УТВЕРЖДЁН ЖТЯИ.00082-01 90 03 06-ЛУ

ЖТЯИ.00082-01 90 03 06



## ПАК «КриптоПро DSS» сервис электронной поллиси

СЕРВИС ЭЛЕКТРОННОЙ ПОДПИСИ Инструкция Оператора СЭП

ООО «КРИПТО-ПРО»

## Аннотация

Настоящая инструкция предназначена для Пользователей сервиса электронной подписи 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 электроннойподписи, созданию и проверке электронной подписи, шифрованию и расшифрованию электронных документов.

## Информация о разработчике ПАКМ "КриптоПро HSM":

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущевский вал, 18

Телефон: (495) 995 4820

http://www.CryptoPro.ru https://saas.cryptopro.ru/Instanceidp/Users E-mail: info@CryptoPro.ru

Аннотация       2         Илформация о разработчике ПАКМ "КриптоПро HSM":       2         1. Общие положения       4         1.1. Требования и подготовка рабочего места Оператора       4         1.1. Требования и подготовка рабочего места Оператора       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 мстю.       6         3. Раздел «Пользователи»       8         3.1. Создание нового Пользователя       8         3.2. Управление существующими Пользователя       8         3.2. Управление существующими Пользователя       10         3.2.1. Редактирование атрибутов Пользователя       10         3.2.2. Настройка парамстров аутентификации пользователя       10         3.2.1.1 Настройка аутентификации по сертификации Пользователя       10         3.2.2.2.1 Настройка аутентификации по протоколу ОАТН       13         3.2.2.2.2 Настройка аутентификации по протоколу ОАТН       13         3.2.2.2.3 Настройка аутентификации по протоколу ОАТН       15         3.2.2.2.4 Настройка аутентификации по пользователя       25         3.2.2.2.4 Настройка аутентификации по пользователя       26         3.2.2.2.4 Настройка аутентификации по п	Оглавление	
Информация о разработчике ПАКМ "КриптоПро HSM":       2         1. Общие положения.       4         1.1. Требования и подготовка рабочего места Оператора.       4         1.1. Пребования и подготовка рабочего места Оператора.       4         1.1.1. Настройка Internet Explorer       4         1.1.2. Настройка Япдекс-браузера.       5         2. Структура меню.       6         3. Раздел «Пользователи»       8         3.1. Создание пового Пользователя.       8         3.2. Управление существующими Пользователя.       10         3.2.1. Редактирование атрибутов Пользователя.       10         3.2.2.1. Настройка параметров аутентификации Пользователя.       10         3.2.2.1. Настройка аутентификации по сретификату.       11         3.2.2.1. Настройка аутентификации по сретификату.       11         3.2.2.2. Настройка аутентификации по проло.       12         3.2.2.1. Настройка аутентификации по SMS.       13         3.2.2.2.1 Настройка аутентификации по протоколу ОАТН.       15         3.2.2.2.2 Настройка аутентификации по протоколу ОАТН.       15         3.2.2.2.3 Настройка аутентификации по протоколу ОАТН.       18         3.2.2.2.4 Настройка аутентификации по протоколу ОАТН.       18         3.2.2.3. Боскировка или разблокировка Пользователя.       25         3.	Аннотация	2
1.         Общие положения         4           1.1.         Требования и подготовка рабочего места Оператора         4           1.1.         Настройка Internet Explorer         4           1.1.1.         Настройка Яндекс-браузера         5           2.         Структура меню         6           3.         Раздел «Пользователи»         8           3.1.         Создание пового Пользователя         8           3.2.         Управление существующими Пользователя         10           3.2.2.         Настройка параметров аутентификации Пользователя         10           3.2.1.         Редактирование атрибутов Пользователя         10           3.2.2.1.         Настройка параметров аутентификации Пользователя         10           3.2.2.1.         Настройка артентификации по сертификатия         11           3.2.2.1.         Настройка аутентификации по пароло.         12           3.2.2.1.         Настройка аутентификации по электронной почте.         17           3.2.2.2.         Настройка аутентификации по электронной почте.         17           3.2.2.2.1         Настройка аутентификации по электронной почте.         17           3.2.2.2.4         Настройка аутентификации по электроной почте.         17           3.2.2.2.4         Настройка аутентификаци	Информация о разработчике ПАКМ "КриптоПро HSM":	2
1.1.1.       Настройка Internet Explorer       4         1.1.2.       Настройка Яндскс-браузера       5         2.       Структура меню	<ol> <li>Оощие положения</li></ol>	4 4
1.1.2.       Настройка Яндекс-браузера       5         2.       Структура меню	1.1.1. Настройка Internet Explorer	4
2.       Структура мешо	1.1.2. Настройка Яндекс-браузера	5
3.       Раздел «Пользователи»	2. Структура меню	6
3.1.       Создание пового Полъзователя       8         3.2.       Управление существующими Пользователями       8         3.2.1.       Редактирование агрибутов Пользователя       10         3.2.2.       Настройка парамстров аутептификации Пользователя       10         3.2.1.       Настройка парамстров аутептификации Пользователя       10         3.2.2.       Настройка первичной аутептификации по сертификату       11         3.2.2.1.       Настройка аутентификации по сертификату       11         3.2.2.2.1       Настройка аутентификации по паролю       12         3.2.2.2.2.       Настройка аутентификации по SMS       13         3.2.2.2.1       Настройка аутентификации по электронной почте       17         3.2.2.2.2       Настройка аутентификации по электронной почте       17         3.2.2.2.3       Настройка аутентификации по электронной почте       17         3.2.2.2.4       Настройка подтверждения и доступа к операциям СЭП       22         3.2.3       Блокировка или разблокировка Пользователя       25         3.2.4.       Удаление Пользователя       25         3.2.5.1.       Удаление всех сертификатов Пользователя       26         3.2.5.2.1.       Создание запроса на сертификат Пользователя       26         3.2.5.2.1.       Создание зап	3. Раздел «Пользователи»	8
3.2.       Управление существующими Пользователями       8         3.2.1.       Редактирование атрибутов Пользователя       10         3.2.2.       Настройка параметров аутентификации Пользователя       10         3.2.1.       Настройка первичной аутентификации Пользователя       10         3.2.2.       Настройка первичной аутентификации по сертификату       11         3.2.2.1.       Настройка первичной аутентификации по сертификату       11         3.2.2.2.       Настройка вутентификации по паролю       12         3.2.2.2.       Настройка вутентификации по паролю       13         3.2.2.2.       Настройка вутентификации по SMS       13         3.2.2.2.       Настройка аутентификации по ротоколу OATH.       15         3.2.2.2.3       Настройка аутентификации по электронной почте       17         3.2.2.4.       Настройка подтверждения и доступа к операциям CЭП       22         3.2.3.       Блокировка или разблокировка Пользователя       25         3.2.4.       Удаление пользователя       25         3.2.5.       Управление сертификатами Пользователя       26         3.2.5.1.       Удаление всех сертификатов Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.       Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)       2	3.1. Создание нового Пользователя	8
3.2.1.       Редактирование атрибутов Пользователя	3.2. Управление существующими Пользователями	8
3.2.2.       Настройка параметров аутентификации Пользователя	3.2.1. Редактирование атрибутов Пользователя	10
3.2.2.1. Настройка первичной аутентификации       11         3.2.2.1.1 Настройка аутентификации по сертификату       11         3.2.2.1.2 Настройка аутентификации по паролю       12         3.2.2.2. Настройка вторичной аутентификации       13         3.2.2.2. Настройка аутентификации по паролю       13         3.2.2.2. Настройка аутентификации по вотоколу ОАТН       13         3.2.2.2.1 Настройка аутентификации по протоколу ОАТН       15         3.2.2.2.2 Настройка аутентификации по электронной почте.       17         3.2.2.2.4 Настройка аутентификации по электронной почте.       17         3.2.2.2.4 Настройка аутентификации с помощью мобильного приложения       18         3.2.2.3. Настройка подтверждения и доступа к операциям СЭП       22         3.2.3. Блокировка или разблокировка Пользователя       25         3.2.4. Удаление Сертификатами Пользователя       25         3.2.5.1. Удаление всех сертификата Пользователя, зарегистрированных вСЭП       26         3.2.5.2. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.1. Создание запроса на сертификат Пользователя       30         3.2.5.2.2. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.3. Установка сертификата Пользователя       30         3.2.5.4. Управление существующим сертификат Пользователя в СЭП	3.2.2. Настройка параметров аутентификации Пользователя	10
3.2.2.1.1       Настройка аутентификации по сертификату	3.2.2.1. Настройка первичной аутентификации	11
3.2.2.1.2       Настройка вутентификации по паролю	3.2.2.1.1 Настройка аутентификации по сертификату	11
3.2.2.2.       Настройка вторичной аутентификации       13         3.2.2.2.1       Настройка аутентификации по SMS	3.2.2.1.2 Настройка аутентификации по паролю	12
3.2.2.2.1       Настройка аутентификации по SMS	3.2.2.2. Настройка вторичной аутентификации	13
3.2.2.2.2       Настройка аутентификации по протоколу ОАТН	3.2.2.2.1 Настройка аутентификации по SMS	13
3.2.2.2.3       Настройка аутентификации по электронной почте.       17         3.2.2.2.4       Настройка аутентификации с помощью мобильного приложения       18         3.2.2.3.       Настройка подтверждения и доступа к операциям СЭП       22         3.2.3.       Блокировка или разблокировка Пользователя       25         3.2.4.       Удаление Пользователя       25         3.2.5.       Управление сертификатами Пользователя, зарегистрированных вСЭП       26         3.2.5.1.       Удаление всех сертификатов Пользователя, зарегистрированных вСЭП       26         3.2.5.2.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.1.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.2.       Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)       28         3.2.5.2.3.       Установка сертификата Пользователя       30         3.2.5.4.       Управление существующим сертификатом Пользователя в СЭП       31         3.2.5.4.       Управление существующим сертификатом Пользователя в СЭП       33         4.       Раздел «Личный кабинет»       34         5.       Раздел «Оповещения оператора»       35         6.       Раздел «Средства аутентификации»       35 <td>3.2.2.2.2 Настройка аутентификации по протоколу ОАТН</td> <td> 15</td>	3.2.2.2.2 Настройка аутентификации по протоколу ОАТН	15
3.2.2.2.4       Настройка аутентификации с помощью мобильного приложения       18         3.2.2.3.       Настройка подтверждения и доступа к операциям СЭП       22         3.2.3.       Блокировка или разблокировка Пользователя       25         3.2.4.       Удаление Пользователя       25         3.2.5.       Управление сертификатами Пользователя, зарегистрированных вСЭП       26         3.2.5.1.       Удаление всех сертификатов Пользователя, зарегистрированных вСЭП       26         3.2.5.2.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.1.       Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)       28         3.2.5.2.3.       Установка сертификата Пользователя       30         3.2.5.4.       Управление существующим сертификат Пользователя в СЭП       31         3.2.5.2.3.       Установка сертификата Пользователя       30         3.2.5.4.       Управление существующим сертификато В СЭП       31         3.2.5.4.       Управление существующим сертификатом Пользователя в СЭП       33         4.       Раздел «Оповещения оператора»       35         6.       Раздел «Средства аутентификации»       35	3.2.2.2.3 Настройка аутентификации по электронной почте	17
3.2.2.3. Настройка подтверждения и доступа к операциям СЭП       22         3.2.3. Блокировка или разблокировка Пользователя       25         3.2.4. Удаление Пользователя       25         3.2.5. Управление сертификатами Пользователя, зарегистрированных вСЭП       26         3.2.5.1. Удаление всех сертификатов Пользователя, зарегистрированных вСЭП       26         3.2.5.2. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2. Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)       28         3.2.5.2.3. Установка сертификата Пользователя       30         3.2.5.4. Управление существующим сертификатом Пользователя в СЭП       31         3.2.5.4. Управление существующим сертификатом Пользователя в СЭП       31         3.2.5.4. Управление существующим сертификатом Пользователя в СЭП       33         4. Раздел «Личный кабинет»       34         5. Раздел «Оповещения оператора»       35         6. Раздел «Средства аутентификации»       35	3.2.2.2.4 Настройка аутентификации с помощью мобильного приложения	18
3.2.3.       Блокировка или разблокировка Пользователя       25         3.2.4.       Удаление Пользователя       25         3.2.5.       Управление сертификатами Пользователя, зарегистрированных вСЭП.       25         3.2.5.1.       Удаление всех сертификатов Пользователя, зарегистрированных вСЭП.       26         3.2.5.2.       Создание запроса на сертификат Пользователя       26         3.2.5.2.1.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.2.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.2.       Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)       28         3.2.5.2.3.       Установка сертификата Пользователя       30         3.2.5.4.       Управление существующим сертификатом Пользователя в СЭП       31         3.2.5.4.       Управление существующим сертификатом Пользователя в СЭП       33         4.       Раздел «Личный кабинет»       34         5.       Раздел «Средства аутентификации»       35	3.2.2.3. Настройка подтверждения и доступа к операциям СЭП	22
3.2.4.       Удаление Пользователя       25         3.2.5.       Управление сертификатами Пользователя       25         3.2.5.1.       Удаление всех сертификатов Пользователя, зарегистрированных вСЭП       26         3.2.5.2.       Создание запроса на сертификат Пользователя       26         3.2.5.2.1.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.1.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)       26         3.2.5.2.2.       Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)       28         3.2.5.2.3.       Установка сертификата Пользователя       30         3.2.5.3.       Установка сертификата, не зарегистрированного в СЭП       31         3.2.5.4.       Управление существующим сертификатом Пользователя в СЭП       33         4.       Раздел «Личный кабинет»       34         5.       Раздел «Оповещения оператора»       35         6.       Раздел «Средства аутентификации»       35	3.2.3. Блокировка или разблокировка Пользователя	25
3.2.5.       Управление сертификатами Пользователя.       25         3.2.5.1.       Удаление всех сертификатов Пользователя, зарегистрированных вСЭП	3.2.4. Удаление Пользователя	25
3.2.5.1. Удаление всех сертификатов Пользователя, зарегистрированных вСЭП	3.2.5. Управление сертификатами Пользователя	25
3.2.5.2.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)	3.2.5.1. Удаление всех сертификатов Пользователя, зарегистрированных вСЭП	26
3.2.5.2.1.       Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)	3.2.5.2. Создание запроса на сертификат Пользователя	26
3.2.5.2.2.       Создание запроса на сертификат Пользователя (хранение ключей в мобильном приложении)	3.2.5.2.1. Создание запроса на сертификат Пользователя (хранение ключей на сервере DSS)	26
приложении)	3.2.5.2.2. Создание запроса на сертификат Пользователя (хранение ключей в мобильном	
3.2.5.2.3.       Установка сертификата Пользователя	приложении)	28
3.2.5.3. Установка сертификата, не зарегистрированного в СЭП       31         3.2.5.4. Управление существующим сертификатом Пользователя в СЭП       33         4. Раздел «Личный кабинет»       34         5. Раздел «Оповещения оператора»       35         6. Раздел «Средства аутентификации»       35	3.2.5.2.3. Установка сертификата Пользователя	30
3.2.5.4. Управление существующим сертификатом Пользователя в СЭП       33         4. Раздел «Личный кабинет»       34         5. Раздел «Оповещения оператора»       35         6. Раздел «Средства аутентификации»       35	3.2.5.3. Установка сертификата, не зарегистрированного в СЭП	31
<ul> <li>4. Раздел «Личный кабинет»</li></ul>	3.2.5.4. Управление существующим сертификатом Пользователя в СЭП	33
<ol> <li>Раздел «Оповещения оператора»</li></ol>	4. Раздел «Личный кабинет»	34
6. Раздел «Средства аутентификации»	5. Раздел «Оповещения оператора»	35
7 <b>DOD TOT</b> ((A VITUT))	6. Раздел «Средства аутентификации»	35
7. Газдел «тудит»	г. паздел «тудит» Перечень рисунков	33

## 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 Пользователя СЭП (далее – Пользователь) 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 <u>https://saas.cryptopro.ru/</u>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*".

Параметры	Параметры
Предлагать Включить Отключить ОТключить ОТключить ОТключить ОТключить ОТключить ОТключить ОТключить ОТключить ОТключить ОТключить ОТтена	Предлагать Включить Допущенных администратором Отключить Предлагать Запускать антивредоносное ПО для элементов управления Включить Отключить Отключить Отключить Отключить Предлагать Котользование влементов управления ActiveX, не помечения Включить Отключить Предлагать Поведение двоичного кодов и сценариев Включить Поведение двоичного кодов и сценариев Включить Поведение двоичного кодов и сценариев Включить Поведение двоичного кодов и сценариев Включить Сброс особых параметров На уровень: Средний (по умолчанию) ОК Отмена

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».



## 2. Структура меню

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



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).

		🛔 Operator 🗸
KPUITIOI IPO	Центр идентификаци	и КриптоПро DSS
Пользователи	Просмотр личной и	иформации Редактировать
Личный кабинет		
Оповещения оператора	Логин	operator
Средства аутентификации	ОИФ	Operator
Аудит	Отпечаток сертификата	53A90223A9CFB27A1333DB2C28355744760510BA
	Номер телефона	не задан
	Адрес эл. почты	не задан

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) *«Aydum»*.

#### 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).

Сентронности Центронности Центронности Пользователи	иденти овател	фикации Кри 1И	птоПро DSS				<b>Т</b> Фильтр					
Пользователи	овател	и					🔻 Фильтр	C				
									здать	нового	пользо	звателя
Личный кабинет	•	14		A		Envir						
Оповещения оператора	-	ями	номер телефона	Адрес почты	дата регистрации	₽ Груп	па упр	авлен	ие пол	ьзоват	элем	
Средства аутентификации	логины:	testovii	78983247238		23.05.2022	forAF	»	8	3 1	. 4	. 🔒	
realsts: t	gad.ru st						3	•				
Аудит								8	3 1			

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).

					Operator
криптопро	Центр идентификации КриптоПро	DSS			
Пользователи	Создание нового пользовател	я		Создать	Отмена
Личный кабинет	поля, помеченные *, обязательные для запол	нения			
Оповещения оператора	Группа	Группа по умолчанию	•		
Средства аутентификации	Логин *	Ivanov			
Аудит	Отображаемое имя	Иванов Иван Иванович			
	Имя Отчество *	иван иванович			
	Общее имя	Иванов Иван Иванович			

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).

										🔒 Operat
Центр ид	дентифин	ации Криптоľ	Tpo DSS							
Пользое	ватели						<b>Т</b> Фильтр	Создат	ь нового п	ользовател:
Логин	\$ NM	ИЯ	Номер телефона	Адрес почты	Дата регистрации	Группа	а Упра	вление по	льзовател	тем
Ivanov	Ие	занов Иван			26.04.2023	Default	Ø	Ð	•	•
		занович					×	٠		
test							I	8	U A	
adfs: test@ac realsts: test	d.ru tes	stovii	78983247238		23.05.2022	forAPI	×	•		
										🛔 Operator 👻
Центр иде	ентифика	ации КриптоПр	oo DSS							
	udonus									
Личная и	нформа	ация пользое	ателя иванов и	иван иванович	⊙ Подтвердить УЗ					
	🗲 Назад	Сертификат	ы 🔒 Заблокировать	В Редактировать	Контакты	нтификац	ия 🔔 Опо	вещения	🔳 Кло	нировать
_										
Отображаем	иое имя	Ива	анов Иван Иванович							
Полиц		T py	ппа по умолчанию							
	80	IVa								
	80	VIBe Mor								
фамилия		VIB:								
		1/100-								
	Центр ид Пользон Логин Ivanov test Внешние ла adfs: test@ adfs: test@ adfs: test@ adfs: test@ adfs: test@ adfs: test@ adfs: test@ adfs: test@ adfs: test@ CoroSpaxaer Группа Логин Имя Отчест Общее имя	Центр идентифии Пользователи логин	Центр идентификации Криптол Пользователи имя имя имя имя ианов Иван изанович test внешине логины: аdfs: test@ad.ru realsts: test иеstovii сертификации КриптоЛи личная информация пользов сертификат Группа Гру Логин иа имя отчество ива общее имя ива	Центр идентификации КриптоПро DSS         Пользователи         Логин       Имя       Номер телефона         Імалоу       Иванов Иван Иванович       Иванов Иван         Імалоу       Иванов Иван Иванович       78983247238         Теяt Внешине логины: аdfs: test@ad ru realsts: test       теstovii       78983247238         Сцентр идентификации КриптоПро DSS         Личная информация пользователя Иванов И с Назад       Сертификаты       Заблокировать         Отображаемое имя       Иванов Иван Иванович       Элогич       Гулпа         Погин       Галоу       Иванов Иван Иванович       Общее имя       Иванов Иван Иванович         Общее имя       Иванов Иван Иванович       Общее имя       Иванов Иван Иванович	Центр идентификации КриптоПро DSS Пользователи  Логин	Центр идентификации КриптоПро DSS Пользователи  Тогин ♥ Имя Номер телефона Адрес почты Дата регистрации ♥  Uvanov Иванов Иван Иванов Иван Иванов Иван Иванович 26.04.2023  test Beeшиие полны: ads.test@ad.ru reats:test  testovii 78983247238 23.05.2022  Lettp идентификации КриптоПро DSS  Личная информация пользователя Иванов Иван Иванович ● Подтвердить УЗ  Ve Hasag ● Ceprификаты ● Заблокировать @ Редактировать ■ Koнтакты ■ Аутее  Oroбражаемое имя Иванов Иван Иванович Vanov Иванов Иван Иванович Vanov Иванов Иван Иванович Общее имя Иванов Иван Иванович Общее имя Иванов Иван Иванович	Центр идентификации КриптоПро DSS Пользователи           Пользователи         Изанов Иван       Номер телефона       Адрес почты       Дата регистрации       С группа         Изанов Иван       Иванов Иван       26.04.2023       Default         Изанов Иван       Иванов Иван       28.04.2023       Default         Itest       Внешине полины: ивановиче полины: аds. test@da1u       Точка       78983247238       23.05.2022       for API         Uests       Внешине полины: иванов Иван       аds. test@da1u       С сертификаты       Ваблокировать       С Редактировать       С Контакты       О Аутентификация         Uesto       Иванов Иван Иванович       Ф полтвераить УЗ       С ображаемое имя       Иванов Иван Иванович       О полтвераить УЗ         Отображаемое имя       Иванов Иван Иванович       Ф полтвераить УЗ       О Аутентификация         Отображаемое имя       Иванов Иван Иванович       О полтвераить УЗ       О Аутентификация         Отображаемое имя       Иванов Иван Иванович       О полтвераить УЗ       О Сображаемое имя       Иванов Иван Иванович         Отображаемое имя       Иванов Иван Иванович       О сображаемое имя       Иванов Иван Иванович       О сображаемое имя       Иванов Иван Иванович         Отображаемое имя       Иванов Иван Иванович       О сображаемое имя       Иванов Иван Иванович	Центр идентификации КриптоПро DSS         Пользователи       ▼ фильтр         Логин       Имя       Номер телефона       Адрес почты       Дата регистрации       Труппа       Упра         Изанов Иван       Иванов Иван       26.04.2023       Default       Image: Color Co	Центр идентификации КриптоПро DSS         ГОЛЬЗОВАТЕЛИ            Тогин	Центр идентификации КриптоПро DSS         ГОЛЬЗОВАТЕЛИ         Image: Colspan=1       Image: Colspan=1         Image: Colspan=1       Image: Colspan=1

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).

			🛔 Operator 👻
KPDIITION PO	Центр идентификации КриптоПро	DSS	
Пользователи	Редактирование учётных данн	ных пользователя Иванов Иван Иванович	Сохранить Отмена
Личный кабинет			
Оповещения оператора	Группа	Группа по умолчанию	
Средства аутентификации	Отображаемое имя	Иванов	
Аудит	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 <u>ЖТЯИ.00082-01 90 03 06. ПАК «КриптоПро DSS». Инструкция Оператора СЭП</u> 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 ОАТН» – подтверждение действий Пользователя в СЭП по одноразовому паролю ОТР-токена; метод доступентолько в случае, если заданы параметры ОТР-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 сертификатаа»*)(см. Рисунок 11 - Импорт сертификата для аутентификации).

Способы входа 👻	
Локальный логин: Ivanov 🕜 Изменить	
Аутентификация по сертификату 👻	
Различительное имя субъекта: "SN="Иванов ", G=Иван Иванович, CN=Иванов Иван Иванович"	
Заполнить компоненты имени из сертификата Выпустить сертификат	
Аутентификация по сертификату 👻	
Файл сертификата : Ivanov.cer	•
Выберите файл файл не выбран 2 Загрузить Отмена 3	

Рисунок 11 - Импорт сертификата для аутентификации

Для включенияпервичной 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

Способы входа -

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).

Аутентификация по паролю 👻		
Отправить пароль:		
отобразить на странице		
Создать новый пароль	Отмена	
	3	

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).

тентификация по паро	ПЮ 🔻	
Пароль успешно сбр	ршен.	
Новый пароль:	b4U0X	
Идентификатор для вхо	да: <b>Ivanov</b> 📝 Изменить	

Пароль назначен 🛛 📝 Сбросить

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)

Методы вторичной аутентификации	
Аутентификация по SMS 👻	
Номер телефона: не назначен <u>В Назначить</u>	
Отсутствуют подтвержденные номера телефонов для отправки одноразовых паролей. + Добавить	
Аутентификация по электронной почте 👻	
Электронная почта: не назначена 📝 Назначить	
Аутентификация с помощью мобильного приложения 👻	

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).

		Operator
KP/IIIIOIIPO	Центр идентификации КриптоПро DSS	
	Контактиза информация пользорателя Иранов Иран Ирановиц	4 Hasan
Пользователи		₹ пазад
Личный кабинет		_
Оповещения оператора	Номера телефонов Варианты использования	Отправка оповещений
Средства аутентификации	Нет добавленных номеров телефонов	
Аудит		
	+993-9-999-9999 Добавить	

Рисунок 16 - Добавление номера телефона в контактной информации

После возращения на страницу настроек аутентификации раскройте блок «*Аутентификация noSMS*» и выберете 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 ОАТН

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

Выбери	ите способ генерации одн	оразовых паролей
	Брелок	Мобильное приложение

Рисунок 18 - Способ генерации одноразовых паролей

3.2.2.2.1. Генерация одноразовых паролей с помощью брелока

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

ЖТЯИ.00082-01 90 03 06. ПАК «Кр	риптоП	ро DSS». Инст	рукция (	Оператор	ра СЭП

## аутентификация» в активное положение.

Брелок	Мобильное приложение	
ерийный номер токена		
Number		
Іервый ОТР		
00000		
Зторой ОТР		
111111		

Рисунок 19 - Ввод параметров аутентификации по протоколу ОАТН

3.2.2.2.2. Генерация одноразовых паролей через мобильное приложение

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

Рисунок 20 - Аутентификация с помощью мобильного приложения

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

#### Аутентификация по протоколу ОАТН -

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 (<u>App Store | Google Play</u>)
- Google Authenticator (<u>App Store | Google Play</u>)
- Microsoft Authenticator (<u>App Store</u> | <u>Google Play</u>)
- Другие приложения, поддерживающие протокол ОАТН

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

П Отвязать приложение

Народни на вернуться

#### Рисунок 21 - QR для сканирования в мобильном приложении

После OR-кода одноразовые сканирования пароли будут генерироваться Для включения метода аутентификации необходимо автоматически. установить «Аутентификация по протоколу ОАТН» переключатель В группе «Вторичная аутентификация» в активное положение.

#### 3.2.2.3 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).

Адреса электронной почты		
Нет добавленных адресов электронной п	очты	
test@test.ru	Добавить	
		)

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).

Аутентификация по электронной почте 🔻	
Электронная почта: не назначена С <u>Назначить</u>	
Выберите адрес для получения одноразовых паролей:	
test@test.ru 🗸	
Выбрать Отмена	

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.

Аутентификация с помощью мобильного приложения 👻	
Нет зарегистрированных устройств для аутентификации.	
<ul> <li>Добавить устройство</li> </ul>	

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).

птирикации с полющою пооблопою приложении -	0
Нет зарегистрированных устройств для аутентификации.	
]анные для инициализации нового устройства	
Система myDSS: DSSClient	
3ремя создания ключа: 17.01.2023 16:25:19	
Срок истечения ключа: 24.01.2023 0:00:00	
Статус: Active 🔒 Заблокировать	
Распечатать QR-код	
Pacnetarate QR-Kog	

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 <u>Google Play</u>, <u>Apple App Store</u>, <u>AppGallery</u>.

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 потребуется 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).

16:29 7	16:30 t/	16:30 7
←	Введите новый пароль	the second s
Выберите способ защиты учётной записи	Введите пароль для использования в случае ошибки TouchID	
ПИН-код / TouchiD / FaceID	9 8 9	
Без ПИН-кода		
	Пароль	Хотите разрешить «КриптоПро DSS Client»
	Подтверждение пароля	использовать Face ID? Идентификация пользователя
		Запретить Разрешить
	I I I	
	I I I	
Применить	Подтвердить	

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)	
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	

Доступ к операциям	
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	

## 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.

		🛔 Operator 🛩
KPUITIOT IPO	Центр идентификации Кр Подт	верждение операции *
Пользователи	Вы под Личная информация по	тверждаете блокировку пользователя?
Личный кабинет		Нет Да акты 🛡 Аутентификация 🌲 Оповещения 📾 Клонировать
Оповещения оператора	Отображаемое имя	Иванов Иван Иванович
Средства аутентификации	Группа	Группа по умолчанию
Аудит	Логин	Ivanov
	Имя Отчество	Иван Иванович
	Общее имя	Иванов Иван Иванович
	Фамилия	Иванов
	Инициалы	

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).

										🔒 Operator	
KPUITIOI IPO	Центр идентифика	ации Кр. Подтвержд	Подтверждение операции ×								
Пользователи	Пользователи	Вы подтвержда	Вы подтверждаете удаление пользователя?				<b>Т</b> Фиј	іьтр Сі	здать но	вого пол)	ьзователя
Личный кабинет		_	Нет Да		Нет Да						
	Логин 🗢	Имя	помор толофони	Афросноты	Hara betweethadam	÷ Г	руппа	Управлен	ие польз	ователем	1
	Ivanov	Иванов Иван Иванович	99399999999		26.04.2023		Default		3 0		<b>a</b>
	test										
	Внешние логины: adfs: test@ad.ru	testovii	78983247238		23.05.2022	fo	orAPI	X	3 0		
	realsts: test										

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).

					🛔 Operator 👻
KPUITIOI IPO	Сервер электр	Управление пользователем test			
Сертификаты	Сертификать	si <b>C</b>		🗎 Удалить все 🕇 Создать зая	прос на сертификат 🎿 Установить сертификат
	Субъект	Удостоверяющий центр	Статус	Расположение ключа 💿	
Завершить управление	test	EnrollName	Обрабатывается	Server	• Просмотр

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».

Далее нужно задать Удостоверяющий центр, к которому будет направлен запрос на сертификат. По умолчанию для экземпляра создается один обработчик УЦ «Сторонний УЦ», который необходим для создания запросов. Прямая интеграция с УЦ возможна при подключении соответствующей услуги.

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

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

Параметры времени действия сертификата 👻							
Тип идентификации заявителя 👻							
	Создать запрос						

#### Рисунок 34 - Создание запроса на сертификат

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

Дополнительные параметры	×
Вы можете задать pin-код для контейнера. Введите его в текстовое поле ниже: Пин-код	
Пин-код Подтверждение пин-кода	
Подтверждение пин-кода	
Отмена	ок

Рисунок 35 - Запрос пин-кода

Откроется информация о запросе на сертификат. Нажмите кнопку «Скачать» для сохранения запроса на сертификат (см. Рисунок 36 - Информация о запросе на сертификат). Статус запроса – «Обрабатывается». Данный файл требуется передать в Удостоверяющий центр для выпуска сертификата.

Сервер электронной подписи КриптоПро DSS	Управление пользователем Ivanov
Запрос на сертификат	
🧕 Информация о запросе	
Субъект	СN=Иванов Иван Иванович
Издатель	EnrollName
Статус	Обрабатывается
🕹 Скачать 🔒 Печать 📋 Удалить	

Рисунок 36 - Информация о запросе на сертификат

Файл запроса имеет расширение \*.req и представляет собой файл, содержащий данные о владельце и другую информацию для выпуска сертификата (см. Рисунок 37 - Файл запроса на сертификат)



Рисунок 37 - Файл запроса на сертификат

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

Выберите УЦ, которому будет направлен запрос на сертификат и заполните данные в «Компоненты имени сертификата». 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 38 - Запрос на сертификат).

Информация о запросе 😂							
	Субъект Издатель Статус	CN=test EnrollName Ожидает подписи					
🛓 Скачать 🔒 Печать	🖻 Удалить						

## Рисунок 38 - 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».

Запрос на сертификат

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 39 - Подписание запроса на мобильном устройстве).

YOTAII 🙃 18,7B/s 🕼	ଷ 🔃 🖸 🗐 85 % 💷 10:31	YOTA 📶 🗟 18,7B/s 🗘	🀱 🔃 🖸 i🗍 185 % 💷 10:32	YOTA 📶 🔶 736B/s	🕸 🕅 ୖୖୗ ଏ 🏳 । 82 % 📶 । 11:53
<b>≕</b> Настройки		÷		КриптоПро CSP	
Учётные записи Сертиф	икаты Ключи подписи	Тест			
Tec	r	Запрос на сертификат не г Запрос на физ. лицо (кл	юдписан юч в моб. приложении)		
<b>Тест</b> Активен		Расширенная инфо	ормация 🗸		
Срок действия: с 03.02.2023 г. 09:33 до 03.05.2023 г. 09:43		Подпис	ать запрос		
		Уд	алить	Биологический д Нажимайте	атчик случайных чисел. на экран пока ключ
Тест Запрос на сертификат не подг	ИСан	Выберите ключевой	носитель	не б	удет создан.
		Это устройство	~ )		
Создать новый	сертификат				
Установить с	ертификат			-	Отмена
< ○ ○		$\bigtriangledown$	0	$\triangleleft$	0 🗆

Рисунок 39 - 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».



В web-интерфейсе нажмите «*Скачать*» для сохранения запроса на сертификат. Файл запроса имеет расширение .req и представляет собой файл, содержащий данные о владельце и другую информацию для выпуска сертификата (см. Рисунок 38 - Запрос на сертификат). Данный файл требуется передать в Удостоверяющий центр для выпуска сертификата.

## 3.2.5.2.3. Установка сертификата Пользователя

После получения сертификата в Удостоверяющем центре требуется его установить в СЭП. Для это выполните следующие действия:

- 1. Откройте список сертификатов пользователя.
- 2. Нажмите кнопку «Установить сертификат».
- 3. Выберите сертификат и нажмите кнопку «Загрузить сертификат» (см. Рисунок 40
  - Загрузка сертификата в СЭП):

		🛓 Operator 👻
KPUITTOTIPO	Сервер электронной подписи КриптоПро DSS	Управление пользователем User
Сертификаты Завершить управление	Загрузка нового сертификата Из файла Выбрать Загрузить сертификат З	
		17

Рисунок 40 - Загрузка сертификата в СЭП

4. После успешной загрузки статус сертификата изменится на «Действителен».

Это означает, что сертификат готов к работе и его можно использовать для формирования ЭП и шифрования данных в адрес владельца сертификата.

При нажатии кнопки «Просмотр» отобразится информация о изданном сертификате (см. Рисунок 41 - Информация о сертификате).

Сертифи	ікат							
	🖗 Информация о сертификате 🥲							
		Субъект	СN=Иванов Иван, C=RU, SN="Иванов *, G=Иван					
		Издатель	CN=Sub-TESTCA20-2012-CA, O="OOO ""КРИПТО-ПРО"", OU=Удостоверяющий центр, STREET=ул. Сущёвский Вал 18, L=Mocxва, C=RU, ИНН=007717107991, ОГРН=1037700085444					
		Статус	Действителен					
		Срок действия	C 26.04.2023 18:29:04 no 26.04.2024 18:39:04					
		Срок действия закрытого ключа	C 26.04.2023 18:39:02 no 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					
🛓 Ска	чать 🔒 Печать	Изменить дружественное имя 🗇 Удалить	Отозвать Приостановить Возобновить СОбновить 🔍 Обновить ч. Сменить пин					
Назна	чить сертификатом	по умолчанию						

Рисунок 41 - Информация о сертификате

## 3.2.5.3. Установка сертификата, не зарегистрированного в СЭП Для установки в СЭП существующего сертификата и ключа из контейнера РFX нужно на странице «Сертификаты» нажать кнопку «Установить сертификат». В открывшемся диалоговом окне следует нажать копку «Выбрать» и указать путь до файла с расширением PFX, после чего нажать кнопку «Открыть» (см. Рисунок 42 - Импорт pfx)

КРИПТОПРО	Сервер электронн	юй подписи КриптоПро	DSS		
Сертификаты	Загрузка нового	сертификата		1	
Завершить управление		Установить сертификат	на сервер электронной подписи	на данный компьютер	
		Из файла		0	Выбрать
			4 Загрузить сертификат		2
		Из хранилища	выорать		
	Открытие				×
	← → • ↑ 🖡 «	Рабочий стол 🕨 серти	ບ Поиск: сертифи	икат 🔎	
	Упорядочить • С	оздать папку			• •
	🔚 Видео	^ Имя	^	Дата изменения	Тип
	[ Документы	🗔 1.cer		07.06.2022 11:07	Сертификат б
	惧 Загрузки	🎲 1.pfx		24.05.2022 17:11	Файл обмена
	🔚 Изображения	🏹 12.pfx		07.06.2022 12:52	Файл обмена
	]) Музыка	🧊 1307_02.pfx		13.07.2022 12:38	Файл обмена 🗸
	늘 Рабочий стол	× <			>
	<u>И</u> мя фа	йла: 1.cer		∽ Пользо	вательскуе файл \vee
		L		<u>О</u> ткр	оыть Отмена

Рисунок 42 - Импорт pfx

Далее в интерфейсе СЭП следует нажать кнопку «Загрузить сертификат». После выполнения указанных выше действий появится диалоговое окно с запросом ПИНкода доступа к ключу электронной подписи, содержащемуся в файле PFX. Необходимо ввести ПИН-код и нажать кнопку «ОК» (см. Рисунок 43 - Ввод ПИН-кода к контейнеру PFX).

Запрос пин-кода для доступа к закрытому ключу	×
Введите пин-код для доступа к закрытому ключу в текстовое поле ниже Пин-код	
•••••	
Отмена	ок

Рисунок 43 - Ввод ПИН-кода к контейнеру PFX

После этого импортированный сертификат появится в списке сертификатов Пользователя (см. Рисунок 44 - Импортированный сертификат в списке сертификатов Пользователя).

	La Operator								
KPUITIOI IPO	Сервер электронной подписи	и КриптоПро DSS			Управление пользователем Ivanov				
Сертификаты	Сертификаты 🤁			🟛 Удалить все	+ Создать запрос на сертификат	🛓 Установить сертификат			
Завершить управление	Субъект	Удостоверяющий центр	Статус	Расположен	ие ключа				
	Иванов Иван Иванович	OOB_EnrollName	Обрабатывается	Server	•	🖲 Просмотр			
	test	OutOfB	Действителен	Server		🖲 Просмотр			

Рисунок 44 - 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 45 - Выбор сертификата для управления).

Сервер электронной подписи КриптоПро DSS Управление пользователем Ivano							
Сертификаты			🗎 Удалить все 🕂 Создать запрос на сертифика	т 🛃 Установить сертификат			
Субъект	Удостоверяющий центр	Статус	Расположение ключа 🕐				
Иванов Иван Иванович	OOB_EnrollName	Обрабатывается	Server	Просмотр			
test	OutOfB	Действителен	Server	• Просмотр			



Оператору доступны следующие операции управления сертификатом (см. Рисунок 46 - 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.
  - «Назначить сертификатом по умолчанию» выбрать данный сертификат

по умолчанию из всех сертификатов Пользователя.

Сервер электронной подписи КриптоПро DSS						
Сертификат						
👰 Информация о сертификате 🤤						
Субъект	CN=Иванов Иван Иванович					
Издатель	CN="Тестовый УЦ ООО ""КРИПТО-ПРО"", О="ООО ""КРИПТО-ПРО"", L=Москва, S=г. Москва, ОГРН=1234567890123					
Статус	Не проверялся					
Срок действия	C 28.04.2023 9:05:49 no 13.07.2023 17:30:01					
Срок действия закрытого ключа	a C 26.04.2023 18:30:56 no 26.07.2024 18:30:56					
Отпечаток	C81AE24E003637A37B8346DD67F79E8CFB7E5B5C					
Серийный номер	7C0009536EED38C70B98F012A200020009536E					
Алгоритм открытого ключа	1.2.643.7.1.1.1.1 (ГОСТ Р 34.10-2012 256 бит)					
Улучшенный ключ	Временный доступ к Центру Регистрации (1.2.643.2.2.34.2)					
	Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)					
	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)					
Дружественное имя	Не задано					
🛓 Скачать 🖨 Печать 🍽 Изменить дружественное имя 🗎 У	/далить					
П Назначить сертификатом по умолчанию						

Рисунок 46 - Функции управления сертификатом

## 4. Раздел «Личный кабинет»

Раздел позволяет просматривать и редактировать личные данные Оператора (см. Рисунок 47 - Просмотр личных данных Оператора). При нажатии на кнопку «*Редактировать*» доступно изменения ФИО Оператора. Для сохранения изменений необходимо нажать кнопку «*Сохранить*».



Рисунок 47 - Просмотр личных данных Оператора

## 5. Раздел «Оповещения оператора»

Раздел позволяет управлять списком операций для оповещения и методами оповещения (см. Рисунок 48 - Настройка оповещений оператора).

			Operator					
KPUITIOI IPO	Центр идентификации КриптоПро DSS							
Пользователи	Политика оповещения оператора							
Личный кабинет								
Оповещения оператора	О	повещать в <b>SMS</b>	Оповещать в <b>Email</b>					
Средства аутентификации								
Аудит	Для получения SMS-уведомлений укажите номер телефона с помощью командлета Powershell "Set-DssIdentityOperator".							
	Управление учетными данными	Φ						
	Изменение данных учетной записи пользователя	۵						
	Ошибка при изменении данных учетной записи пользователя	۵						

Рисунок 48 - Настройка оповещений оператора

## 6. Раздел «Средства аутентификации»

Раздел позволяет просматривать перечень назначенных Пользователям средств аутентификации (см. Рисунок 49 - Перечень средств аутентификации).

	🛔 Operator 🛩							
KPUITTOTIPO	Центр идентификации КриптоПро DSS							
Пользователи	Средства аутентификации 🔻 Фил							
Личный кабинет								
	Серийный номер 🗘	Назначен	Логин пользователя	Псевдоним 🗘	Тип токена 🗘	Лицензия на средство 🗘		
Оповещения оператора	444962581827928020			5af980ac-037c-4c8b- a82d-c1eed869e525	MobileAuth			
Средства аутентификации	7335984			M18E6DE19EL3	MyDss			
Аудит	70///05							
	./341435			0UN8N988Y5KY	MyDss			
	99399999999	+	lvanov		SmsOtp			

Рисунок 49 - 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 50 - Аудит событий СЭП).

								🛔 Operator 👻
КРИПТОПРО	Центр	иденти	фикации Крипт	оПро DSS				
Пользователи	Журнал Аудита							Фильтр 🔻
Личный кабинет						Тредыдушая	↔	Следующая
Оповещения оператора								
Средства аутентификации	ID	Статус	Код события	Дата	Данные			Учетные данные
Аудит	13133	~	Пользователь аутентифицирован по токену (JWT/SAML) (331)	2023-04-27 17:39:10	озователь аутентифицирован по токену (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. Ли	Іогин: 14_09.		Оператор: 14_09 Пользователь: 14_09

Рисунок 50 - Аудит событий СЭП

Перечень рисунков	
Рисунок 1 – Добавление сайта в зону надежных сайтов	4
Рисунок 2 – Включение ActiveX	5
Рисунок 3 – Включение поддержки ГОСТ	5
Рисунок 4 - Аутентификация Оператора	6
Рисунок 5 - Начальная страница веб-интерфейса Оператора	6
Рисунок 6 - Создание нового Пользователя.	8
Рисунок 7 - Ввод сведений о Пользователе	8
Рисунок 8 - Управление Пользователем	9
Рисунок 9 - Лействия лля управления Пользователем	9
Рисунок 10 - Релактирование атрибутов Пользователя	
Рисунок 11 - Импорт сертификата для аутентификации	
Рисунок 12 - Генерация пароля Пользователя	
Рисунок 13 - Выбор метода отправки пародя	13
Рисунок 13 - Включение аутентификации по паролю	13
Рисунок 15 - Лобавление номера телефона	14
Рисунок 16 - Добавление номера телефона в контактной информации	14
Рисунок 17 - Включение метода аутентификации по SMS	
Рисунок 18 - Способ генерации одноразовых пародей	
Рисунск 19 - Врод параметров аутентификации по протокоду ОАТН	
Pисунок 19 - Бвод нараметров аутентификации по протоколу ОТТП	
Рисунок 20 - Аутентификация с помощью мобильного приложения	
Тисунок 21 - QK для сканирования в мооильном приложении	
Рисунок 22 - Добавление адреса электронной почты	
$P_{\rm Heymore} 23 - Бысор адреса электронной почты$	
Provider 25 OB rou and DSS Client	
Тисунок 25 - QR-код для DSS Спент Рисунок 26 - Первый запуск мобильного приложения	
Рисунок 20 - Первый запуск моойльного приложения	
Provider 28 - Solution and the north processing	
Рисунок 20 - Защита мобильного приложения Рисунок 20 - Информация об уцетной записи пользователя	
Рисунок 20 - Политика доступа и полтверу дения операций	
Рисунок 31 - Блокировка Пользователя	
Рисунок 31 - Блокировка пользователя	
Рисунок 32 - Удаление пользователя	
Pucyhok $33 - 5$ danchuc beex ceptuquikatob	
Pucyhok 35 - Запрос пиц-кола	
$P_{\rm Heyhok} 35 - Запрос пин-кода$	
Pucyнok 37 - Файд запроса на сертификат	
Preverok $38 - 3$ appoe ha ceptudukat	
Рисунок 30 – Запрос на сертификат	20
Рисунок $40 - 3а спуска сертификата в СЭП$	
Pucyhok $40 - 3ai pyska cepinquikara B CS11$	
Pucyhok 47 - Импорт сертификате	
Рисунок 42 - Пипорт сертификат ріх полого РЕХ	
Рисунок 44 - Импортированный сертификат в списке сертификатов Пользователя	
Рисунок 15 - Выбор сертификата для управления	
г неунок то - Быоор сертификата для управления Рисунок 46 - Функции управления сертификатом	
1 поунок 10 - Функции управления сертификатом	
т неупок т / - просмотр литных данных Оператора Рисупок 48 - Настройка опорешений оператора	
исунок 40 - Пастроика оповещении оператора Рисунок 40 - Перецець средств аутентификации	
г неупок $\tau_2$ - перечень средеть аутентификации Рисупок 50 - Аулит событий СЭП	
т неупок это - лудит сообщий Сэтг	