Инструкция по смене квалифицированного сертификата с использованием электронной подписи

(не требуется посещение территориального органа Федерального казначейства)

Важная информация! **Для смены сертификата посредством Портала заявителя без посещения ТОФК необходимо наличие выданных в УЦ ФК действующих ключей ЭП и соответствующих им действующих сертификатов владельца ЭП УЦ ФК, а также лица, действующего от имени Заявителя (при условии, что ранее предоставленные в ТОФК сведения не изменились).**

Содержание

Перечень сокращений 3

Системные требования к АРМ пользователя 3

Подготовка к работе 5

Формирование запроса для смены сертификата 5

Скачивание готового сертификата Получателем сертификата 23

Перечень сокращений

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
ВРС	Подсистема ведения реестра сертификатов, обеспечивающая ввод, проверку, централизованное хранение сведений, представленных заявителями, информирование владельцев сертификатов и публикацию списка аннулированных сертификатов
ИНН	Идентификационный номер налогоплательщика
ОГРН	Основной государственный регистрационный номер
ПО	Программное обеспечение
Портал заявителя	Онлайн сервис подачи документов для получения сертификатов
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
СМЭВ	Система межведомственного электронного взаимодействия
СКЗИ	Средство криптографической защиты информации
СНИЛС	Страховой номер индивидуального лицевого счета
ТОФК	Территориальный орган Федерального казначейства
УЦ ФК	Удостоверяющий центр Федерального казначейства

Системные требования к АРМ пользователя

Системные требования к рабочему месту пользователя приведены в таблицах (см. Таблица 1, Таблица 2, Таблица 3).

Таблица 1. Общие системные требования к рабочему месту пользователя

Минимальные аппаратные требования	
Процессор	Тактовая частота не менее 2,3 ГГц
Оперативная память	Не менее 1 024 МБ
Пропускная способность канала	Не менее 1 024 Кбит/сек

Рекомендуемая скорость подключения к информационно-телекоммуникационной сети Интернет от 256 Кбит/сек.

Таблица 2. Дополнительные требования к рабочему месту пользователя при использовании СКЗИ КриптоПро CSP

Требования к ПО	
Операционная система (семейство Microsoft)	Microsoft Windows 7 и выше при условии совместимости используемой версии СКЗИ и веб-браузера с данной версией ОС
Интернет-браузер для ОС семейства Microsoft	Яндекс.Браузер версии 18.9.1.954 и выше, Chromium-gost версии 83.0.4103.61 и выше.
Операционная система (семейство Linux)	Альт Линукс, Astra Linux, РЕД ОС, GosLinux
Интернет-браузер для ОС семейства Linux	Chromium-gost версии 83.0.4103.61 и выше. Яндекс Браузер
Плагин (дополнение) к браузеру	КриптоПро ЭЦП Browser Plug-In версии 2.0 и выше
Средство криптографической защиты информации	СКЗИ «КриптоПро CSP 5.0» и выше

Таблица 3. Дополнительные требования к рабочему месту пользователя при использовании СКЗИ VipNet CSP

Требования к ПО	
Операционная система (семейство Microsoft)	Microsoft Windows 7 и выше при условии совместимости используемой версии СКЗИ и веб-браузера с данной версией ОС
Интернет-браузер для ОС семейства Microsoft	Яндекс.Браузер версии 18.9.1.954 и выше, Chromium-gost версии 83.0.4103.61 и выше
Операционная система (семейство Linux)	Альт Линукс, Astra Linux, РЕД ОС, GosLinux
Интернет-браузер для ОС семейства Linux	Chromium-gost версии 83.0.4103.61 и выше, Яндекс Браузер
Средство криптографической защиты информации	ViPNet PKI Client версии 1.6 и выше

Подготовка к работе

- Обеспечить на АРМ наличие поддерживаемой ОС, согласно разделу «Системные требования к АРМ пользователя»
- Обеспечить на АРМ наличие одного из поддерживаемых Web-браузеров, согласно разделу «Системные требования к АРМ пользователя»
- Установить сертифицированную версию СКЗИ КриптоПро CSP 5.0 и выше либо ViPNet PKI Client (Инструкция по установке ViPNet PKI Client)
- Установить «КриптоПро ЭЦП Browser Plugin» версии 2.0 и выше (инструкция по настройке для Яндекс.Браузера).

Примечание: в случае использования ViPNet PKI Client не требуется

- Установить сертификаты Минцифры России (ГУЦ) и УЦ ФК согласно инструкции
- Проверить настройку АРМ (проверить).

ВНИМАНИЕ! В случае использования ViPNet PKI Client необходимо осуществить настройку АРМ согласно инструкции.

Формирование запроса для смены сертификата

Для формирования запроса для смены сертификата необходимо выполнить следующие действия:

1. Подключить к компьютеру ключевой носитель (Рутокен, eToken и др.).
2. Перейти на главную страницу открытой части Портала заявителя, расположенную по адресу https://fzs.roskazna.ru/ либо осуществить вход в личный кабинет авторизованного пользователя с помощью действующего сертификата УЦ ФК, расположенного по адресу https://lk-fzs.roskazna.ru/ (Рисунок 1).

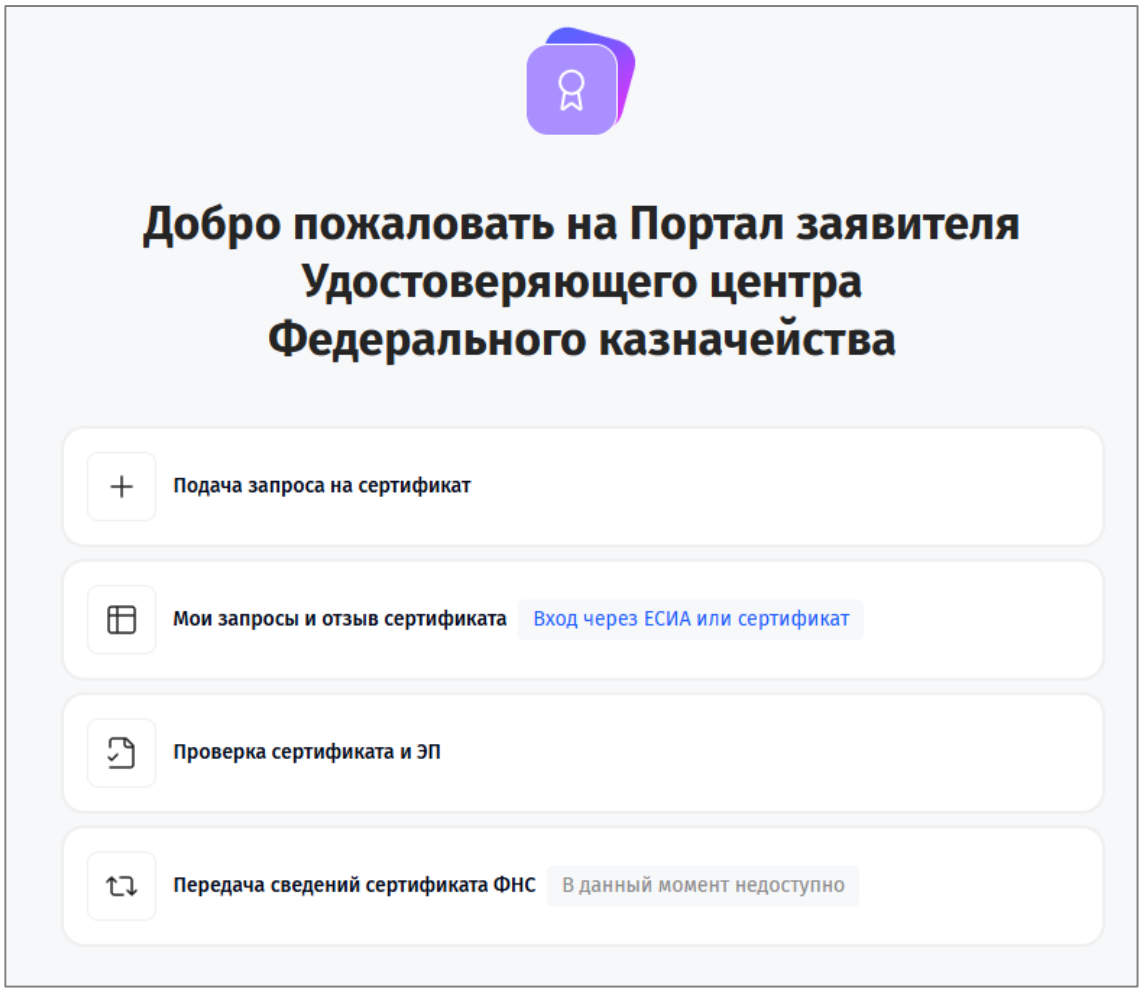


Рисунок 1. Главная страница открытой части Портала заявителя

3. Перейти по пункту меню «Подача запроса на сертификат» (Рисунок 2).

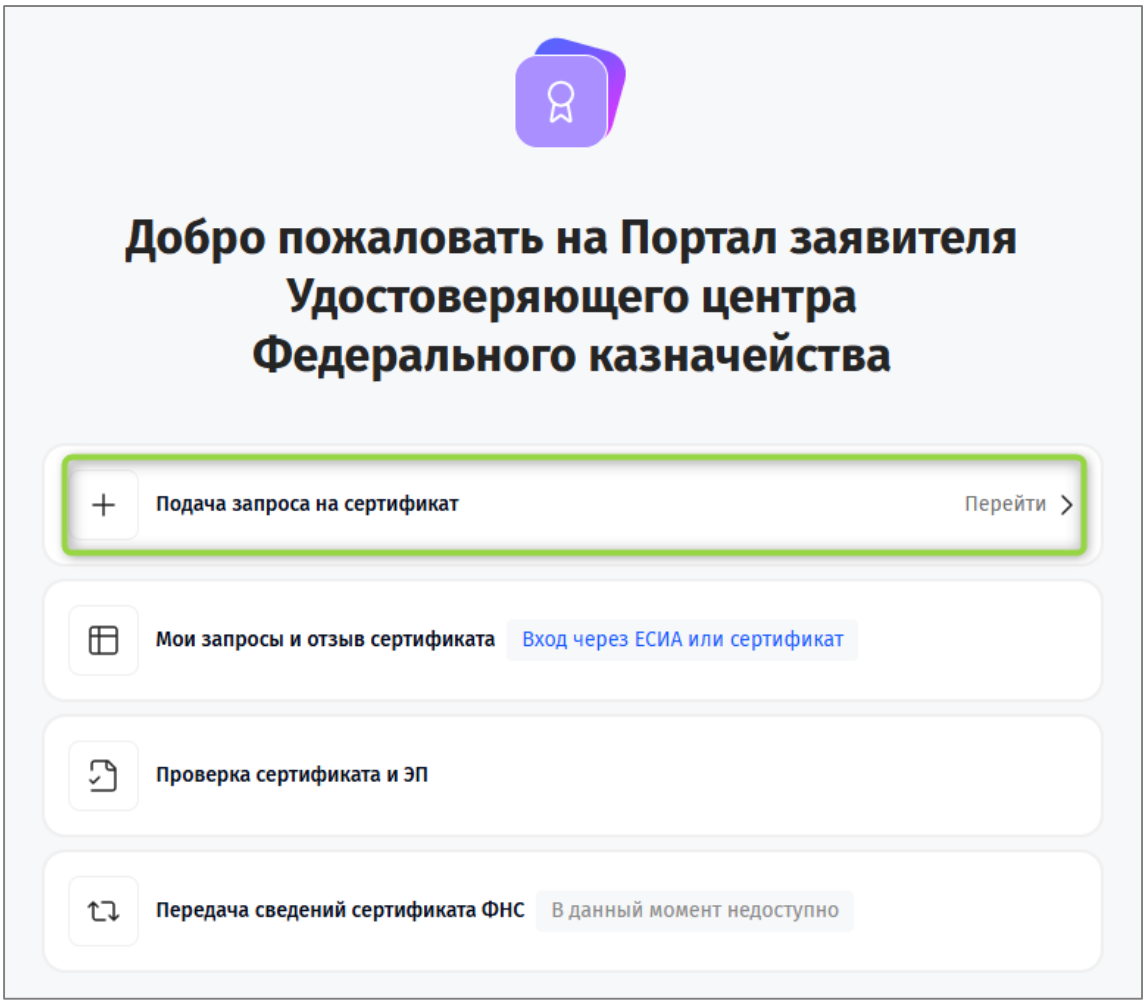


Рисунок 2. Переход к подаче запроса на сертификат

Отображается форма подачи запроса на создание сертификата на шаге 1 (Рисунок 3).

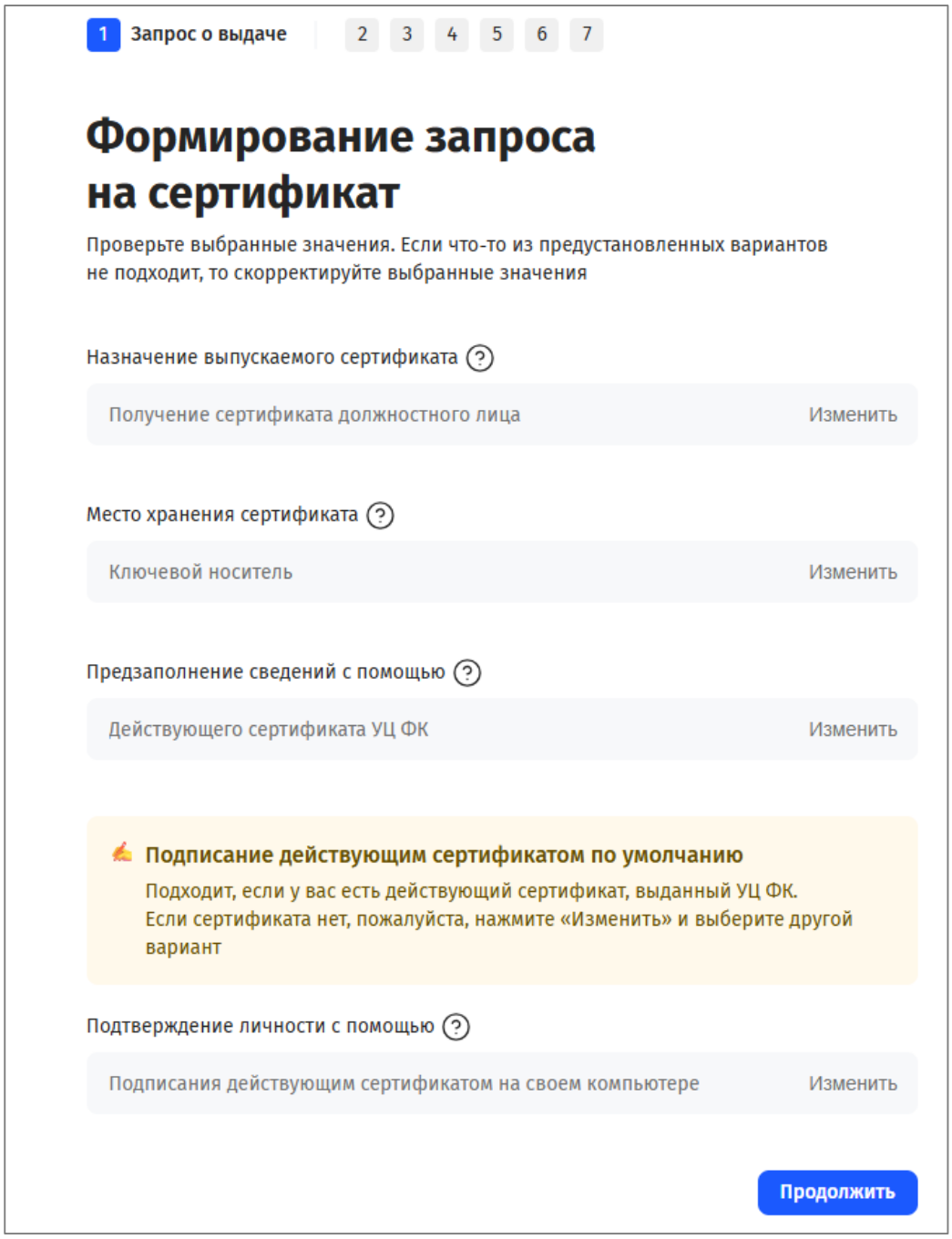


Рисунок 3. Форма подачи запроса. Шаг 1

На форме доступны для изменения следующие элементы:

- **Назначение выпускаемого сертификата**. По умолчанию установлено значение «Получение сертификата должностного лица». Выбрать иное значение можно, используя кнопку «Изменить».
- **Место хранения сертификата**. По умолчанию установлено значение «Ключевой носитель». При необходимости выбора подачи запроса в приложение «Госключ» использовать кнопку «Изменить».

Примечание! *В случае выбора места хранения сертификата значения «Приложение «Госключ» обязательна авторизация на портале с помощью Госуслуг и наличие установленного приложения «Госключ» на мобильном телефоне.*

- **Предзаполнение сведений с помощью**. По умолчанию установлено значение «Действующего сертификата УЦ ФК», который предполагает плановую смену и дальнейшую авторизацию по сертификату.
- **Подтверждение личности с помощью**. По умолчанию установлено значение «Подписание действующим сертификатом на своем компьютере», который предполагает установленный на АРМ действующий сертификат УЦ ФК.

4. Нажать «Продолжить». *В случае, если подача осуществляется с открытой части Портала заявителя потребуется выбрать сертификат, с помощью которого осуществить авторизацию на портале , и авторизоваться.*

Отображается шаг 2 подачи запроса на получение сертификата (Рисунок 4). На форме данные предзаполнены:

- Данные организации, от которой будет осуществляться подача предзаполнены на основании сертификата, которым была осуществлена авторизация, и недоступны для редактирования;
- Данные субъекта РФ и адреса ТОФК для подачи. Данные доступны для редактирования. При необходимости их можно скорректировать с помощью нажатия ссылки «Изменить».

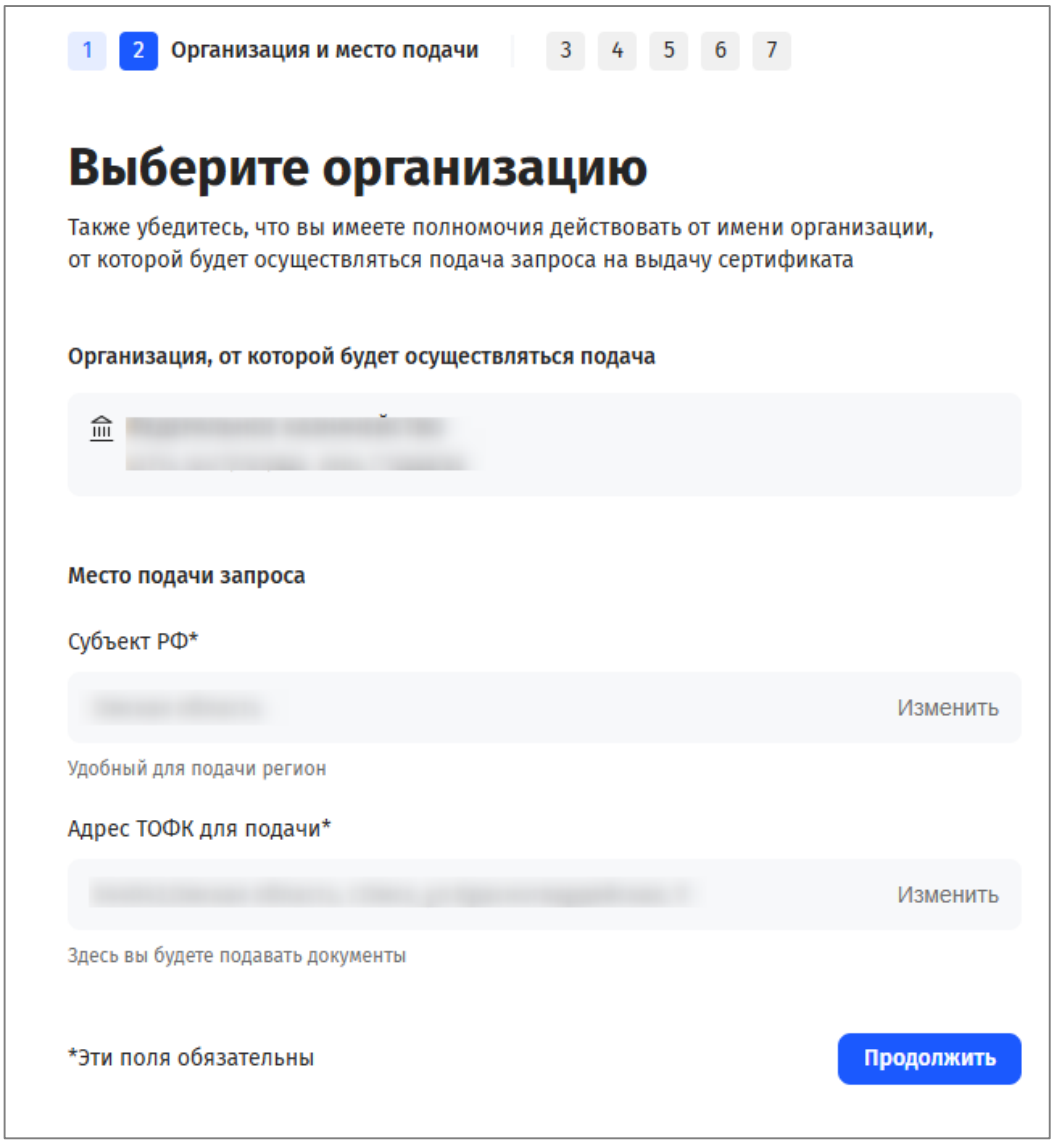


Рисунок 4. Выбор организации и места подачи

5. При необходимости внести изменения и нажать «Продолжить».
6. Проверить указанные на шаге 3 данные и нажать «Продолжить» (Рисунок 5). В случае необходимости внесения изменения на предыдущих шагах можно вернуться к ним.

Примечание! *После подтверждения сведений на шаге 3 внести изменения на 1 и 2 шагах невозможно*

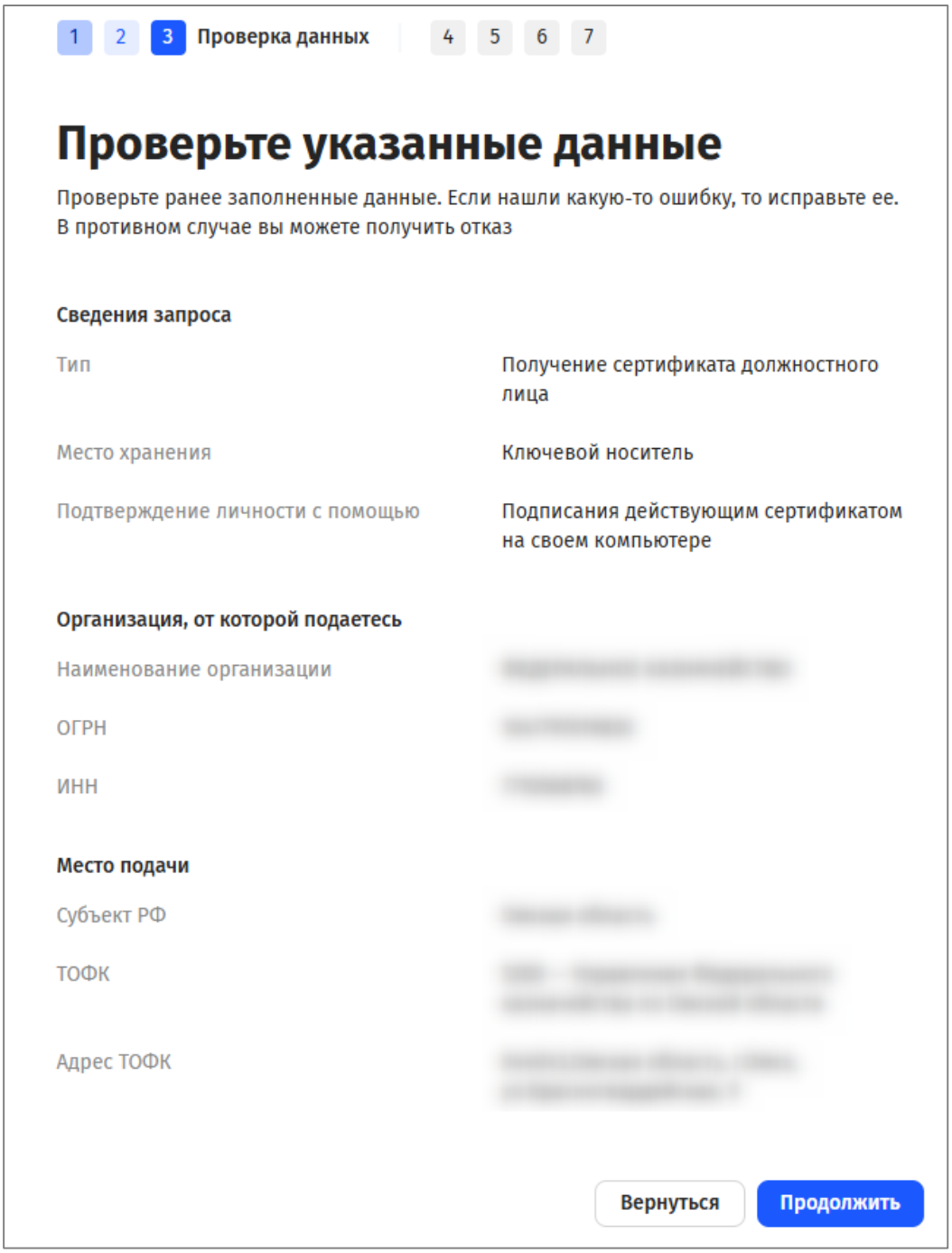


Рисунок 5. Шаг 3. Подтверждение указанных данных

7. Осуществляется переход к шагу 4. Данные на форме предзаполнены и часть недоступна для редактирования (Рисунок 6). В случае необходимости внести изменения в данные и нажать «Продолжить».

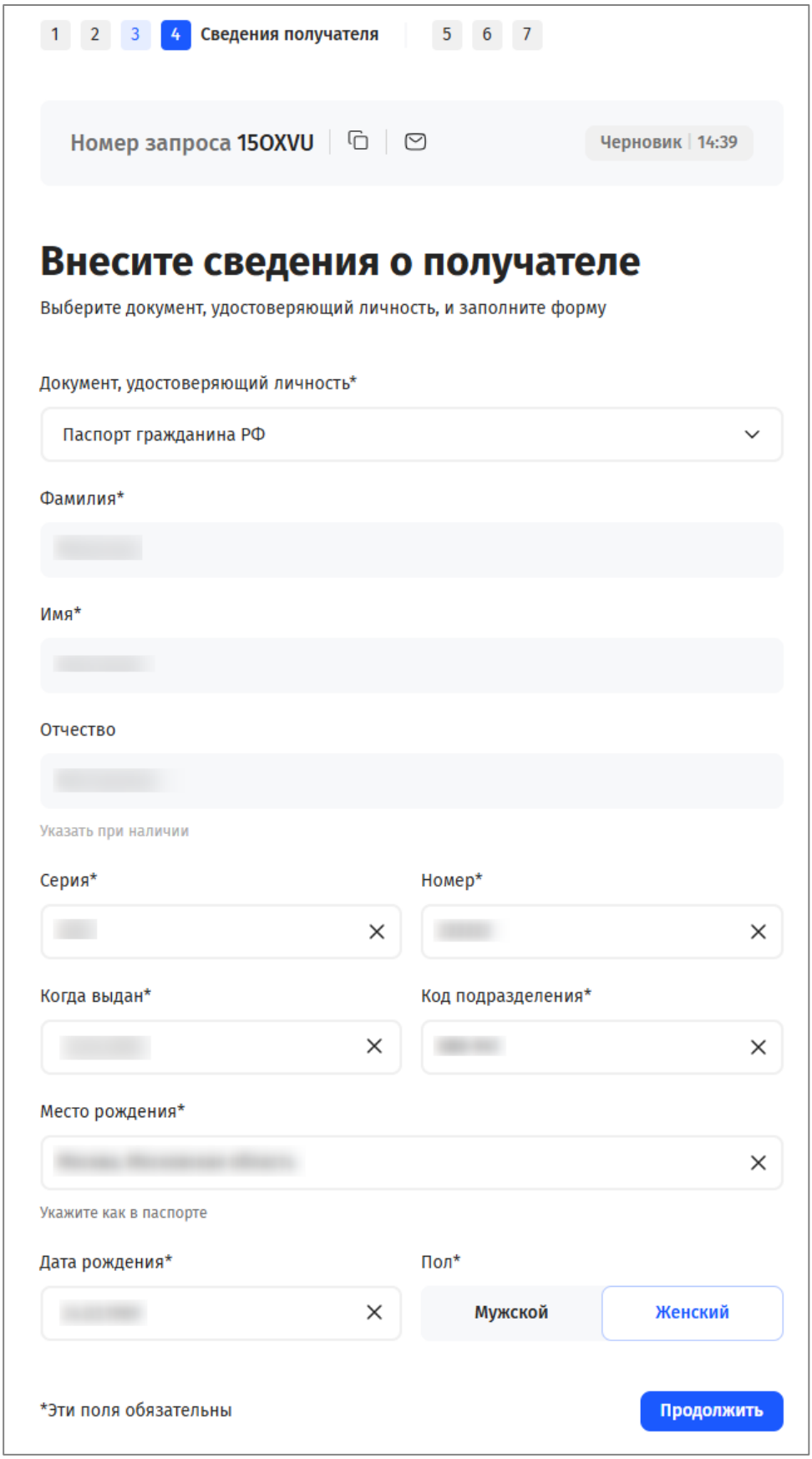


Рисунок 6. Шаг 4. Форма внесения данных документа, удостоверяющего личность

8. В зависимости от выбранного на шаге 1 назначения сертификата на следующем шаге отображается:

- Форма ввода данных для формирования файла запроса (Рисунок 7). Часть данных на форме предзаполнена. Также часть данных на форме недоступна для изменения;
- Форма выбора формирования файла запроса на портале заявителя либо загрузка файла запроса (Рисунок 8);
- Форма загрузки файла запроса (Рисунок 9).

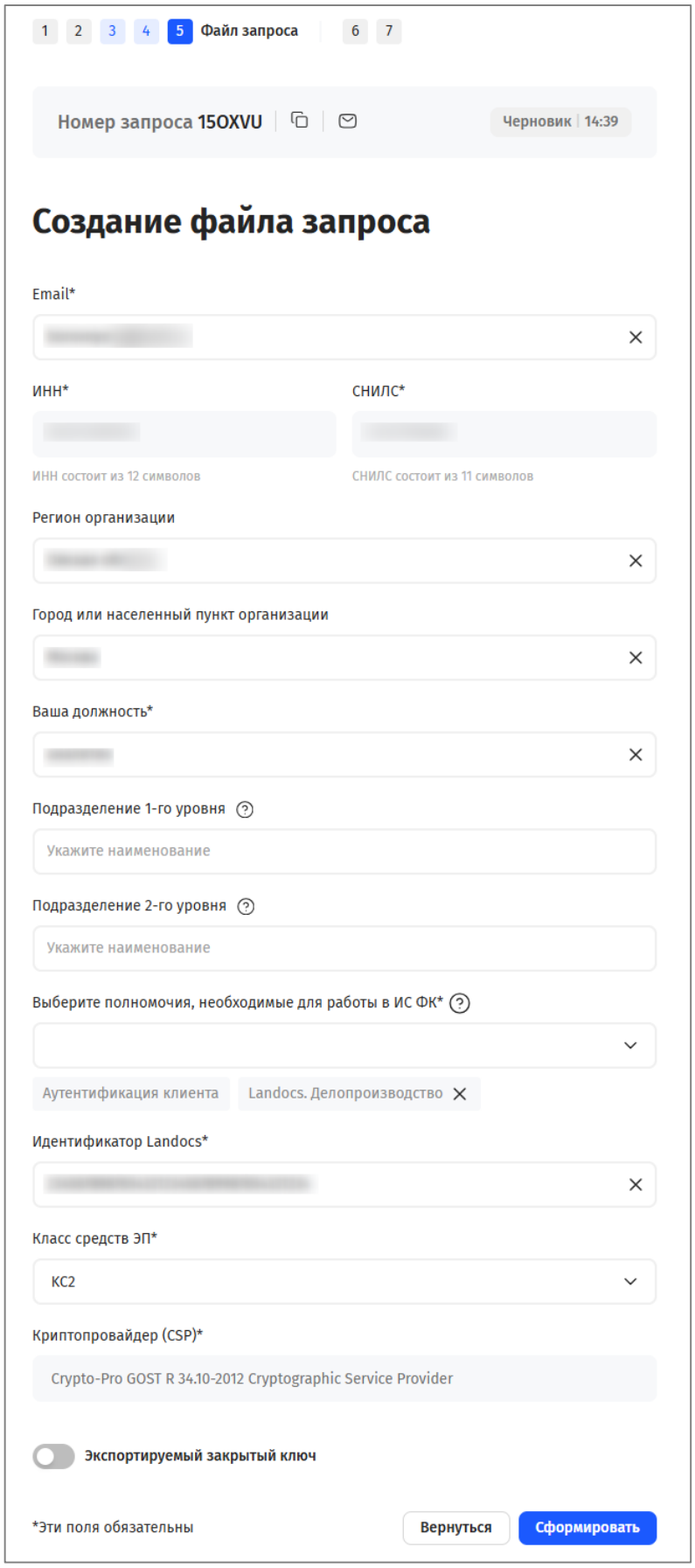


Рисунок 7. Шаг 5. Формирование файла запроса

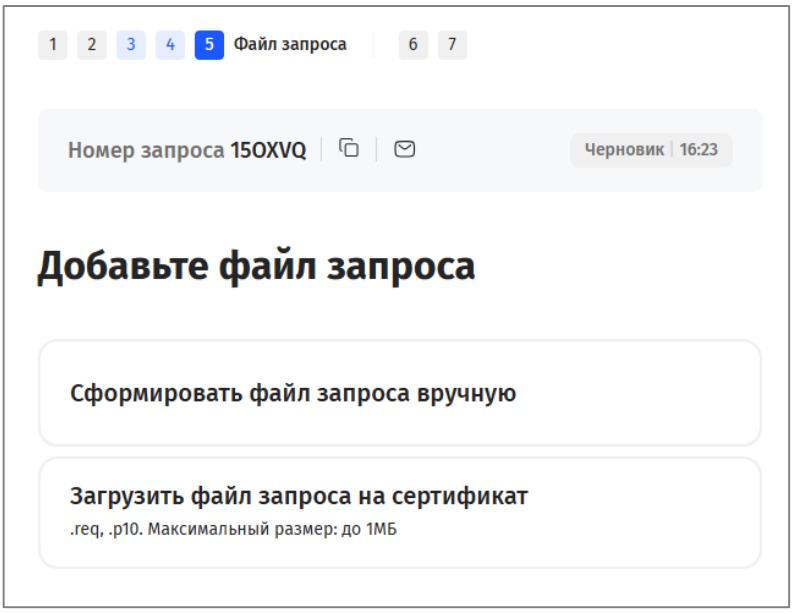


Рисунок 8. Шаг 5. Выбор формата добавления файла запроса

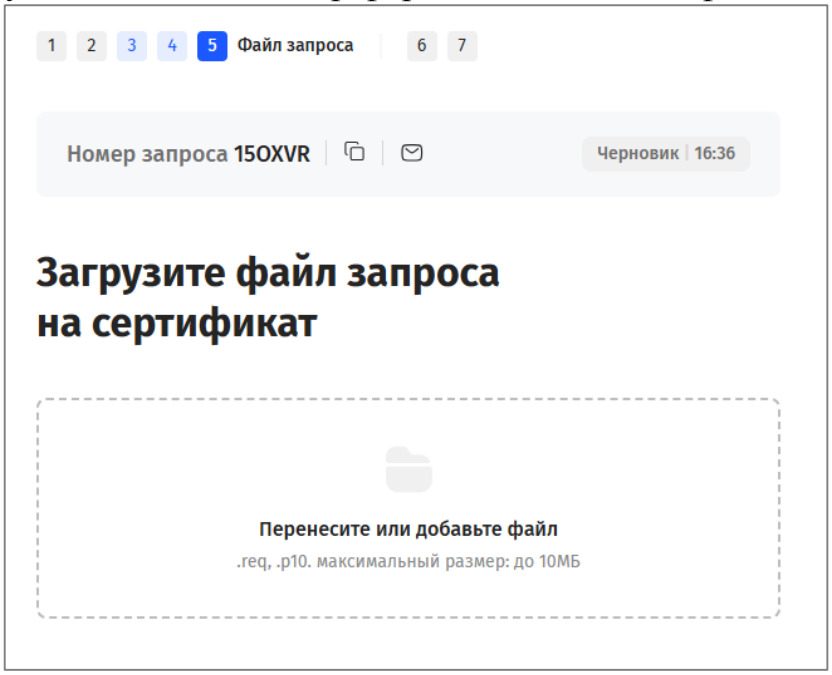


Рисунок 9. Шаг 5. Форма загрузки файла запроса

8. В случае формирования файла запроса на Портале заявителя вставить носитель ключа электронной подписи в системный блок АРМ.

9. Заполнить на форме необходимые данные. Обязательные для заполнения поля отмечены *.

10. После внесения сведений нажать на кнопку «Сформировать».

11. На форме создания запроса на сертификат со сформированными данными нажать «Сформировать» и сформировать запрос (Рисунок 10).

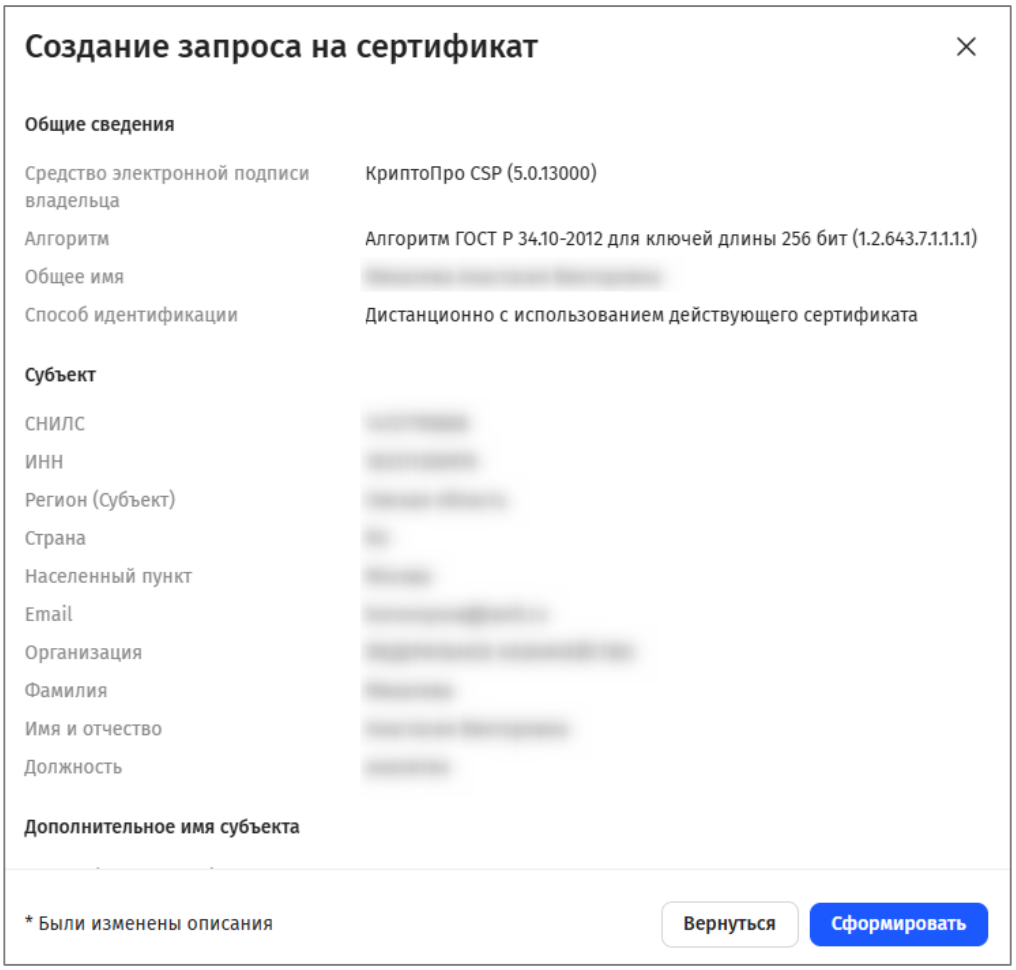


Рисунок 10. Форма создания запроса на сертификат со сформированными полями запроса

Важно! Формирование запроса осуществляется с помощью СКЗИ «КриптоПро CSP 5.0» и ПО «КриптоПро ЭЦП Browser Plug-In» версии 2.0. Для формирования запроса необходимо подключить отформатированный ключевой носитель (Рутокен, флеш-накопитель и т.п.) к системному блоку АРМ. После выбора носителя необходимо ввести пароль и подтвердить его.

Внимание! Введенный пароль необходимо запомнить, в случае утери, его восстановление невозможно. После генерации запроса на сертификат владелец должен обеспечивать хранение носителя ключевой информации с ключом электронной подписи в соответствии с установленными требованиями (приказ ФАПСИ от 13.06.2001 № 152).

12. Осуществляется переход к шагу 6 для прикрепления документов (Рисунок 11). Если ранее при выпуске сертификата документ, подтверждающий полномочия, был прикреплен, то он и его данные автоматически заполняются. При необходимости его можно отредактировать, используя кнопку «Изменить».

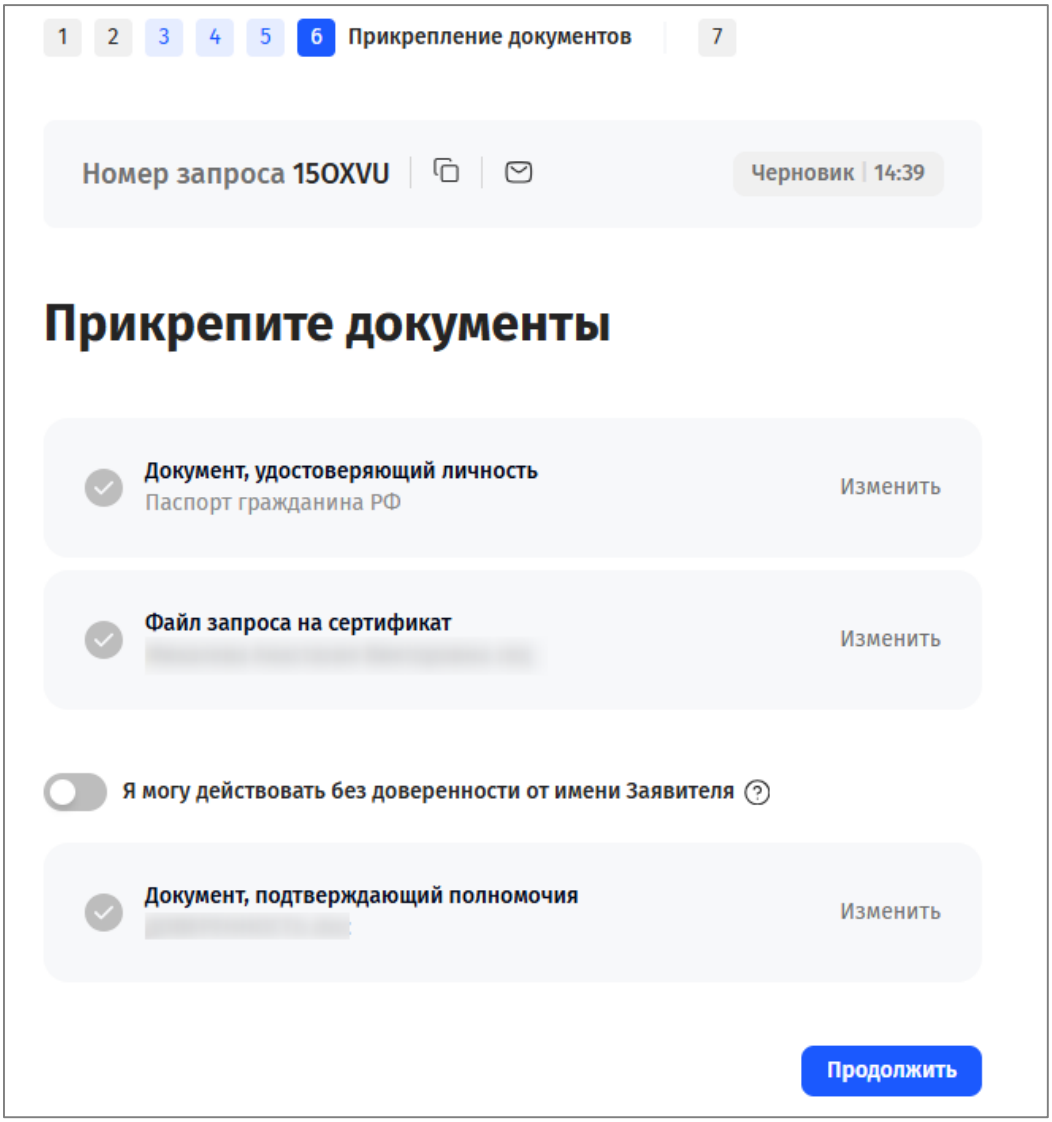


Рисунок 11. Шаг 6. Прикрепление документов

1. Добавить документ, подтверждающий полномочия при необходимости:
   a. В случае, если Получатель сертификата является лицом, имеющим право действовать без доверенности от имени Заявителя, необходимо установить признак «Я могу действовать без доверенности от имени Заявителя»;
   b. Если владелец сертификата не является лицом, имеющим право действовать без доверенности от имени Получателя сертификата, необходимо заполнить данные в разделе «Документ, подтверждающий полномочия»

i. прикрепить сканированный документ, используя кнопку «Добавить» (Рисунок 12, Рисунок 13)
ii. указать название, дату и номер документа и сохранить сведения (Рисунок 14).

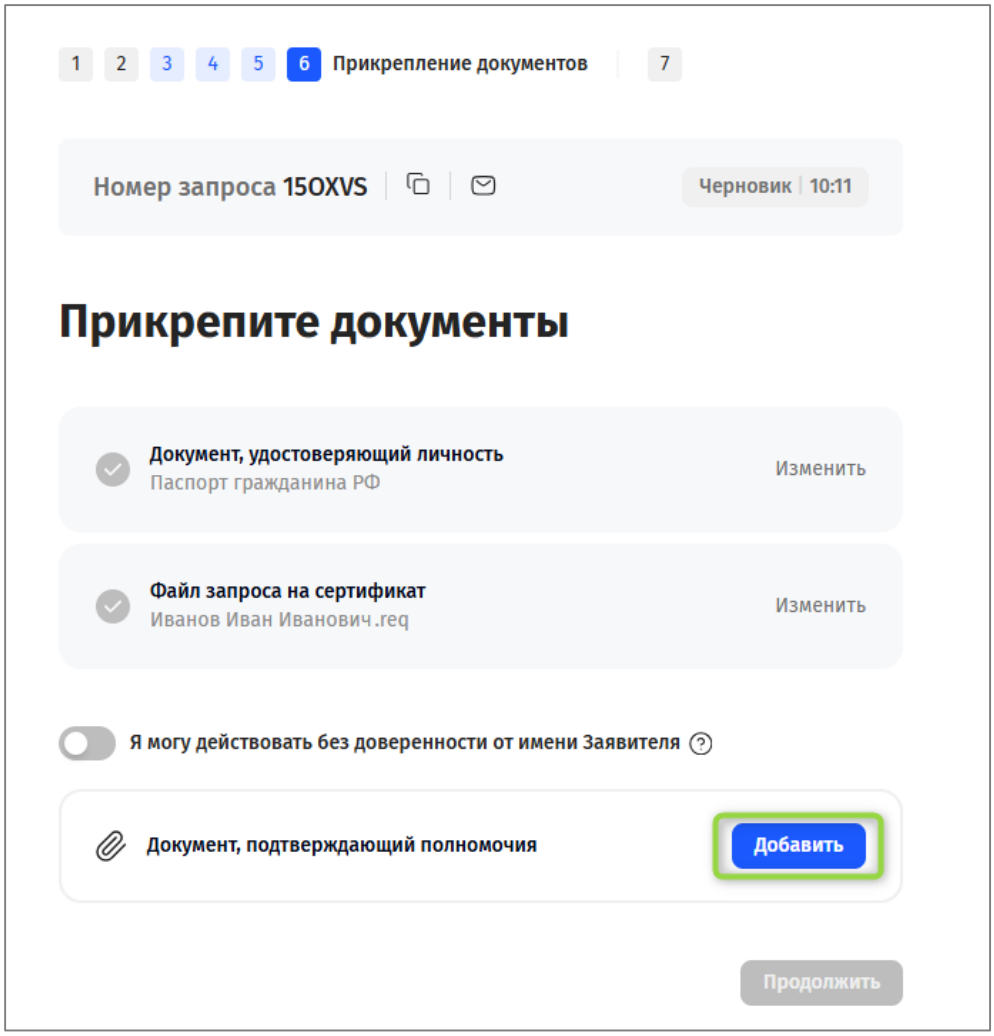


Рисунок 12. Шаг 6. Кнопка добавления документа

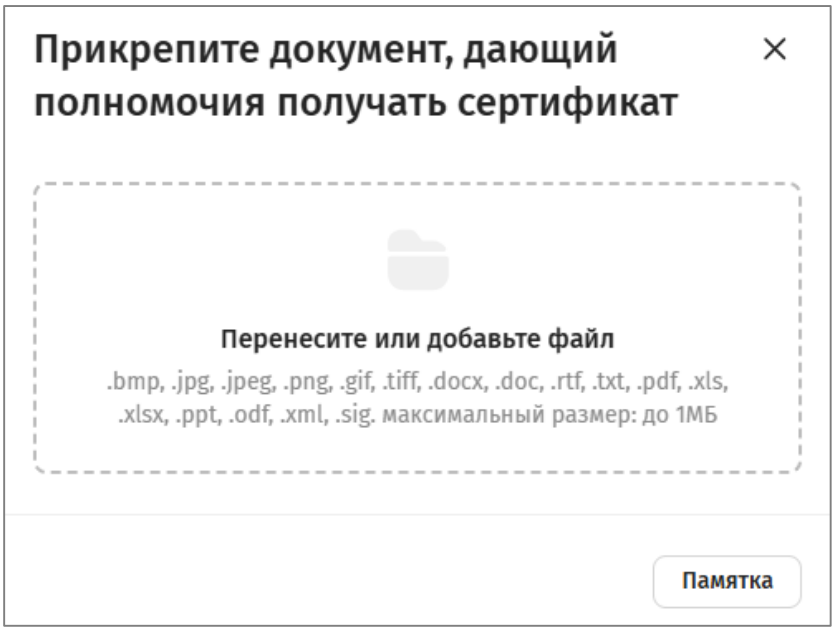


Рисунок 13. Форма прикрепления документа

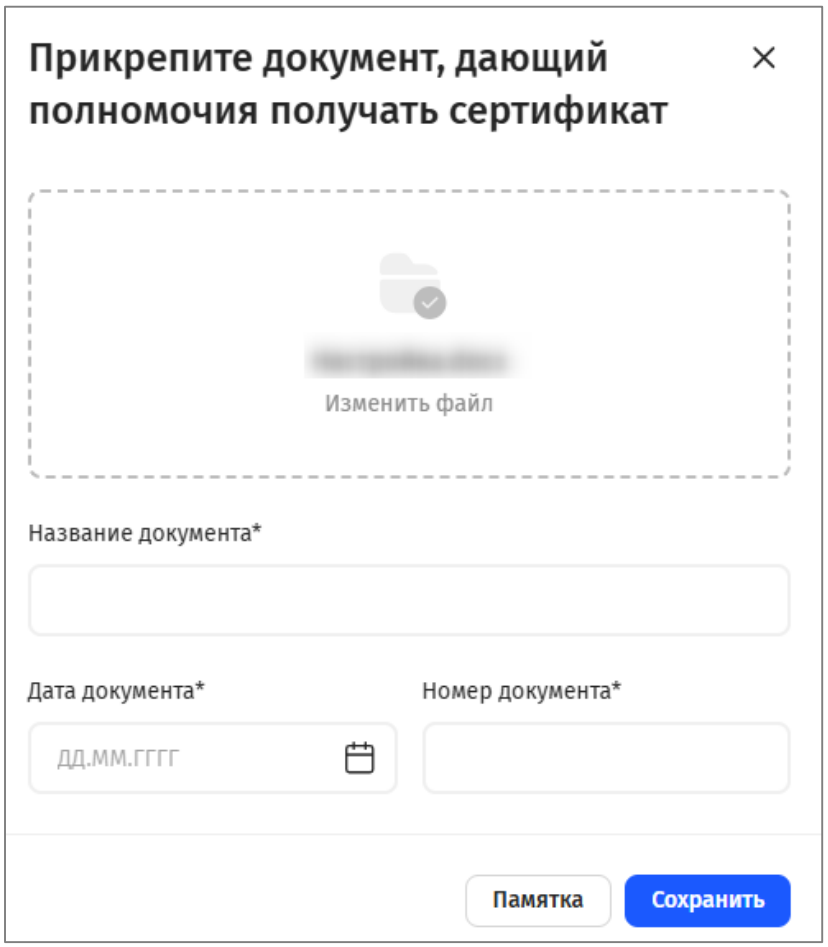


Рисунок 14. Форма указания данных документа

14. Перейти к следующему шагу, используя кнопку «Продолжить».

15. Отображается шаг 7 с полями для ввода контактных данных. Указать номер телефона и при необходимости изменить адрес электронной почты для уведомлений (Рисунок 15).

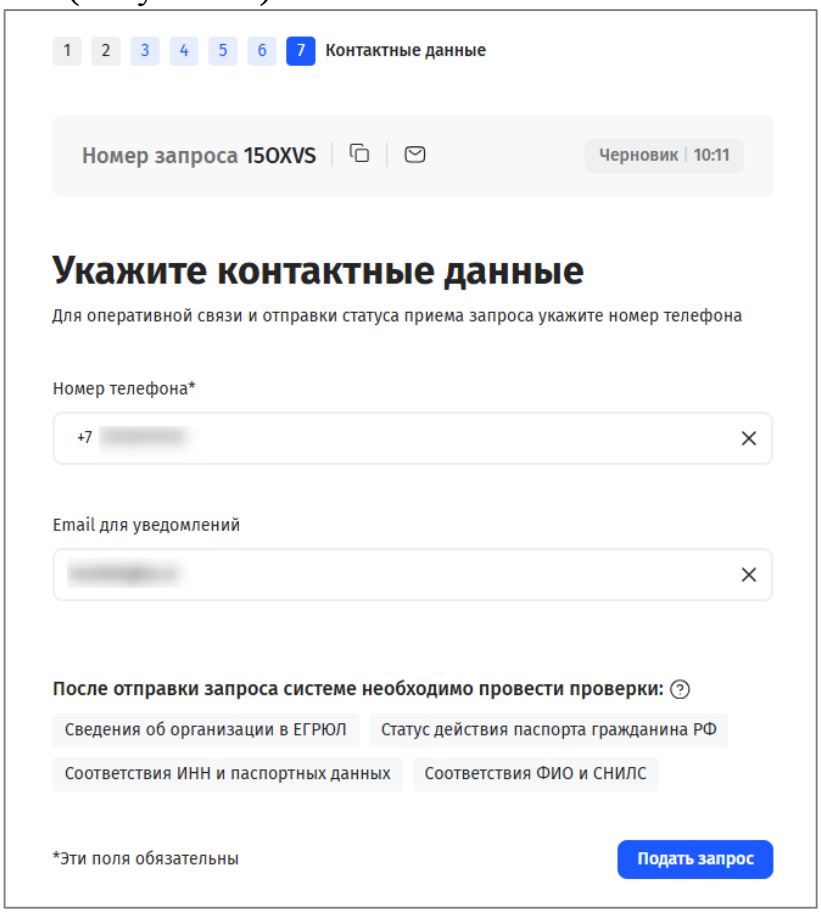


Рисунок 15. Шаг 7. Контактные данные

16. Нажать на кнопку «Подать запрос».

14. На отобразившейся форме нажать «Подписать» и подписать сведения (Рисунок 16).

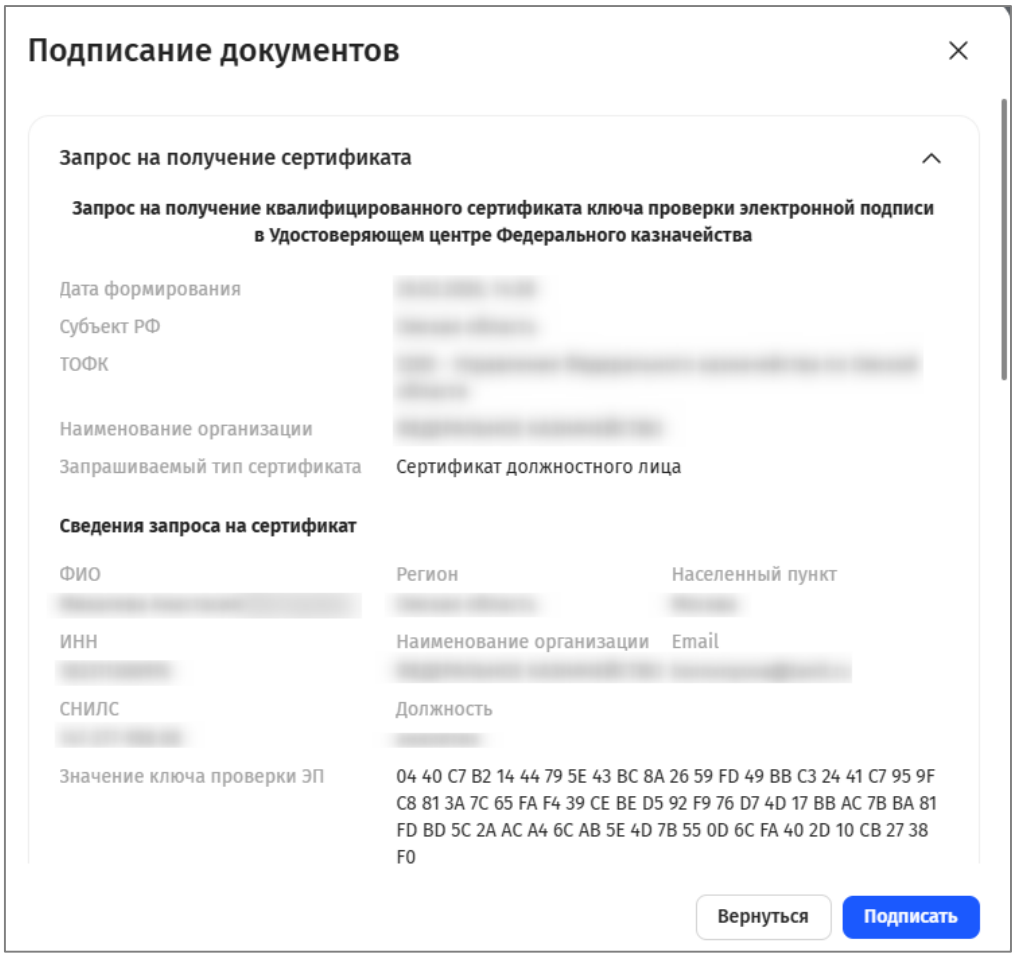


Рисунок 16. Форма «Подписание документов»

15. В результате отобразится окно подтверждения о подписании сведений ЭП (Рисунок 17).

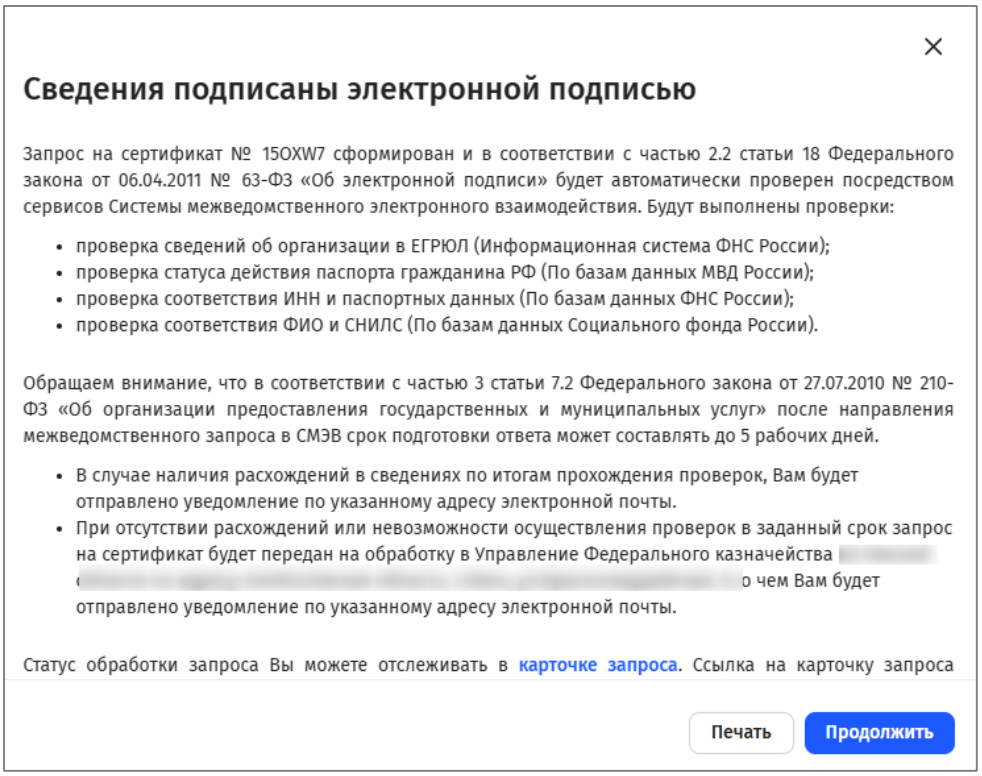


Рисунок 17. Окно подтверждения о подписания сведений ЭП

16. Нажать на кнопку «Продолжить» для закрытия информационного окна.

Сведения запроса на создание сертификата передаются на проверку посредством СМЭВ.

Внимание! *После направления запроса в СМЭВ срок подготовки ответа может составлять до 5 рабочих дней.*

В случае успешных проверок запроса в СМЭВ, запрос передается на обработку в УЦ ФК

17. Оператор УЦ ФК осуществит проверку комплекта электронных документов на создание сертификата.

24. Оператор УЦ ФК согласует запрос на сертификат и изготовит сертификат. Получателю сертификата придет соответствующее уведомление на адрес электронной почты и появится возможность получить сертификат в личном кабинете Портала заявителя.

25. Если Оператор УЦФК отклонит запрос, запрос перейдет в статус «Отклонен», о чем Получателю сертификата придет соответствующее уведомление на адрес электронной почты.

Скачивание готового сертификата Получателем сертификата

Для скачивания готового сертификата Получателем сертификата необходимо выполнить следующие действия:

1. Авторизоваться на Портале заявителя (Рисунок 18).

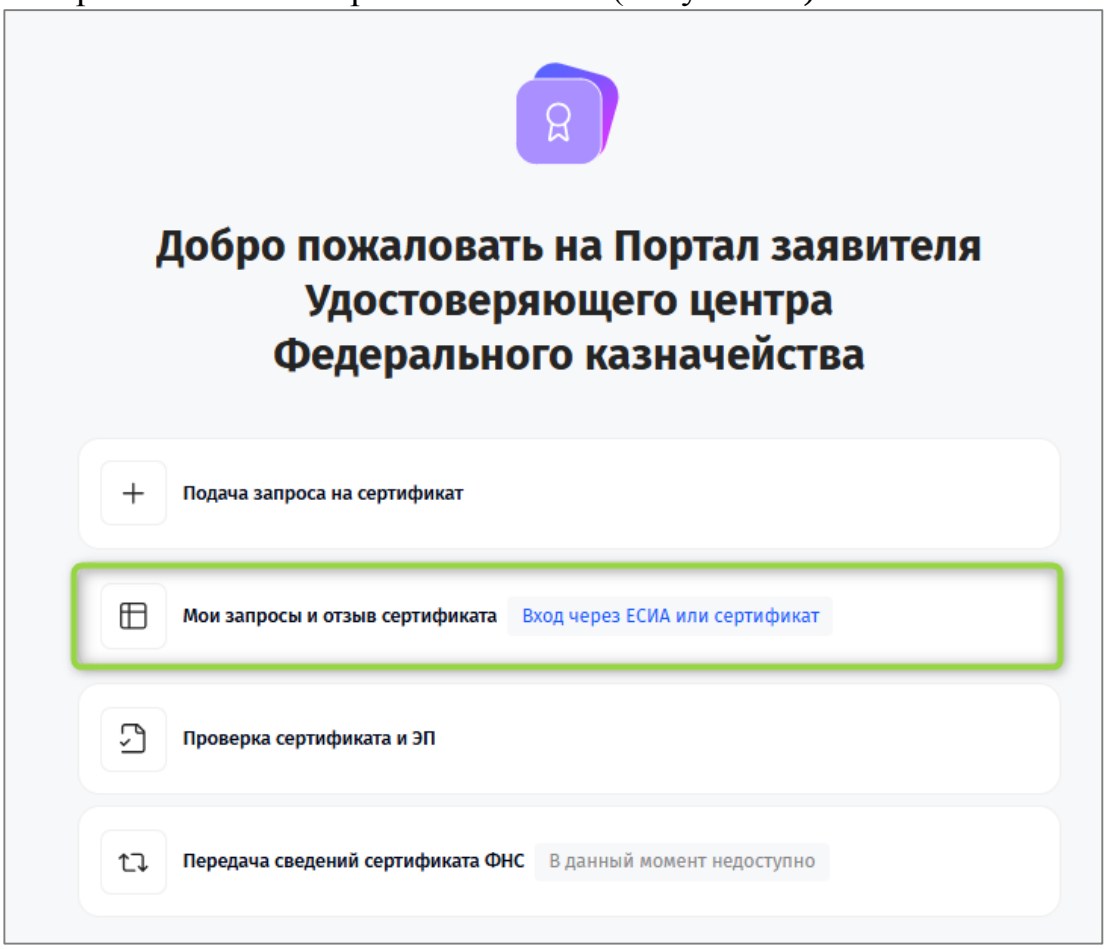


Рисунок 18. Вход в личный кабинет авторизованного пользователя Портала Заявителя

2. Перейти к вкладке «Запросы» (Рисунок 19).

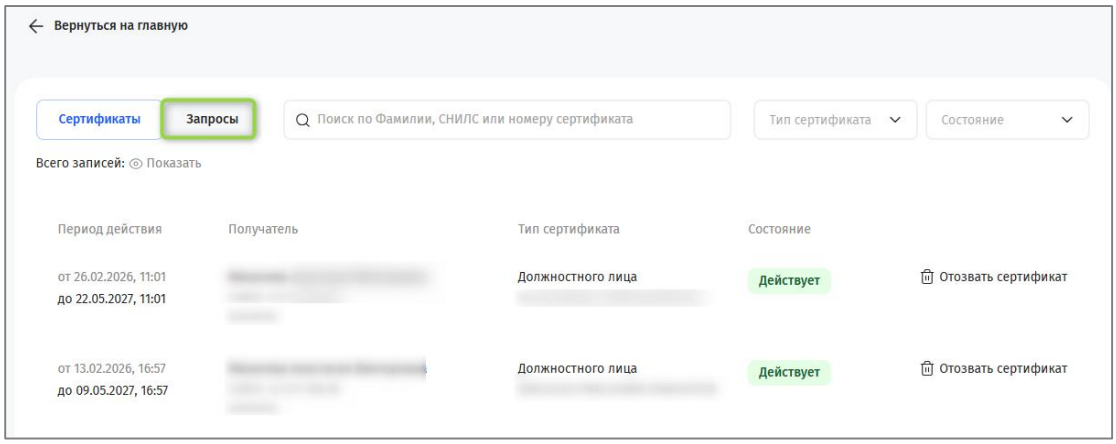


Рисунок 19. Меню перехода между реестрами сертификатов и запросов Получателя сертификата

3. Открыть карточку запроса, по которому изготовлен сертификат, и структура сертификата которого еще не подтверждена.

4. В отобразившейся карточке запроса на создание сертификата нажать на кнопку «Скачать» (Рисунок 20)

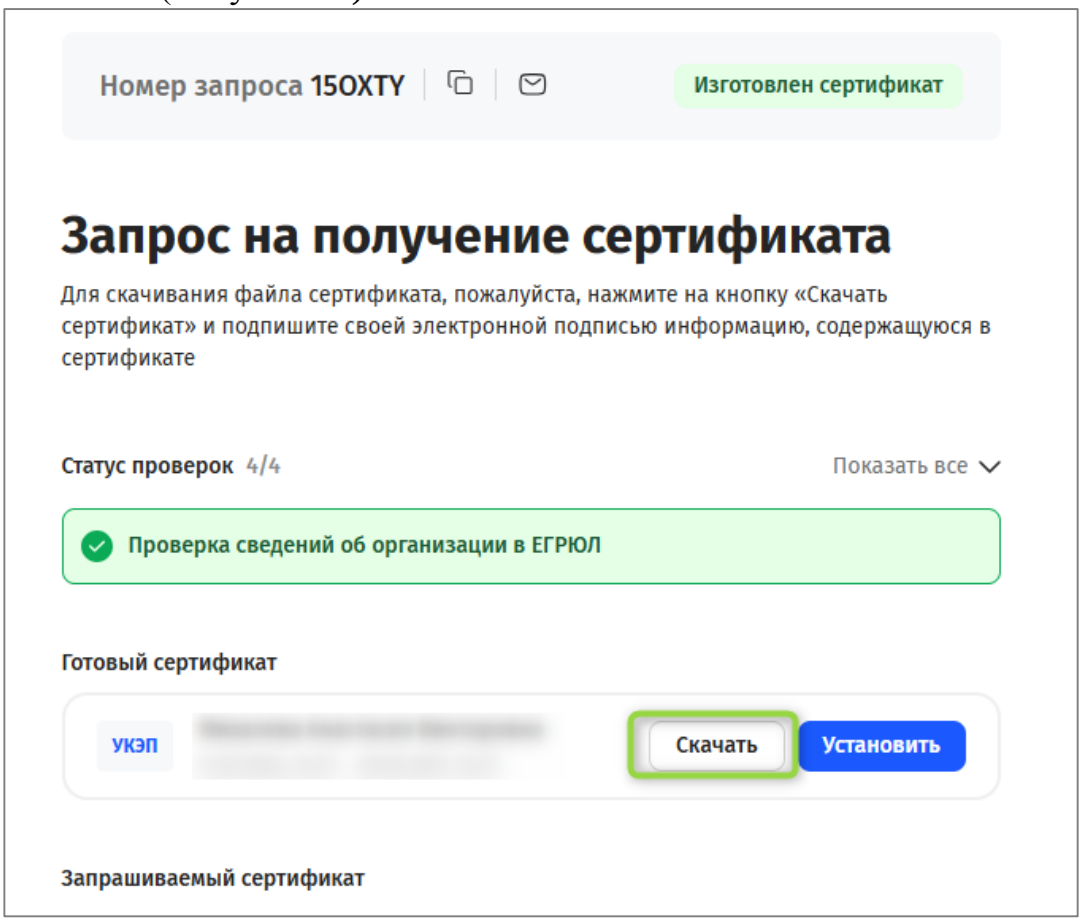


Рисунок 20. Карточка запроса на создание сертификата. Кнопка «Скачать»

5. В отобразившейся форме «Расписка в ознакомлении с информацией, содержащейся в квалифицированном сертификате» установить переключатели (Рисунок 21):

- Ознакомлен с Руководством по обеспечению безопасности использования КЭП и средств КЭП;
- Ознакомлен с сублицензионным договором - офертой на предоставление неисключительных прав на использование программы для ЭВМ;
- Ознакомлен с информацией, содержащейся в квалифицированном сертификате

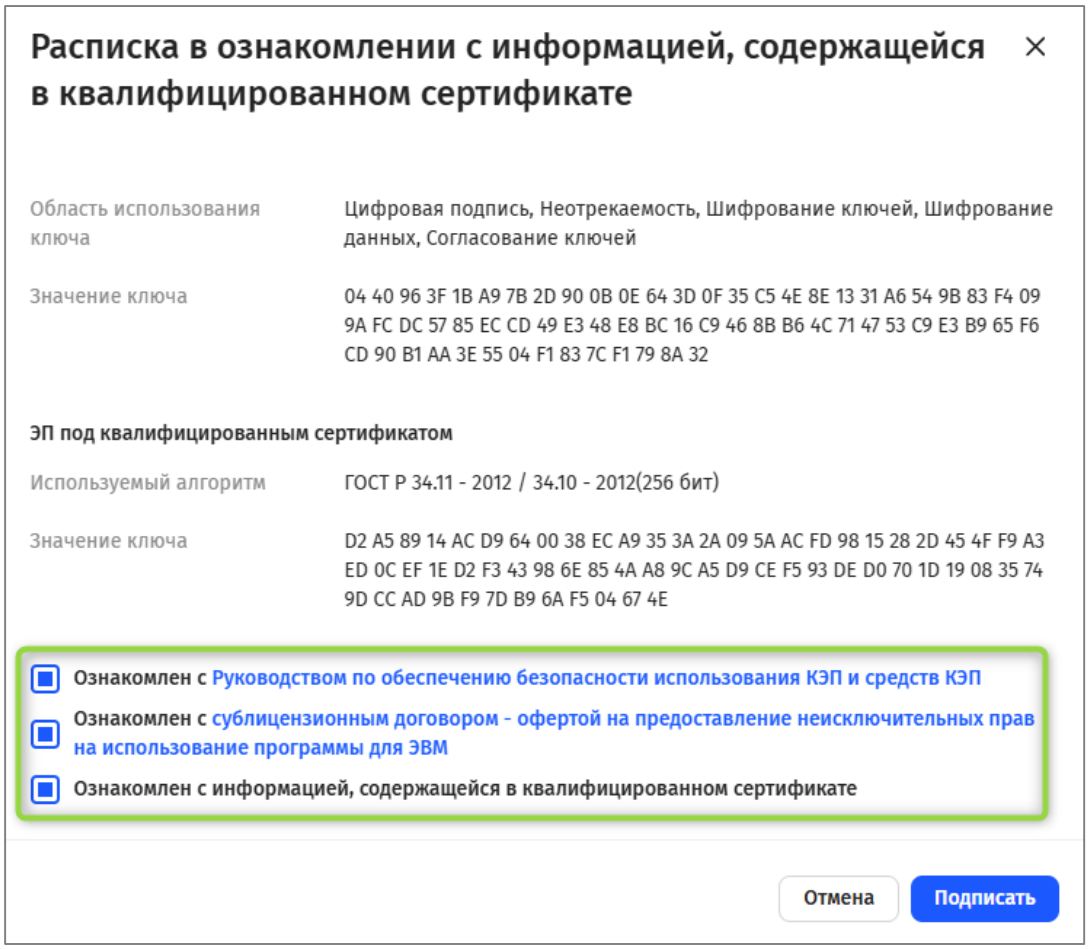


Рисунок 21. Ознакомление с информацией, содержащейся в сертификате

18. Подписать сведения электронной подписью, нажав на кнопку «Подписать».

После подписания автоматически запустится процесс сохранения файла сертификата на АРМ.