

ПАК «КриптоПро **DSS**»

СЕРВИС ЭЛЕКТРОННОЙ ПОДПИСИ

Инструкция Оператора Удостоверяющего центра

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Операторов Удостоверяющего центра ООО «КРИПТО-ПРО» на базе ПАКМ "КриптоПро HSM" (далее – СЭП) и определяет порядок использования Веб-интерфейса СЭП для осуществления операций по доступу и управлению сертификатами ключей проверки электронной подписи, созданию и проверке электронной подписи, шифрованию и расшифрованию электронных документов.

Информация о разработчике ПАКМ "КриптоПро HSM":

ООО «КРИПТО-ПРО»

127018, Москва, ул. Суцневский вал, 18

Телефон: (495) 995 4820

<http://www.CryptoPro.ru>

<https://saas.cryptopro.ru/Instanceidp/Users>

E-mail: info@CryptoPro.ru

Оглавление

Аннотация	2
Информация о разработчике ПАКМ "КриптоПро HSM":	2
1. Общие положения.....	4
1.1. Требования и подготовка рабочего места Оператора	4
1.1.1. Настройка Internet Explorer.....	4
1.1.2. Настройка Яндекс-браузера	5
2. Структура меню.....	7
3. Раздел «Пользователи»	9
3.1. Создание нового Пользователя	9
3.2. Управление существующими Пользователями	9
3.2.1. Редактирование атрибутов Пользователя.....	11
3.2.2. Настройка параметров аутентификации Пользователя.....	11
3.2.2.1. Настройка первичной аутентификации	12
3.2.2.1.1 Настройка аутентификации по сертификату.....	12
3.2.2.1.2 Настройка аутентификации по паролю	13
3.2.2.2. Настройка вторичной аутентификации	14
3.2.2.2.1 Настройка аутентификации по SMS	14
3.2.2.2.2 Настройка аутентификации по протоколу OATH	16
3.2.2.2.3 Настройка аутентификации по электронной почте	18
3.2.2.2.4 Настройка аутентификации с помощью мобильного приложения	19
3.2.2.3. Настройка подтверждения и доступа к операциям СЭП	24
3.2.3. Блокировка или разблокировка Пользователя	27
3.2.4. Удаление Пользователя.....	27
3.2.5. Управление сертификатами Пользователя.....	27
3.2.5.1. Удаление всех сертификатов Пользователя, зарегистрированных в СЭП	28
3.2.5.2. Создание запроса на сертификат Пользователя.....	28
3.2.5.2.1. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)	28
3.2.5.2.2. Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)	29
3.2.5.3. Управление существующим сертификатом Пользователя в СЭП	31
4. Раздел «Личный кабинет»	32
5. Раздел «Оповещения оператора».....	33
6. Раздел «Средства аутентификации»	33
7. Раздел «Аудит».....	34
Перечень рисунков	35

1. Общие положения

Сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПАКМ "КриптоПро HSM" версии 2.0 (далее – СЭП) предназначен для создания и хранения ключей электронной подписи, выполнения операций по созданию и проверке электронной подписи различного формата криптографических сообщений, шифрования и расшифрования электронных документов.

Настоящая инструкция определяет порядок действия Оператора УЦ (далее – Оператор) при выполнении операций формирования, усовершенствования и проверки электронной подписи, шифрования и расшифрования электронных документов.

1.1. Требования и подготовка рабочего места Оператора

На рабочем месте Оператора под управлением MS Windows 7 или выше, macOS версии 10.10 и выше, *Unix-системы (совместимые ОС см. формуляр СКЗИ Криптопро CSP ЖТЯИ.00087-03 30 01) должен быть установлен СКЗИ «КриптоПро CSP» версии 4.0 или выше. Для подключения к СЭП необходимо использовать Интернет-браузер с поддержкой ГОСТ-TLS: Яндекс-браузер, Chromium-GOST, Internet Explorer. Для использования модуля Cloud необходимо установить СКЗИ «КриптоПро CSP» версии 5.0.

1.1.1. Настройка Internet Explorer

Для корректной работы с СЭП необходимо добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выбрать вкладку «**Безопасность**», в список надежных сайтов добавить узел <https://saas.cryptopro.ru/> и сохранить изменения свойств (см. Рисунок 1 – Добавление сайта в зону надежных сайтов).

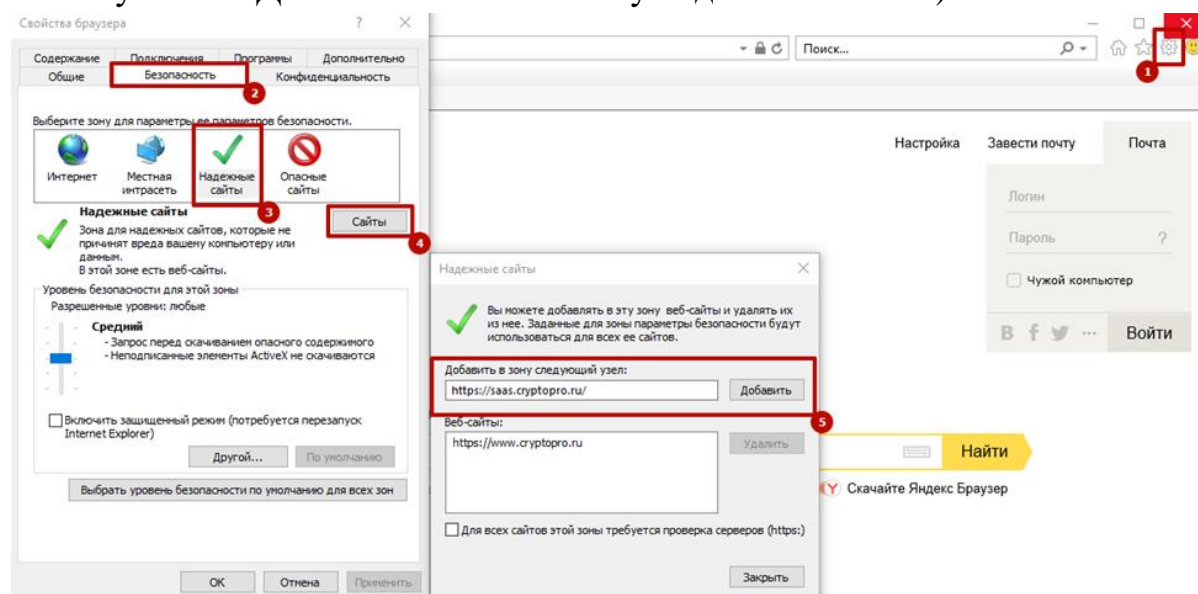


Рисунок 1 – Добавление сайта в зону надежных сайтов

В разделе "**Элементы ActiveX и модуль подключения**" проверить состояние настройки "**Использование элементов управления ActiveX, не помеченных как**

безопасные для использования" - должно быть **"Включить"** (см. Рисунок 2 – Включение ActiveX). Для этого зайти в Internet Explorer меню **«Сервис» - «Свойства обозревателя» - «Безопасность»** - для зоны **"Надежные узлы"** нажать кнопку **"Другой"**.

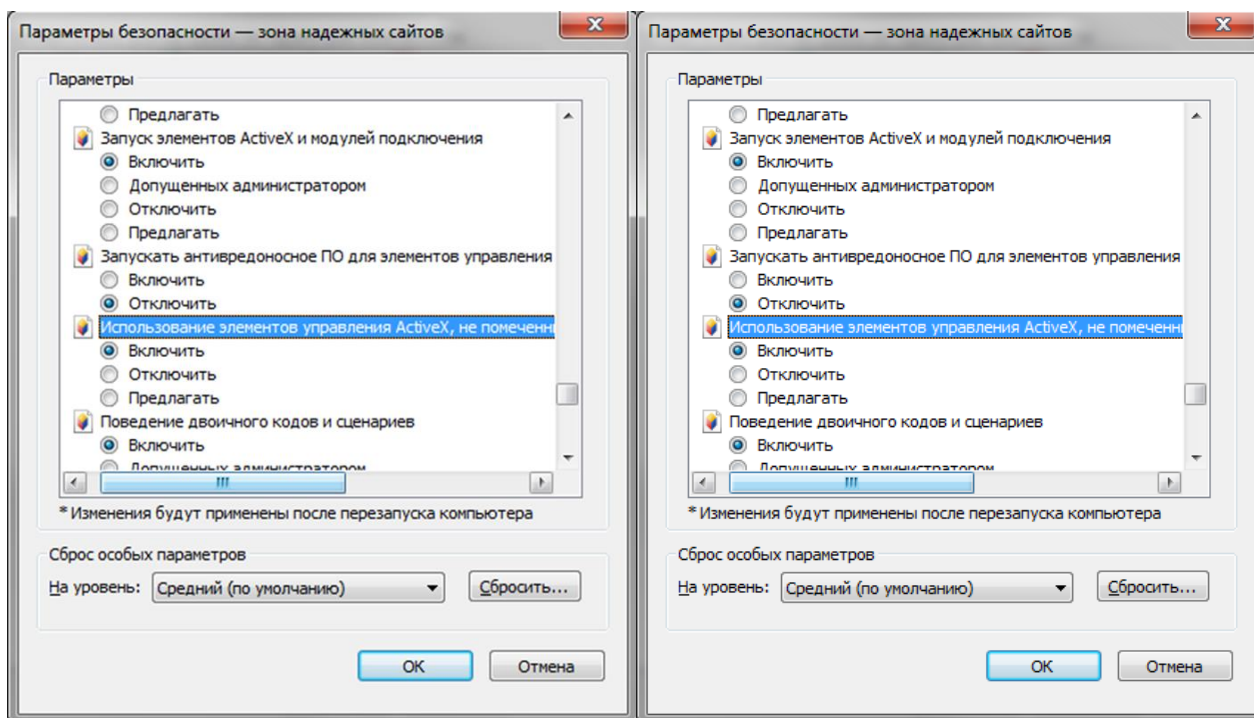


Рисунок 2 – Включение ActiveX

1.1.2. Настройка Яндекс-браузера

Перейдите в **«Настройки» - «Системные»**.

Убедитесь, что в разделе **«Сеть»** включена опция **«Подключаться к сайтам, использующим шифрование по ГОСТ. Требуется КриптоПро CSP»**.

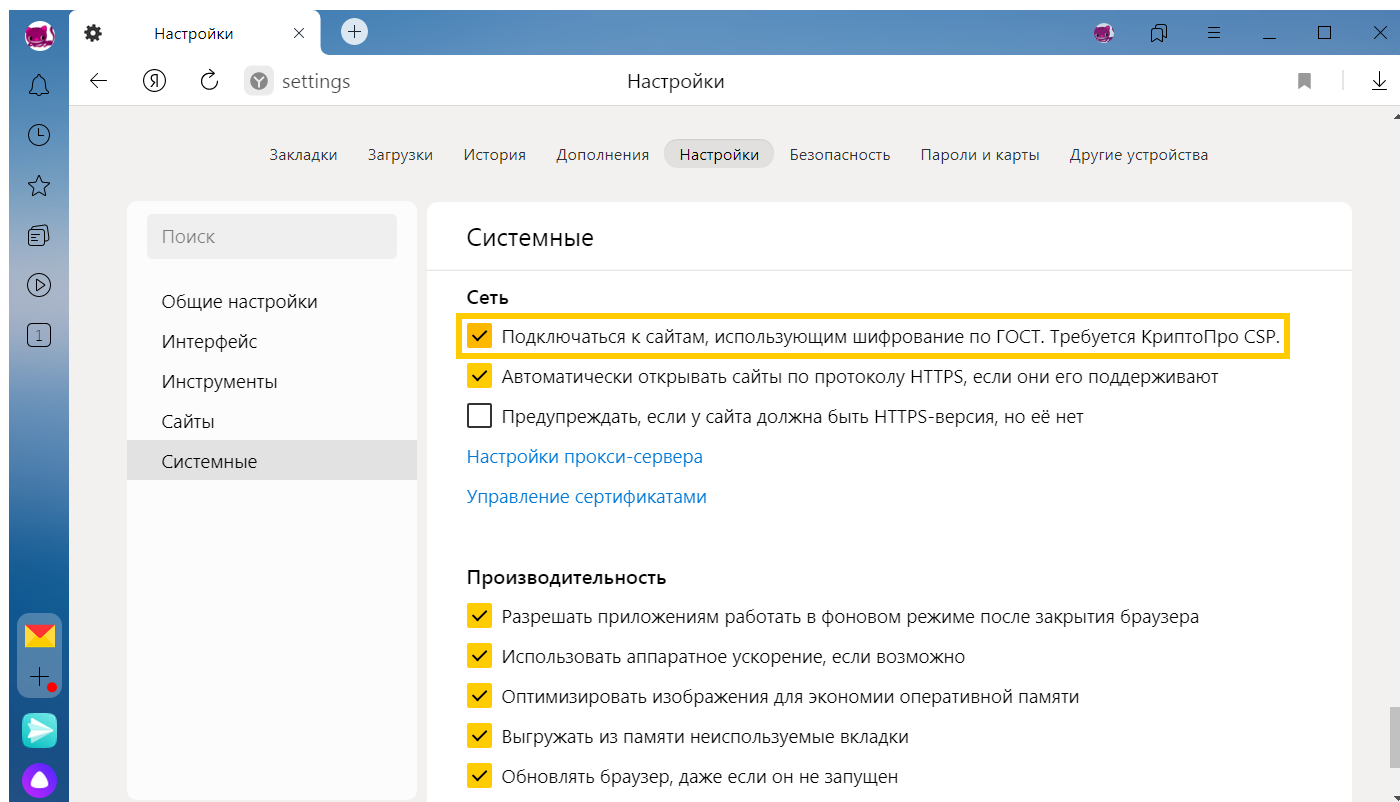


Рисунок 3 – Включение поддержки ГОСТ

2. Структура меню

Для работы в СЭП Оператору необходимо осуществить вход в веб-интерфейс Оператора по адресу <https://saas.cryptopro.ru/InstanceIDP/admins/>¹ (Адрес передается после создания экземпляра и подключения Оператора) и выбрать пункт «Вход по сертификату» (см. Рисунок 4 - Аутентификация Оператора), после чего в появившемся окне подтверждения сертификата выбрать сертификат Оператора и нажать кнопку «ОК».

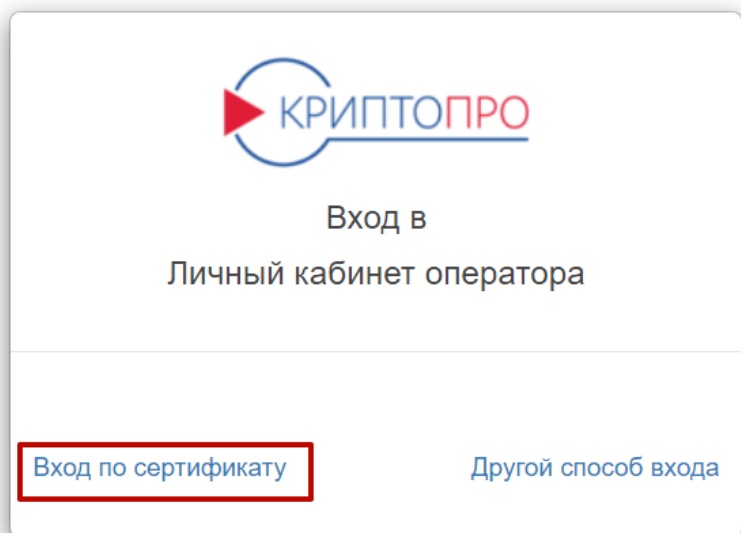


Рисунок 4 - Аутентификация Оператора

После выбора сертификата и ввода ПИН-кода ключевого контейнера будет отображена начальная страница веб-интерфейса Оператора (см. Рисунок 5 - Начальная страница веб-интерфейса Оператора).

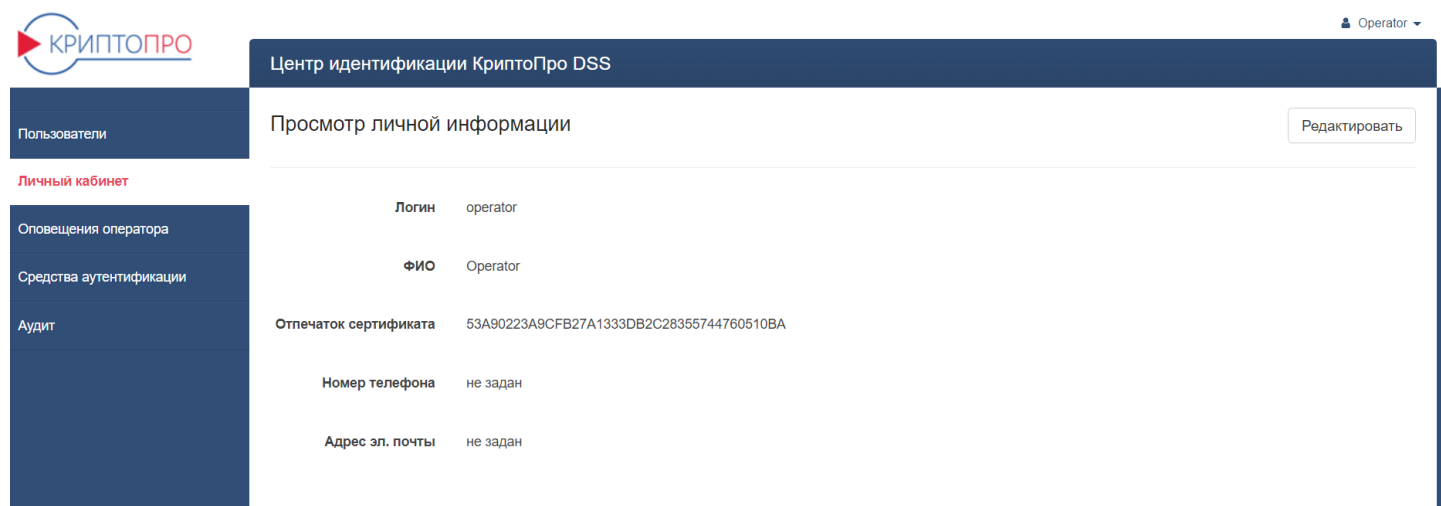


Рисунок 5 - Начальная страница веб-интерфейса Оператора

В меню начальной страницы Оператора доступны 5 разделов:

- 1) «Пользователи».
- 2) «Личный кабинет».

- 3) *«Оповещения оператора».*
- 4) *«Средства аутентификации».*
- 5) *«Аудит».*

3. Раздел «Пользователи»

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

3.1. Создание нового Пользователя

Для регистрации нового Пользователя требуется нажать кнопку «Создать нового пользователя» (см. Рисунок 6 - Создание нового Пользователя).

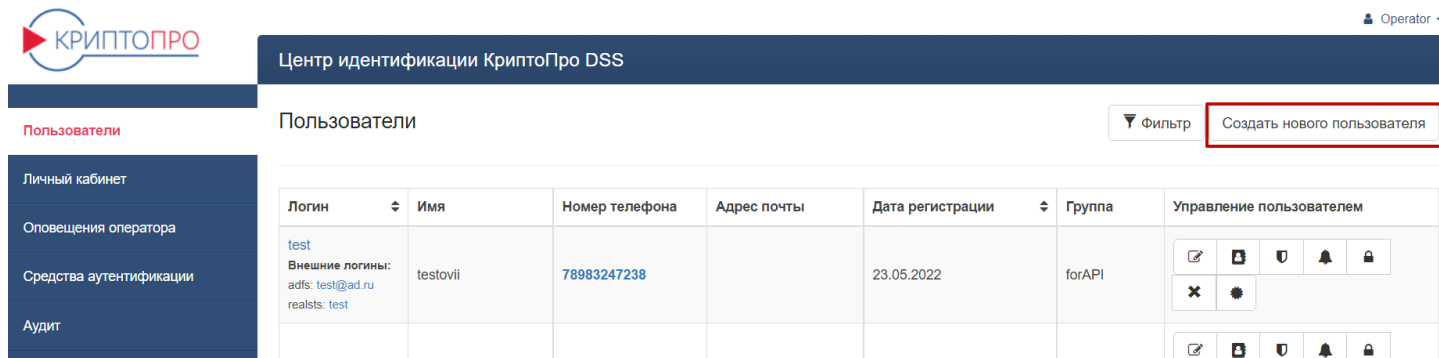


Рисунок 6 - Создание нового Пользователя

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

После корректного заполнения всех полей формы следует нажать кнопку «Создать» (см. Рисунок 7 - Ввод сведений о Пользователе).

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

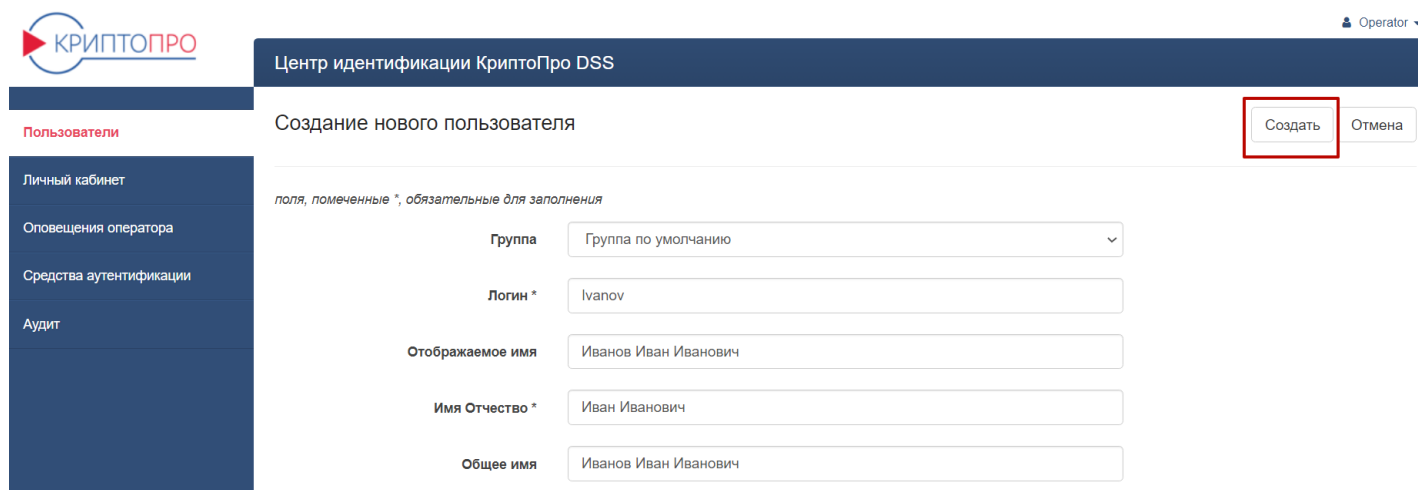


Рисунок 7 - Ввод сведений о Пользователе

3.2. Управление существующими Пользователями

Для управления существующими Пользователями перейдите в раздел «Пользователи» в интерфейсе Оператора. СЭП отобразит всех зарегистрированных

Пользователей, для каждого из которых в графе «Управление пользователем» доступны следующие действия:

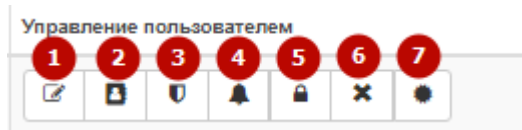


Рисунок 8 - Управление Пользователем

- 1) «Редактировать» – редактирование атрибутов Пользователя.
- 2) «Управление контактной информацией» - редактирование контактной информации (номер телефона, e-mail, PUSH-адреса)
- 3) «Настройки аутентификации» – редактирование методов аутентификации, политик подтверждения и доступа Пользователя к операциям в СЭП.
- 4) «Управление политикой оповещения» -выбор способа оповещения и событий, о которых необходимо оповещать Пользователя.
- 5) «Заблокировать» – блокировка или разблокировка Пользователя.
- 6) «Удалить» – удаление Пользователя.
- 7) «Сертификаты» – управление сертификатами Пользователя.

Те же действия можно найти, открыв Пользователя, нажав на его логин (см. Рисунок 9 - Действия для управления Пользователем).

Логин	Имя	Номер телефона	Адрес почты	Дата регистрации	Группа	Управление пользователем
Ivanov	Иванов Иван Иванович			26.04.2023	Default	[Edit] [Lock] [Shield] [Bell] [Padlock] [X] [Gear]
test	Внешние логины: adfs: test@ad.ru realsts: test	78983247238		23.05.2022	forAPI	[Edit] [Lock] [Shield] [Bell] [Padlock] [X] [Gear]

Личная информация пользователя **Иванов Иван Иванович** Подтвердить УЗ

← Назад Сертификаты Заблокировать Редактировать Контакты Аутентификация Оповещения Клонировать

Отображаемое имя	Иванов Иван Иванович
Группа	Группа по умолчанию
Логин	Ivanov
Имя Отчество	Иван Иванович
Общее имя	Иванов Иван Иванович
Фамилия	Иванов
Инициалы	

Рисунок 9 - Действия для управления Пользователем

3.2.1. Редактирование атрибутов Пользователя

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

После завершения редактирования атрибутов Пользователя следует нажать кнопку «*Сохранить*» для сохранения изменений (см. Рисунок 10 - Редактирование атрибутов Пользователя).

The screenshot shows a web interface for editing user data. At the top left is the 'КРИПТОПРО' logo. The main header is 'Центр идентификации КриптоПро DSS'. Below it, the page title is 'Редактирование учётных данных пользователя Иванов Иван Иванович'. On the right, there are two buttons: 'Сохранить' (highlighted with a red box) and 'Отмена'. On the left, there is a navigation menu with items: 'Личный кабинет', 'Оповещения оператора', 'Средства аутентификации', and 'Аудит'. The main form area contains the following fields:

Группа	Группа по умолчанию
Отображаемое имя	Иванов
Имя Отчество *	Иван Иванович
Общее имя	Иванов Иван Иванович
Фамилия	Иванов

Рисунок 10 - Редактирование атрибутов Пользователя

3.2.2. Настройка параметров аутентификации Пользователя

В СЭП предусмотрены методы первичной аутентификации (применяются для аутентификации Пользователя в интерфейсе 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). Использование данного метода не является безопасным и допускается только при включении вторичных методов аутентификации и требования подтверждения операции входа с использованием вторичного метода аутентификации.

- «*Аутентификация по сертификату*» – аутентификация Пользователя по сертификату; метод доступен только в случае, если Пользователю назначен сертификат. Сертификат для первичной аутентификации может быть выпущен Оператором при регистрации Пользователя в СЭП.

- «*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.

- *«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 СЭП в мобильном приложении «DSS Client».

Пользователю должен быть назначен хотя бы один метод первичной аутентификации, а также хотя бы один метод вторичной аутентификации.

3.2.2.1. *Настройка первичной аутентификации*

3.2.2.1.1 *Настройка аутентификации по сертификату*

Для создания сертификата первичной аутентификации пользователя необходимо импортировать компоненты имени Пользователя из существующего сертификата (кнопка *«Заполнить компоненты имени из сертификата»*) (см. Рисунок 11 - Импорт сертификата для аутентификации) или выпустить сертификат (для включения такой возможности необходимо обратиться к администратору СЭП).

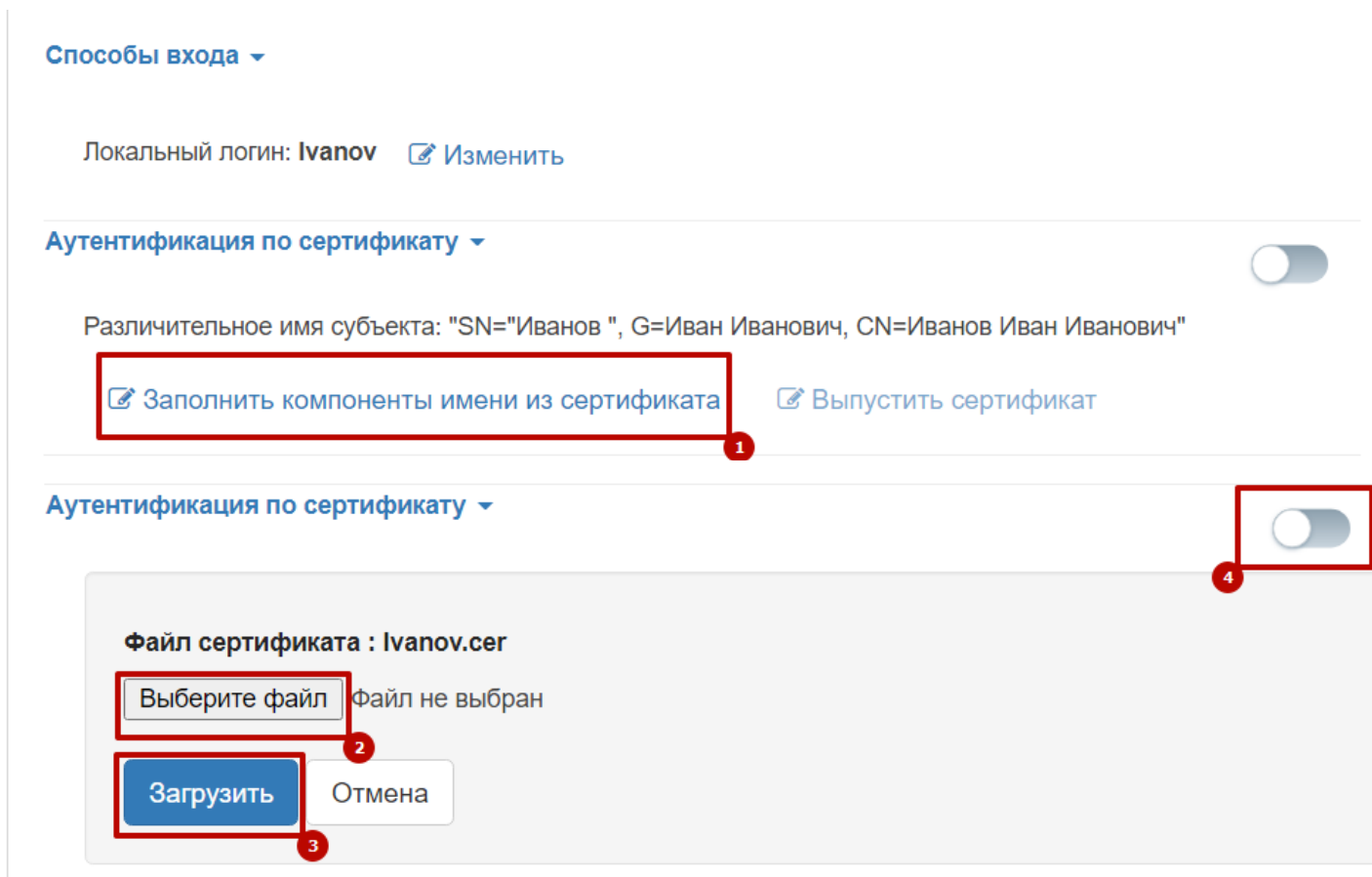


Рисунок 11 - Импорт сертификата для аутентификации

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:

1) В группе «Методы первичной аутентификации» раскрыть блок «Аутентификация по паролю» и нажать кнопку «Сгенерировать» (см. Рисунок 12 - Генерация пароля Пользователя).

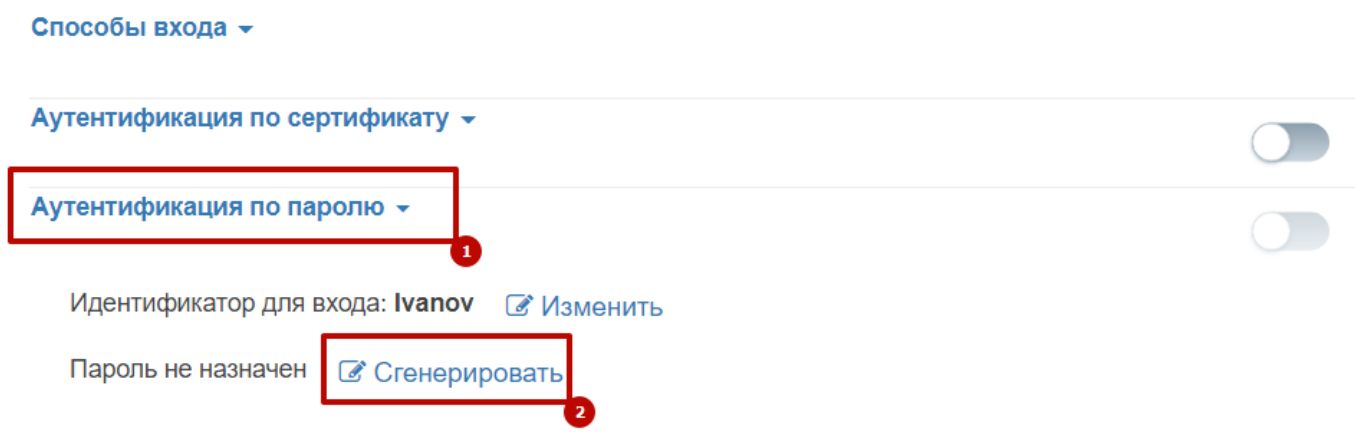


Рисунок 12 - Генерация пароля Пользователя

2) Выбрать метод отправки пароля из доступных (см. Рисунок 13 - Выбор метода отправки пароля).

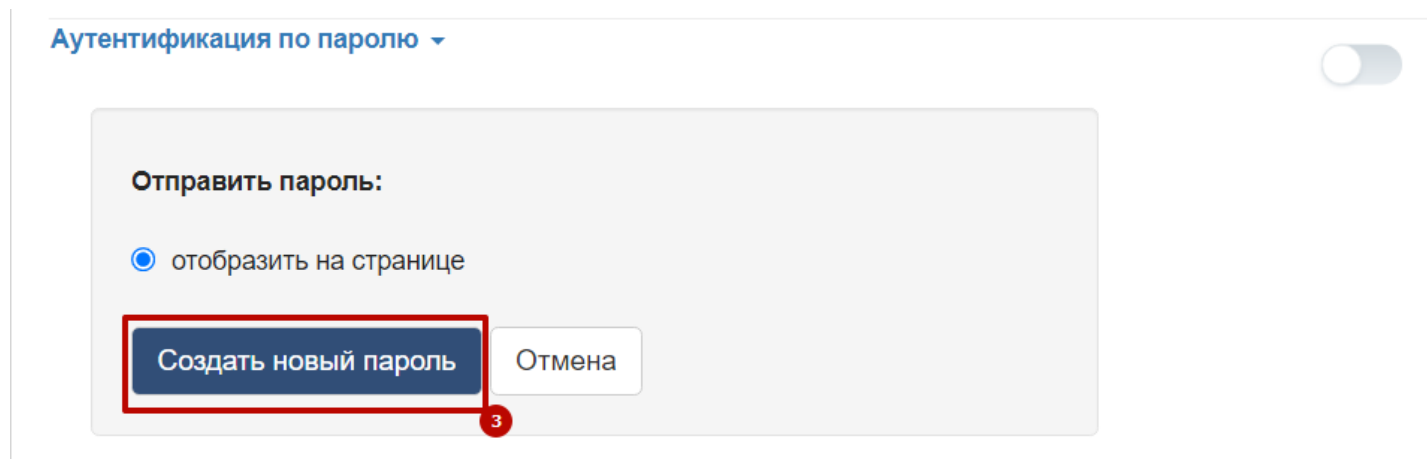


Рисунок 13 - Выбор метода отправки пароля

3) Пароль успешно сгенерирован, Пользователь может поменять его самостоятельно в своем личном кабинете.

Для включения первичной аутентификации по паролю необходимо установить переключатель «Аутентификация по паролю» в группе «Первичная аутентификация» в активное положение (см. Рисунок 14 - Включение аутентификации по паролю).

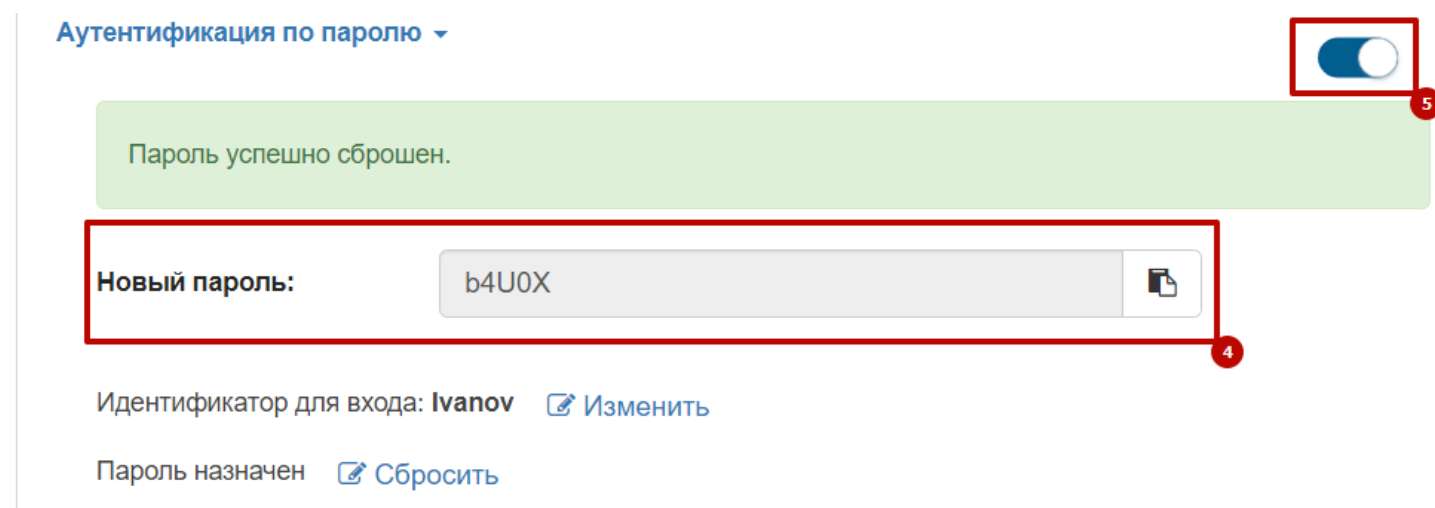


Рисунок 14 - Включение аутентификации по паролю

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 номер телефона для Пользователя не добавлен, то будет предложено его добавить (см. Рисунок 15 - Добавление номера телефона)

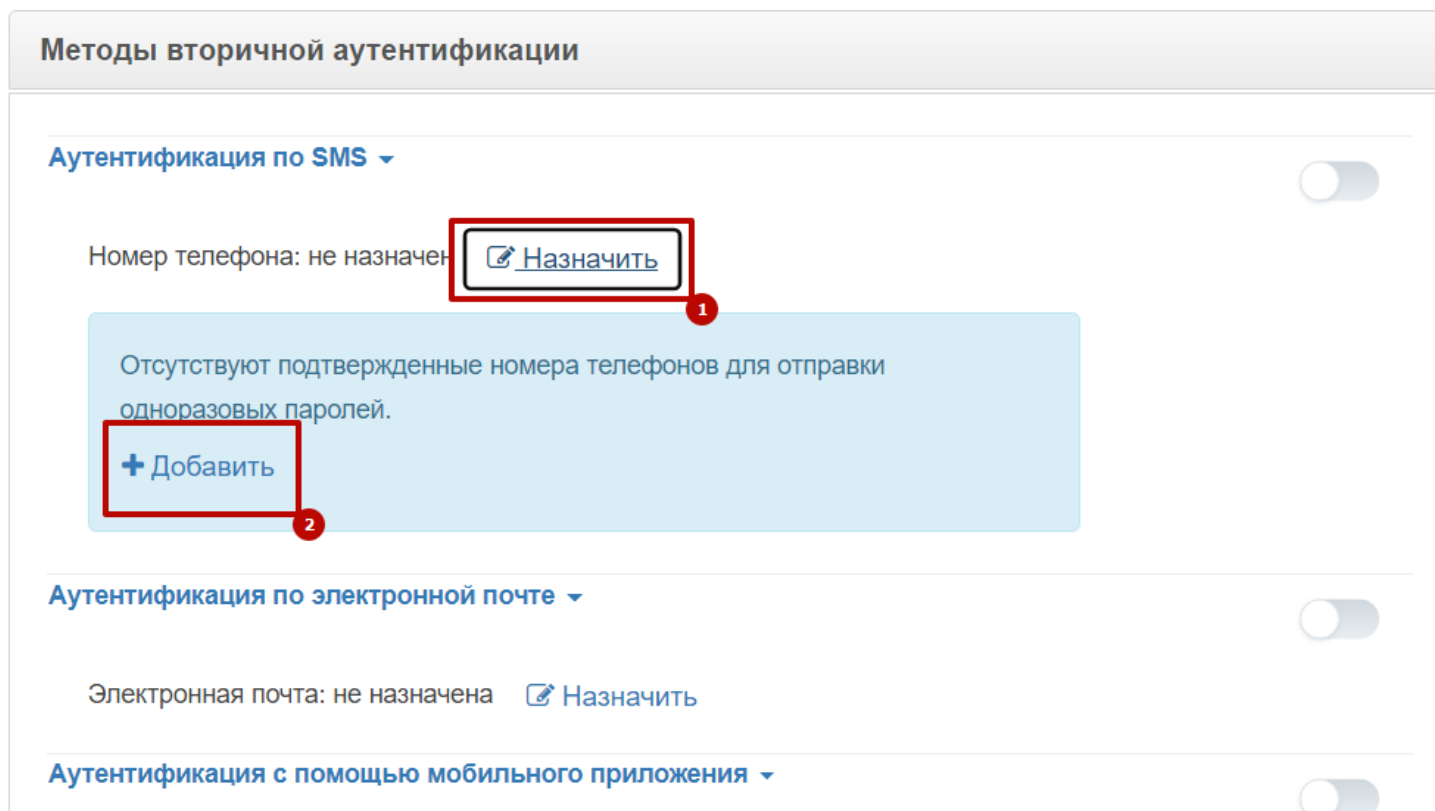


Рисунок 15 - Добавление номера телефона

Далее произойдет перенаправление на страницу редактирования контактной информации Пользователя. Введите номер телефона и нажмите кнопку «Добавить». После появления сообщения, что номер успешно сохранен нажмите кнопку «Назад» (см. Рисунок 16 - Добавление номера телефона).

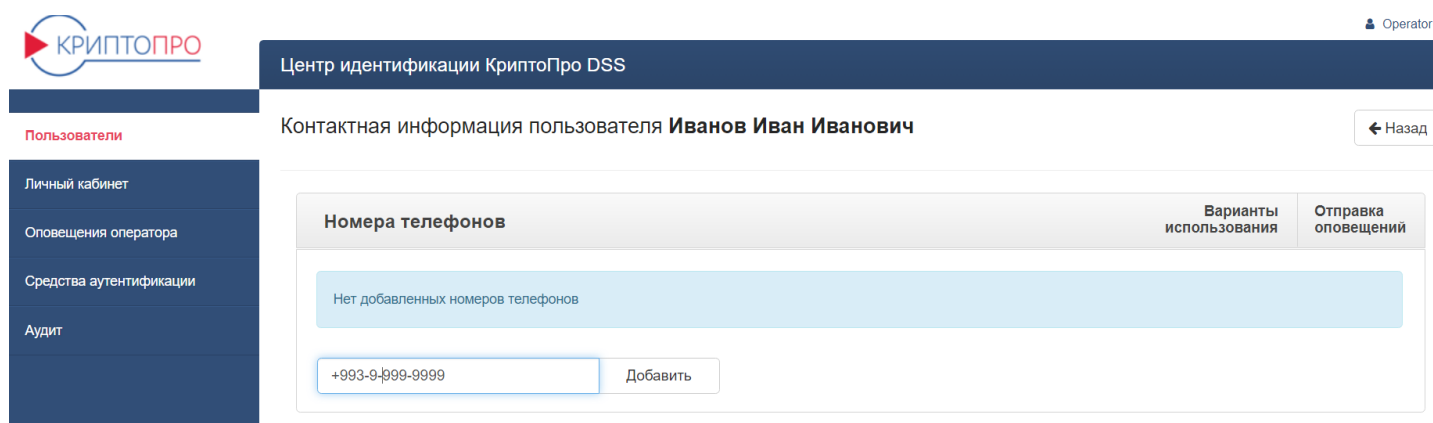


Рисунок 16 - Добавление номера телефона в контактной информации

После возвращения на страницу настроек аутентификации раскройте блок «Аутентификация по SMS» и выберите добавленный номер телефона.

Для включения вторичной аутентификации по SMS необходимо установить переключатель «Аутентификация по SMS» в группе «Вторичная аутентификация» в активное положение (см. Рисунок 17 - Включение метода аутентификации по SMS).

Методы вторичной аутентификации

Аутентификация по SMS

Номер телефона: +993-9-999-9999 [Изменить](#) [Сбросить](#)

Аутентификация по электронной почте

Электронная почта: не назначена [Назначить](#)

Аутентификация с помощью мобильного приложения

Рисунок 17 - Включение метода аутентификации по SMS

3.2.2.2.2 *Настройка аутентификации по протоколу OATH*

Для настройки вторичной аутентификации Пользователя по протоколу OATH (токену TOTP/HOTP, например, eToken Pass) в группе «Методы вторичной аутентификации» необходимо раскрыть блок «Аутентификация по протоколу OATH» и выбрать способ генерации одноразовых паролей: «Брелок» или «мобильное приложение». (см. Рисунок 18 - Способ генерации одноразовых паролей)

Аутентификация по протоколу OATH

Выберите способ генерации одноразовых паролей

Рисунок 18 - Способ генерации одноразовых паролей

3.2.2.2.2.1. Генерация одноразовых паролей с помощью брелока

В окне выбора генератора одноразовых паролей выберите «Брелок». В появившемся поле ввода параметров аутентификации по протоколу OATH требуется указать серийный номер OTP-токена, первый и второй пароли OTP, после чего нажать кнопку «Зарегистрировать» (см. Рисунок 19 - Ввод параметров аутентификации по протоколу OATH). Для включения вторичной аутентификации по протоколу OATH необходимо установить переключатель «Аутентификация по протоколу OATH» в группе «**Вторичная**

аутентификация» в активное положение.

Аутентификация по протоколу OATH ▾

Выберите способ генерации одноразовых паролей

Брелок Мобильное приложение

Серийный номер токена

Number

Первый OTP

00000

Второй OTP

111111

Зарегистрировать

Рисунок 19 - Ввод параметров аутентификации по протоколу OATH

3.2.2.2.2. Генерация одноразовых паролей через мобильное приложение

В окне выбора генератора одноразовых паролей выберите «Мобильное приложение». Далее нажмите «Назначить аутентификатор».

Аутентификация по протоколу OATH ▾

Выберите способ генерации одноразовых паролей

Брелок Мобильное приложение

Назначить аутентификатор

Рисунок 20 - Аутентификация с помощью мобильного приложения

С помощью приложения, поддерживающего протокол OATH отсканируйте появившийся QR-код или введите указанный код (см. Рисунок 21 - QR для сканирования в мобильном приложении).

Аутентификация по протоколу OATH ▾



Установите одно из приложений для генерации одноразовых паролей. Приложения для генерации одноразовых паролей позволяют получать коды даже без доступа к сети. Данная настройка выполняется один раз для синхронизации мобильного приложения с сервером.

Список доступных приложений для генерации одноразовых паролей:

- Яндекс.Ключ ([App Store](#) | [Google Play](#))
- Google Authenticator ([App Store](#) | [Google Play](#))
- Microsoft Authenticator ([App Store](#) | [Google Play](#))
- Другие приложения, поддерживающие протокол OATH

Отсканируйте QR-код в мобильном приложении



Распечатать QR-код

Или введите этот код в мобильном приложении вручную
4IGW HRDF AY6O 3RDA L3RE GOAY UBFO MIVY

Отвязать приложение

Вернуться

Рисунок 21 - QR для сканирования в мобильном приложении

После сканирования QR-кода одноразовые пароли будут генерироваться автоматически. Для включения метода аутентификации 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 в группе «Методы вторичной аутентификации» раскрыть блок «Аутентификация по электронной почте» и нажать кнопку «Назначить», если для пользователя нет сохраненных адресов электронной почты, то по кнопке «Добавить» произойдет перенаправление на страницу с контактной информацией пользователя. Введите адрес электронной почты и нажмите кнопку «Добавить» (см. Рисунок 22 - Добавление адреса электронной почты).

Рисунок 22 - Добавление адреса электронной почты

Если адрес электронной почты задан в контактах пользователя, то выберите нужный адрес (см. Рисунок 23 - Выбор адреса электронной почты).

Рисунок 23 - Выбор адреса электронной почты

Для включения вторичной аутентификации по электронной почте 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 «DSS Client» в группе «Методы вторичной аутентификации» раскройте блок «Аутентификация с помощью мобильного приложения» и нажмите кнопку «Добавить устройство» (см. Рисунок 24 - Аутентификация с помощью мобильного приложения). Выберите способ отправки кода активации и передайте Пользователю QR-код для сканирования в мобильном приложении.

Рисунок 24 - Аутентификация с помощью мобильного приложения

Установите переключатель «Аутентификация с помощью мобильного приложения» в группе «Вторичная аутентификация» в активное положение (см. Рисунок 25 - QR-код для DSS Client).

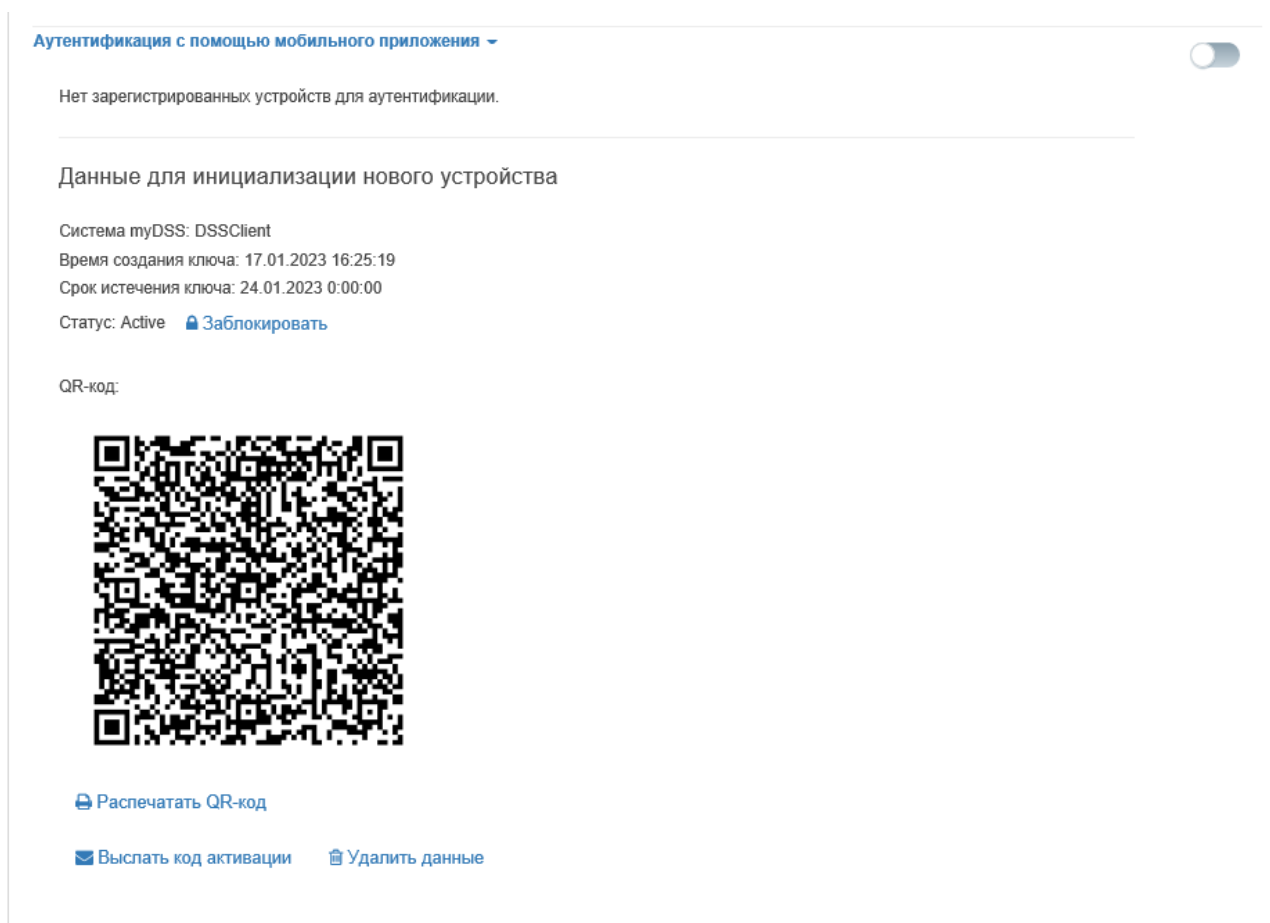


Рисунок 25 - QR-код для DSS Client

Для обеспечения работоспособности вторичной аутентификации с помощью мобильного приложения Пользователю необходимо установить мобильное приложение «DSS Client» из магазина [Google Play](#), [Apple App Store](#), [AppGallery](#).

При первом запуске мобильное приложение запросит разрешение на отправку уведомлений и установку способа защиты приложения (см. Рисунок 26 - Первый запуск мобильного приложения).

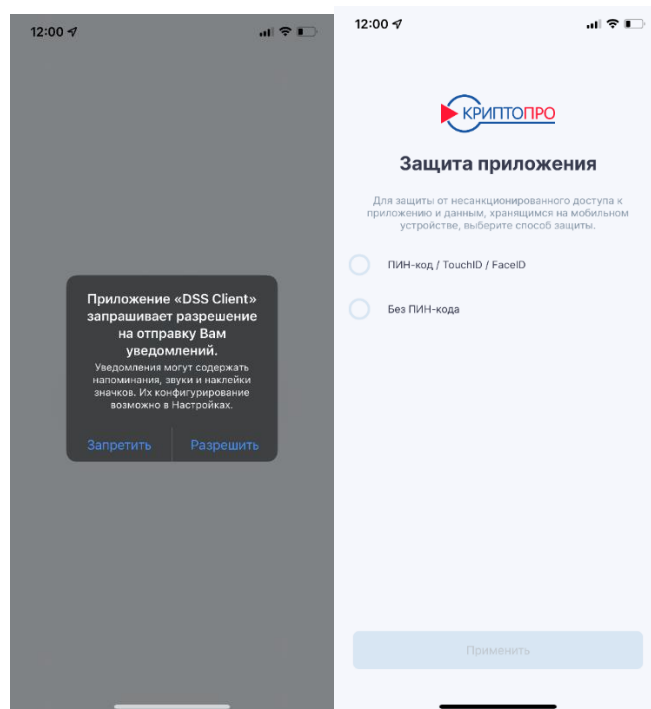


Рисунок 26 - Первый запуск мобильного приложения

В мобильном приложении Пользователь должен выбрать способ привязки «через QR-код» и ввести имя учетной записи.

На следующем шаге мобильное приложение попросит отсканировать QR-код. Как только QR-код будет успешно отсканирован, Пользователь должен ввести полученный им ранее при регистрации код активации (см. Рисунок 27 - Регистрация учетной записи в DSS Client).

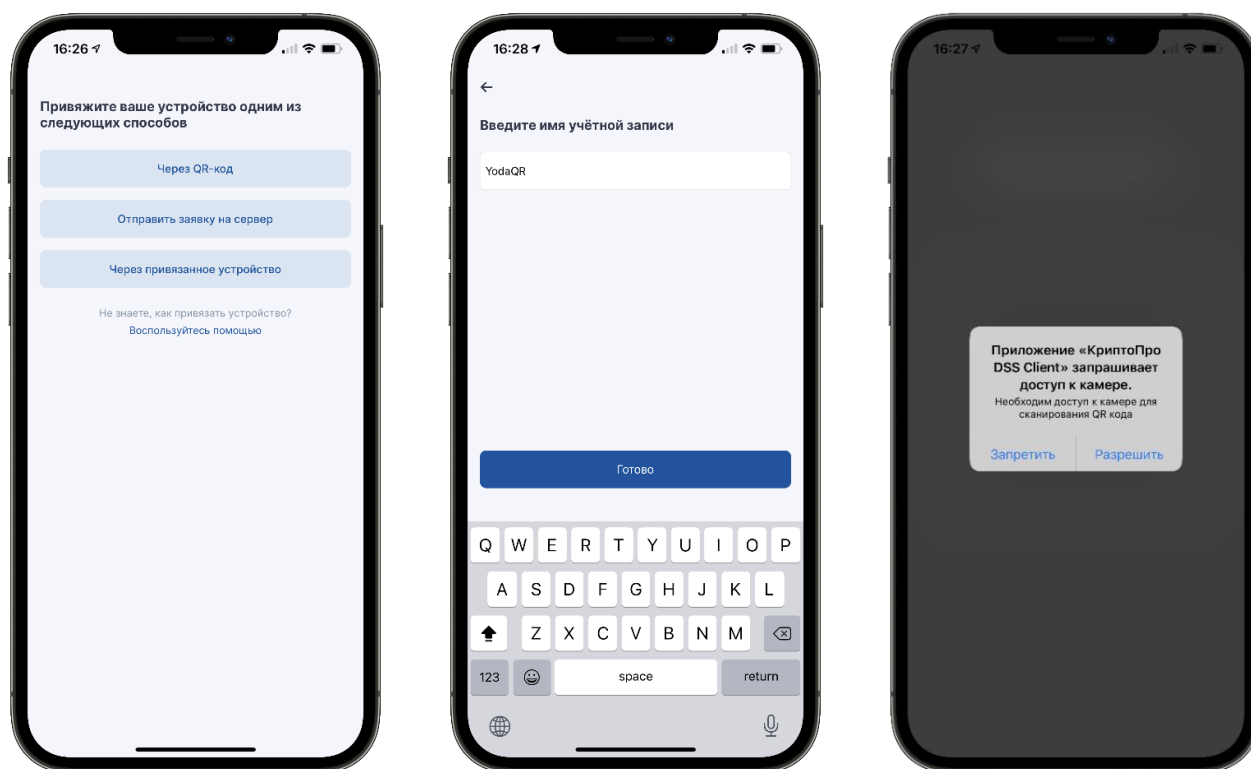


Рисунок 27 - Регистрация учетной записи в DSS Client

После ввода кода активации Пользователю будет предложено выбрать способ защиты учетной записи. Если Пользователь выбрал пункт «**ПИН-код / Face ID**», то в следующем окне потребуются задать ПИН-код. Данный ПИН-код необходимо будет вводить в дальнейшем при подтверждении операций, создании запросов на сертификаты, добавлении новых устройств и других действий, требующих аутентификации. Если ранее в приложении не использовалась биометрия (например, при задании кода-пароля защиты приложения), то требуется предоставить приложению разрешение использовать биометрические данные (отпечаток пальца или скан формы лица). Биометрия может заменять ввод ПИН-кода при подтверждении операций и прочих действий, требующих аутентификации (см. Рисунок 28 - Защита мобильного приложения).

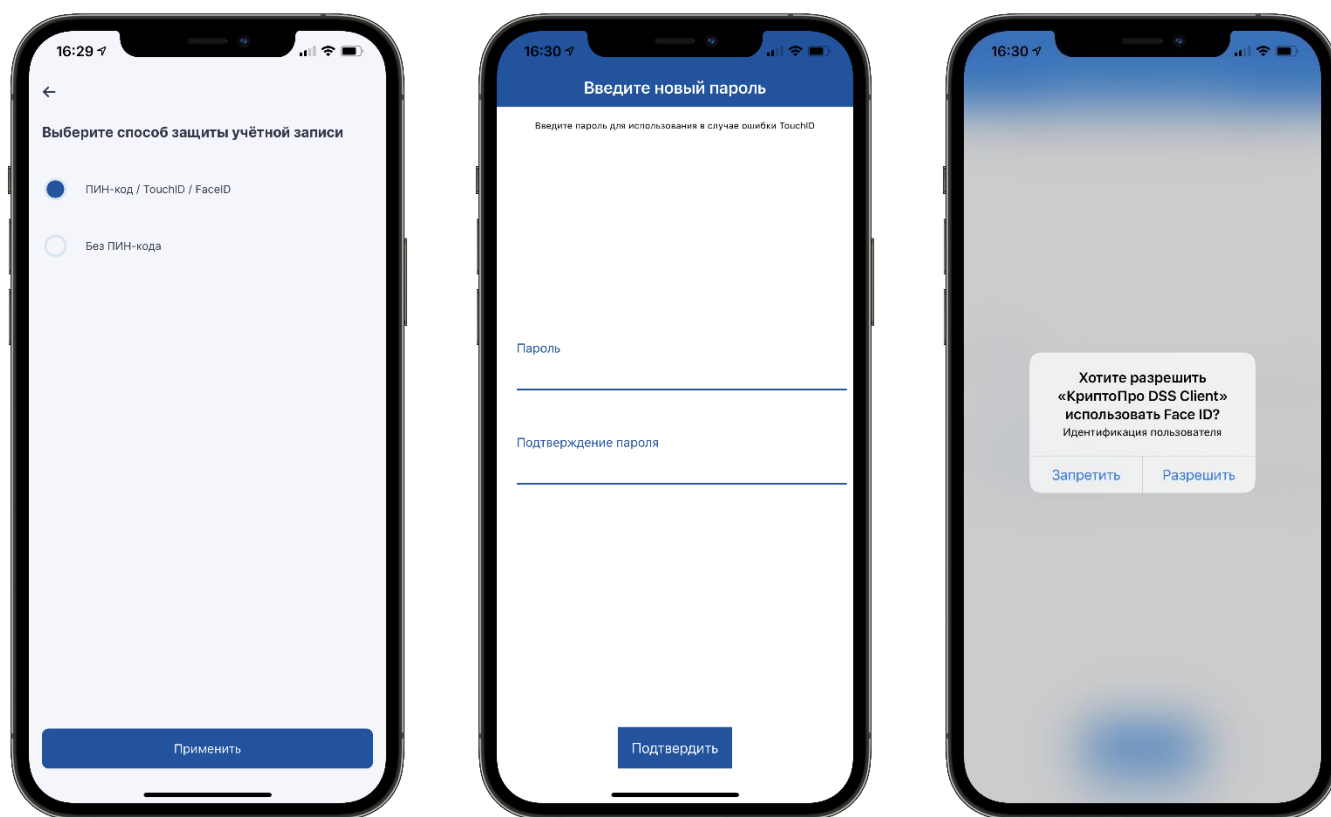


Рисунок 28 - Защита мобильного приложения

На экране мобильного устройства отобразится информация об учетной записи Пользователя. Мобильное приложение запросит подтверждение, что данные верны, после чего привязка устройства будет завершена и его можно будет использовать для подтверждения подписи документов. В случае если данные не верны, следует отказаться от подтверждения привязки учетной записи и отредактировать учетную запись Пользователя в личном кабинете Оператора. Если данные учётной записи верны, и Вы подтвердили привязку, на экране отобразится соответствующее информационное уведомление (см. Рисунок 29 - Информация об учетной записи пользователя).

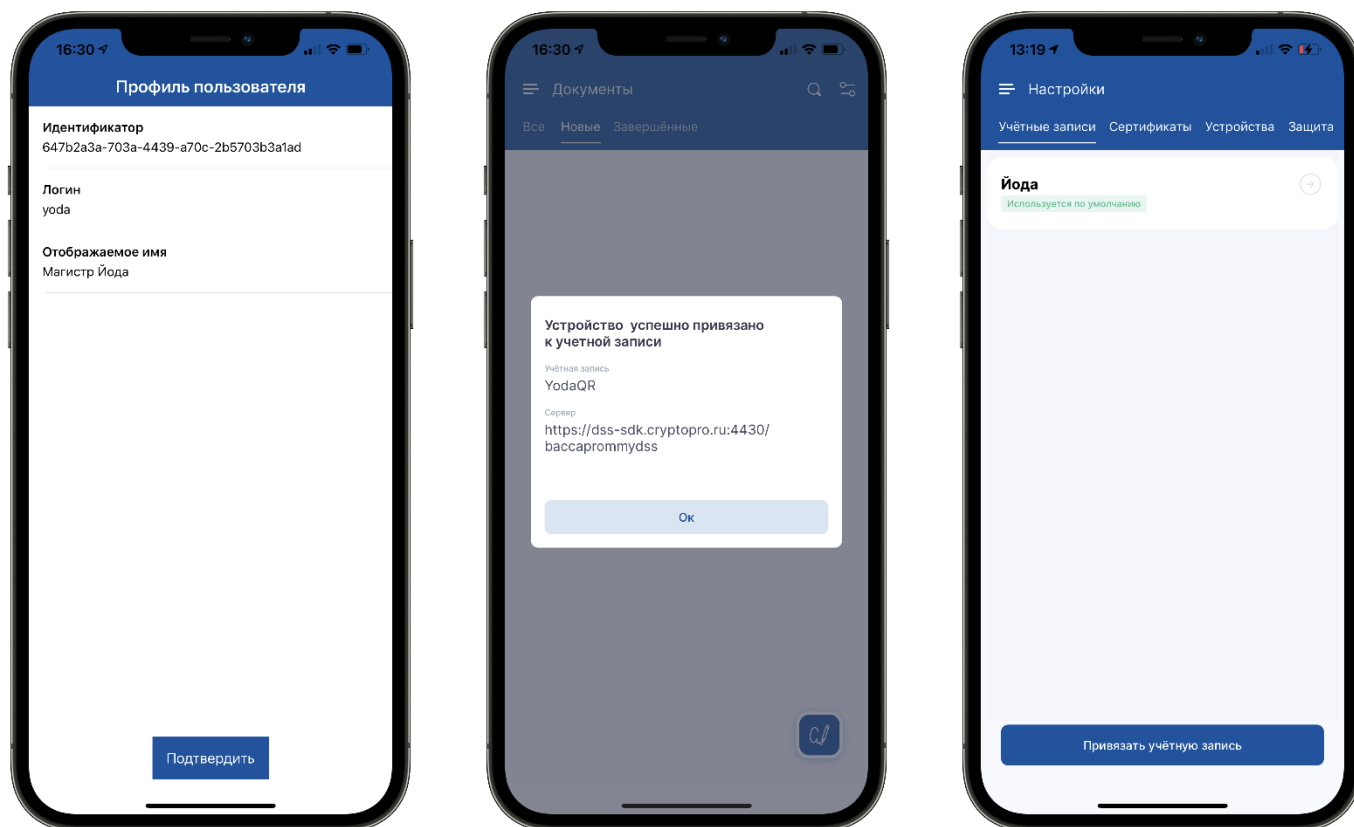


Рисунок 29 - Информация об учетной записи пользователя

3.2.2.3. Настройка подтверждения и доступа к операциям СЭП

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

Оператор может дать Пользователю доступ к следующим операциям в СЭП (список операций может меняться в зависимости от настройки экземпляра):

- Подпись документа.
- Шифрование/расшифрование документа.
- Создание запроса на сертификат.
- Удаление сертификата.
- Обновление сертификата.
- Смена ПИН-кода закрытого ключа.

Оператор может установить подтверждение Пользователем методом выбранной вторичной аутентификации следующих операций в СЭП (список операций может меняться в зависимости от настройки экземпляра):

- Выпуск маркера (вход в ЦИ).
- Подпись документа.
- Подпись пакета документов.
- 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 разделе *«Настройки аутентификации Пользователя»* в блоках *«Подтверждение операций»* и *«Доступ к операциям»* (см. Рисунок 30 - Политика доступа и подтверждения операций).

Подтверждение операций	
Выпуск маркера (вход в ЦИ)	<input type="checkbox"/>
Подпись документа	<input type="checkbox"/>
Подпись пакета документов	<input type="checkbox"/>
Расшифрование документа	<input type="checkbox"/>
Создание запроса на сертификат	<input type="checkbox"/>
Смена пин-кода закрытого ключа	<input type="checkbox"/>
Обновление сертификата	<input type="checkbox"/>
Отзыв сертификата	<input type="checkbox"/>
Приостановление действия сертификата	<input type="checkbox"/>
Возобновление действия сертификата	<input type="checkbox"/>
Удаление сертификата	<input type="checkbox"/>
Доступ к закрытому ключу	<input type="checkbox"/>

Доступ к операциям	
Подпись документа	<input checked="" type="checkbox"/>
Шифрование/расшифрование документа	<input checked="" type="checkbox"/>
Создание запроса на сертификат	<input checked="" type="checkbox"/>
Удаление сертификата	<input checked="" type="checkbox"/>
Обновление сертификата	<input checked="" type="checkbox"/>
Отзыв сертификата	<input checked="" type="checkbox"/>
Приостановление действия сертификата	<input checked="" type="checkbox"/>
Возобновление действия сертификата	<input checked="" type="checkbox"/>
Смена пин-кода закрытого ключа	<input checked="" type="checkbox"/>

Рисунок 30 - Политика доступа и подтверждения операций

3.2.3. Блокировка или разблокировка Пользователя

Для блокировки, либо разблокировки Пользователя необходимо нажать на значок «Заблокировать», далее утвердительно ответить на запрос о блокировке/разблокировке Пользователя (см. Рисунок 31 - Блокировка Пользователя). При успешной блокировке (разблокировке) Пользователя значок «Заблокировать» меняется соответственно на изображение открытого (закрытого) замка.

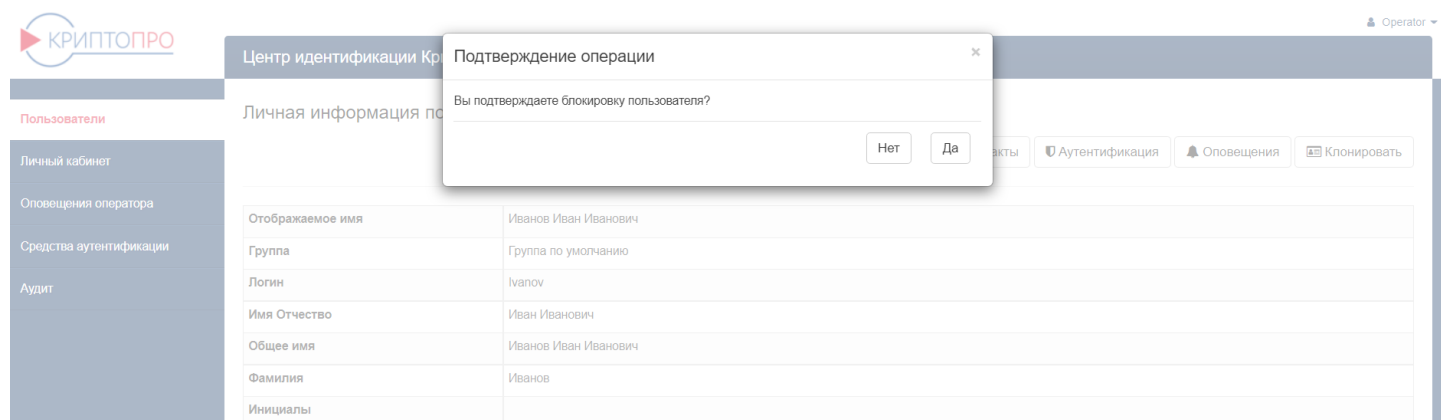


Рисунок 31 - Блокировка Пользователя

3.2.4. Удаление Пользователя

Для удаления Пользователя необходимо нажать на значок «Удалить», далее утвердительно ответить на запрос об удалении Пользователя (см. Рисунок 32 - Удаление Пользователя).

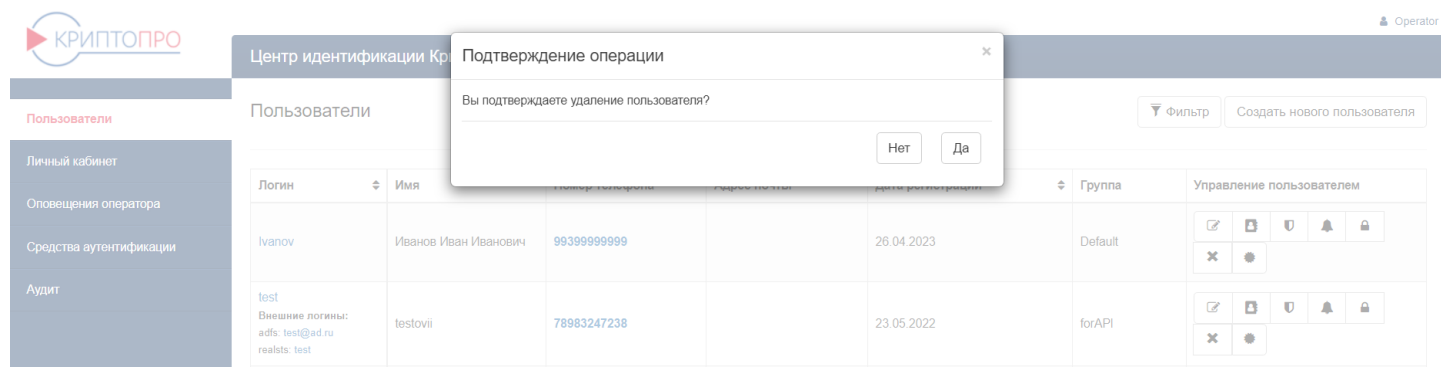


Рисунок 32 - Удаление Пользователя

3.2.5. Управление сертификатами Пользователя

Для управления сертификатами Пользователя требуется перейти в раздел «Сертификаты». Оператору доступны следующие операции с сертификатами Пользователя:

- «Удалить все» – удаление всех зарегистрированных в СЭП сертификатов

Пользователя.

- «Создание запроса на сертификат» – создание запроса на новый сертификат Пользователя.
- «Установить сертификат» – установка сертификата Пользователя.
- «Просмотр» - управление выбранным сертификатом Пользователя в СЭП.

3.2.5.1. Удаление всех сертификатов Пользователя, зарегистрированных в СЭП

Для удаления всех зарегистрированных в СЭП сертификатов Пользователя следует нажать кнопку «Удалить все», далее подтвердить удаление нажатием кнопки «Да» (см. Рисунок 33 - Удаление всех сертификатов).

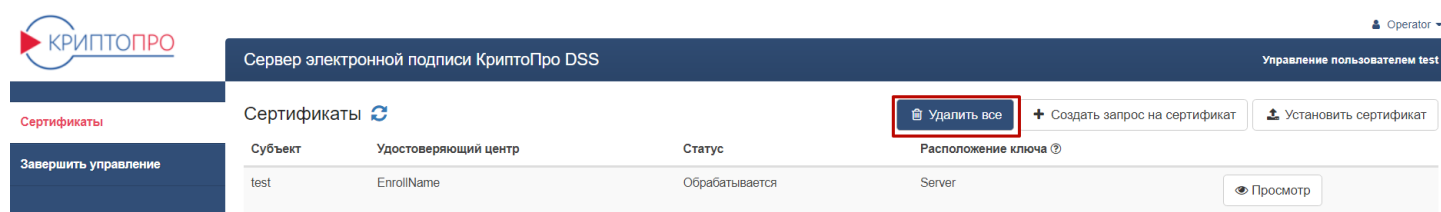


Рисунок 33 - Удаление всех сертификатов

3.2.5.2. Создание запроса на сертификат Пользователя

Для создания запроса на сертификат Пользователя нажмите кнопку «Создать запрос на сертификат».

3.2.5.2.1. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)

Выберите шаблон сертификата и заполните данные в «Компоненты имени сертификата». Нажмите кнопку «Создать запрос» (см. Рисунок 34 - Создание запроса на сертификат)

The screenshot shows a form for creating a certificate request. It features two dropdown menus: 'Параметры времени действия сертификата' (Certificate validity parameters) and 'Тип идентификации заявителя' (Applicant identification type). Below these menus is a button labeled 'Создать запрос' (Create request).

Рисунок 34 - Создание запроса на сертификат

При появлении окна «Дополнительные параметры» задайте pin-код и нажмите кнопку «Ок» (см. Рисунок 35 - Запрос пин-кода).

Рисунок 35 - Запрос пин-кода

Сертификат будет создан автоматически и откроется окно с перечнем сертификатов Пользователя и информацией о статусе сертификата.

Откроется информация о сертификате.

Сертификат

Субъект	CN=Иванов Иван, C=RU, SN="Иванов ", G=Иван
Издатель	CN=Sub-TESTCA20-2012-CA, O="ООО "КРИПТО-ПРО"", OU=Удостоверяющий центр, STREET=ул. Суцёвский Вал 18, L=Москва, C=RU, ИНН=007717107991, ОГРН=1037700085444
Статус	Действителен
Срок действия	C 26.04.2023 18:29:04 по 26.04.2024 18:39:04
Срок действия закрытого ключа	C 26.04.2023 18:39:02 по 26.07.2024 18:39:02
Отпечаток	A4C04365F1847436768603AA168B977B20DBCE9B
Серийный номер	02EC0101F0AFDC9F43C8B3300C1500DC
Алгоритм открытого ключа	1.2.643.7.1.1.1.1 (ГОСТ Р 34.10-2012 256 бит)
Улучшенный ключ	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Шаблон сертификата	Неизвестное использование ключа (1.2.643.2.2.50.1.9.11403974.16312490.11289102.16046170.10280.51614)
Дружественное имя	Не задано

Рисунок 36 - Информация о сертификате

3.2.5.2.2. Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)

Выберите шаблон сертификата и заполните данные в «Компоненты имени сертификата». Нажмите кнопку «Создать запрос». Обязательно проставьте чек-бокс «Неподписанный запрос» Нажмите кнопку «Создать запрос» (см. Рисунок 34 - Создание запроса на сертификат).

Откроется информация о запросе на сертификат. Статус запроса - «Ожидает подписи» (см. Рисунок 37 - Запрос на сертификат).

Запрос на сертификат

Информация о запросе ↻	
Субъект	CN=test
Издатель	EnrollName
Статус	Ожидает подписи

Рисунок 37 - Запрос на сертификат

Дальнейшие действия нужно выполнять в мобильном устройстве Пользователя.

1. Откройте приложение DSS Client, откройте «Настройки» -> «Сертификаты».
2. В списке сертификатов выберите со статусом «Запрос на сертификат не подписан» и откройте его.
3. Нажмите «Подписать запрос».
4. Откроется датчик случайных чисел. Нажимайте на экран телефона для генерации ключей до тех пор, пока шкала в нижней части экране не будет заполнена (см. Рисунок 38 - Подписание запроса на мобильном устройстве).

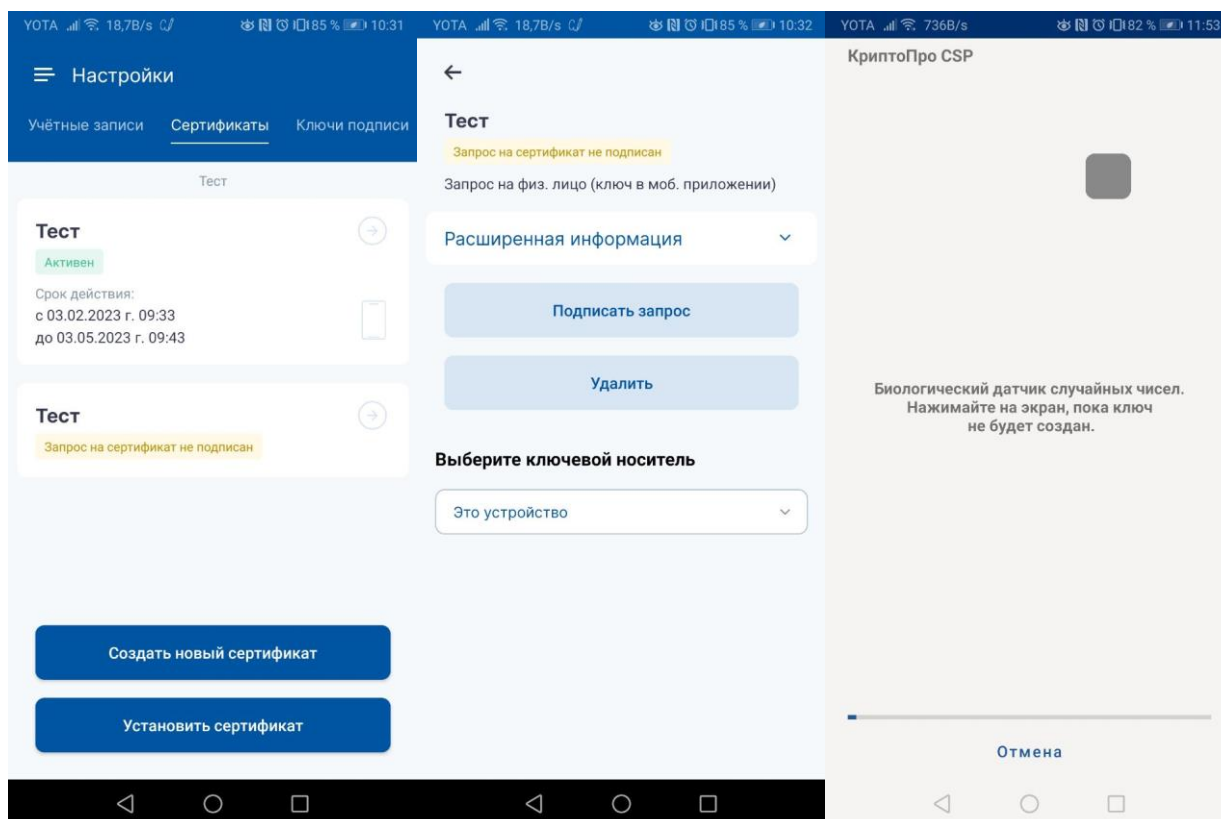


Рисунок 38 - Подписание запроса на мобильном устройстве

После появления сообщения «Запрос успешно подписан» запрос в мобильном приложении изменит статус на «Отправлен запрос», а в веб-интерфейсе на «Обрабатывается».

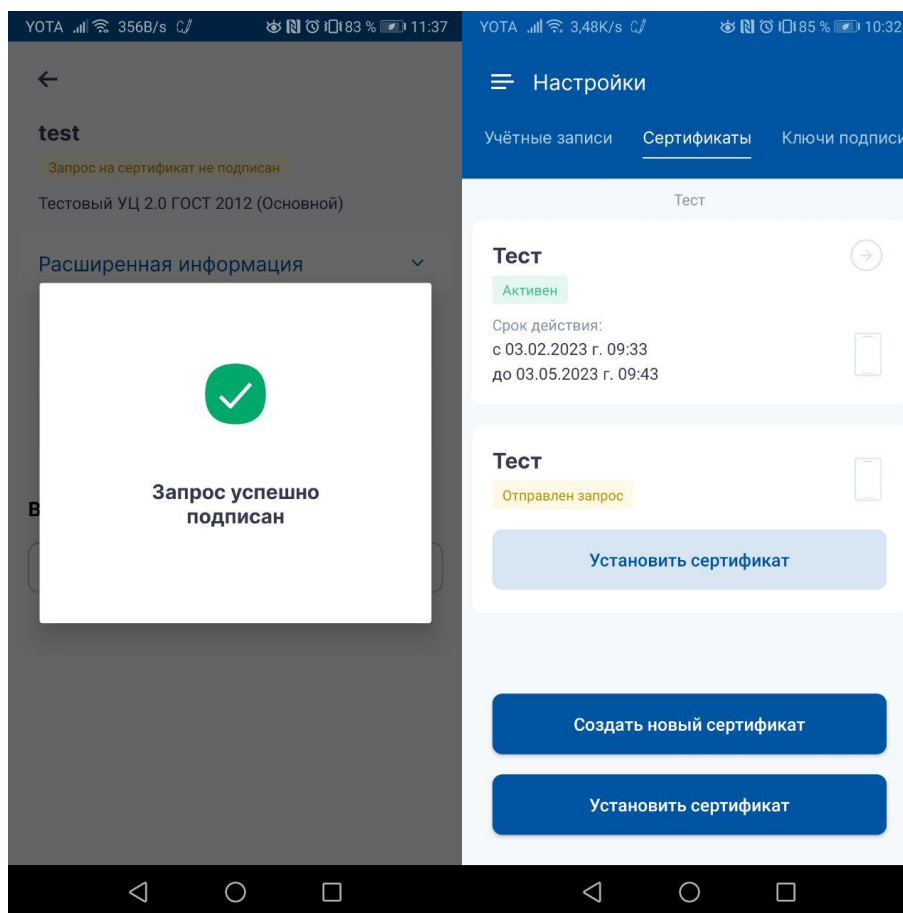


Рисунок 39 - Завершение подписания запроса

После подписания запроса в мобильном приложении он будет направлен в Удостоверяющий центр и обработан. Далее откроется окно с информацией о сертификате (см. Рисунок 36 - Информация о сертификате).

3.2.5.3. Управление существующим сертификатом Пользователя в СЭП

Для управления существующим сертификатом Пользователя в СЭП нужно нажать кнопку «Просмотр» в соответствующей строке раздела «Сертификаты» (см. Рисунок 40 - Выбор сертификата для управления).

Сервер электронной подписи КриптоПро DSS				Управление пользователем Ivanov
Сертификаты				
Субъект	Удостоверяющий центр	Статус	Расположение ключа	
Иванов Иван Иванович	ООВ_EnrollName	Обрабатывается	Server	Просмотр
test	OutOVB	Действителен	Server	Просмотр

Рисунок 40 - Выбор сертификата для управления

Оператору доступны следующие операции управления сертификатом (см. Рисунок 41 - Функции управления сертификатом):

- «Скачать» – скачать файл сертификата (*.cer).
- «Печать» – вывести бумажную копию сертификата на печать.
- «Изменить дружественное имя» – изменить дружественное имя сертификата (в случае если у Пользователя несколько сертификатов в СЭП).
- «Удалить» – удалить сертификат из СЭП.
- «Отозвать» - отозвать сертификат.
- «Приостановить» - приостановить действие сертификата на определенный срок.
- «Возобновить» - только для сертификатов в статусе «приостановлен».

Возобновить действие сертификата.

- «Обновить» - выпустить новый сертификат с теми же компонентами имени.
- «Сменить пин» - Изменить пин-код.
- «Назначить сертификатом по умолчанию» – выбрать данный сертификат по умолчанию из всех сертификатов Пользователя.

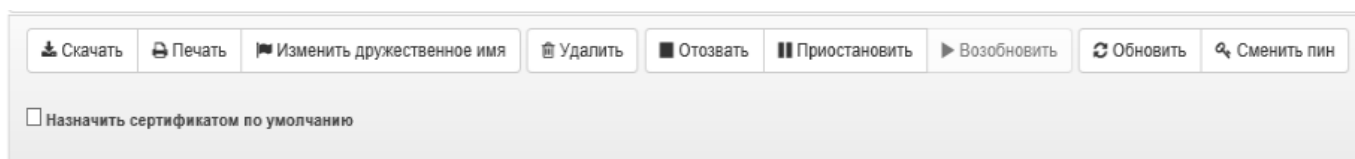


Рисунок 41 - Функции управления сертификатом

4. Раздел «Личный кабинет»

Раздел позволяет просматривать и редактировать личные данные Оператора (см. Рисунок 42 - Просмотр личных данных Оператора). При нажатии на кнопку «Редактировать» доступно изменения ФИО Оператора. Для сохранения изменений необходимо нажать кнопку «Сохранить».

КриптоПро

Центр идентификации КриптоПро DSS

Пользователи

Просмотр личной информации Редактировать

Личный кабинет

Оповещения оператора

Средства аутентификации

Аудит

Логин	operator
ФИО	Operator
Отпечаток сертификата	53A90223A9CFB27A1333DB2C28355744760510BA
Номер телефона	не задан
Адрес эл. почты	не задан

Рисунок 42 - Просмотр личных данных Оператора

5. Раздел «Оповещения оператора»

Раздел позволяет управлять списком операций для оповещения и методами оповещения (см. Рисунок 43 - Настройка оповещений оператора).

КриптоПро

Центр идентификации КриптоПро DSS

Пользователи

Личный кабинет

Оповещения оператора

Средства аутентификации

Аудит

Политика оповещения оператора ← Назад

Список событий	Оповещать в SMS	Оповещать в Email
Для получения SMS-уведомлений укажите номер телефона с помощью командлета Powershell "Set-DssIdentityOperator".		
Управление учетными данными	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Изменение данных учетной записи пользователя	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ошибка при изменении данных учетной записи пользователя	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Рисунок 43 - Настройка оповещений оператора

6. Раздел «Средства аутентификации»

Раздел позволяет просматривать перечень назначенных Пользователям средств аутентификации (см. Рисунок 44 - Перечень средств аутентификации).

Серийный номер	Назначен	Логин пользователя	Псевдоним	Тип токена	Лицензия на средство
444962581827928020			5af980ac-037c-4c8b-a82d-c1eed869e525	MobileAuth	
7335984			M18E6DF19FL3	MyDss	
7341435			0UN8N988Y5KY	MyDss	
99399999999	+	Ivanov		SmsOtp	

Рисунок 44 - Перечень средств аутентификации

7. Раздел «Аудит»

Раздел «Аудит» предназначен для отображения журнала событий, связанных с действиями Пользователей и Операторов в СЭП с возможностью фильтрации по типам событий (см. Рисунок 45 - Аудит событий СЭП).

ID	Статус	Код события	Дата	Данные	Учетные данные
13133	✓	Пользователь аутентифицирован по токenu (JWT/SAML) (331)	2023-04-27 17:39:10	Пользователь аутентифицирован по токenu (JWT/SAML). Логин: 14_09.	Оператор: 14_09 Пользователь: 14_09
13132	✓	Пользователь аутентифицирован с помощью мобильного приложения (340)	2023-04-27 17:39:10	Пользователь аутентифицирован с помощью мобильного приложения. Логин: 14_09.	Оператор: 14_09 Пользователь: 14_09

Рисунок 45 - Аудит событий СЭП

Перечень рисунков

Рисунок 1 – Добавление сайта в зону надежных сайтов	4
Рисунок 2 – Включение ActiveX.....	5
Рисунок 3 – Включение поддержки ГОСТ	6
Рисунок 4 - Аутентификация Оператора	7
Рисунок 5 - Начальная страница веб-интерфейса Оператора	7
Рисунок 6 - Создание нового Пользователя.....	9
Рисунок 7 - Ввод сведений о Пользователе	9
Рисунок 8 - Управление Пользователем	10
Рисунок 9 - Действия для управления Пользователем	10
Рисунок 10 - Редактирование атрибутов Пользователя.....	11
Рисунок 11 - Импорт сертификата для аутентификации	13
Рисунок 12 - Генерация пароля Пользователя.....	13
Рисунок 13 - Выбор метода отправки пароля	14
Рисунок 14 - Включение аутентификации по паролю	14
Рисунок 15 - Добавление номера телефона	15
Рисунок 16 - Добавление номера телефона в контактной информации	15
Рисунок 17 - Включение метода аутентификации по SMS	16
Рисунок 18 - Способ генерации одноразовых паролей.....	16
Рисунок 19 - Ввод параметров аутентификации по протоколу OATH	17
Рисунок 20 - Аутентификация с помощью мобильного приложения	17
Рисунок 21 - QR для сканирования в мобильном приложении	18
Рисунок 22 - Добавление адреса электронной почты	19
Рисунок 23 - Выбор адреса электронной почты.....	19
Рисунок 24 - Аутентификация с помощью мобильного приложения	19
Рисунок 25 - QR-код для DSS Client.....	20
Рисунок 26 - Первый запуск мобильного приложения	21
Рисунок 27 - Регистрация учетной записи в DSS Client	22
Рисунок 28 - Защита мобильного приложения.....	23
Рисунок 29 - Информация об учетной записи пользователя.....	24
Рисунок 30 - Политика доступа и подтверждения операций	26
Рисунок 31 - Блокировка Пользователя	27
Рисунок 32 - Удаление Пользователя.....	27
Рисунок 33 - Удаление всех сертификатов	28
Рисунок 34 - Создание запроса на сертификат	28
Рисунок 35 - Запрос пин-кода	29
Рисунок 36 - Информация о сертификате	29
Рисунок 37 - Запрос на сертификат	30
Рисунок 38 - Подписание запроса на мобильном устройстве	30
Рисунок 39 - Завершение подписания запроса	31
Рисунок 40 - Выбор сертификата для управления	32
Рисунок 41 - Функции управления сертификатом	32
Рисунок 42 - Просмотр личных данных Оператора.....	33
Рисунок 43 - Настройка оповещений оператора	33
Рисунок 44 - Перечень средств аутентификации	34
Рисунок 45 - Аудит событий СЭП.....	34