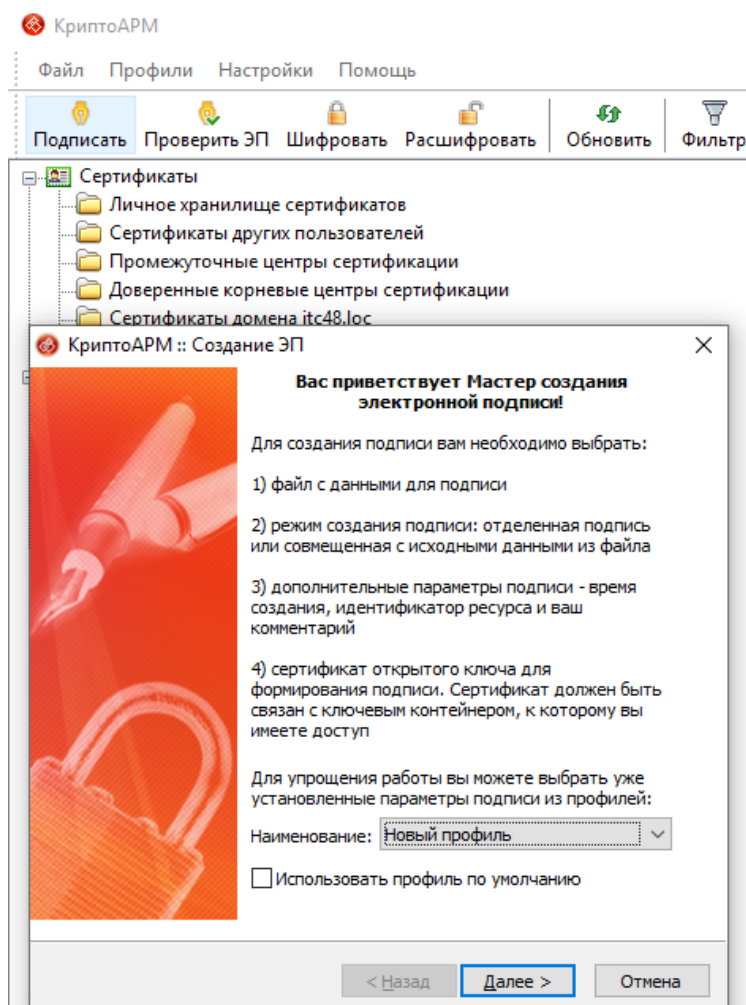
Скачать программу КристоАрм можно с официального сайта ООО «Цифровые технологии» <https://www.trusted.ru/>

У КристоАРМ имеется **14-дневный ознакомительный период**. На это время предоставляется возможность бесплатно ознакомиться с программой в полном объеме без ограничений ее функциональности. Ознакомительный период активируется автоматически только единожды при первой установке программы на рабочем месте.

Устанавливаем программу КристоАрм.

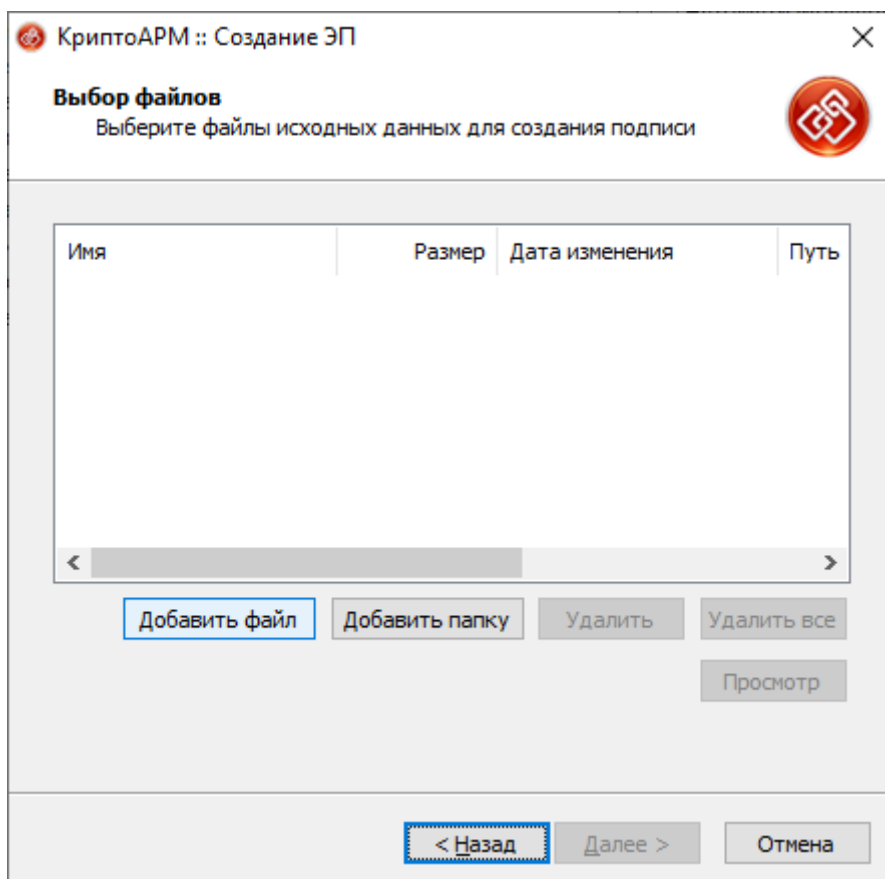
Запускаем программу КристоАрм.

Выбираем пункт меню **Подписать**, запускается Мастер создания электронной подписи.

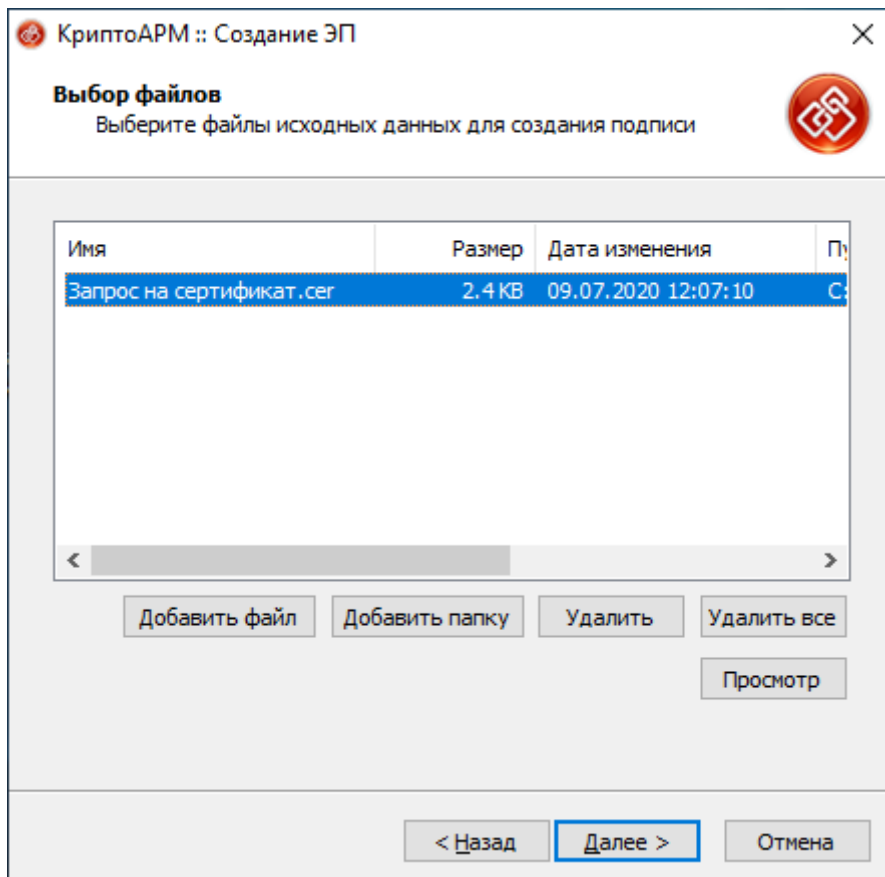


Далее

В открывшемся окне добавляем файл для подписания (файл запроса).



Далее.



Далее

Укажите папку для сохранения подписанного файла.

КриптоАРМ :: Создание ЭП

Выходной формат
Выберите желаемый выходной формат файла подписи

Кодировка и расширение

DER-кодировка *.sig

BASE64-кодировка *.sig

Отключить служебные заголовки

Архивировать файлы после создания подписи

Имя файла: C:\Users\User\Desktop\Запрос на сертификаты

Помещать выходные файлы в указанный каталог

C:\Users\User\Desktop

Сохранять структуру вложенности каталогов

Отправить выходные файлы по электронной почте

Открыть окно почтового клиента

< Назад **Далее >** Отмена

Далее

КриптоАРМ :: Создание ЭП

Параметры подписи
Установите желаемые параметры подписи

Свойства подписи

Использование подписи: [Не задано]

Комментарий к подписи:

Идентификатор ресурса: Запрос на сертификат.cer

Поместить имя исходного файла в поле "Идентификатор ресурса"

Включить в подпись: Только сертификат владельца

Сохранить подпись в отдельном файле

Удалить исходный файл после выполнения операции

Уровень безопасного удаления: Выключено

Включить время создания подписи

Включить штамп времени на подписываемые данные

Включить штамп времени на подпись

Включить в подпись доказательства подлинности

< Назад **Далее >** Отмена

Далее

Выбрать действующий сертификат пользователя УЦ для подписания запроса

КриптоАРМ :: Создание ЭП

Выбор сертификата подписи
Выберите сертификат подписи

Сертификат для создания подписи _____

Владелец сертификата: _____

Хеш алгоритм: _____

Выбрать Просмотреть

< Назад Далее > Отмена

КриптоАРМ :: Создание ЭП

Статус _____
Данные, необходимые для создания электронной подписи, собраны

Параметры _____

Сертификат подписи	Елагина Ольга Джоновна
Формат подписи	DER-кодировка (*.sig)
Входной файл 1	C:\Users\User\Desktop\За
Файл подписи 1	C:\Users\User\Desktop\За

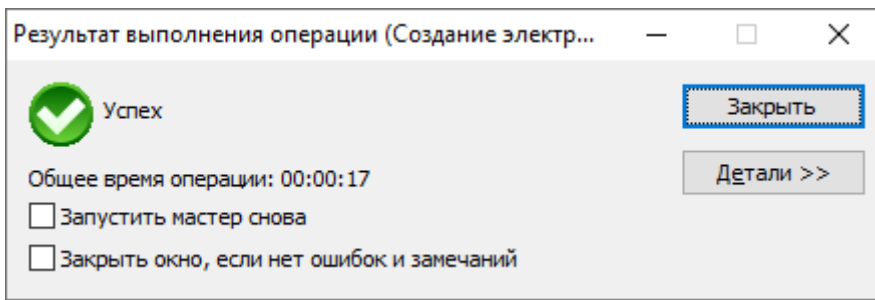
Сохранить данные в профиль для дальнейшего использования

Наименование: Новый профиль

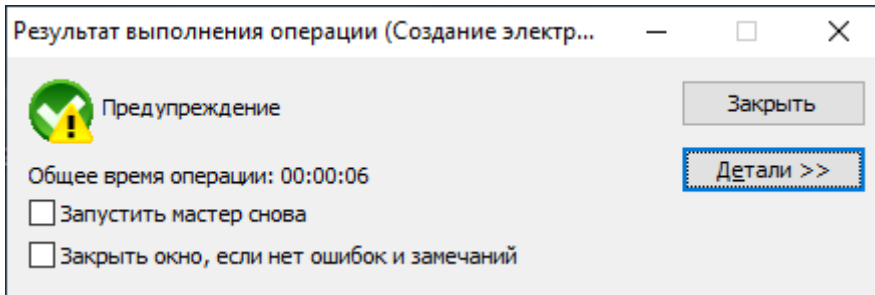
Настроить отображение шагов Мастера Вы можете в меню приложения "Управление профилями".

< Назад **Готово** Отмена

Готово.



Если результат выполнения операции Предупреждение, то необходимо обновить списки отзыва сертификатов.



Подписанный файл с расширением sig передать в Удостоверяющий центр.