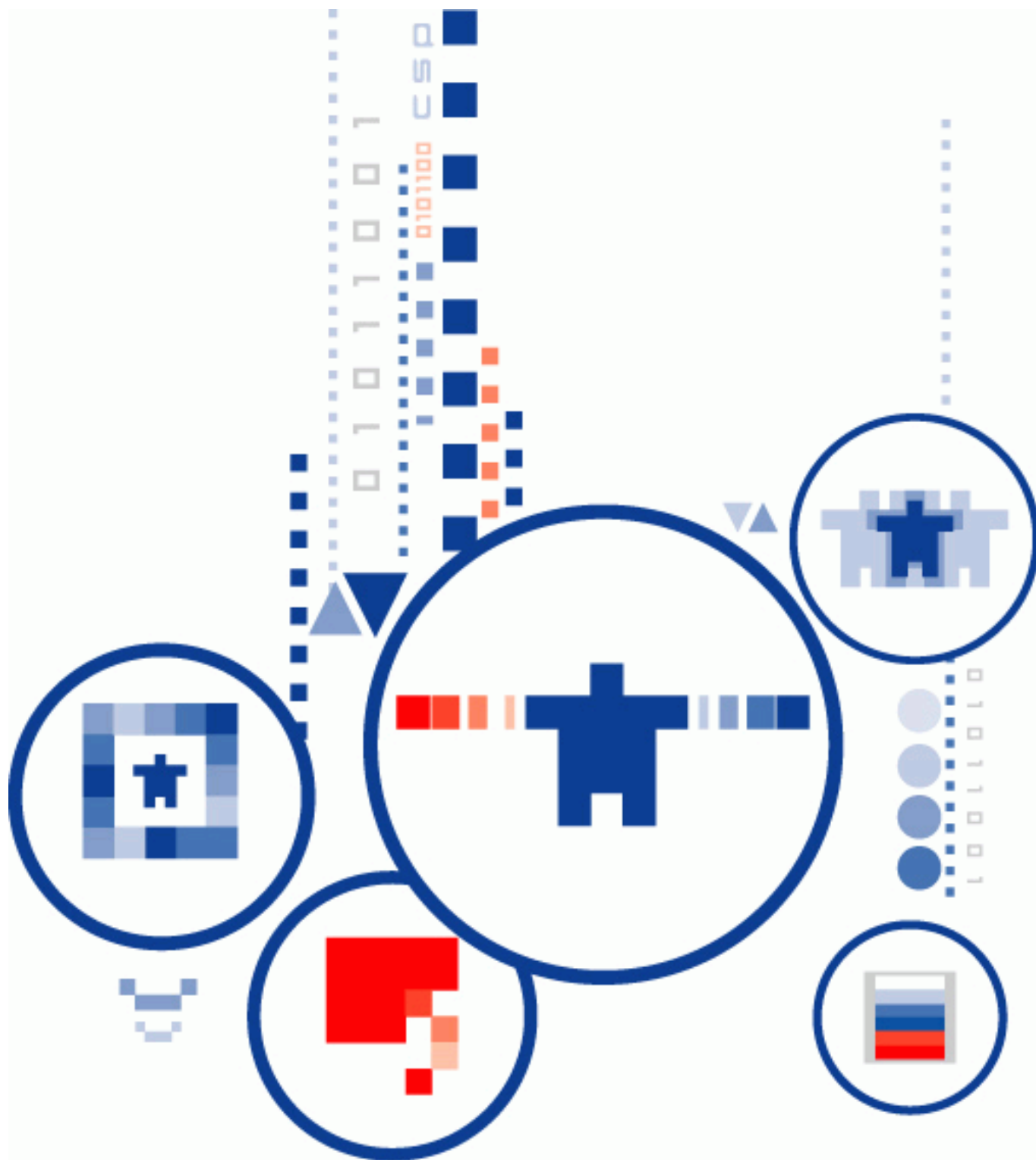




КриптоПро DSS Lite

СЕРВИС ЭЛЕКТРОННОЙ ПОДПИСИ

Инструкция Оператора Удостоверяющего центра

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Операторов Удостоверяющего центра ООО «КРИПТО-ПРО» (УЦ) и определяет порядок использования Веб-интерфейса Сервиса электронной подписи ООО «КРИПТО-ПРО» на базе ПО «КриптоПро DSS Lite» (далее – СЭП) для осуществления операций по регистрации и управлению Пользователями УЦ и их сертификатами ключей проверки электронной подписи.

Информация об Удостоверяющем центре и разработчике ПО «КриптоПро DSS Lite»:

ООО «КРИПТО-ПРО»

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

Телефон: (495) 995 4820

<http://www.CryptoPro.ru>

<http://cpca.cryptopro.ru/>

Е-mail: info@CryptoPro.ru

cpca@cryptopro.ru

Содержание

АННОТАЦИЯ.....	1
СОДЕРЖАНИЕ.....	2
1. ОБЩИЕ ПОЛОЖЕНИЯ.	3
1.1. РЕГИСТРАЦИЯ НОВОГО ПОЛЬЗОВАТЕЛЯ.....	5
2. СОЗДАНИЕ ПЕРВОГО СЕРТИФИКАТА ПОЛЬЗОВАТЕЛЯ	8
3. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ	15
3.1. УПРАВЛЕНИЕ РЕГИСТРАЦИОННЫМИ ДАННЫМИ	15
4. УПРАВЛЕНИЕ СЕРТИФИКАТАМИ ПОЛЬЗОВАТЕЛЕЙ.....	17

1. Общие положения.

Сервис электронной подписи ООО «КРИПТО-ПРО» на базе ПО «КриптоПро DSS Lite» (далее – СЭП) предназначен для предоставления Веб-интерфейса Операторам и Пользователям УЦ, позволяющий осуществлять взаимодействие при выполнении операций по созданию ключей электронной подписи, передачи запросов на создание и управление сертификатами ключей проверки электронной подписи (далее – сертификаты), выполнять операций по созданию и проверке электронной подписи различного формата криптографических сообщений, шифрования и расшифрования электронных документов с использованием СКЗИ «КриптоПро CSP» и ключей электронной подписи на рабочих местах Пользователей УЦ.

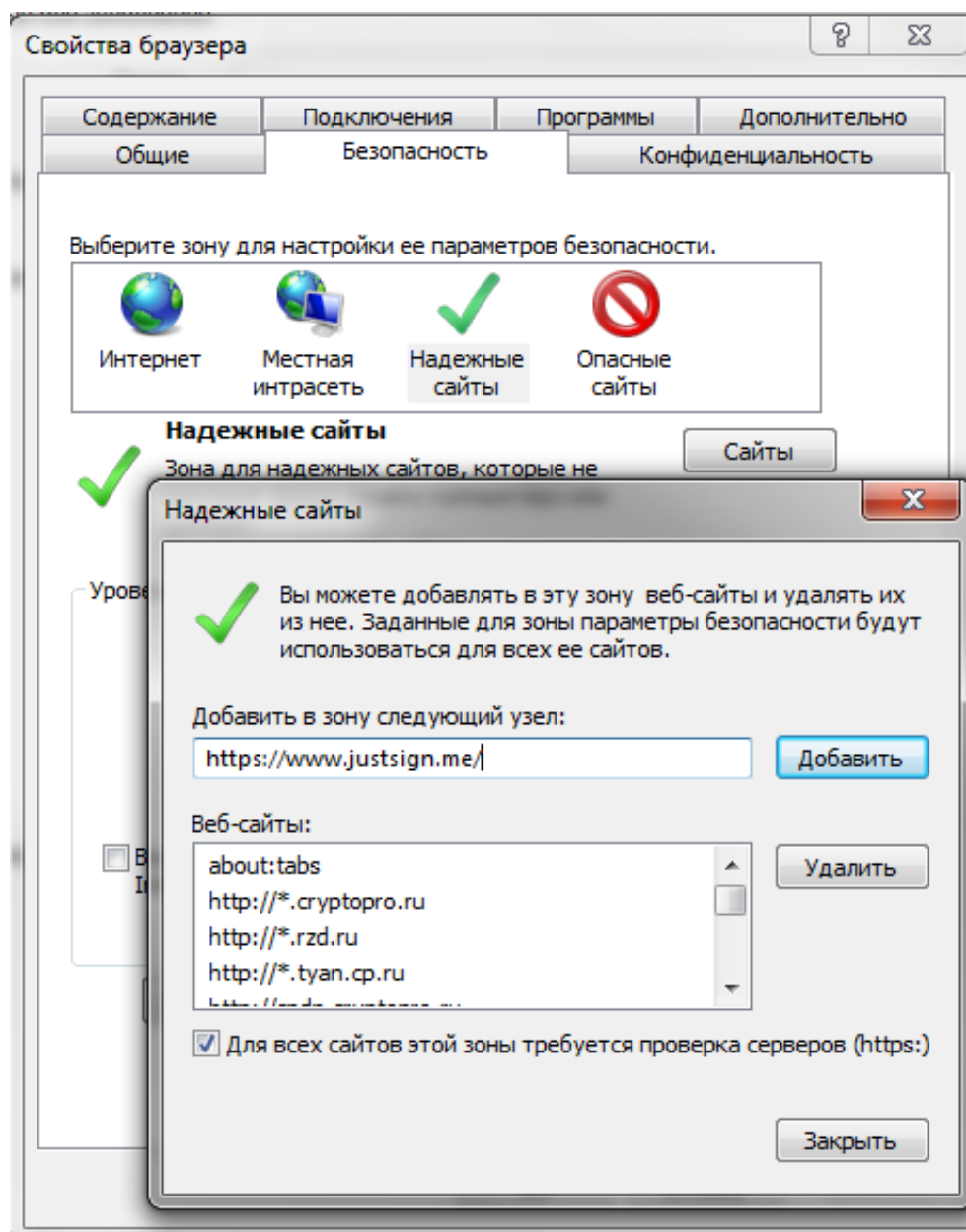
Настоящая инструкция определяет порядок действия Оператора УЦ (далее – Оператор) при выполнении следующих операций:

1. Регистрация нового Пользователя;
2. Создание первого сертификата Пользователя ключа проверки электронной подписи;
3. Управление сертификатами Пользователей (приостановление, возобновление и прекращение действия или обновление сертификатов);
4. Управление Пользователями (редактирование регистрационных данных и параметров аутентификации).

Для выполнения указанных выше операций Оператор должен быть зарегистрирован в СЭП Администратором УЦ.

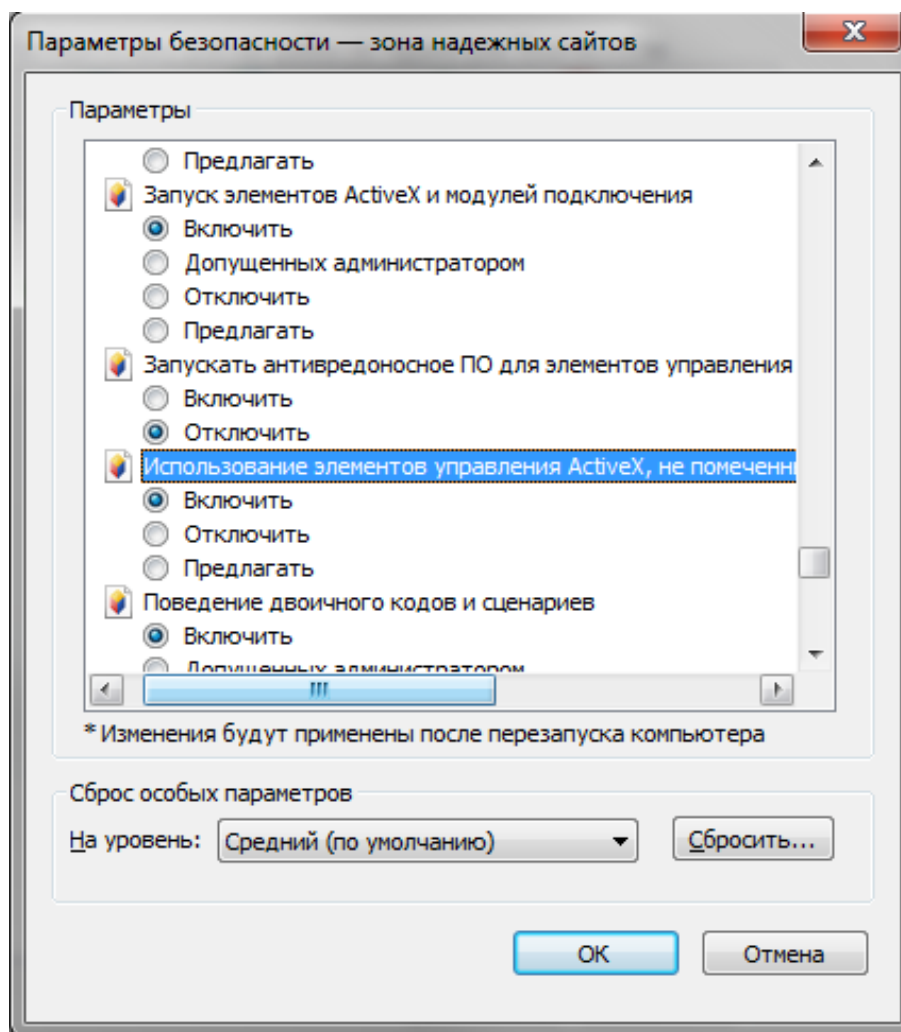
На рабочем месте Оператора под управлением MS Windows 7 или выше должен быть установлен [СКЗИ «КриптоПро CSP» версии 3.9](#) или выше и [КриптоПро ЭЦП Browser plug-in версии 2.0](#). Для подключения к СЭП использовать Интернет-браузер Internet Explorer версии 10 или выше.

Для корректной работы с СЭП необходимо добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выбрать вкладку «Безопасность», в список надежных сайтов добавить узел <https://www.justsign.me/> и сохранить изменения свойств:

Рисунок А. Добавление безопасного узла.

В разделе "Элементы ActiveX и модуль подключения" проверить состояние настройки "Использование элементов управления ActiveX, не помеченных как безопасные для использования" - должно быть "Включить". Для этого зайти в Internet Explorer меню «Сервис - Свойства обозревателя – Безопасность» - для зоны "Надежные узлы" нажать кнопку "Другой":

Рисунок Б. Включение элементов ActiveX.



2. Управление Пользователями

2.1. Регистрация нового Пользователя

1. Регистрация Пользователя осуществляется Оператором в присутствии Пользователя или его уполномоченного представителя в соответствии с полученными заявительными документами.

2. Осуществить вход на СЭП по адресу web-интерфейса Оператора <https://www.justsign.me/opertlitecpcaidp/admins/>, откроется окно выбора сертификата, выбрать сертификат Оператора и нажать «ОК» (см. Рисунок 1):

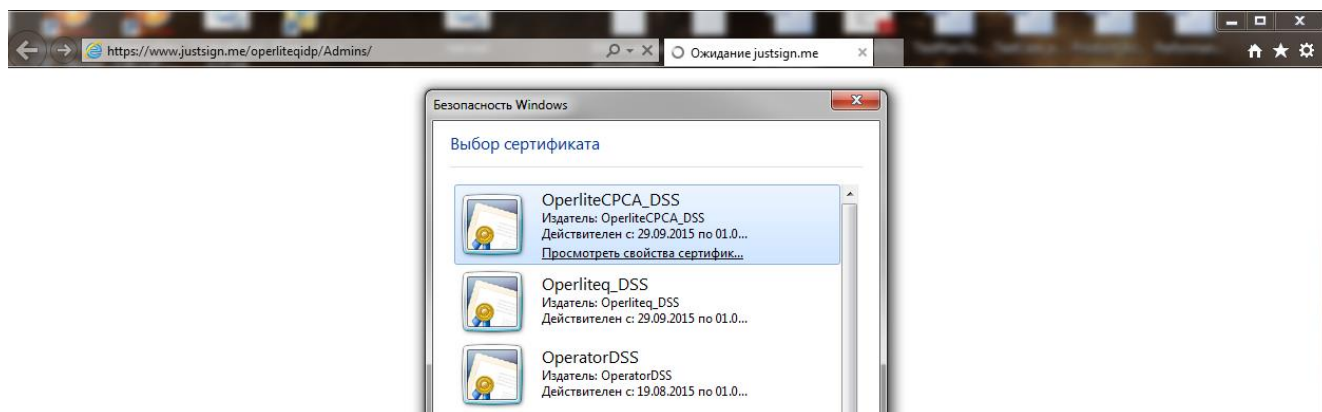


Рисунок 1. Вход в личный кабинет Оператора по сертификату

3. Откроется личный кабинет Оператора (см. Рисунок 2):

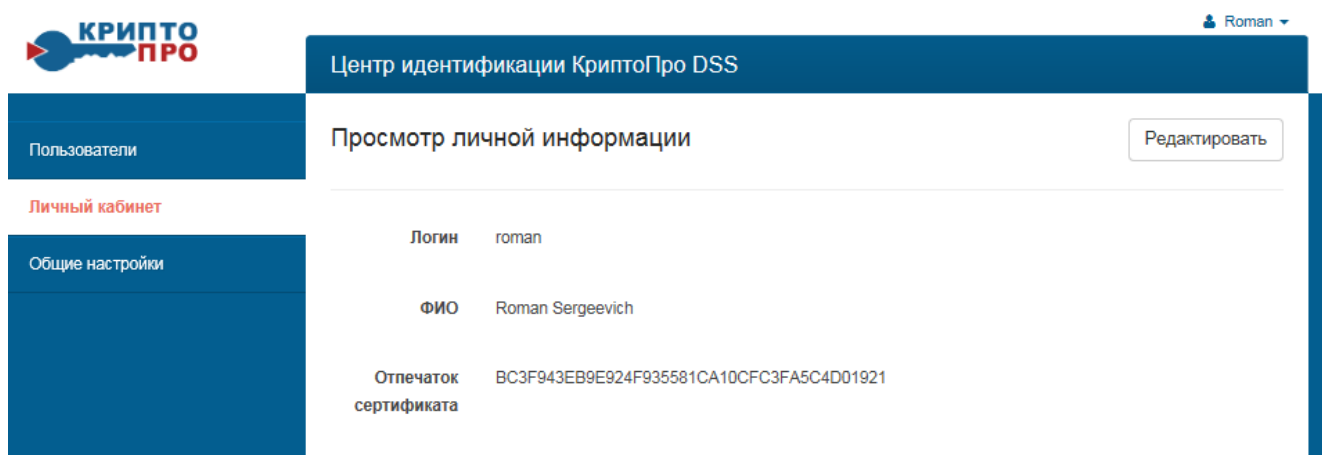


Рисунок 2. Личный кабинет Оператора

4. В меню слева нажать «Пользователи», откроется таблица со списком Пользователей (см. Рисунок 3):

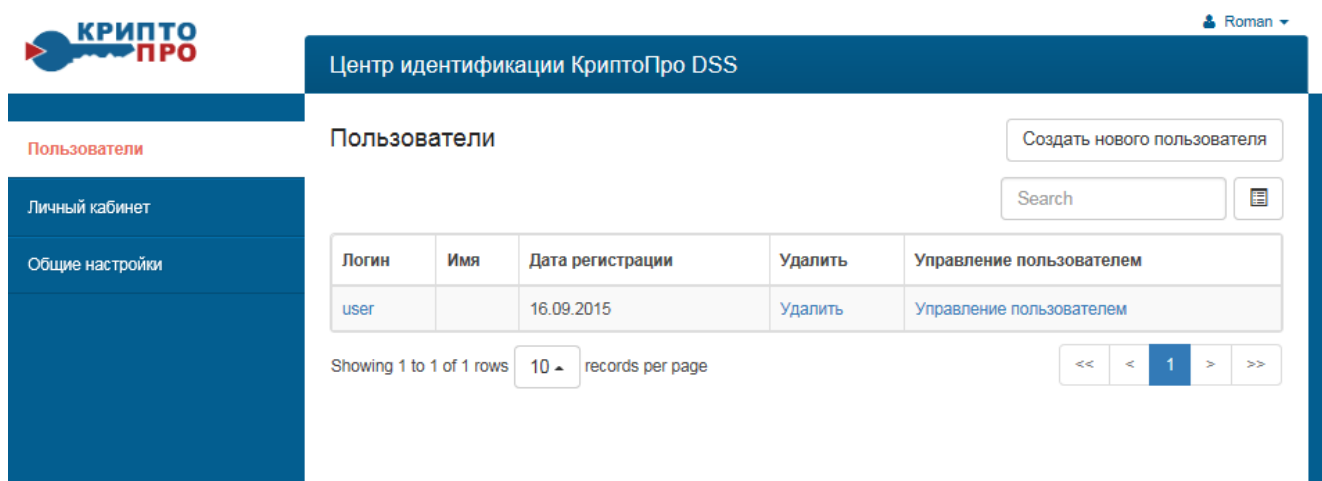


Рисунок 3. Список Пользователей

5. В открывшемся окне справа вверху нажать «Создать нового пользователя», откроется форма регистрации нового Пользователя.

6. Заполнить все поля в соответствии с полученными от Пользователя заявительными документами, и справа вверху нажать «Создать» (см. Рисунок 4):

Рисунок 4. Заполнение регистрационной формы нового Пользователя

7. Откроется окно с уведомлением о создании нового Пользователя и его временный пароль (см. Рисунок 5):

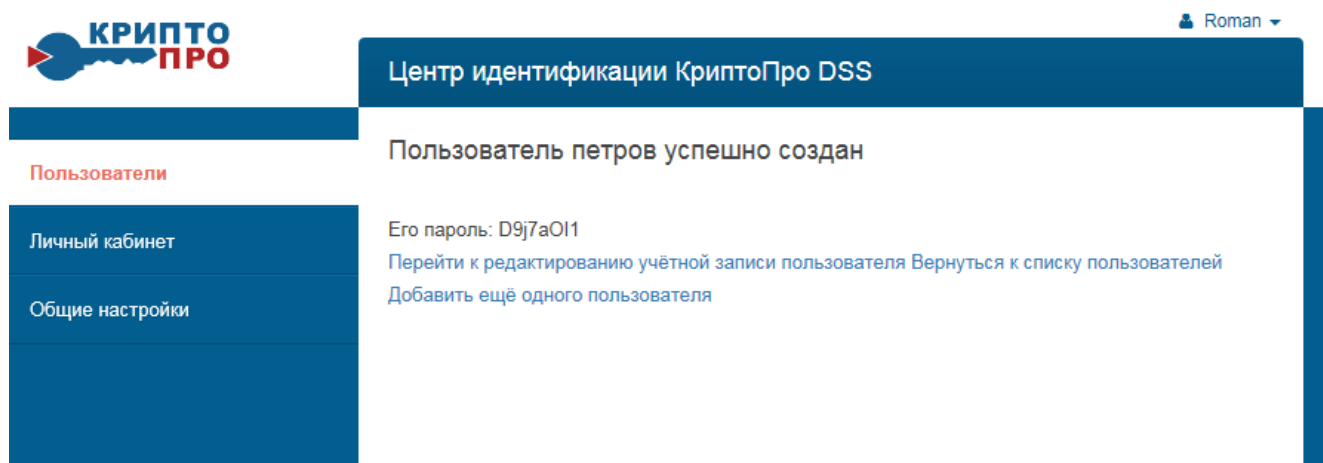


Рисунок 5. Уведомление об успешном создании нового Пользователя

После первого самостоятельного входа пользователь должен сменить полученный пароль. Новый пароль должен состоять не менее чем из 8 буквенно-цифровых знаков и храниться в тайне от прочих лиц.

3. Создание первого сертификата Пользователя

Порядок создания первого сертификата или проведения внеплановой смены сертификата Пользователя (когда отсутствует действующий сертификат Пользователя):

1. Осуществить вход на СЭП – личный кабинет Оператора в соответствии с п. 2-4 Раздела 2.1.
2. На странице списка Пользователей в строке записи Пользователя нажать на ссылку «Управление пользователем» (см. Рисунок 6):

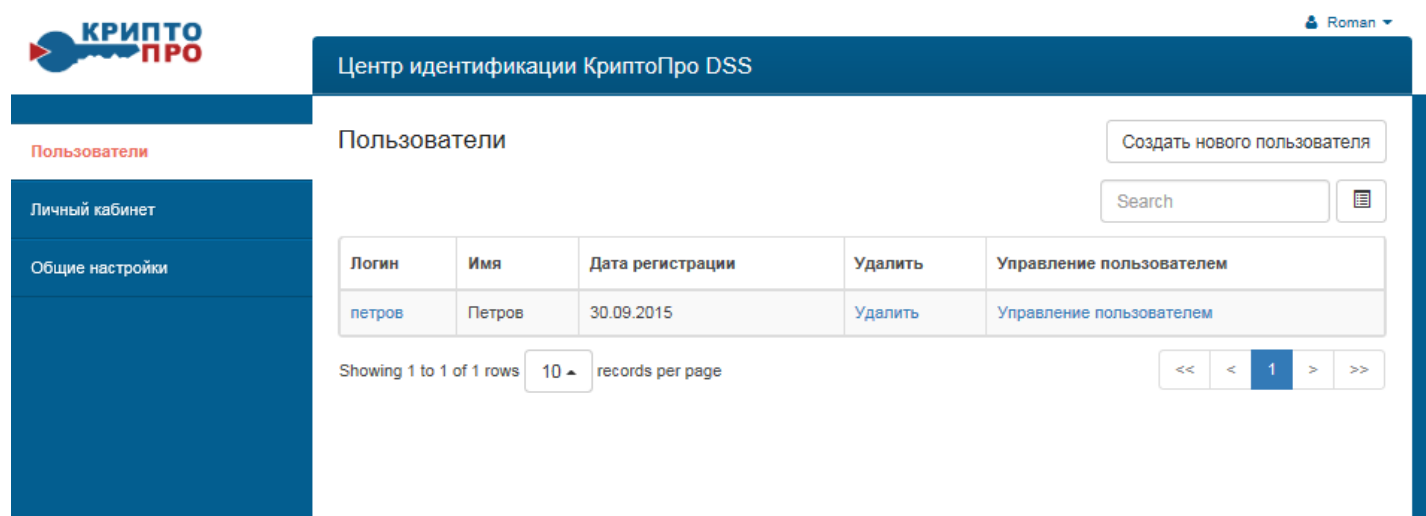


Рисунок 6. Список Пользователей

3. Откроется окно управления сертификатами Пользователя (см. [Рисунок 7](#)):

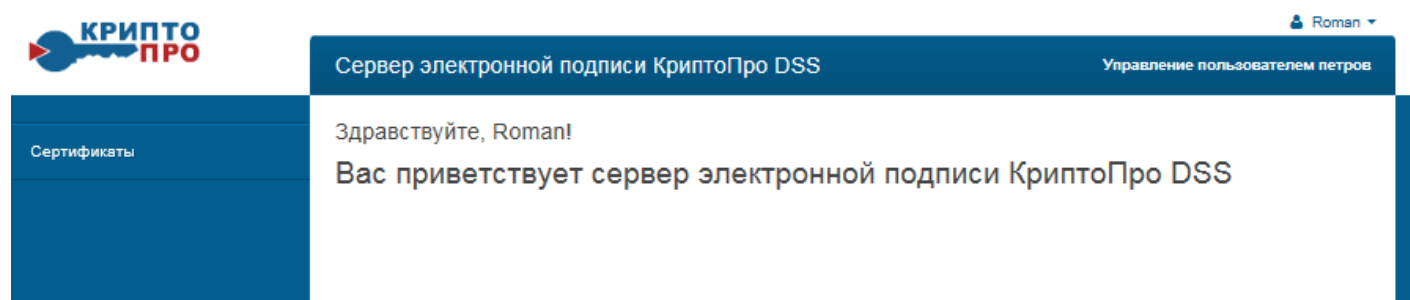


Рисунок 7. Окно управления сертификатами Пользователя

4. Слева нажать на «Сертификаты», откроется окно с перечнем имеющихся сертификатов Пользователя (см. [Рисунок 8](#)):



Рисунок 8. Перечень сертификатов Пользователя

5. Сверху нажать «+ Создать запрос на сертификат», откроется форма с регистрационными данными Пользователя, проверить корректность данных в соответствии с полученными заявительными документами, при необходимости исправить и слева внизу нажать «Создать запрос» (см. [Рисунок 9](#)):

Создание запроса на сертификат

Создание запроса на сертификат для пользователя петров

Выберите УЦ, к которому будет
направлен запрос на сертификат

Тест УЦ DSS



Выберите криптопровайдер

GOST R 34.11-94 + GOST R 34.10-2001 512



Заполните необходимые компоненты имени

Фамилия (SN)

Петров

Имя (G)

Сергей

Инициалы (I)

С.И

Должность/звание (T)

Бухгалтер

Адрес (2.5.4.9)

Пушкин 45

Серийный номер устройства (2.5.4.5)

Общее имя (CN)*

"ОАО ""Очень хорошая компания"""

Подразделение (OU)

Бухгалтерия

Организация (O)

"ОАО ""Очень хорошая компания"""

Город (L)

Москва

Область (S)

Москва

Страна/регион (C)

RU

Электронная почта (E)

petrov@goodcompany.ru

Почтовый адрес (Почтовый адрес)

Выберите шаблон сертификата

Пользователь DSS Lite



Создать запрос

Рисунок 9. Форма запроса на создание сертификата Пользователя

6. При создании ключевого контейнера система отобразит окно выбора ключевого носителя (см. Рисунок 10):

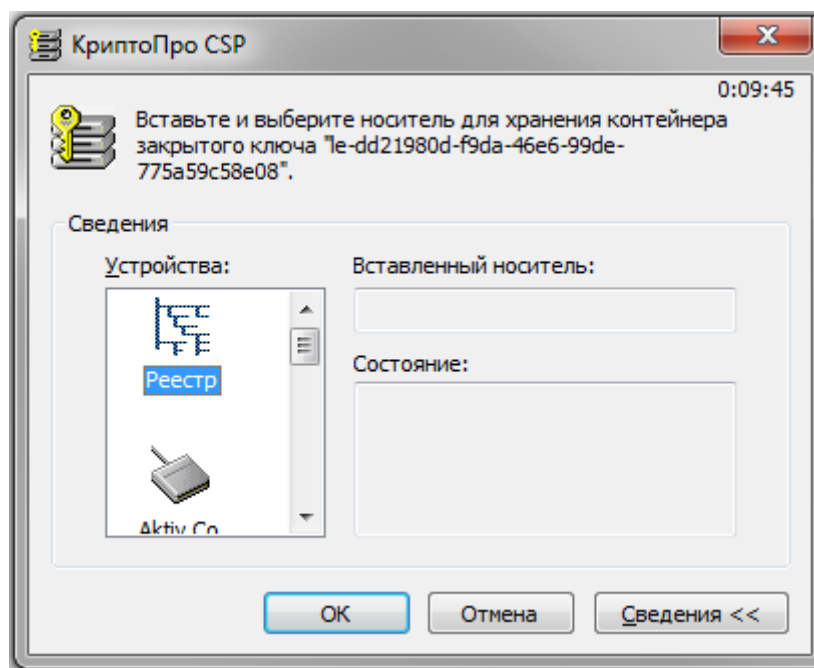


Рисунок 10. Выбор ключевого носителя

7. После выбора ключевого считывателя, если в системе не установлен аппаратный ДСЧ, система отобразит окно «Биологический датчик случайных чисел» (см. Рисунок 11).

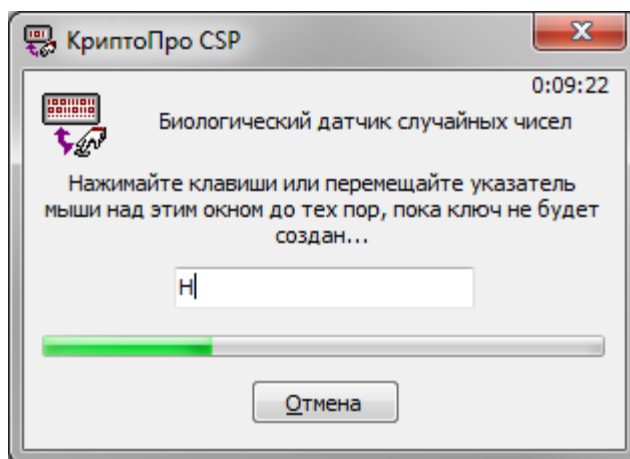


Рисунок 11. Биологический датчик случайных чисел

8. После завершения работы биологического датчика случайных чисел система отобразит окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рисунок 12)

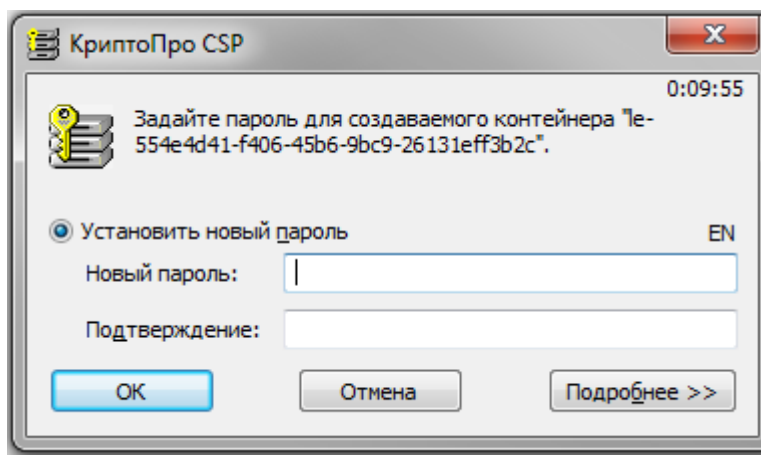


Рисунок 12. Ввод пароля на доступ к закрытому ключу

В этом окне существует возможность ввода текстового пароля на доступ к закрытому ключу создаваемого контейнера (один и тот же пароль необходимо ввести в поля «**Новый пароль**» и «**Подтверждение**»).

После ввода пароля нажмите кнопку «**ОК**».

Если ключ генерируется на носитель, поддерживающий аппаратный пароль или пин-код, то необходимо ввести тот пароль (пин-код), который установлен на этот ключевой носитель.

9. Сертификат будет создан автоматически и откроется окно с перечнем сертификатов Пользователя и информацией о статусе сертификатов (см. Рисунок 13):

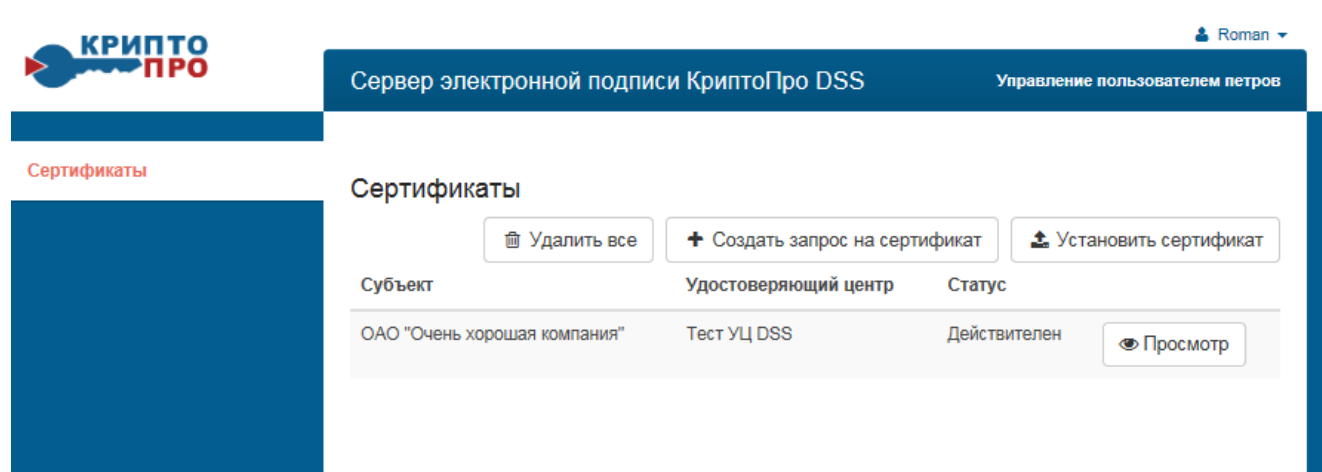


Рисунок 13. Перечень сертификатов Пользователя

10. Нажать кнопку «**Просмотр**», откроется окно с информацией о сертификате и меню управления сертификатом (см. Рисунок 14):

Сертификат



Информация о сертификате

Субъект	SN=Петров, G=Иван, I=И.С, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания"", OU=Бухгалтерия, O="ОАО ""Очень хорошая компания"", L=Москва, S=Москва, C=RU, E=petrov@goodcompany.ru, ОГРН=11223344559512, СНИЛС=10786566676
Издатель	CN=Тестовый УЦ для DSS, O="ООО ""КРИПТО-ПРО"", L=Москва, S=77 г. Москва, C=RU, STREET="ул. Суцёвский вал, д. 18", ИНН=007712345678, ОГРН=1007712345678
Статус	Действителен
Срок действия	С 29.09.2015 14:38:00 по 29.12.2016 14:48:00
Отпечаток	7DCA7DB057F4B6BF11D579AFD945038B717223E7
Серийный номер	23BD0F7C0000000000029
Алгоритм открытого ключа	1.2.643.2.2.19 (ГОСТ Р 34.10-2001)

 Скачать

 Печать

 Удалить

 Отозвать

 Приостановить

 Возобновить

 Обновить

☐ Назначить сертификатом по умолчанию

Рисунок 14. Меню управления сертификатом

11. Нажать кнопку «Печать» откроется печатная форма (см. [Рисунок 15](#))

Наименование организации-Удостоверяющего Центра Сертификат ключа проверки электронной подписи

Сведения о сертификате:**Кому выдан:**

ОАО "Очень хорошая компания"

Кем выдан:

Тестовый УЦ для DSS

Действителен с 29.09.2015 14:38:00 по 29.12.2016 14:48:00

Версия: 3 (0x2)

Серийный номер: 23BD0F7C0000000000029

Издатель сертификата: CN = Тестовый УЦ для DSS, O = ООО "КРИПТО-ПРО", L = Москва, S = 77 г. Москва, C = RU, STREET = ул. Сушэвский вал, д. 18, ИНН = 007712345678, ОГРН = 1007712345678

Срок действия:

Действителен с: 29.09.2015 14:38:00

Действителен по: 29.12.2016 14:48:00

Владелец сертификата: СНИЛС = 10786566676, ОГРН = 1122334459512, ИНН = 007712345678, E = petrov@goodcompany.ru, C = RU, S = Москва, L = Москва, O = ОАО "Очень хорошая компания", OU = Бухгалтерия, CN = ОАО "Очень хорошая компания", STREET = Пушкин 34, T = Бухгалтер, I = И.С., G = Иван, SN = Петров

Ключ проверки электронной подписи:

Алгоритм ключа проверки электронной подписи:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01

Значение: 04 40 b1 fc 02 c1 1b 98 bb a8 8a 43 a6 4c aa 2b 4f 2e 54 72 43 a2 b8 30 43 06 be 15 bb d9 ea 41 cc 53 38 20 00 70 04 ba fa f1 bb a2 5d da c8 1e 2c 8f f2 4d 62 b2 c4 5b f7 56 df 23 b1 5c 77 59 fa 99

Расширения сертификата X.509

1. Расширение

Название: Улучшенный ключ

Значение: Неизвестное использование ключа (1.2.643.2.2.34.33)

2. Расширение (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

3. Расширение

Название: Идентификатор ключа субъекта

Значение: 1e ec de be ab 57 13 57 4a ab 50 55 d5 eb e7 7e 06 28 89 d3

4. Расширение

Название: Идентификатор ключа центра сертификации

Значение: Идентификатор ключа=0c 9a a9 a6 c7 7d 40 fb 76 3d a3 97 ef 03 4e 8f ba 4d 08 85, Поставщик сертификата: Адрес каталога: CN=Тестовый УЦ для DSS, O="ООО "КРИПТО-ПРО"", L=Москва, S=77 г. Москва, C=RU, STREET="ул. Сушэвский вал, д. 18", ИНН=007712345678, ОГРН=1007712345678, Серийный номер сертификата=3d 4b 95 91 f0 c1 a1 88 44 df d8 98 c2 1e 25 4c

5. Расширение

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распространения списка отзыва (CRL): Имя точки распространения: Полное имя: URL=http://testuc-dss/ca/cdp/0c9aa9a6c77d40fb763da397ef034e8fba4d0885.crl, [2]Точка распространения списка отзыва (CRL): Имя точки распространения: Полное имя: URL=http://www.justsign.me/ca/cdp/0c9aa9a6c77d40fb763da397ef034e8fba4d0885.crl

6. Расширение

Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1), дополнительное имя=URL=http://testuc-dss/ocsp/ocsp.srf, [2]Доступ к сведениям центра сертификации: метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1), дополнительное имя=URL=http://www.justsign.me/ocsp/ocsp.srf

7. Расширение

Название: Период использования закрытого ключа

Значение: Действителен с 29 сентября 2015 г. 14:38:00 по 29 декабря 2016 г. 14:38:00

8. Расширение

Название: Политики сертификата

Значение: [1]Политика сертификата: Идентификатор политики=Класс средств ЭП КС1, [2]Политика сертификата: Идентификатор политики=Класс средств ЭП КС2

9. Расширение

Название: Средство электронной подписи владельца

Значение: Средство электронной подписи: КриптоПро CSP (версия 3.6)

10. Расширение

Название: Средства электронной подписи и УЦ издателя

Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6) (заключение: Заключение № 149/3/2-1495 от 02.09.2015), средство удостоверяющего центра: "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 (заключение: Сертификат соответствия № СФ/128-2351 от 15.04.2014)

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2001

Идентификатор: 1.2.643.2.2.3

Значение: 1f 72 55 7b c8 88 7d b8 8e c0 9c 4b cc ca 85 77 c8 76 c6 aa 4e c6 37 d6 ab 92 49 1b 2b e8 fe 47 68 5c 82 d6 ce af f9 9a 85 d3 90 9f 2e 40 f0 4a c2 81 7a f9 c0 2c bc 9b f5 24 55 a0 74 85 b6 0a

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

М. П.

Средство электронной подписи "КриптоПро CSP"

Подписанный бланк сертификата ключа проверки электронной подписи следует переслать по адресу:111111, Москва, ул. XXXXXXXX, д. XX. XXXXXXXXXXXXXXXXXXXXАдминистратору информационной безопасности.

Рисунок 15. Печатная форма сертификата Пользователя

12. Распечатать форму, нажав ctrl+p и выбрав доступный принтер (см. Рисунок 16):

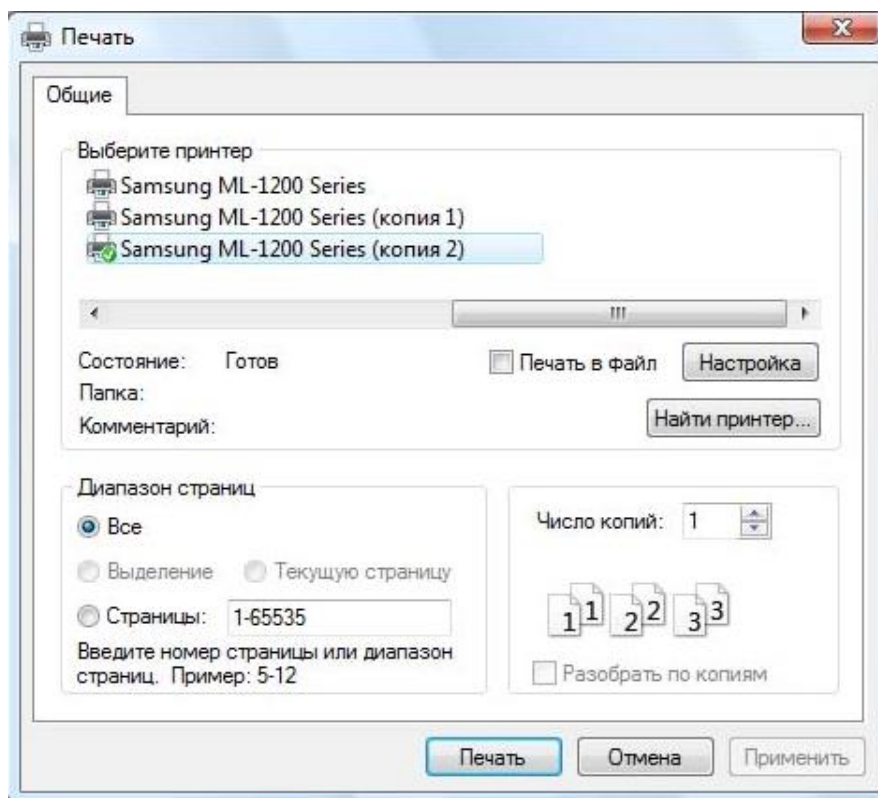


Рисунок 16. Выбор принтера для печати запроса на сертификат

13. Распечатать и подписать копию сертификата Пользователя.
14. Выдать Пользователю логин и временный пароль доступа к СЭП, временный ПИН-код доступа к закрытому ключу.

4. Управление Пользователями

Управление Пользователями, включающее редактирование регистрационных данных и параметров аутентификации, осуществляется в следующем порядке:

4.1. Управление регистрационными данными

1. Осуществить вход на СЭП – личный кабинет Оператора в соответствии с п. 2-4 Раздела 2.1.
2. Нажать на имя Пользователя в поле логин, откроется окно «Просмотр информации о пользователе» (см. Рисунок 17):

КРИПТО ПРО

Центр идентификации КриптоПро DSS

Пользователи

Личный кабинет

Общие настройки

Просмотр информации о пользователе петров

Редактировать

Учётные данные

Параметры аутентификации

Отображаемое имя	Петров
Группа	Группа по умолчанию
Логин	петров
Номер телефона	
Общее имя	"ОАО ""Очень хорошая компания"""
Электронная почта	petrov@goodcompany.ru
Страна	RU
Область	Москва
Город	Москва
Организация	"ОАО ""Очень хорошая компания"""
Подразделение	Бухгалтерия
Адрес	Пушкин 45
Должность	Бухгалтер
Инициалы	С.И
Имя	Сергей
Фамилия	Петров

Сбросить пароль

Заблокировать

Рисунок 17. Просмотр информации о Пользователе

3. Нажать кнопку «**Редактировать**». Откроется окно с редактируемой информацией о Пользователе, исправить данные в соответствии с полученными заявительными и подтверждающими документами (см. Рисунок 18):

КРИПТО ПРО

Центр идентификации КриптоПро DSS

Роман

Пользователи

Личный кабинет

Общие настройки

Редактирование пользователя **петров** Сохранить

Учётные данные Параметры аутентификации

Отображаемое имя

Номер телефона

Общее имя * ×

Электронная почта

Страна

Область

Город

Организация

Подразделение

Адрес

Должность

Инициалы

Имя

Фамилия

Группа ▼

Рисунок 18. Редактирование учетных данных Пользователя

5. Управление сертификатами Пользователей

Порядок управления сертификатами Пользователя (приостановление, возобновление и прекращение действия или обновление сертификата – при наличии действующего сертификата):

1. Открыть окно управления сертификатами Пользователя в соответствии с п. 1-3 Раздела 3.
2. Слева нажать на «Сертификаты», откроется окно с перечнем действующих сертификатов Пользователя (см. Рисунок 19):

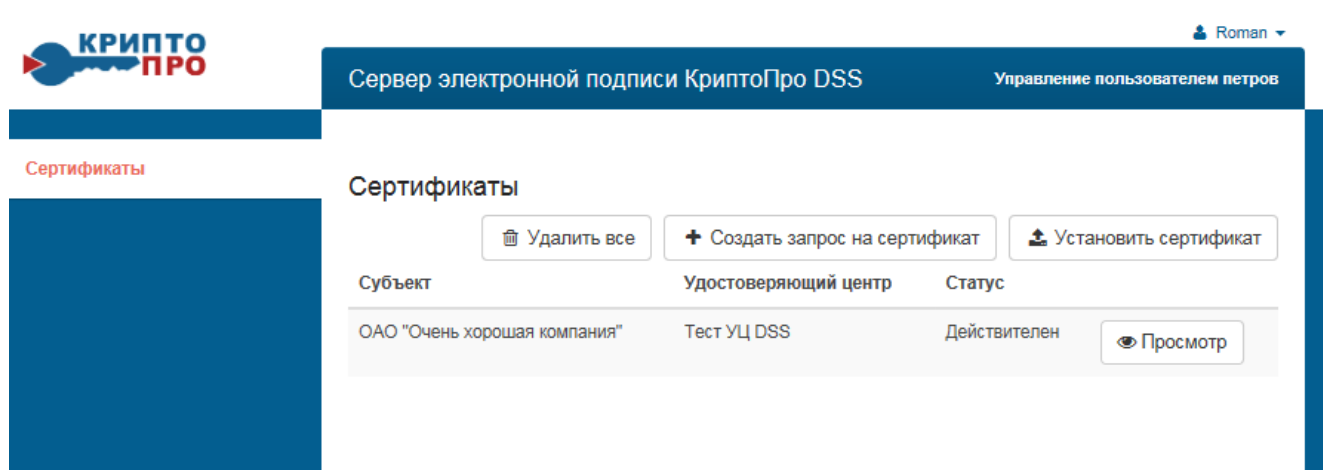


Рисунок 19. Информация о сертификатах Пользователя

3. В записи действующего сертификата нажать кнопку «**Просмотр**», откроется окно с информацией о сертификате и меню управления сертификатом (см. Рисунок 20):

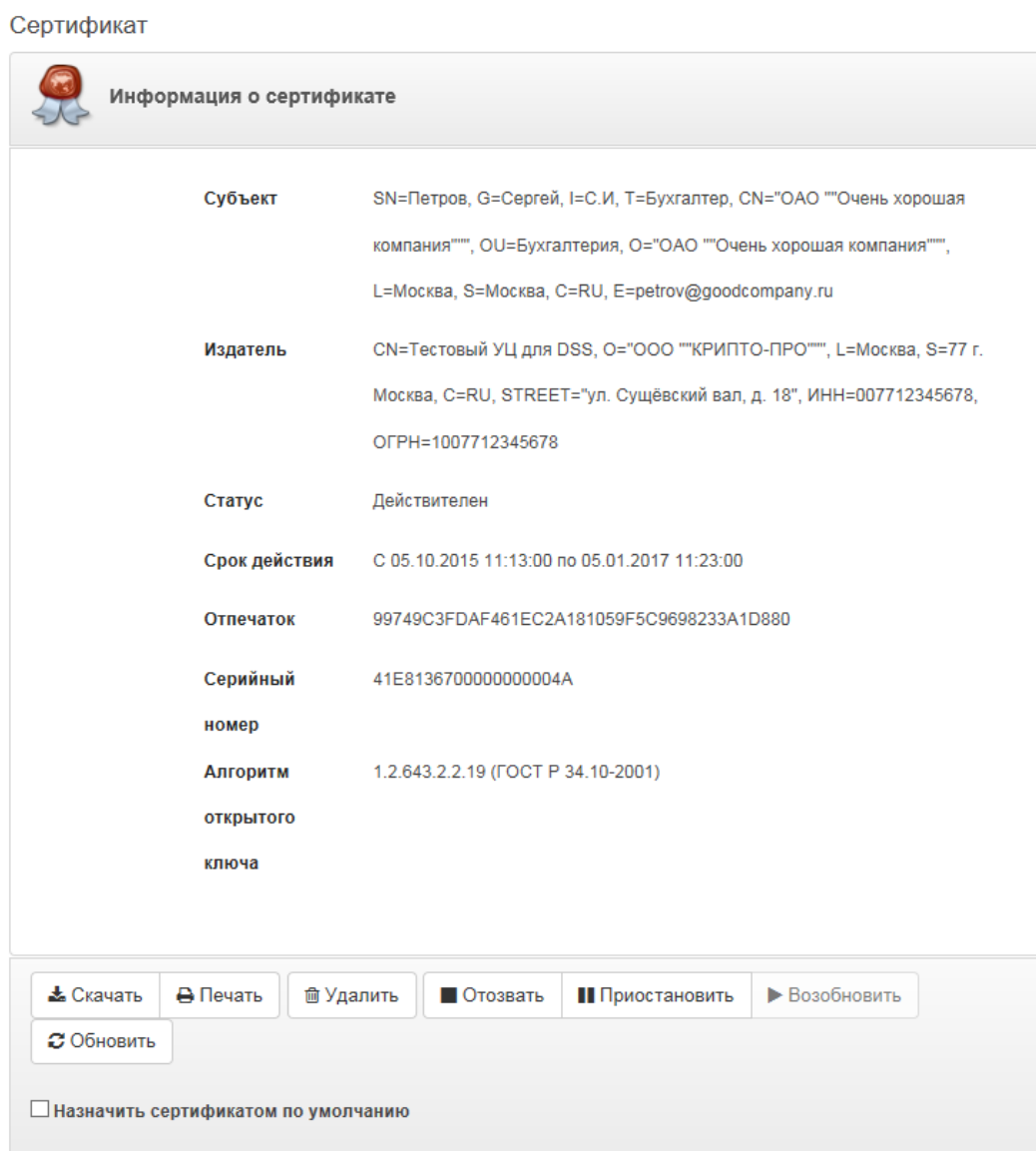


Рисунок 20. Меню управления сертификатом Пользователя

4. В соответствии с требуемой операцией нажать кнопку **«Отозвать»**, **«Приостановить»**, **«Возобновить»** или **«Обновить»** сертификат Пользователя.
5. Сертификаты, действие которых прекращено, могут быть удалены из системы путем нажатия кнопки **«Удалить»**.
6. Сертификат может быть выгружен в оригинальном формате на рабочее место Оператора путем нажатия кнопки **«Скачать»** (см. Рисунок 21):

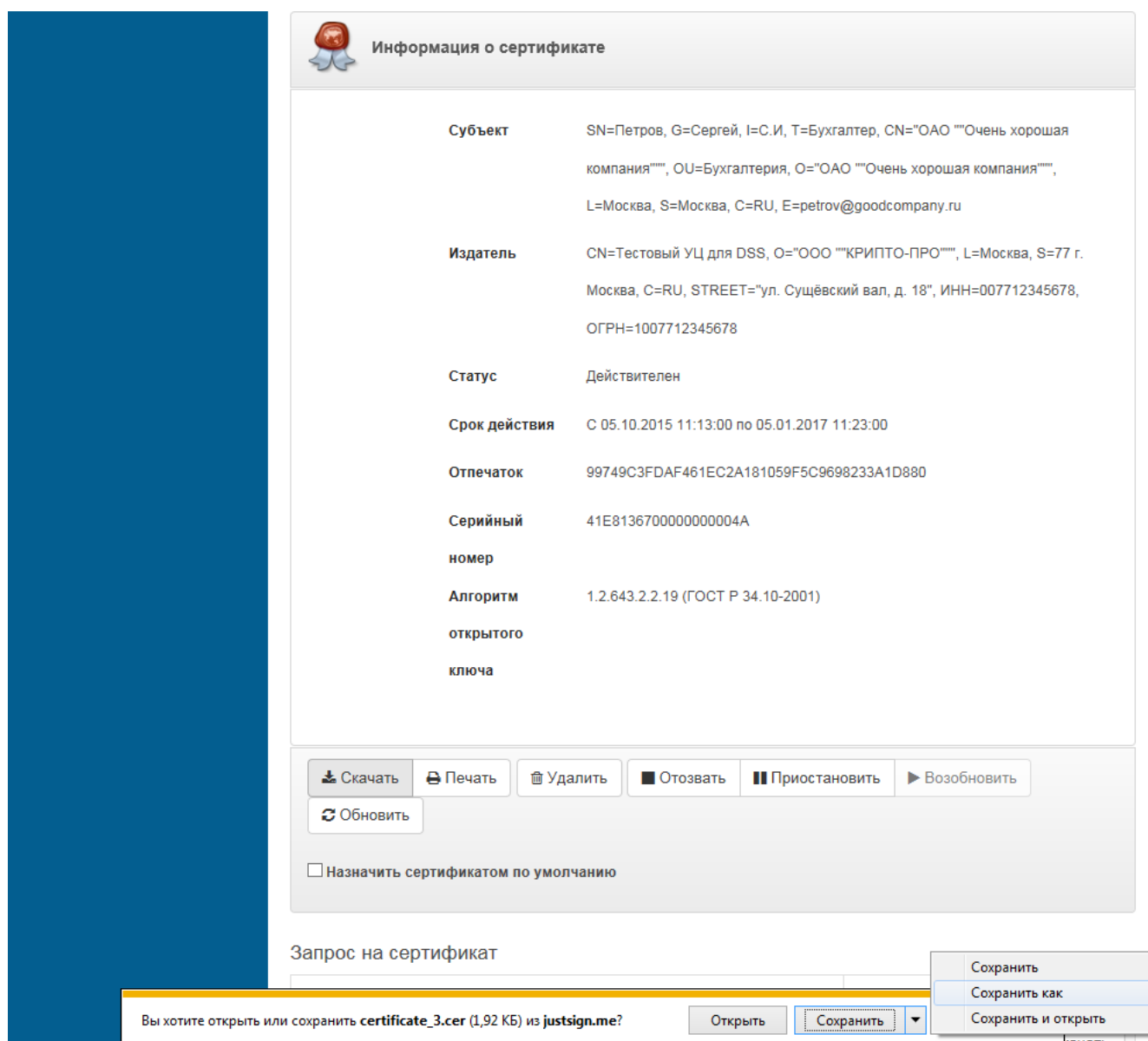


Рисунок 21. Выгрузка сертификата на рабочее место Оператора

7. Выбрать папку для сохранения сертификата и нажать **«Сохранить»** (см. Рисунок 22):

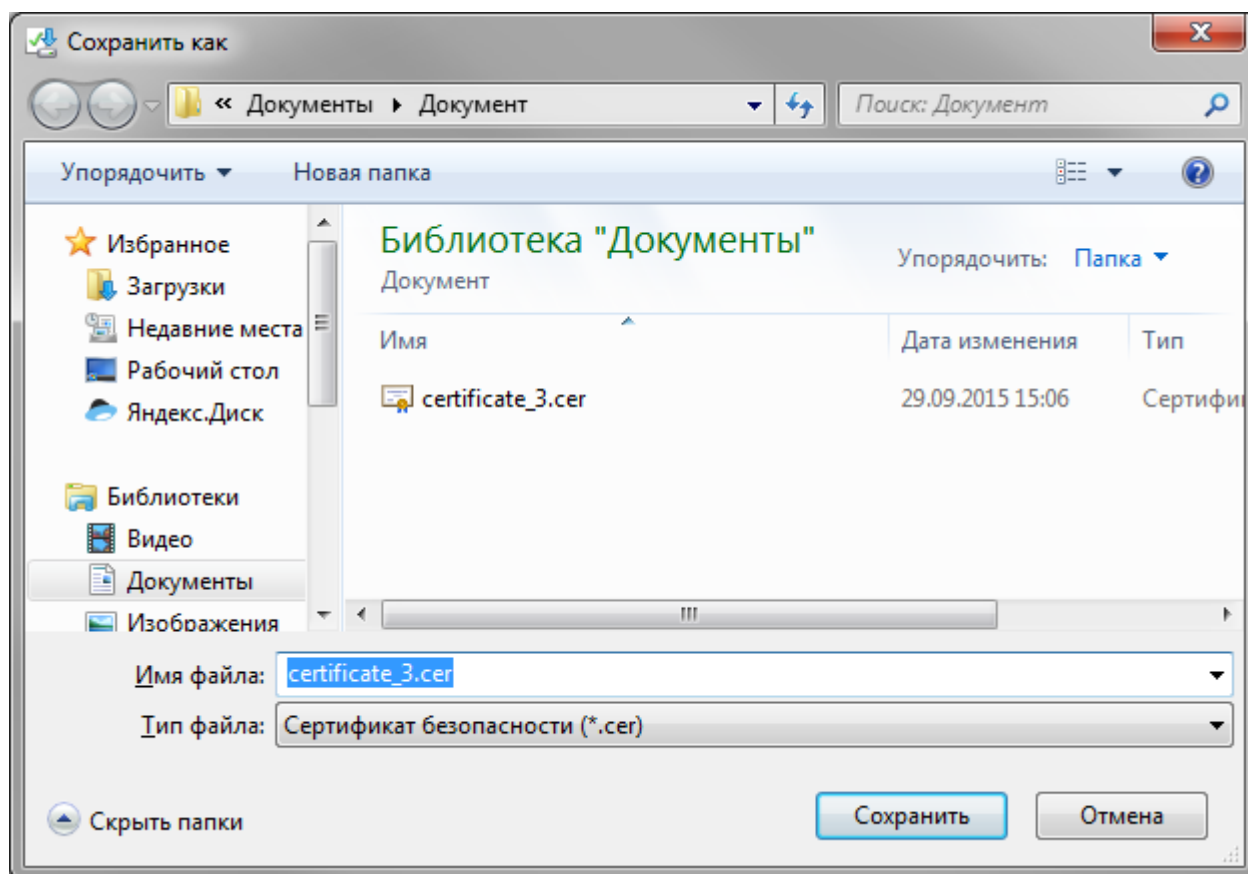


Рисунок 22. Выбор папки для сохранения сертификата

1. Перечень рисунков

Рисунок 1. Вход в личный кабинет Оператора по сертификату	6
Рисунок 2. Личный кабинет Оператора.....	6
Рисунок 3. Список Пользователей	6
Рисунок 4. Заполнение регистрационной формы нового Пользователя	7
Рисунок 5. Уведомление об успешном создании нового Пользователя	8
Рисунок 6. Список Пользователей	8
Рисунок 7. Окно управления сертификатами Пользователя	9
Рисунок 8. Перечень сертификатов Пользователя	9
Рисунок 9. Форма запроса на создание сертификата Пользователя.....	10
Рисунок 10. Выбор ключевого носителя	11
Рисунок 11. Биологический датчик случайных чисел	11
Рисунок 12. Ввод пароля на доступ к закрытому ключу	12
Рисунок 13. Перечень сертификатов Пользователя	12
Рисунок 14. Меню управления сертификатом.....	13
Рисунок 15. Печатная форма сертификата Пользователя.....	14
Рисунок 16. Выбор принтера для печати запроса на сертификат	15
Рисунок 17. Просмотр информации о Пользователе	16
Рисунок 18. Редактирование учетных данных Пользователя	17
Рисунок 19. Информация о сертификатах Пользователя	18
Рисунок 20. Меню управления сертификатом Пользователя	18
Рисунок 21. Выгрузка сертификата на рабочее место Оператора	19
Рисунок 22. Выбор папки для сохранения сертификата.....	20