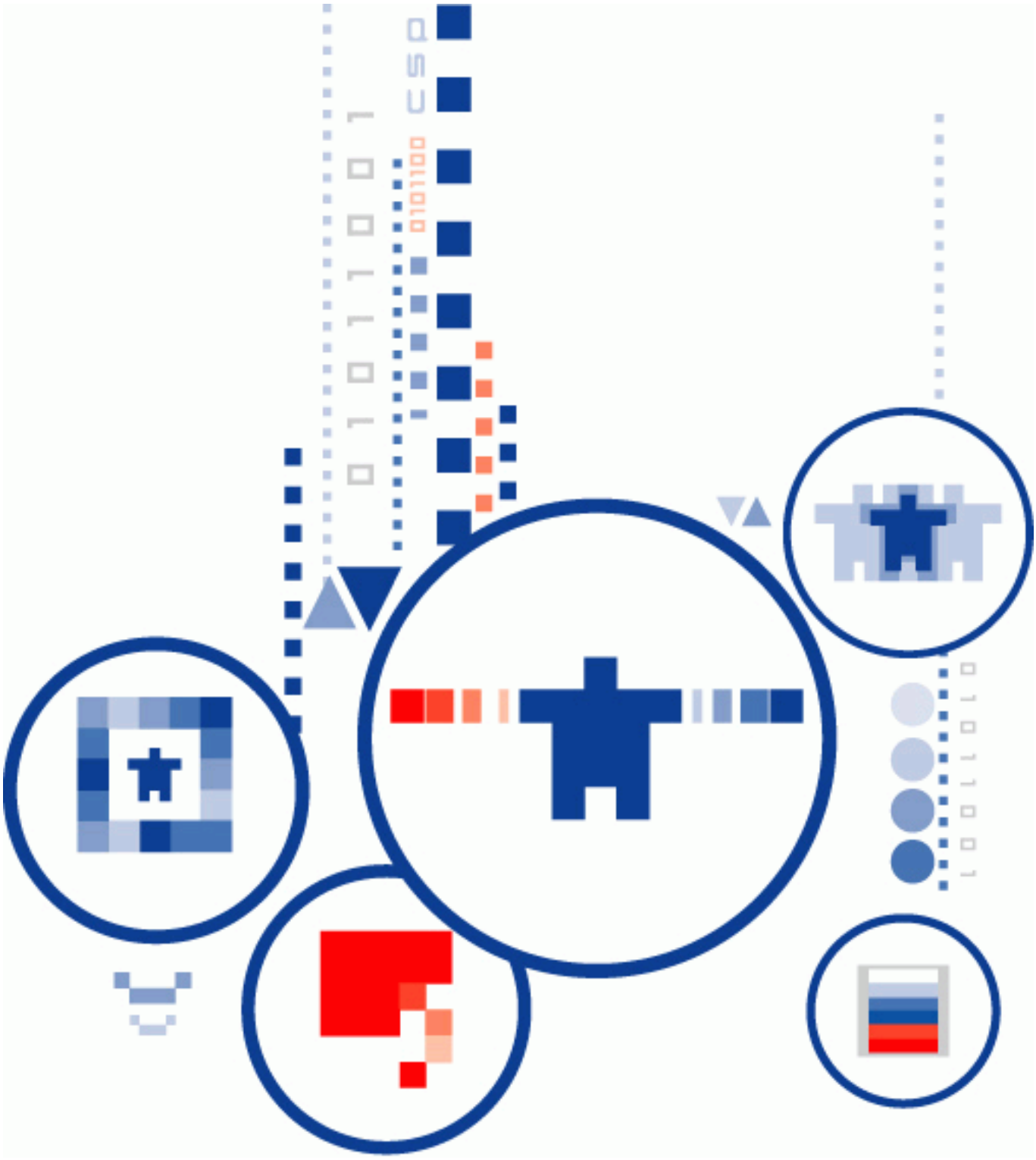
УТВЕРЖДЁН
ЖТЯИ.00082-01 90 03 06-ЛУ

ЖТЯИ.00082-01 90 03 06



ПАК «КриптоПро DSS»

Тестовый сервис электронной подписи

Инструкция Оператора СЭП

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Операторов тестового сервиса электронной подписи ООО «КРИПТО-ПРО» базе ПАК «КриптоПро DSS» (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 DSS»:

ООО «КРИПТО-ПРО»

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

Телефон: (495) 995 4820

http://www.CryptoPro.ru

https://www.cryptopro.ru/service/sign

E-mail: info@CryptoPro.ru

Содержание

1. Общие положения

Тестовый сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПАК «КриптоПро DSS» (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 операционной системы (далее – ОС) Microsoft Windows 7 или выше должно быть установлено СКЗИ «КриптоПро CSP» версии 4.0 или выше в соответствии с эксплуатационной документацией на СКЗИ. Для подключения к СЭП необходимо использовать Интернет-обозреватель Internet Explorer версии 10 (далее – браузер) или выше.

Для выпуска сертификатов первичной аутентификации Пользователя на рабочем месте должен быть установлен КриптоПро ЭЦП Browser plug-in версии 2.0.

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

- **Сертификат Тестового УЦ ООО «КРИПТО-ПРО» (УЦ 2.0)** – в хранилище «Доверенные корневые центры сертификации».
- **Сертификат Sub-TESTCA20-CA** – в хранилище «Промежуточные центры сертификации».
- **Сертификат Оператора** – в хранилище «Личное».

Для корректной работы с СЭП следует добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выбрать вкладку «*Безопасность*»,

в список надежных сайтов добавить узел https://stenddss.cryptopro.ru/ и сохранить изменения свойств (см. **Рисунок 1. Добавление в надёжные сайты**):

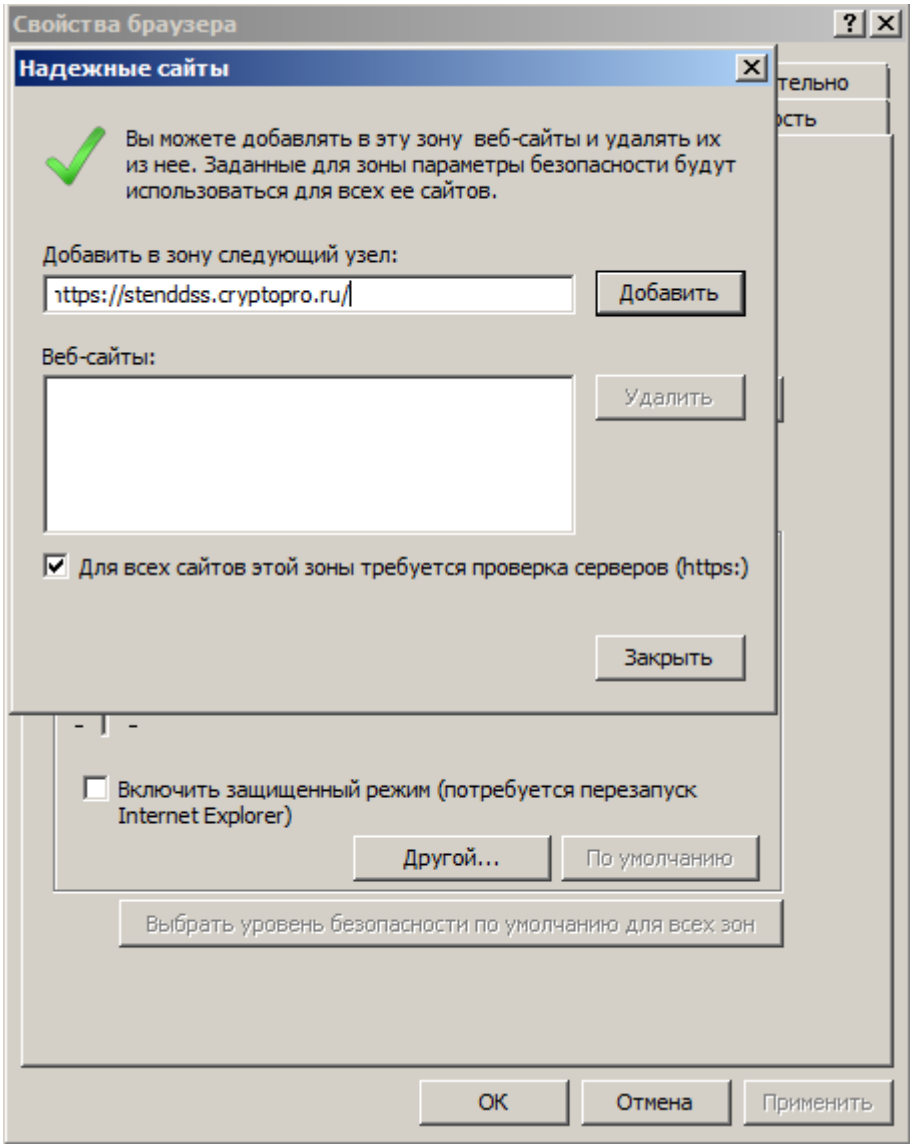


Рисунок 1. Добавление в надёжные сайты

2. Структура меню

Для работы в СЭП Оператору необходимо осуществить вход в веб-интерфейс Оператора по адресу https://stenddss.cryptopro.ru/STS/admins/[1] и выбрать пункт «Вход по сертификату», после чего в появившемся окне подтверждения сертификата выбрать сертификат Оператора и нажать кнопку «*ОК*» (см. **Рисунок 2. Выбор сертификата**).

[1] Для каждого конкретного экземпляра СЭП следует использовать настройки доступа, предоставленные ООО «КРИПТО-ПРО». В настоящем документе в качестве примера используется экземпляр «STS».

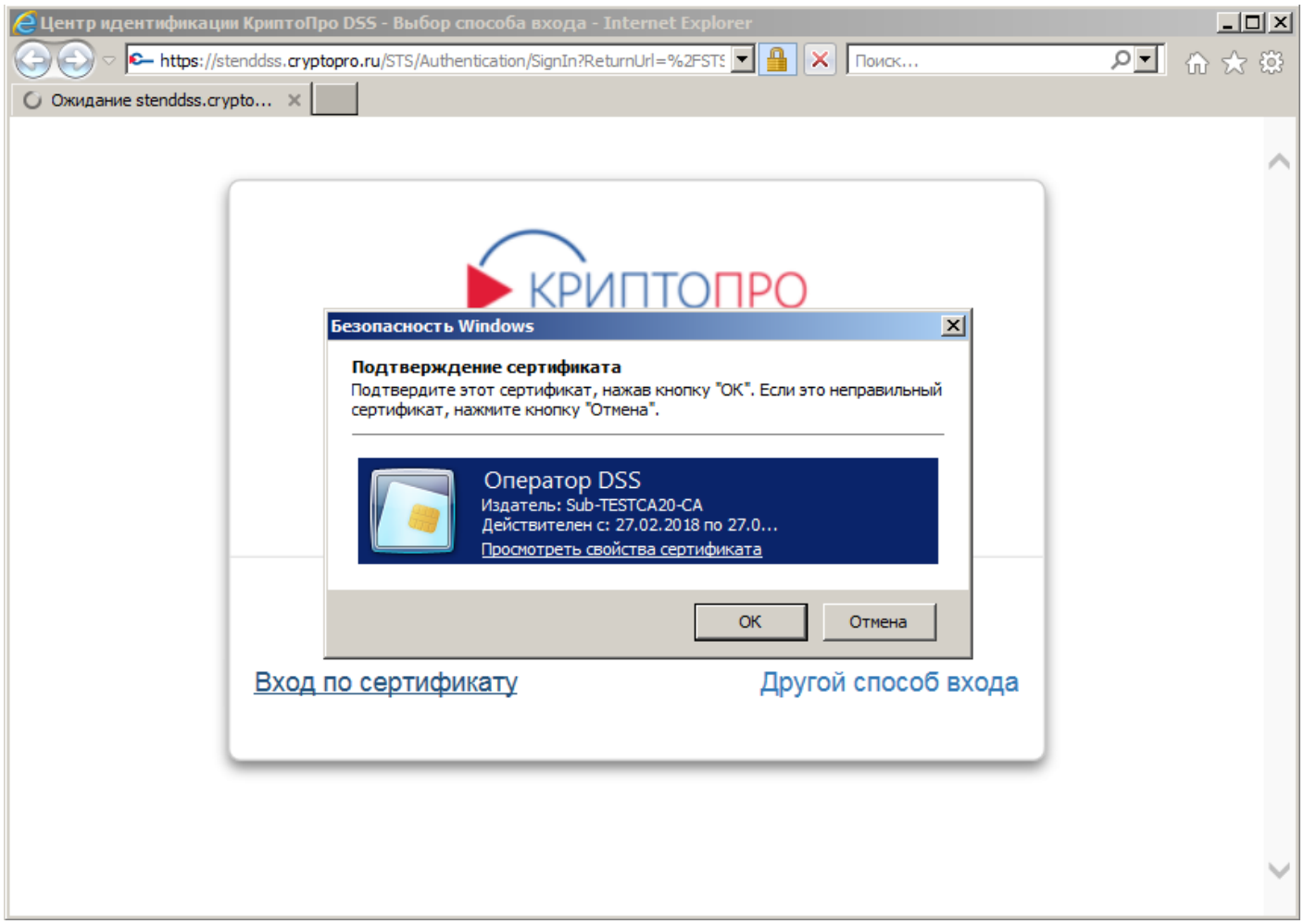


Рисунок 2. Выбор сертификата

После подтверждения сертификата и ввода ПИН-кода ключевого контейнера будет отображена начальная страница веб-интерфейса Оператора (см. **Рисунок 3. Начальная страница веб-интерфейса Оператора**).

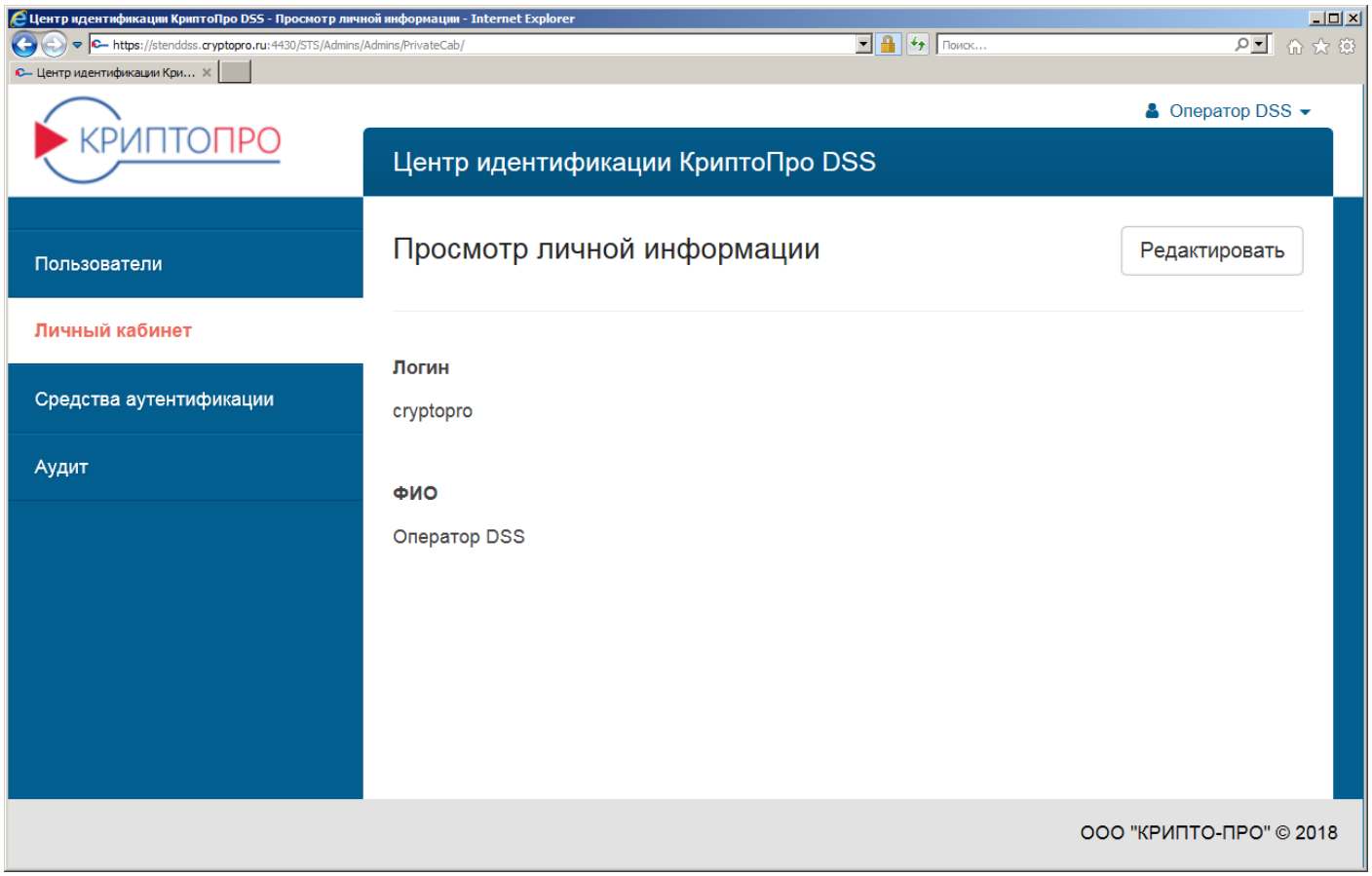


Рисунок 3. Начальная страница веб-интерфейса Оператора

В меню начальной страницы Оператора доступны 4 раздела:

- «*Пользователи*».
- «*Личный кабинет*».
- «*Средства аутентификации*».
- «*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 нужно нажать кнопку «*Создать нового пользователя*» (см. **Рисунок 4. Создание нового Пользователя**).

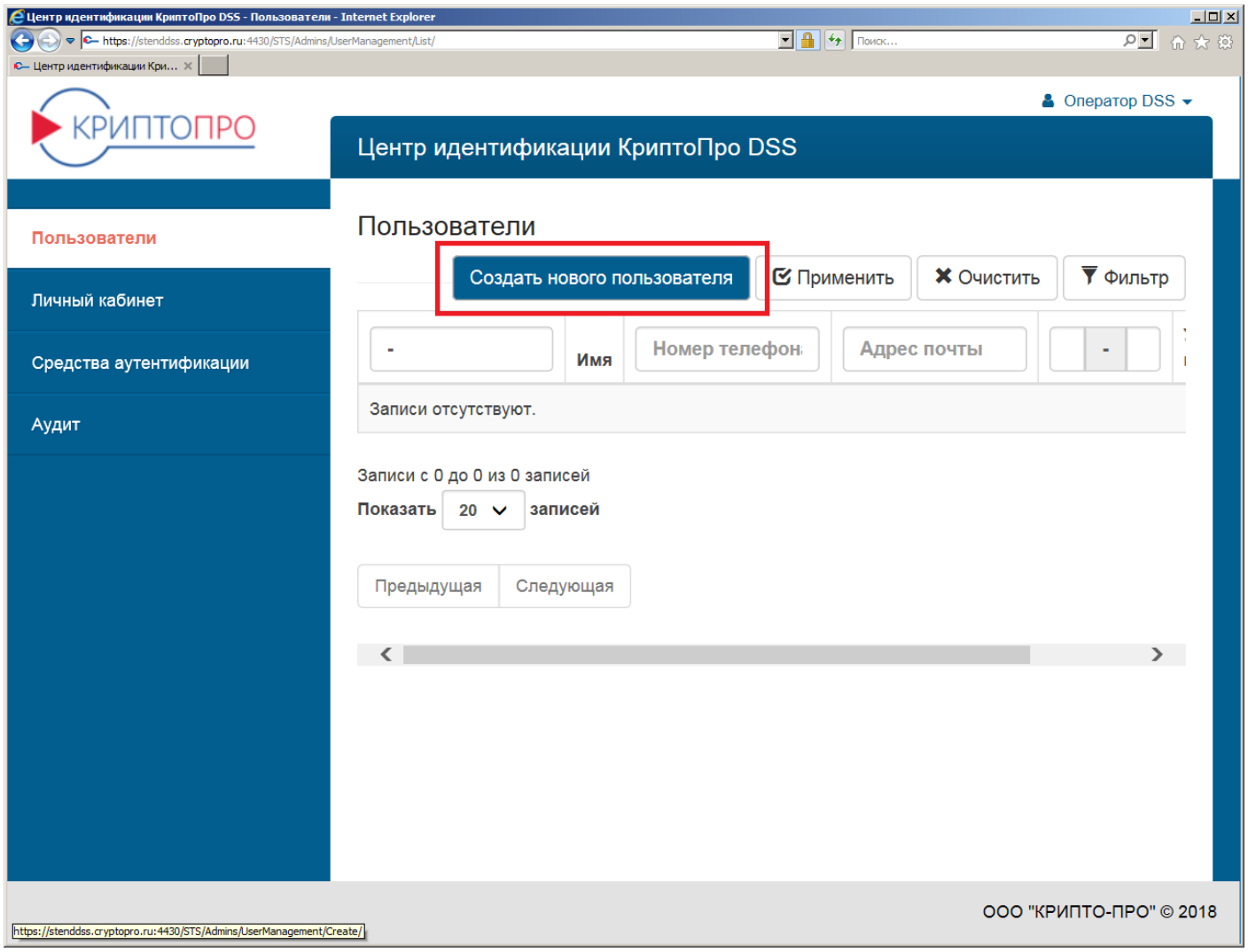


Рисунок 4. Создание нового Пользователя

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

После корректного заполнения всех полей формы следует нажать кнопку «*Создать*» (см. **Рисунок 5. Ввод сведений о Пользователе**).

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

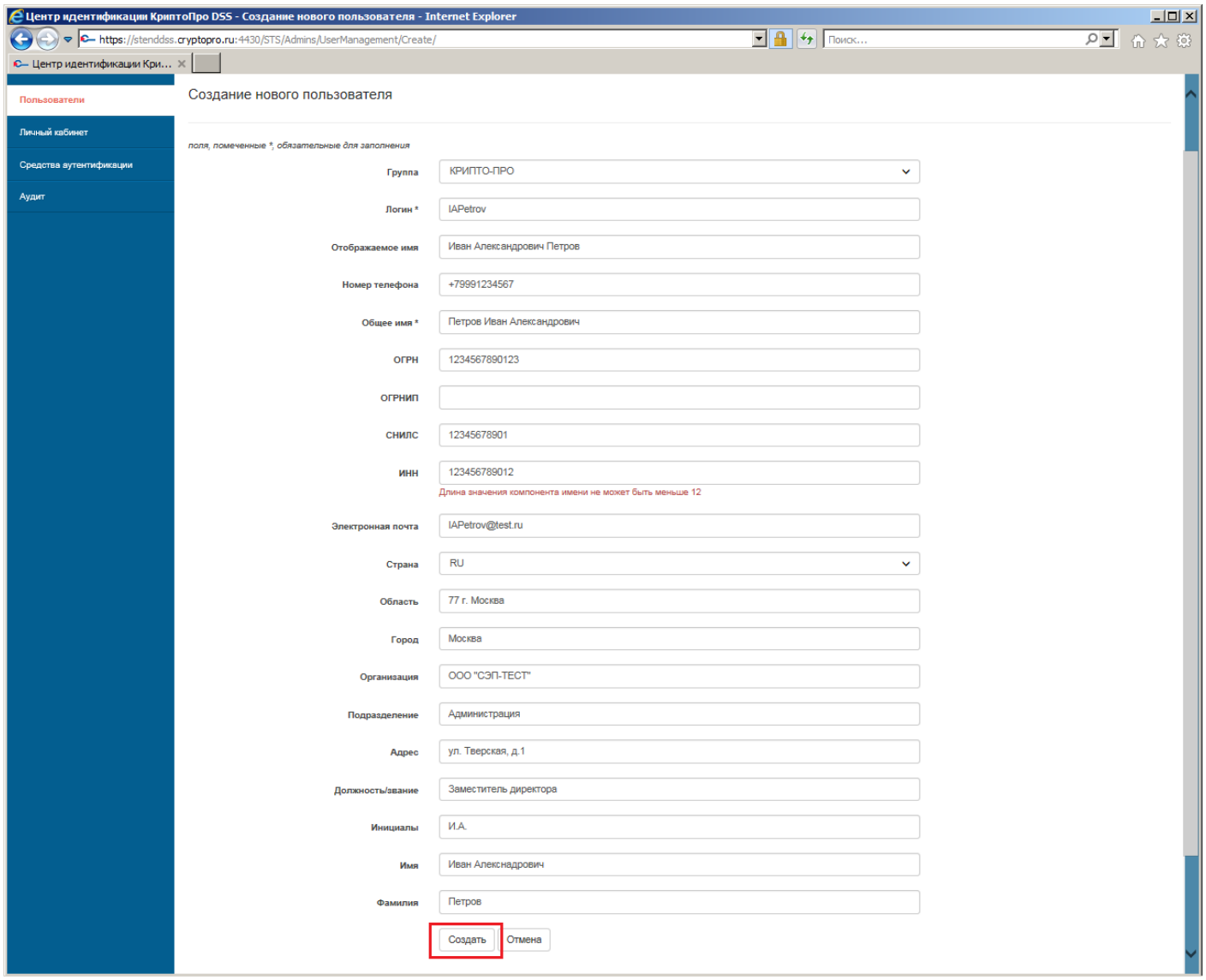


Рисунок 5. Ввод сведений о Пользователе

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 6. Управление Пользователями СЭП**):

- «*Редактировать*» – редактирование атрибутов Пользователя.
- «*Настройки аутентификации*» – редактирование методов аутентификации, подтверждения и доступа Пользователя к операциям в СЭП.
- «*Заблокировать*» – блокировка или разблокировка Пользователя.

- «*Удалить*» – удаление Пользователя.
- «*Сертификаты*» – управление сертификатами Пользователя.

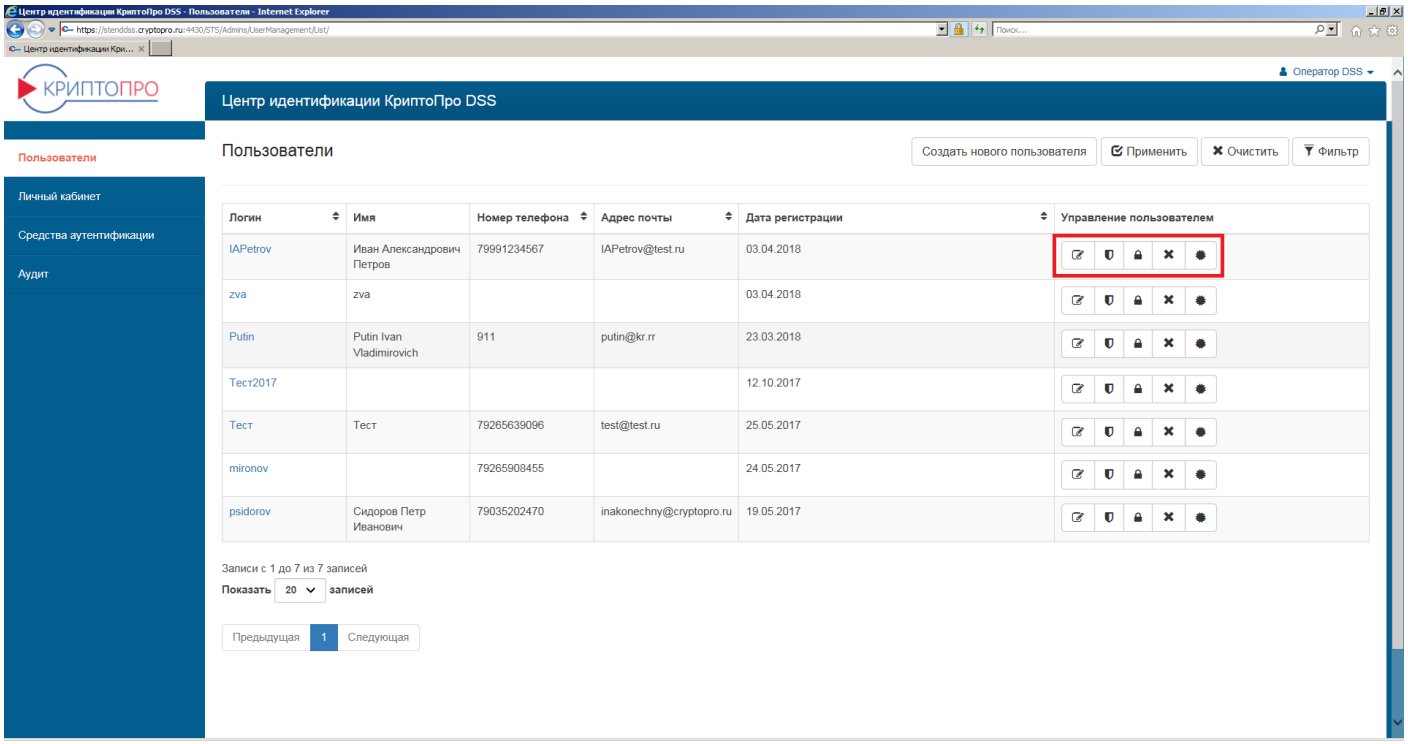


Рисунок 6. Управление Пользователями СЭП

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 7. Редактирование атрибутов Пользователя**).

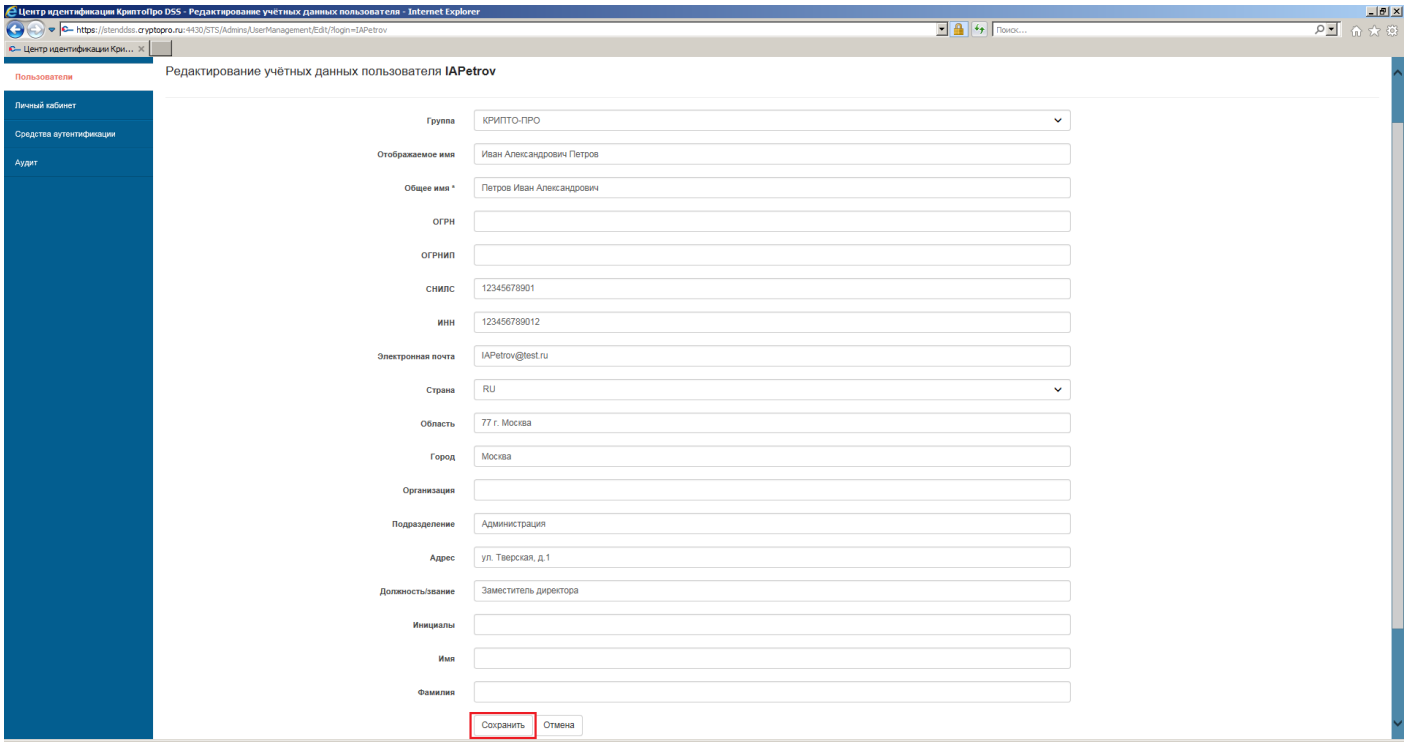


Рисунок 7. Редактирование атрибутов Пользователя

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. 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 в СЭП в мобильном приложении «КриптоПро myDSS».

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 возможно импортировать компоненты имени Пользователя из существующего сертификата (кнопка «*Заполнить компоненты имени из сертификата*»), либо выпустить сертификат в соответствии с данными Пользователя, заданными Оператором при регистрации Пользователя. Для выпуска сертификата для первичной аутентификации Пользователя нужно нажать кнопку «*Выпустить сертификат*» (см. **Рисунок 8. Выпуск сертификата для первичной аутентификации Пользователя**).

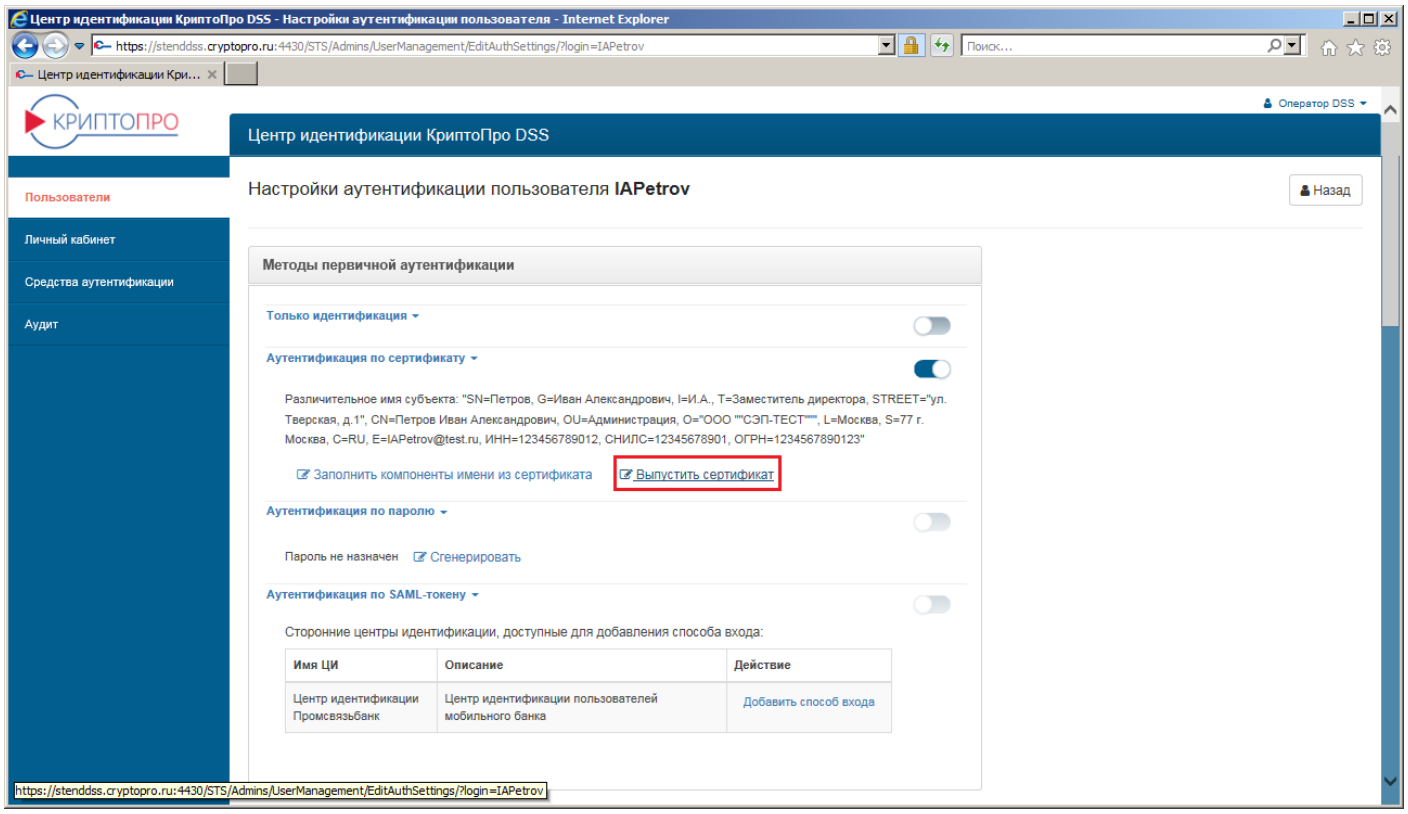


Рисунок 8. Выпуск сертификата для первичной аутентификации Пользователя

Далее Оператору необходимо задать Удостоверяющий центр (УЦ) для выпуска сертификата и криптографический провайдер для формирования ключевой информации (см. **Рисунок 9. Формирование ключевой информации**).

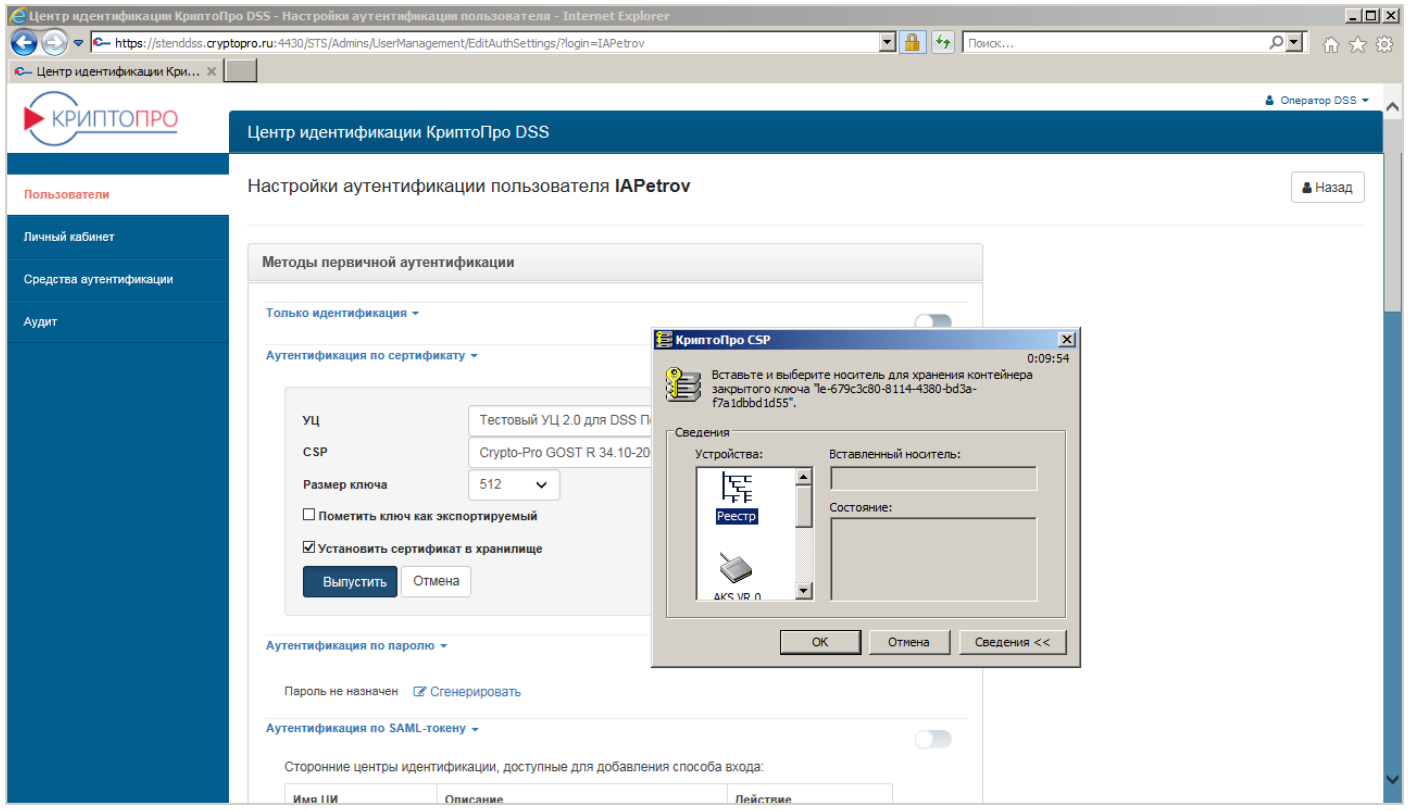


Рисунок 9. Формирование ключевой информации

В случае если требуется, чтобы ключевой контейнер был экспортируемым, нужно установить флажок «*Пометить ключ как экспортируемый*».

В случае если требуется установить выпущенный сертификат в ключевой контейнер, следует установить флажок «*Установить сертификат в хранилище*».

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 «*Сгенерировать*» (см. **Рисунок 10. Генерация пароля для первичной аутентификации Пользователя**).

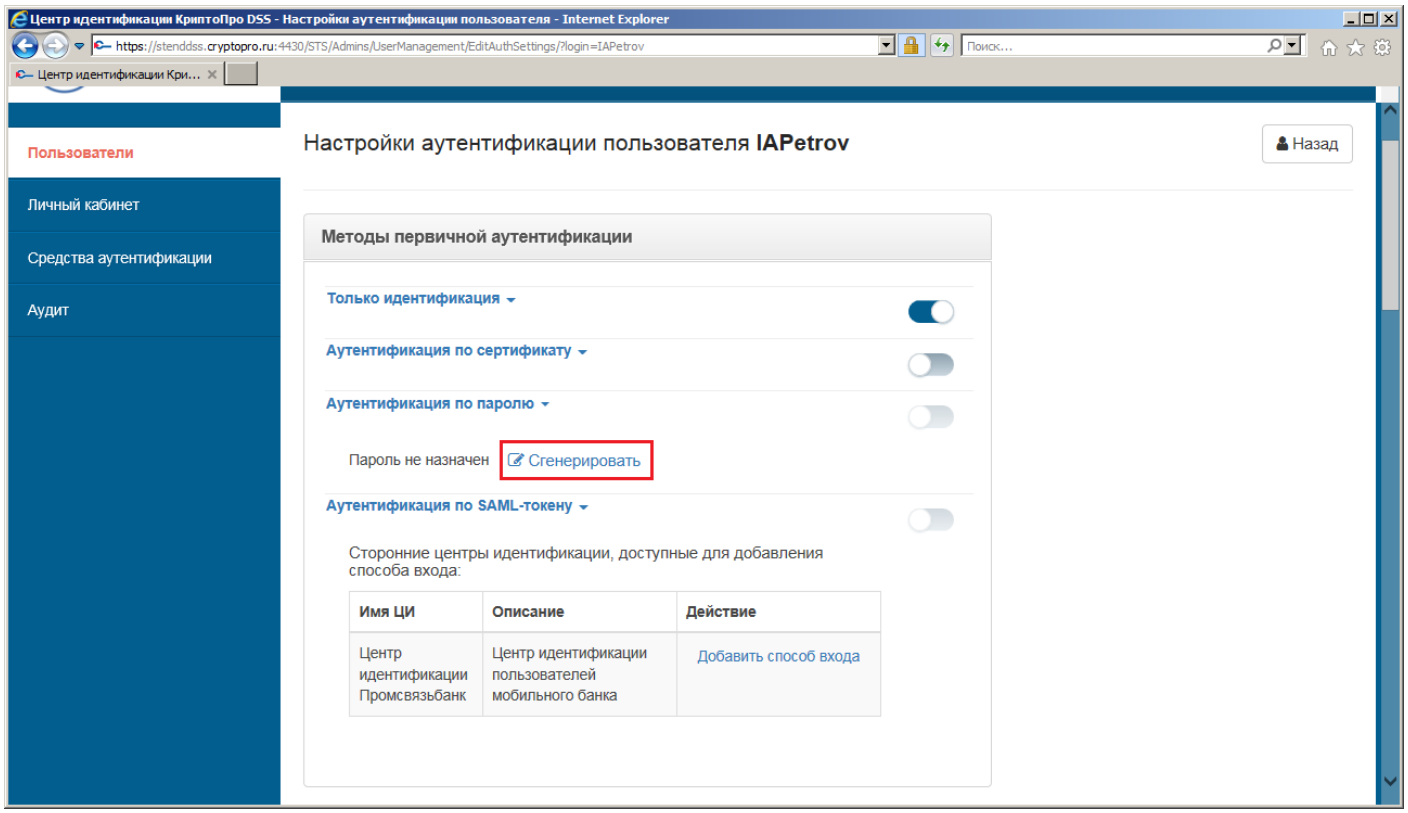


Рисунок 10. Генерация пароля для первичной аутентификации Пользователя

В появившемся диалоге есть возможность отобразить сгенерированный пароль на экране, либо вывести его на печать. Далее нужно нажать кнопку «*Создать новый пароль*» (см. **Рисунок 11. Способ отображения созданного пароляРисунок 11.**).

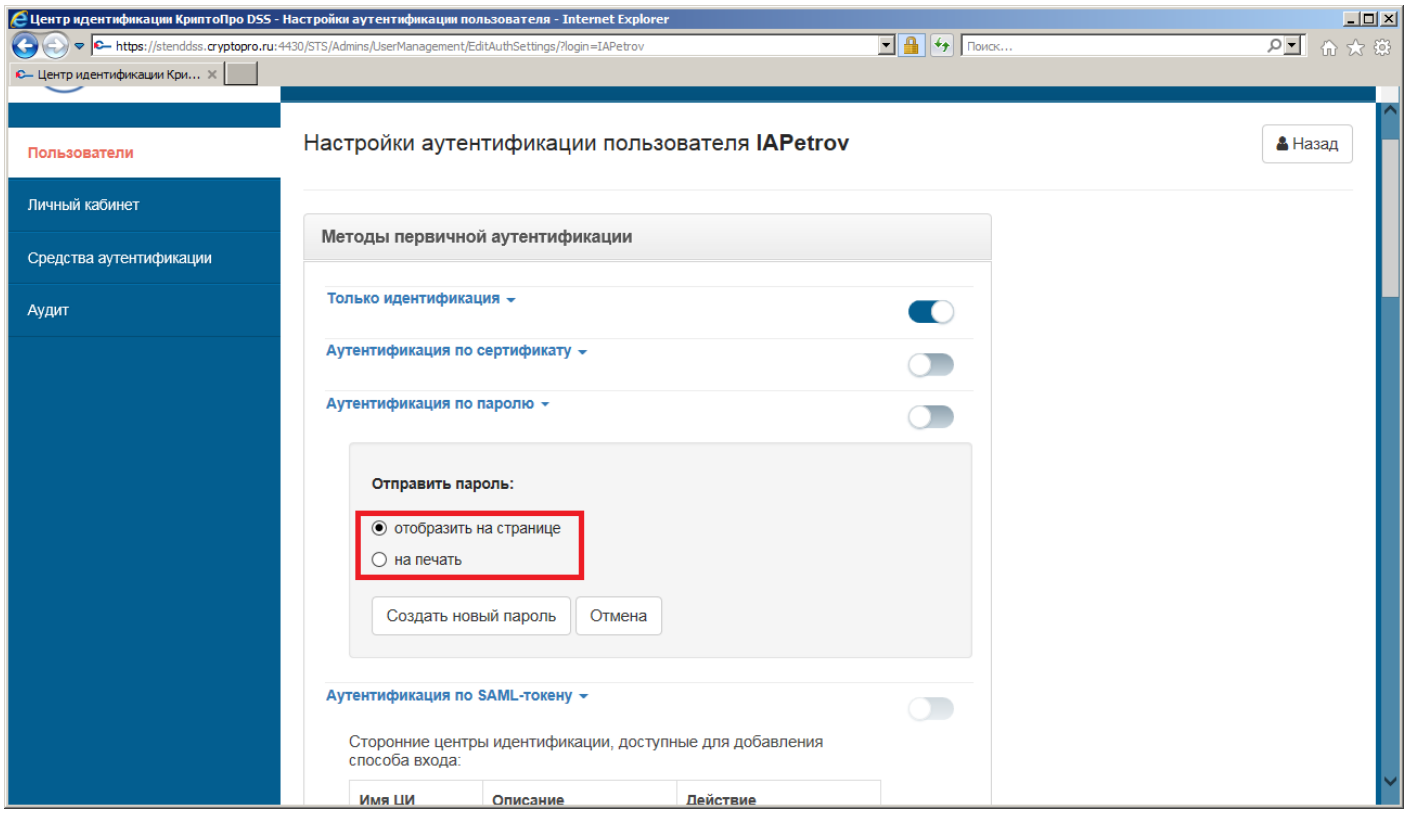


Рисунок 11. Способ отображения созданного пароля

После нажатия кнопки «Создать новый пароль» отобразится сообщение об успешной смене пароля первичной аутентификации Пользователя, а сам пароль будет выведен, соответственно, на экран или принтер (см. **Рисунок 12. Успешная смена (задание) пароля**). Для включения первичной аутентификации по паролю нужно установить переключатель «*Аутентификация по паролю*» в группе «*Первичная аутентификация*» в активное положение.

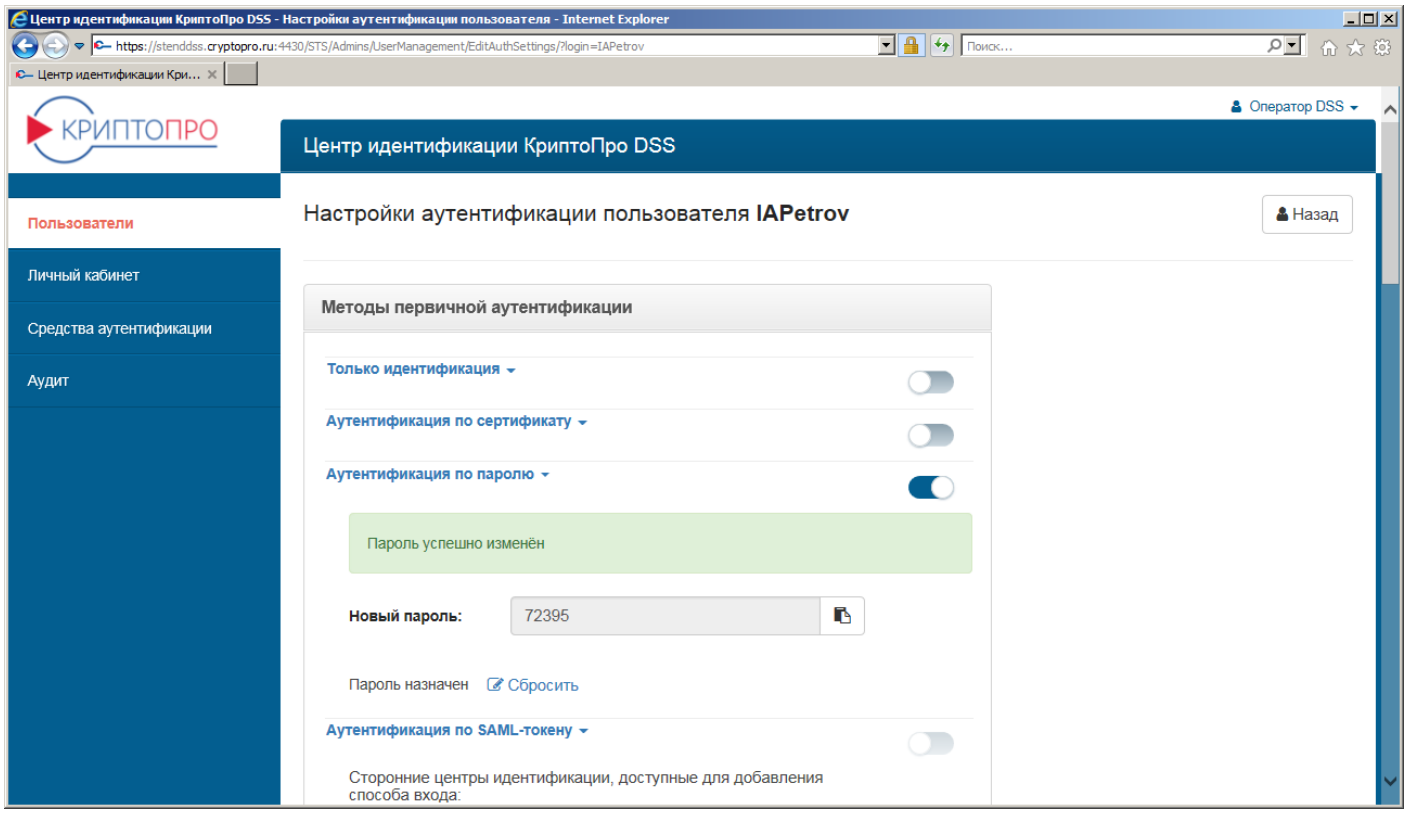


Рисунок 12. Успешная смена (задание) пароля

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 «*Изменить*», после чего ввести номер телефона в поле ввода и нажать кнопку «*Сохранить*» (см. **Рисунок 13. Настройка аутентификации по SMS**, **Рисунок 14. Ввод номера Пользователя для отправки SMS**). Для включения вторичной аутентификации по SMS необходимо установить переключатель «*Аутентификация по SMS*» в группе «*Вторичная аутентификация*» в активное положение.

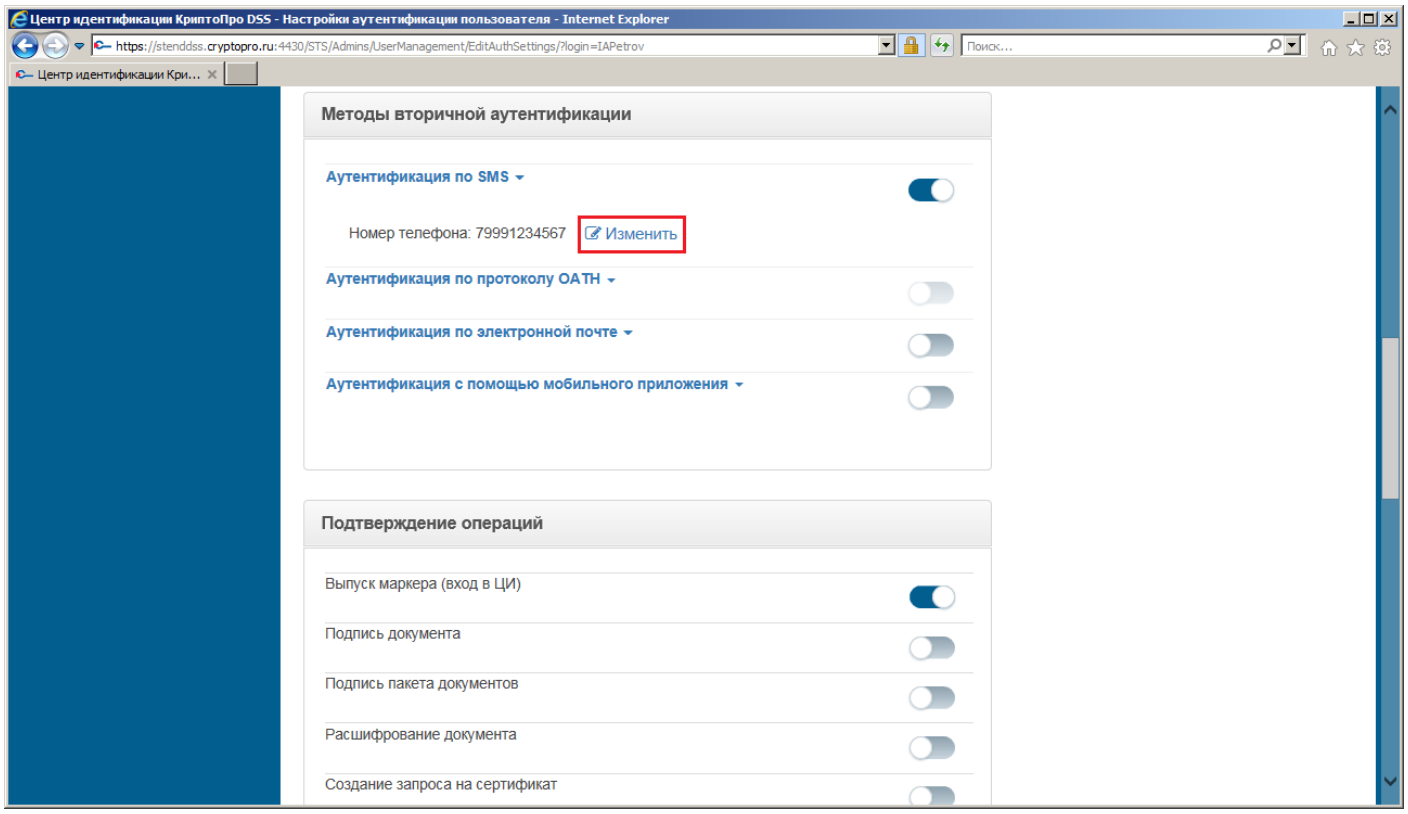


Рисунок 13. Настройка аутентификации по SMS

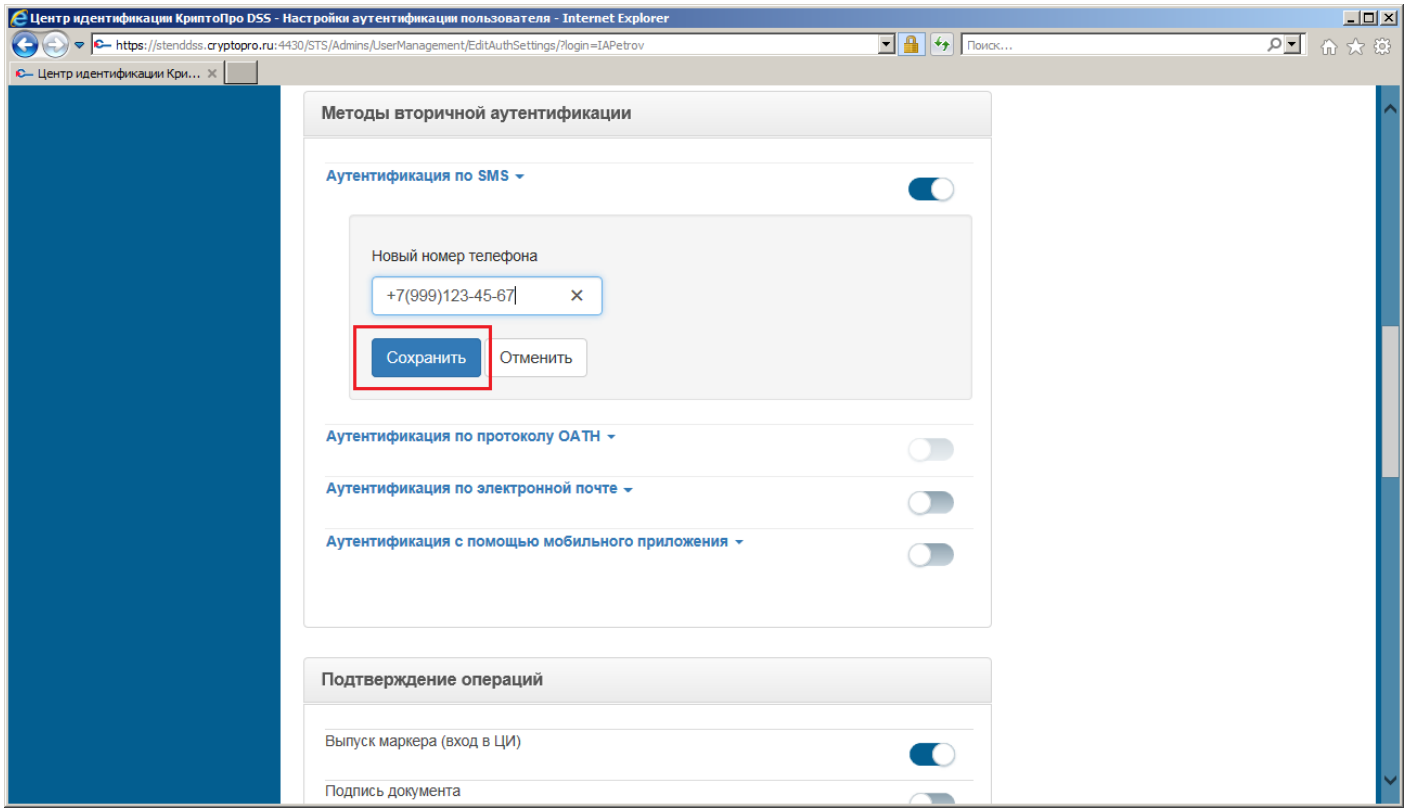


Рисунок 14. Ввод номера Пользователя для отправки SMS

3.2.2.2.2 Настройка аутентификации по протоколу OATH

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

аутентификации» раскрыть блок «*Аутентификация по протоколу OATH*» и нажать ссылку «*Задать*» (см. **Рисунок 15. Настройка аутентификации по протоколу OATH**).

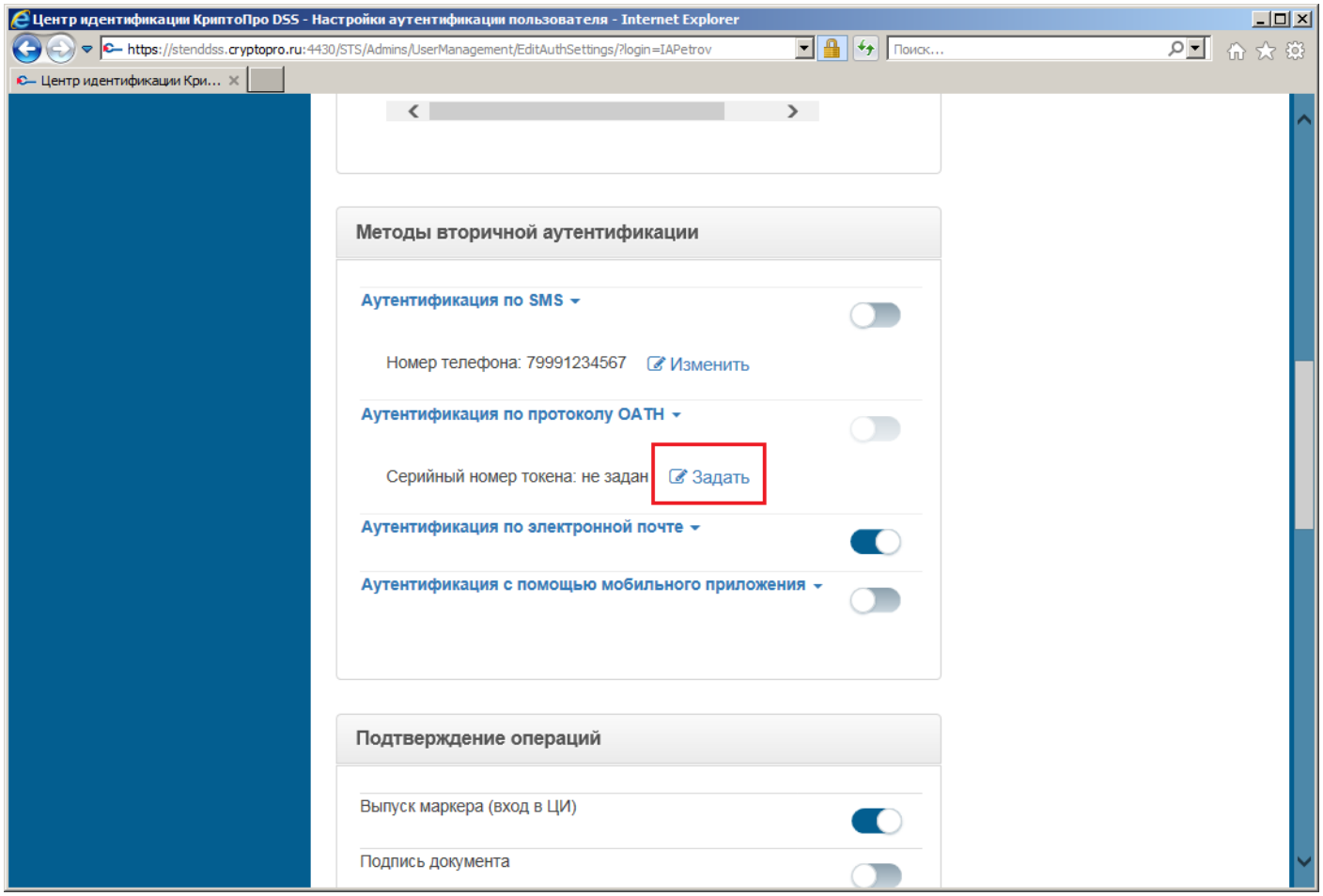


Рисунок 15. Настройка аутентификации по протоколу OATH

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 16. 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.

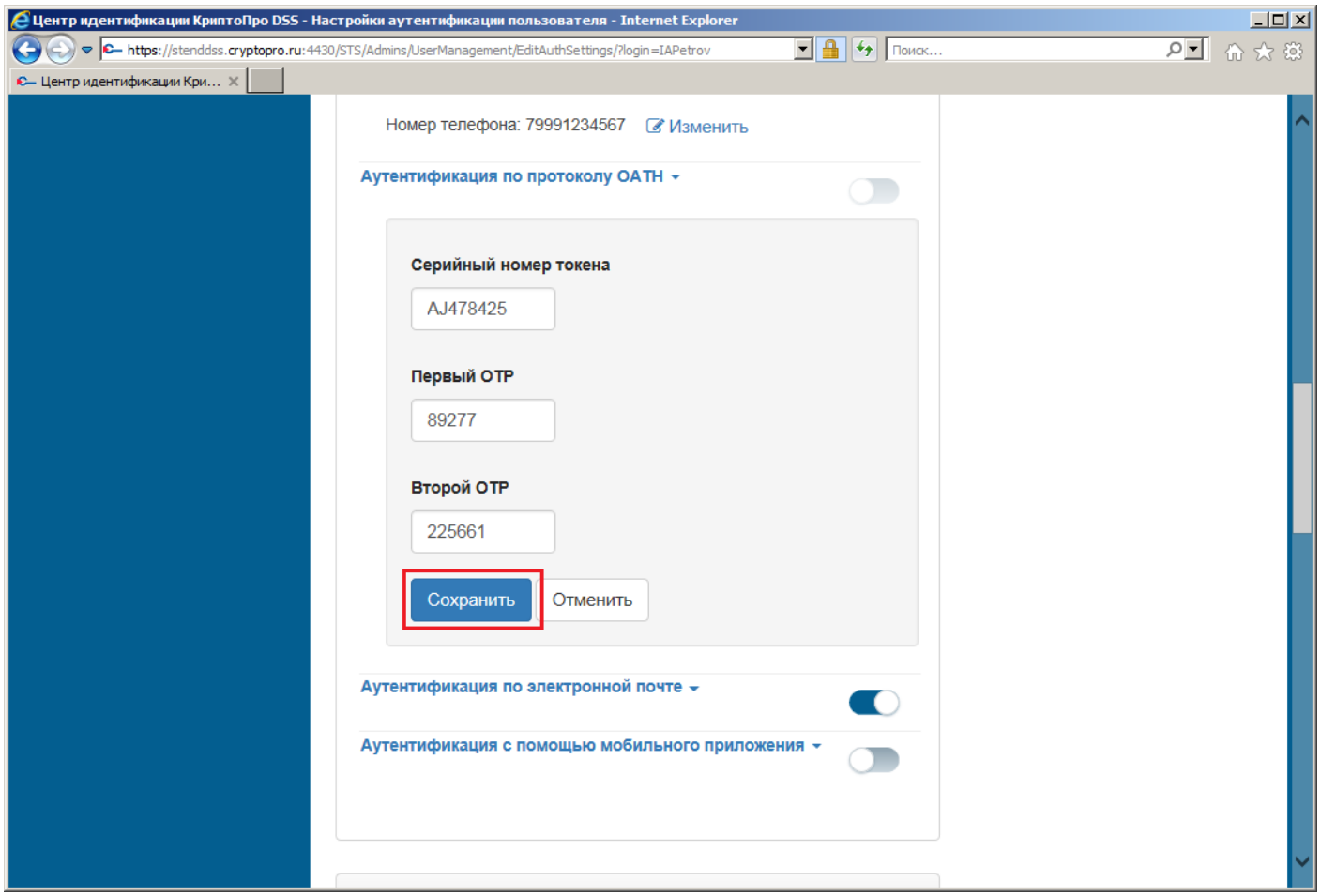


Рисунок 16. Ввод параметров аутентификации по протоколу OATH

3.2.2.2.3 Настройка аутентификации по электронной почте

Для настройки вторичной аутентификации Пользователя по электронной почте нужно в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация по электронной почте*» и нажать кнопку «*Изменить*», после чего ввести номер телефона в поле ввода нажать кнопку «*Сохранить*» (см. **Рисунок 17. Настройка аутентификации по электронной почте**, **Рисунок 18. Ввод параметров аутентификации по электронной почте**). Для включения вторичной аутентификации по электронной почте необходимо установить переключатель «*Аутентификация по электронной почте*» в группе «*Вторичная аутентификация*» в активное положение.

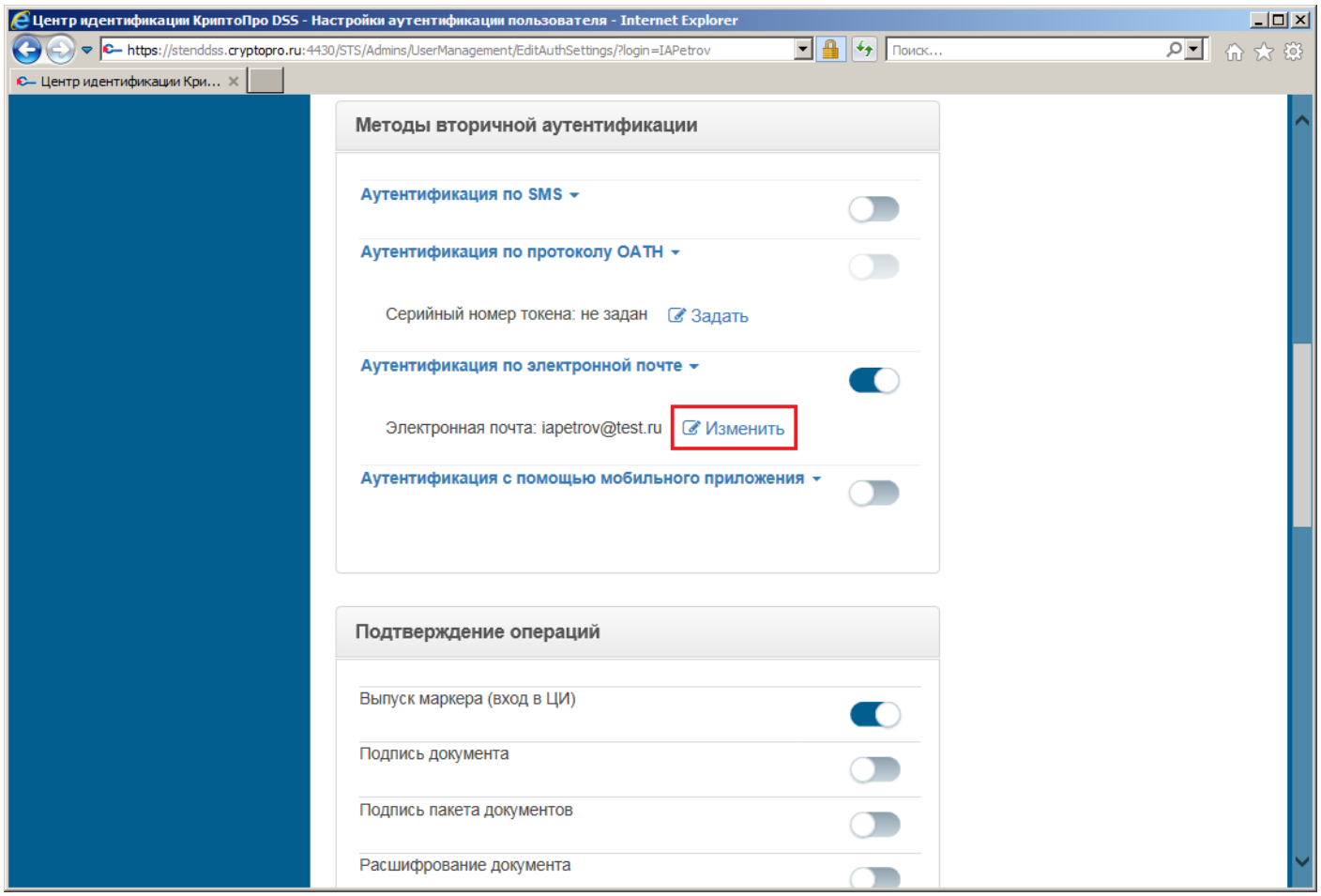


Рисунок 17. Настройка аутентификации по электронной почте

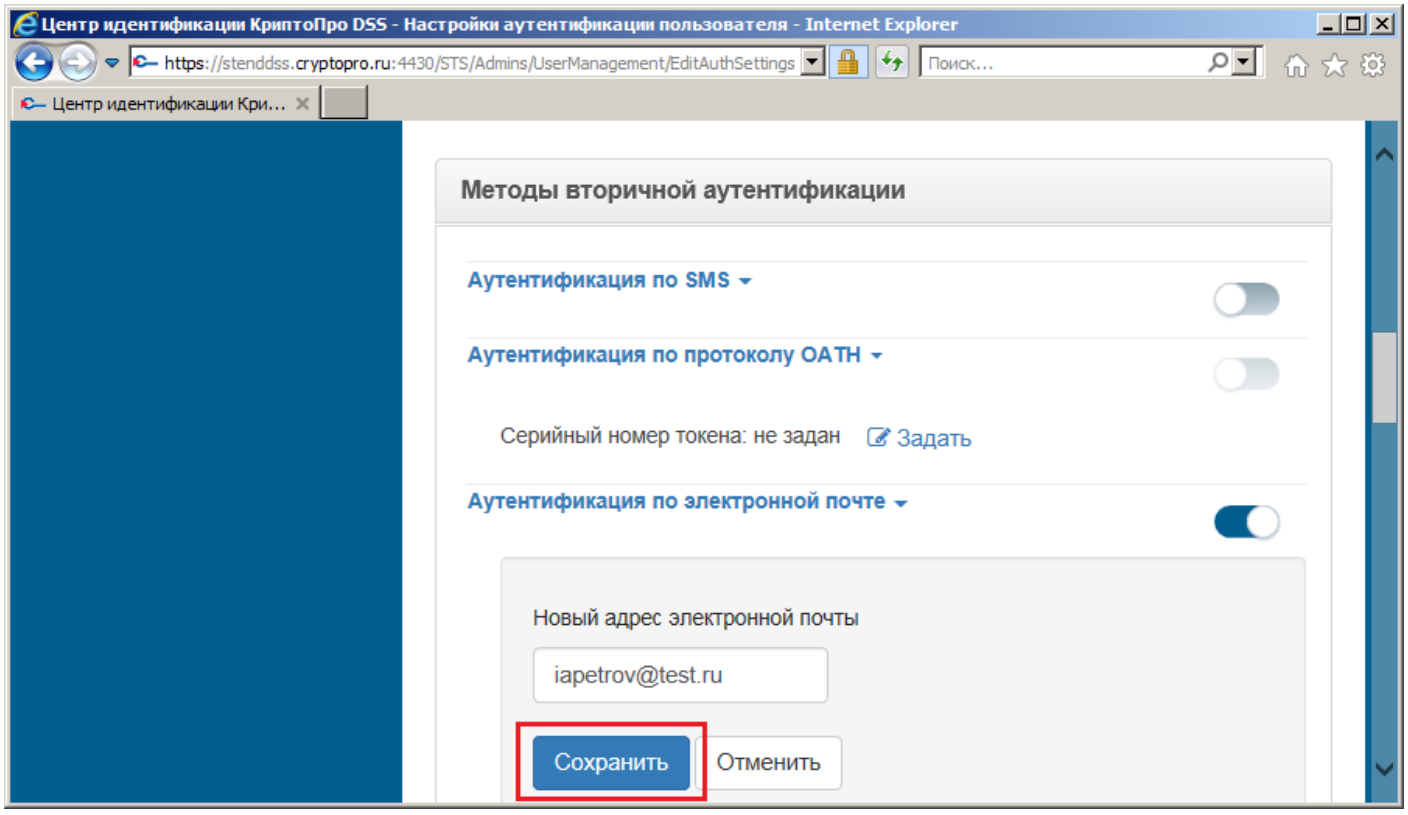


Рисунок 18. Ввод параметров аутентификации по электронной почте

3.2.2.2.4 Настройка аутентификации с помощью мобильного приложения

Для настройки вторичной аутентификации Пользователя с помощью мобильного приложения «КриптоПро myDSS» (далее – myDSS) нужно в группе «*Методы вторичной аутентификации*» раскрыть блок «*Аутентификация с помощью мобильного приложения*» и нажать кнопку «*Запросить*» (см. **Рисунок 19. Настройка аутентификации с помощью мобильного приложения**).

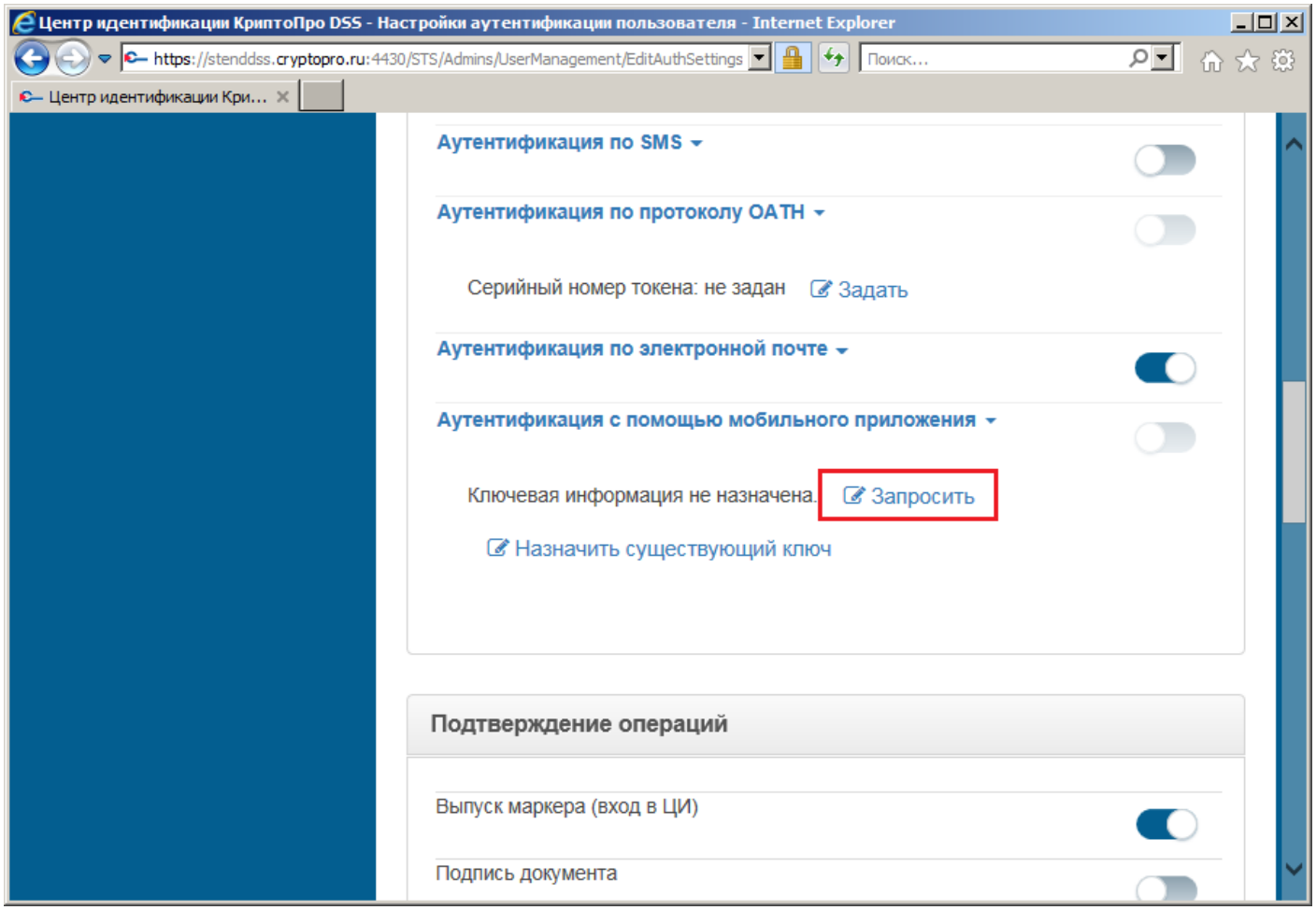


Рисунок 19. Настройка аутентификации с помощью мобильного приложения

Далее необходимо выбрать способ отправки секретного ключа для активации мобильного приложения myDSS (см. **Рисунок 20. Выбор способа доставки секретного ключа**).

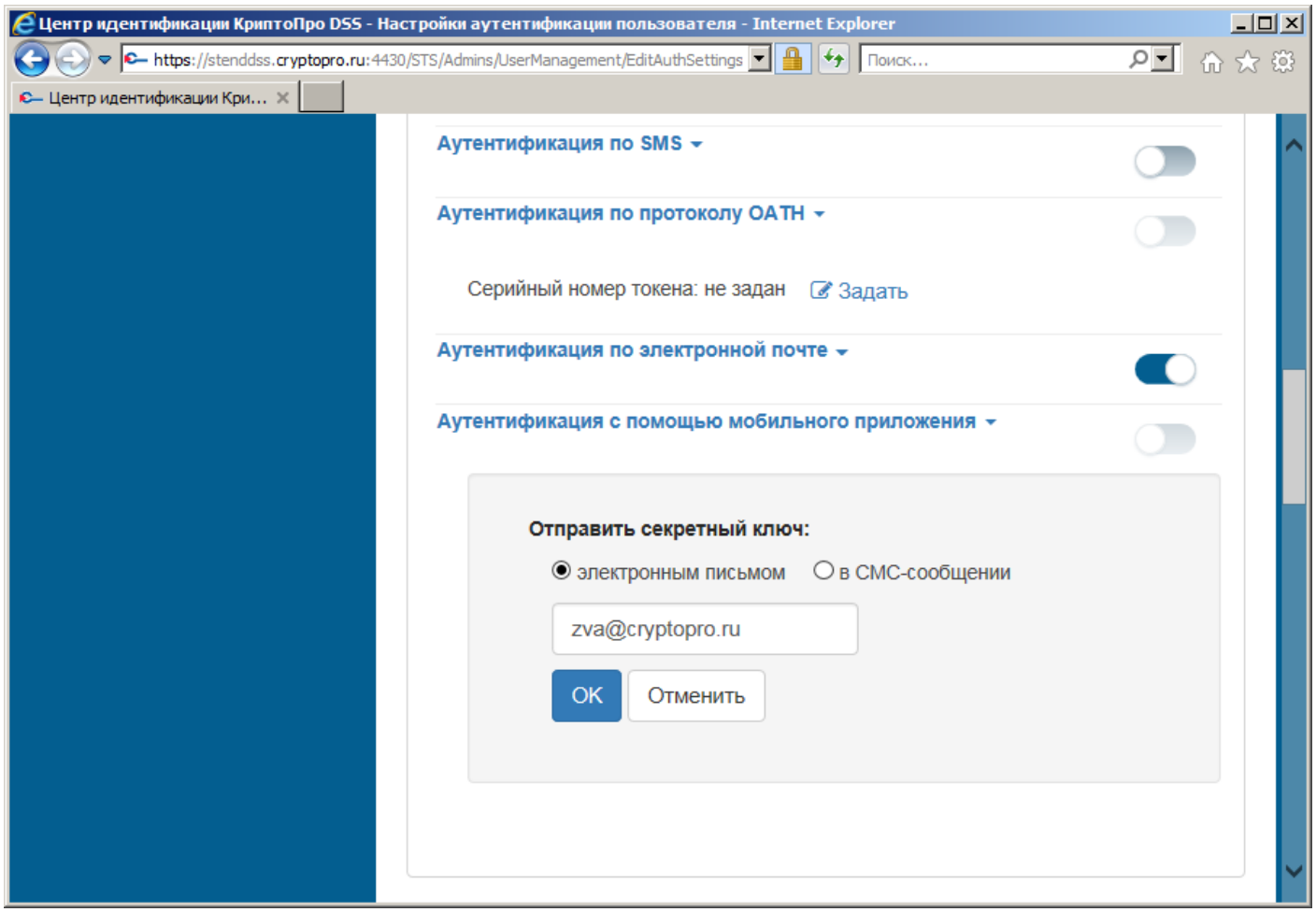


Рисунок 20. Выбор способа доставки секретного ключа

После нажатия кнопки «*ОК*» секретный ключ будет отправлен Пользователю выбранным способом (сообщение вида: «Код активации ключа в myDSS: 123456»), а СЭП предложит скачать QR-код (см. **Рисунок 21. Скачивание QR-кода**, **Рисунок 22. QR-код**), который Пользователю нужно будет отсканировать в приложении myDSS (доступно в Google Play (Android), App Store (iOS)). Для включения вторичной аутентификации по мобильному приложению нужно установить переключатель «*Аутентификация по мобильному приложению*» в группе «*Вторичная аутентификация*» в активное положение.

После первого запуска мобильное приложение myDSS предложит Пользователю отсканировать полученный ранее QR-код. Как только QR-код будет успешно отсканирован, Пользователь должен ввести полученный им ранее секретный ключ. Далее предложение myDSS предложит создать ключ на устройстве пользователя, для чего нужно будет задать имя и пароль доступа к ключу. После выполнения всех описанных выше действий Пользователю станет доступна вторичная аутентификация с

помощью мобильного приложения myDSS (см. **Рисунок 23. Создание ключей в мобильном приложении myDSS**).

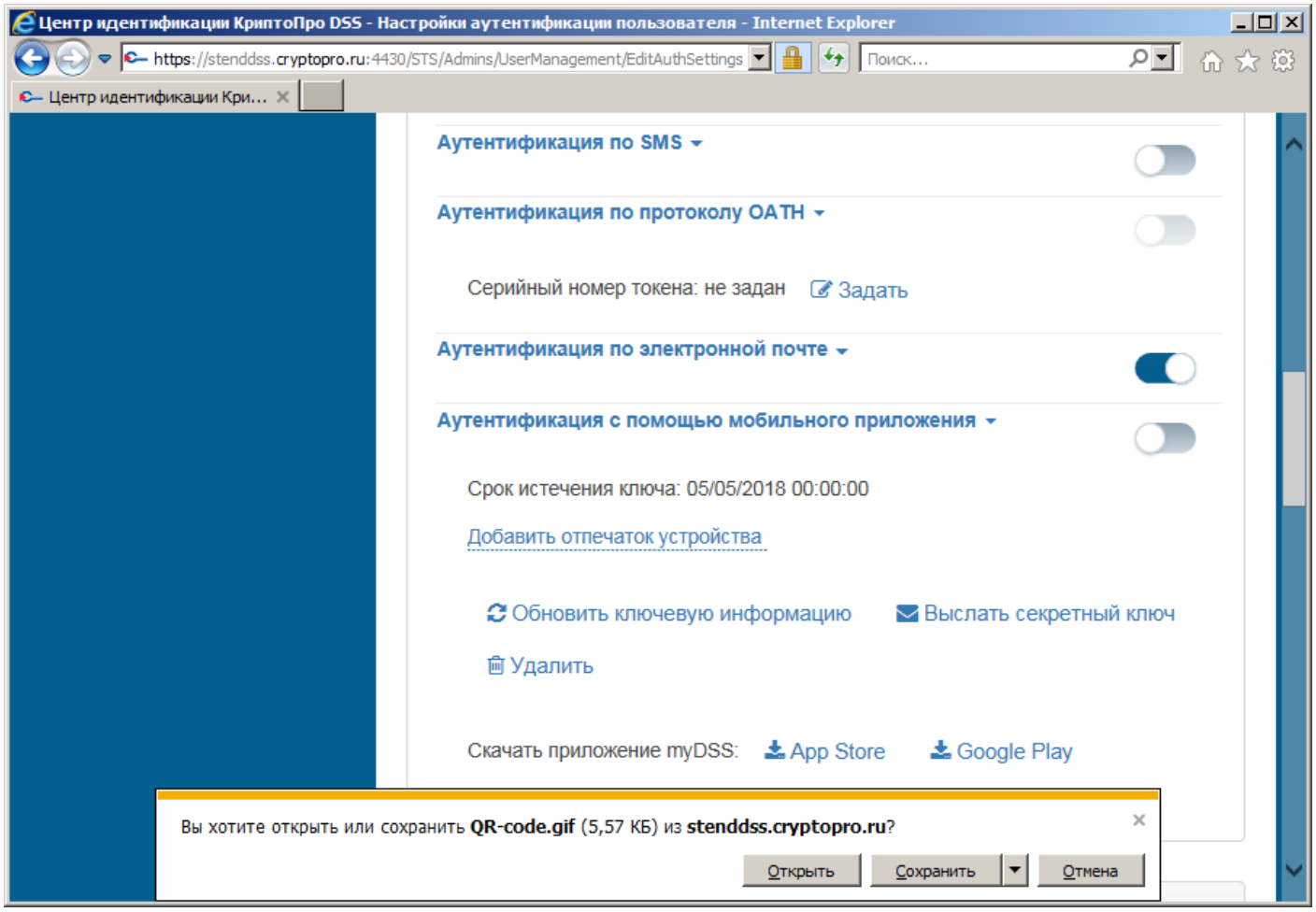


Рисунок 21. Скачивание QR-кода

Рисунок 22. QR-код

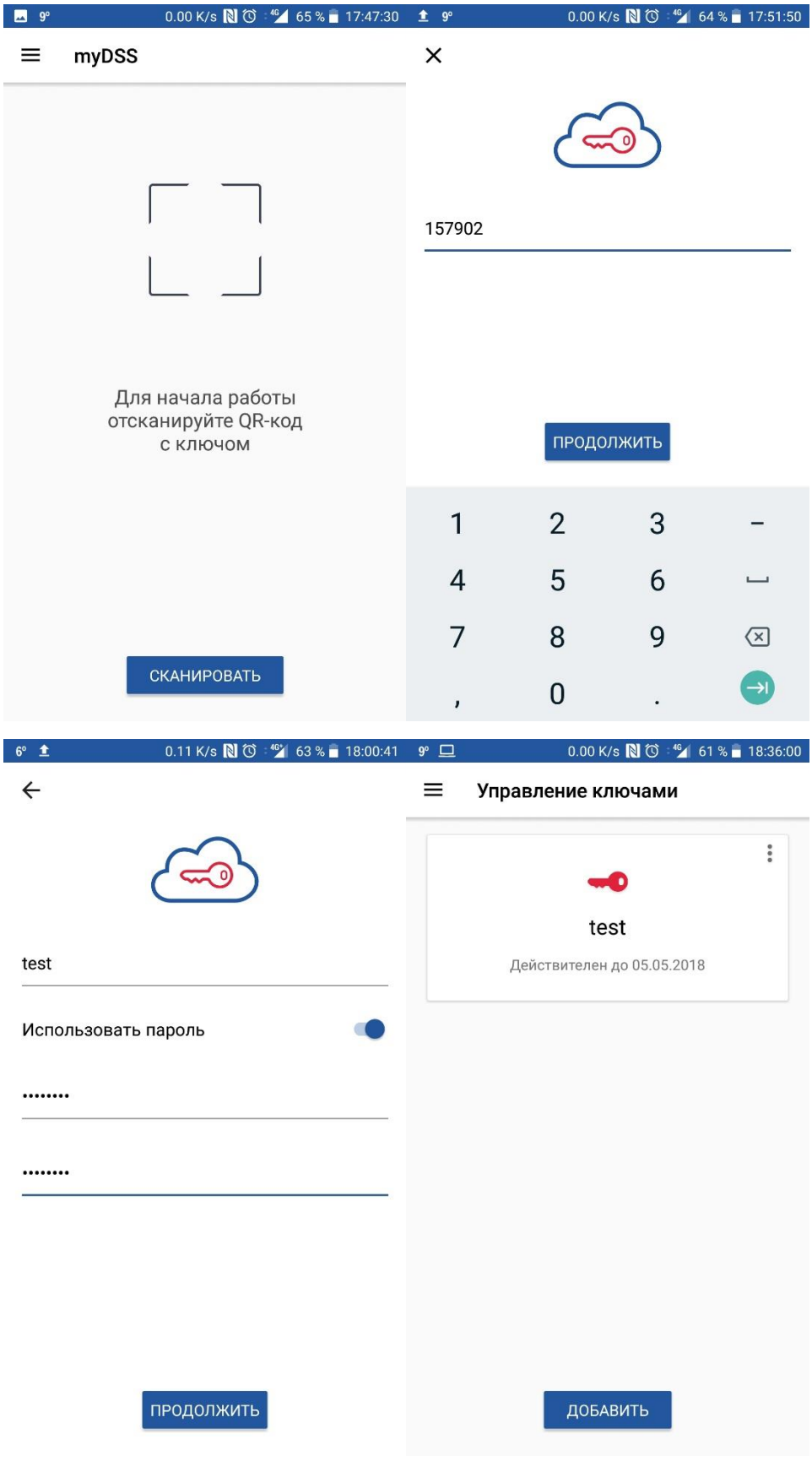


Рисунок 23. Создание ключей в мобильном приложении myDSS

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.
- 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 параметрах настройки аутентификации Пользователя (см. **Рисунок 24. Настройка подтверждения и доступа Пользователя к операциям СЭП**).

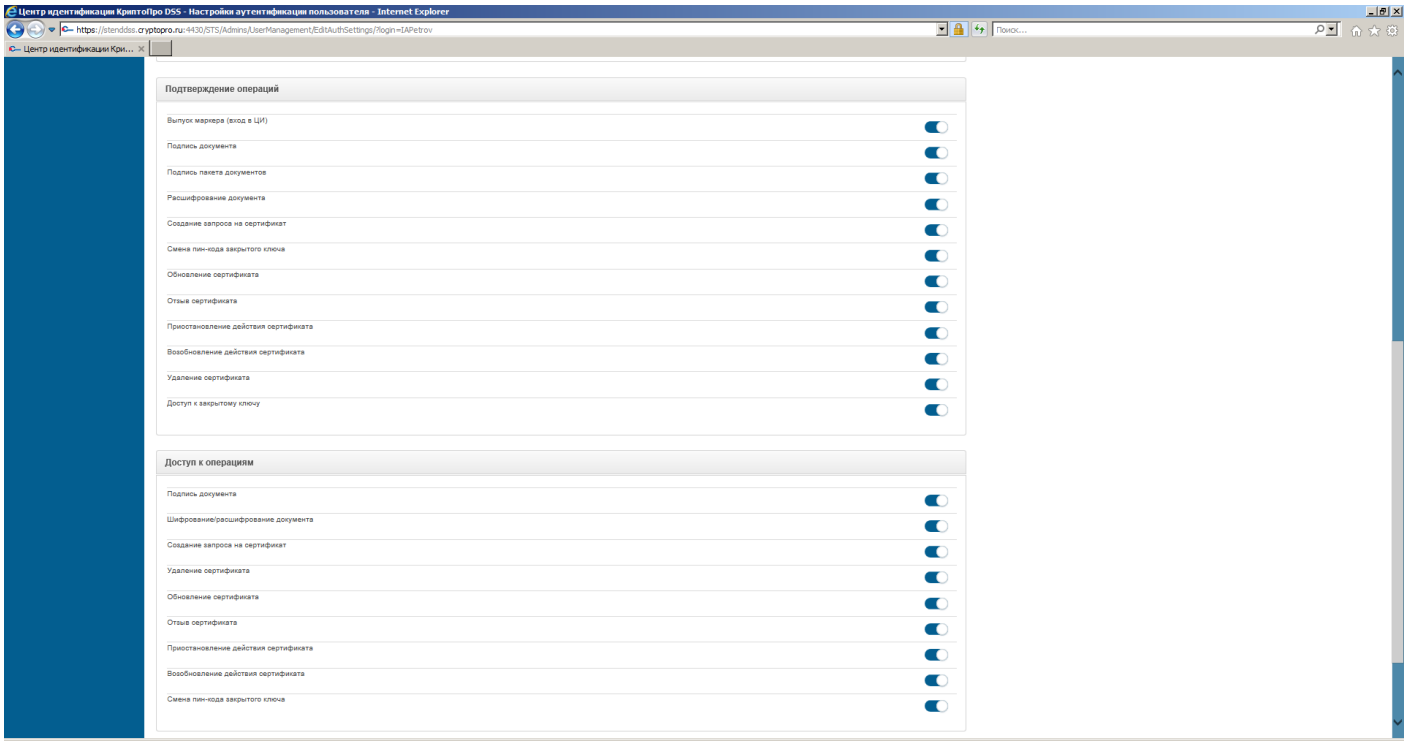


Рисунок 24. Настройка подтверждения и доступа Пользователя к операциям СЭП

3.2.3. Блокировка или разблокировка Пользователя

Для блокировки, либо разблокировки Пользователя нужно нажать на значок «*Заблокировать*», далее утвердительно ответить на запрос о блокировке/разблокировке Пользователя (см. **Рисунок 25. Блокировка и разблокировка Пользователя**). При успешной блокировке (разблокировке) Пользователя значок «*Заблокировать*» меняется соответственно на изображение открытого (закрытого) замка.

3.2.4. Удаление Пользователя

Для удаления Пользователя необходимо нажать на значок «*Удалить*», далее утвердительно ответить на запрос об удалении Пользователя (см. **Рисунок 26. Удаление Пользователя**).

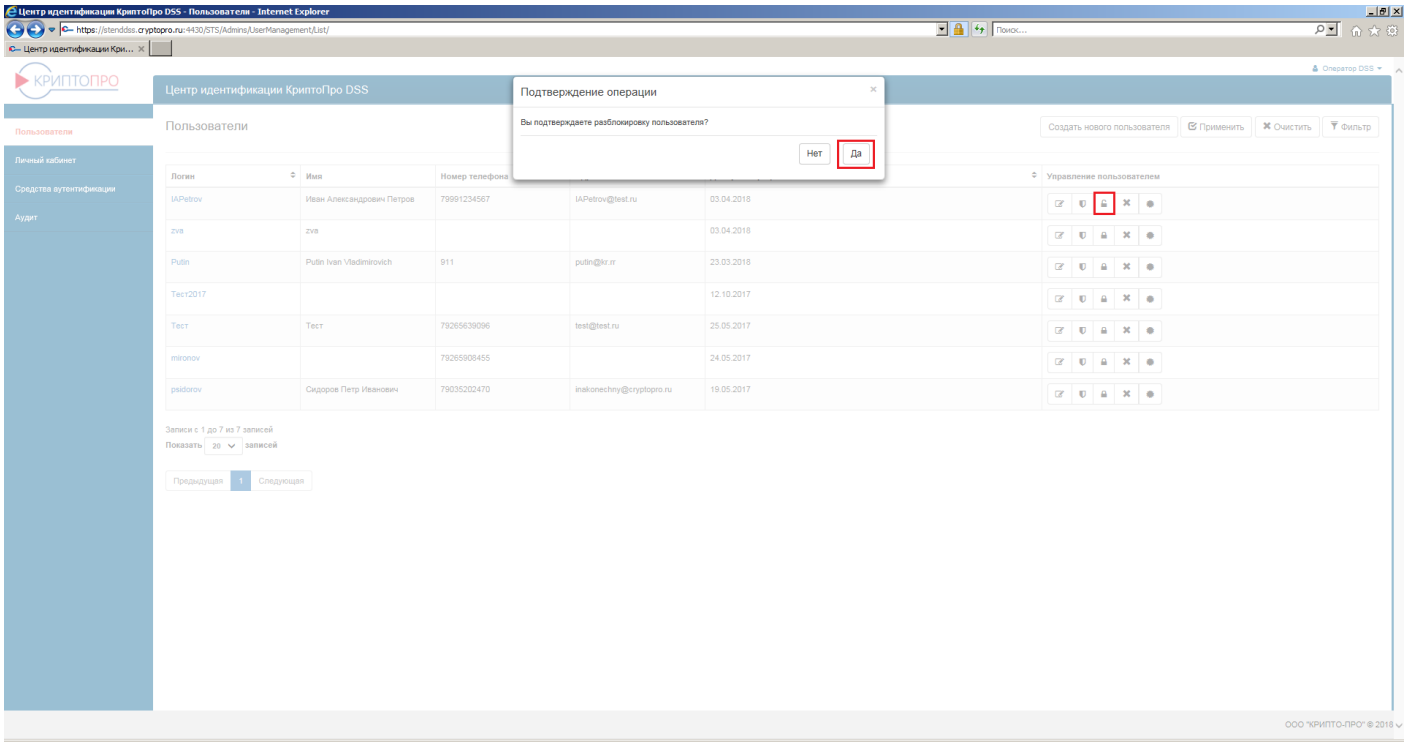


Рисунок 25. Блокировка и разблокировка Пользователя

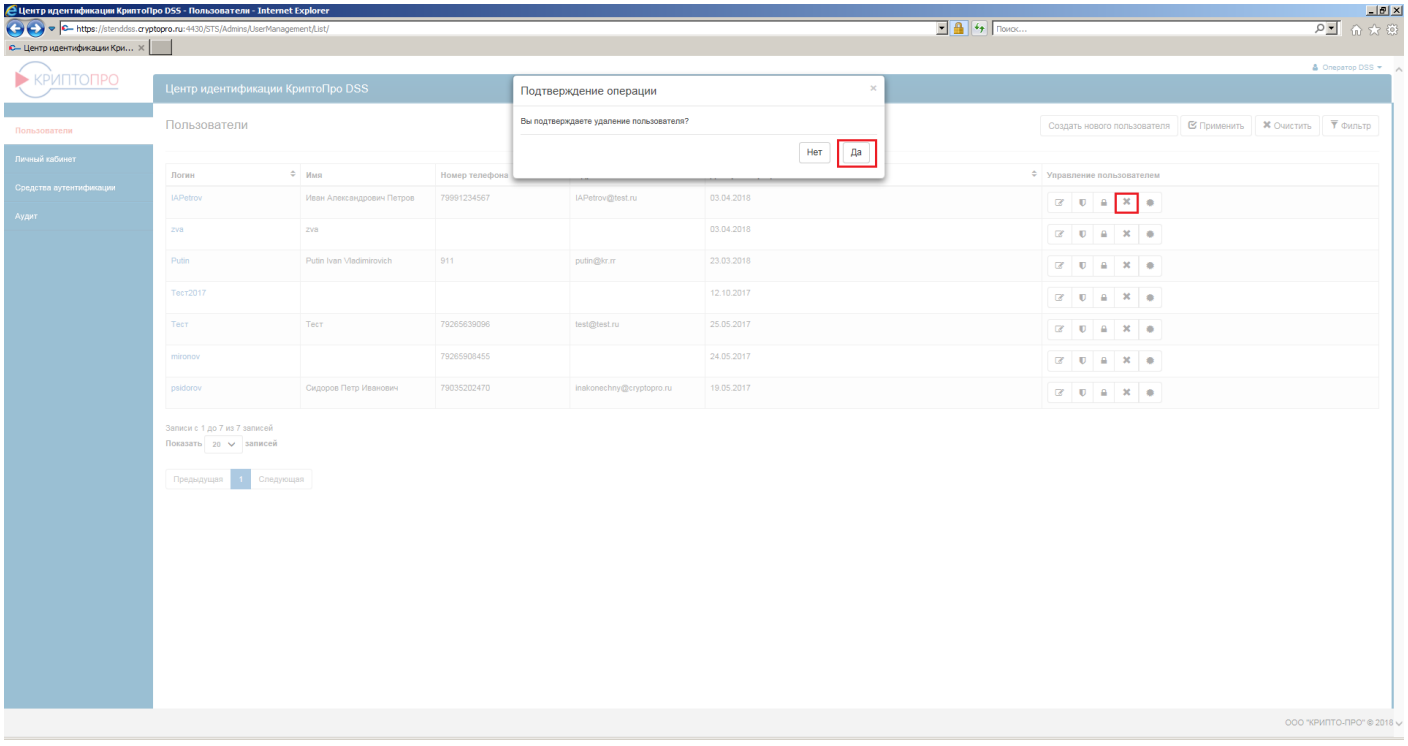


Рисунок 26. Удаление Пользователя

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.
- «*Установить 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 27. Удаление всех сертификатов Пользователя**).

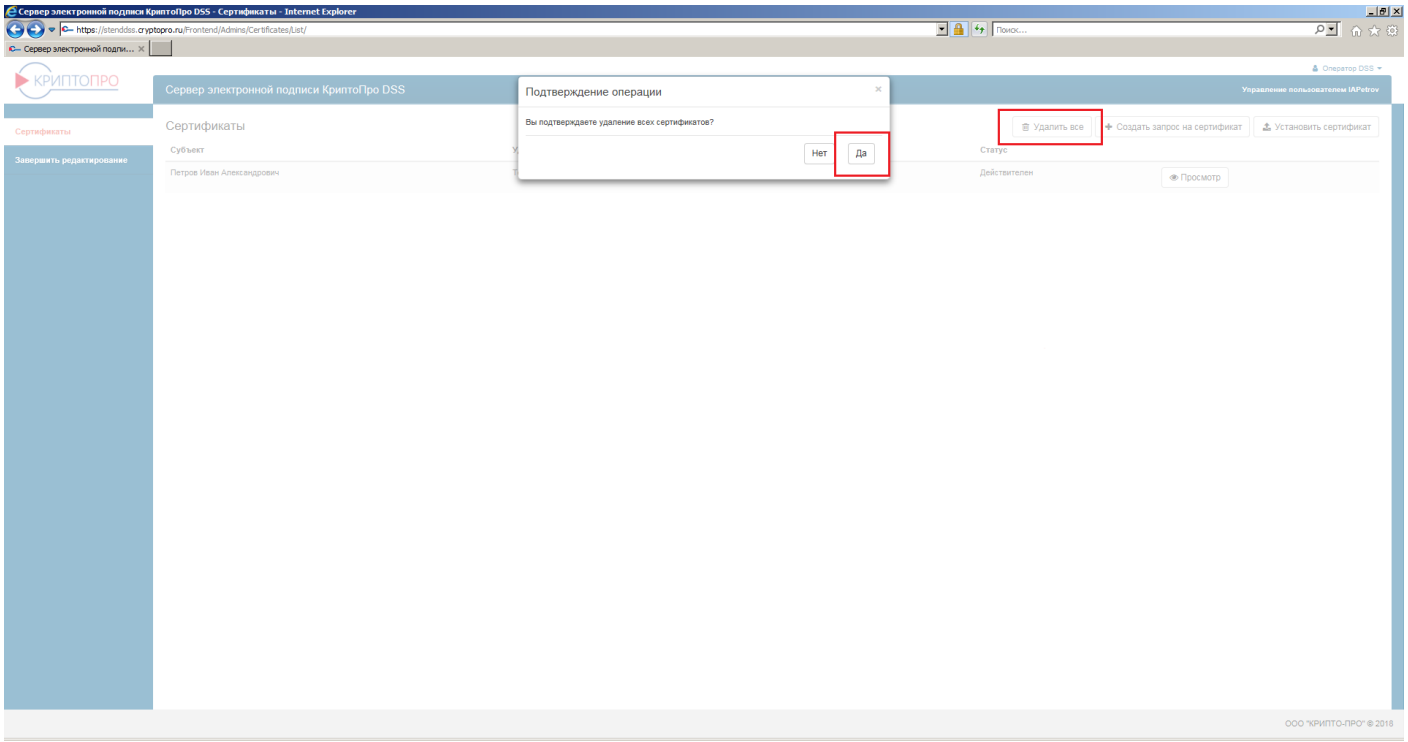


Рисунок 27. Удаление всех сертификатов Пользователя

3.2.5.2. Создание запроса на сертификат Пользователя

Для создания запроса на сертификат Пользователя нужно нажать кнопку «*Создать запрос на сертификат*» (см. **Рисунок 28. Создание запроса на сертификат Пользователя**).

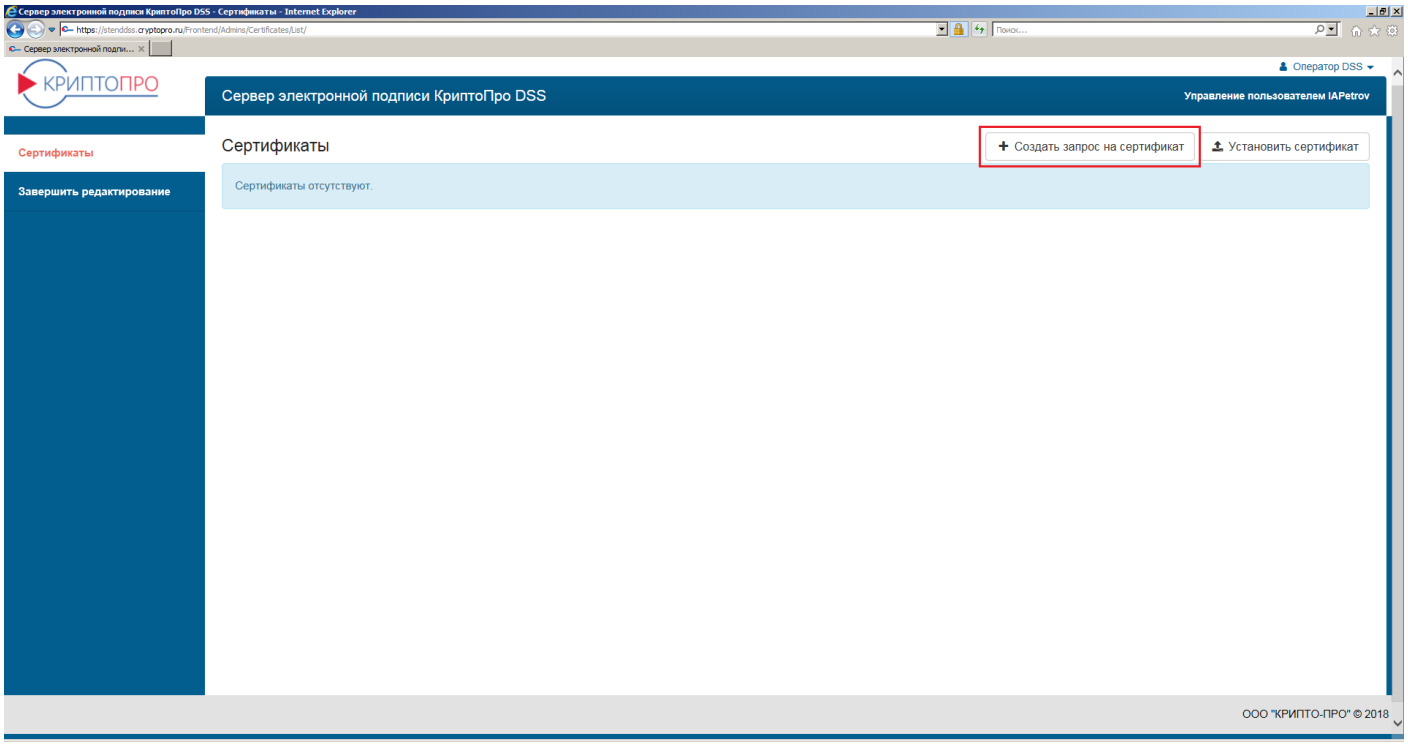


Рисунок 28. Создание запроса на сертификат Пользователя

Далее нужно задать Удостоверяющий центр, к которому будет направлен запрос на сертификат (в настоящее время к тестовому СЭП подключен «*Тестовый УЦ 2.0 для DSS подчиненный*»), отредактировать атрибуты Пользователя, выбрать шаблон сертификата (по умолчанию «*Пользователь DSS*») и нажать кнопку «*Создать запрос*» (см. **Рисунок 29. Подтверждение создания запроса на сертификат Пользователя**).

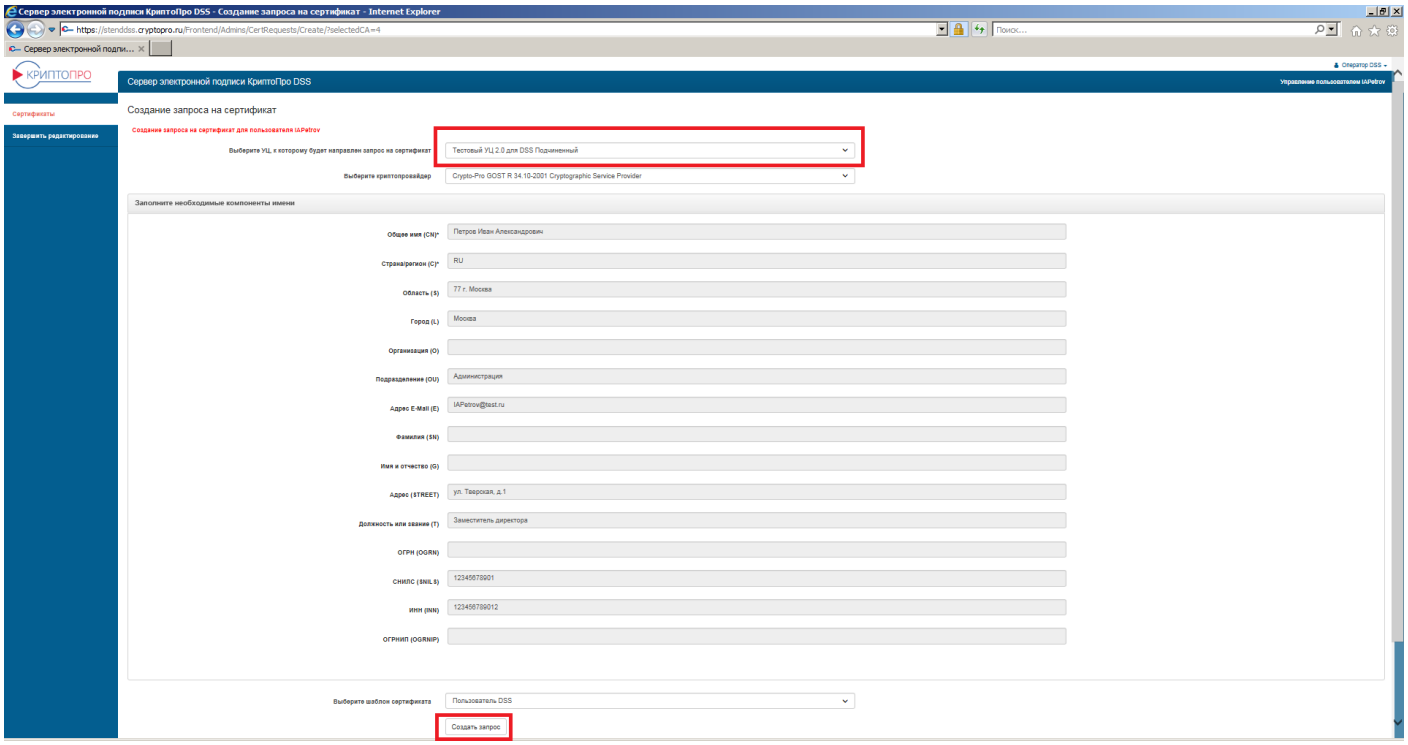


Рисунок 29. Подтверждение создания запроса на сертификат Пользователя

После нажатия кнопки «*Создать запрос*» появится диалог задания ПИН-кода ключевого контейнера. Необходимо задать ПИН-код, подтверждение ПИН-кода и нажать кнопку «*ОК*» (см. **Рисунок 30. Задание ПИН-кода ключевого контейнера**).

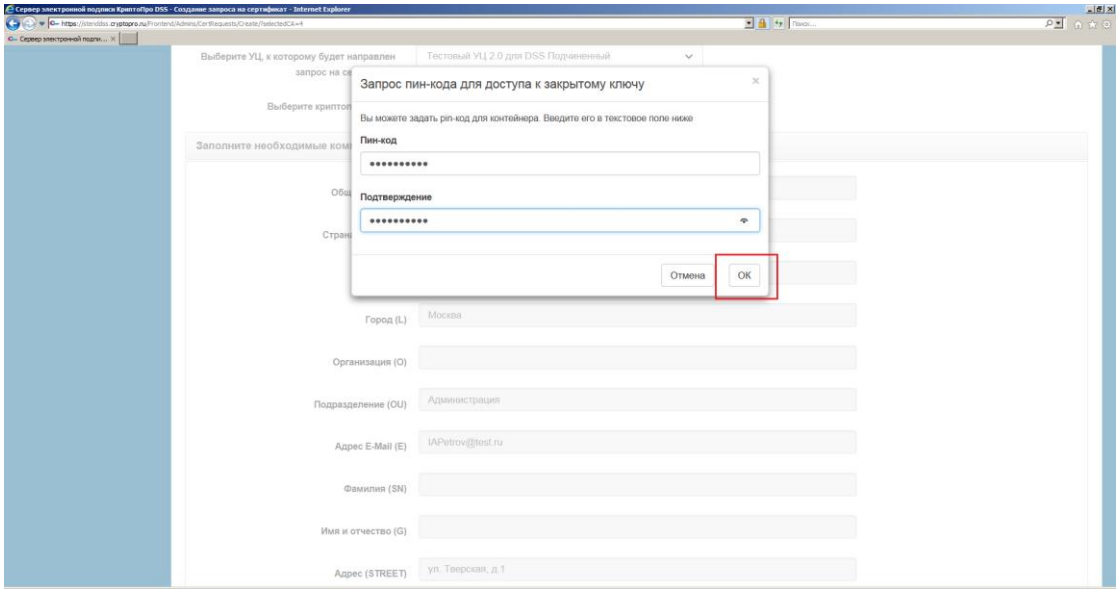


Рисунок 30. Задание ПИН-кода ключевого контейнера

По завершению создания ключевого контейнера сертификат будет выпущен автоматически, после чего информация о нём будет отображена в интерфейсе Оператора (см. **Рисунок 31. Информация о сертификате**).

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

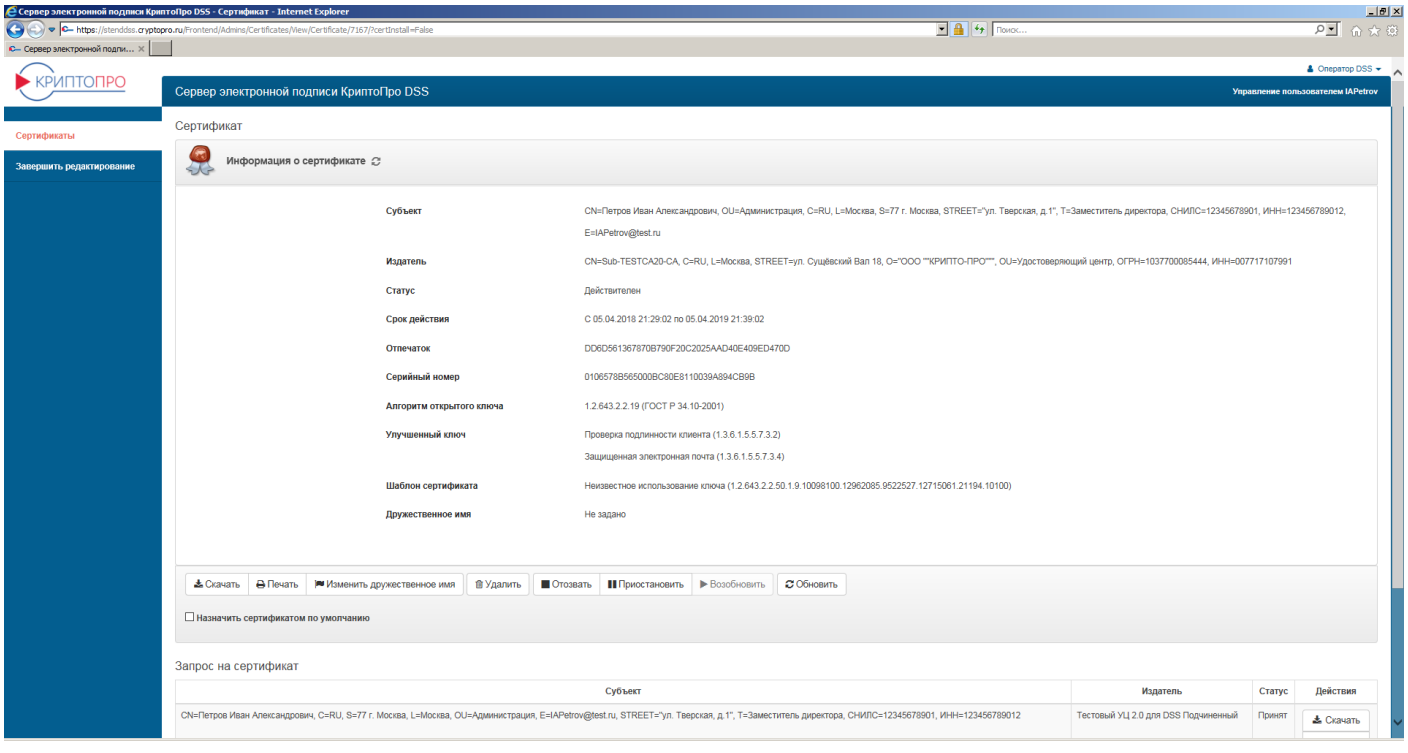


Рисунок 31. Информация о сертификате

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 «*Установить сертификат*» (см. **Рисунок 32. Установка сертификата**).

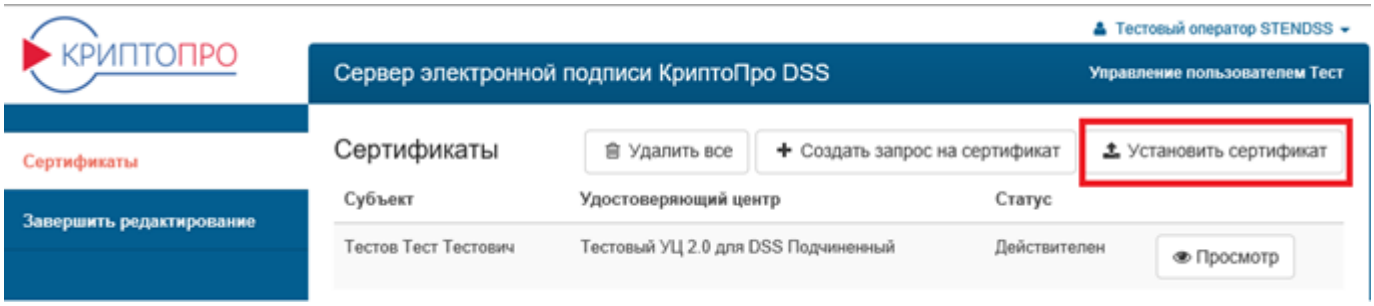


Рисунок 32. Установка сертификата

В открывшемся диалоговом окне следует нажать копку «*Выбрать*» и указать путь до файла с расширением PFX, после чего нажать кнопку «*Открыть*» (см. **Рисунок 33. Выбор файла PFX для импорта сертификата**).

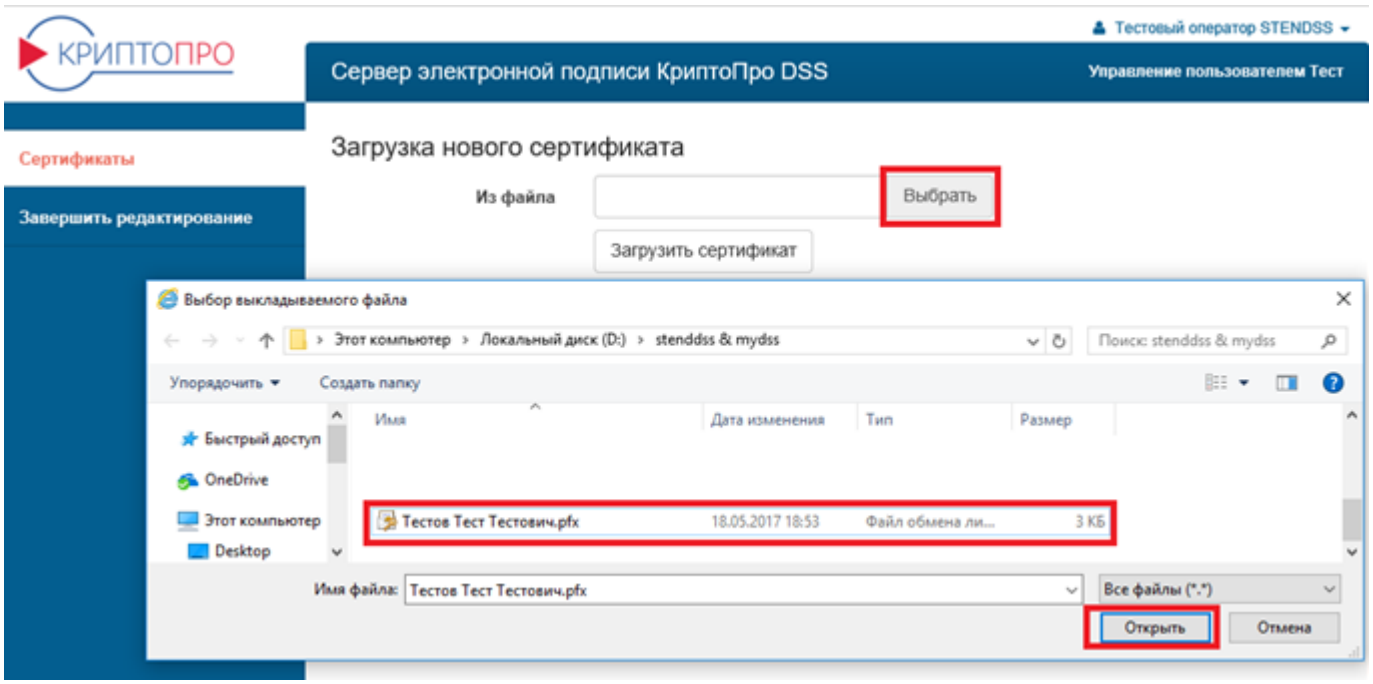


Рисунок 33. Выбор файла PFX для импорта сертификата

Далее в интерфейсе СЭП следует нажать кнопку «*Загрузить сертификат*» (см. **Рисунок 34. Загрузка сертификата**).

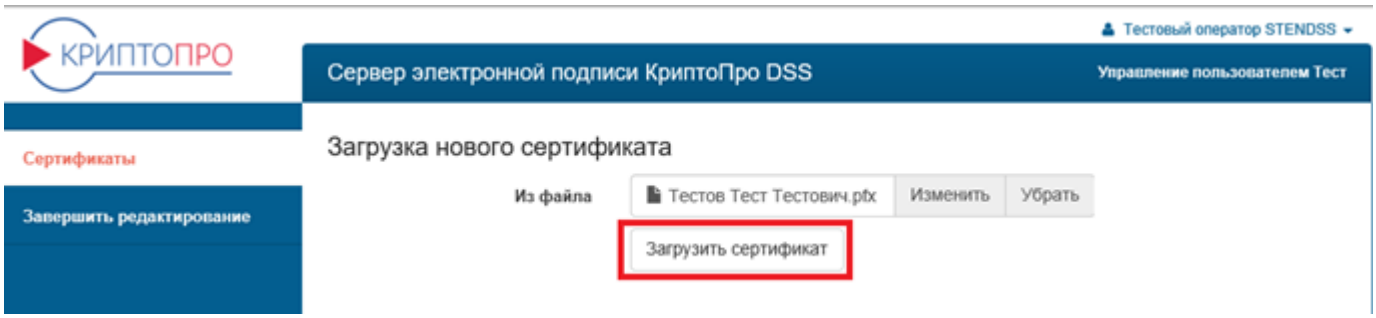


Рисунок 34. Загрузка сертификата

После выполнения указанных выше действий появится диалоговое окно с запросом ПИН-кода доступа к ключу электронной подписи, содержащемуся в файле PFX. Необходимо ввести ПИН-код и нажать кнопку «*ОК*» (см. **Рисунок 35. Ввод ПИН-кода к контейнеру PFX**).

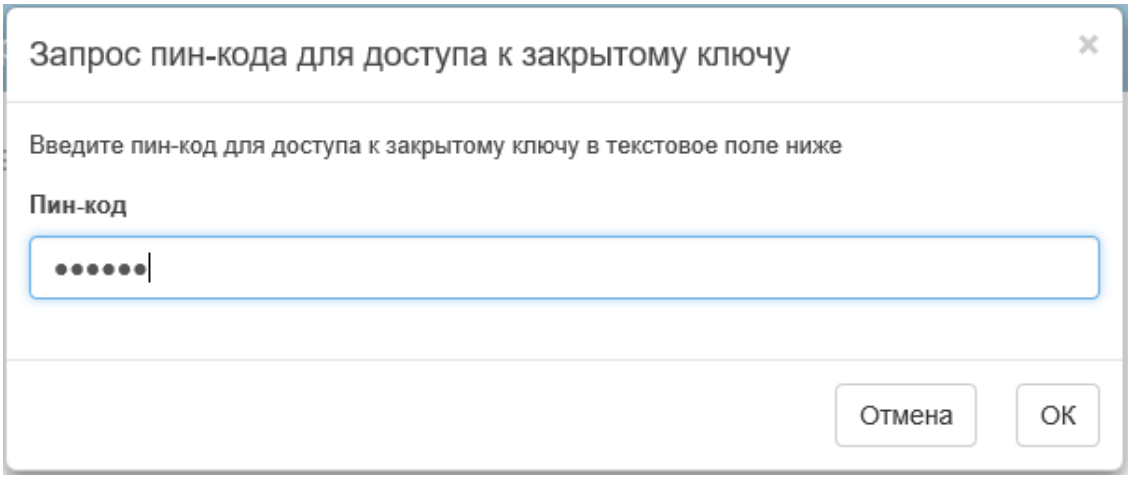


Рисунок 35. Ввод ПИН-кода к контейнеру PFX

После этого импортированный сертификат появится в списке сертификатов Пользователя (см. **Рисунок 36. Импортированный сертификат в списке сертификатов Пользователя**).

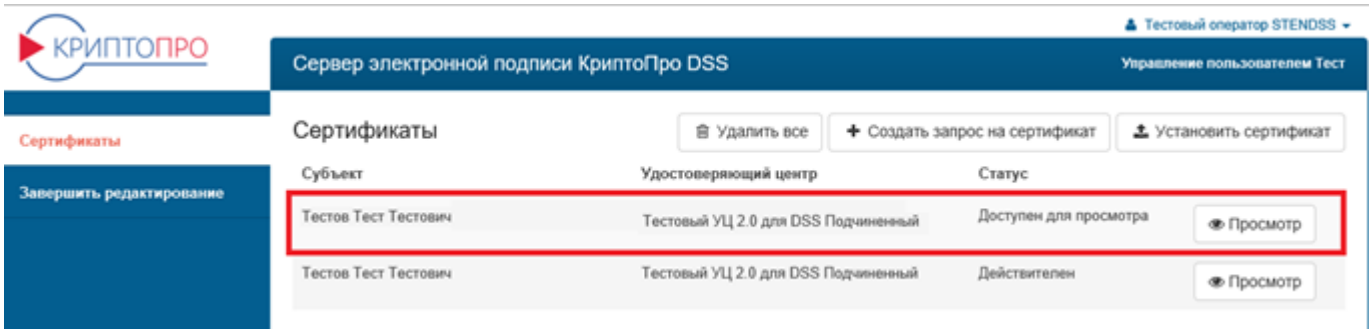


Рисунок 36. Импортированный сертификат в списке сертификатов Пользователя

3.2.5.4. Управление существующим сертификатом Пользователя в СЭП

Для управления существующим сертификатом Пользователя в СЭП нужно нажать кнопку «*Просмотр*» в соответствующей строке раздела «*Сертификаты*» (см. **Рисунок 37. Выбор сертификата для управления**).

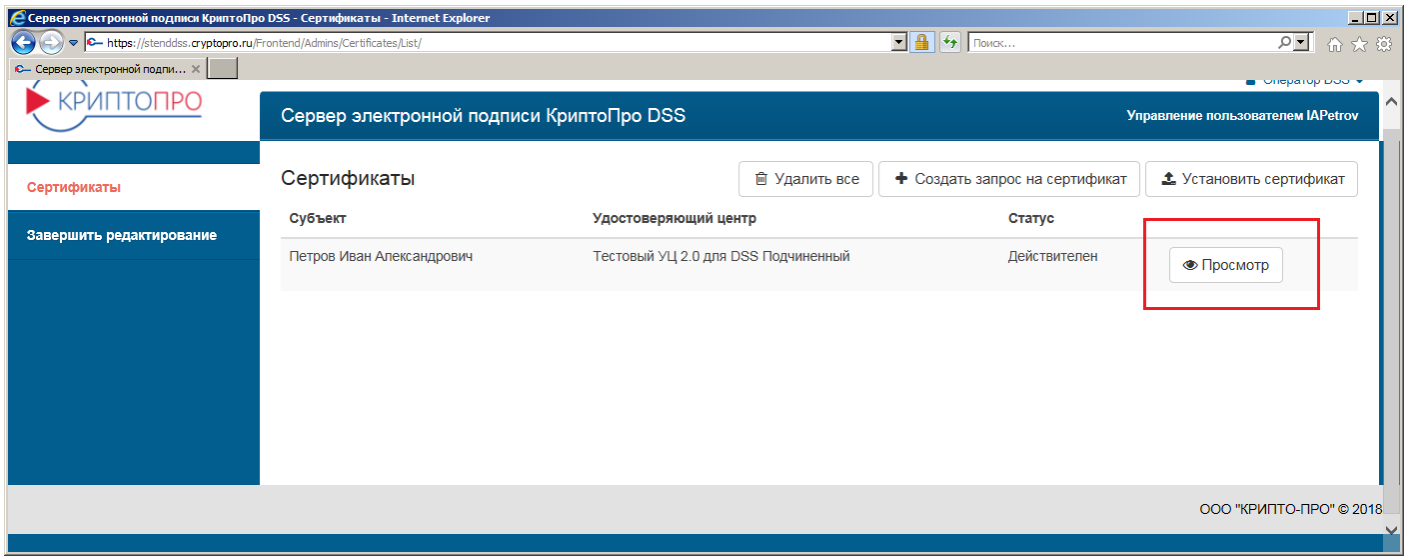


Рисунок 37. Выбор сертификата для управления

Оператору доступны следующие операции управления сертификатом (см. **Рисунок 38. 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 (надо будет указать ПИН-код к ключевому контейнеру в СЭП, причину отзыва, дату отзыва).
- «*Приостановить*» – приостановить действие сертификата (надо будет указать ПИН-код к ключевому контейнеру в СЭП, причину приостановления, дату приостановления, дату окончания приостановления и действие после приостановления).
- «*Возобновить*» – возобновить действие приостановленного сертификата.
- «*Обновить*» – обновить сертификат в случае (скорого) истечения срока его действия.

- «*Назначить сертификатом по умолчанию*» – выбрать данный сертификат по умолчанию из всех сертификатов Пользователя.

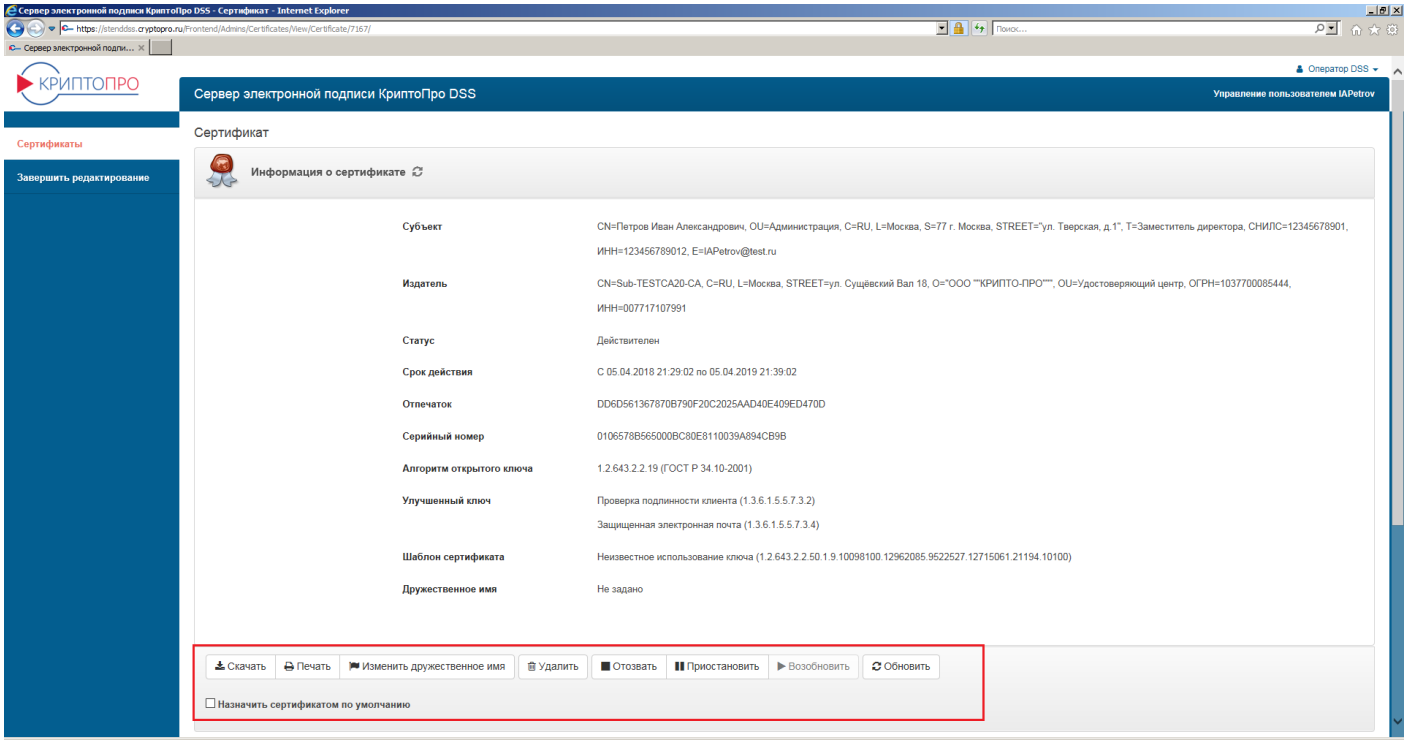


Рисунок 38. Функции управления сертификатом

4. Раздел «Личный кабинет»

Раздел позволяет просматривать и редактировать личные данные Оператора (см. **Рисунок 39. Просмотр личных данных Оператора**). При нажатии на кнопку «*Редактировать*» доступно изменения ФИО Оператора. Для сохранения изменений необходимо нажать кнопку «*Сохранить*» (см. **Рисунок 40. Изменение ФИО Оператора**).

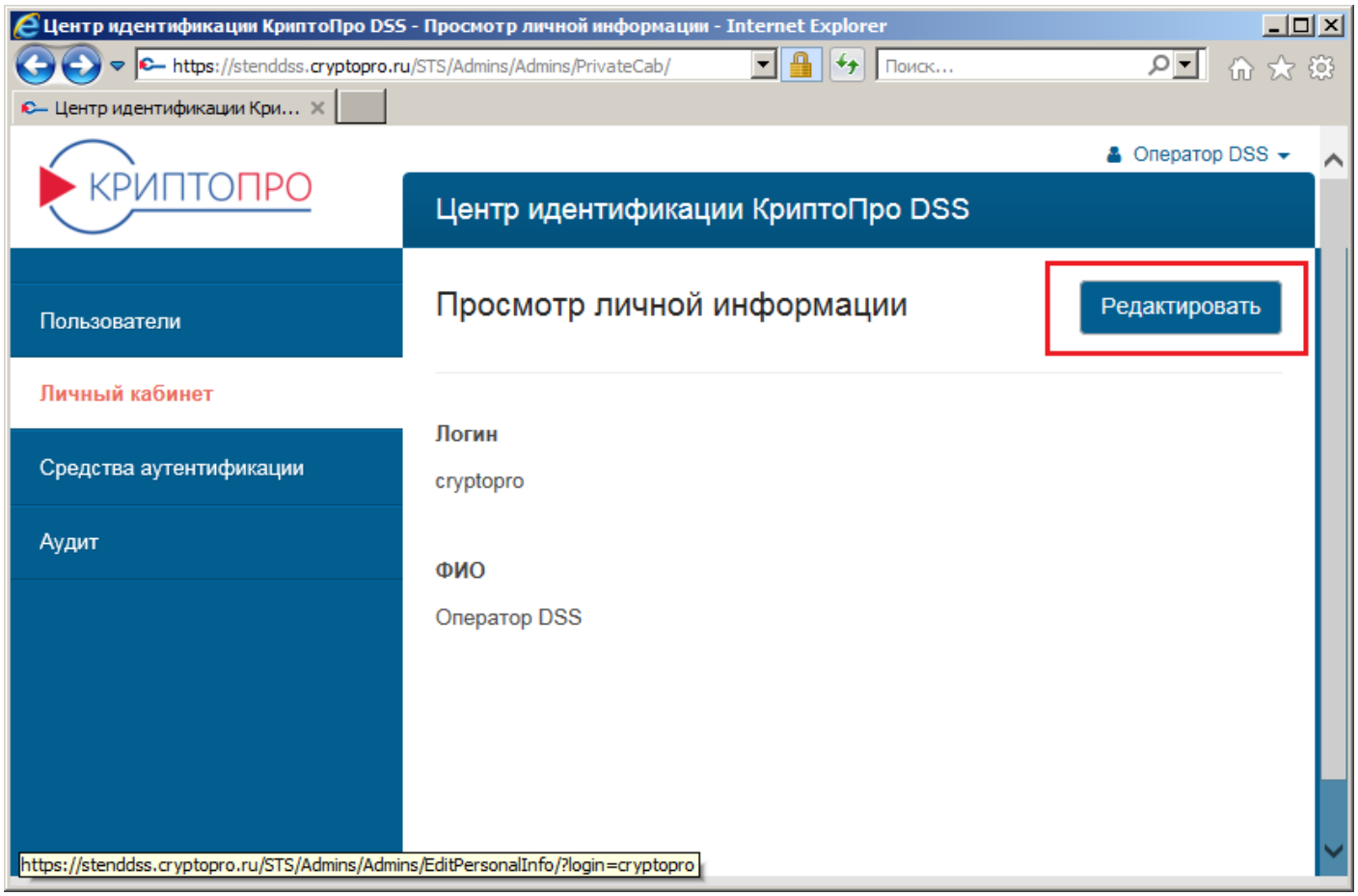


Рисунок 39. Просмотр личных данных Оператора

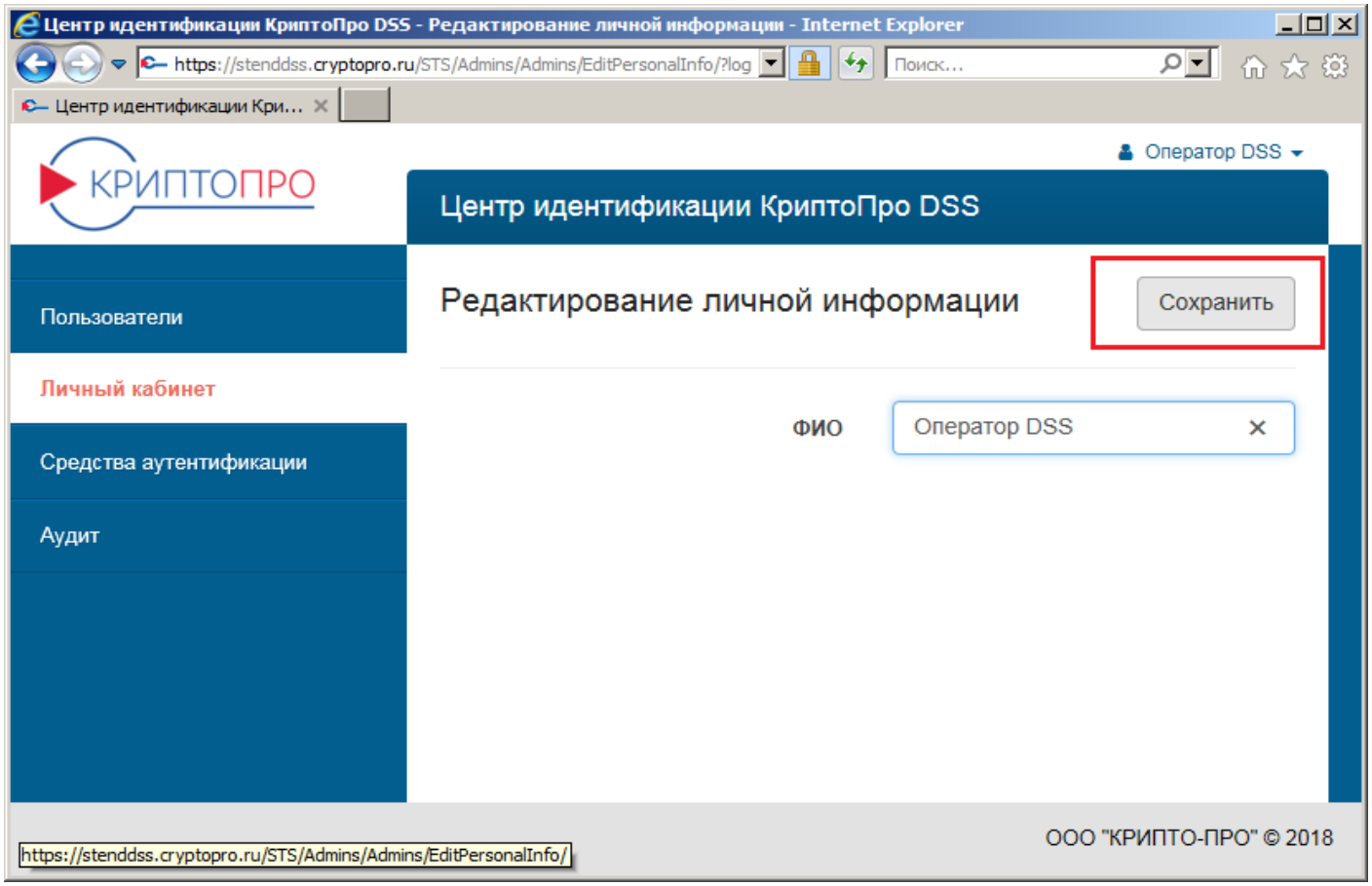


Рисунок 40. Изменение ФИО Оператора

5. Раздел «Средства аутентификации»

Раздел позволяет просматривать перечень назначенных Пользователям средств аутентификации (см. **Рисунок 41. Перечень средств аутентификации**).

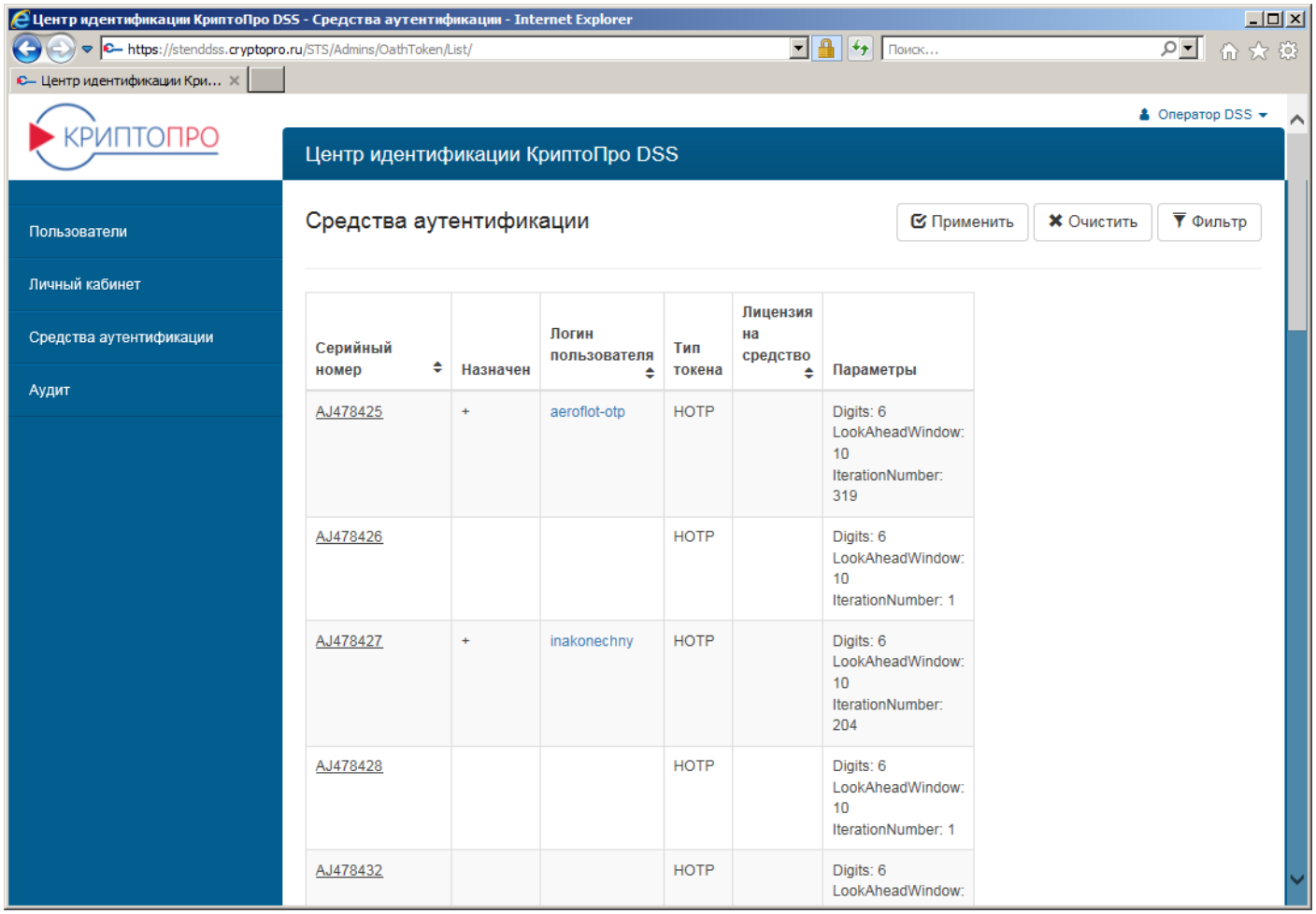


Рисунок 41. Перечень средств аутентификации

6. Раздел «Аудит»

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

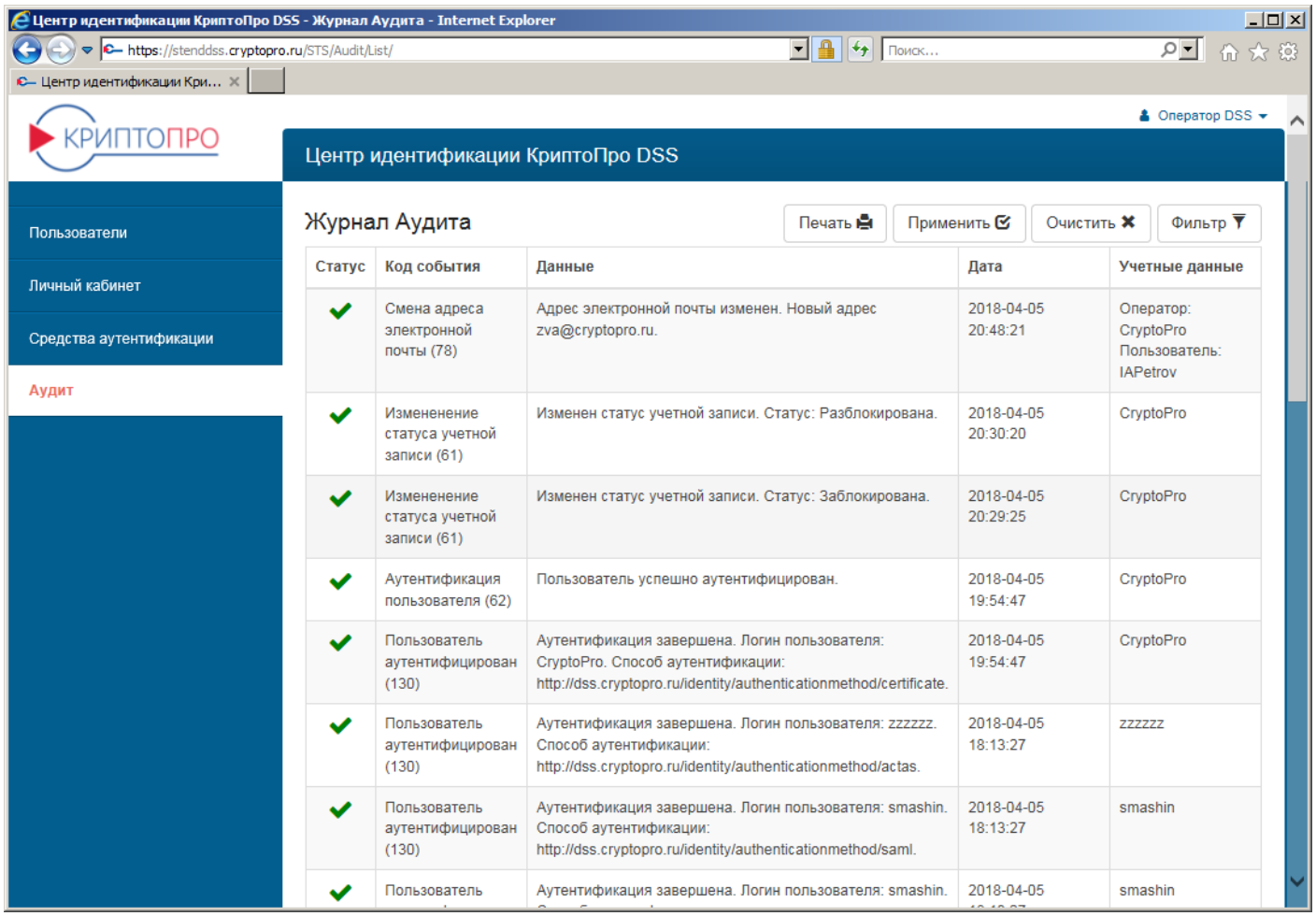


Рисунок 42. Аудит событий СЭП

Перечень рисунков