Межрегиональное операционное УФК

Инструкция по смене квалифицированного сертификата с использованием электронной подписи

(посещение ТОФК не требуется)

Важная информация! Для смены сертификата посредством Портала заявителя без посещения ТОФК необходимо наличие действующего сертификата, выданного УЦ ФК и соответствующего ему действующего ключа электронной подписи.

Содержание

Перечень сокращений 3

Системные требования к к рабочему месту пользователя 4

Подготовка к работе 5

Формирование запроса для смены сертификата 6

Скачивание готового сертификата Получателем сертификата 20

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 рабочему месту 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

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	«КриптоПро CSP» 5.0 и выше, имеющее действующий сертификат соответствия ФСБ России (Возможно получение дистрибутива в Межрегиональном операционном УФК. Примерная форма запроса расположена на сайте в разделе ГИС – АОКЗ)

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, имеющее действующий сертификат соответствия ФСБ России

Подготовка к работе

- Обеспечить на АРМ наличие поддерживаемой ОС, согласно разделу «Системные требования к »;

- Обеспечить на АРМ наличие одного из поддерживаемых Web-браузеров, согласно разделу «Системные требования к »;

- 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

Пакет документов для получения сертификата

При обращении в Региональный центр регистрации Межрегионального операционного управления Федерального казначейства с помощью Портала заявителя ИС УЦ ФК предоставляется:

– Заявление на выдачу сертификата, подписанное действующей подписью владельца сертификата;

– Один из следующих документов:

Для получения сертификата должностного лица - документ, которым подтверждается замещение должностным лицом государственной должности, должности в государственном органе, учреждении, подведомственном государственному органу, организации, определенной в пункте 4 части 3 статьи 17.2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». *Один из следующих документов:*

- **Заверенная**[1] копия приказа о назначении на должность;
- Выписка из приказа о назначении на должность;
- Справка о замещении должности, выданная кадровым подразделением.

Примечание: при смене должности, либо фамилии, достаточно предоставить скан-копию нового документа (приложить к запросу, см. п. 12 данной инструкции).

Для получения сертификата юридического лица без ФИО:

- Распорядительный акт юридического лица, которым определяется физическое лицо, ответственное за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе, и лицо, ответственное за содержание информации, подписываемой данной электронной подписью (в соответствии с частью 3 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»).

Примечание: в случае отсутствия указанного распорядительного акта лицом, ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе, является руководитель юридического лица. Сертификат в данном случае выдается руководителю организации.

Сертификаты юридического лица с указанием ФИО в соответствии с частью 3 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» выдаются только лицам, действующим от имени юридического лица *без доверенности* в соответствии с гражданским законодательством Российской Федерации. Данные лица указаны в Едином государственном реестре юридических лиц (ЕГРЮЛ).

---

[1] В порядке, установленном в Вашей организации, либо нотариально. Требования к заверению копий документов указаны в пункте 5.26 ГОСТ Р 7.0.97-2025.

Для формирования запроса для смены сертификата необходимо выполнить следующие действия:

1. Подключить к компьютеру ключевой носитель с действующим ключом электронной подписи (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).

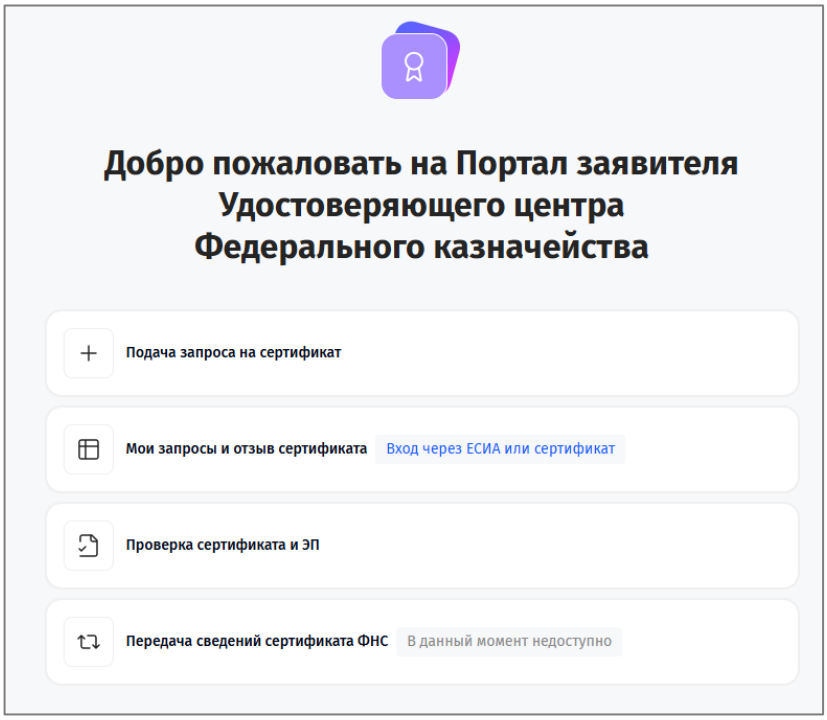


Рисунок 1. Главная страница открытой части Портала заявителя

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

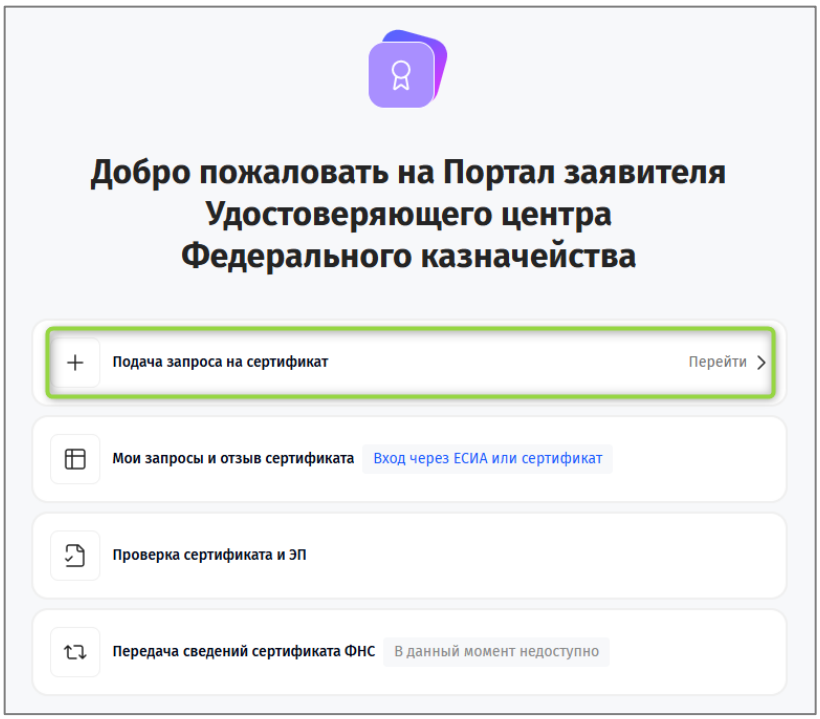


Рисунок 2. Переход к подаче запроса на сертификат

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

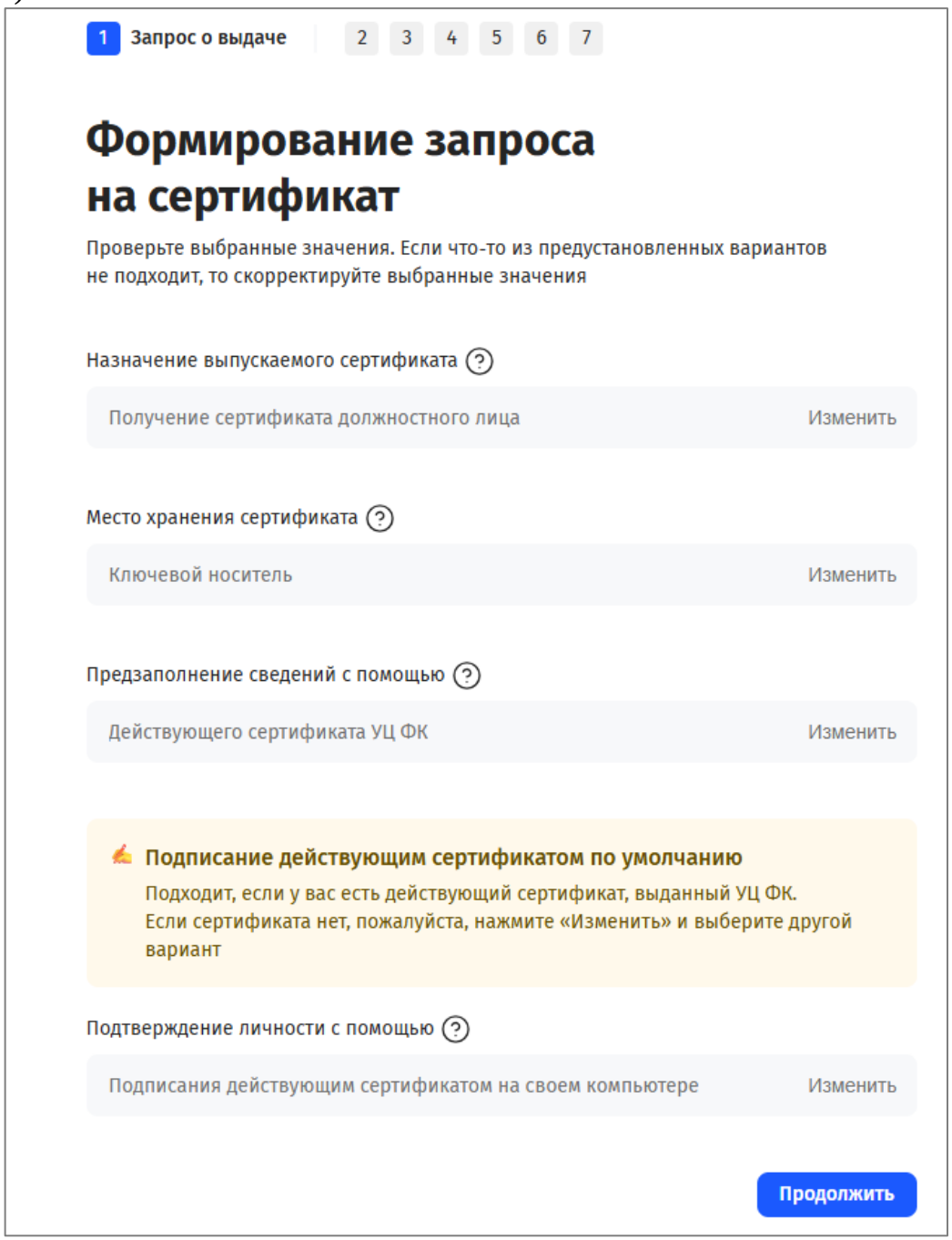


Рисунок 3. Форма подачи запроса. Шаг 1

На форме доступны для изменения следующие элементы:

- **Назначение выпускаемого сертификата**. По умолчанию установлено значение «Получение сертификата должностного лица». Выбрать иное значение (например, для получения сертификата юридического лица) 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 откроется окно выбора сертификата, с помощью которого необходимо осуществить авторизацию на портале.

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».

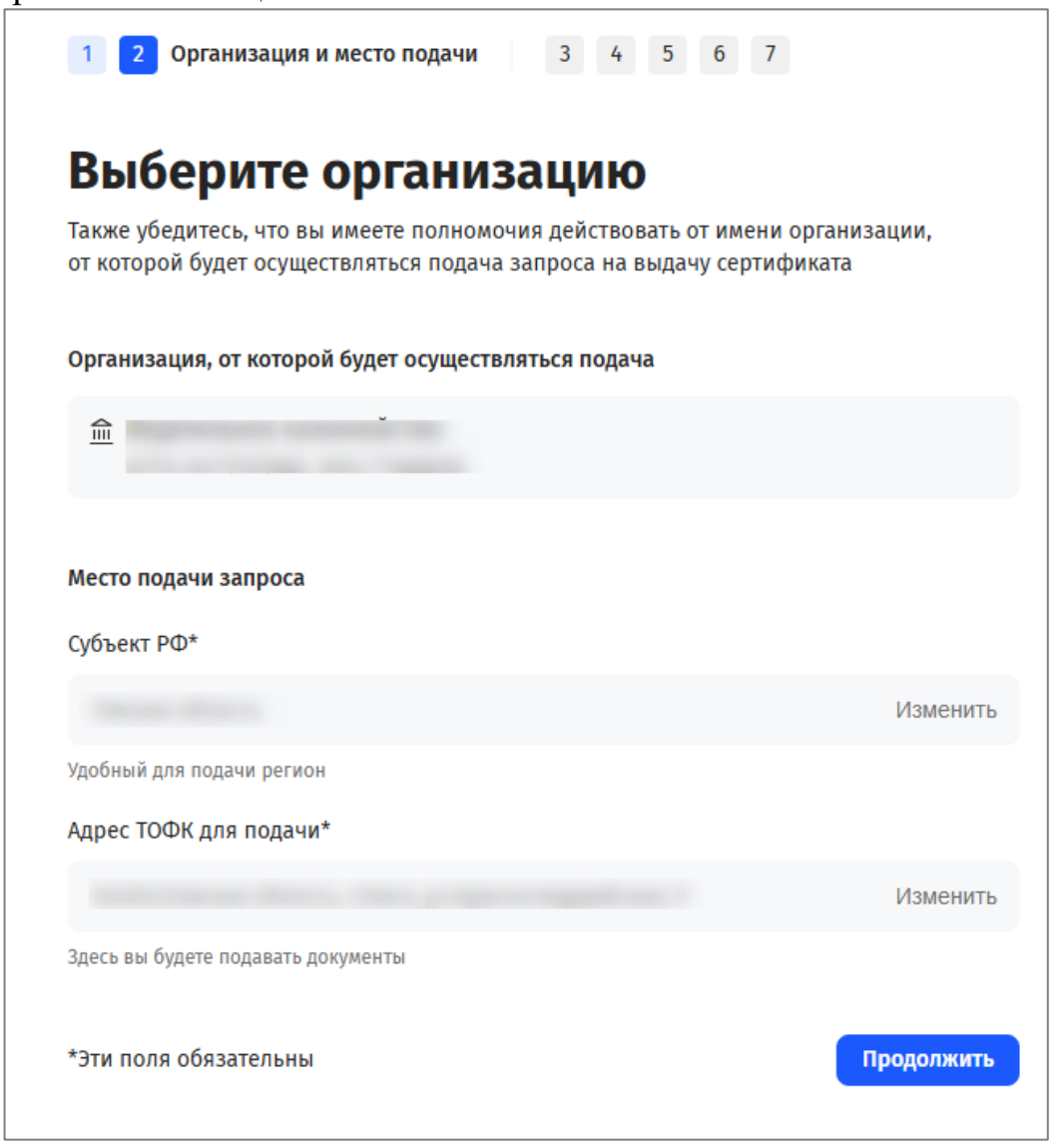


Рисунок 4. Выбор организации и места подачи

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*

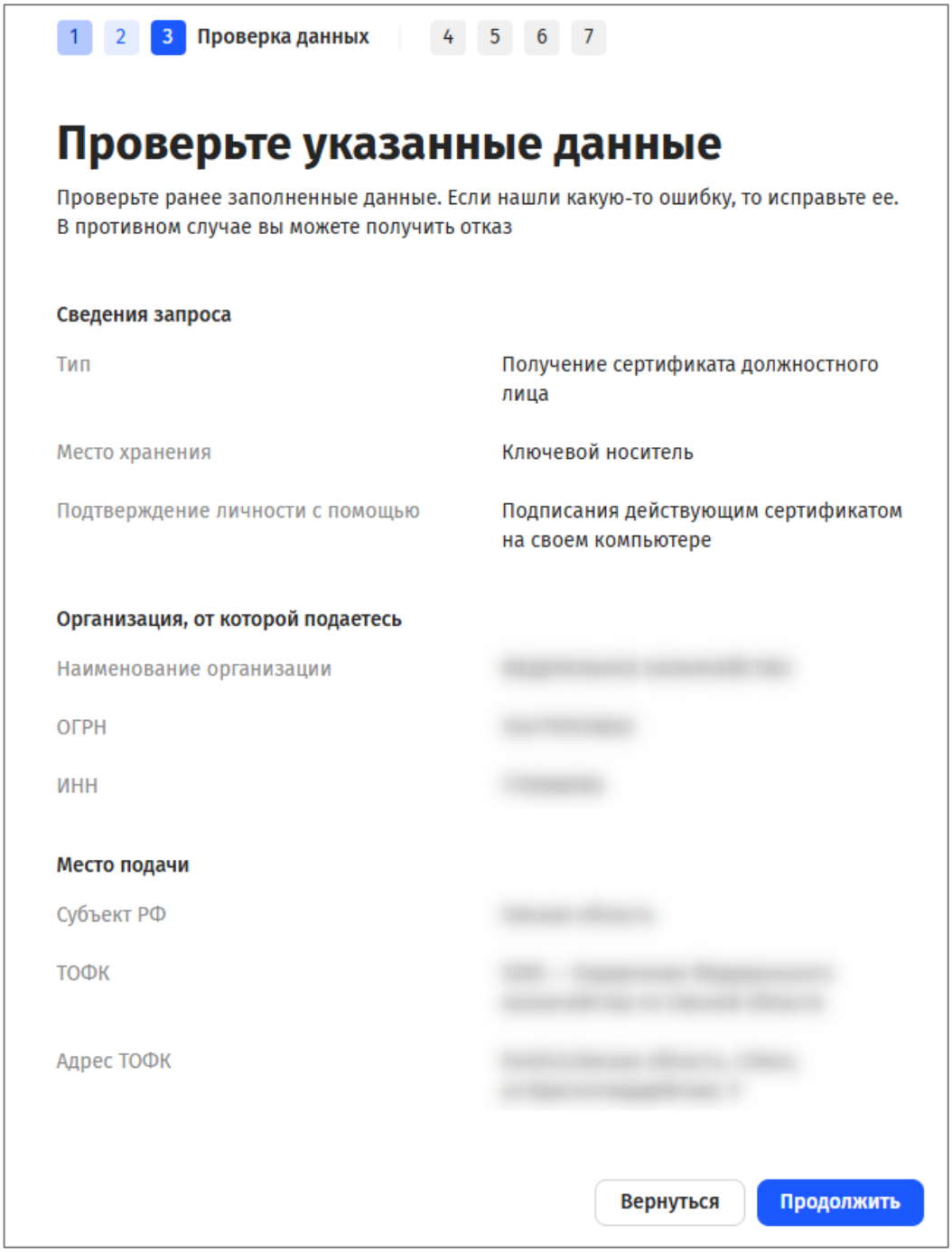


Рисунок 5. Шаг 3. Подтверждение указанных данных

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».

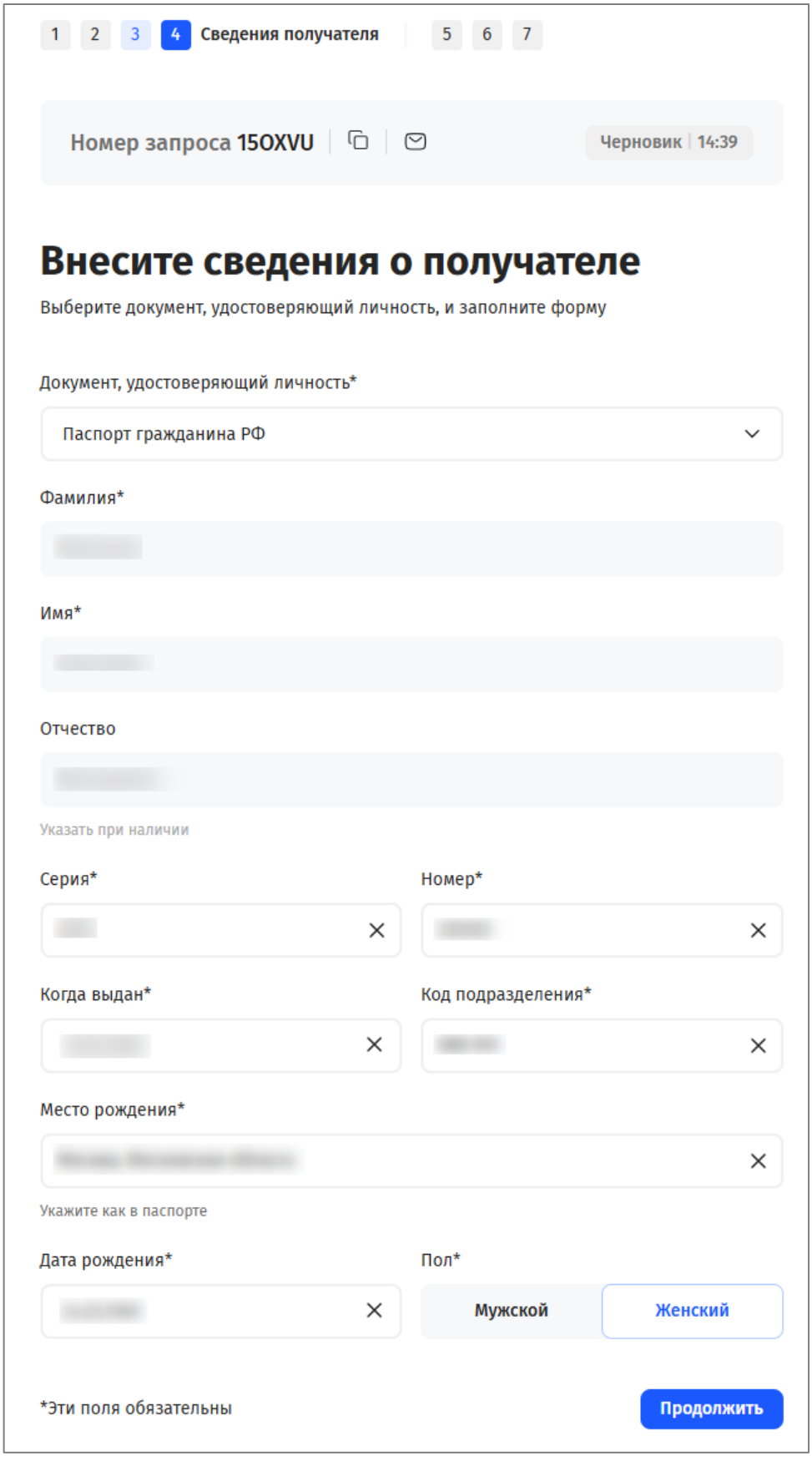


Рисунок 6. Шаг 4. Форма внесения данных документа, удостоверяющего личность

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

- 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).

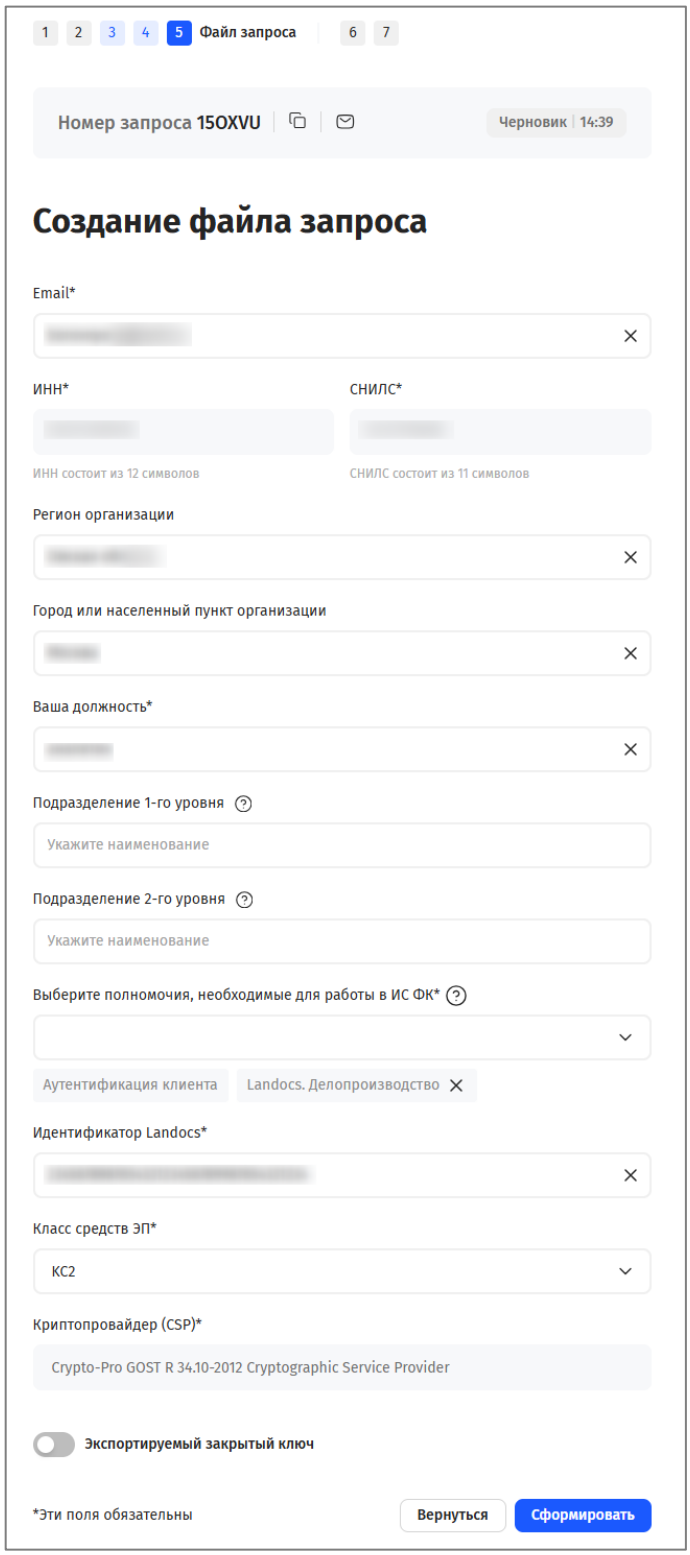


Рисунок 7. Шаг 5. Формирование файла запроса

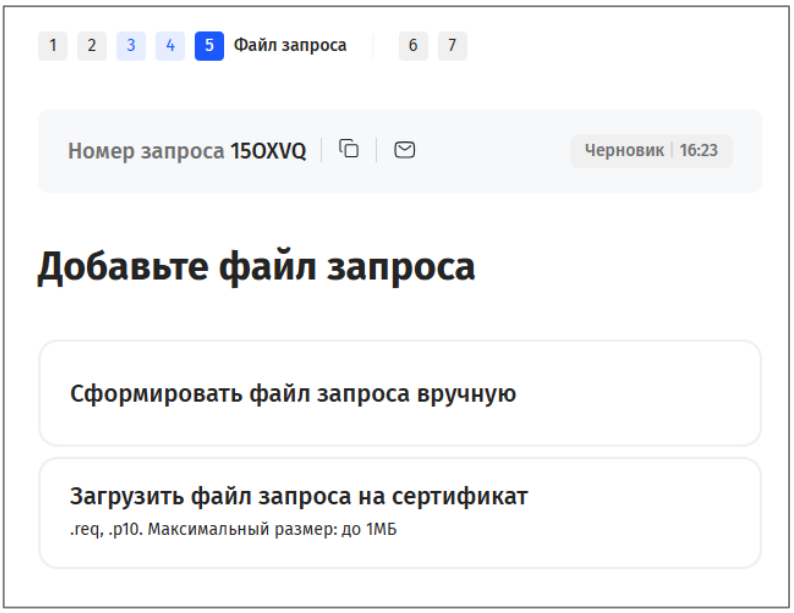


Рисунок 8. Шаг 5. Выбор формата добавления файла запроса

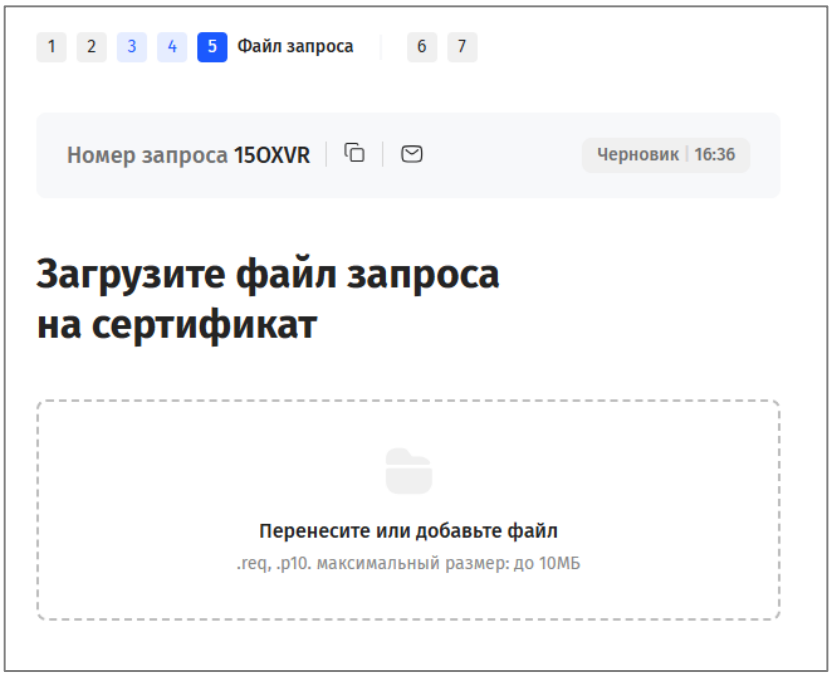


Рисунок 9. Шаг 5. Форма загрузки файла запроса

Примечание: для работы сертификата в большинстве информационных систем достаточно наличия полномочия по умолчанию «Аутентификация клиента».

Значение в поле «Класс средств ЭП» необходимо установить в соответствии с установленным СКЗИ (например, узнать необходимое значение можно зайдя в «Пуск» - «Все программы» - «КриптоПро» - запустив «КриптоПро CSP». Значение указано в поле «Версия ядра СКЗИ»).

В значении «Экспортируемый закрытый ключ» указывается возможность копирования ключа ЭП на другой носитель (если значение не выбрано, то контейнер с ключом нельзя будет копировать). По умолчанию указано возможность копирования не выбрана.

8. В случае формирования файла запроса на Портале заявителя, заполните на форме необходимые данные. Обязательные для заполнения поля отмечены *.

9. После внесения сведений убедитесь, что вставлен необходимый ключевой носитель для записи нового ключа и нажмите на кнопку «Сформировать».

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

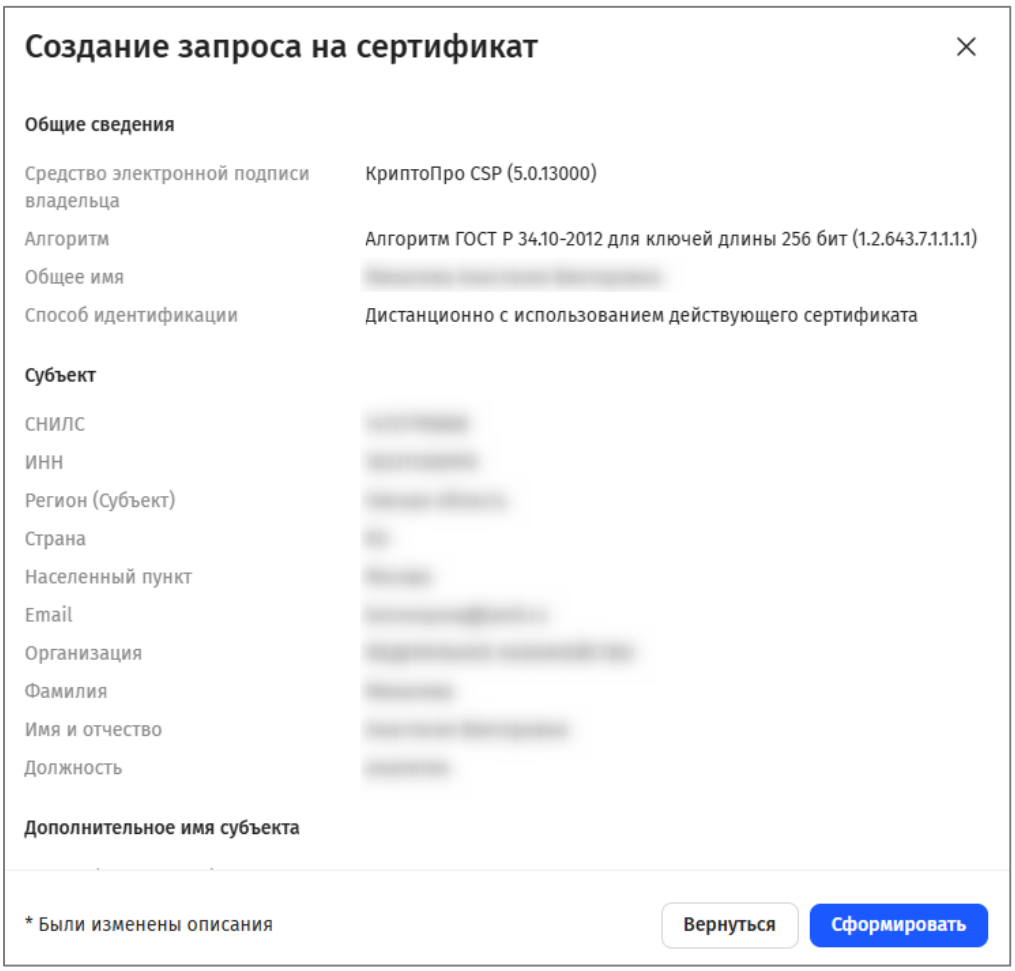


Рисунок 10. Форма создания запроса на сертификат со сформированными полями запроса

ВАЖНО!

На данном шаге будет сформирован закрытый ключ. Срок действия закрытого ключа отсчитывается то данного момента и составляет 1 год 3 месяца.

Необходимо выбрать съемный носитель – Рутокен, Etoken, флеш-накопитель и т.п. Обязательно запомните, куда Вы записали закрытый ключ, он вам потребуется для работы после получения сертификата.

Откроется соответствующее установленному на АРМ СКЗИ окно выбора устройства для записи закрытого ключа. После выбора носителя необходимо ввести пароль и подтвердить его. **Если пароль от закрытого ключа будет утерян или забыт, его восстановление невозможно.** Пароль от закрытого ключа известен только тому, кто его устанавливал.

Носитель должен быть учтен в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателей конфиденциальной информации)» (форма утверждена приказом ФАПСИ от 13.06.2001 № 152).

Закрытый ключ всегда должен храниться у владельца сертификата, несанкционированное копирование и использование ключа другими лицами запрещено. Требования к хранению носителя ключевой информации с ключом электронной подписи указаны в приказе ФАПСИ от 13.06.2001 № 152).

11. Осуществляется переход к шагу 6 для прикрепления документов (Рисунок *11*).

Если ранее при выпуске сертификата документ был прикреплен, то он и его данные автоматически заполняются.

При необходимости его можно отредактировать, используя кнопку «Изменить».

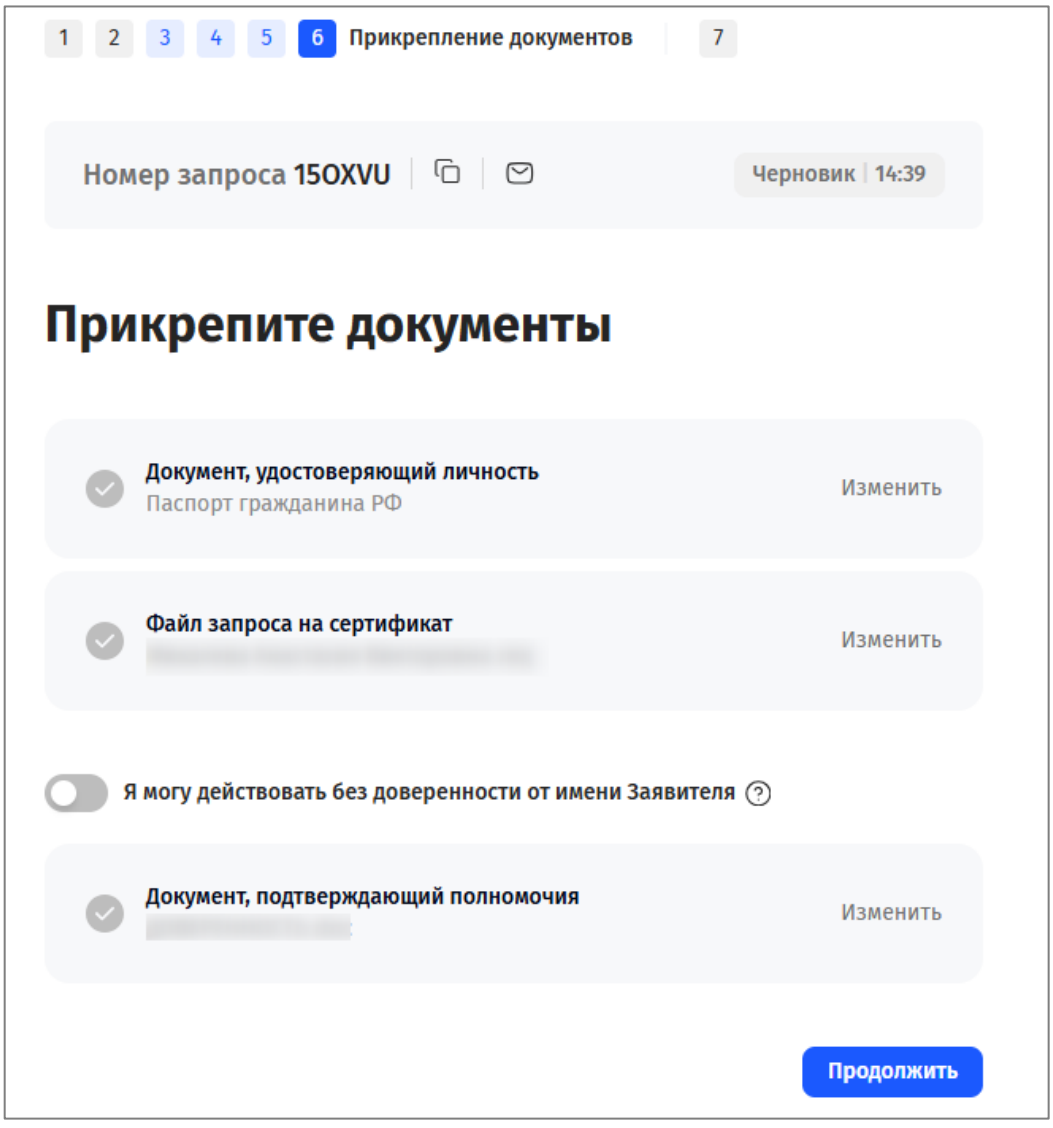


Рисунок 11. Шаг 6. Прикрепление документов

12. Удалить предыдущий прикрепленный документ (Рисунок *11*).

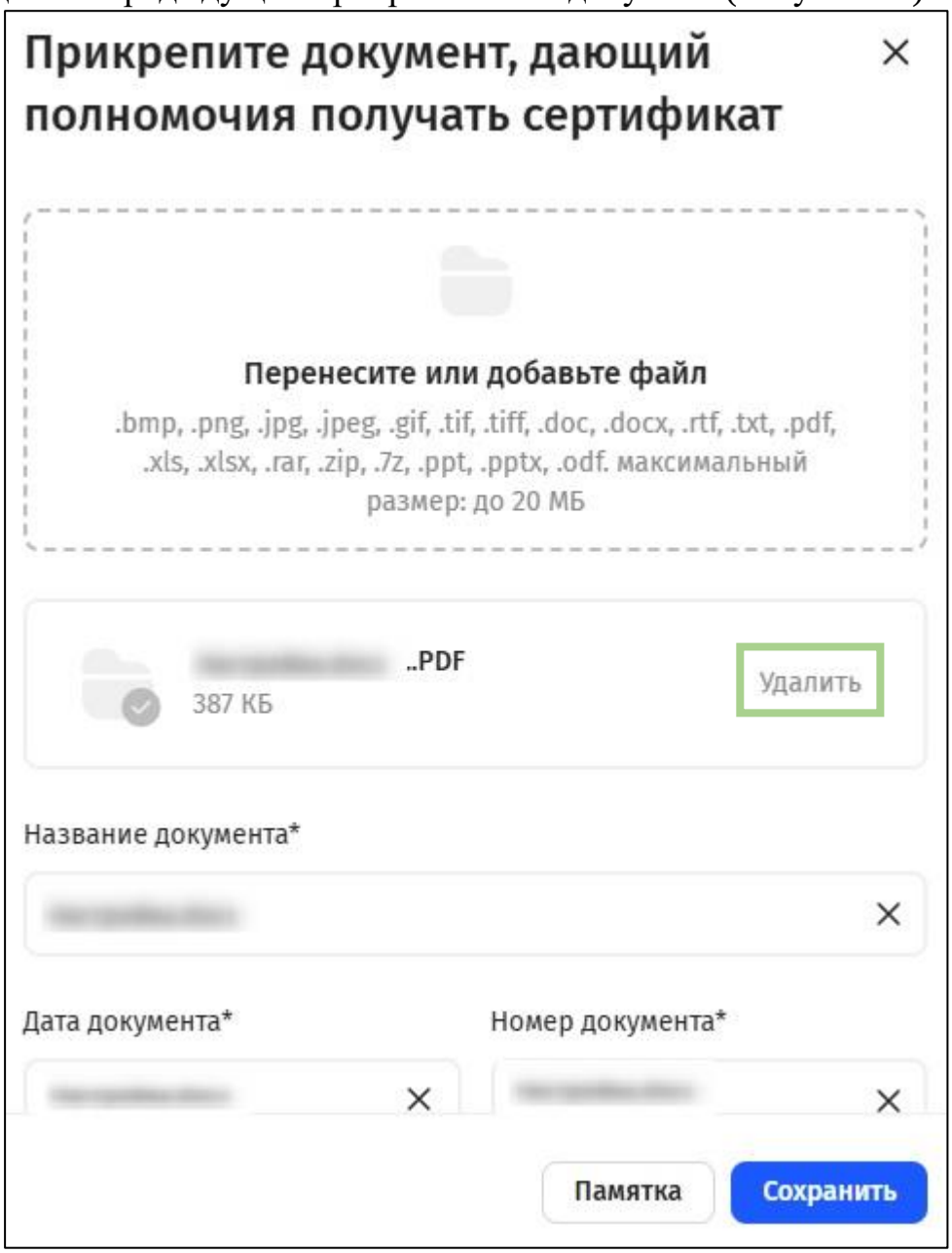


Рисунок 12. Шаг 6. Удаление ранее прикрепленного документа

13. Добавить новый документ:

В случае, если Получатель сертификата является лицом, имеющим право действовать без доверенности от имени Заявителя (руководитель организации и иные лица, указанные в ЕГРЮЛ), необходимо установить признак «Я могу действовать без доверенности от имени Заявителя».

Если владелец сертификата не является лицом, имеющим право действовать без доверенности от имени Заявителя, необходимо заполнить данные в разделе «Документ, подтверждающий полномочия»:

- прикрепить сканированный документ(**Ошибка! Источник ссылки не найден.**). Например, заверенную в соответствии с ГОСТ копию приказа о назначении, выписку из данного приказа, справку. (См. стр. 6 данной инструкции);
- указать название, дату и номер документа и сохранить сведения (Рисунок *13*).

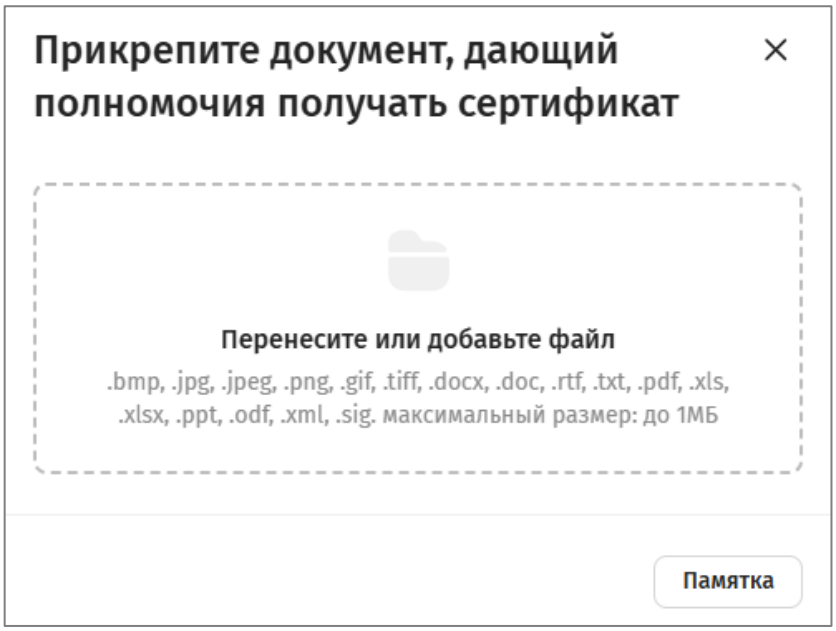


Рисунок 12. Форма прикрепления документа

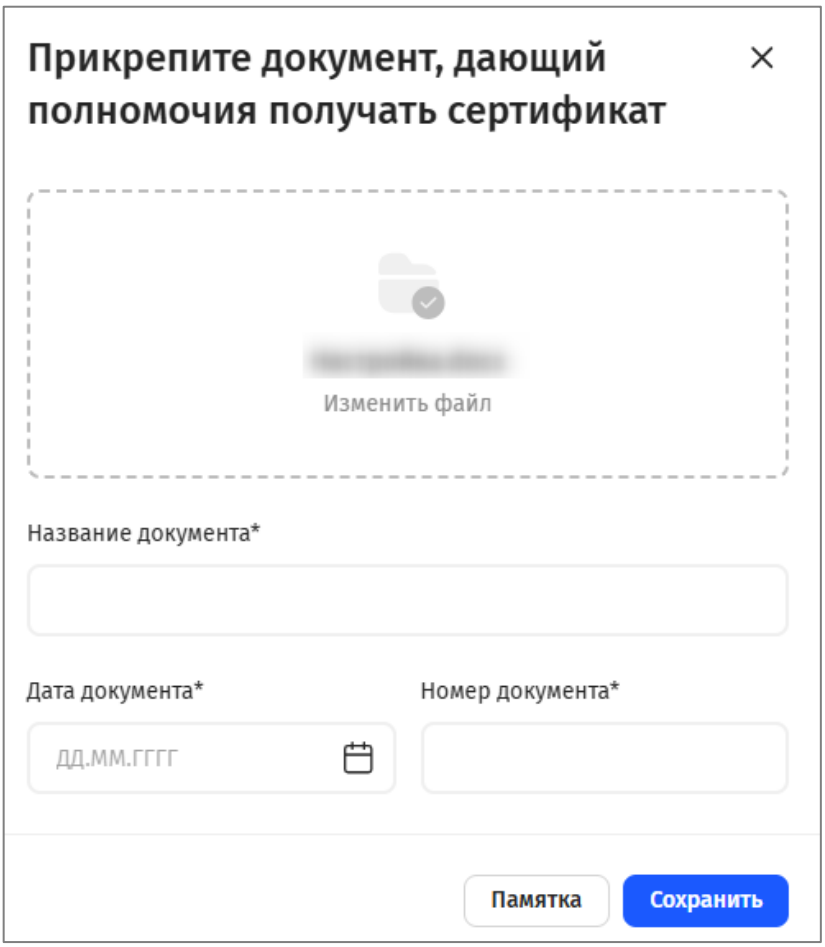


Рисунок 13. Форма указания данных документа

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 14).

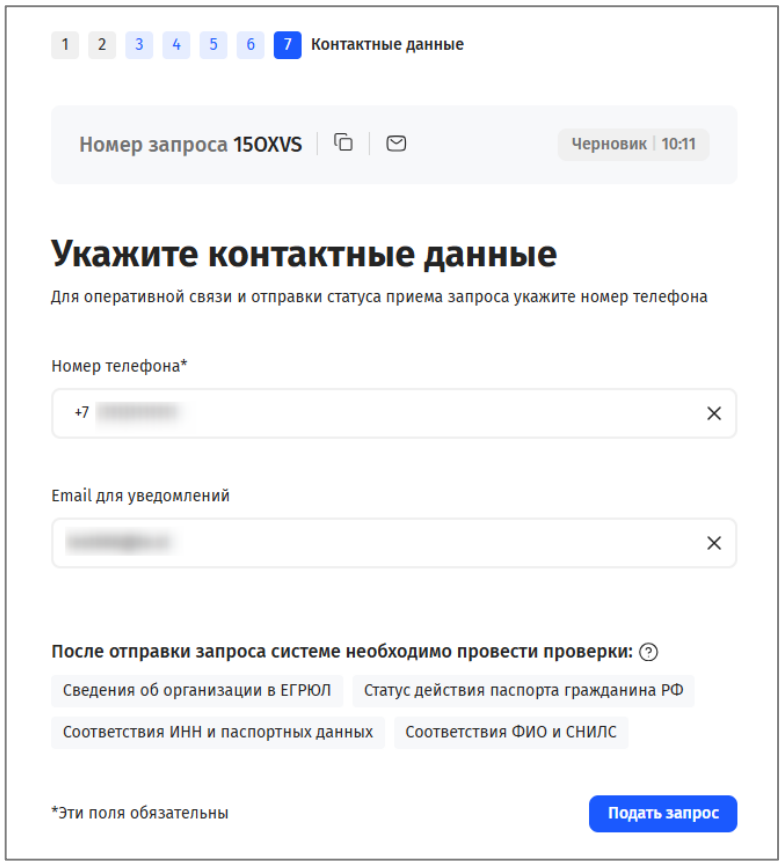


Рисунок 14. Шаг 7. Контактные данные

16. Нажать на кнопку «Подать запрос».

17. На отобразившейся форме нажать «Подписать» и подписать сведения (Рисунок 15).

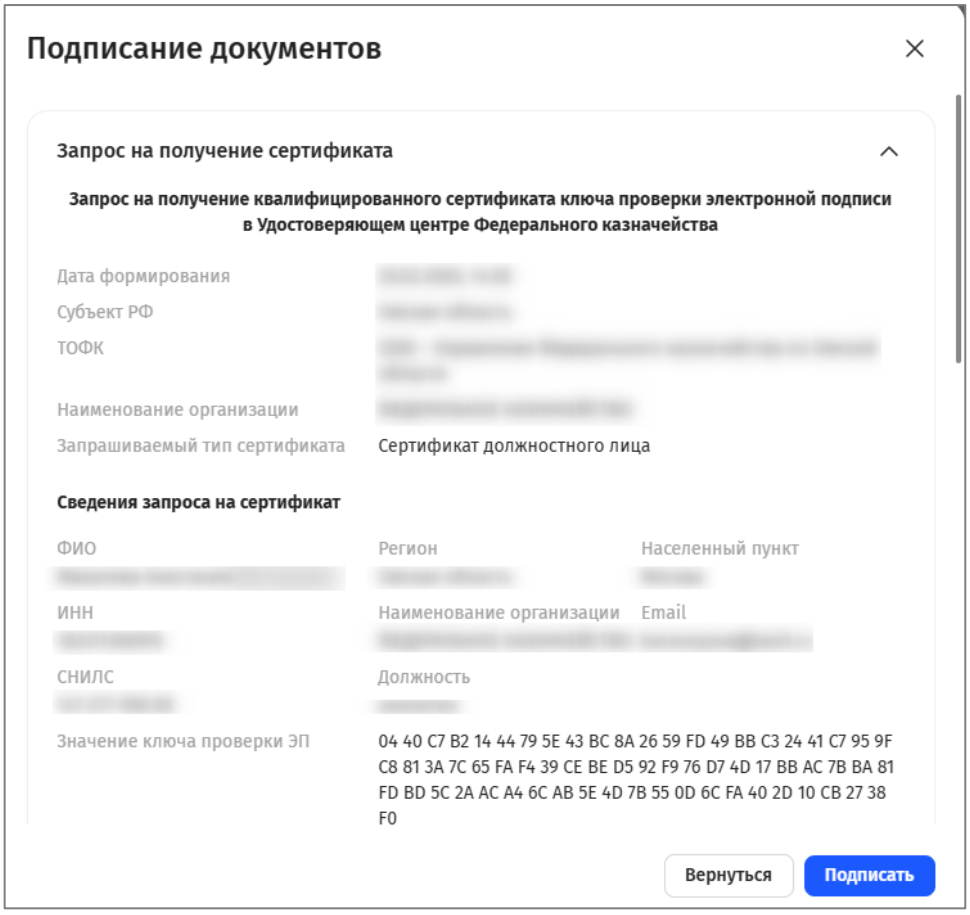


Рисунок 15. Форма «Подписание документов»

18. В результате отобразится окно подтверждения о подписании сведений ЭП (Рисунок 16).

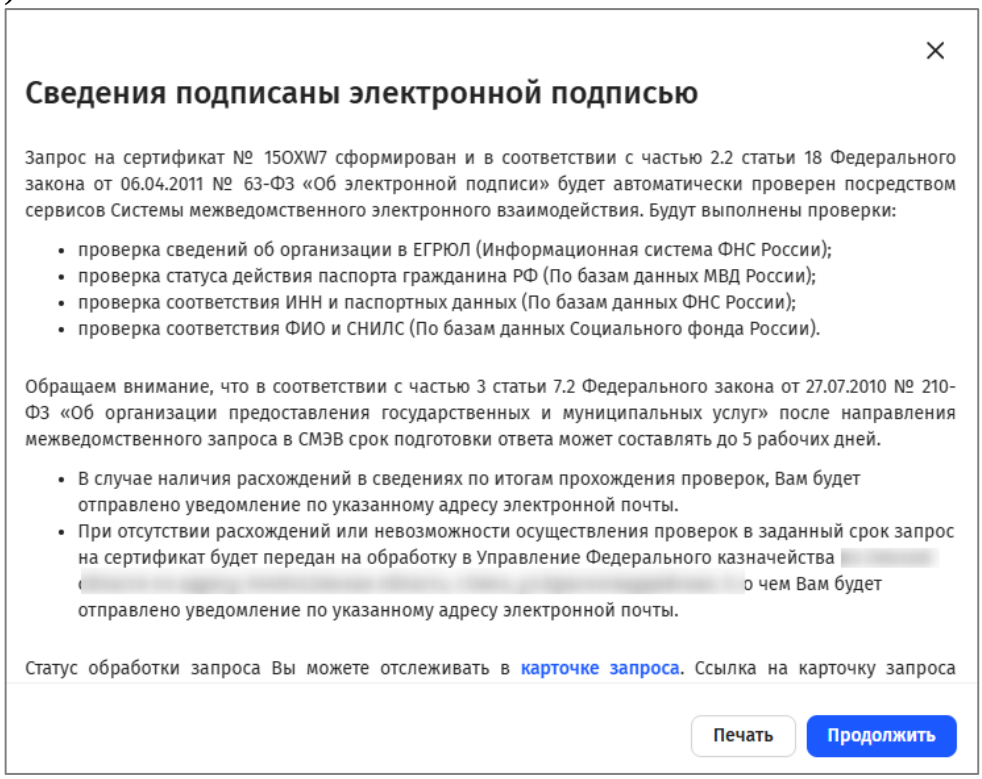


Рисунок 16. Окно подтверждения о подписания сведений ЭП

19. Нажать на кнопку «Продолжить» для закрытия информационного окна. Данные запроса будут отправлены на проверку сервисами СМЭВ, срок подготовки ответа от сервисов СМЭВ может составлять до 5 рабочих дней.

20. После успешных проверок сведений запроса на создание сертификата с помощью сервисов СМЭВ, запрос автоматически передается в подсистему ВРС для рассмотрения оператором УЦ.

В случае нахождения расхождений сведений запроса и сведений, полученных из СМЭВ, запрос автоматически отклоняется, и получатель сертификата получает соответствующее уведомление.

21. Оператор УЦ осуществит проверку пакета электронных документов на создание сертификата в подсистеме ВРС. В случае положительного результата проверки, Оператор УЦ изготовит сертификат. Получателю сертификата придет соответствующее уведомление на адрес электронной почты и появится возможность получить сертификат в личном кабинете Портала заявителя.

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. Осуществить вход в личный кабинет авторизованного пользователя Портала Заявителя на Портале заявителя используя свой действующий сертификат и ключ ЭП (Рисунок 17).

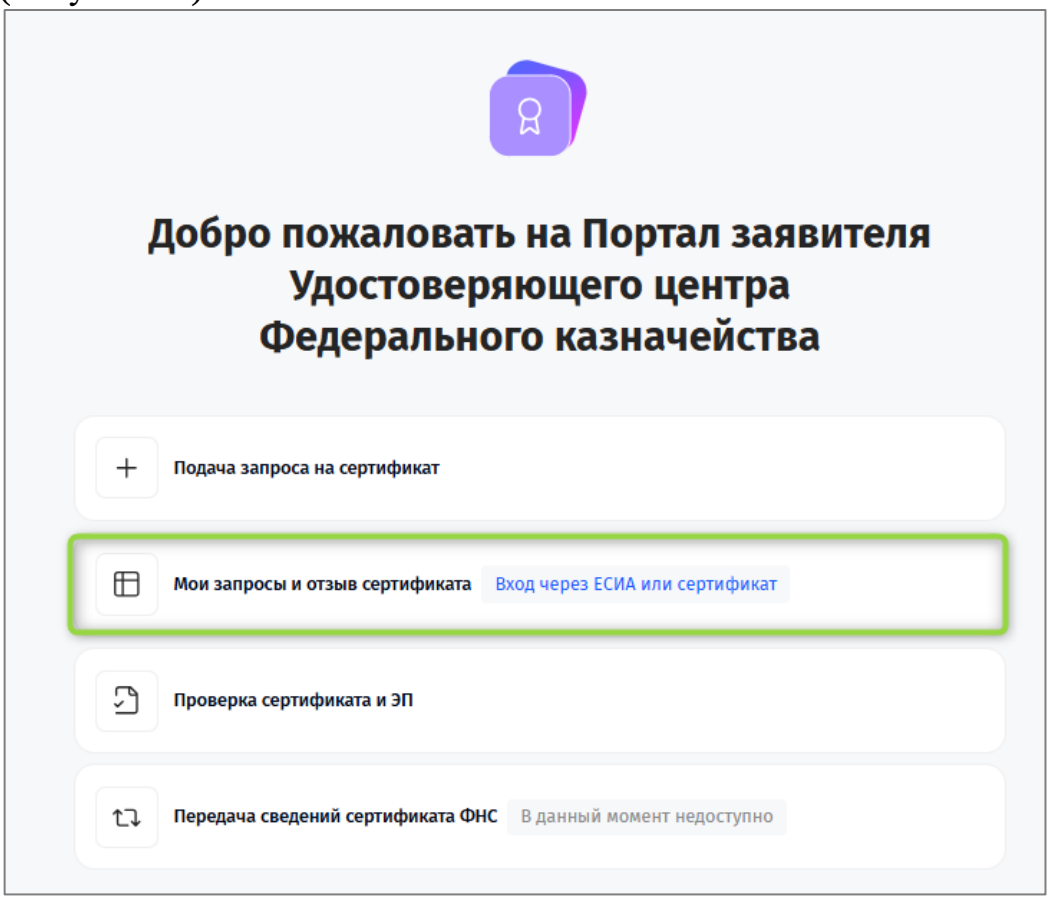


Рисунок 17. Вход в личный кабинет авторизованного пользователя Портала Заявителя

2. Перейти к вкладке «Запросы» (Рисунок 18).

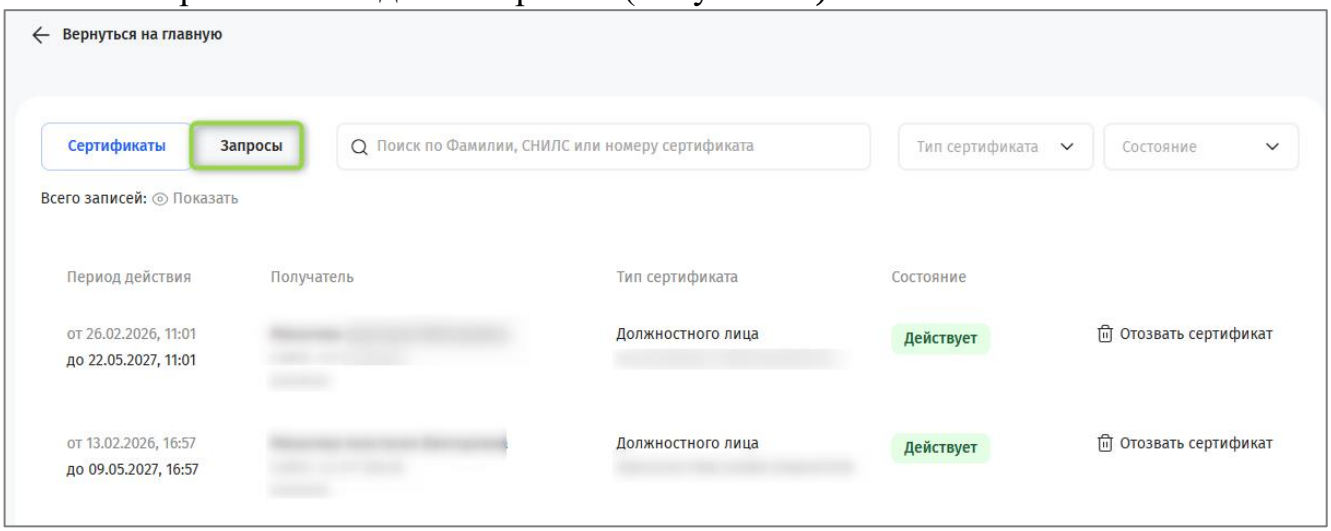


Рисунок 18. Меню перехода между реестрами сертификатов и запросов Получателя сертификата

3. Открыть карточку запроса, по которому изготовлен сертификат.

Внимание! Сертификат доступен для скачивания в течении 30 дней с момента изготовления.

4. В отобразившейся карточке запроса на создание сертификата нажать на кнопку «Скачать» (Рисунок 19)

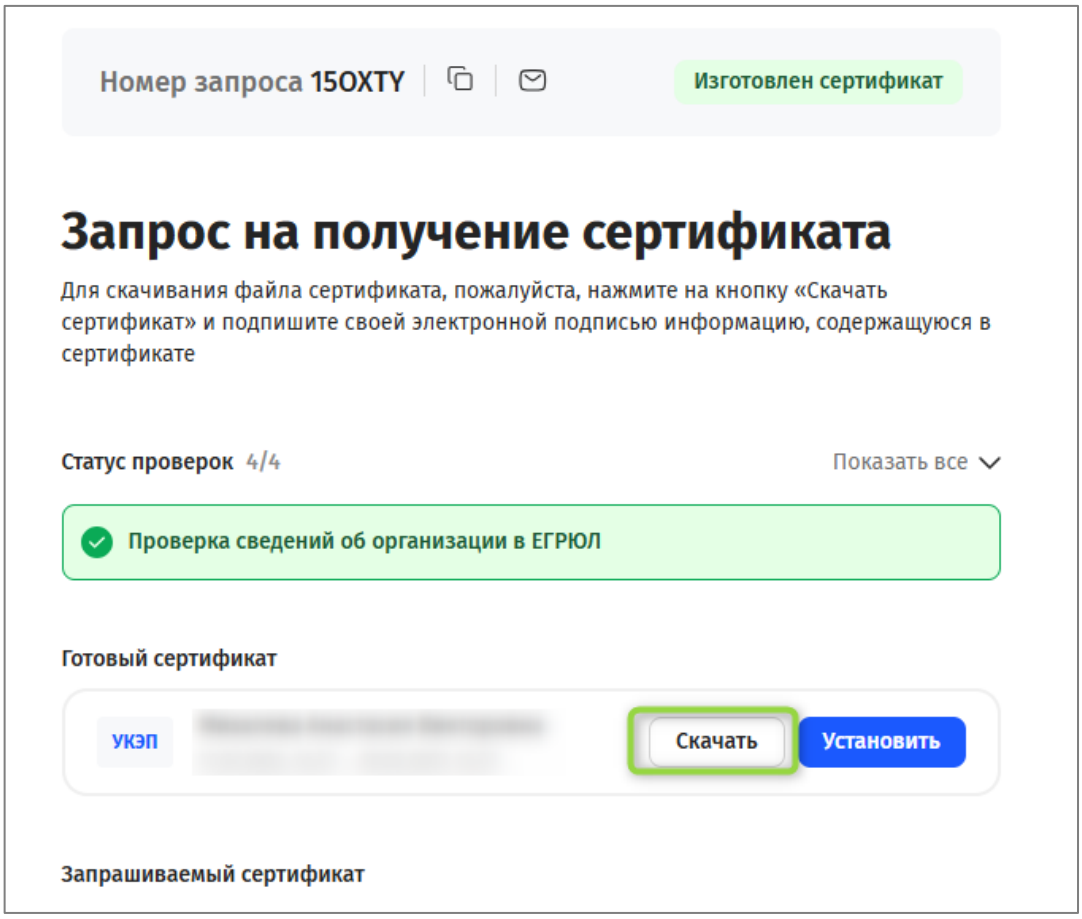


Рисунок 19. Карточка запроса на создание сертификата. Кнопка «Скачать»

5. В отобразившейся форме «Расписка в ознакомлении с информацией, содержащейся в квалифицированном сертификате» установить переключатели (Рисунок 20):

- 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.

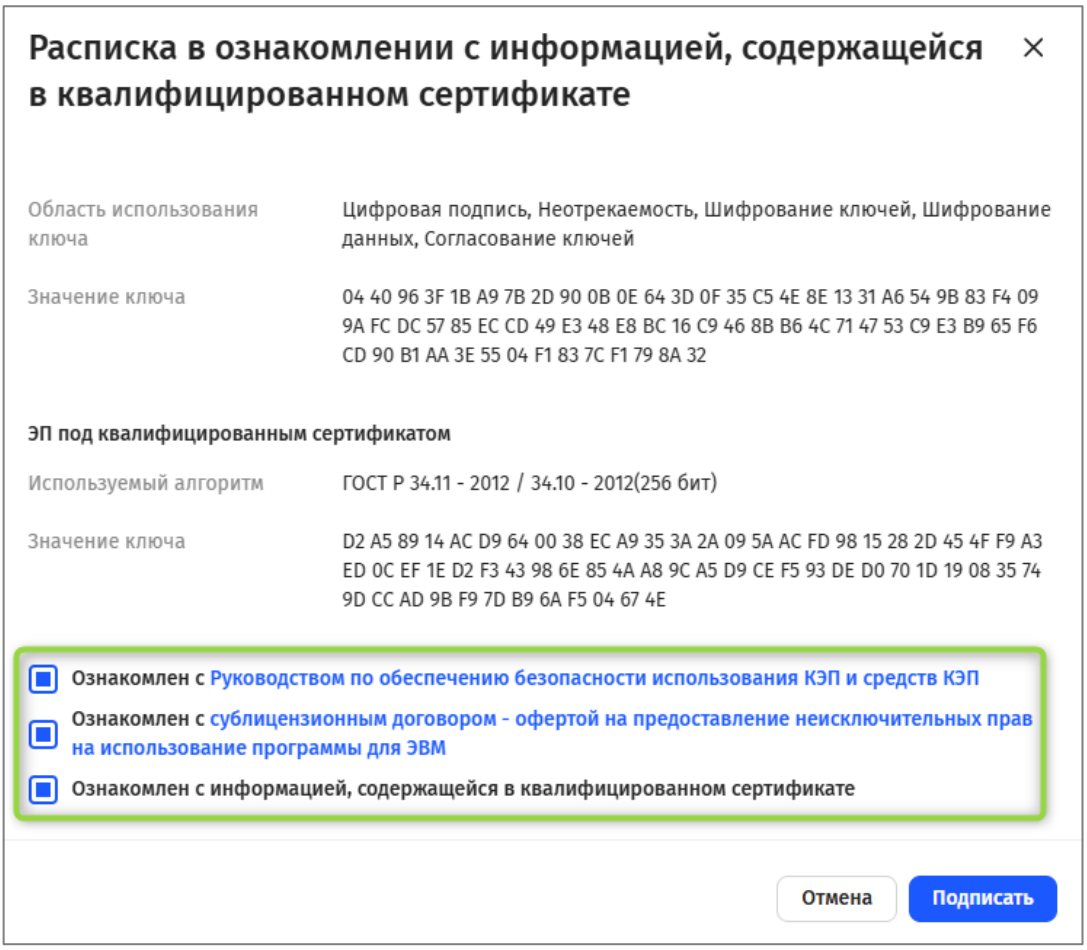


Рисунок 20. Ознакомление с информацией, содержащейся в сертификате

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

После подписания автоматически запустится процесс сохранения файла сертификата на АРМ.