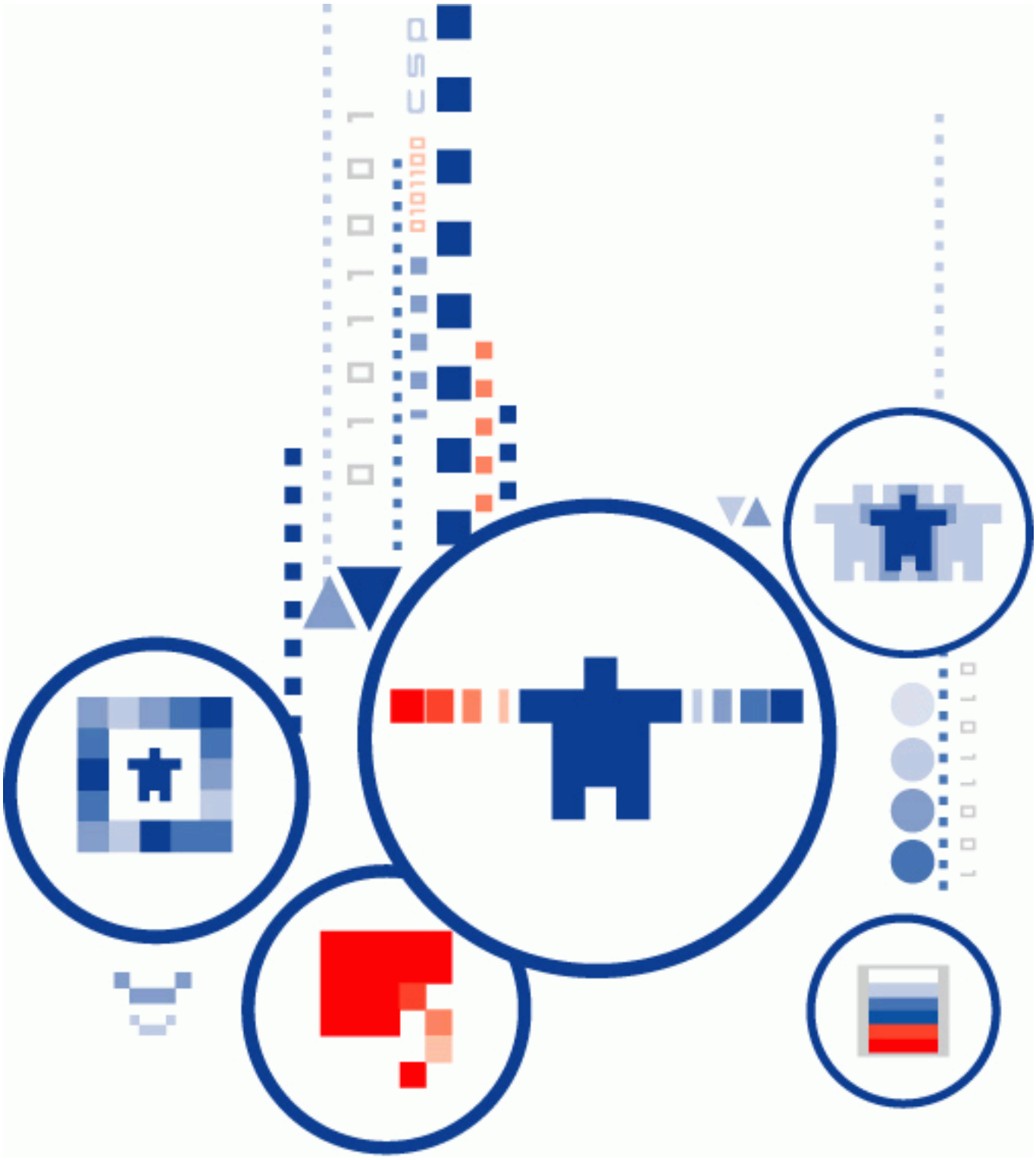

ПАК «КриптоПро Ключ»

Тестовый сервис электронной подписи

Инструкция Оператора тестового стенда

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Операторов тестового сервиса электронной подписи ООО «КРИПТО-ПРО» базе ПАК «КриптоПро Ключ» (далее – СЭП) и определяет порядок использования Веб-интерфейса СЭП на для осуществления операций по регистрации и управлению Пользователями СЭП и их тестовыми сертификатами ключей проверки электронной подписи.

Информация о разработчике ПАК «КриптоПро Ключ»:

ООО «КРИПТО-ПРО»

127 018, Москва, Улица Сущевский Вал, д.18, эт.17

Телефон: (495) 995 4820

https://www.cryptopro.ru/

E-mail: info@CryptoPro.ru

Содержание

Общие положения

Тестовый сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПАК «КриптоПро Ключ» (далее – СЭП) предназначен для демонстрации и тестирования операций создания и хранения ключей электронной подписи, формирования запросов на создание и управление тестовыми сертификатами ключей проверки электронной подписи (далее – сертификаты), выполнения операций по созданию и проверке электронной подписи различного формата криптографических сообщений, шифрования и расшифрования электронных документов.

Настоящая инструкция определяет порядок действия Оператора СЭП (далее – Оператор) при выполнении операций создания, редактирования, блокировки, разблокировки, удаления, управления Пользователями и их сертификатами.

1.1. *Требования и подготовка рабочего места Оператора*

На рабочем месте Оператора под управлением ОС Astra Linux Common Edition / Astra Linux Special Edition, Microsoft Windows 7/8/10/11 должно быть установлено СКЗИ «КриптоПро CSP» в соответствии с эксплуатационной документацией на это СКЗИ. Для подключения к СЭП необходимо использовать браузер с поддержкой криптографических алгоритмов ГОСТ.

Для аутентификации Оператора в СЭП нужно из предоставленного ООО «КРИПТО-ПРО» контейнера с расширением *.p7b установить содержащиеся в нём сертификаты в следующие хранилища сертификатов:

- Сертификат Тестового УЦ ООО «КРИПТО-ПРО» (УЦ 2.0) – в хранилище «Доверенные корневые центры сертификации».
- Сертификат Оператора – в хранилище «Личное».

2. Структура меню

Для работы в СЭП Оператору необходимо осуществить вход в веб-интерфейс Оператора по адресу https://stendkey.cryptopro.ru/frontend/[1] и выбрать пункт «Вход по

[1] Для каждого конкретного экземпляра СЭП следует использовать настройки доступа, предоставленные ООО «КРИПТО-ПРО»..

сертификату», после чего в появившемся окне подтверждения сертификата выбрать сертификат Оператора и нажать кнопку «*ОК*» (см. Рисунок 1. - Выбор сертификата).

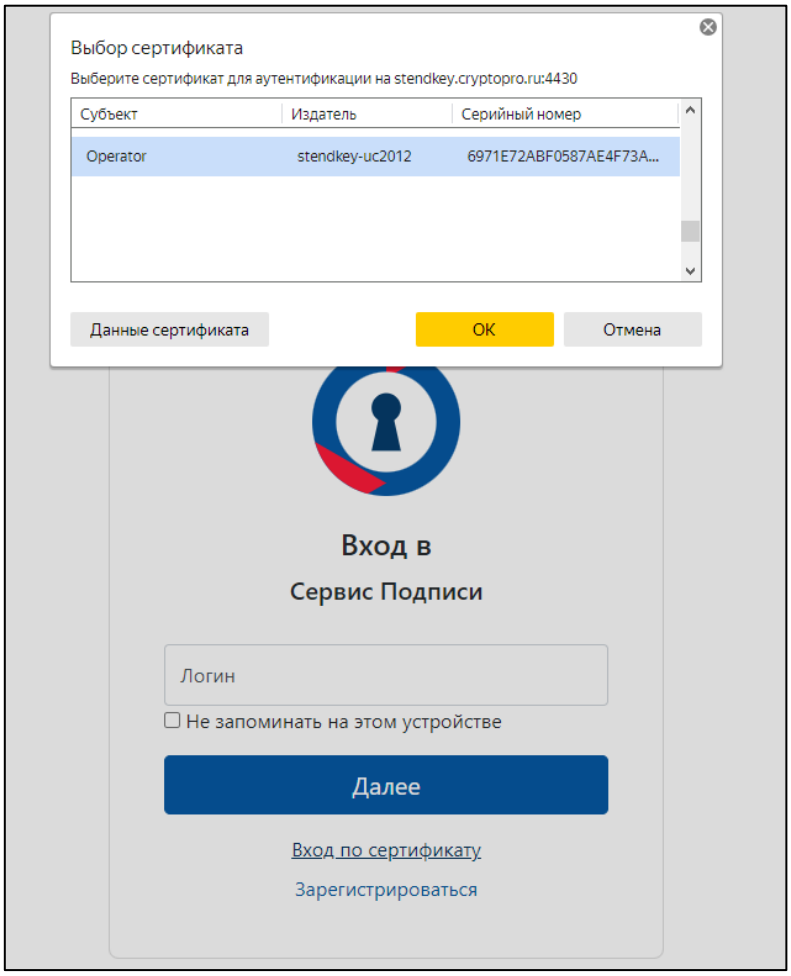

Рисунок 1. - Выбор сертификата

После подтверждения сертификата и ввода ПИН-кода ключевого контейнера будет отображена начальная страница веб-интерфейса Оператора (см. Рисунок 1. - Выбор сертификата)

В меню начальной страницы Оператора доступны 4 раздела:

- «*Пользователи*».
- «*Средства аутентификации*»
- «*Оповещения*».
- «*Журнал*»
- «*Отчеты*»

3. Раздел «Пользователи»

Раздел предназначен для создания новых и управления существующими Пользователями (далее – Пользователи).

3.1. *Создание нового Пользователя*

Для регистрации нового Пользователя нужно нажать кнопку «*Создать нового пользователя*» (см. Рисунок 2. - Создание нового Пользователя).

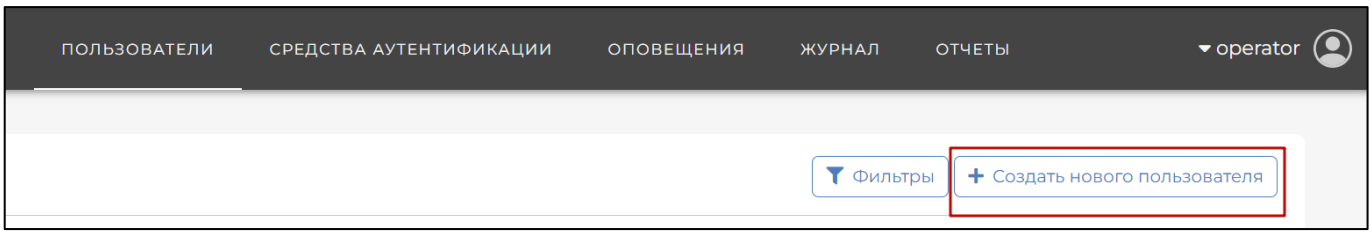

Рисунок 2. - Создание нового Пользователя

В появившейся форме «*Создание нового пользователя*» необходимо ввести информацию о создаваемом Пользователе.

После корректного заполнения всех полей формы следует нажать кнопку «*Создать пользователя*» (см. Рисунок 3. - Ввод сведений о Пользователе).

После создания Пользователя СЭП предложит настроить параметры аутентификации Пользователя (см. *Настройка параметров аутентификации Пользователя*).

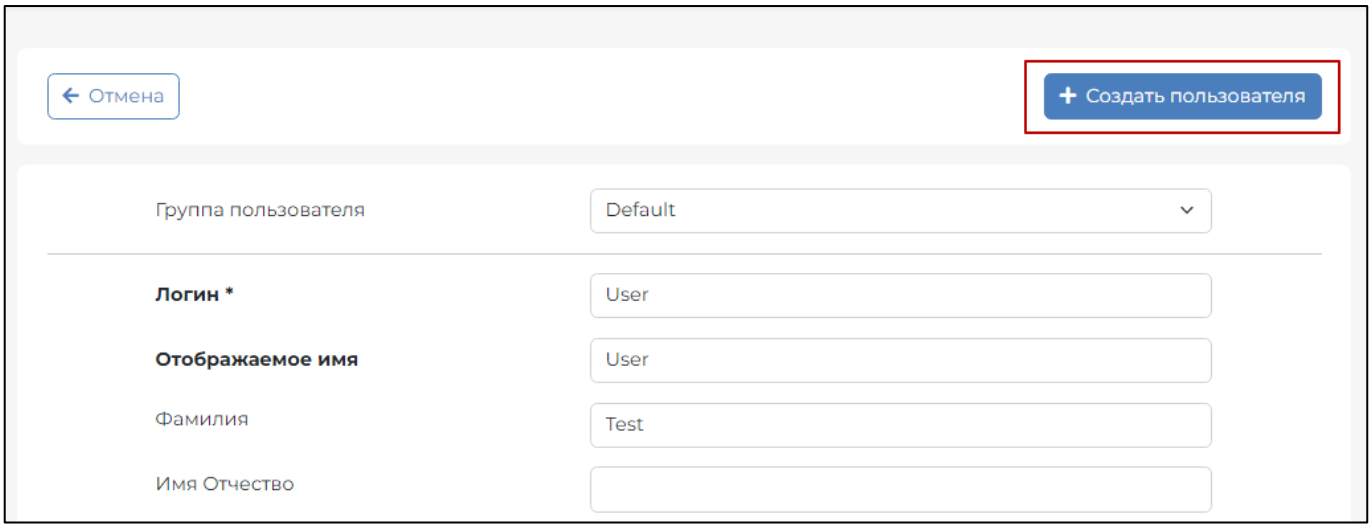

Рисунок 3. - Ввод сведений о Пользователе

3.2. *Управление существующими Пользователями*

Для управления существующими Пользователями нужно войти в раздел «*Пользователи*» в интерфейсе Оператора. СЭП отобразит всех зарегистрированных Пользователей, для каждого из которых в графе «*Управление пользователем*» доступны следующие действия (в соответствии с порядком значков в графе, см. Рисунок 4. - Управление Пользователями СЭП):

- «*Редактировать*» – редактирование атрибутов Пользователя.
- «*Контакты*» – редактирование контактов Пользователя.
- «*Аутентификация*» – редактирование методов аутентификации, подтверждения и доступа Пользователя к операциям в СЭП.
- «*Оповещения*» – редактирование методов и операций, оповещение о которых необходимо Пользователю.
- *Разрешения*» – просмотр и управление разрешениями других приложений.
- «*Сертификаты*» – управление сертификатами Пользователя.
- «*Удалить*» – удаление Пользователя.

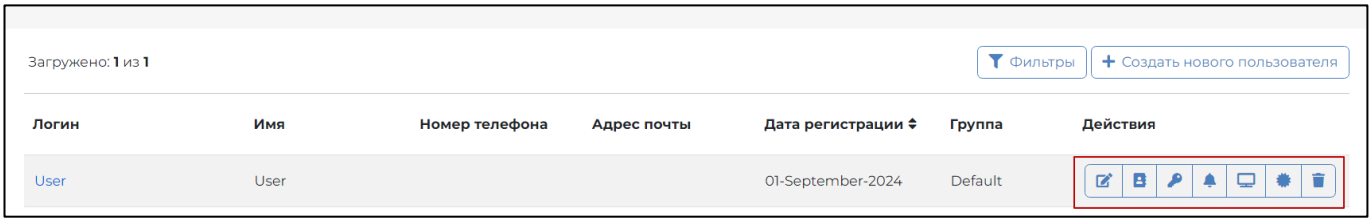

Рисунок 4. - Управление Пользователями СЭП

3.2.1. *Редактирование атрибутов Пользователя*

Для редактирования атрибутов Пользователя нужно нажать значок «*Редактировать*» в графе «*Управление пользователем*».

После завершения редактирования атрибутов Пользователя следует нажать кнопку «Сохранить» для сохранения изменений (см. Рисунок 5. - Редактирование атрибутов Пользователя).

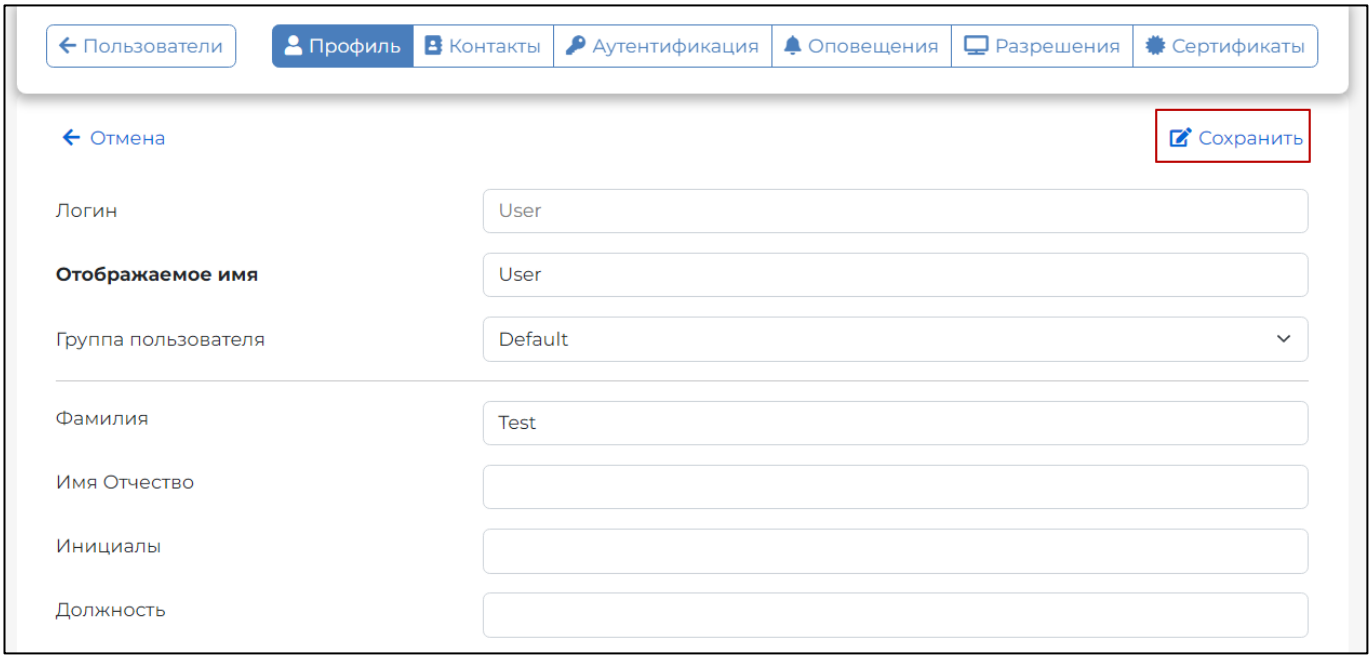

Рисунок 5. - Редактирование атрибутов Пользователя

3.2.2. *Настройка параметров аутентификации Пользователя*

В СЭП предусмотрены методы первичной аутентификации (применяются для аутентификации входа Пользователя в интерфейс СЭП) и методы вторичной аутентификации (применяются для подтверждения действий Пользователя в СЭП).

Доступны следующие методы первичной аутентификации Пользователя:

- «*Только идентификация*» – отсутствие первичной аутентификации (только ввод логина Пользователя при входе в СЭП).
- «*Аутентификация по сертификату*» – аутентификация Пользователя по сертификату; метод доступен только в случае, если Пользователю назначен сертификат.
- «*Аутентификация по паролю*» – аутентификация Пользователя по паре «логин-пароль»; пароль может быть сгенерирован Оператором в интерфейсе СЭП и передан Пользователю.
- «*Аутентификация по SAML-токену*» – аутентификация Пользователя в стороннем центре идентификации (далее – ЦИ); метод доступен в случае, если в СЭП зарегистрирован хотя бы один сторонний ЦИ.

Доступны следующие методы вторичной аутентификации Пользователя:

- «*Аутентификация по SMS*» – подтверждение действий Пользователя в СЭП по коду в SMS, отправляемых СЭП на мобильный телефон Пользователя; метод доступен только в случае, если задан номер мобильного телефона Пользователя. В тестовом СЭП не выполняется отправка реальных SMS-сообщений; используется эмуляция, посредством записи текста SMS-сообщений в текстовые файлы. Адрес, по которому публикуются файлы, предоставляется в списке данных для подключения.
- «*Аутентификация по протоколу OATH*» – подтверждение действий Пользователя в СЭП по одноразовому паролю OTP-токена; метод доступен только в случае, если заданы параметры OTP-токена.
- «*Аутентификация по электронной почте*» – подтверждение действий Пользователя в СЭП по коду в сообщениях электронной почты,

отправляемых СЭП на адрес электронной почты Пользователя; метод доступен только в случае, если задан адрес электронной почты Пользователя.

- «*Аутентификация с помощью мобильного приложения*» – подтверждение действий Пользователя в СЭП в мобильном приложении «DSS Client»

Пользователю должен быть назначен хотя бы один метод первичной аутентификации.

3.2.2.1. Настройка первичной аутентификации

3.2.2.1.1 Настройка аутентификации по сертификату

Для создания сертификата первичной аутентификации пользователя возможно импортировать компоненты имени Пользователя из существующего сертификата (кнопка «*Заполнить компоненты имени из сертификата*) (см. Рисунок 6. - Назначение сертификата для первичной аутентификации Пользователя).

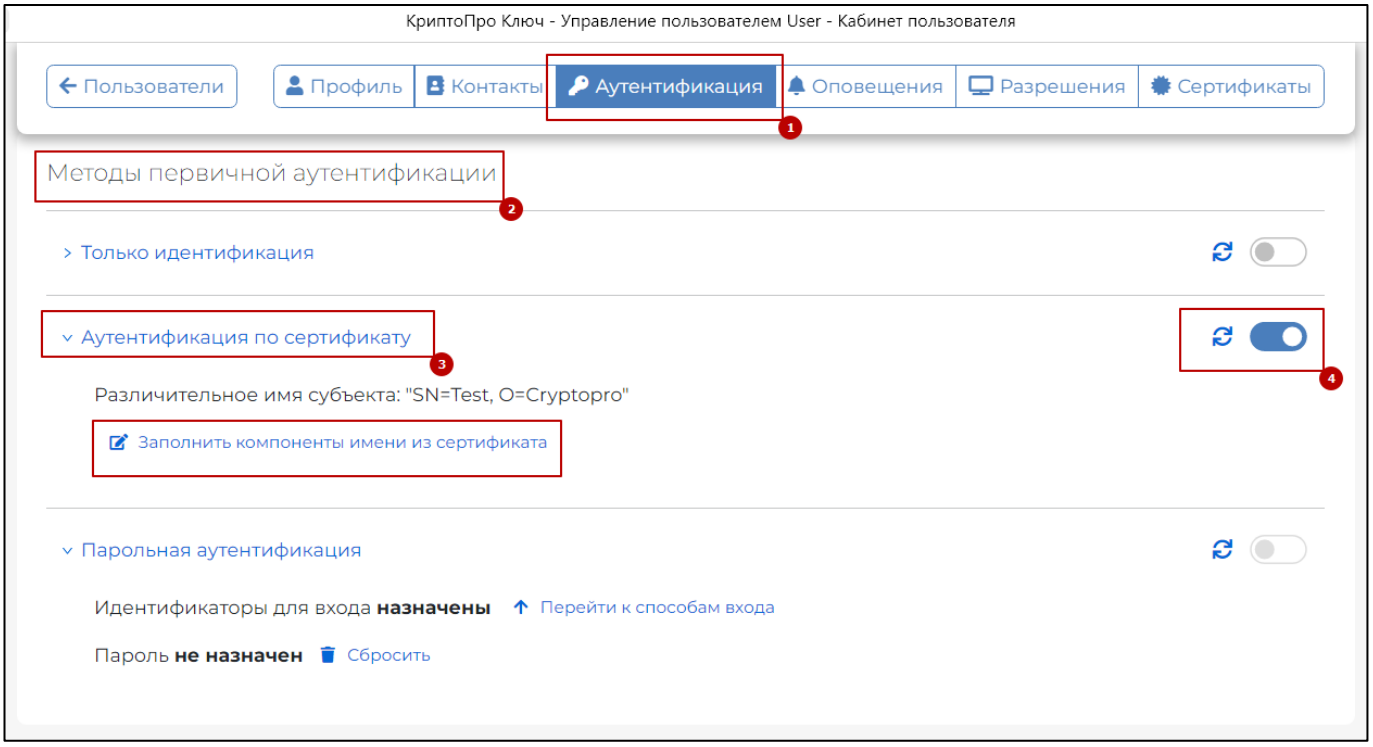

Рисунок 6. - Назначение сертификата для первичной аутентификации Пользователя

Далее нужно следовать инструкциям СКЗИ «КриптоПро CSP». Для включения первичной аутентификации по сертификату необходимо установить переключатель «*Аутентификация по сертификату*» в группе «*Первичная аутентификация*» в активное положение.

3.2.2.1.2 Настройка аутентификации по паролю

Для настройки первичной аутентификации Пользователя по паролю нужно в группе «*Методы первичной аутентификации*» раскрыть блок «*Аутентификация по паролю*» и нажать кнопку «*Сбросить*» (см. Рисунок 7. - Генерация пароля для первичной аутентификации Пользователя).

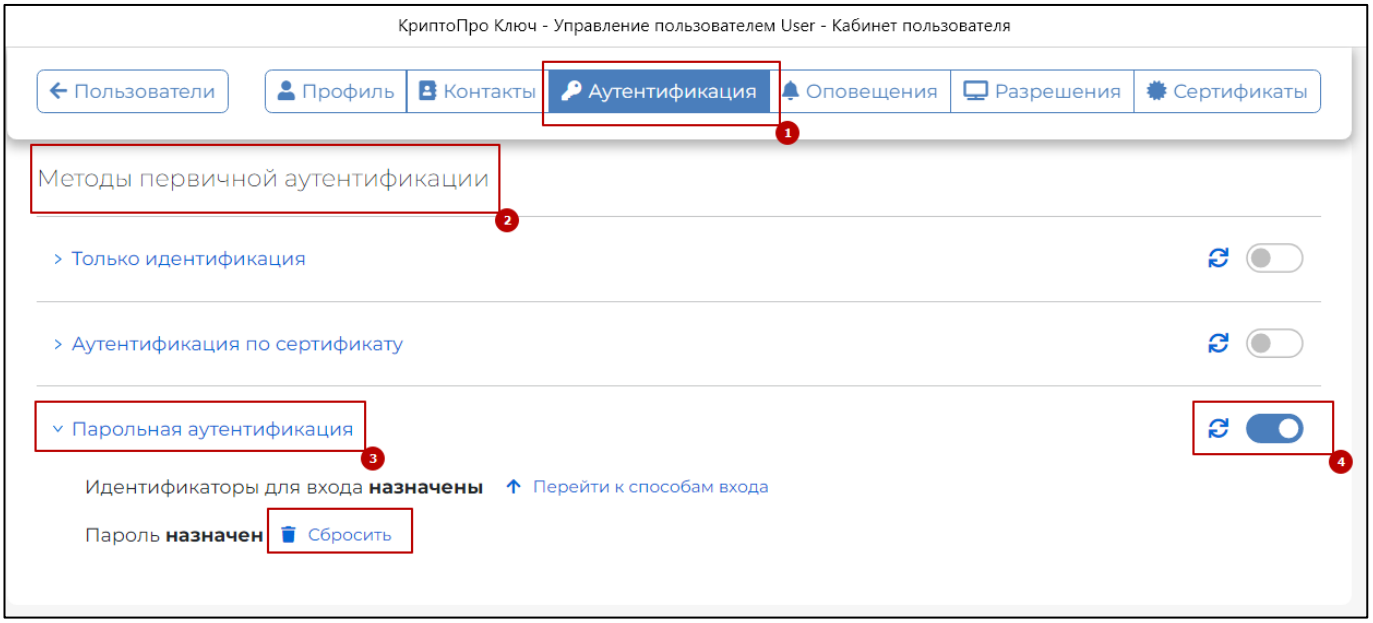

Рисунок 7. - Генерация пароля для первичной аутентификации Пользователя

В появившемся диалоге есть возможность отобразить сгенерированный пароль на экране, отправить по email, смс, либо вывести его на печать или отобразить в отдельном окне. Далее нужно нажать кнопку «Сбросить пароль» (см. Рисунок 8. - Способ отображения созданного пароля).

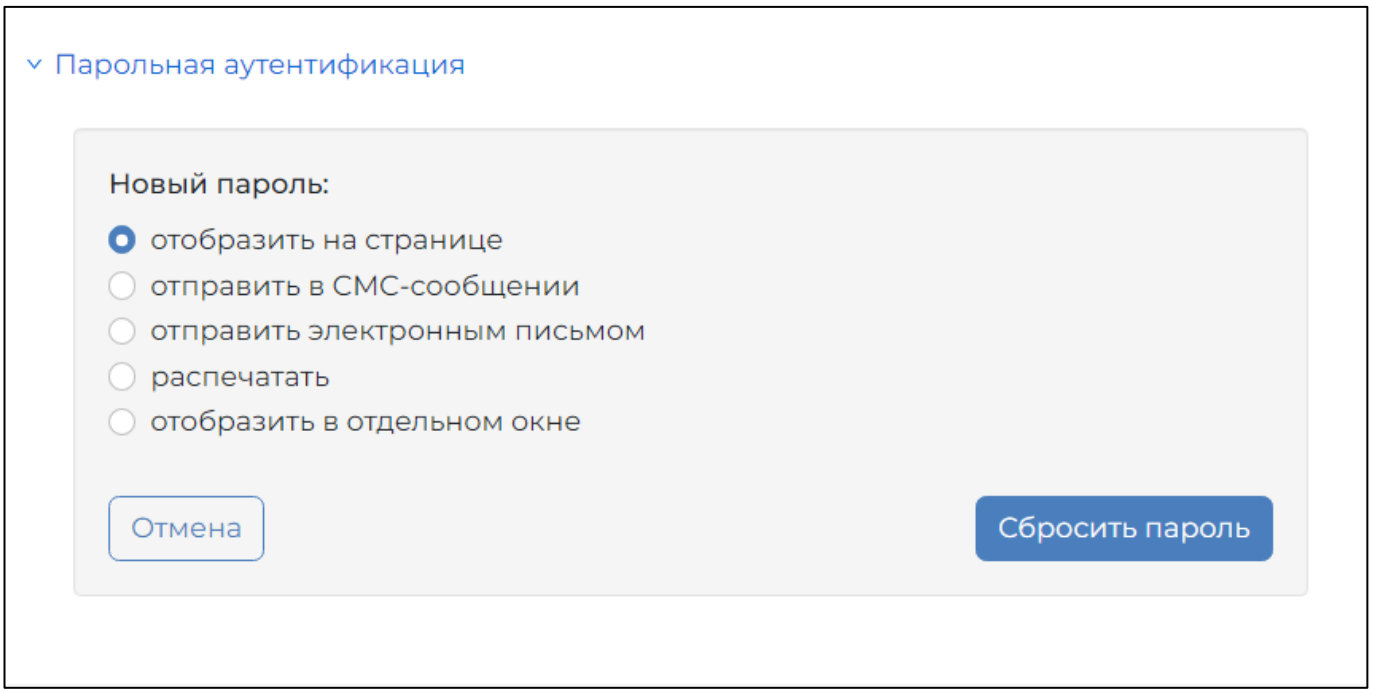

Рисунок 8. - Способ отображения созданного пароля

После нажатия кнопки «Сбросить пароль» отобразится сообщение об успешной смене пароля первичной аутентификации Пользователя, а сам пароль будет выведен, соответственно, на экран или принтер (см. Рисунок 9. - Успешная смена (задание) пароля). Для включения первичной аутентификации по паролю нужно установить переключатель «*Аутентификация по паролю*» в группе «*Первичная аутентификация*» в активное положение.

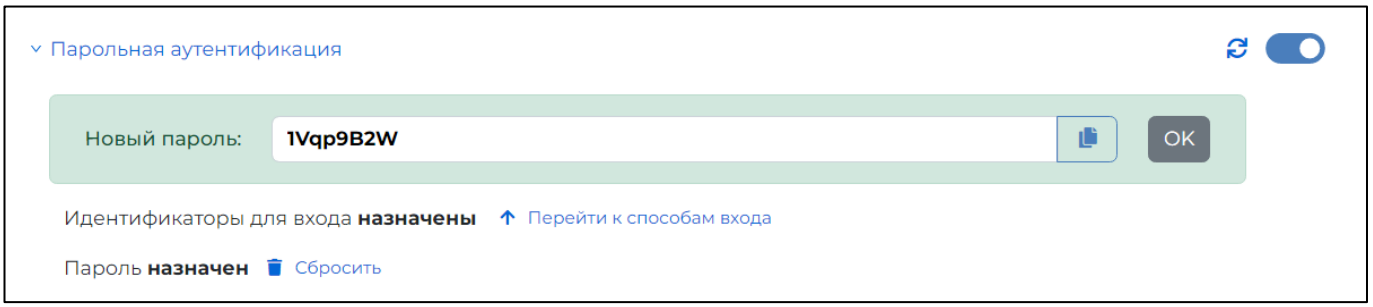

Рисунок 9. - Успешная смена (задание) пароля

3.2.2.2. Настройка вторичной аутентификации

3.2.2.2.1 Настройка аутентификации по SMS

Для настройки вторичной аутентификации Пользователя по SMS следует в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация по SMS*» и нажать кнопку «*Назначить*». Если ранее Пользователю не был указан контактный

номер телефона, то отобразится информация о необходимости добавления контактного номера телефона. Для добавления номера необходимо нажать кнопку «Добавить».

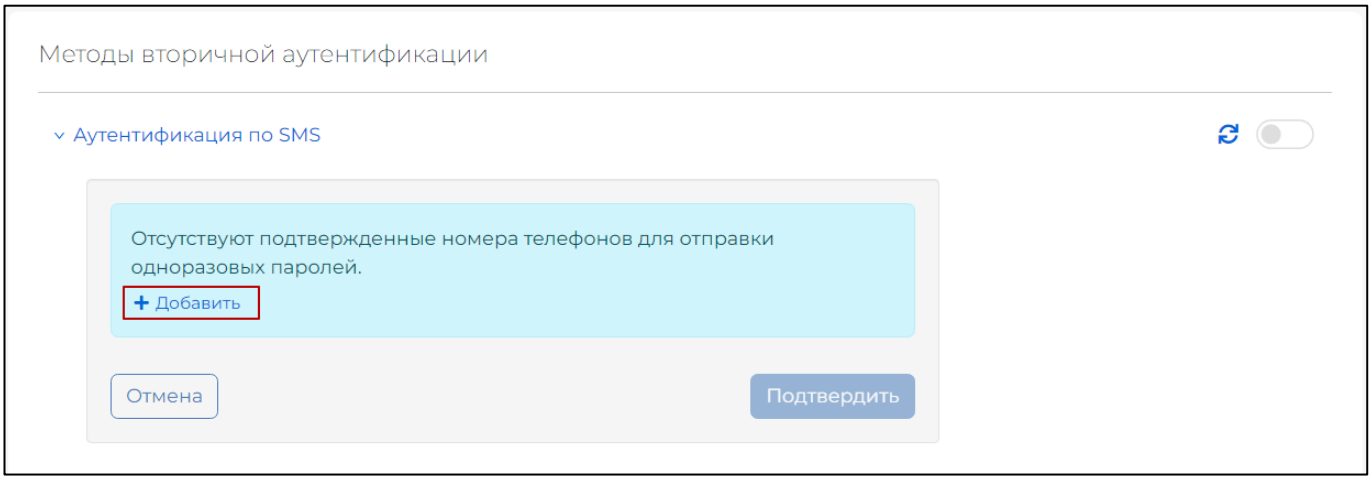

Рисунок 10 - Аутентификация по SMS

После чего Вы будете перенаправлены на страницу «Контакты». Укажите контактный номер телефона и нажмите кнопку «Добавить».

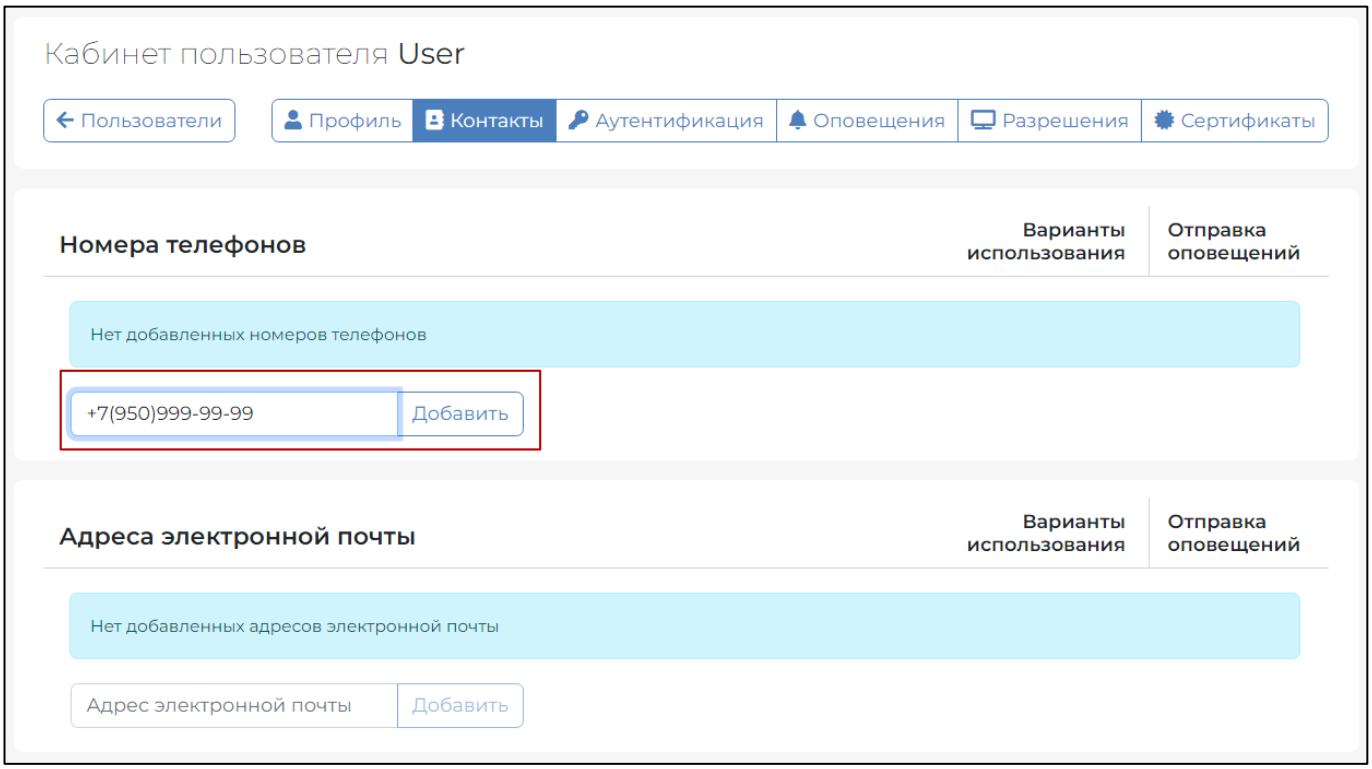

Рисунок 11 – Добавление номера телефона

После успешного добавления номера телефона появится сообщение: «Номер телефона успешно добавлен». Перейдите во вкладку «Аутентификация».

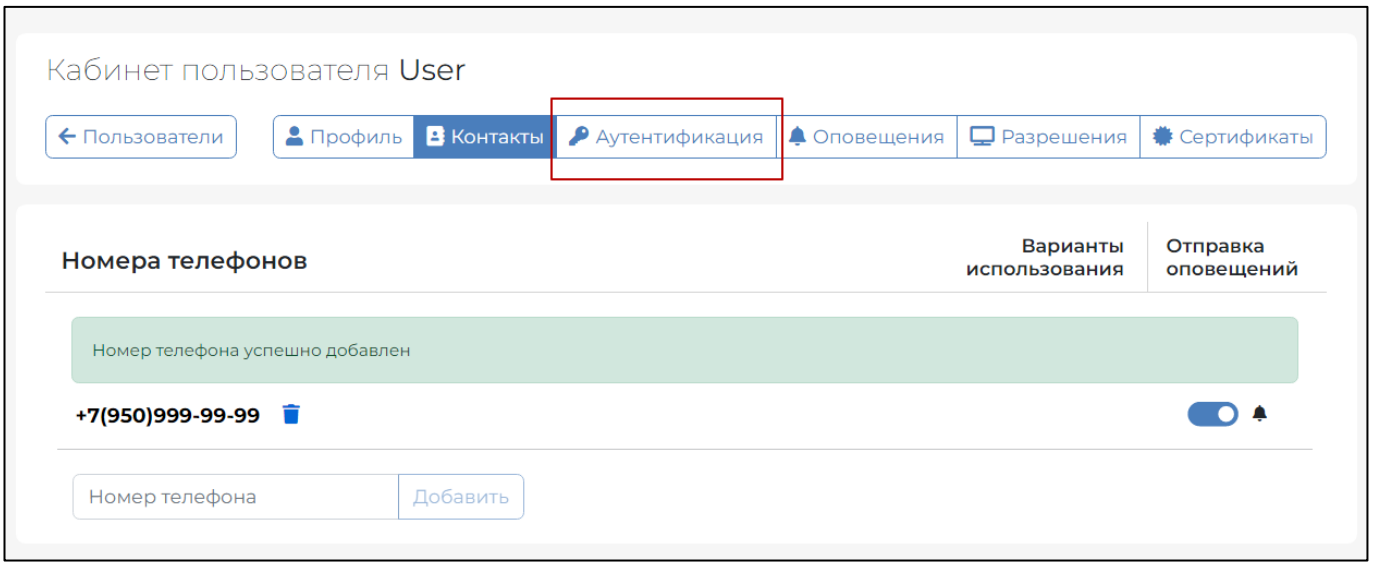

Рисунок 12 – Успешное добавление номера телефона

Раскройте блок «*Аутентификация по SMS*» в «*Методах вторичной аутентификации*» и нажмите кнопку «*Назначить*». Добавленный ранее номер телефона теперь будет доступен для выбора. Для выбора добавленного номера телефона для получения одноразовых паролей нажмите кнопку «Подтвердить».

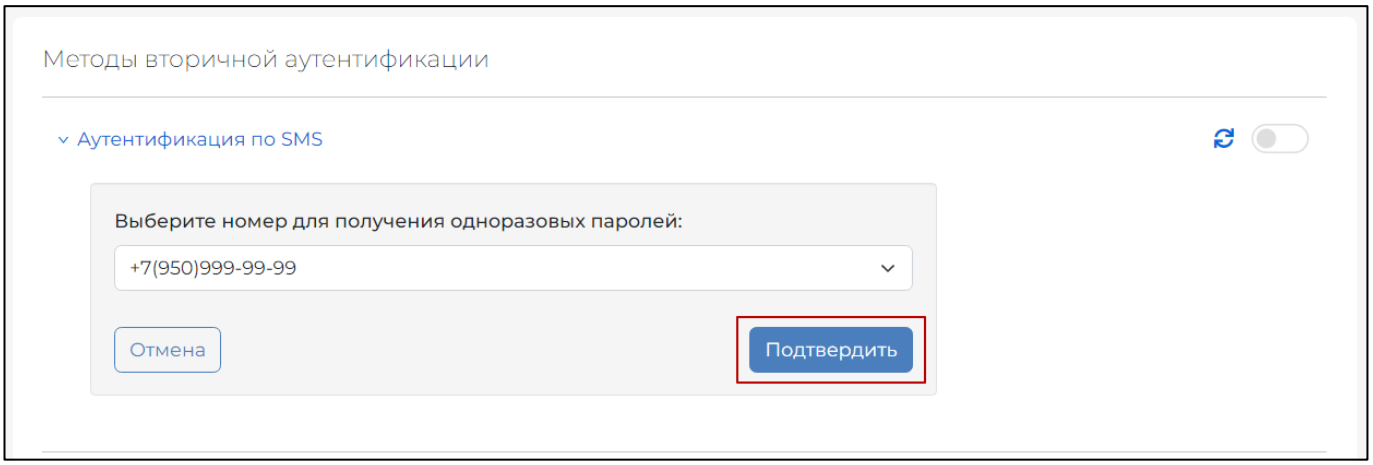

Рисунок 13 – Выбор номера телефона для получения одноразовых паролей

. Для включения вторичной аутентификации по SMS необходимо установить переключатель «*Аутентификация по SMS*» в группе «*Вторичная аутентификация*» в активное положение.

3.2.2.2.2 Настройка аутентификации по протоколу OATH

Для настройки вторичной аутентификации Пользователя по протоколу OATH (токену TOTP/HOTP, например, eToken Pass) нужно в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация по протоколу OATH*» и нажать

ссылку «*Добавить токен*» (см. Рисунок 14. - Настройка аутентификации по протоколу OATH).

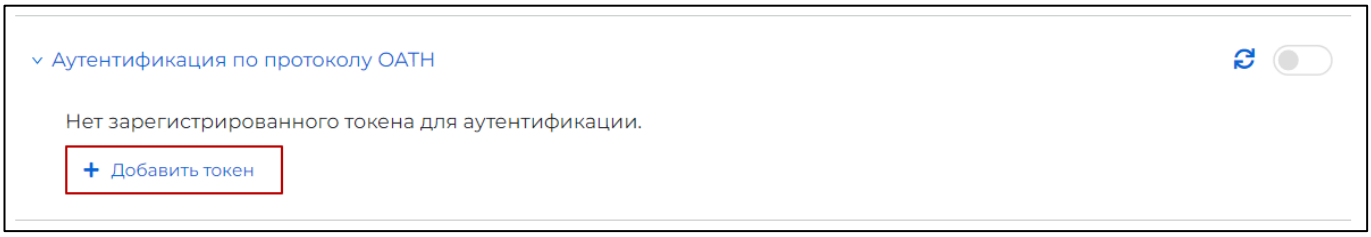

Рисунок 14. - Настройка аутентификации по протоколу OATH

Далее необходимо выбрать способ генерации одноразовых паролей: брелок или мобильное приложение.

1) Брелок

В появившемся поле ввода параметров аутентификации по протоколу OATH следует указать серийный номер OTP-токена, первый и второй пароли OTP, после чего нажать кнопку «*Сохранить*» (см. Рисунок 15. - Ввод параметров аутентификации по протоколу OATH).

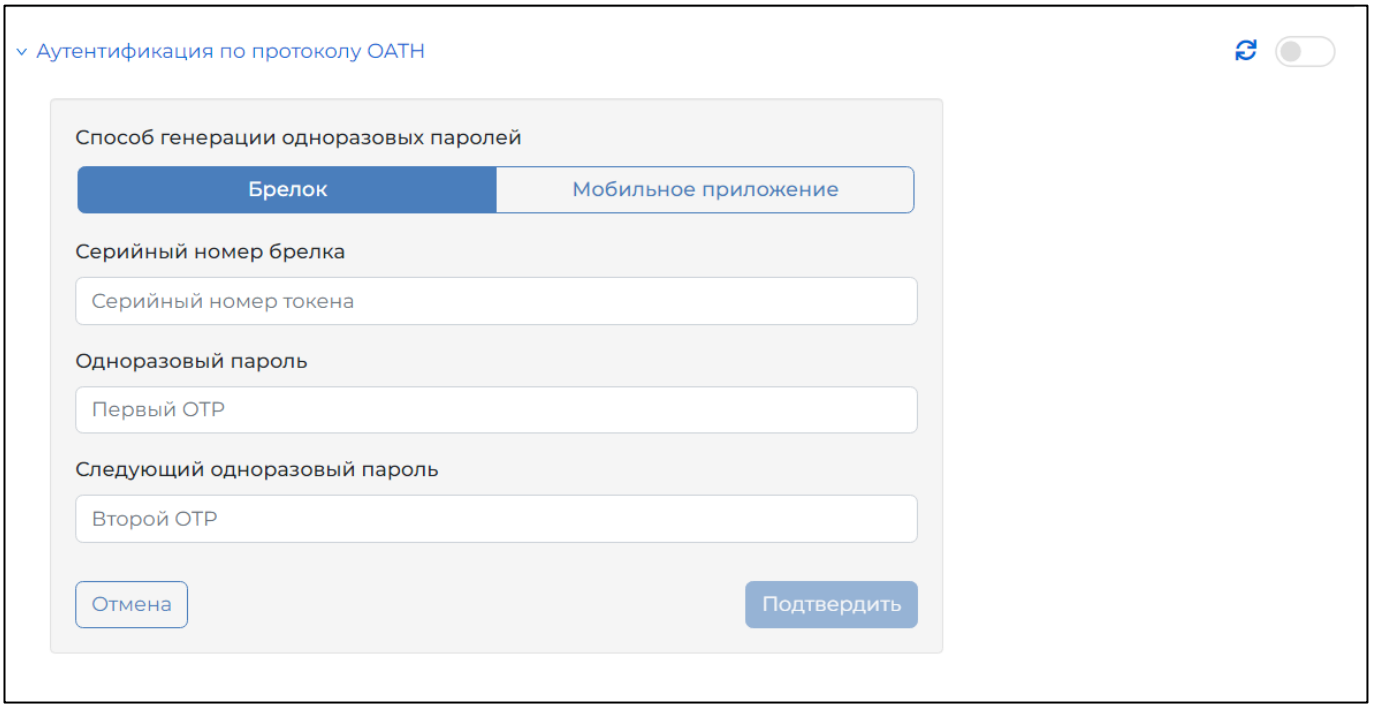

Рисунок 15. - Ввод параметров аутентификации по протоколу OATH

2) Мобильное приложение

Для получения данных инициализации для настройки мобильного приложения нажмите кнопку «*Подтвердить*». Необходимые данные отобразятся на экране.

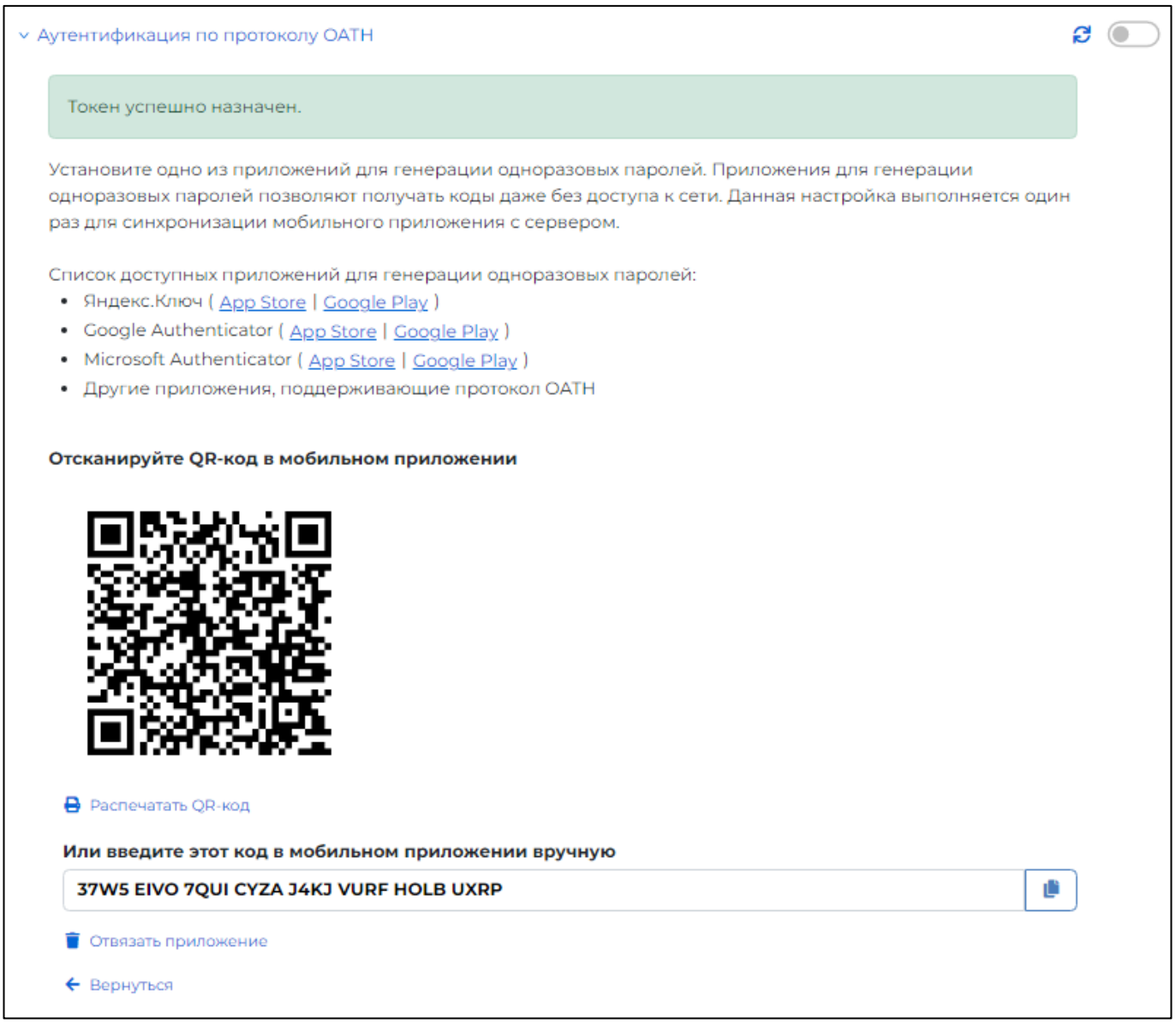

Рисунок 16 – Назначение oath-токена для мобильного приложения

Для включения вторичной аутентификации по протоколу OATH необходимо установить переключатель «*Аутентификация по протоколу OATH*» в группе «*Вторичная аутентификация*» в активное положение.

3.2.2.2.3 Настройка аутентификации по электронной почте

Для настройки вторичной аутентификации Пользователя по электронной почте следует в группе «Методы вторичной аутентификации» раскрыть блок «Аутентификация по электронной почте» и нажать кнопку «*Назначить*». Если ранее Пользователю не был указан контактный номер телефона, то отобразится информация о необходимости добавления контактного номера телефона. Для добавления номера необходимо нажать кнопку «*Добавить*».

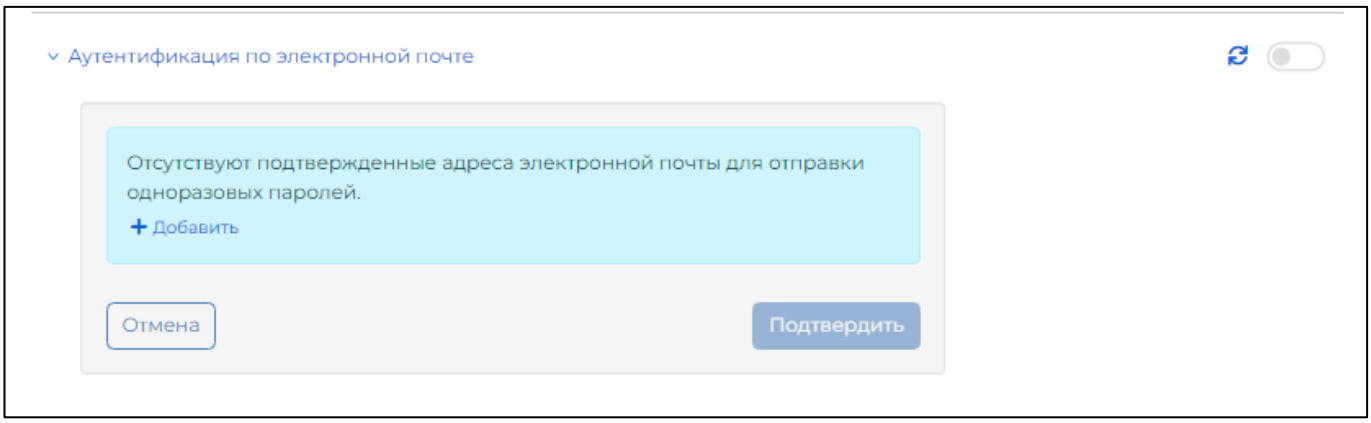

Рисунок 17 - Аутентификация по email

После чего Вы будете перенаправлены на страницу «*Контакты*». Укажите контактный адрес электронной почты и нажмите кнопку «Добавить».

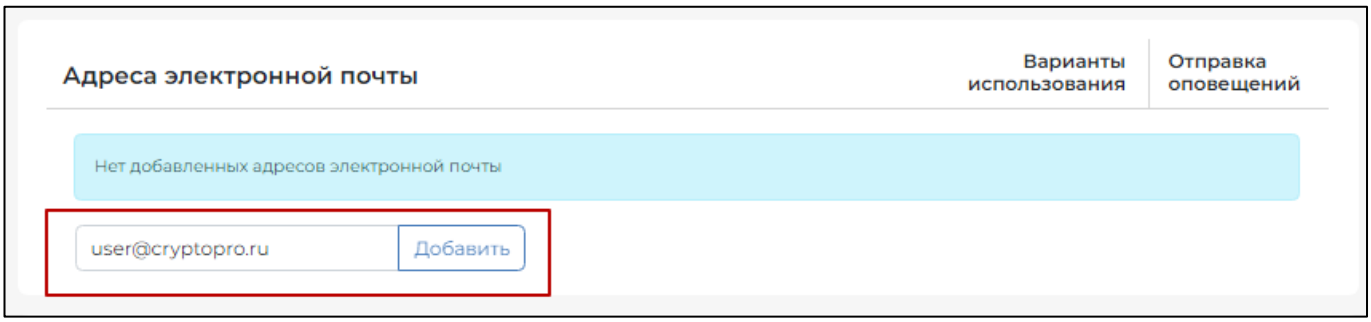

Рисунок 18 – Добавление адреса электронной почты

После успешного добавления адреса электронной почты появится сообщение: «Адрес электронной почты успешно добавлен». Перейдите во вкладку «Аутентификация».

Раскройте блок «*Аутентификация по электронной почте*» в «*Методах вторичной аутентификации*» и нажмите кнопку «*Назначить*». Добавленный ранее адрес электронной почты теперь будет доступен для выбора. Для выбора добавленного адреса электронной почты для получения одноразовых паролей нажмите кнопку «Подтвердить».

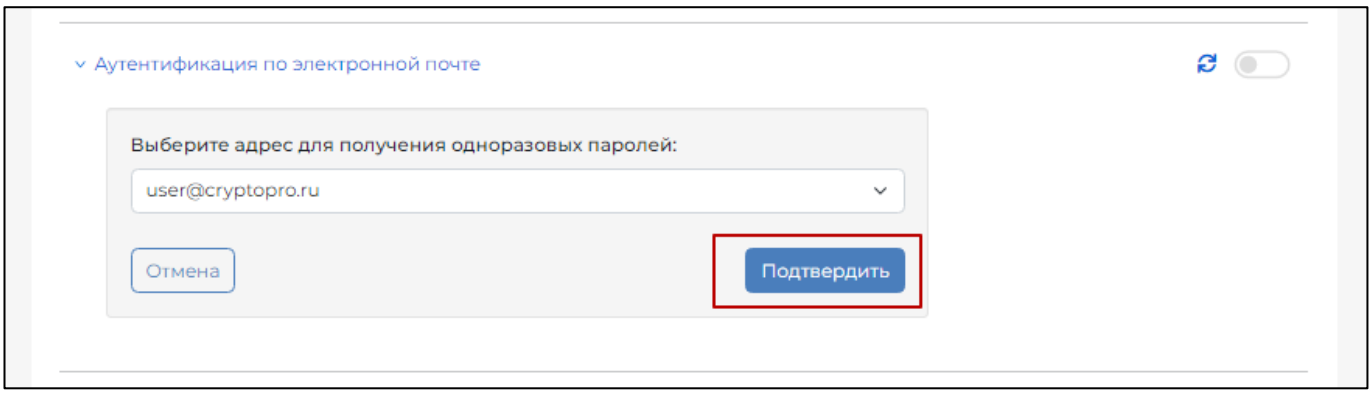

Рисунок 19 – Выбор адреса email для получения одноразовых паролей

. Для включения вторичной аутентификации по SMS необходимо установить переключатель «*Аутентификация по электронной почте*» в группе «*Вторичная аутентификация*» в активное положение.

3.2.2.2.4 Настройка аутентификации с помощью мобильного приложения

Для настройки вторичной аутентификации Пользователя с помощью мобильного приложения «КриптоПро DSSClient» нужно в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация с помощью мобильного приложения*» и нажать кнопку «*Добавить устройство*» (см. Рисунок 20. - Настройка аутентификации с помощью мобильного приложения).

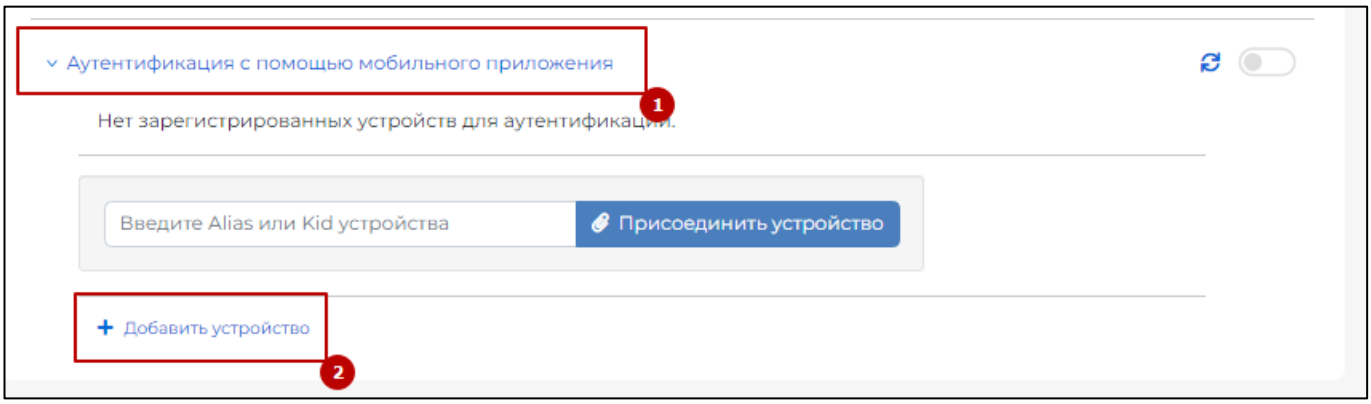

Рисунок 20. - Настройка аутентификации с помощью мобильного приложения

Далее отобразится QR-код, который необходимо отсканировать в мобильном приложении dssclient.

Рисунок 21 – Данные для инициализации устройства

Для включения вторичной аутентификации по мобильному приложению нужно установить переключатель «*Аутентификация по мобильному приложению*» в группе «*Вторичная аутентификация*» в активное положение.

3.2.2.2.5 Настройка подтверждения и доступа к операциям СЭП

После успешной настройки параметров аутентификации Пользователя необходимо определить операции, которые пользователь должен подтверждать выбранным Оператором методом вторичной аутентификации и доступ Пользователя к операциям в СЭП.

Оператор может дать Пользователю доступ к следующим операциям в СЭП:

- Подпись документа.

- Шифрование/расшифрование документа.
- Создание запроса на сертификат.
- Удаление сертификата.
- Обновление сертификата.
- Отзыв сертификата.
- Приостановление действия сертификата.
- Возобновление действия сертификата.
- Смена ПИН-кода закрытого ключа.

Оператор может установить подтверждение Пользователем методом выбранной вторичной аутентификации следующих операций в СЭП:

- Выпуск маркера (вход в ЦИ).
- Подпись документа.
- Шифрование/Расшифрование документа.
- Создание запроса на сертификат.
- Смена ПИН-кода закрытого ключа.
- Обновление сертификата.
- Отзыв сертификата.
- Приостановление действия сертификата.
- Возобновление действия сертификата.
- Удаление сертификата.
- Доступ к закрытому ключу.

Подтверждение и доступ Пользователя к операциям в СЭП настраиваются в параметрах настройки аутентификации Пользователя (см. Рисунок 22 – Настройка подтверждения операций Пользователям и Рисунок 23. - Настройка доступа Пользователя к операциям СЭП).

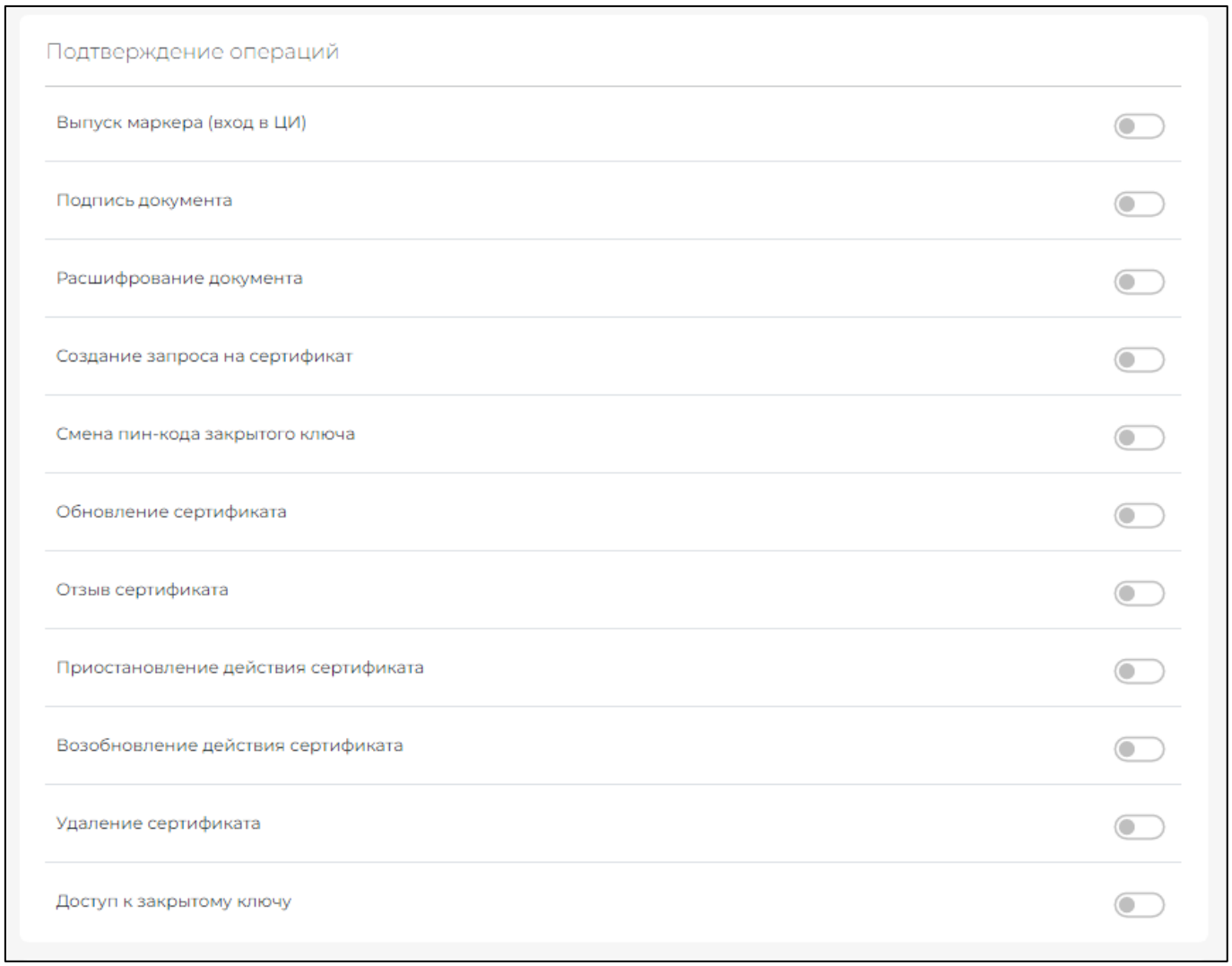

Рисунок 22 – Настройка подтверждения операций Пользователям

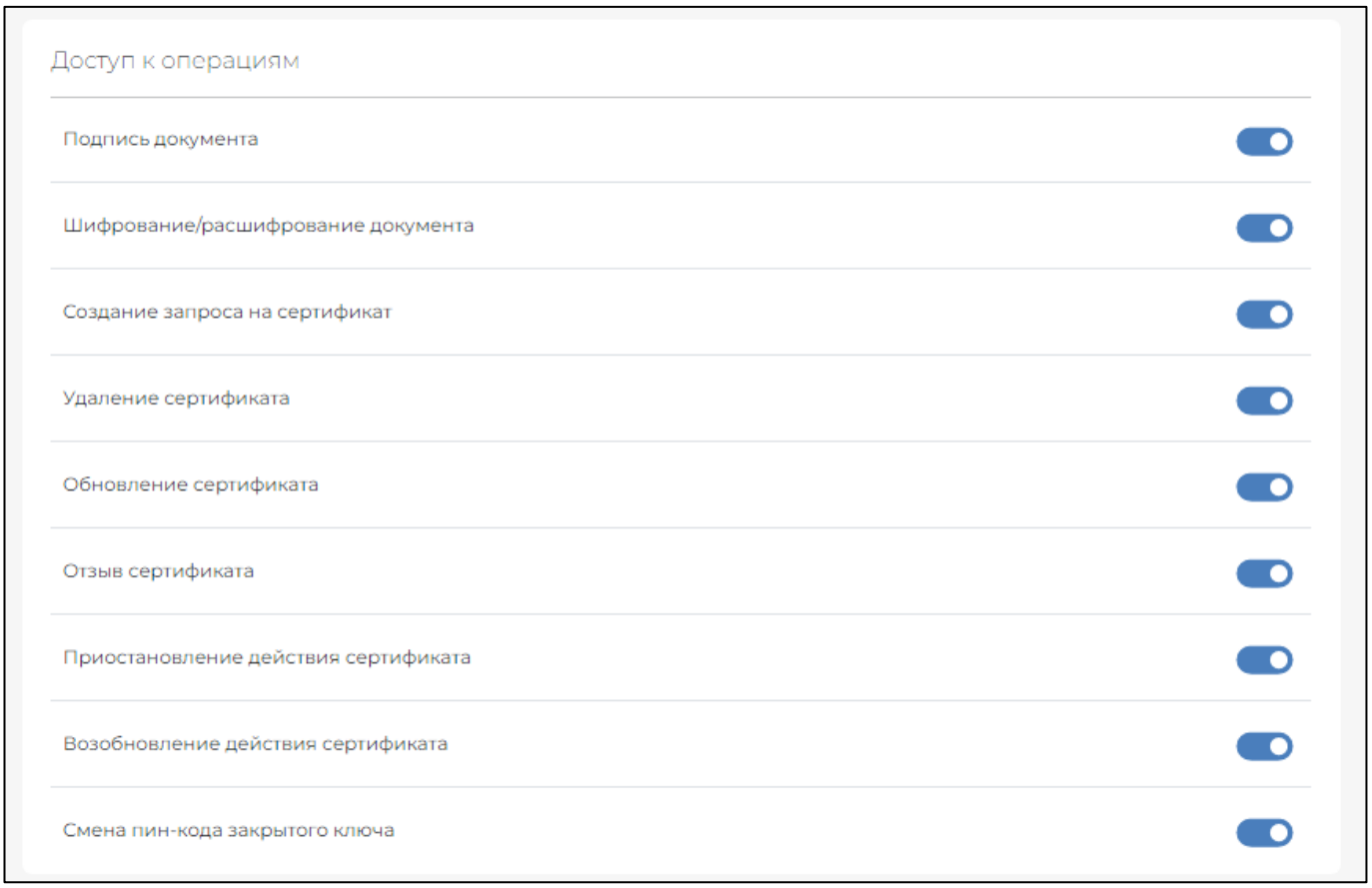

Рисунок 23. - Настройка доступа Пользователя к операциям СЭП

3.2.3. *Блокировка или разблокировка Пользователя*

Для блокировки, либо разблокировки Пользователя нужно в профиле Пользователя нажать кнопку «*Заблокировать пользователя*». При успешной блокировке (разблокировке) Пользователя значок «*Заблокировать*» меняется соответственно на изображение открытого (закрытого) замка.

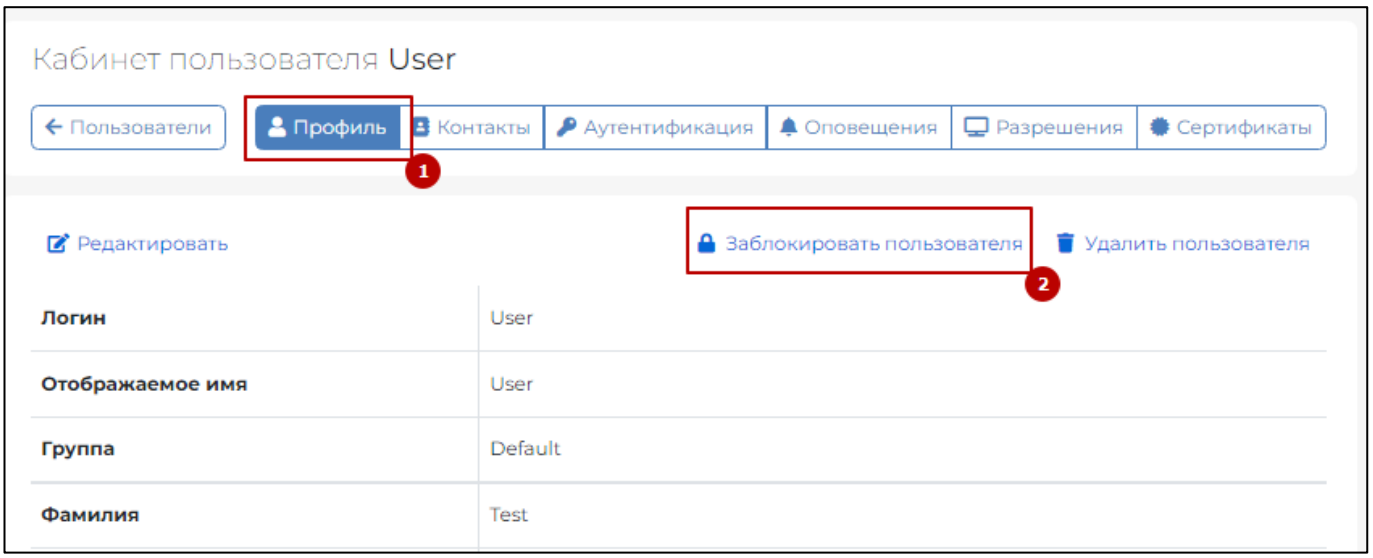

Рисунок 24 – блокировка Пользователя

3.2.4. *Удаление Пользователя*

Для удаления Пользователя необходимо нажать в профиле Пользователя на кнопку «*Удалить пользователя*», далее утвердительно ответить на запрос об удалении Пользователя (см. Рисунок 25. Удаление Пользователя).

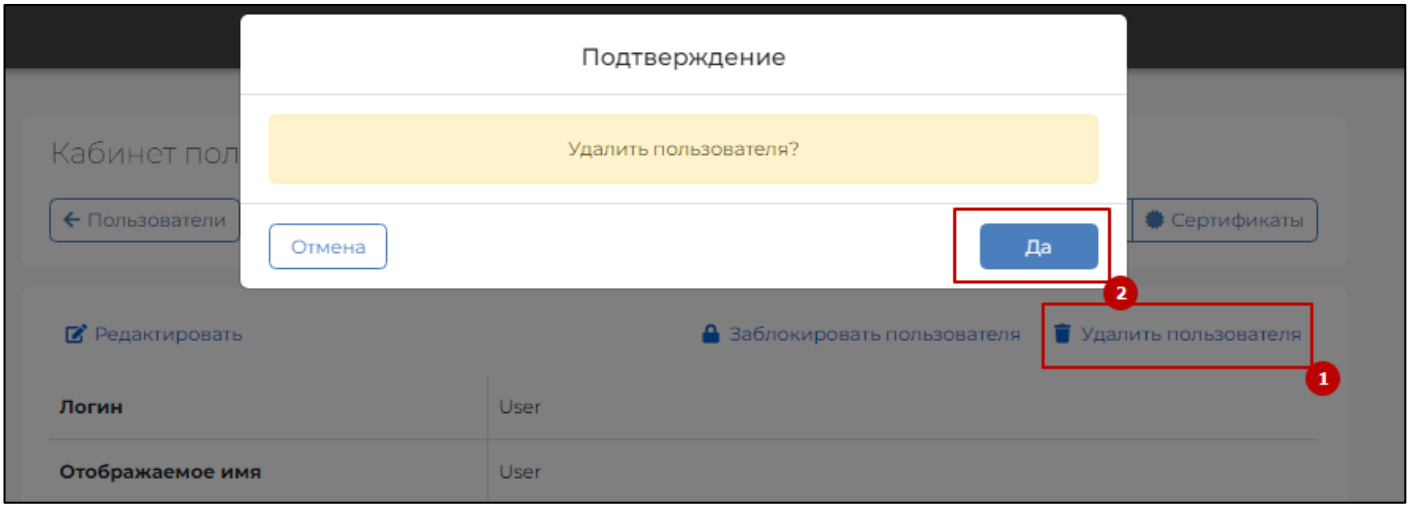

Рисунок 25. Удаление Пользователя

3.2.5. *Управление сертификатами Пользователя*

Для управления сертификатами Пользователя нужно нажать на значок «*Сертификаты*». Оператору доступны следующие операции с сертификатами Пользователя:

- «*Удалить все*» – удаление всех сертификатов Пользователя, зарегистрированных в СЭП.
- «*Создание запроса на сертификат*» – создание запроса на новый сертификат Пользователя.
- «*Загрузить новый сертификат*» – установка сертификата Пользователя, не зарегистрированного в СЭП.
- Управление существующим сертификатом Пользователя в СЭП.

3.2.5.1. Удаление всех сертификатов Пользователя, зарегистрированных в СЭП

Для удаления всех зарегистрированных в СЭП сертификатов Пользователя нужно нажать кнопку «*Удалить все*», далее подтвердить удаление нажатием кнопки «*Да*» (см. Рисунок 26. Удаление всех сертификатов Пользователя).

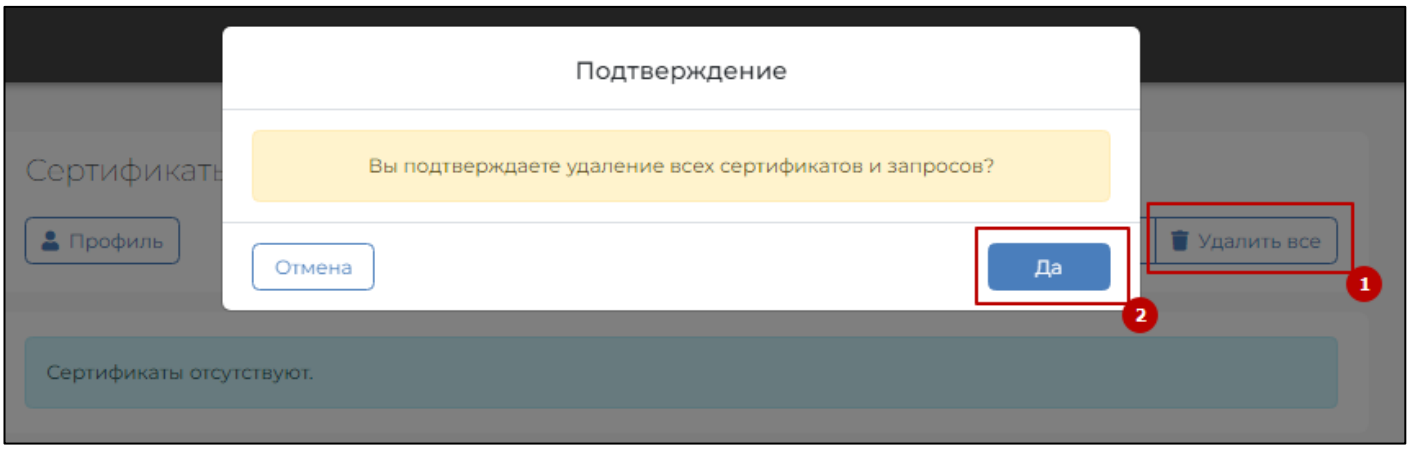

Рисунок 26. Удаление всех сертификатов Пользователя

3.2.5.2. Создание запроса на сертификат Пользователя

Для создания запроса на сертификат Пользователя нужно нажать кнопку «*Создать запрос на сертификат*» (см. Рисунок 27. Создание запроса на сертификат Пользователя).

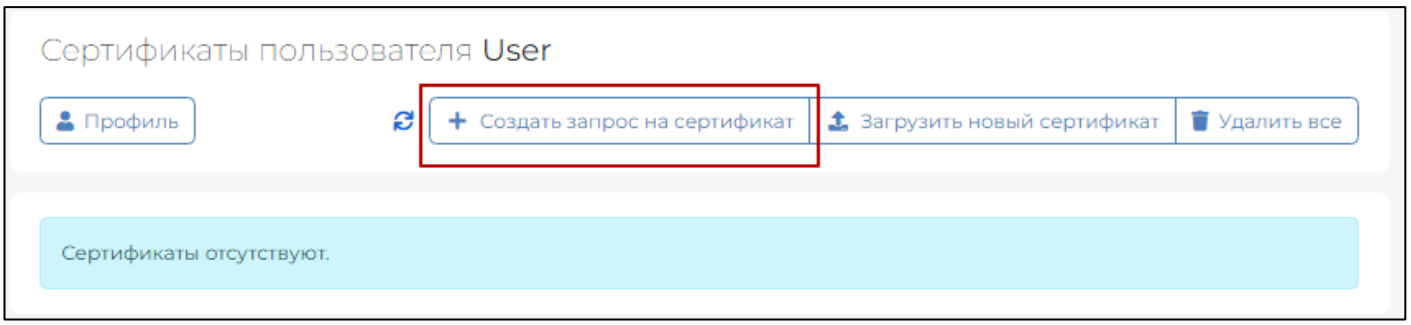

Рисунок 27. Создание запроса на сертификат Пользователя

Далее нужно задать Удостоверяющий центр, к которому будет направлен запрос на сертификат, отредактировать атрибуты Пользователя, выбрать шаблон сертификата (по умолчанию «*Пользователь 6 месяцев*») и нажать кнопку «*Создать запрос*» (см. **Ошибка! Источник ссылки не найден.**).

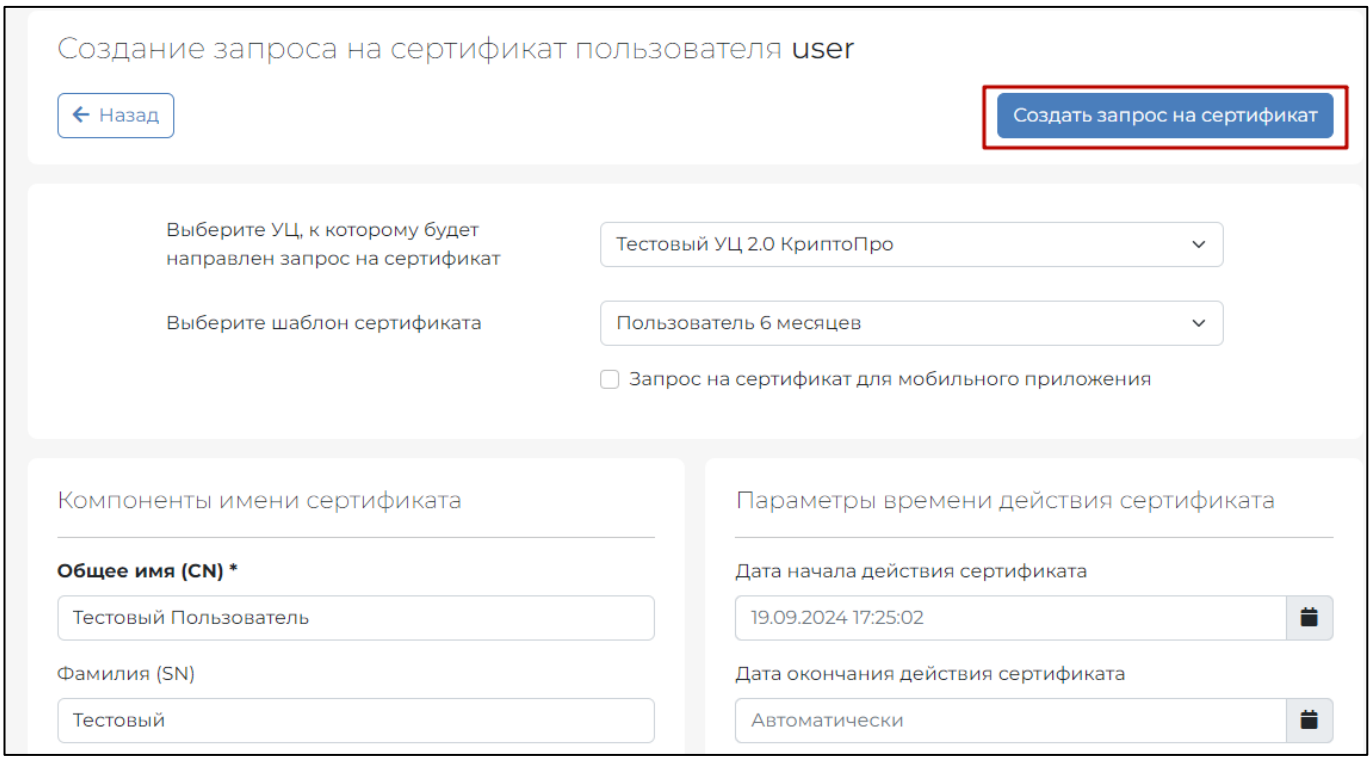

Рисунок 28 – Создание запроса на сертификат

После нажатия кнопки «*Создать запрос на сертификат*» в случае успешной обработки запроса появится окно с информацией о сертификате (см. Рисунок 29 – Информация о сертификате).

Рисунок 29 – Информация о сертификате

Управление выпущенным сертификатом описано в пункте *Управление существующим сертификатом Пользователя в СЭП*.

3.2.5.3. Установка сертификата, не зарегистрированного в СЭП

Для установки в СЭП существующего сертификата из контейнера PFX нужно на странице «*Сертификаты*» нажать кнопку «*Загрузить новый сертификат*» (см. Рисунок 30. - Установка сертификата).

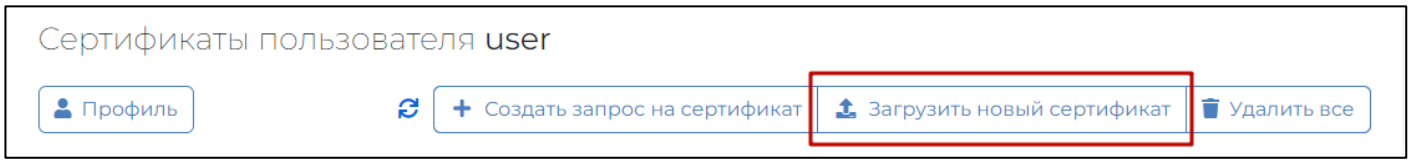

Рисунок 30. - Установка сертификата

В открывшемся диалоговом окне следует нажать копку «*Выберите файл*» и указать путь до файла с расширением PFX, после чего нажать кнопку «*Открыть*» (см. Рисунок 31. - Выбор файла PFX для импорта сертификата).

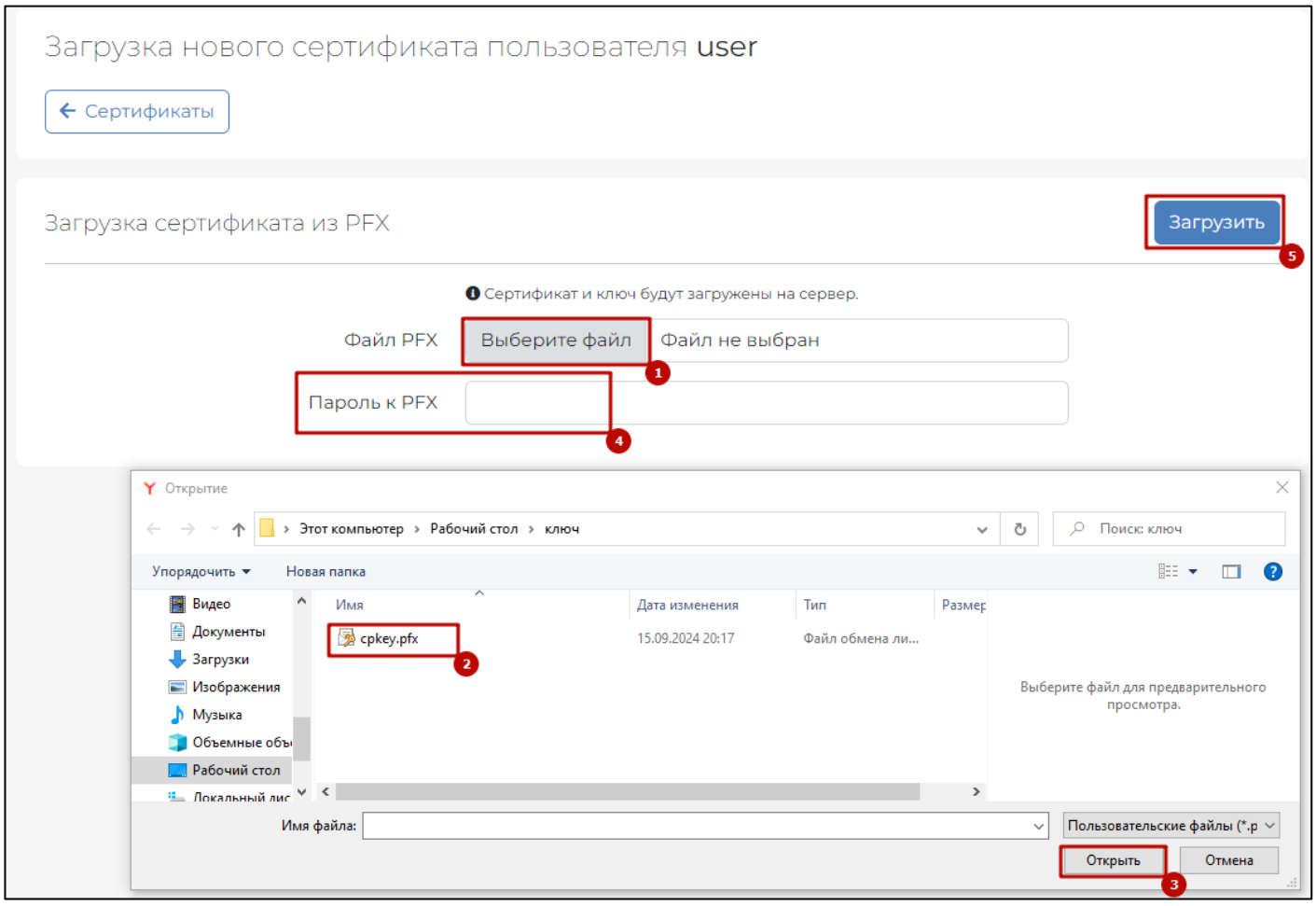

Рисунок 31. - Выбор файла PFX для импорта сертификата

Далее в интерфейсе следует ввести пин-код нажать кнопку «*Загрузить*».

После этого появится информация, что «Сертификат успешно установлен» и кнопка «Перейти к сертификату» (см. Рисунок 32 – Успешная загрузка сертификата).

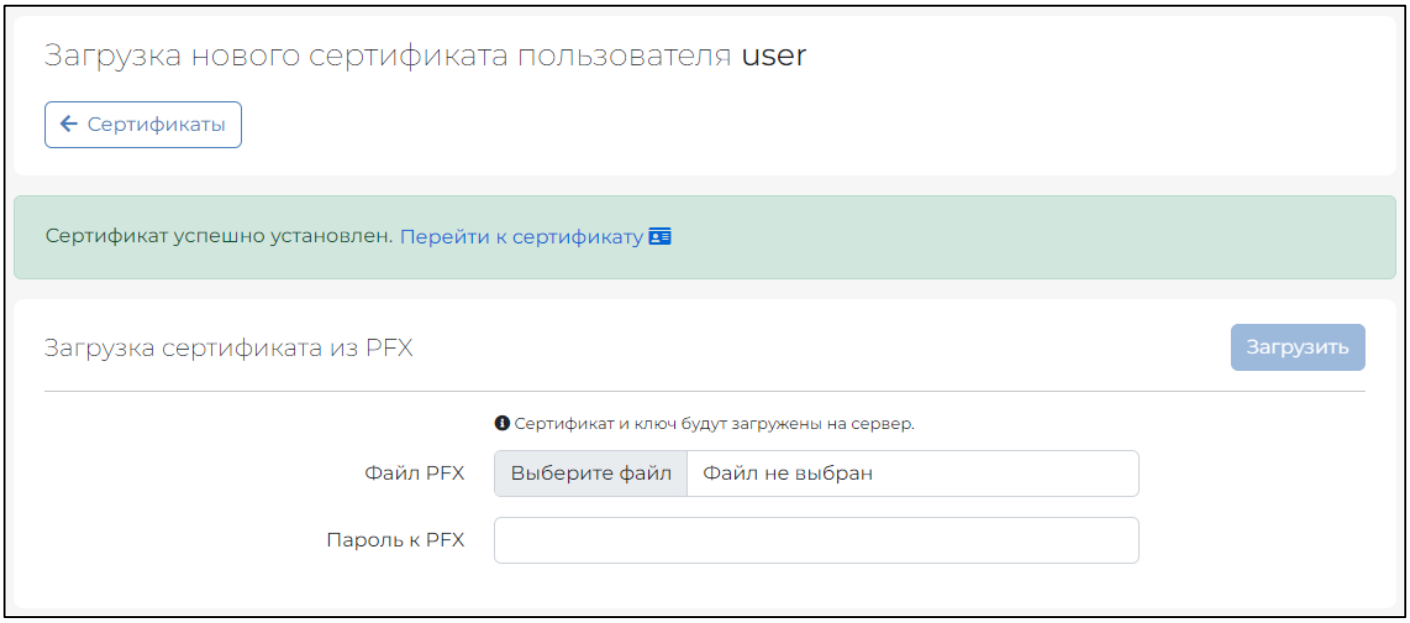

Рисунок 32 – Успешная загрузка сертификата

3.2.5.4. Управление существующим сертификатом Пользователя в СЭП

Для управления существующим сертификатом Пользователя в нужно перейти в сертификаты кнопку «*Просмотр*» в соответствующей строке раздела «*Сертификаты*» и выполнить необходимое действие с нужным сертификатом из списка (см. Рисунок 33. - Управление сертификатом).

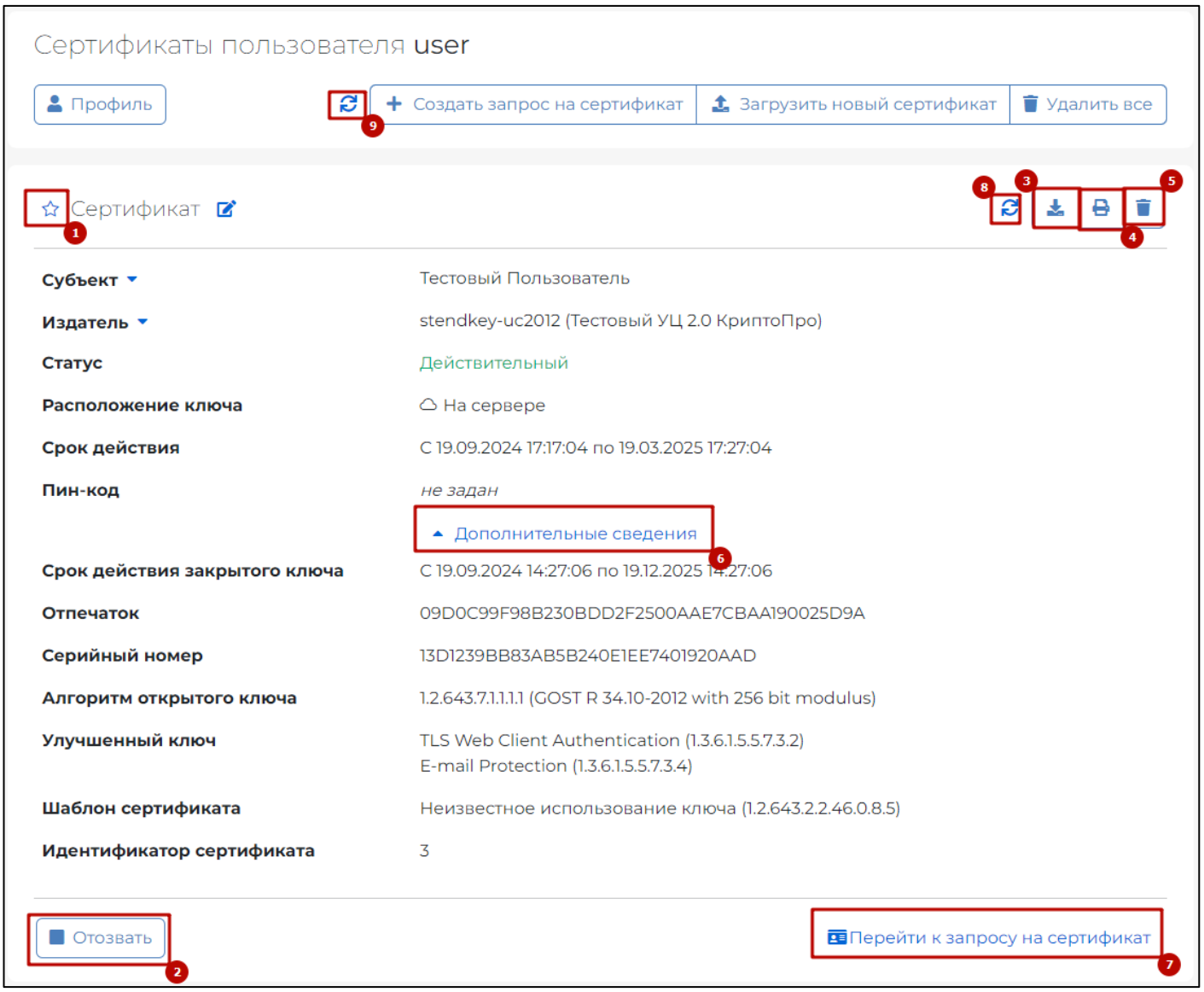

Рисунок 33. - Управление сертификатом

Оператору доступны следующие операции управления сертификатом (см. Рисунок 33. - Управление сертификатом):

1) «*Назначить сертификатом по умолчанию*» – выбрать данный сертификат по умолчанию из всех сертификатов Пользователя.
2) «*Отозвать*» – отозвать сертификат (надо будет указать ПИН-код к ключевому контейнеру в СЭП, причину отзыва, дату отзыва).
3) «*Скачать*» – скачать файл сертификата (*.cer).
4) «*Печать*» – вывести бумажную копию сертификата на печать.
5) «*Удалить*» – удалить сертификат из СЭП.
6) «*Дополнительные сведения*» - просмотр дополнительных сведений о сертификате:
    - Срок действия закрытого ключа

- Отпечаток
- Серийный номер
- Алгоритм открытого ключа
- Улучшенный ключ
- Шаблон сертификата
- Идентификатор сертификата

7) *«Перейти к запросу на сертификат»* - открыть информацию о запросе на сертификат.

Из-за особенности работы браузера иногда необходимо обновить информацию о сертификате с сервера Ключа – для этого необходимо нажать стрелочки (8 и 9 на рис. Рисунок 33. - Управление сертификатом*)*

4. Раздел «Средства аутентификации»

Раздел позволяет просматривать перечень назначенных Пользователям средств аутентификации (см. Рисунок 34. - Перечень средств аутентификации).

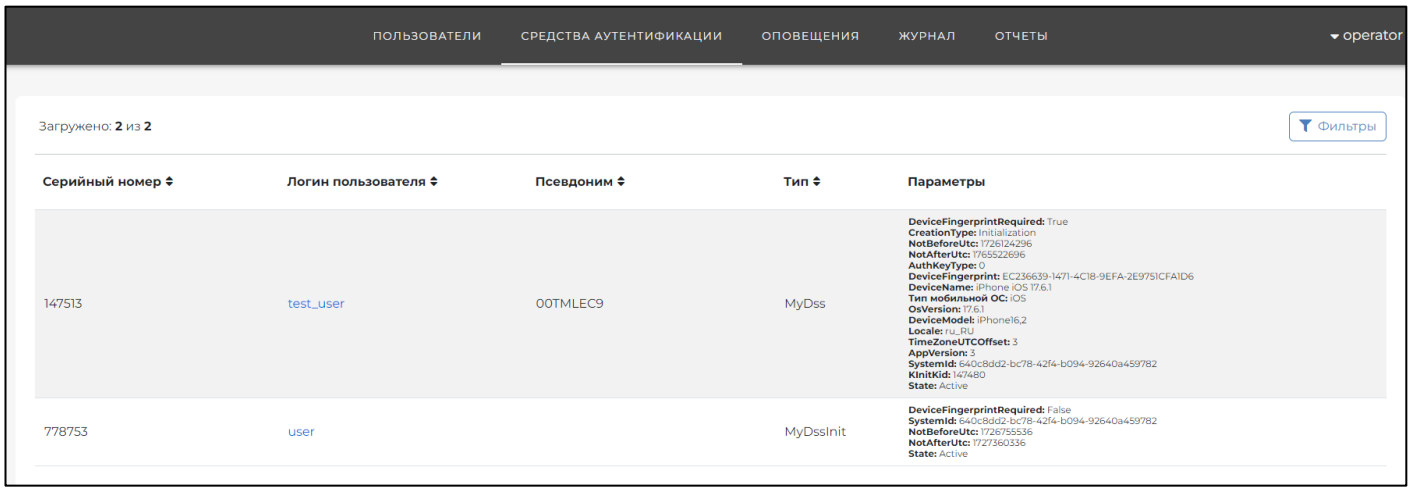

Рисунок 34. - Перечень средств аутентификации

5. Раздел «Оповещения»

Раздел позволяет управлять Оповещениями Оператора. Доступные способы получения уведомлений для оператора:

1) SMS
2) email

6. Раздел «Журнал»

Раздел «Журнал» предназначен для отображения журнала событий, связанных с действиями Пользователей и Операторов в СЭП с возможностью фильтрации по типам событий.

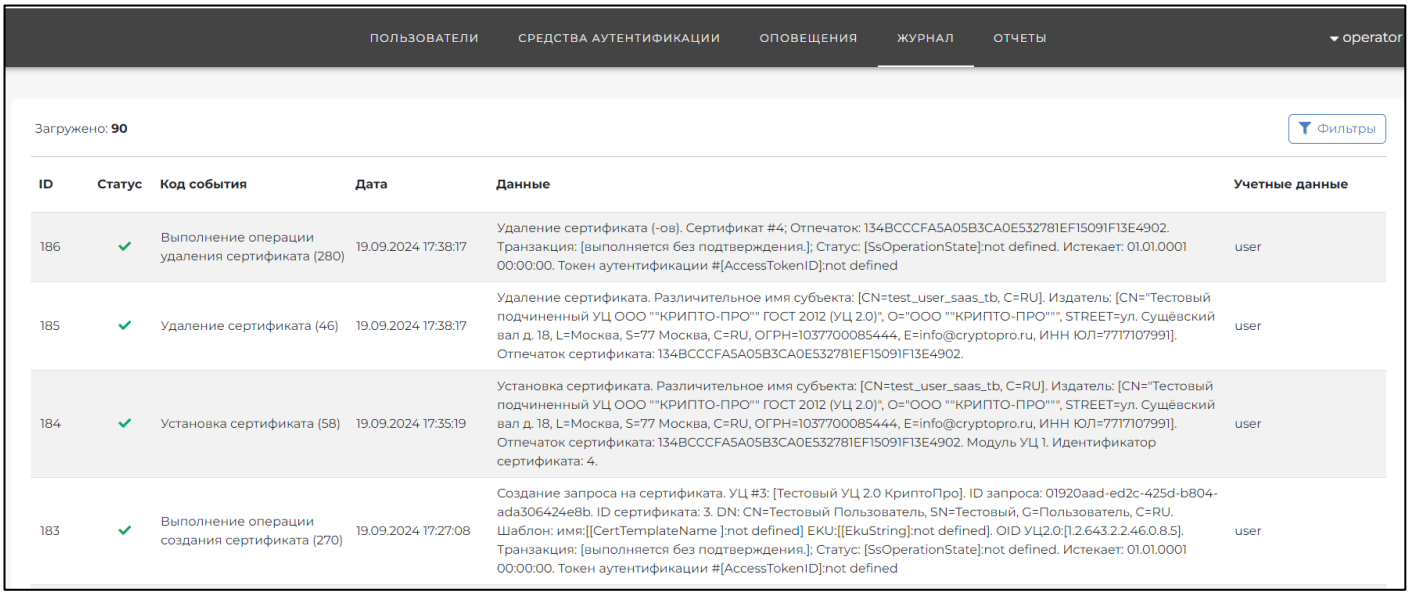

Рисунок 35. - Аудит событий СЭП

7. Раздел «Отчеты»

Раздел «Отчеты» предназначен для создания отчетов. Типы отчетов настраиваются Администратором.

Перечень рисунков