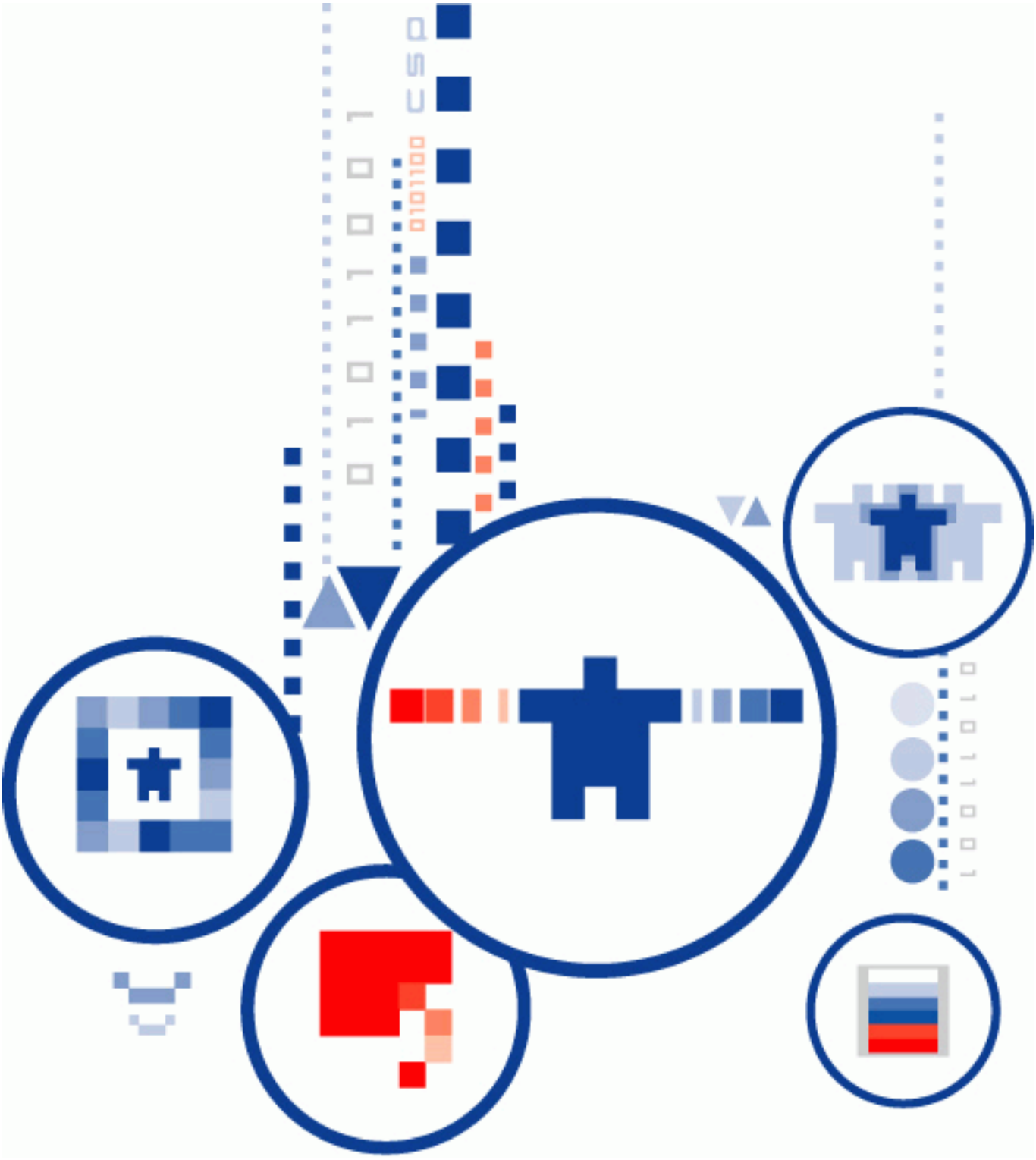
УТВЕРЖДЁН
ЖТЯИ.00082-01 90 04 06-ЛУ

ЖТЯИ.00082-01 90 04 06



ПАК «КриптоПро DSS»

Сервис электронной подписи

Инструкция Пользователя Аккредитованного Удостоверяющего центра ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Пользователей Аккредитованного Удостоверяющего центра ООО «КРИПТО-ПРО» (УЦ), обслуживаемых Уполномоченной организацией (Оператором УЦ), и определяет порядок использования Веб-интерфейса Сервиса электронной подписи ООО «КРИПТО-ПРО» на базе ПАК «КриптоПро DSS» (далее – СЭП) для осуществления операций по управлению квалифицированными сертификатами ключей проверки электронной подписи, созданию и проверке электронной подписи, шифрованию и расшифрованию электронных документов.

Информация об Удостоверяющем центре и 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

http://q.cryptopro.ru/

E-mail: info@CryptoPro.ru

qca@cryptopro.ru

Содержание

АННОТАЦИЯ....1

СОДЕРЖАНИЕ....2

1. ОБЩИЕ ПОЛОЖЕНИЯ....3

2. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ И РЕДАКТИРОВАНИЕ РЕГИСТРАЦИОННЫХ ДАННЫХ 3

3. ПОЛУЧЕНИЕ ПЕРВОГО ИЛИ ВНЕПЛАНОВАЯ СМЕНА СЕРТИФИКАТА....10

3. ВЫГРУЗКА СЕРТИФИКАТА....20

4. ПЛАНОВАЯ СМЕНА СЕРТИФИКАТА....21

5. СОЗДАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ ДОКУМЕНТА....23

6. ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ И СЕРТИФИКАТА....33

6.1.ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ С ИСПОЛЬЗОВАНИЕМ «СЛУЖБЫ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ» В СОСТАВЕ СЭП.....33

6.2.ПРОВЕРКА СЕРТИФИКАТА, ПОЛУЧЕННОГО ОТ ДРУГОГО ПОЛЬЗОВАТЕЛЯ....38

7. ШИФРОВАНИЕ ФАЙЛОВ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ....39

8. РАСШИФРОВЫВАНИЕ ФАЙЛОВ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ....43

ПРИЛОЖЕНИЕ 1. НАСТРОЙКА ИНТЕРНЕТ-БРАУЗЕРА....49

Настройка Google Chrome....49

Настройка Internet Explorer IE9 и выше....50

Настройка Mozilla Firefox 4.0 и выше....53

ПЕРЕЧЕНЬ РИСУНКОВ....56

1. Общие положения.

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

Для доступа пользователей к СЭП может быть использован любой стандартный Интернет-браузер.

Для корректной работы с СЭП рекомендуется подготовить рабочее место Пользователя в соответствии с Приложение 1. Настройка Интернет-браузера.

2. Регистрация пользователя и редактирование регистрационных данных

Регистрация пользователя осуществляется в следующем порядке:

1. Подать заявление на регистрацию в Удостоверяющем центре в соответствии с порядком, установленным Уполномоченной организацией (Оператором УЦ). Получить у Оператора УЦ адрес подключения к СЭП (вида https://www.justsign.me/<oper-name>/), свой логин и временный пароль, OTP-токен (при необходимости).
2. На своем рабочем месте выполнить настройку используемого Интернет-браузера в соответствии с Приложение 1. Настройка Интернет-браузера.
3. В адресной строке Интернет-браузер ввести полученный у Оператора УЦ адрес подключения к СЭП (вида https://www.justsign.me/<oper-name>/), в открывшемся окне аутентификации ввести полученный от Оператора логин и пароль, нажать кнопку «**Войти**» (см. Рисунок 1):

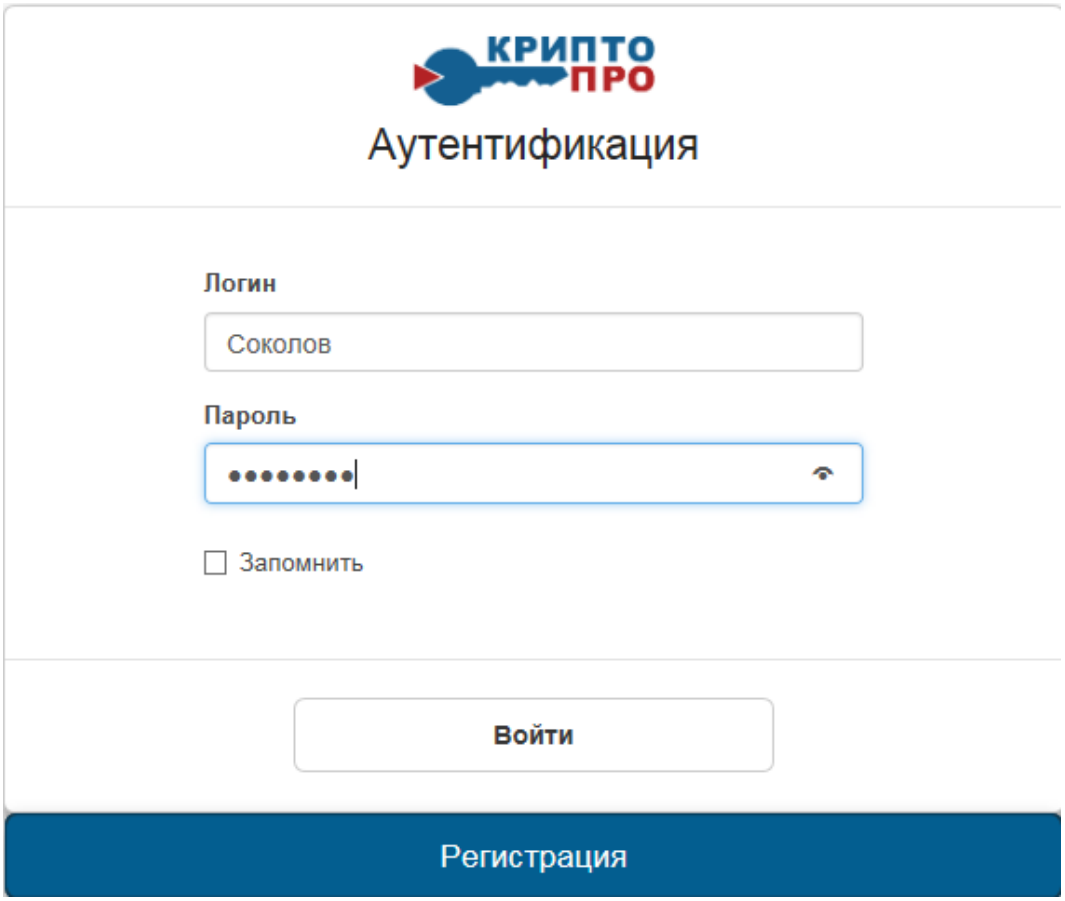


Рисунок 1. Окно аутентификации пользователя

4. Откроется окно для ввода одноразового кода, подтверждающего вход, и на зарегистрированный Оператором номер мобильного телефона придет SMS-сообщение с одноразовым кодом (или сформировать код с использованием OTP-токена, полученного у Оператора), ввести код в поле и нажать «**ОК**» (см. Рисунок 2):

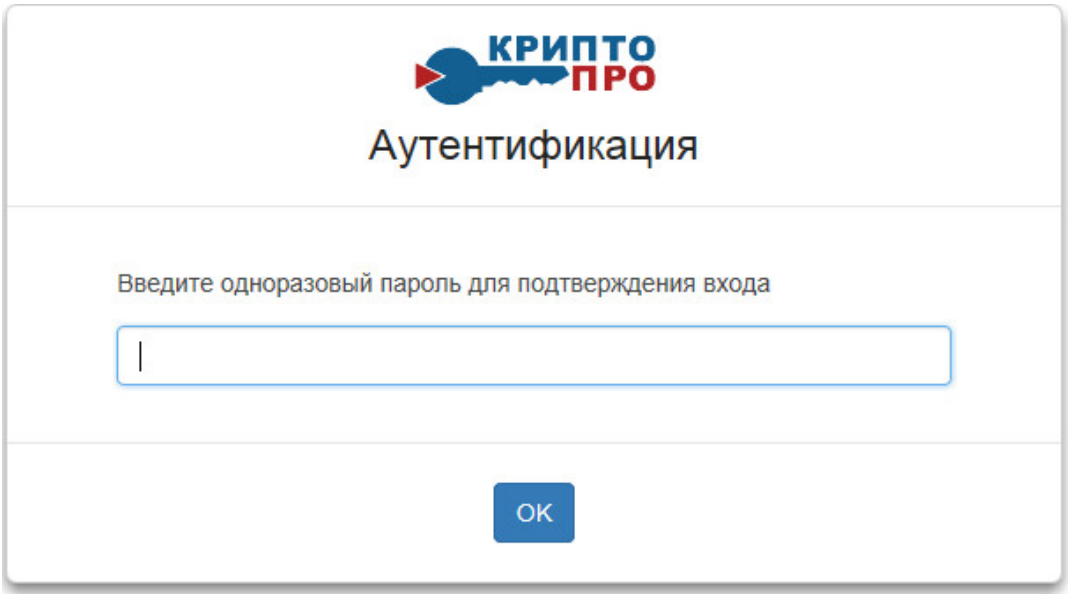


Рисунок 2. Ввод одноразового пароля

5. Будет выполнен вход на СЭП и откроется основное функциональное меню личного кабинета Пользователя. При первом входе на СЭП необходимо сменить временный пароль, полученный от Оператора.

6. В правом верхнем углу на имени пользователя открыть выпадающее меню и нажать «**Личный кабинет**» (см. Рисунок 3):

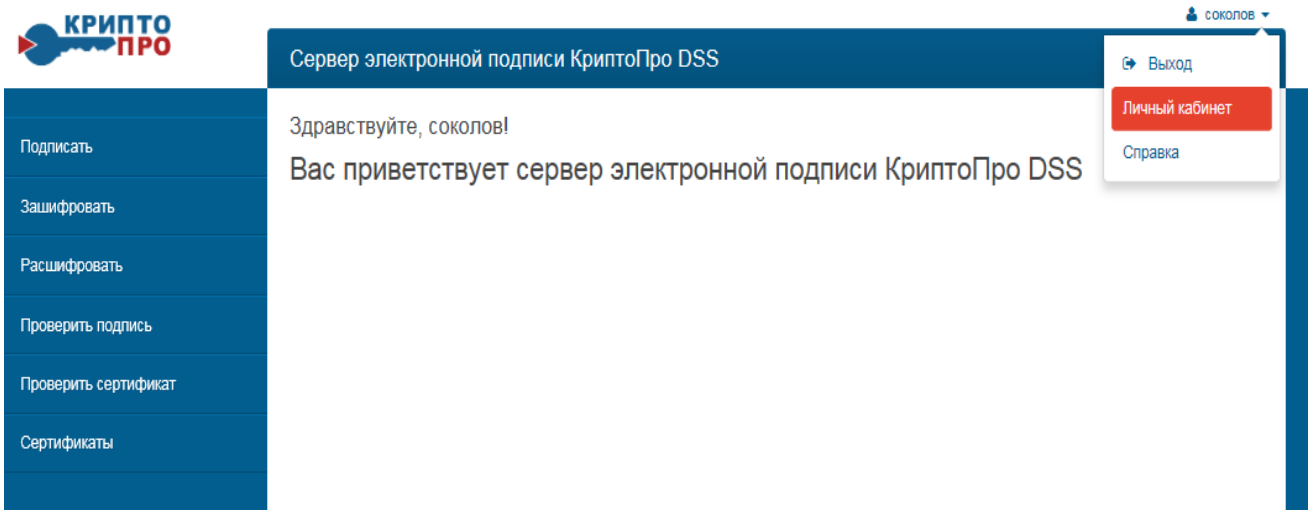


Рисунок 3. Личный кабинет пользователя СЭП

7. Откроется окно с регистрационной информацией Пользователя (см. Рисунок 4):

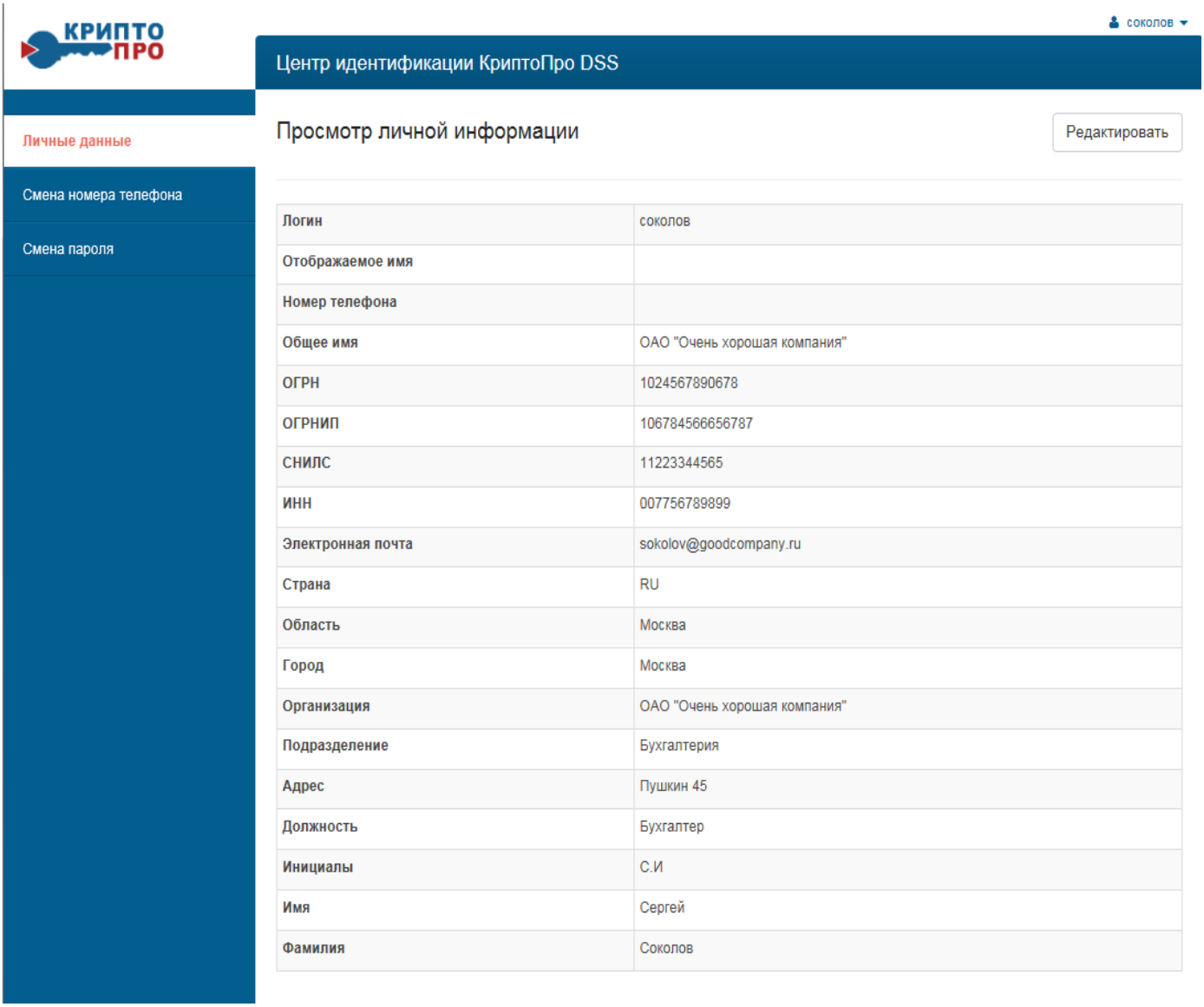


Рисунок 4. Личная информация пользователя

8. В меню слева нажать «**Смена пароля**», в соответствующие поля ввести текущий пароль (временный пароль, полученный от Оператора), новый пароль и повторно новый пароль для подтверждения, справа вверху нажать кнопку «**Сменить пароль**» (см. Рисунок 5):

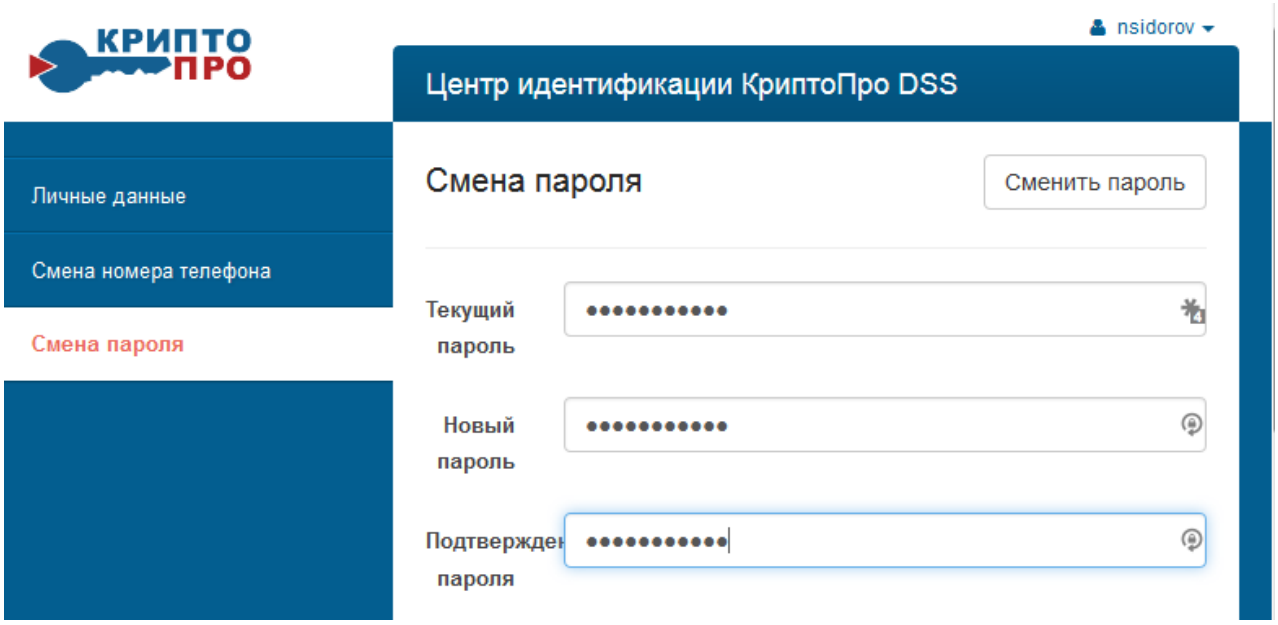


Рисунок 5. Смена пароля

Новый пароль должен состоять не мене чем из 8 буквенно-цифровых и знаков в разных регистрах и сохраняться втайне от прочих лиц.

9. Слева нажать на ссылку «**Личные данные**», справа вверху нажать кнопку «**Редактировать**», откроется форма для редактирования личной информации. Исправить сведенья в случае обнаружения ошибки или изменения каких-либо регистрационных данных и справа вверху нажать «**Сохранить**». (см. Рисунок 6):

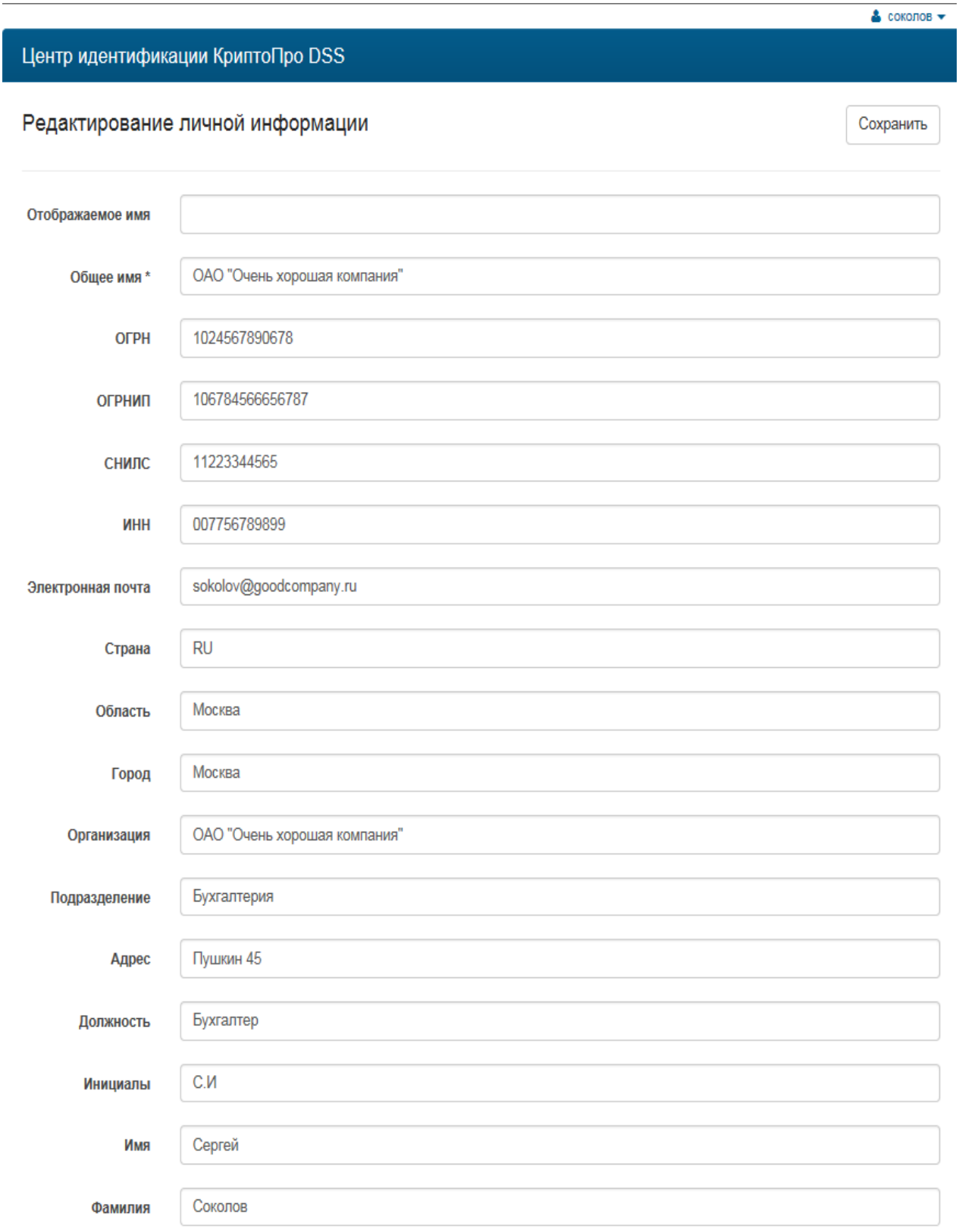


Рисунок 6. Окно редактирования личной информации

10. Для получения SMS-сообщений с уведомлениями о выполняемых операциях и одноразовыми паролями для подтверждения входа в СЭП и использования закрытого ключа электронной подписи, необходимо ввести свой номер мобильного

телефона, выбрав слева «**Смена номера телефона**», откроется окно регистрации номера телефона (см. Рисунок 7):

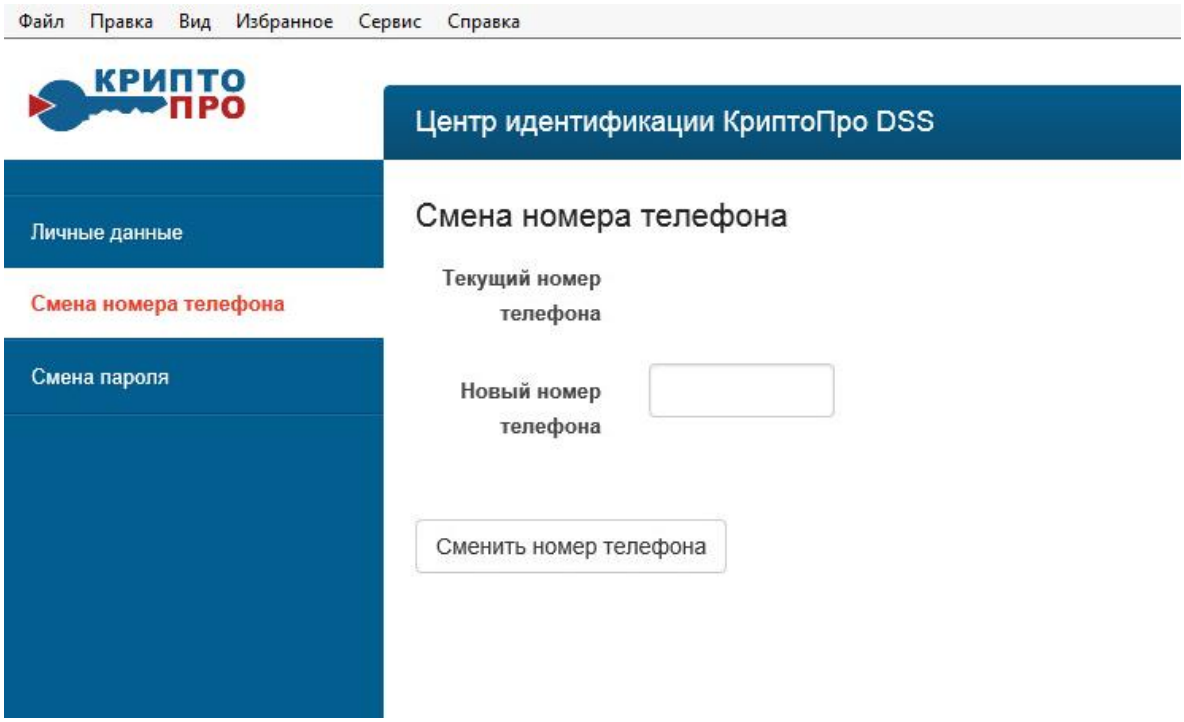


Рисунок 7. Окно регистрации номера телефона

11. Ввести свой номер мобильного телефона в формате +7(xxx)xxx-xx-xx, нажать кнопку «**Сменить номер**», выйдет сообщение «**Номер телефона успешно изменен**» (см. Рисунок 8):

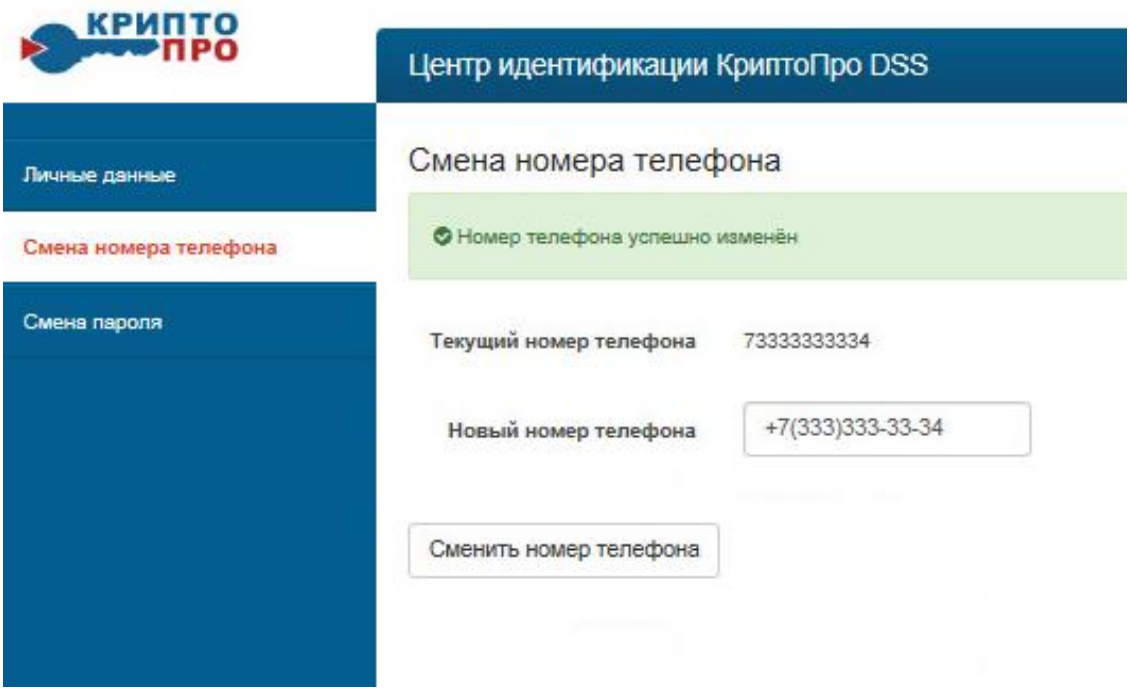


Рисунок 8. Смена телефонного номера

12. По завершении редактирования в правом верхнем углу на имени пользователя открыть выпадающее меню и нажать «**Выход**» и закрыть Интернет-Браузер (см. Рисунок 9):

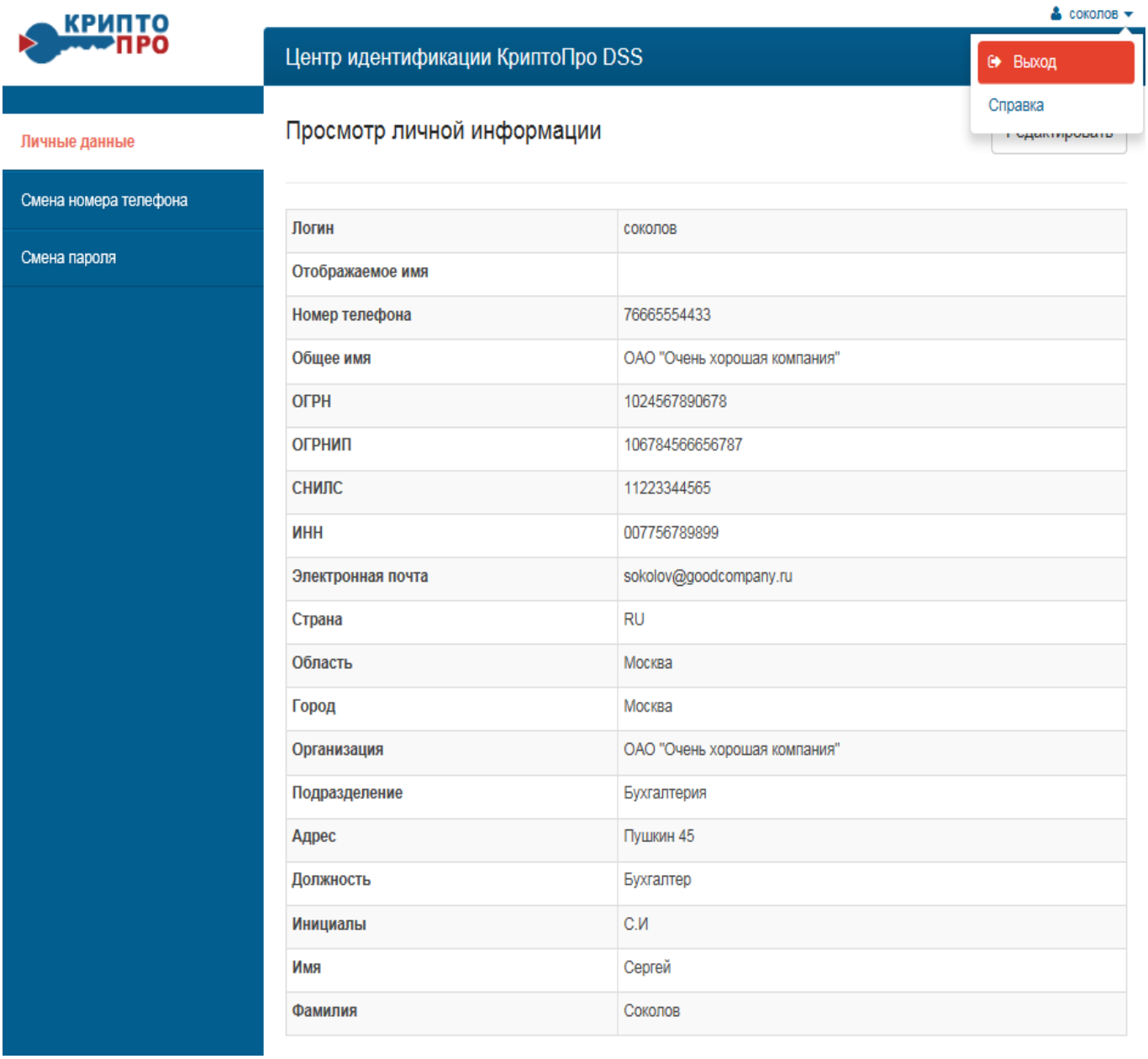


Рисунок 9. Завершение редактирования личных данных

3. Получение первого или внеплановая смена сертификата

1. Выполнить вход на СЭП (см. п.**3** Раздела **2**) и слева в меню нажать «**Сертификаты**» (см. Рисунок 10):

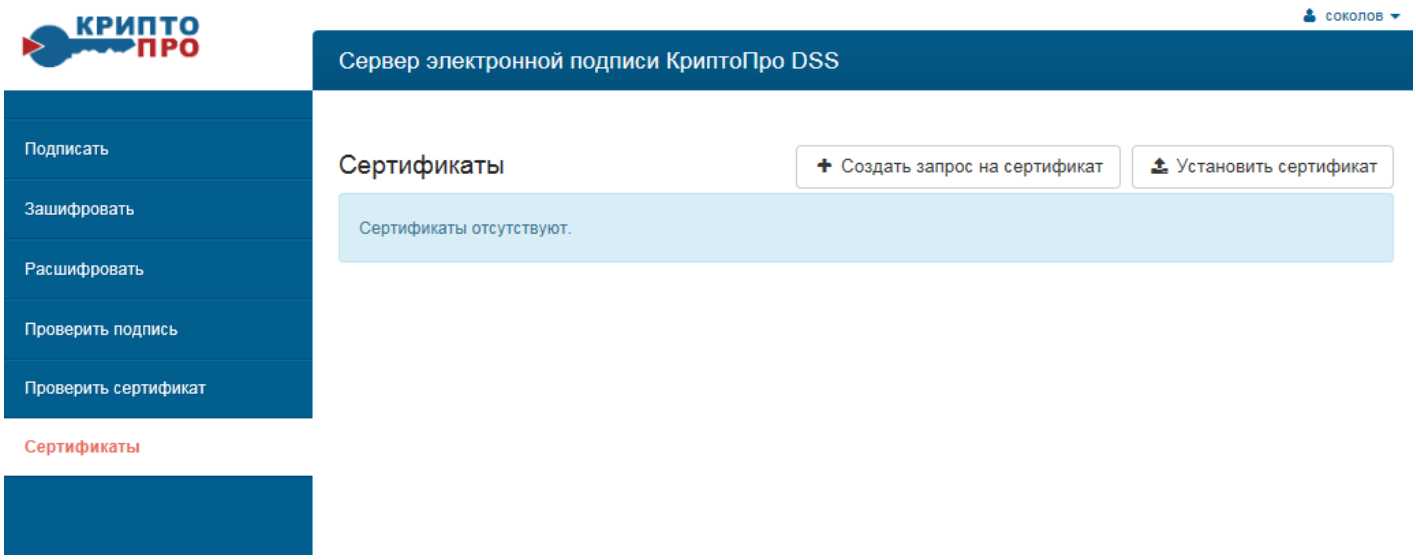


Рисунок 10. Сертификаты в личном кабинете пользователя СЭП

2. Нажать «**Создать запрос на сертификат**», заполнить форму запроса в соответствии с поданной заявкой на выдачу сертификата согласно Регламенту деятельности Уполномоченной организации (Оператора УЦ), выбрать шаблон сертификата «Пользователь DSS», нажать «**Создать запрос**» (см. Рисунок 11):

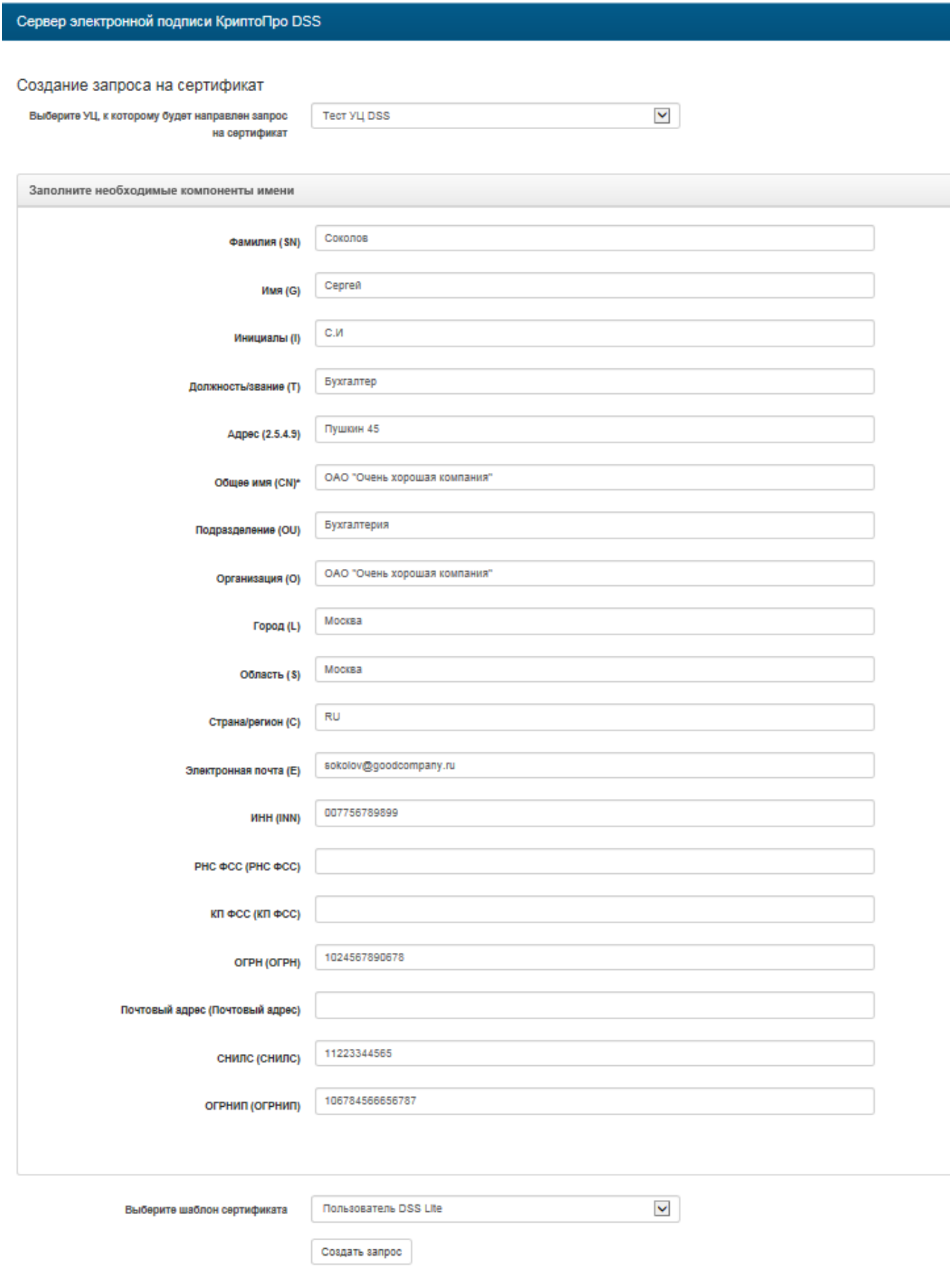


Рисунок 11. Форма запроса на сертификат

3. В открывшемся окне задать персональный ПИН-код доступа к закрытому ключу электронной подписи и нажать «**ОК**» (см. Рисунок 12):

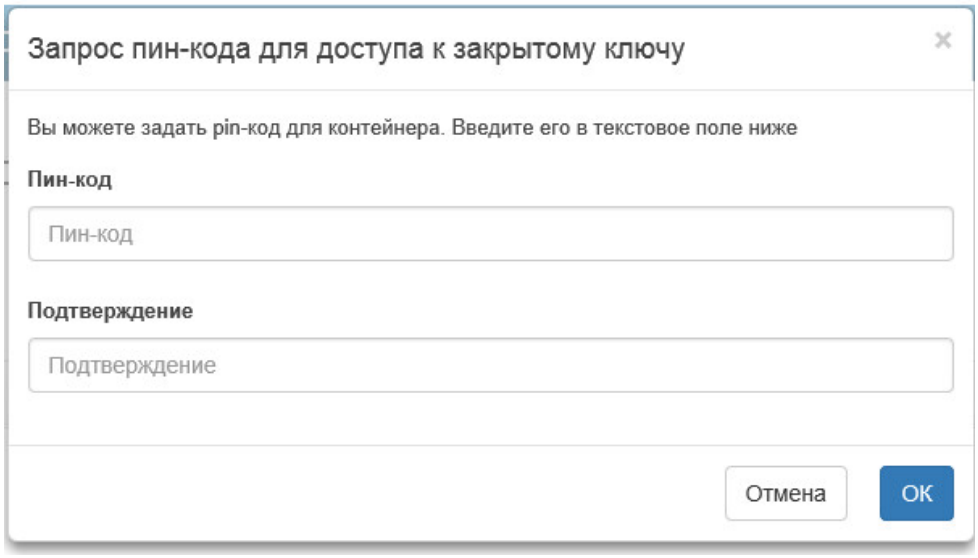


Рисунок 12. Запрос ПИН-кода для доступа к закрытому ключу

ПИН-код должен содержать не менее 5 символов (буквы латинского алфавита, цифры, специальные символы) и храниться в тайне.

4. Откроется окно для подтверждения операции одноразовым паролем, на зарегистрированный номер мобильного телефона придет SMS-сообщение с одноразовым кодом (или сформировать код с использованием полученного у Оператора OTP-токена), ввести код и нажать «**ОК**» (см. Рисунок 13):

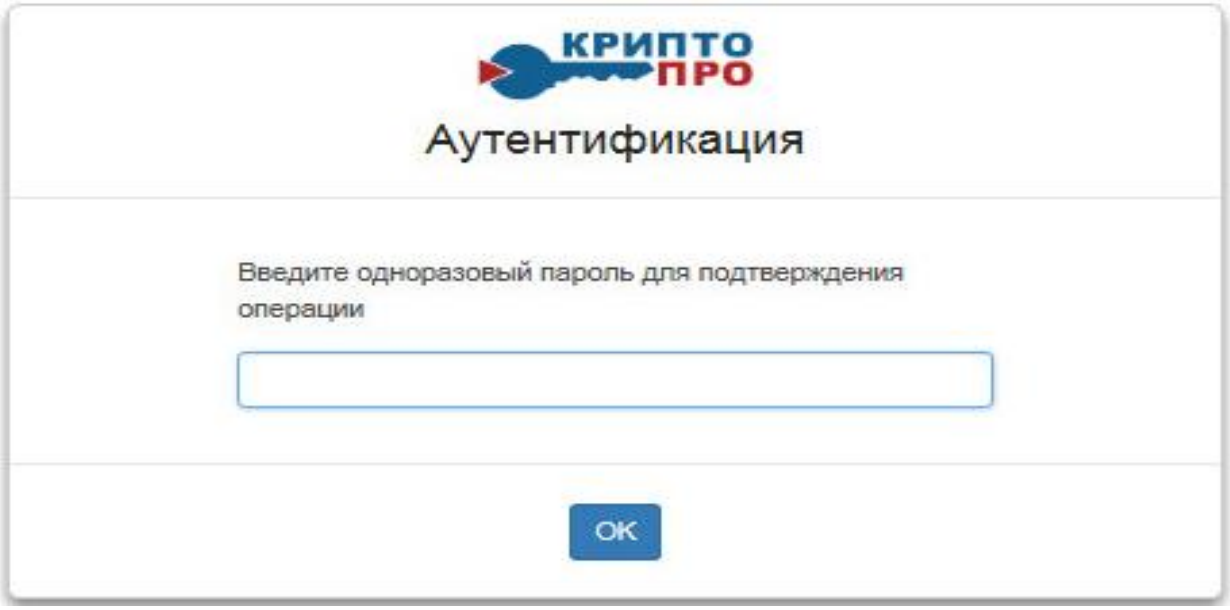


Рисунок 13. Ввод одноразового пароля для подтверждения операции

5. Откроется окно с информацией о статусе сертификата (см. Рисунок 14):

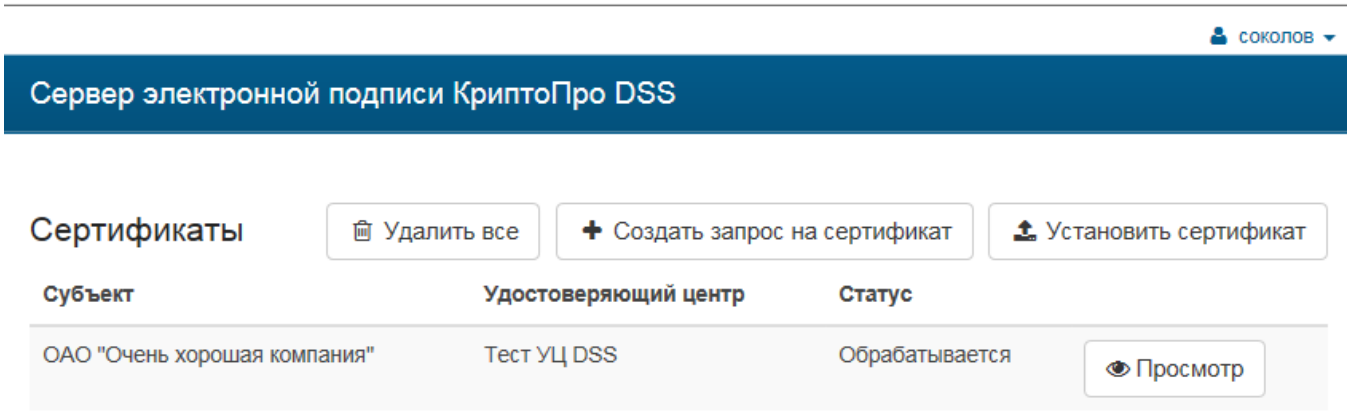


Рисунок 14. Информация о статусе имеющихся сертификатов

6. Справа нажать кнопку «**Просмотр**», отобразится окно с запросом на сертификат и статусом «**Обрабатывается**» (см. Рисунок 15):

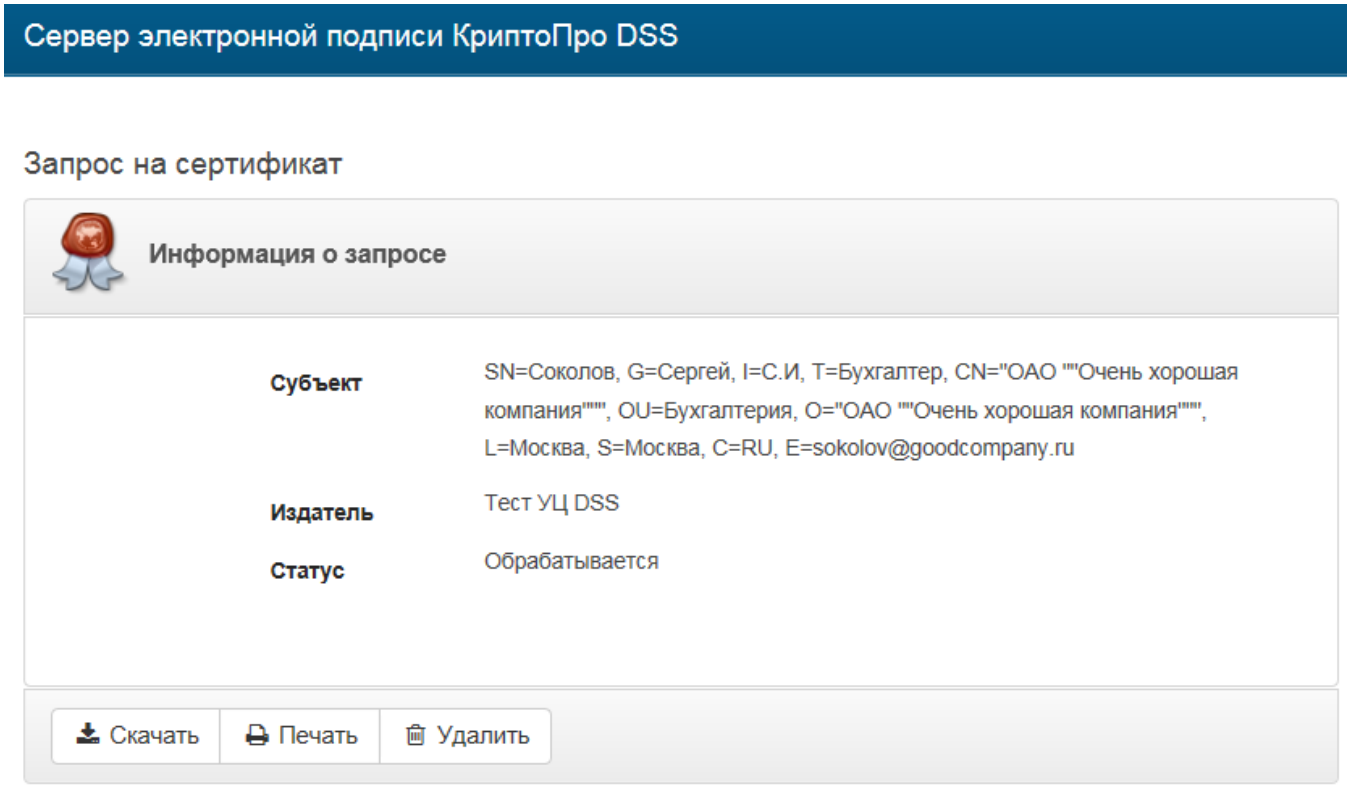


Рисунок 15. Информация о запросе на сертификат

7. Нажать кнопку «Печать», откроется форма запроса на сертификат для печати (см. Рисунок 16):

Наименование организации-Удостоверяющего Центра

Запрос на сертификат ключа проверки электронной подписи

Сведения о запросе на сертификат:
Кем выпущен:
ОАО "Очень хорошая компания"
Версия: 1 (0x0)
Субъект запроса на сертификат: SN = Соколов, G = Сергей, I = С.И, T = Бухгалтер, STREET = Пушкин 45, CN = ОАО "Очень хорошая компания", OU = Бухгалтерия, O = ОАО "Очень хорошая компания", L = Москва, S = Москва, C = RU, E = sokolov@goodcompany.ru
Ключ проверки электронной подписи:
Алгоритм ключа проверки электронной подписи:
Название: ГОСТ Р 34.10-2001
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 04 40 c7 7c 4c 25 ff 12 31 51 c0 8c ed 4c 25 f5 22 12 4b 41 15 d7 4d f1 ba c2 ec 0a 87 15 a4 21 6b 5d 04 16 2c 9f 3f f5 51 1a cf ab 34 9e 53 83 c0 6c e3 ed 0b 48 82 50 82 f8 c9 cd a7 a4 86 6a 8a a3
Атрибуты запроса на сертификат X.509
Название: Расширения сертификатов
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: bb 74 c2 88 cb d4 38 9c 5a bd 89 8d d3 74 75 d1 b0 d3 65 db
Название: CSP подачи заявок
Сведения о провайдере
Название провайдера : Crypto-Pro HSM Svc CSP
Подпись провайдера :
Название: Версия ОС
Значение: 6.3.9600.2
Название: Сведения о клиенте
Значение: 30 4b 02 01 05 0c 12 64 73 73 2d 73 71 6c 31 2e 64 73 73 2e 6c 6f 63 61 6c 0c 28 49 49 53 20 41 50 50 50 4f 4f 4c 5c 43 72 79 70 74 6f 50 72 6f 44 53 53 2d 31 2d 63 6f 6d 6c 69 74 65 63 70 63 61 73 73 0c 08 77 33 77 70 2e 65 78 65
Подпись запроса:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Значение: 2B 4A 85 9F E7 51 50 06 27 36 36 81 67 B5 DD F4 6C 1A 18 A8 51 72 41 7A 5D A5 00 D1 61 A5 70 7A F3 04 91 13 0B DD 2F B1 D3 BE DF 1A 7A 6C 44 05 E4 4A A0 F6 C8 26 B4 1C 10 FE DB AE AC 67 38 F6

Подпись владельца запроса на сертификат: _____/_____

"___" _____ 20__ г.

М. П.

Средство электронной подписи "КриптоПро CSP"

Подписанный запрос на сертификат ключа проверки электронной подписи следует переслать по адресу:
111111, Москва, ул. XXXXXXXX, д.XX. XXXXXXXXXXXXXXXXXXX
Администратору информационной безопасности.

Рисунок 16. Печатная форма запроса на сертификат

8. Распечатать форму, нажав ctrl+p и выбрав доступный принтер (см. Рисунок 17):

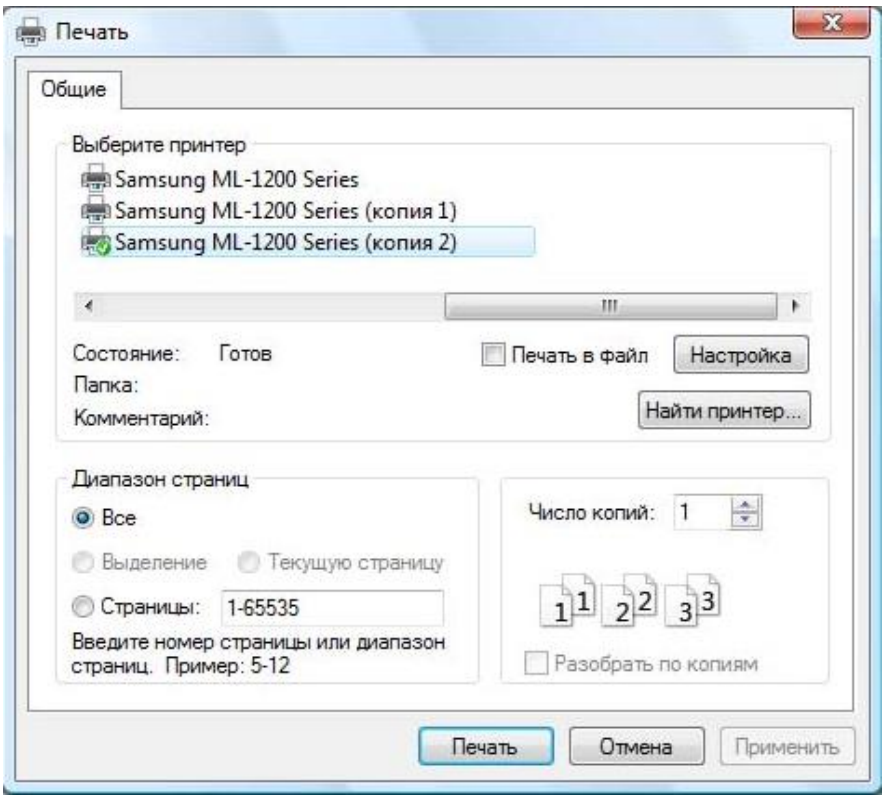


Рисунок 17. Выбор принтера для печати запроса на сертификат

Распечатанный запрос подписать, отсканировать и отправить на адрес электронной почты Оператора УЦ, оригинал с собственноручной подписью доставить Оператору УЦ.

9. Оператор УЦ получает запрос, проверяет достоверность полученных данных и подтверждает обработку запроса. После обработки запроса Пользователю высылается сообщение о создании сертификата (или отклонении запроса).

10. После получения сообщения о создании сертификата выполнить вход в личный кабинет СЭП (в соответствии с п.**3** Раздела 2) и в меню слева нажать ссылку «**Сертификаты**». Откроется окно с информацией о полученном сертификате со статусом «Действителен» (см. Рисунок 18):

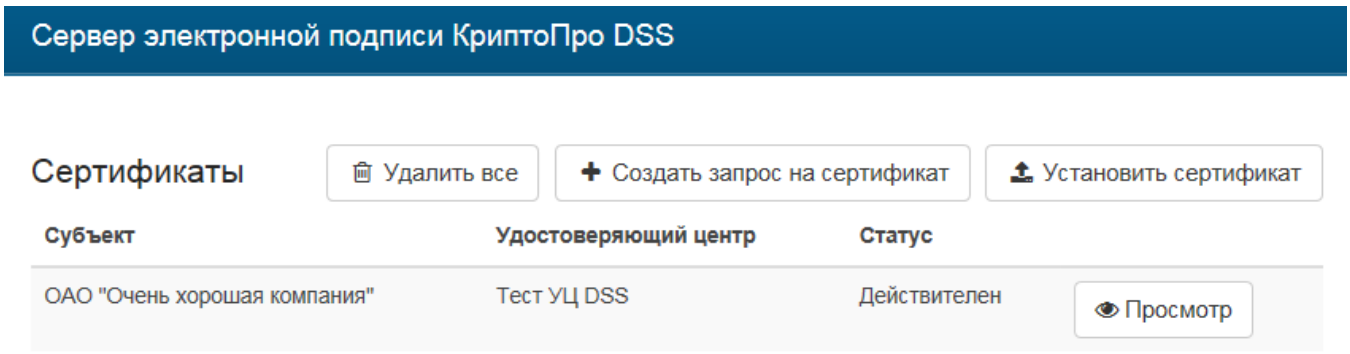


Рисунок 18. Перечень полученных сертификатов и их статус

11. Справа нажать кнопку «**Просмотр**», откроется окно с информацией о сертификате и меню управления сертификатом (см. Рисунок 19):

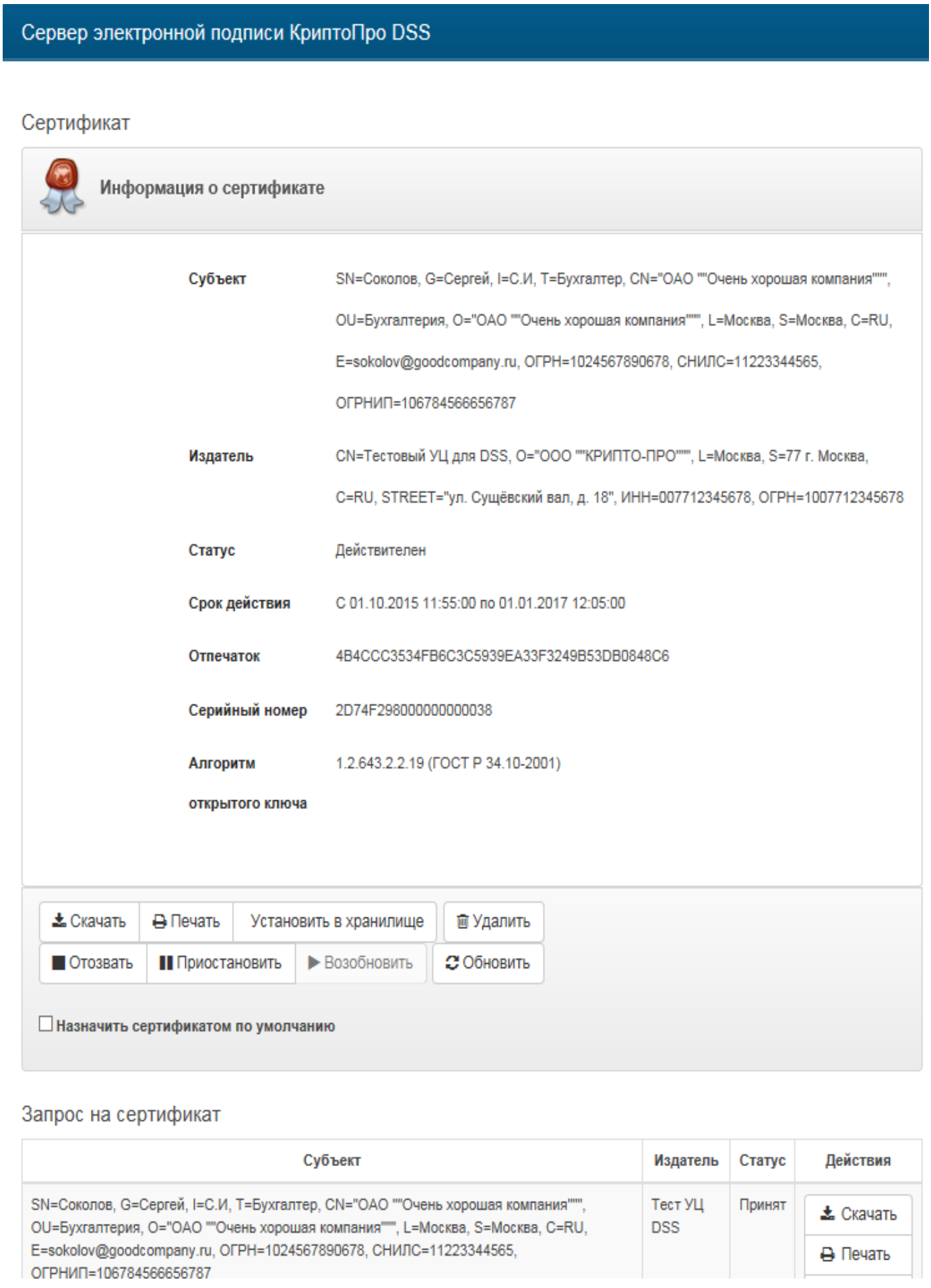
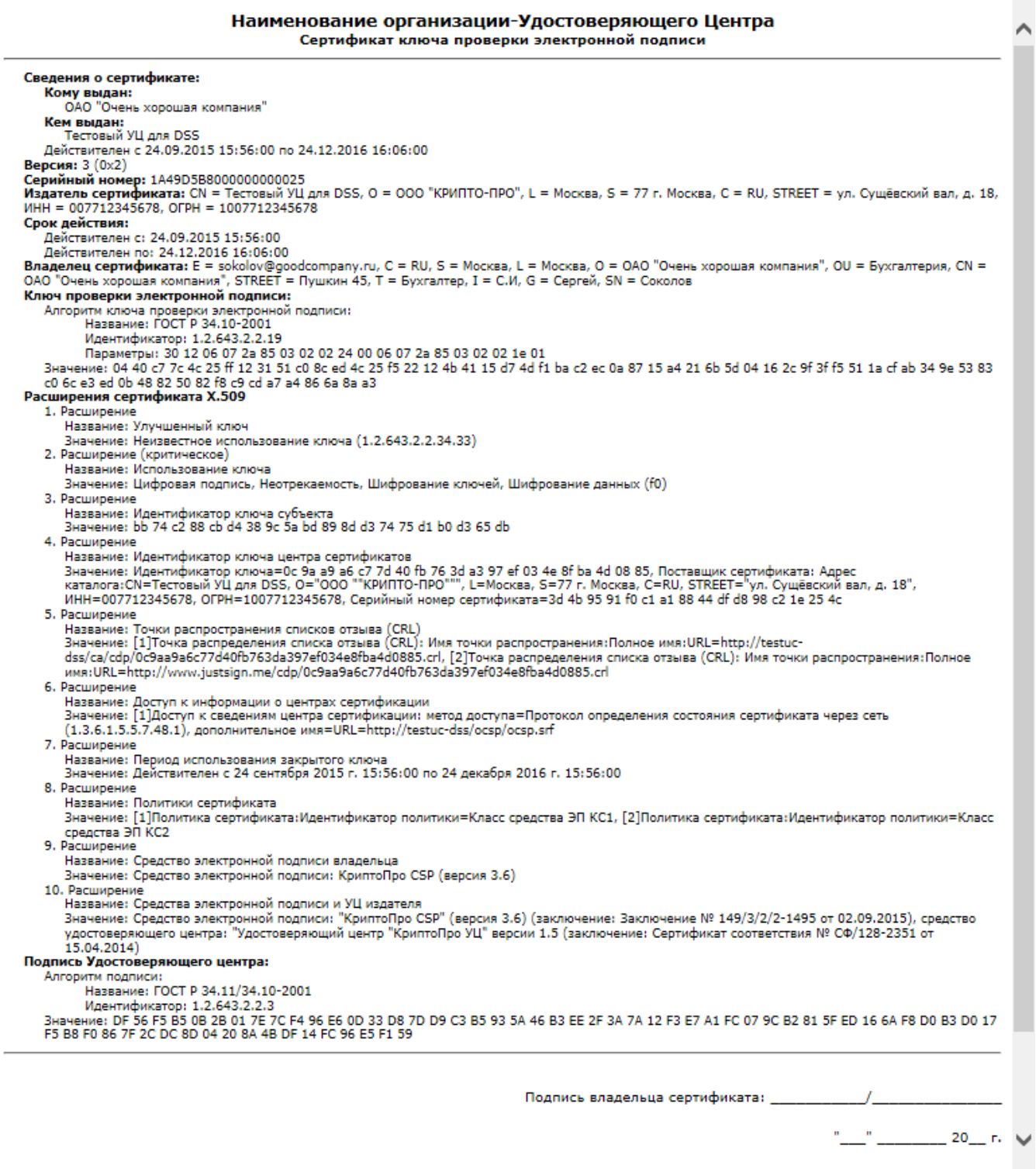


Рисунок 19. Информация о сертификате и меню управления сертификатом

12. Выбрать «**Печать**», откроется печатная форма копии сертификата (см. Рисунок 20):



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 24.09.2015 15:56:00 по 24.12.2016 16:06:00
Версия: 3 (0x2)
Серийный номер: 1A49D5B8000000000025
Издатель сертификата: CN = Тестовый УЦ для DSS, O = ООО "КРИПТО-ПРО", L = Москва, S = 77 г. Москва, C = RU, STREET = ул. Сущёвский вал, д. 18, ИНН = 007712345678, ОГРН = 1007712345678
Срок действия:
Действителен с: 24.09.2015 15:56:00
Действителен по: 24.12.2016 16:06:00
Владелец сертификата: E = sokolov@goodcompany.ru, C = RU, S = Москва, L = Москва, O = ОАО "Очень хорошая компания", OU = Бухгалтерия, CN = ОАО "Очень хорошая компания", STREET = Пушкин 45, T = Бухгалтер, I = С.И, G = Сергей, SN = Соколов
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 c7 7c 4c 25 ff 12 31 51 c0 8c ed 4c 25 f5 22 12 4b 41 15 d7 4d f1 ba c2 ec 0a 87 15 a4 21 6b 5d 04 16 2c 9f 3f f5 51 1a cf ab 34 9e 53 83 c0 6c e3 ed 0b 48 82 50 82 f8 c9 cd a7 a4 86 6a 8a a3
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: bb 74 c2 88 cb d4 38 9c 5a bd 89 8d d3 74 75 d1 b0 d3 65 db
4. Расширение
Название: Идентификатор ключа центра сертификатов
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. Сущёвский 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 распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://testuc-dss/ca/cdp/0c9aa9a6c77d40fb763da397ef034e8fba4d0885.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://www.justsign.me/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
7. Расширение
Название: Период использования закрытого ключа
Значение: Действителен с 24 сентября 2015 г. 15:56:00 по 24 декабря 2016 г. 15:56:00
8. Расширение
Название: Политики сертификата
Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата:Идентификатор политики=Класс средства 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 № 149/3/2/2-1495 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: DF 56 F5 B5 0B 2B 01 7E 7C F4 96 E6 0D 33 D8 7D D9 C3 B5 93 5A 46 B3 EE 2F 3A 7A 12 F3 E7 A1 FC 07 9C B2 81 5F ED 16 6A F8 D0 B3 D0 17 F5 B8 F0 86 7F 2C DC 8D 04 20 8A 4B DF 14 FC 96 E5 F1 59

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

Рисунок 20. Печатная форма копии сертификата

13. Распечатать форму, подписать и отправить Оператору УЦ аналогично п.**8** Раздела 3.

3. Выгрузка сертификата

1. В случае необходимости отправки своего сертификата контрагенту по переписки (для шифрования электронных документов или проверки электронной подписи) сертификат необходимо сохранить на рабочем месте Пользователя. Для этого после входа на СЭП (в соответствии с п.**3** Раздела 2) слева нажать «**Сертификаты**» (см. Рисунок 14), в открывшемся окне справа от записи требуемого сертификата нажать «**Просмотр**» и далее выбрать «**Скачать**», появится сообщение «**Сохранить,** в всплывшем окне нажать стрелку и выбрать «**Сохранить как**» (см. Рисунок 21):

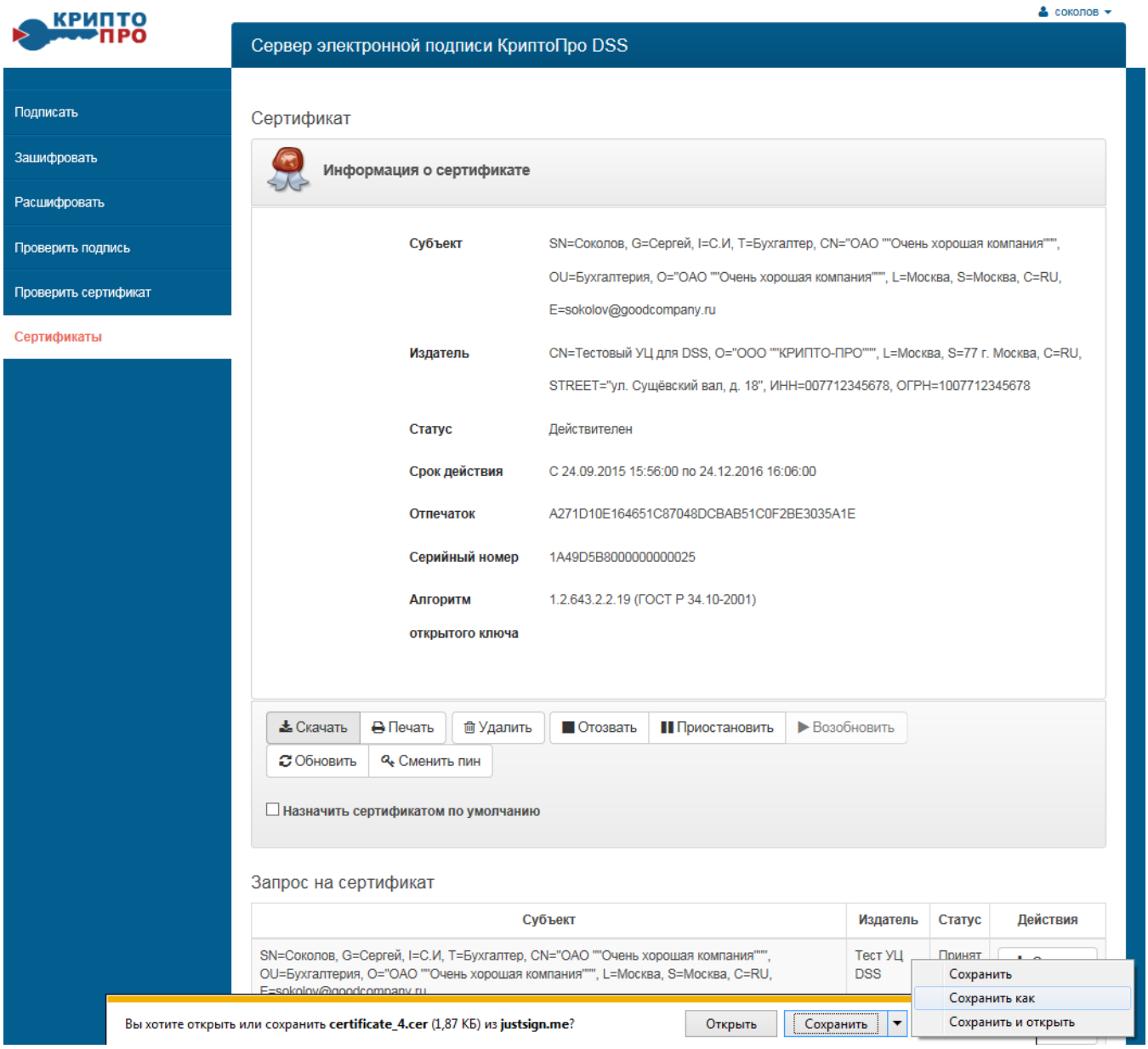


Рисунок 21. Выгрузка сертификата

2. Далее выбрать папку и нажать «**Сохранить**» (см. Рисунок 22):

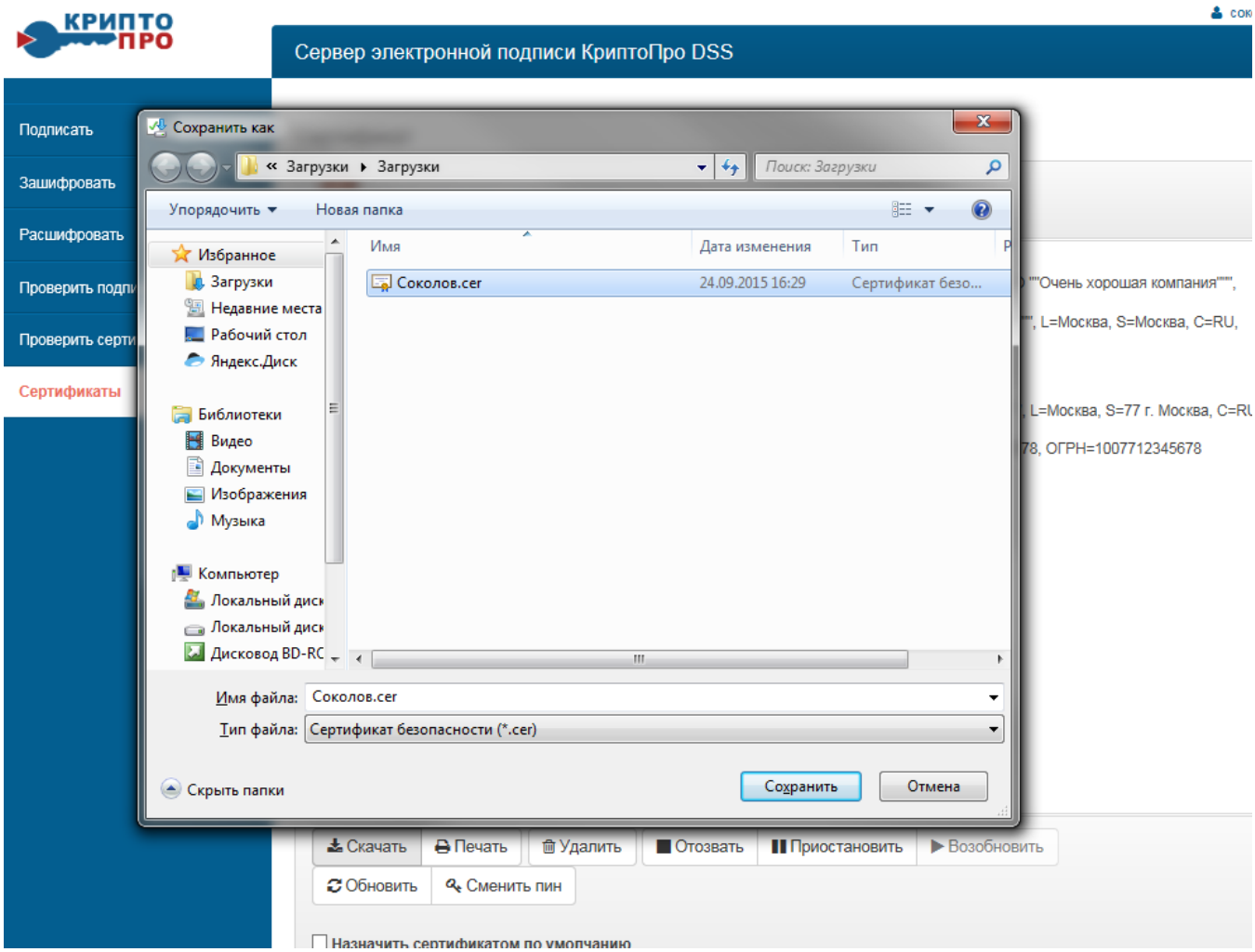


Рисунок 22. Выбор папки для сохранения сертификата

При отправке контрагенту сертификат рекомендуется заархивировать любым доступным архиватором (WinRAR, WinZIP и т.п.)

4. Плановая смена сертификата

1. Для плановой смены сертификата, выполнить вход на СЭП (в соответствии с п.3 Раздела 2) и в меню слева нажать «**Сертификаты**».
2. Нажать «**Просмотр**» напротив сертификата, для которого требуется плановая смена (см. п.**11** Раздела 3).
3. Нажать «**Обновить**», откроется окно для выбора шаблон сертификата, выбрать шаблон «**Пользователь DSS**», указать и подтвердить новый ПИН-код и нажать «**ОК**» (см. Рисунок 23):

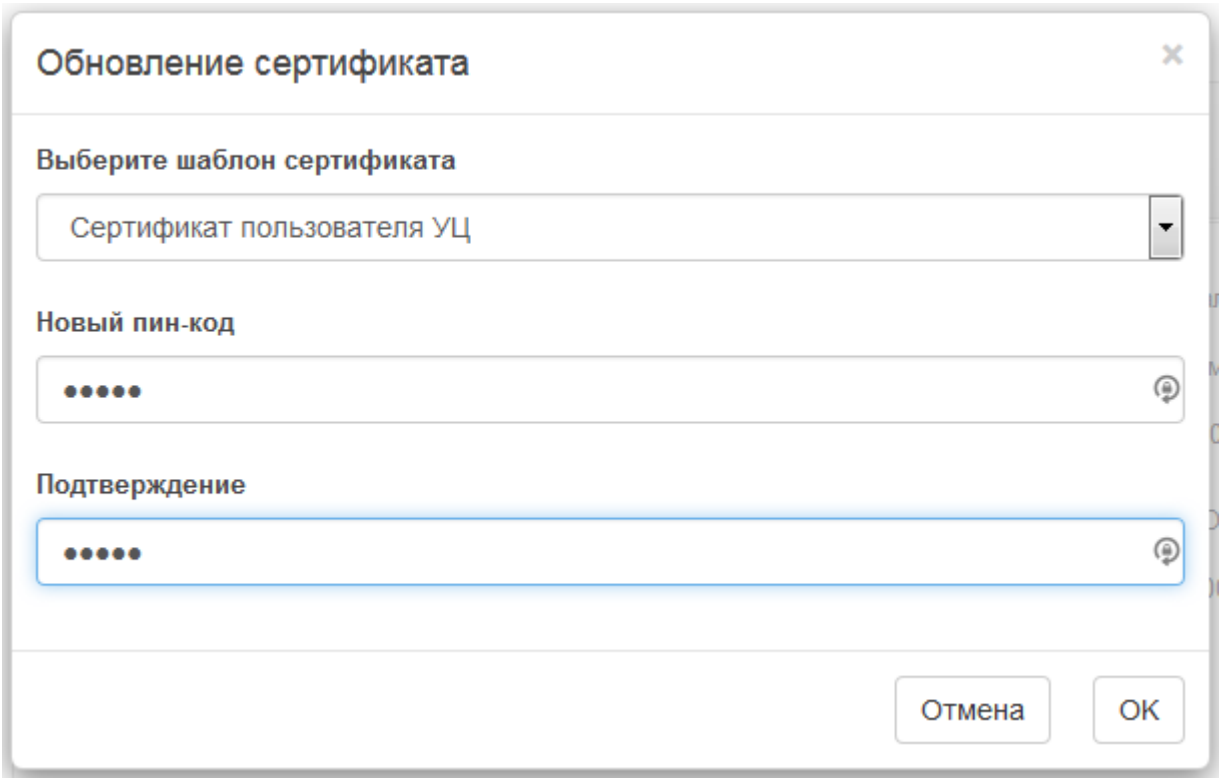


Рисунок 23. Формирование запроса на обновление сертификата

4. В открывшемся окне ввести одноразовый код (полученный в SMS на зарегистрированный номер мобильного телефона или сформированный с использованием полученного у Оператора OTP-токена) для подтверждения операции создания ключа электронной подписи и нажать «**ОК**» (см. Рисунок 24):

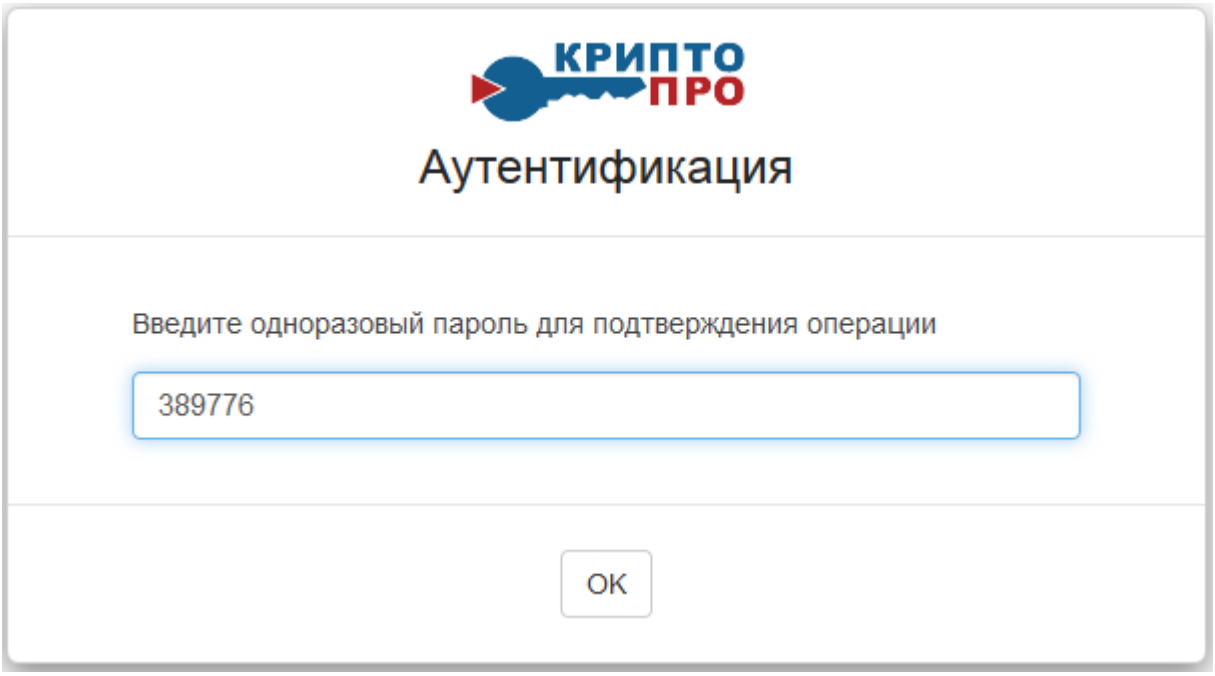


Рисунок 24. Подтверждение операции одноразовым паролем

5. Нажать слева на кнопку «**Сертификаты**». Справа нажать кнопку «**Просмотр**», отобразится окно с запросом на сертификат и статусом «**Обрабатывается**» (см. п.**6** Раздел 3)
6. После получения запроса на сертификат выполнить процедуры отправки запроса и получения сертификата (в соответствии п.**7**-**13** Раздела 3).
7. В соответствии с Регламентом Уполномоченной организацией (Оператора УЦ) возможна автоматическая обработка запроса на обновление сертификата и отправка подписанной копии сертификата Оператору УЦ в электронной форме с использованием старого действующего ключа электронной подписи. Для этого при выводе на печать копии нового сертификата (в соответствии с п.**12**-**13** Раздела 3) выбрать доступный виртуальный принтер PDF, нажать «**ОК**» (см. Рисунок 25):

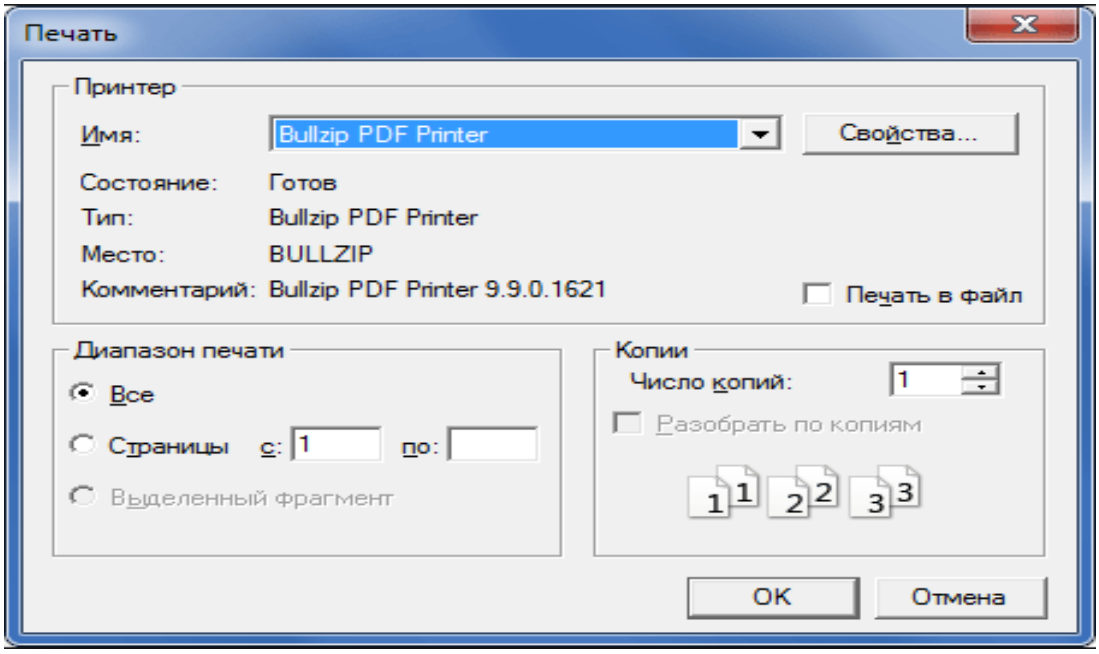


Рисунок 25. Печать копии сертификата в файл формата PDF

8. Сохраненную копию сертификата в формате PDF подписать старым действующим сертификатом (см. Раздел 5) и отправить на адрес электронной почты Оператора УЦ.

5. Создание электронной подписи документа

1. Осуществить вход в личный кабинет Пользователя СЭП (в соответствии с п.3 Раздела 2) и в меню слева нажать «**Подписать**», далее в открывшемся окне

загрузить файл электронного документа для подписания, для этого нажать «**Документ**» (см. Рисунок 26):

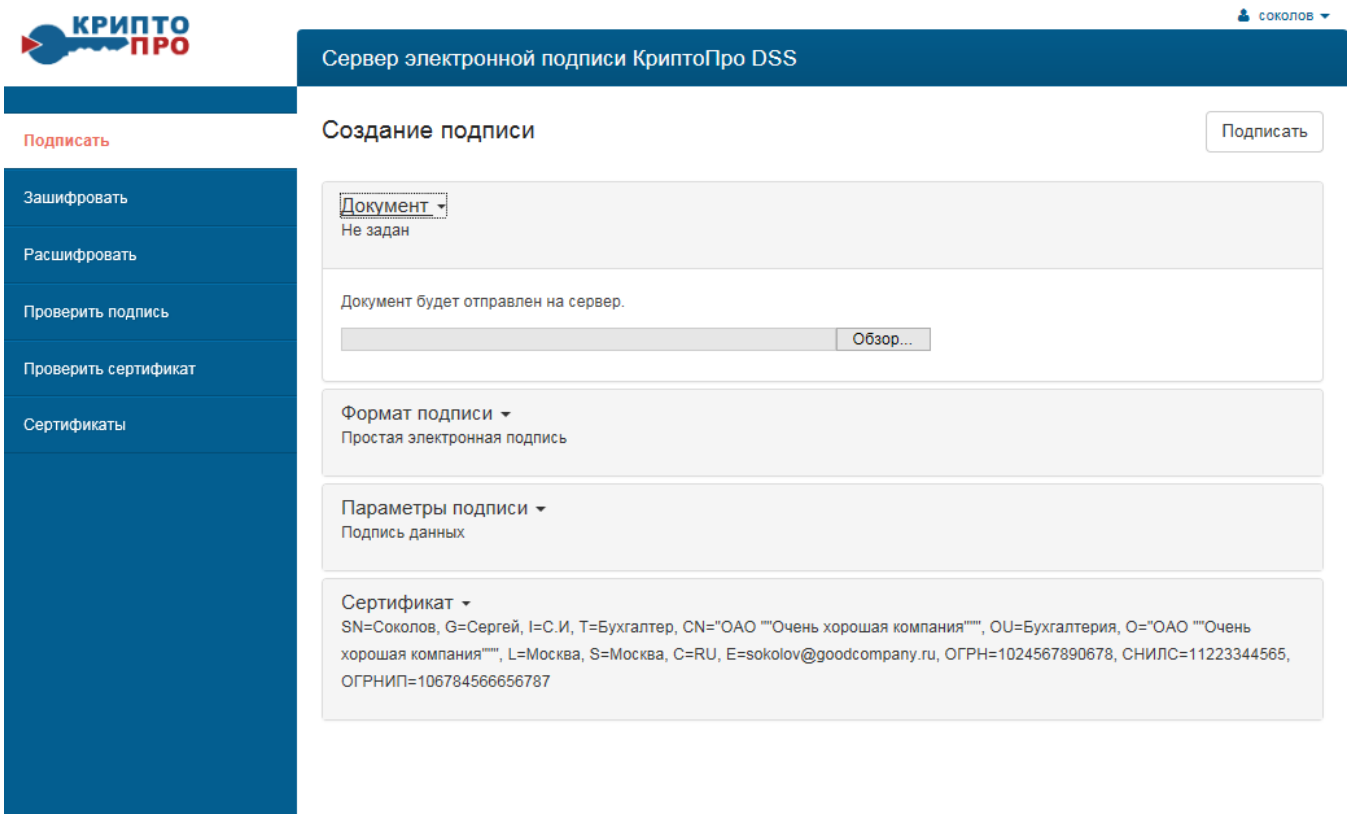


Рисунок 26. Выбор документа для создания электронной подписи

2. Далее – «**Обзор**», выбрать нужный файл и нажать кнопку «**Открыть**» (см. Рисунок 27):

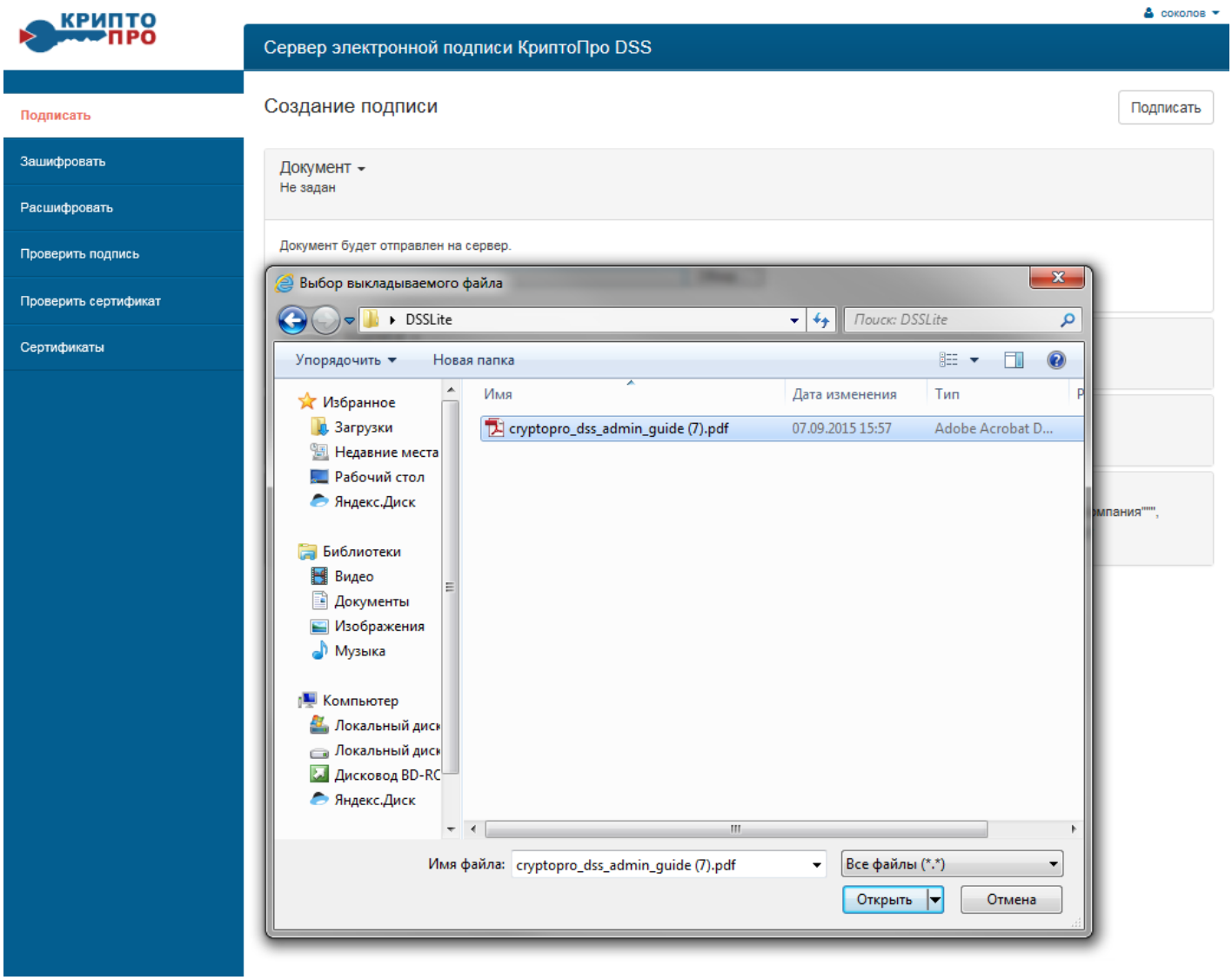


Рисунок 27. Выбор файла электронного документа для загрузки

3. Нажимая кнопку «**Вперед**» просмотреть отображаемое содержание подписываемого электронного документа (см. Рисунок 29):

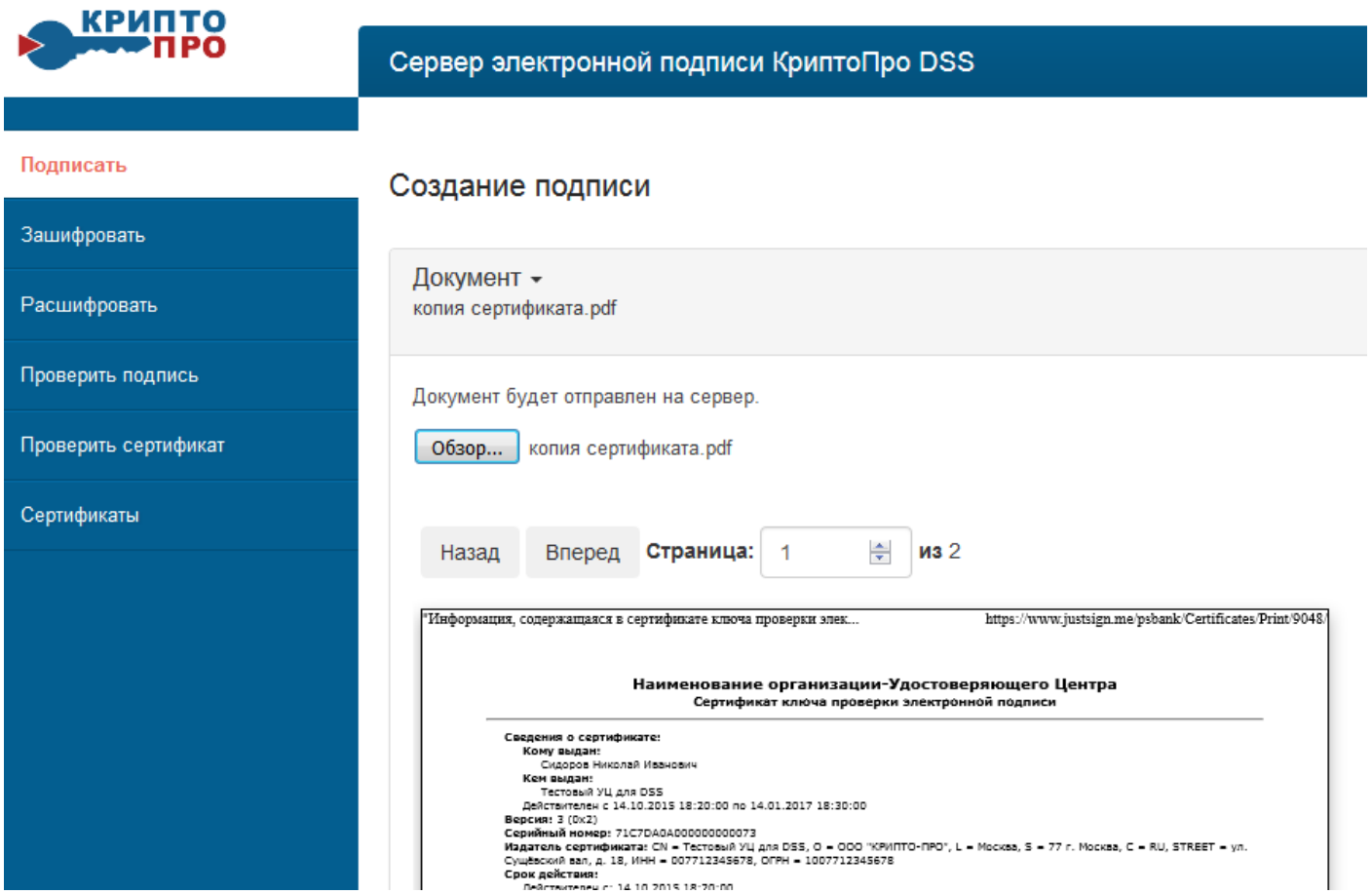


Рисунок 28. Просмотр содержания электронного документа

4. Выбрать формат электронной подписи, соответствующий формату файла подписываемого электронного документа (в данном случае «**Подпись документов PDF**») и параметр подписи «**Формат подписи CAdES**» (см. Рисунок 29):

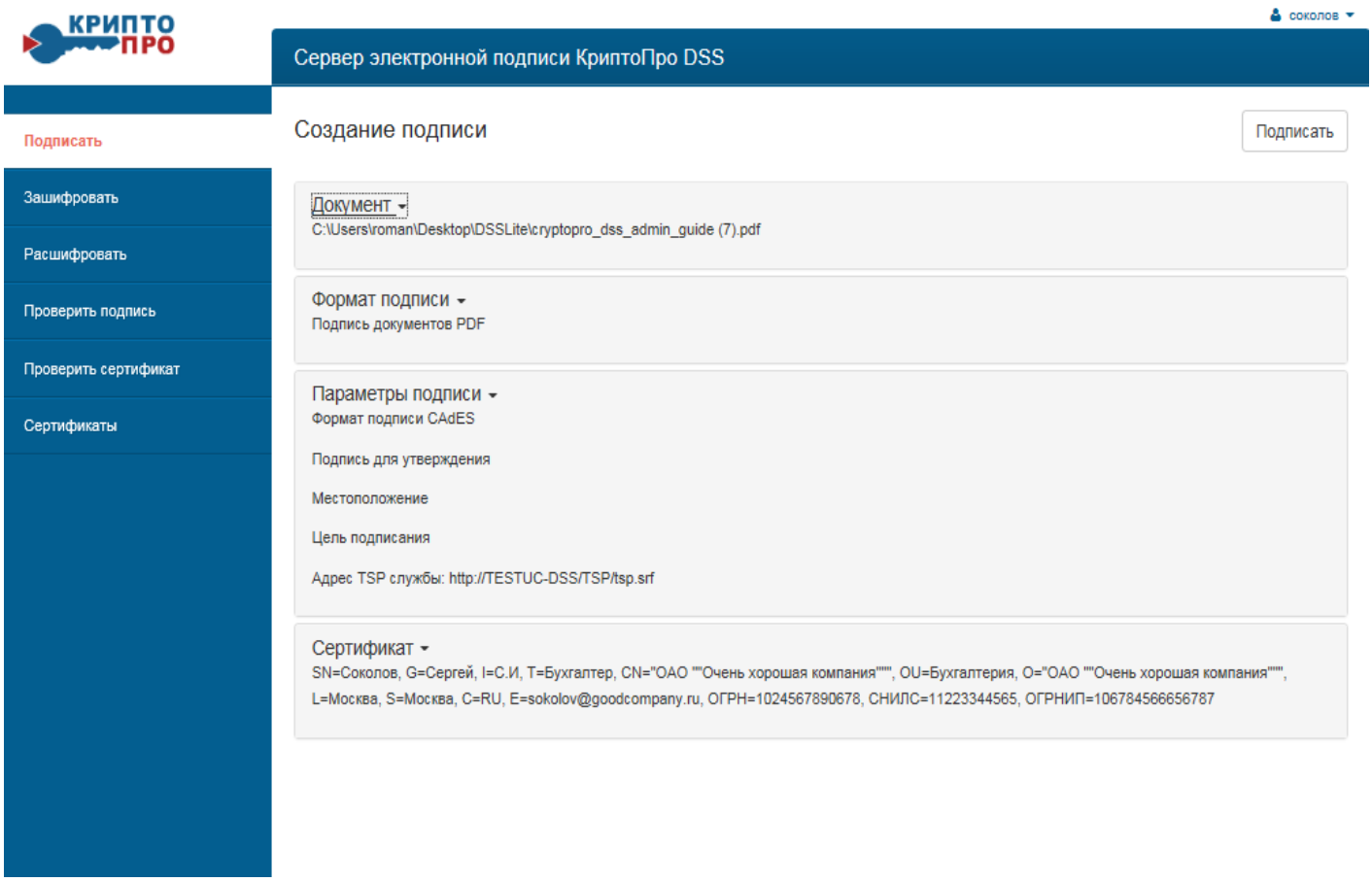


Рисунок 29. Выбор формата и параметров электронной подписи

«**Подпись документов PDF**» используется для файлов с расширением .pdf, «**Подпись документов Word и Excel**» – с расширениями .docx или .xlsx.

Формат усовершенствованной электронной подписи (CAdeS), используется как универсальный для произвольного формата файлов (не .pdf/.docx/.xlsx).

При выборе усовершенствованного формата подписи CMS (CAdES), появляется выбор присоединенной или отделенной подписи и версии формата CAdES (см. Рисунок 30):

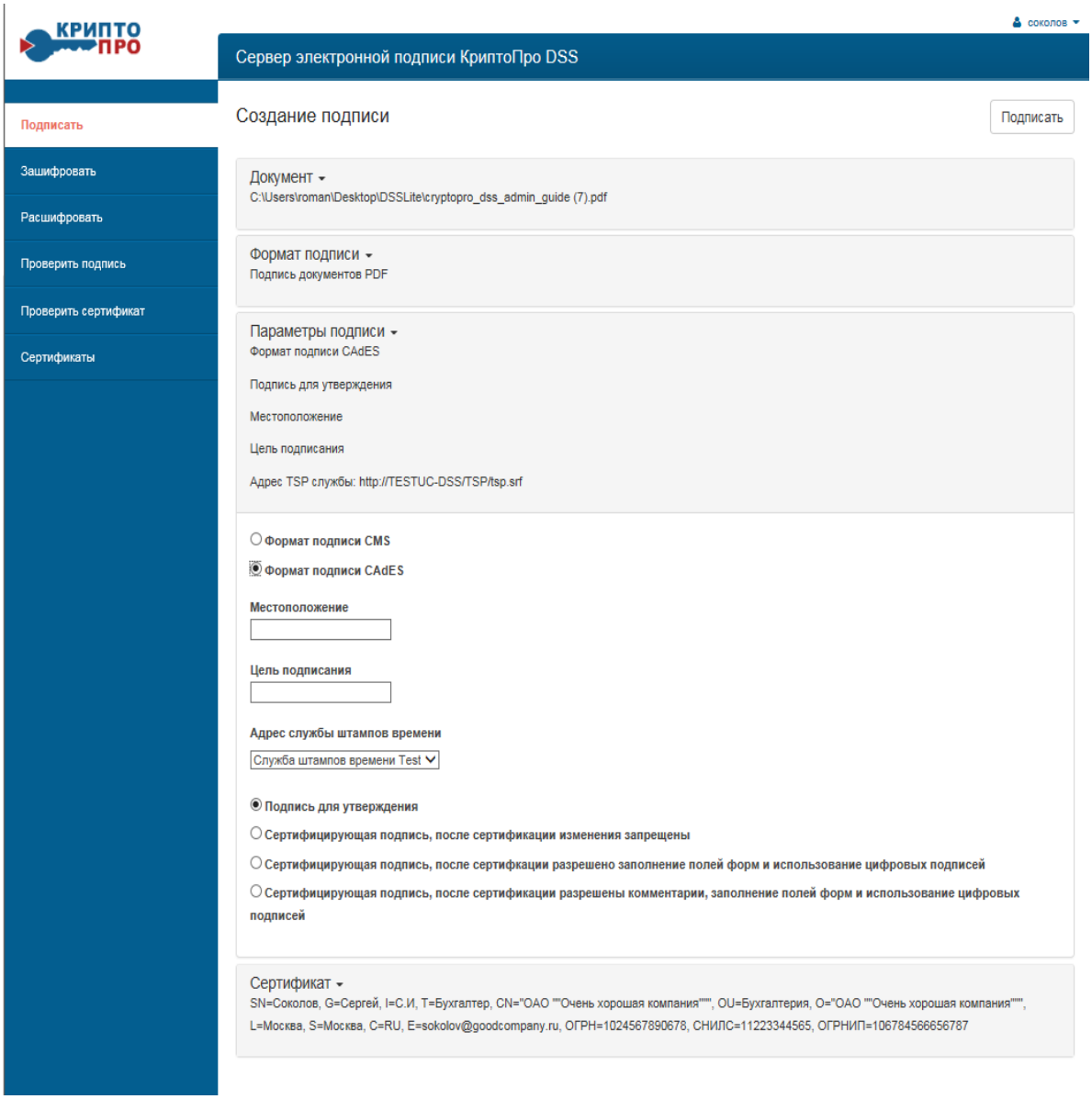


Рисунок 30. Выбор параметров электронной подписи CAdES

5. Выбрать действующий сертификат (см. Рисунок 31):

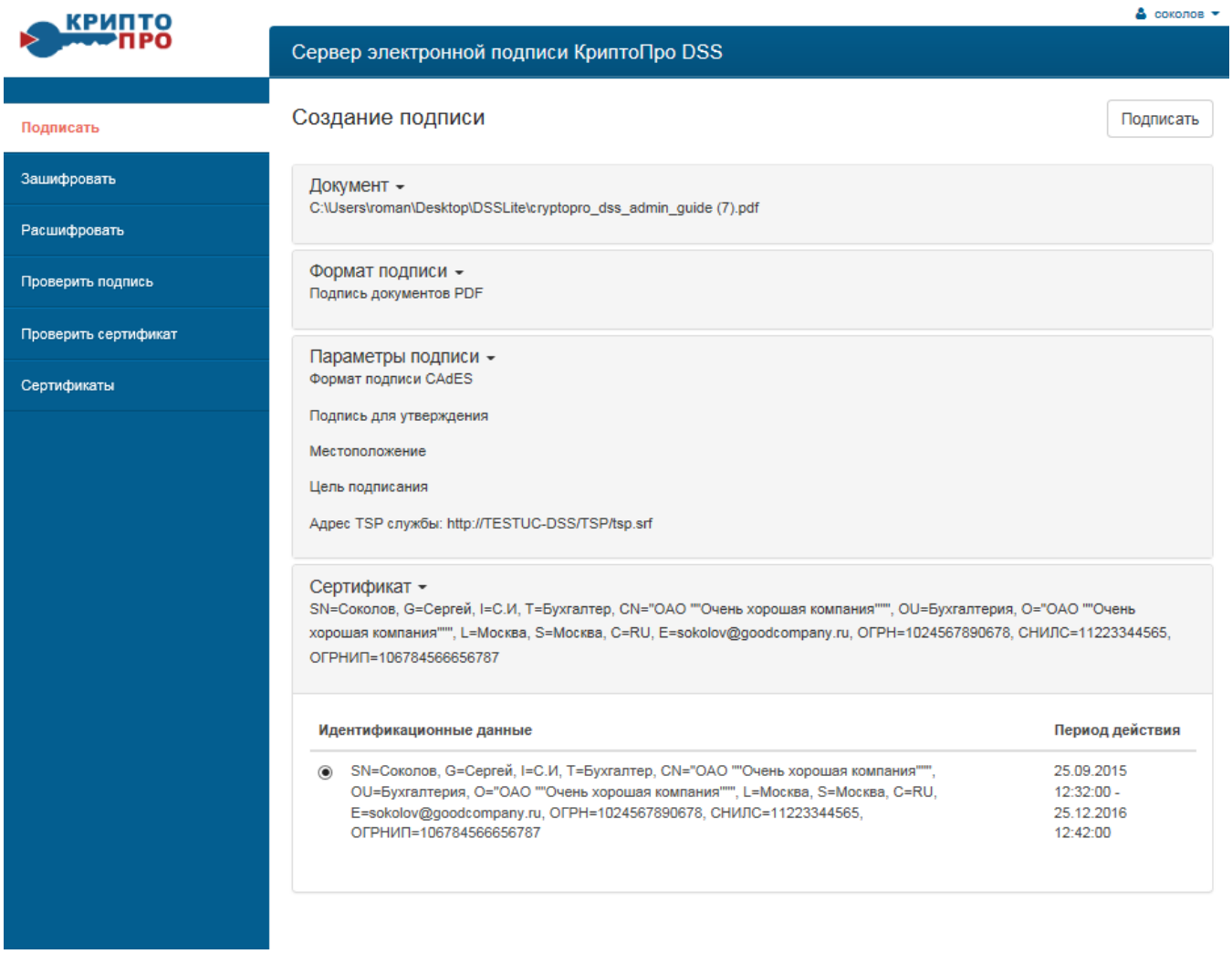


Рисунок 31. Выбор сертификата

6. После того как все параметры заданы, нажать сверху справа кнопку «**Подписать**» (см. Рисунок 32):

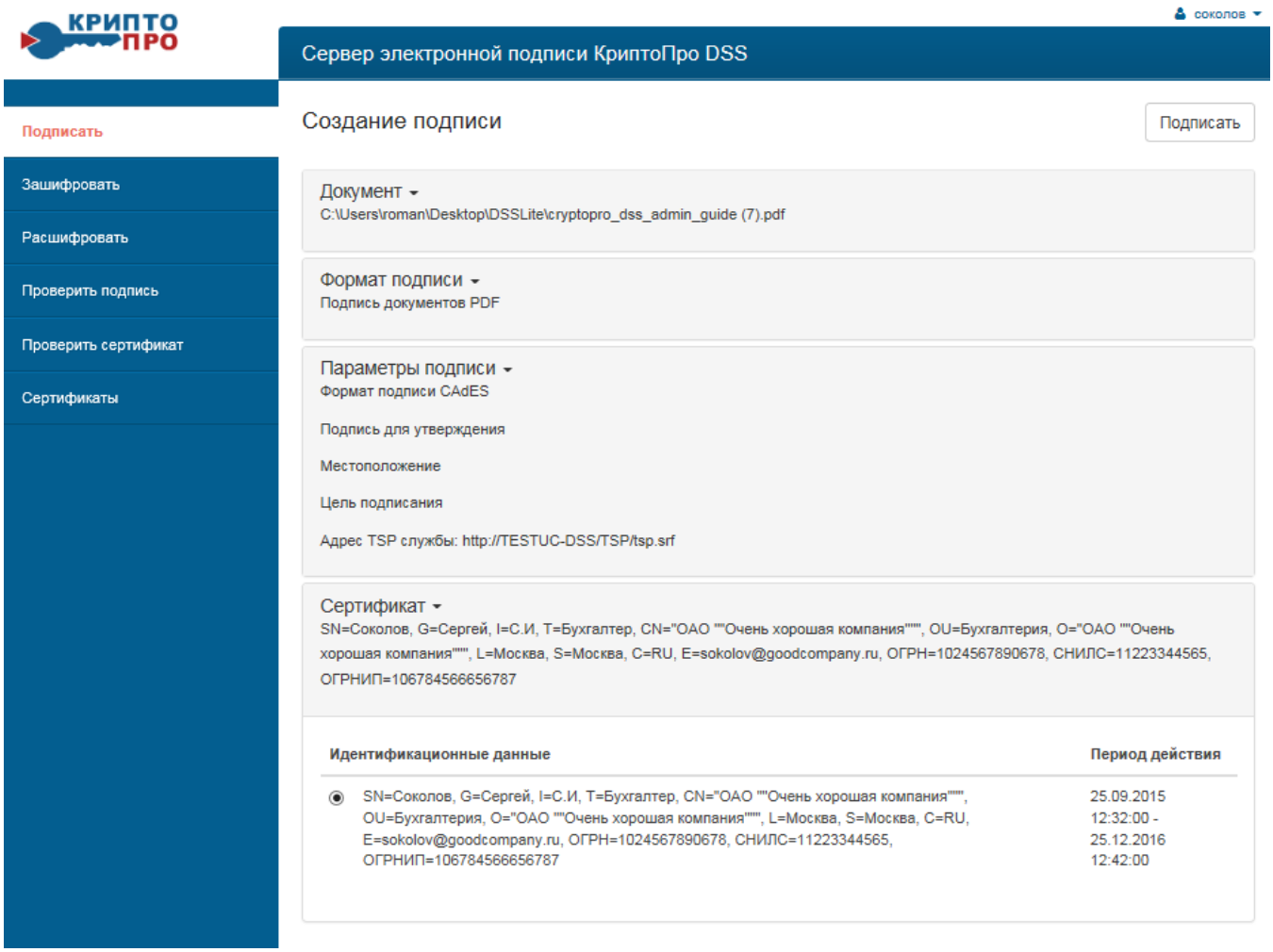


Рисунок 32. Подготовка документа к подписанию

7. В открывшемся окне ввести ПИН-код доступа к ключу электронной подписи и нажать «**ОК**» (см. Рисунок 33):

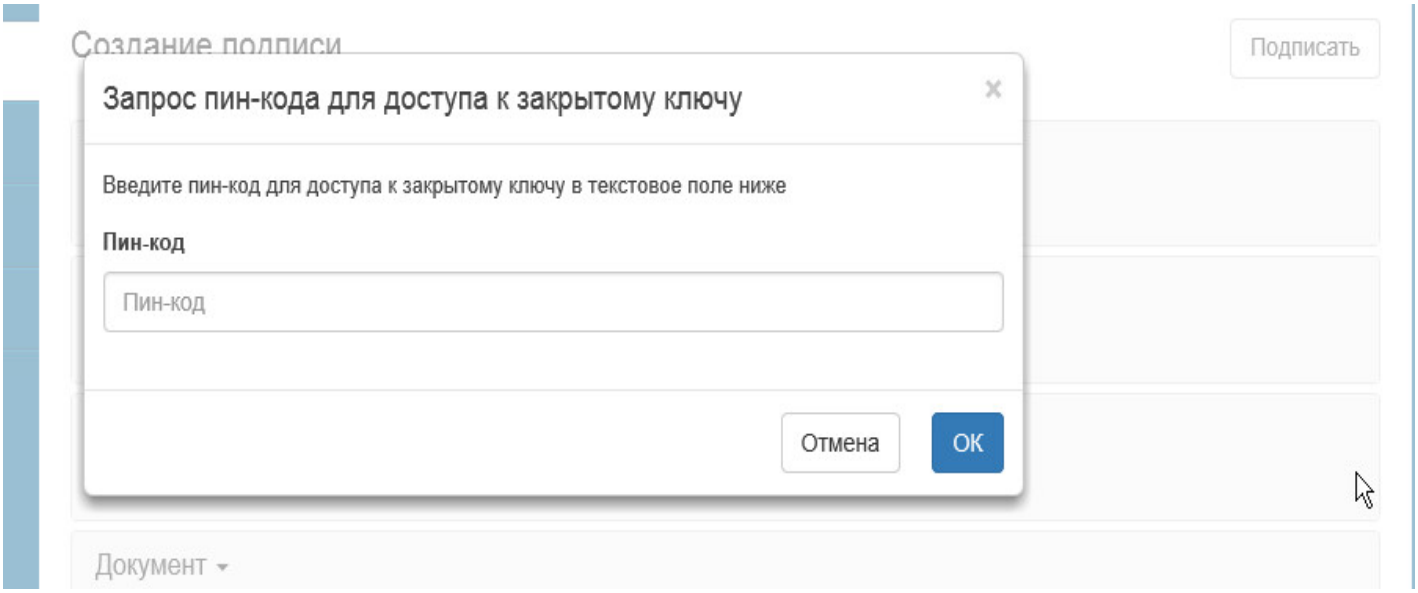


Рисунок 33. Ввод ПИН-кода к закрытому ключу электронной подписи

8. В открывшемся окне ввести одноразовый код (полученный в SMS на зарегистрированный номер мобильного телефона или сформированный с использованием полученного у Оператора OTP-токена) для подтверждения операции создания электронной подписи и нажать «**ОК**» (см. Рисунок 34):

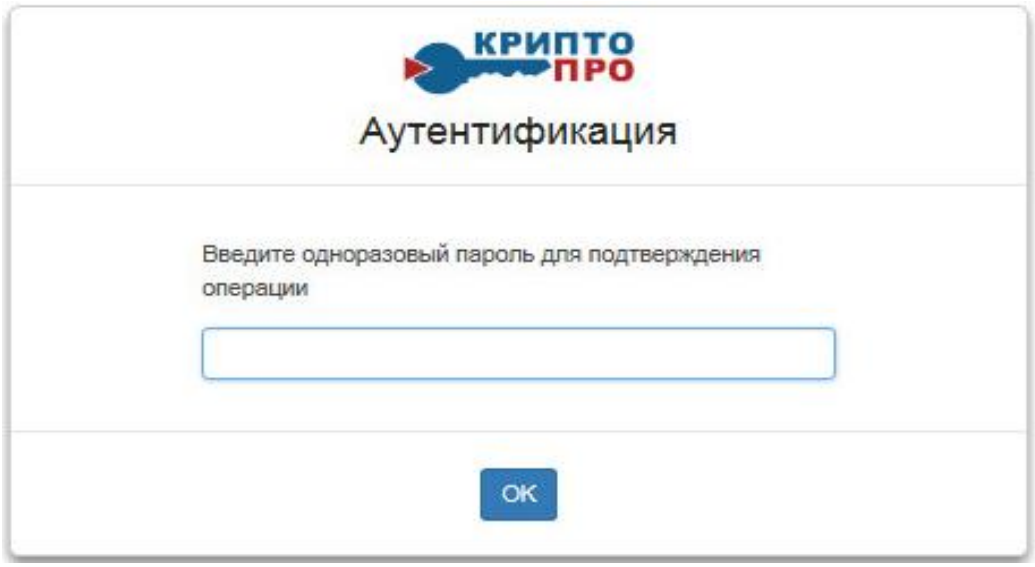


Рисунок 34. Ввод одноразового пароля для подтверждения операции

9. Документ будет подписан, после чего в низу открывшегося окна нажать стрелку, далее - «**Сохранить как**» (см. Рисунок 35):

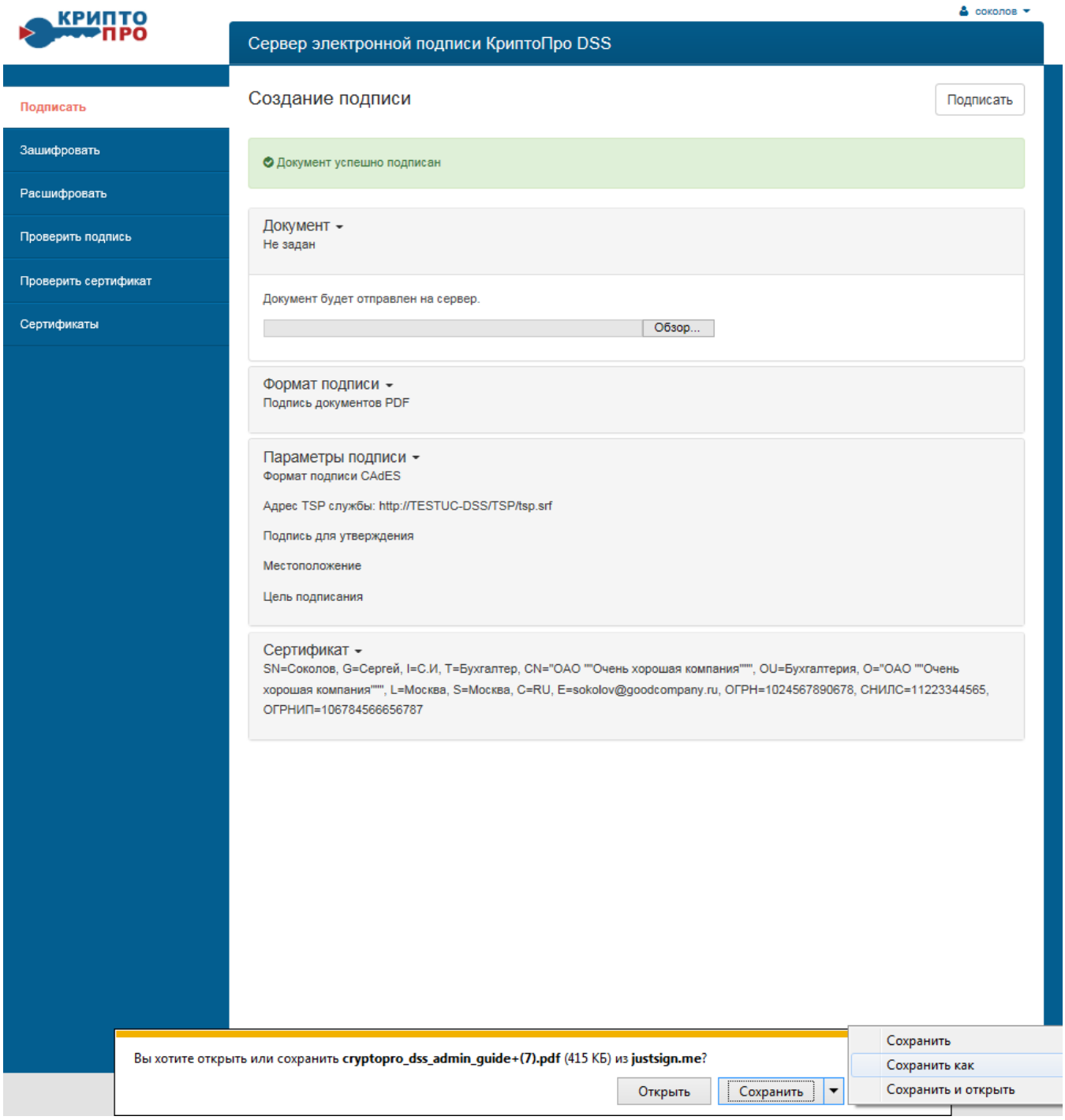


Рисунок 35. Сохранение подписанного электронного документа

10. Выбрать каталог и название файла для подписанного электронного документа (см. Рисунок 36):

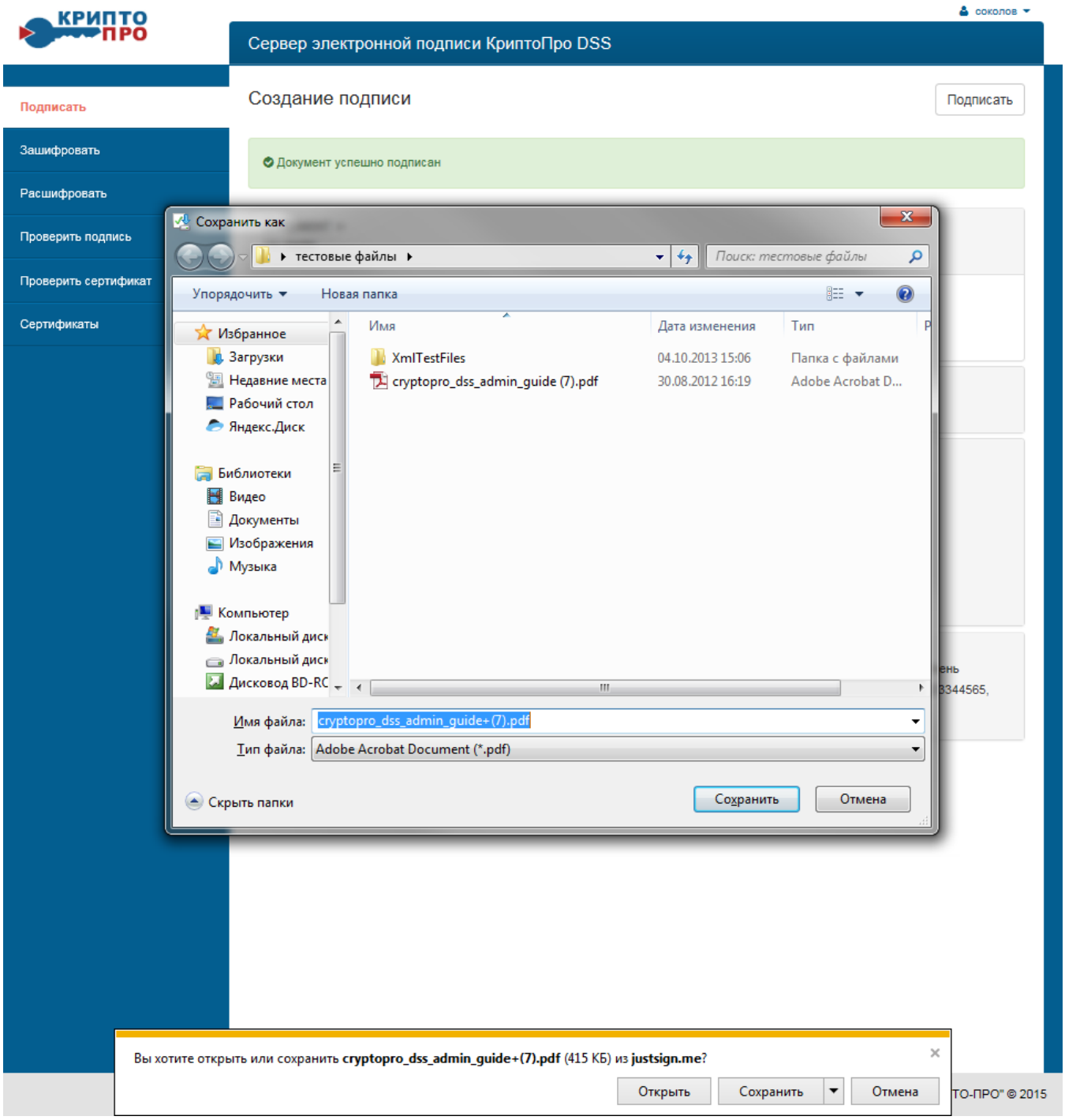


Рисунок 36. Выбор папки и названия файла для сохранения подписанного электронного документа

6. Проверка электронной подписи и сертификата

6.1. Проверка электронной подписи с использованием «Службы проверки электронной подписи» в составе СЭП.

С использованием Службы проверки электронной подписи (SVS) в составе СЭП может осуществляться проверка электронной подписи любого формата,

создание которого поддерживается в СЭП, а также проверка действительности сертификата ключа проверки электронной подписи.

1. Осуществить вход в личный кабинет Пользователя СЭП (в соответствии с п.3 Раздела 2) или в адресной строке Интернет-браузера ввести адрес https://www.justsign.me/verifyqca и в меню слева нажать на кнопку «**Проверить подпись**», откроется окно «**Проверка подписи**» (см. Рисунок 37):

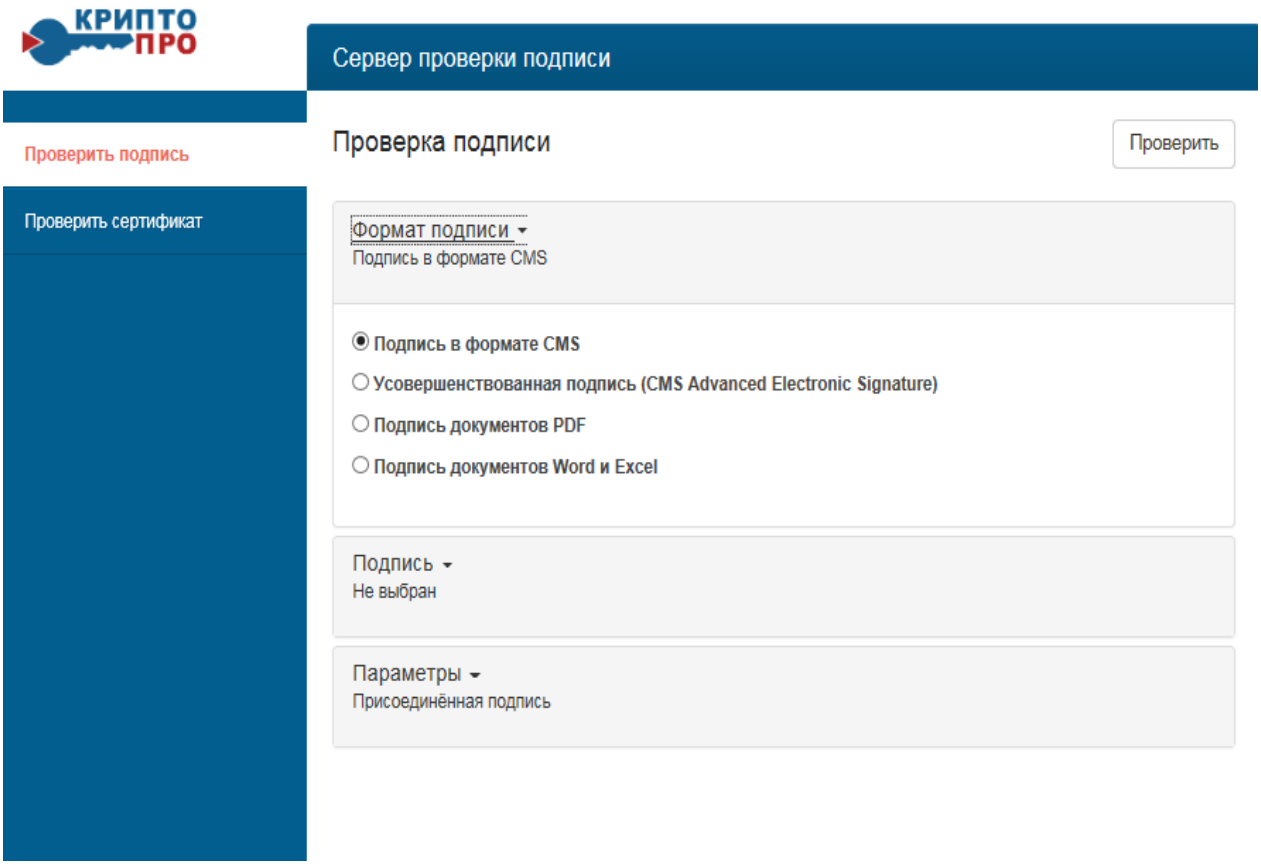


Рисунок 37. Окно проверка подписи

Выбрать формат подписи в соответствии с проверяемым документом:

«**Подпись документов PDF**» используется для файлов с расширением .pdf;

«**Подпись документов Word и Excel**» – с расширениями .docx или .xlsx.

«Подпись в формате CMS» и «**Усовершенствованная подпись (CAdeS)**» – для файлов с расширением .sig, содержащих электронную подпись в составе подписанного документа (Присоединенная подпись) или подпись отдельным файлом (Отсоединенная подпись).

Для проверки Присоединенной электронной подписи (в составе элетронного документа с расширением .sig) выбрать «**Подпись в формате CMS**», далее выбрать

«**Подпись**» и нажать «**Обзор**» откроется окно, выбрать подписанный документ (с расширением .sig) и нажать «**Открыть**» (см. Рисунок 38):

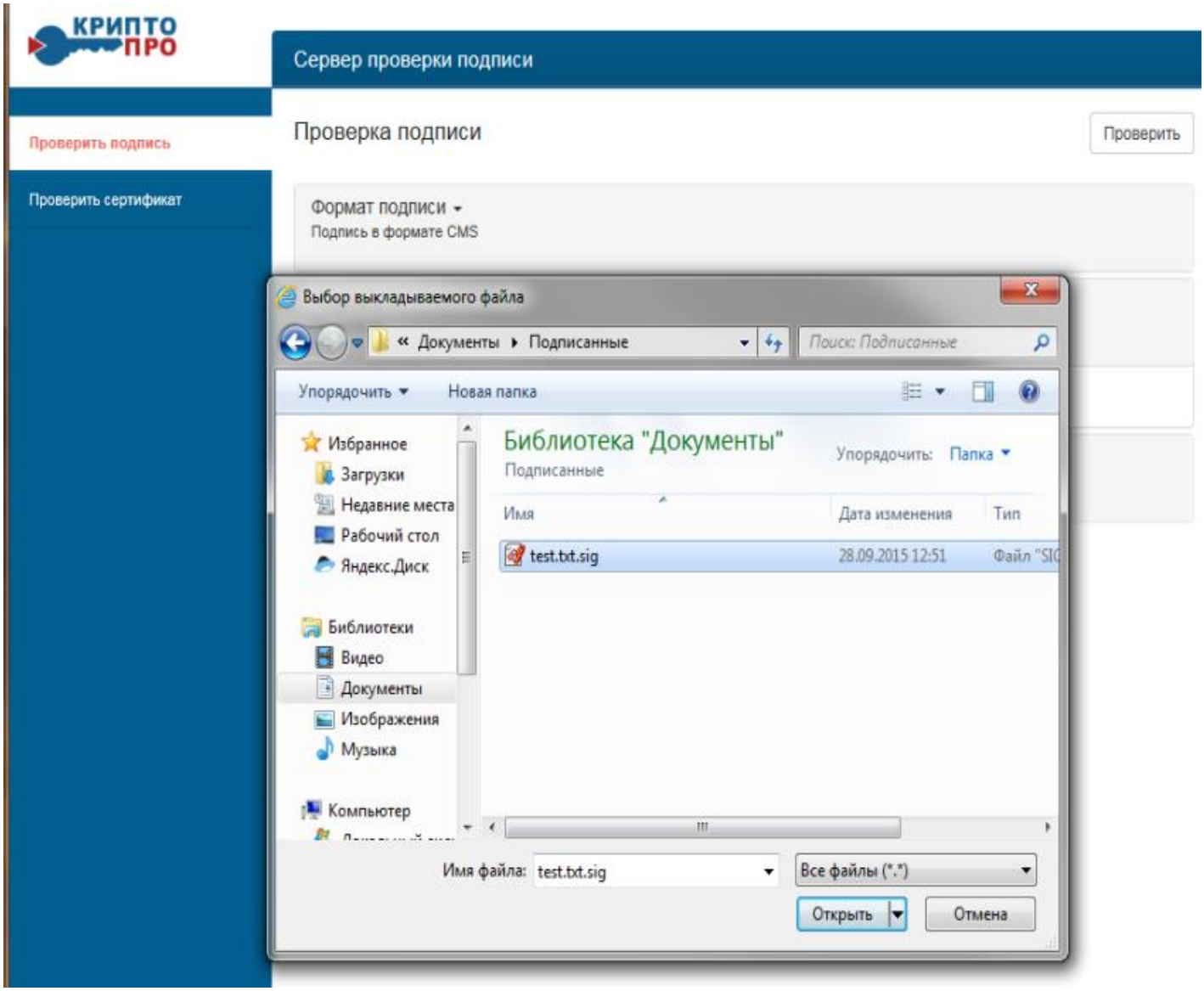


Рисунок 38. Выбор файла для проверки присоединенной электронной подписи (в составе электронного документа)

2. Выбрать Параметры «**Присоединенная подпись**», после нажать кнопку «**Проверить**» (см. Рисунок 39):

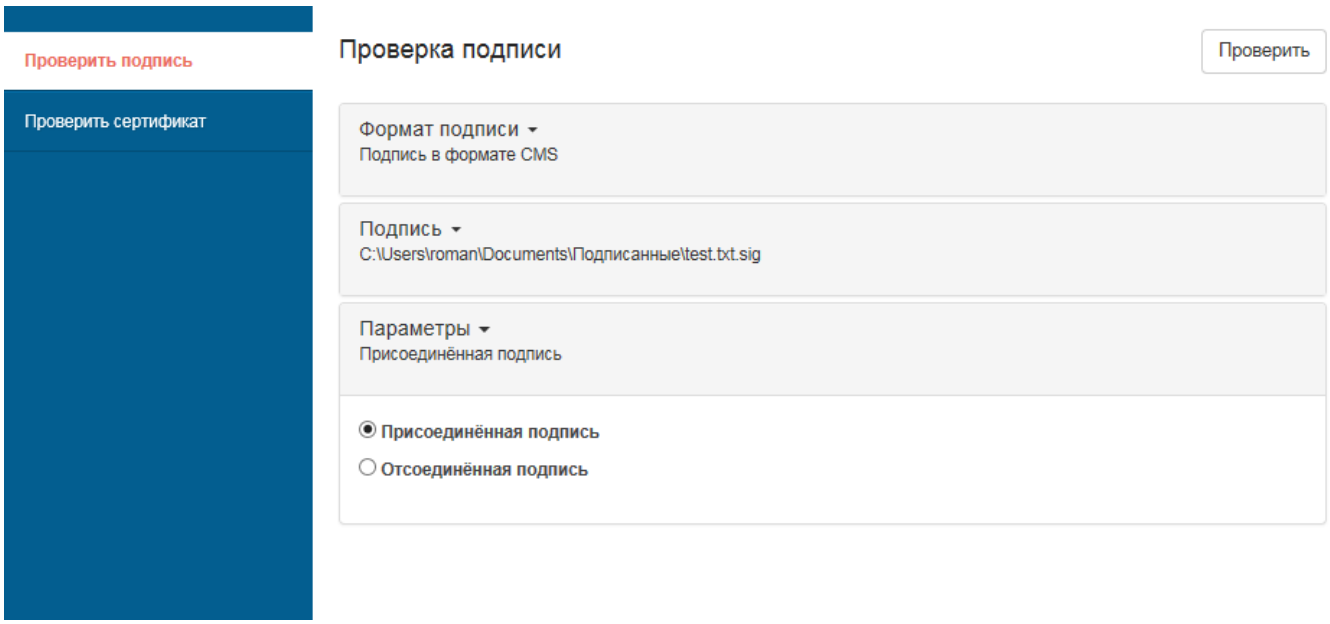


Рисунок 39. Параметр присоединённой подписи

3. Будет выполнено действие проверки электронной подписи документа и откроется окно с результатом (см. Рисунок 40):

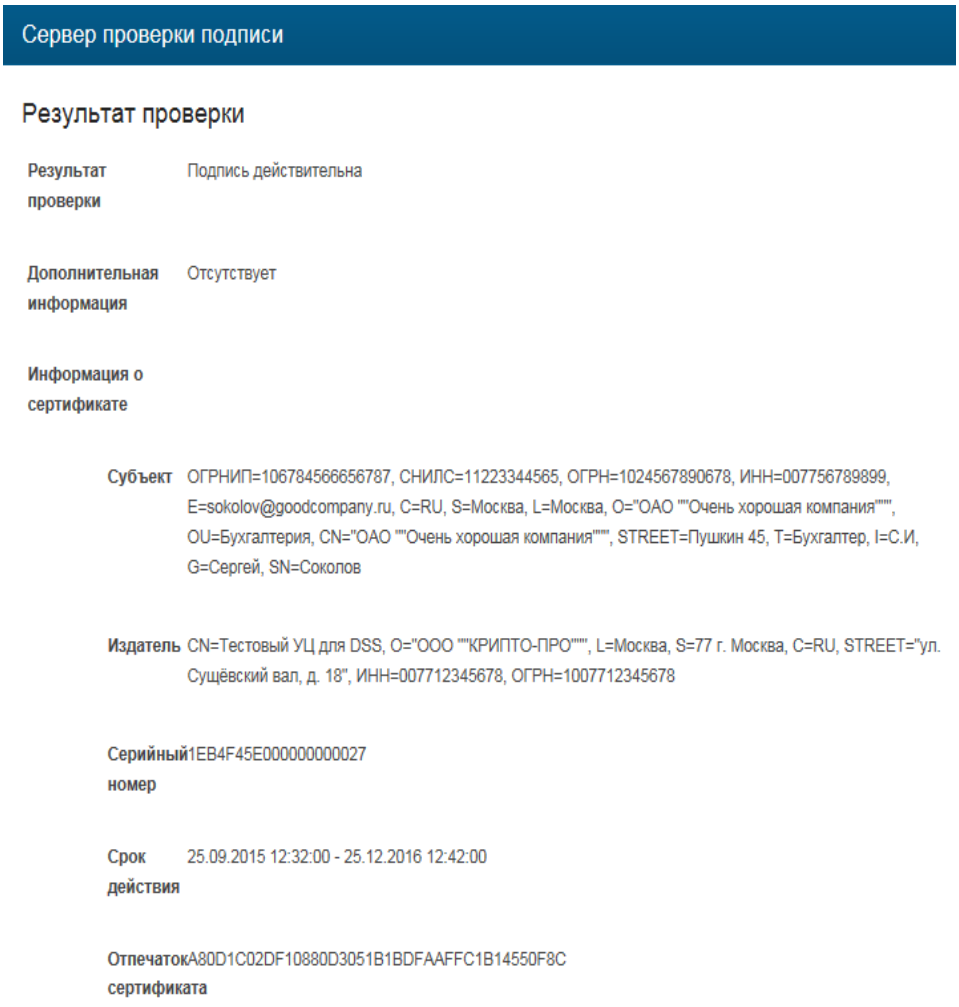


Рисунок 40. Результат проверки электронной подписи

4. Для проверки Отсоединенной электронной подписи (отдельным файлом с расширением .sig к первоначальному неподписанному документу произвольного формата файла) после загрузки файла подписи выбрать Параметры «**Отсоединенная подпись**», в открывшемся поле «**Документ**» нажать «Обзор» и выбрать файл первоначального неподписанного документа (см. Рисунок 41):

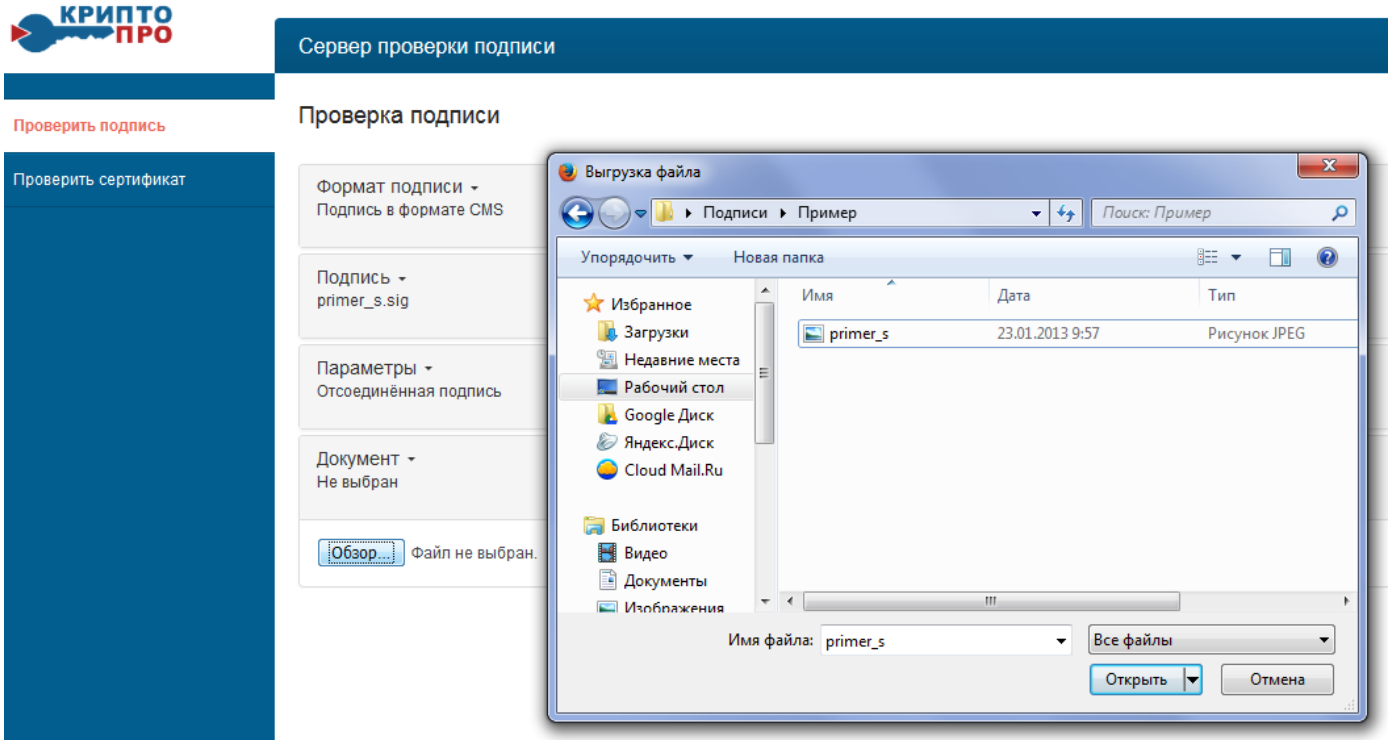


Рисунок 41. Выбор файла первоначального документа для проверки отсоединенной электронной подписи

5. Нажать кнопку «**Проверить**».

6. В случае отрицательного результата проверки «**Подпись не действительна**» по причине недействительного сертификата ключа проверки электронной подписи выполнить повторную проверку, выбрав Формат подписи «**Усовершенствованная подпись (CMS Advanced Electronic Signature)**». В случае использования соответствующего формата при создании подписи проверка будет произведена на момент подписания электронного документа и подпись будет считаться действительной, если сертификат действовал в момент создания подписи.

6.2. Проверка сертификата, полученного от другого пользователя

1. Проверка действительности сертификата ключа проверки электронной подписи, полученного от контрагента (например, для шифрования электронных документов в соответствии с Разделом 7) осуществляется с использованием «Службы проверки электронной подписи». Доступ к Службе проверки осуществляется из личного кабинета Пользователя СЭП или по адресу https://www.justsign.me/verifycpca в меню слева нажать кнопку «**Проверить сертификат**» (см. Рисунок 42):

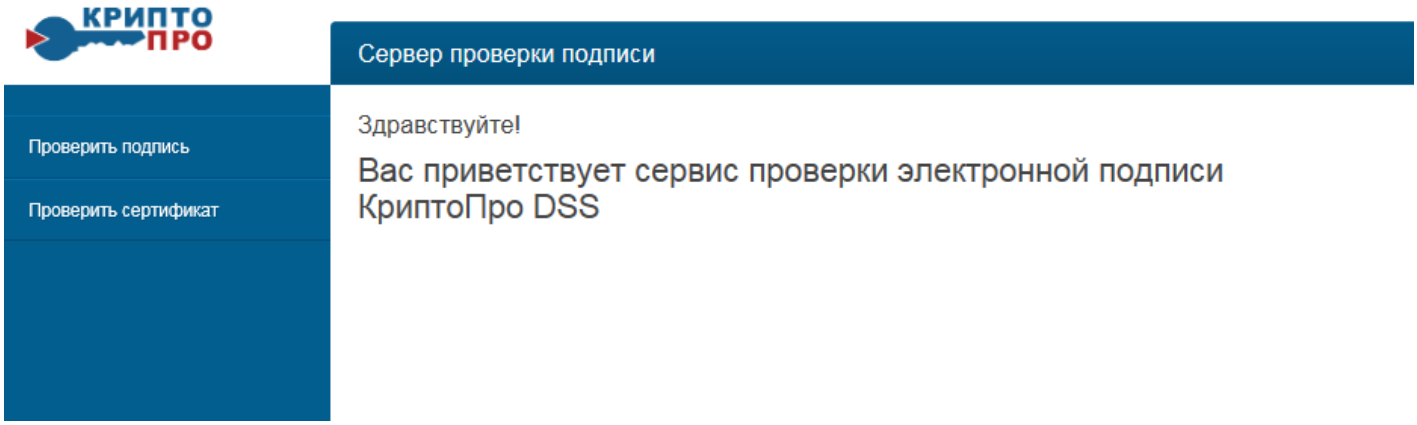


Рисунок 42. Проверка сертификата

2. Далее нажать на «**Обзор**» и выбирать ранее полученный от контрагента сертификат, нажать «**Проверить**», откроется окно с результатом проверки (см. Рисунок 43):

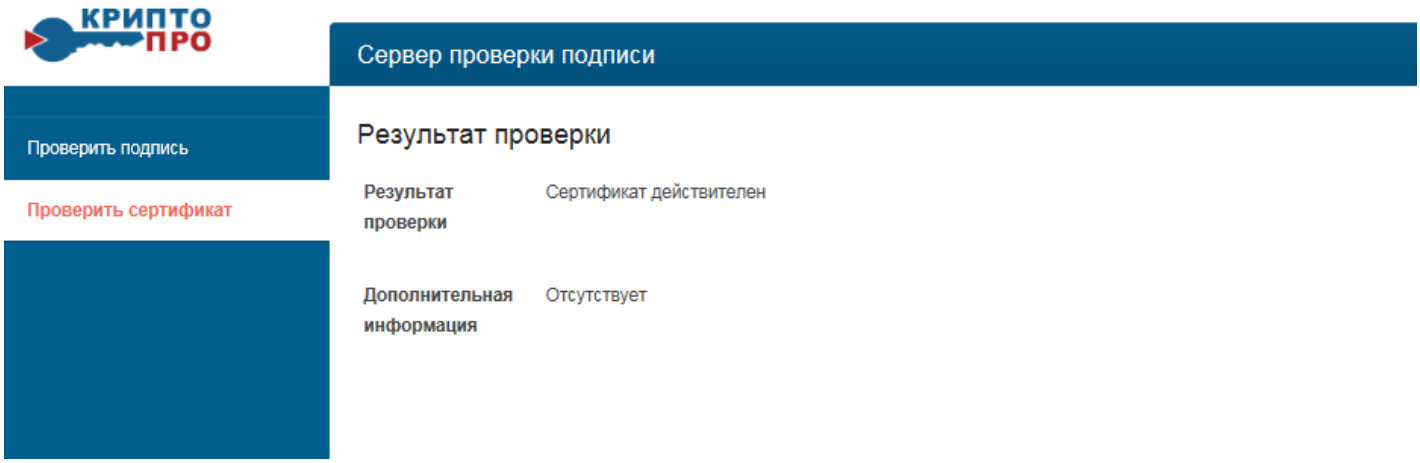


Рисунок 43. Результат проверки сертификата

7. Шифрование файлов электронных документов

1. Осуществить вход в личный кабинет Пользователя СЭП (в соответствии с п.3 Раздела 2) и в меню слева нажать «**Зашифровать**» (см. Рисунок 44):

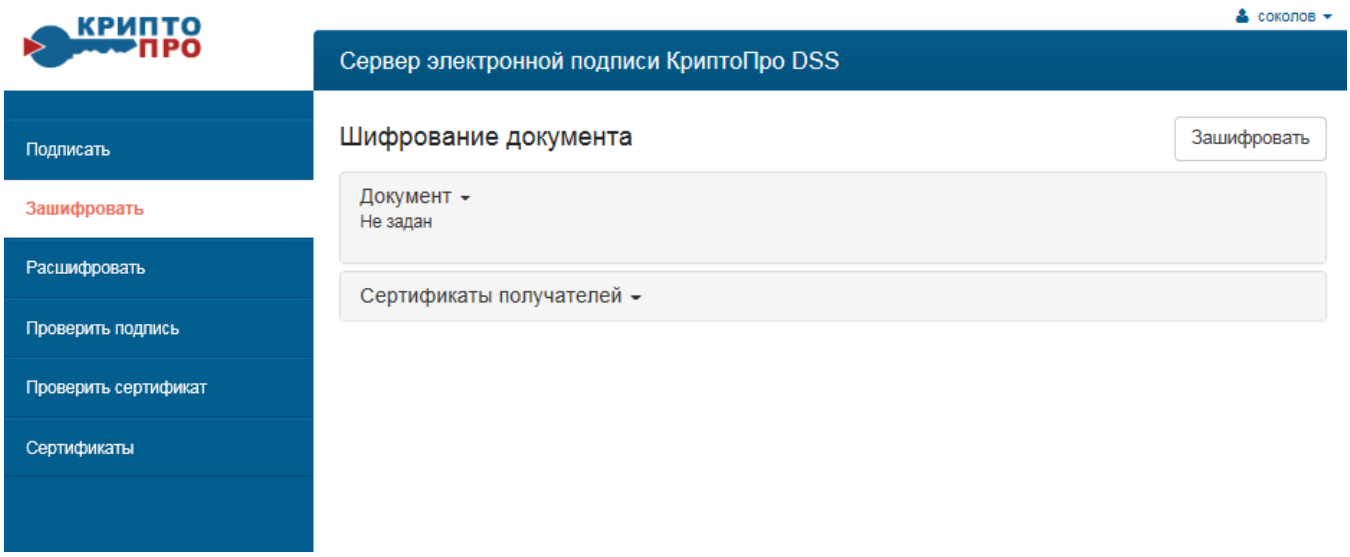


Рисунок 44. Шифрование документа

2. Нажать кнопку «**Сертификаты получателей**» и выбрать предварительно полученный сертификат от того пользователя, которому предназначается зашифрованный файл или выбрать сертификаты получателей из хранилища сертификатов «**Другие пользователи**» (см. Рисунок 45):

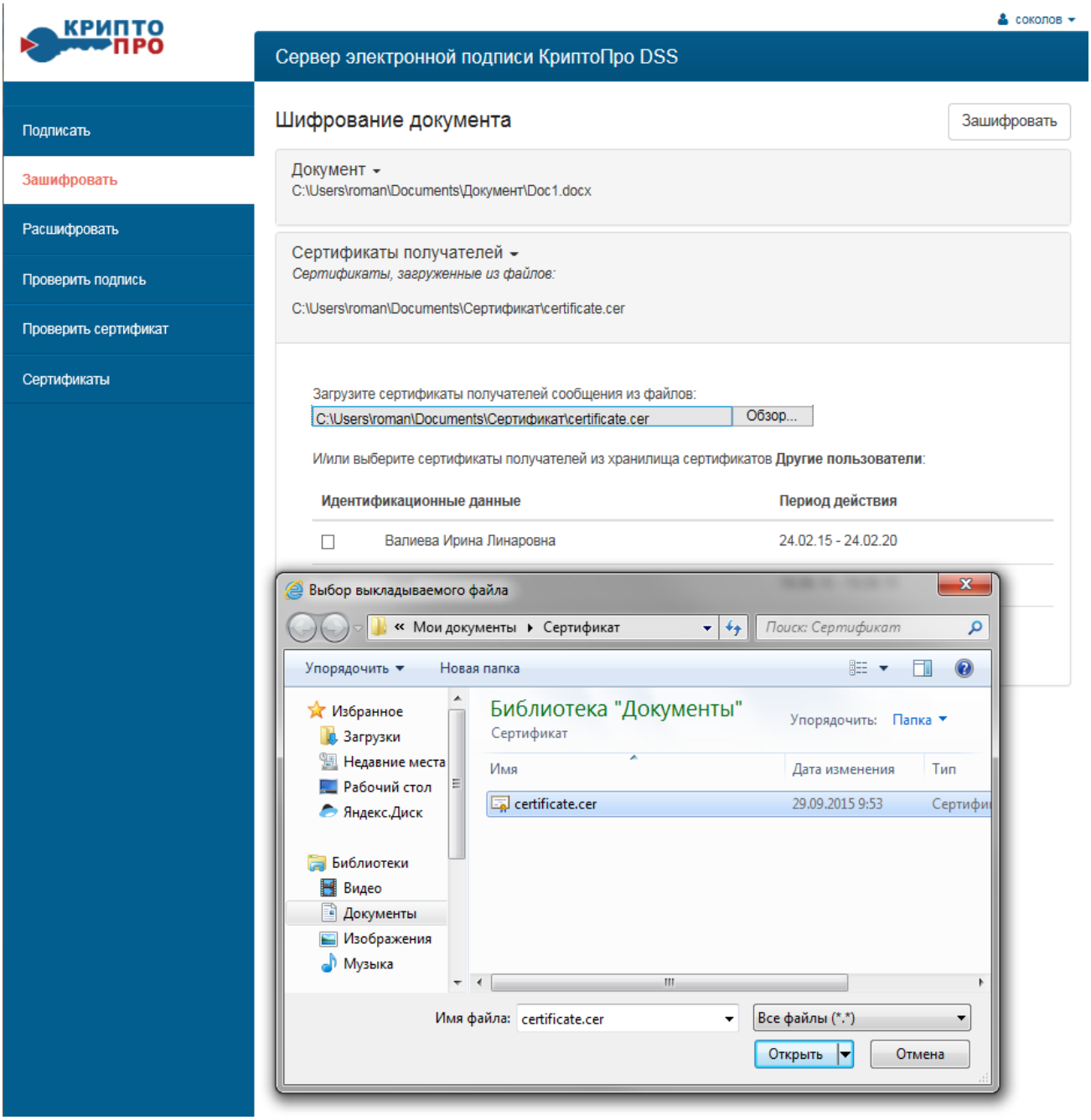


Рисунок 45. Выбор сертификата пользователя

3. Нажать кнопку «**Обзор**» выбрать документ для шифрования (см. Рисунок 46):

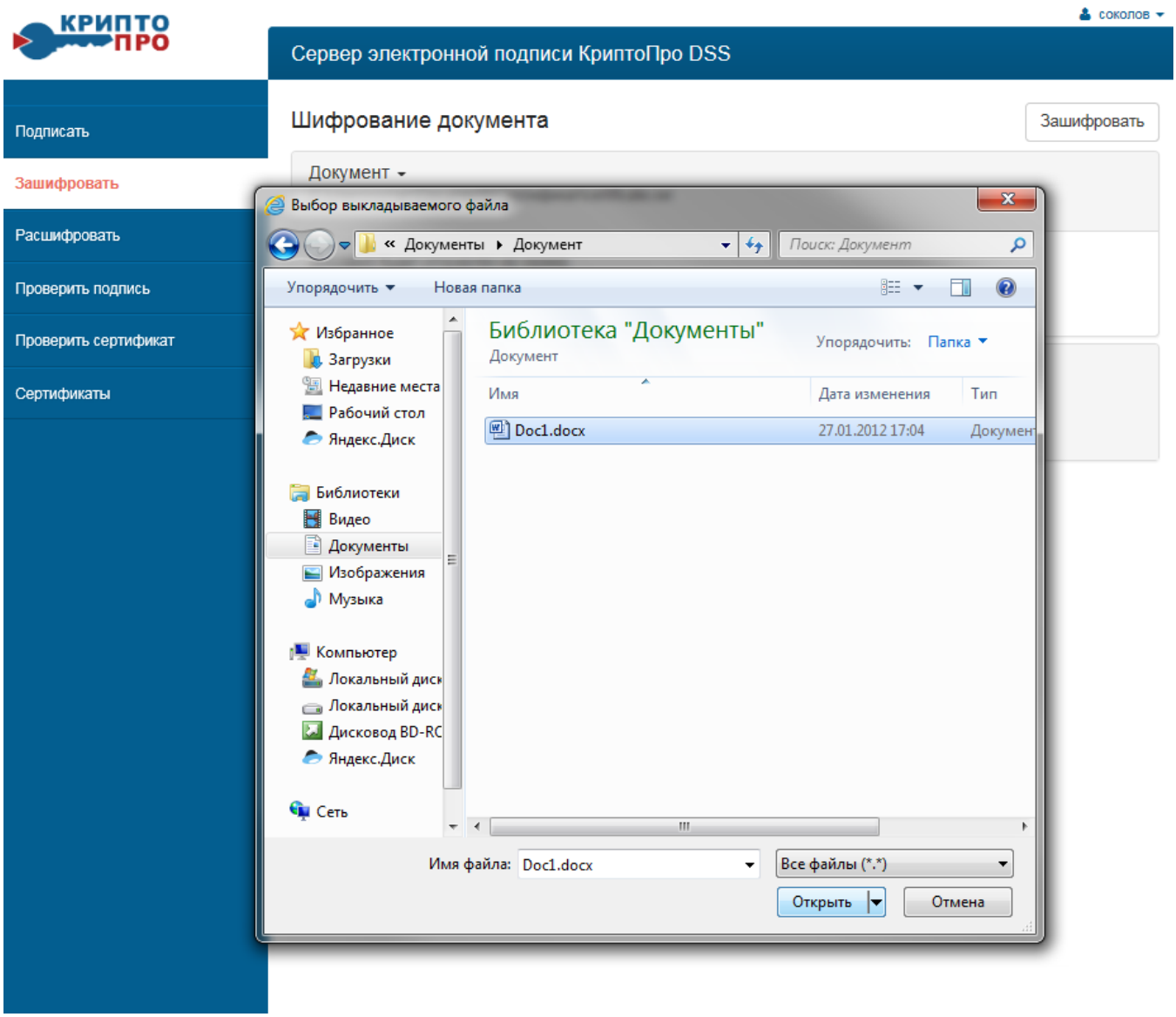


Рисунок 46. Выбор документа для шифрования

4. Нажать кнопку «Зашифровать» откроется окно с результатом действия «**Документ зашифрован**» и будет предложено его сохранить, нажать «**Сохранить как**» (см. Рисунок 47 и Рисунок 48):

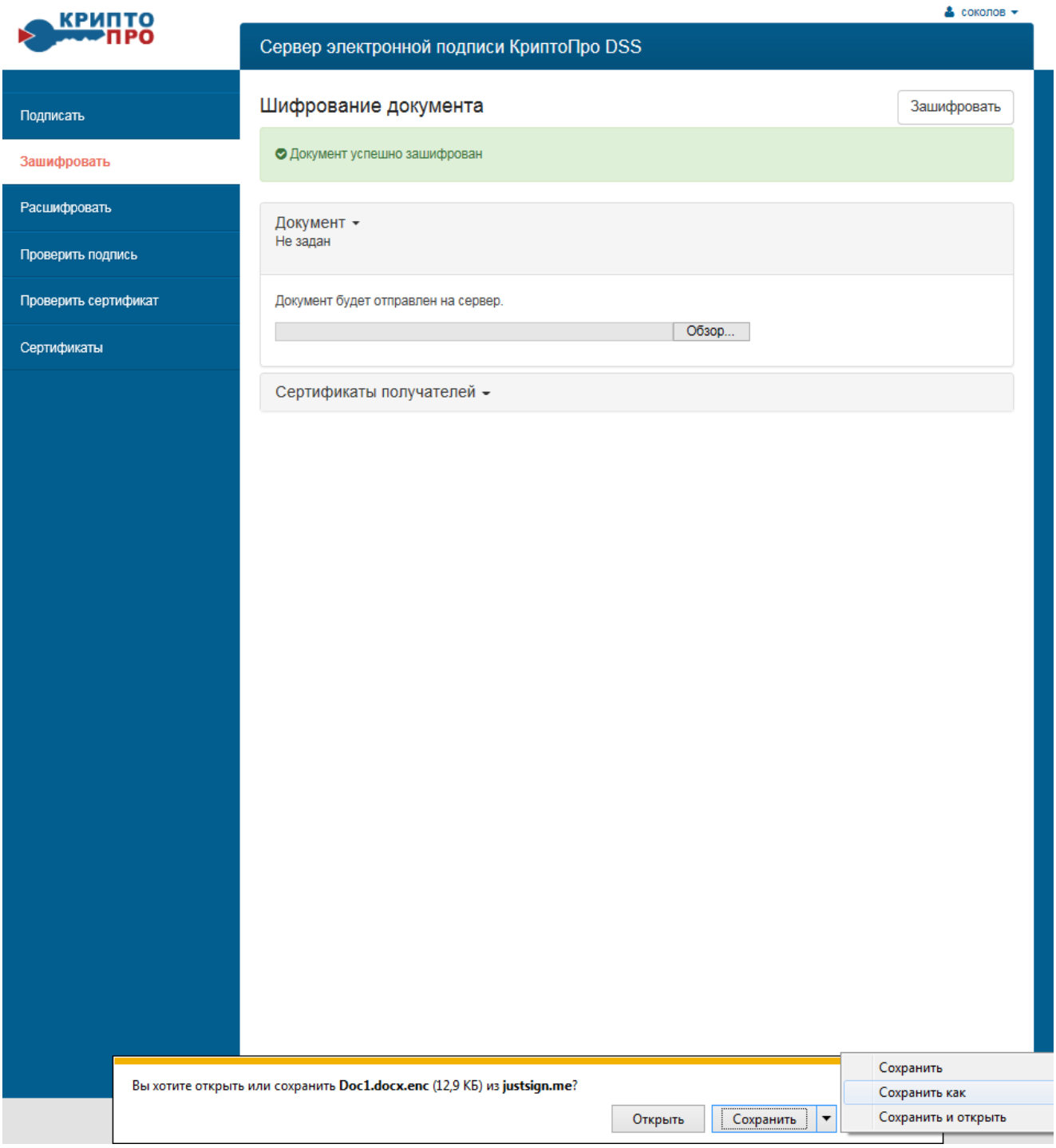


Рисунок 47. Завершение операции шифрования документа

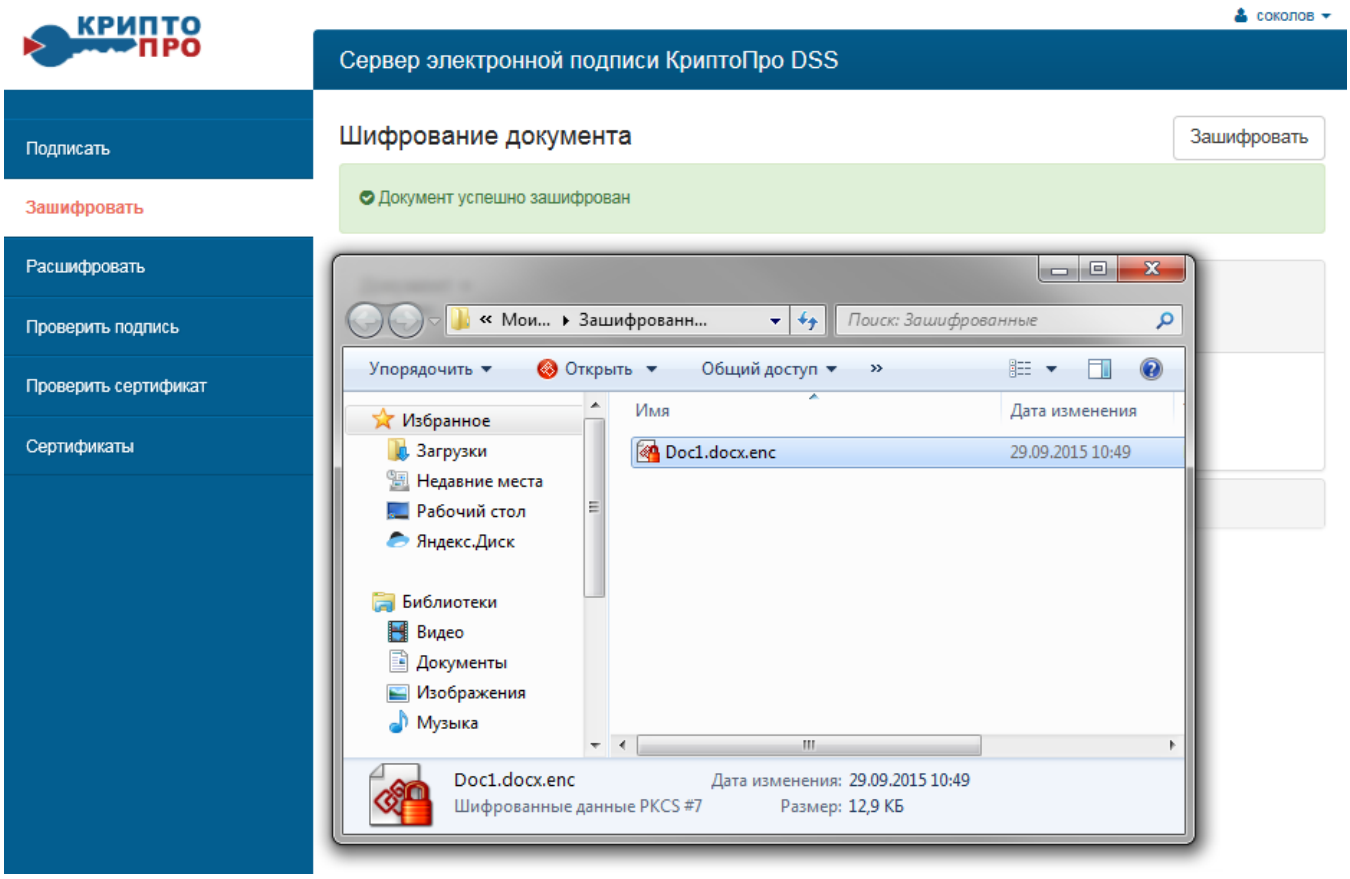


Рисунок 48. Сохранение зашифрованного документа

5. Для шифрования своих документов предварительно выгрузить с СЭП свой сертификат (см. Раздел **3**). Далее шифрование, выполнить, как описано в текущем разделе.

8. Расшифровывание файлов электронных документов

1. Осуществить вход в личный кабинет Пользователя СЭП (в соответствии с п.3 Раздела 2) и в меню слева нажать «**Расшифровать**» (см. Рисунок 49):

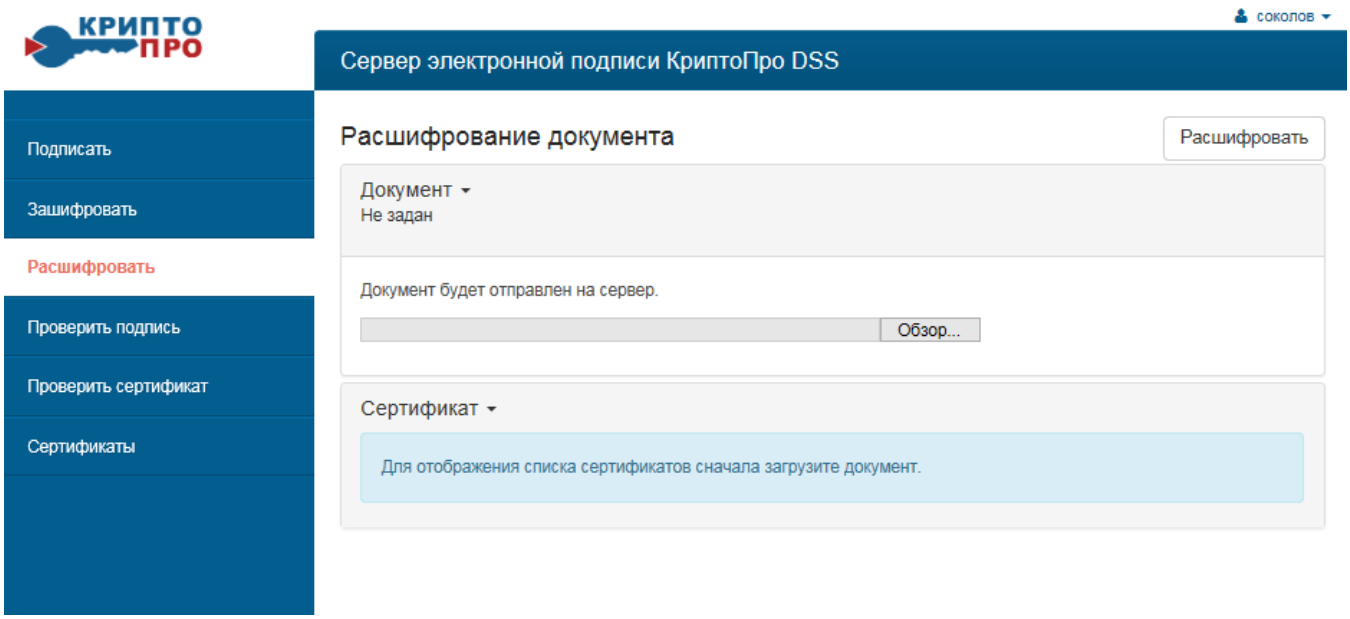


Рисунок 49. Расшифровывание документа

2. Нажать кнопку «**Обзор**» выбрать документ для расшифровывания, нажать кнопку «**Открыть**» (см. Рисунок 50):

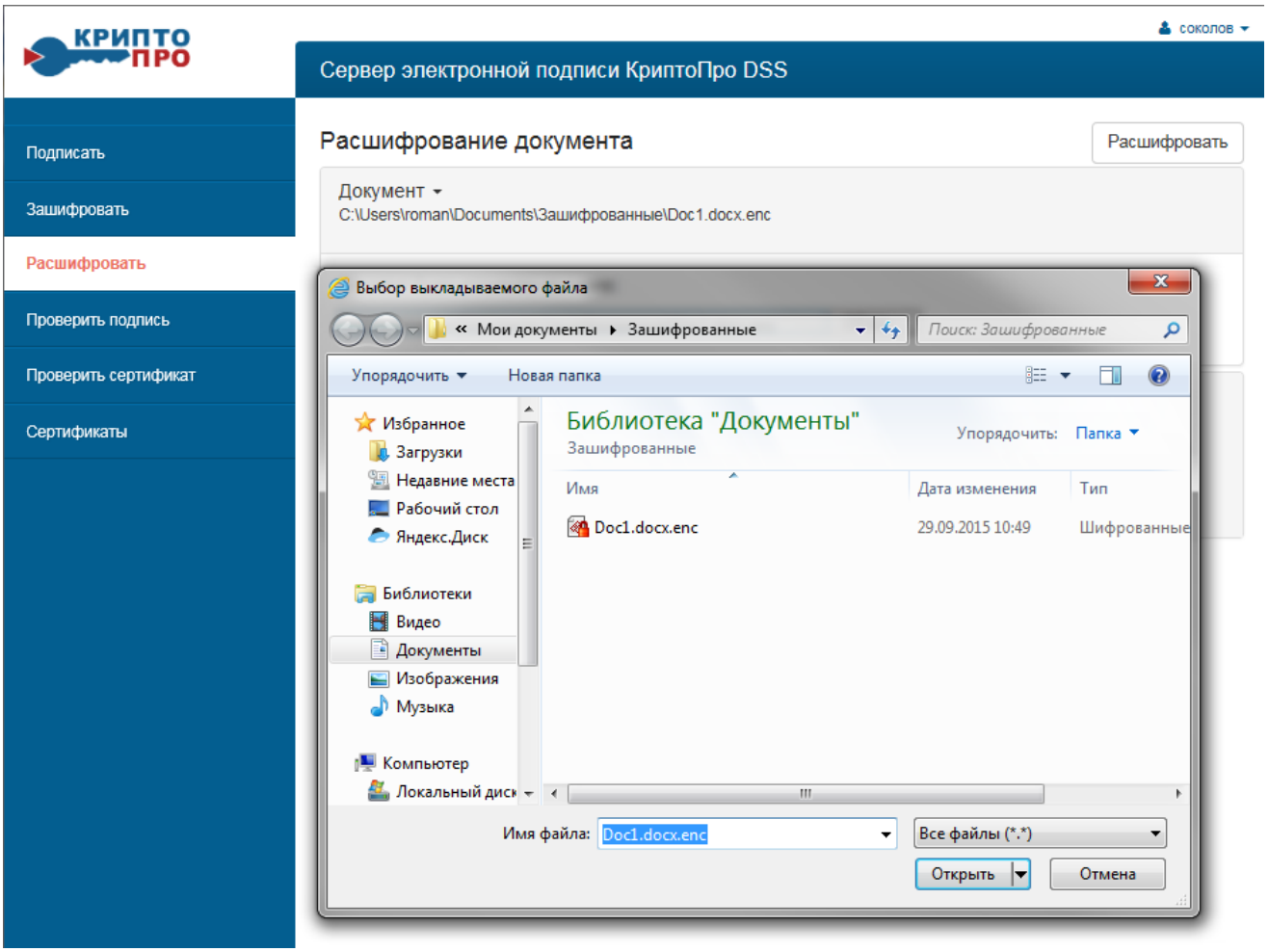


Рисунок 50. Выбор документа для расшифровывания

3. Далее будет автоматически произведена проверка используемого сертификата и отображены его сведения (см. Рисунок 51):

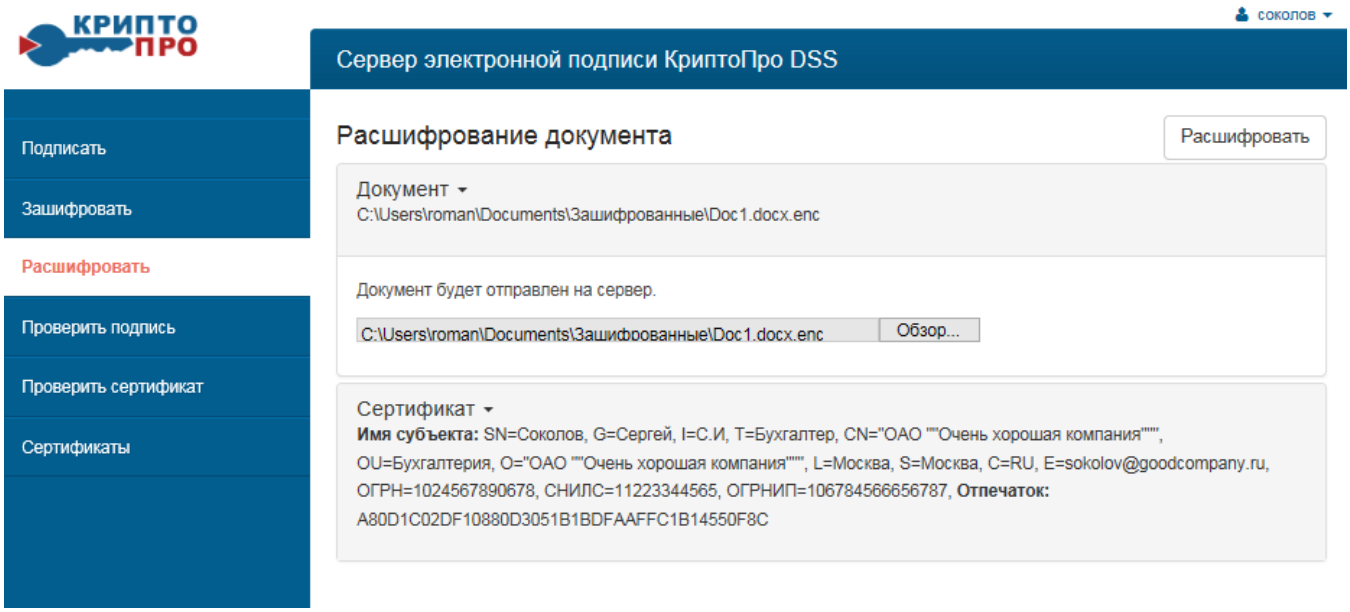


Рисунок 51. Вывод информации об используемом сертификате

4. Если сертификат недействительный, то отобразится соответствующее сообщение (см. Рисунок 52):

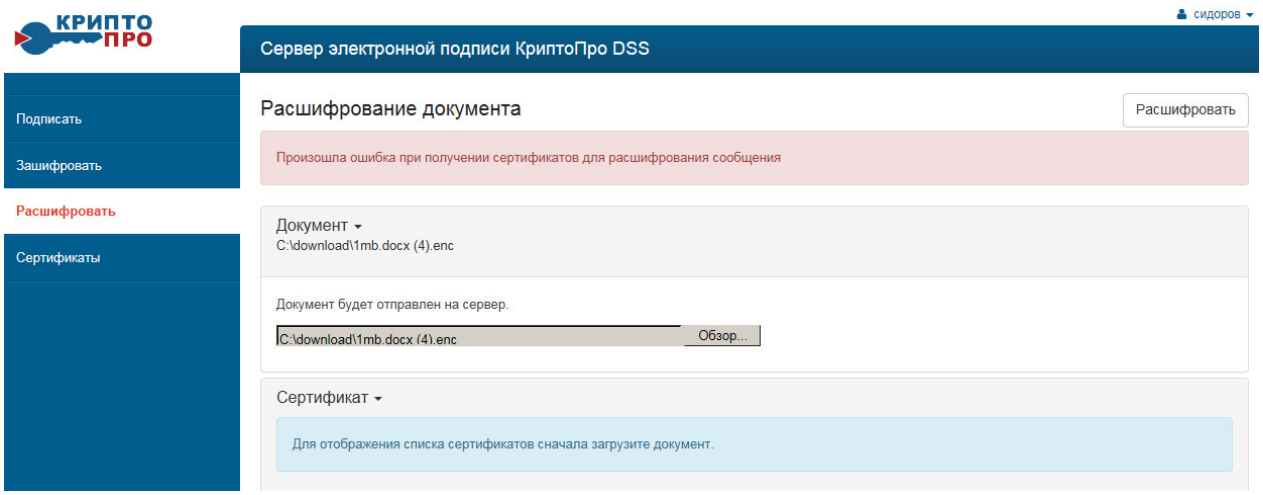


Рисунок 52. Отрицательный результат проверки сертификата

В этом случае необходимо запросить у контрагента новый действующий сертификат.

5. После успешной проверки сертификата, нажать кнопку «**Расшифровать**» и в открывшемся окне ввести ПИН-кода доступа к закрытому ключу и нажать кнопку «**ОК**» (см. Рисунок 53):

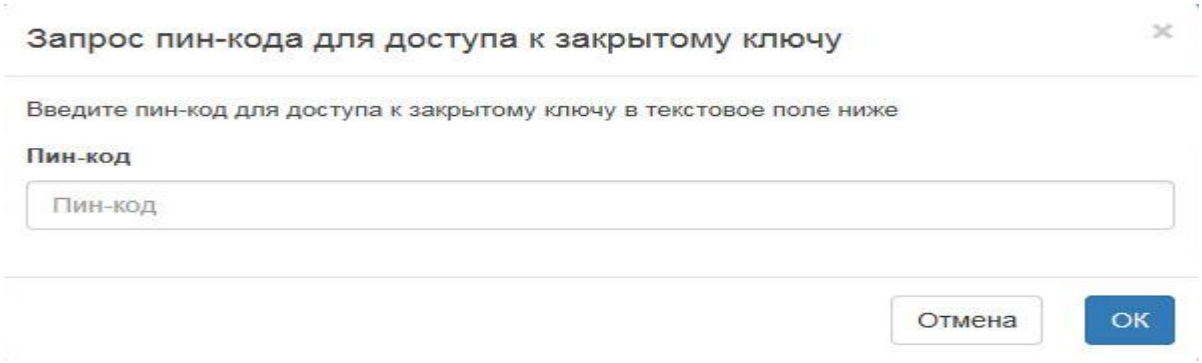


Рисунок 53. Окно для ввода ПИН-кода доступа к закрытому ключу

6. В открывшемся окне ввести одноразовый код (полученный в SMS на зарегистрированный номер мобильного телефона или сформированный с использованием полученного у Оператора OTP-токена) для подтверждения операции и нажать «**ОК**» (см. Рисунок 54):

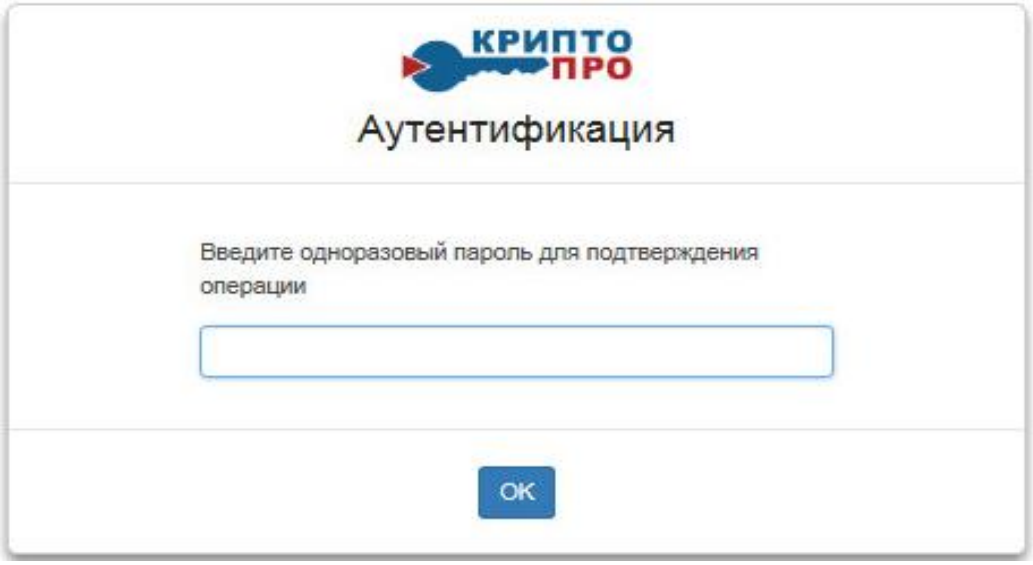


Рисунок 54. Ввод одноразового пароля для подтверждения операции

7. Откроется окно «Документ успешно расшифрован» и будет предложено его сохранить, нажать «**Сохранить как**» (см. Рисунок 55):

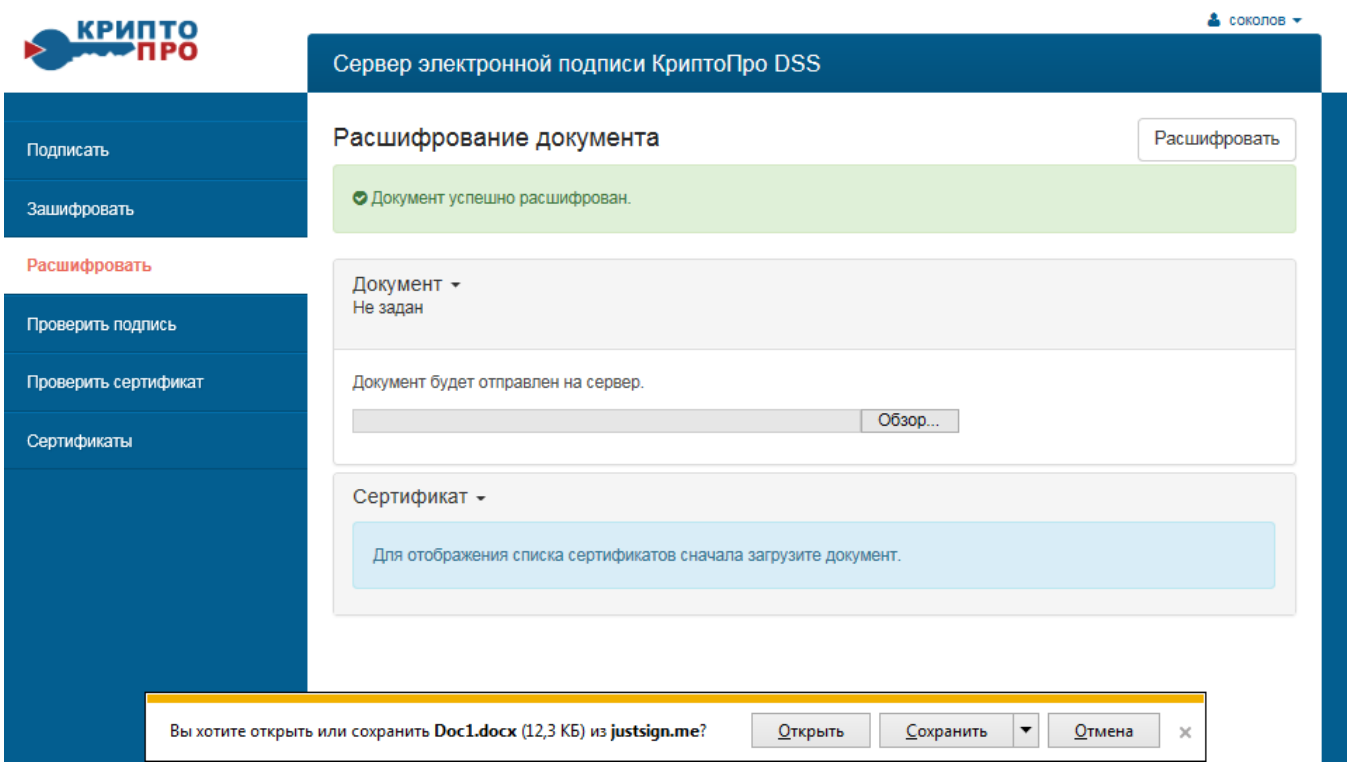


Рисунок 55. Сохранение расшифрованного документа

8. Откроется окно, ввести имя расшифрованного документа и нажать «**Сохранить**» (см. Рисунок 56):

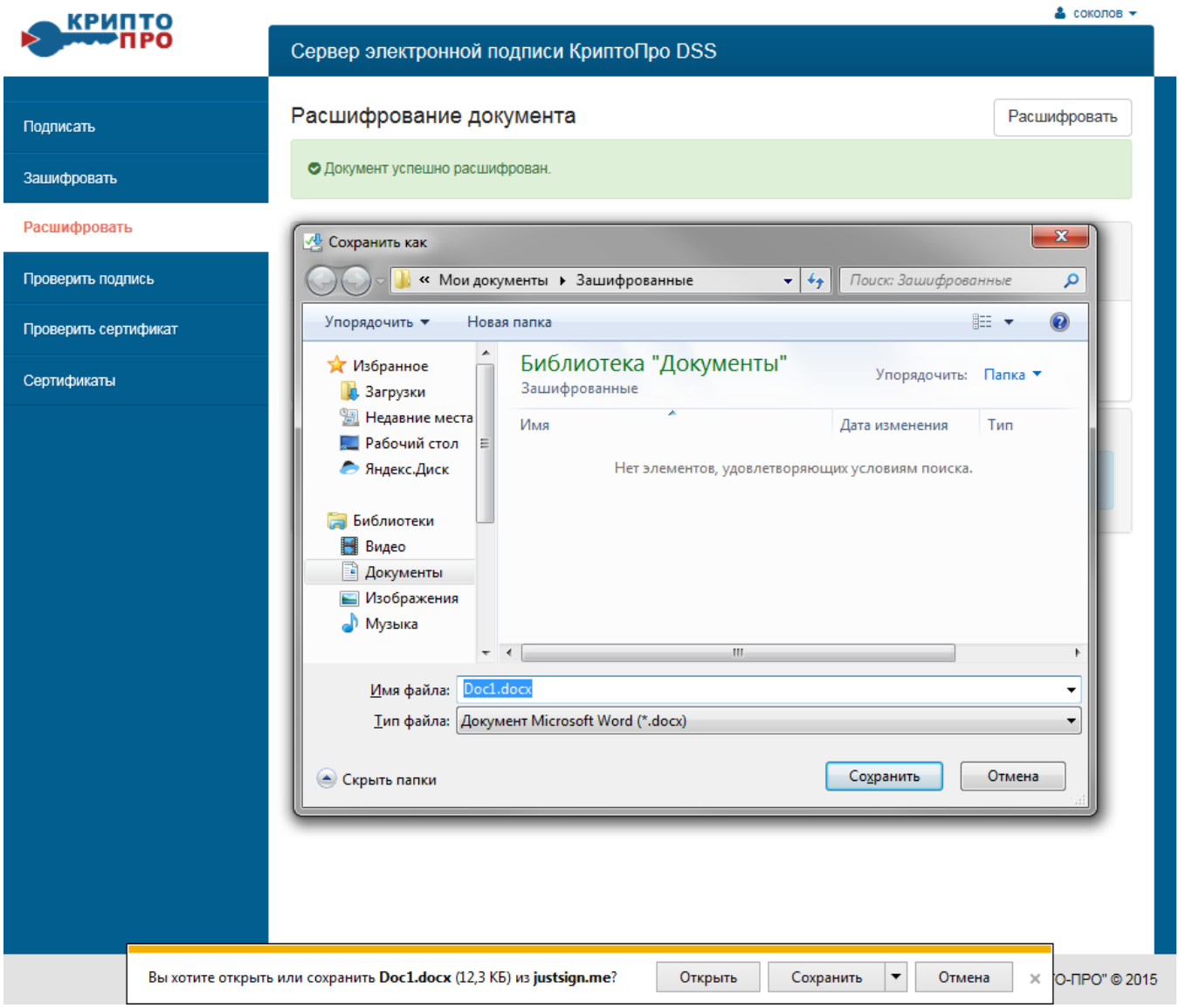


Рисунок 56. Выбор папки для сохранения расшифрованного документа

Приложение 1.

Настройка Интернет-браузера

Настройка Google Chrome

1) Открыть меню Chrome на панели инструментов.
2) Выбрать «**Дополнительные инструменты**».
3) Нажать «**Удаление данных о просмотренных страницах».**
4) В открывшемся диалоговом окне установить флажки рядом с пунктами «**Файлы cookie и другие данные с сайтов и плагинов**» и «**Изображения и другие файлы, сохраненные в кеше**».
5) Чтобы удалить все данные, выбрать временной интервал «**За все время**».
6) Нажмите «**Очистить историю**» (см. Рисунок 57 и Рисунок 58):

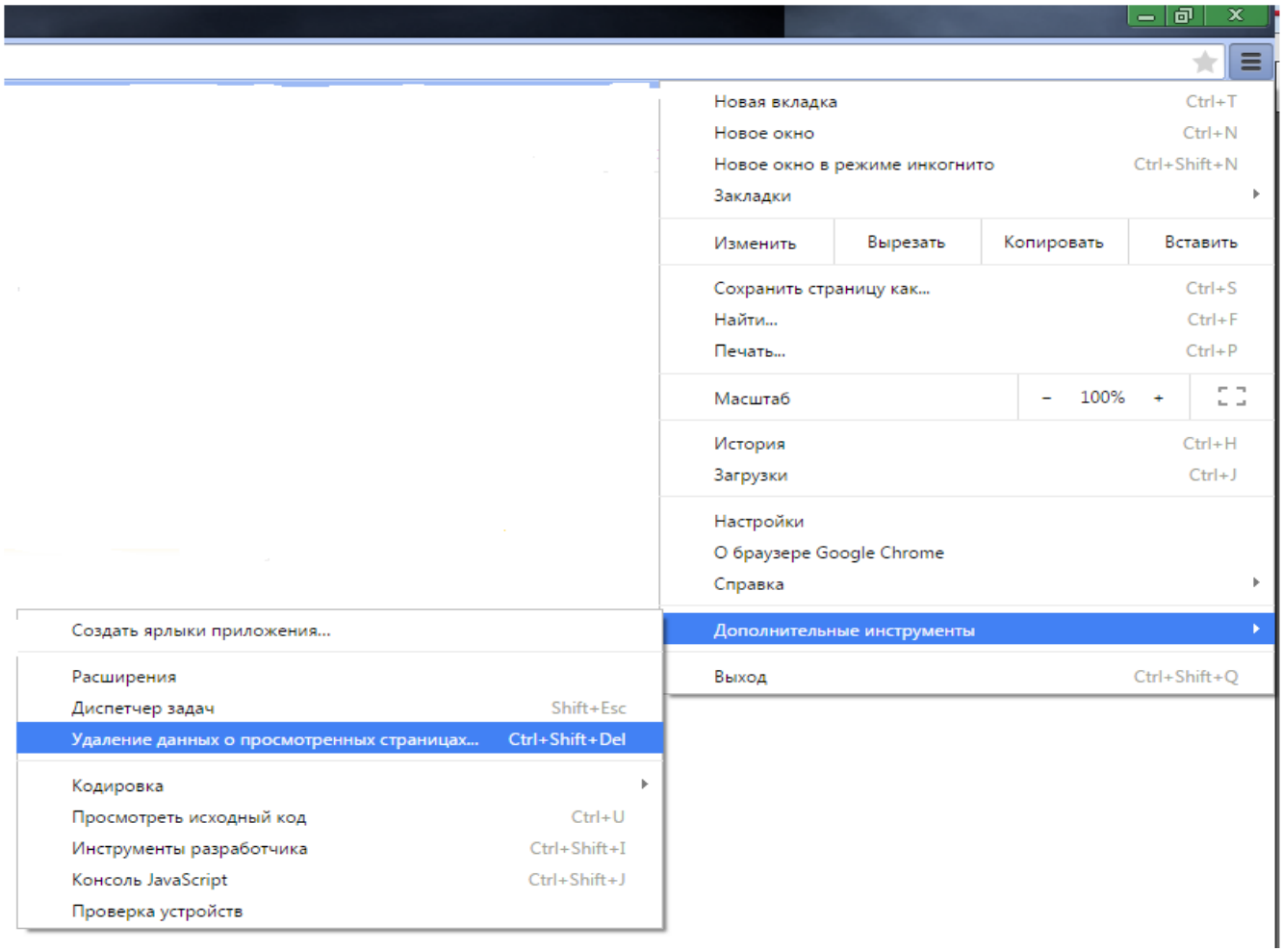


Рисунок 57. Удаление данных

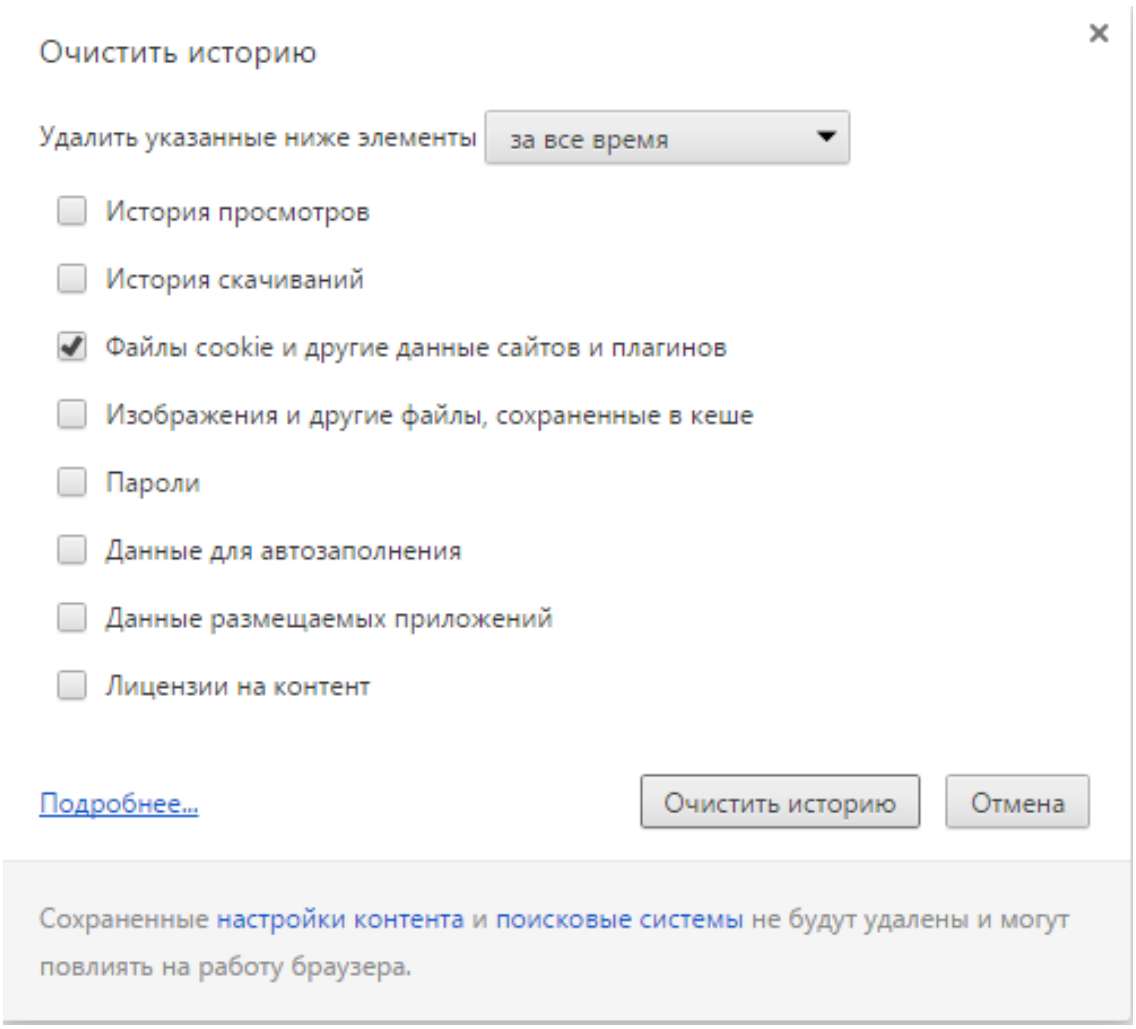


Рисунок 58. Очистка историй

Настройка Internet Explorer IE9 и выше

1) В меню браузера выбрать пункт «**Сервис**». Для отображения меню браузера (если оно скрыто) нажать «Alt».
2) В открывшемся меню нужный пункт — «**Удалить журнал браузера**».
3) В окне «**Удаление истории обзора**» нужно установить флажок «**Файлы cookie**» и убедиться, что все прочие флажки сняты.
4) Для завершения процесса нужно нажать «**Удалить**» (см. Рисунок 59 и Рисунок 60):

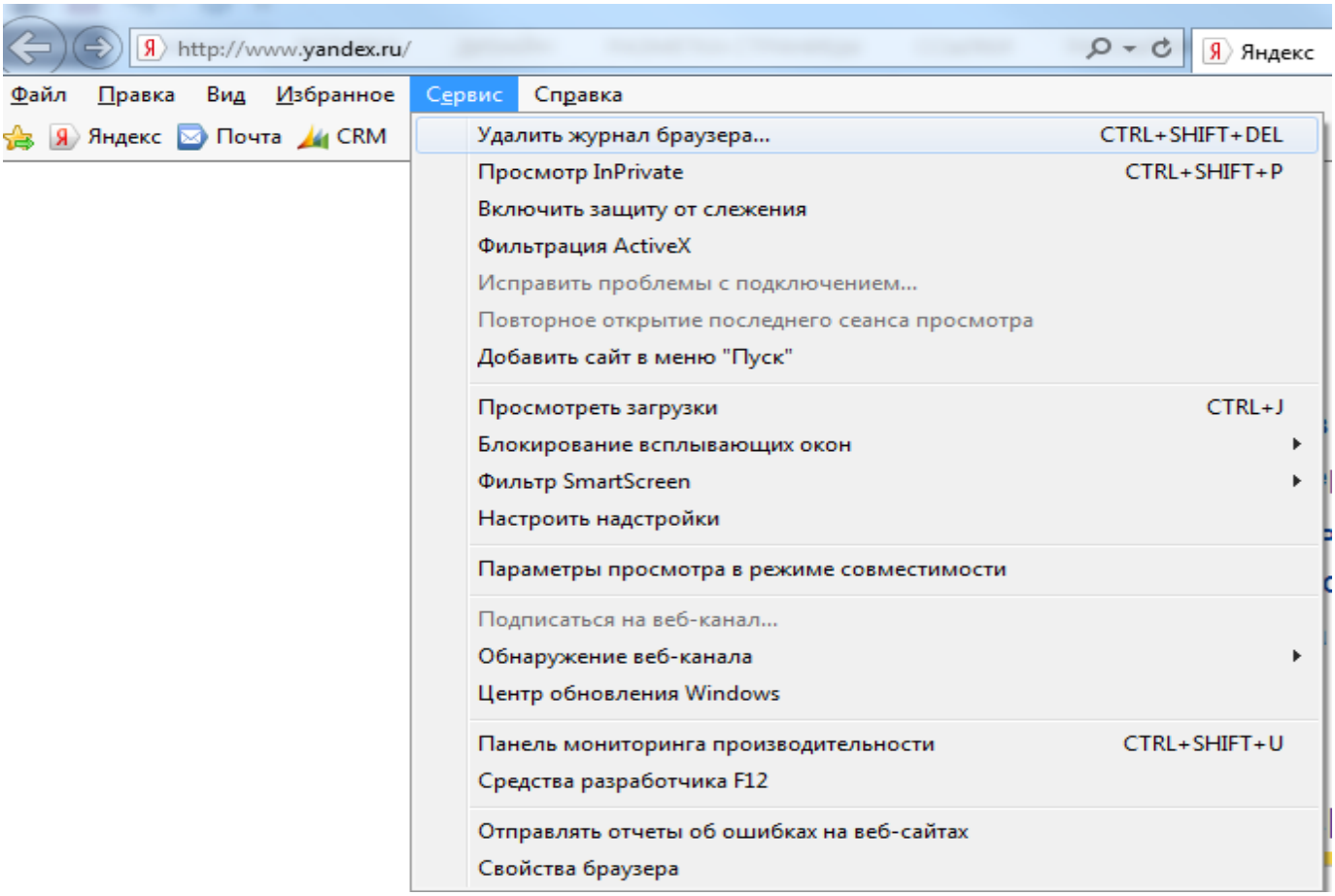


Рисунок 59. Удаление журнала браузера

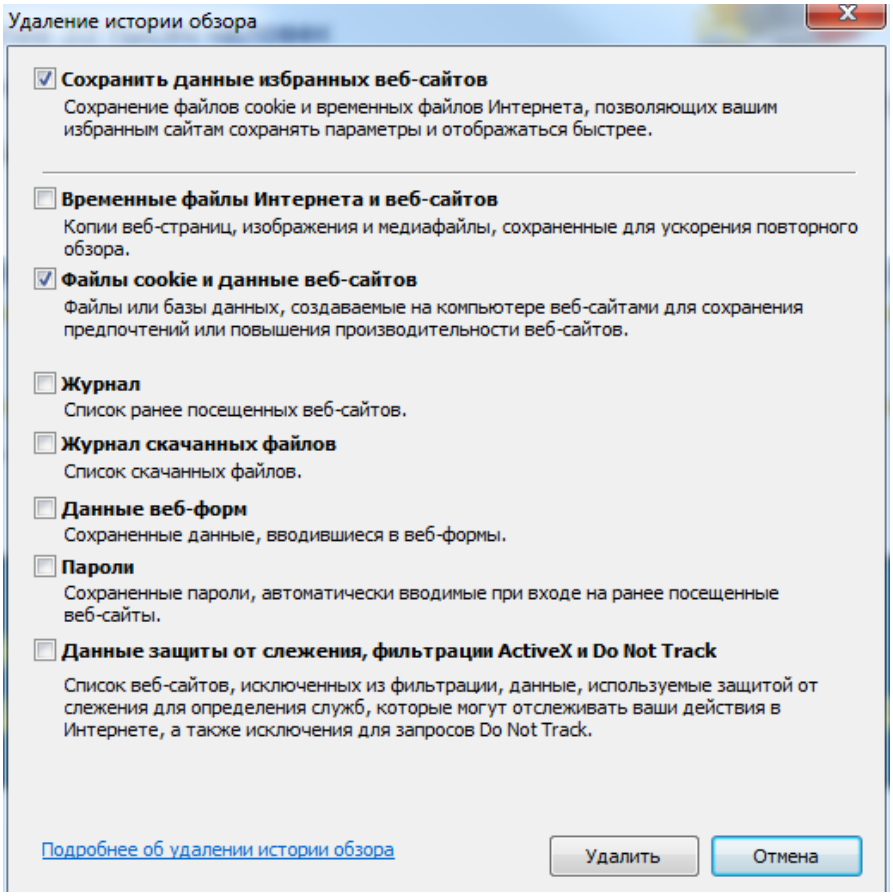


Рисунок 60. Удаление истории обзора

Для корректной работы с СЭП необходимо добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выберите вкладку «**Безопасность»**, в список надежных сайтов добавьте узел https://www.justsign.me/ и сохраните изменения (см. Рисунок 61):

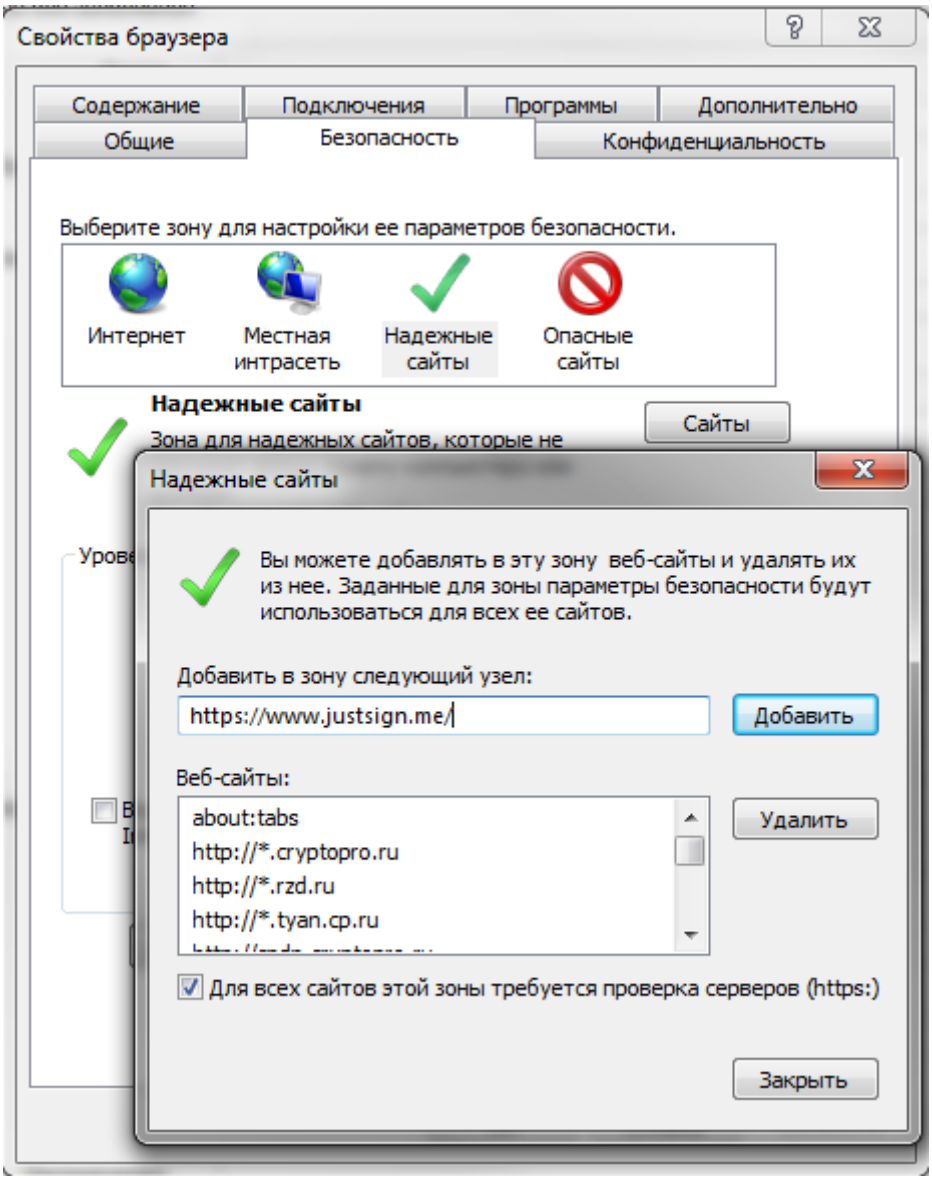


Рисунок 61. Добавление безопасного узла

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**" (см. Рисунок 62).

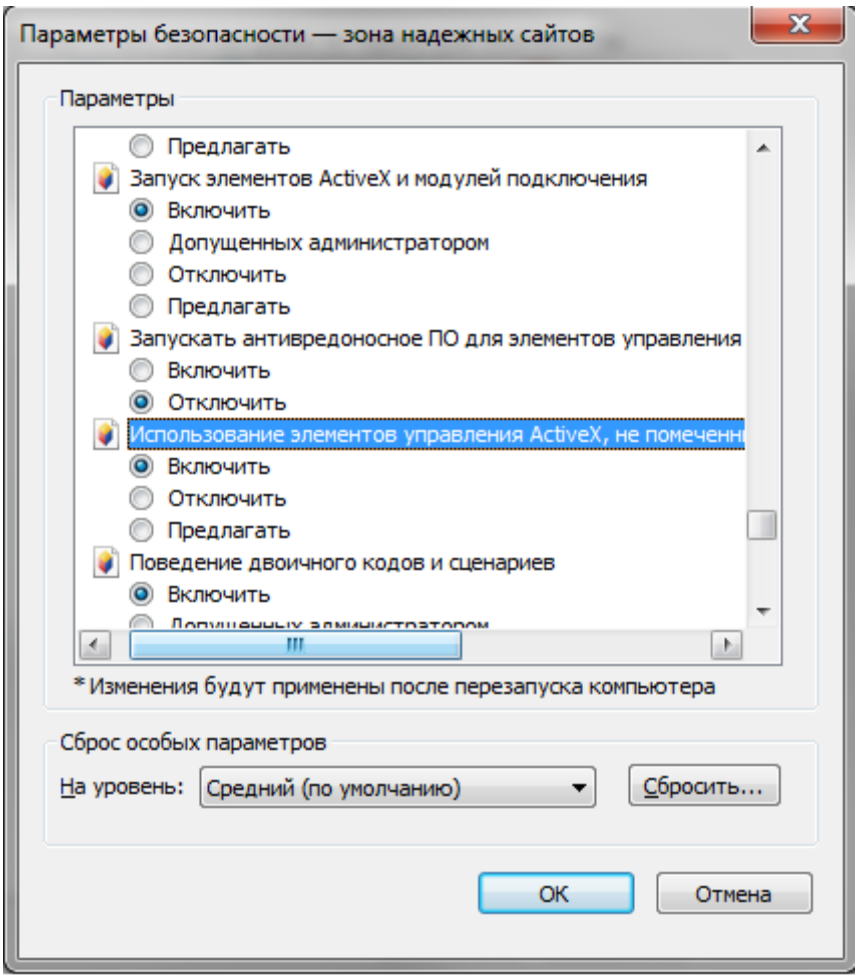


Рисунок 62. Включение элементов ActiveX

Настройка Mozilla Firefox 4.0 и выше

1) В меню браузера нужно выбрать пункт «**Инструменты**» и далее раздел «**Настройки**». Для отображения меню браузера (если оно скрыто) нажать «Alt».
2) В «**Настройках**» нужно перейти в закладку «**Приватность**».
3) В блоке «**История**» в поле «**Firefox**» нужно выбрать «**Будет запоминать историю**» и нажать ссылку «**Удалить отдельные куки**».
4) В открывшемся окне нужно нажать кнопку «**Удалить все куки**».
5) Окно «**Cookies**» закрывается нажатием «**Закрыть**».
6) Чтобы закрыть «**Настройки**», нужно нажать «ОК». (См. Рисунок 63, Рисунок 64 и Рисунок 65):

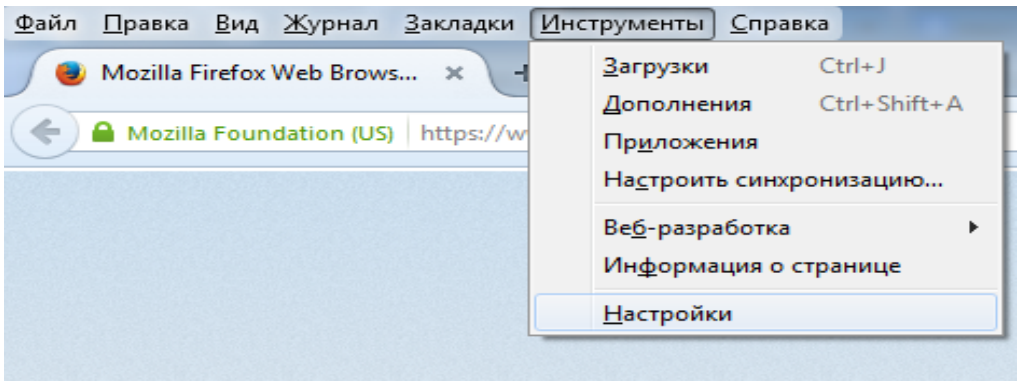


Рисунок 63. Настройки

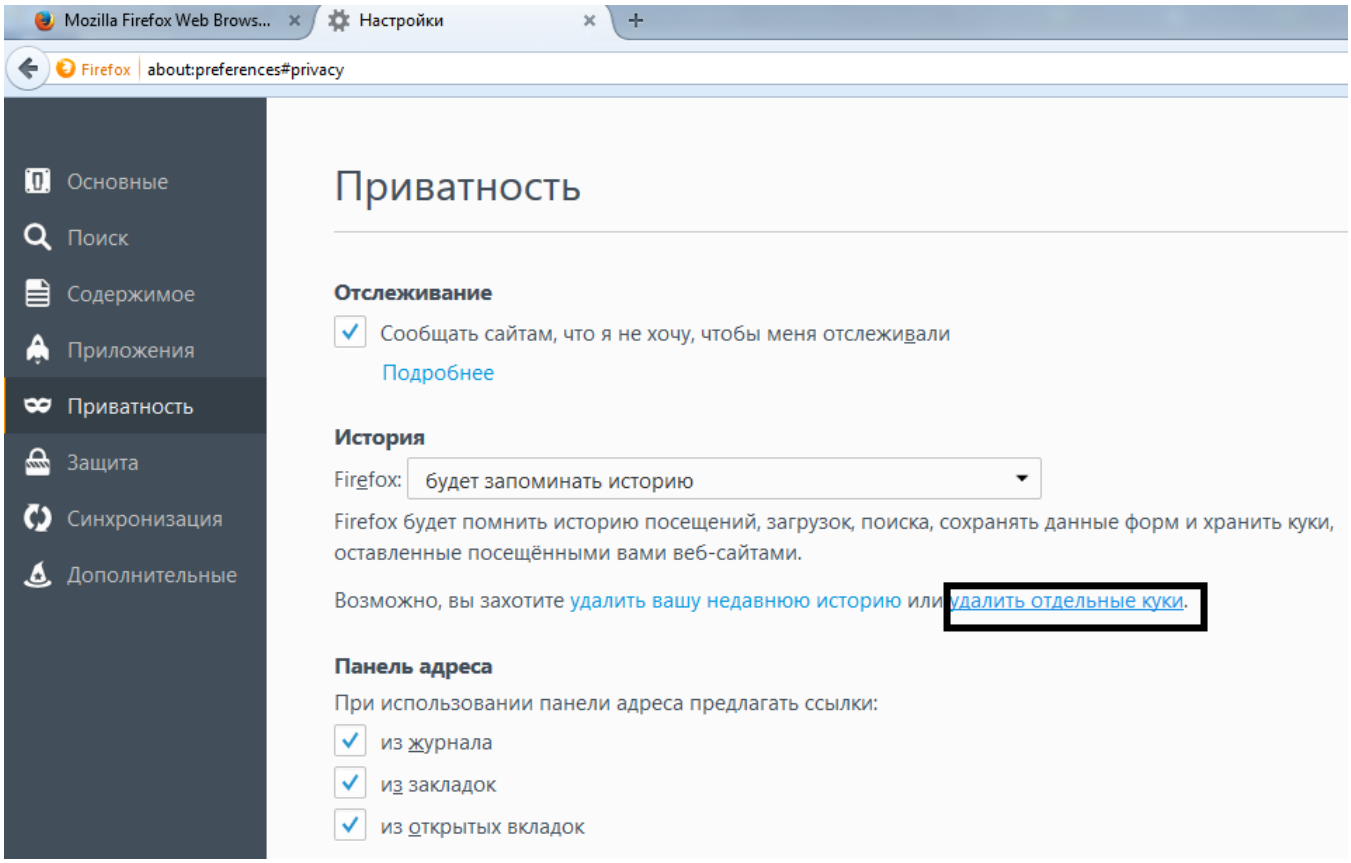


Рисунок 64. Приватность

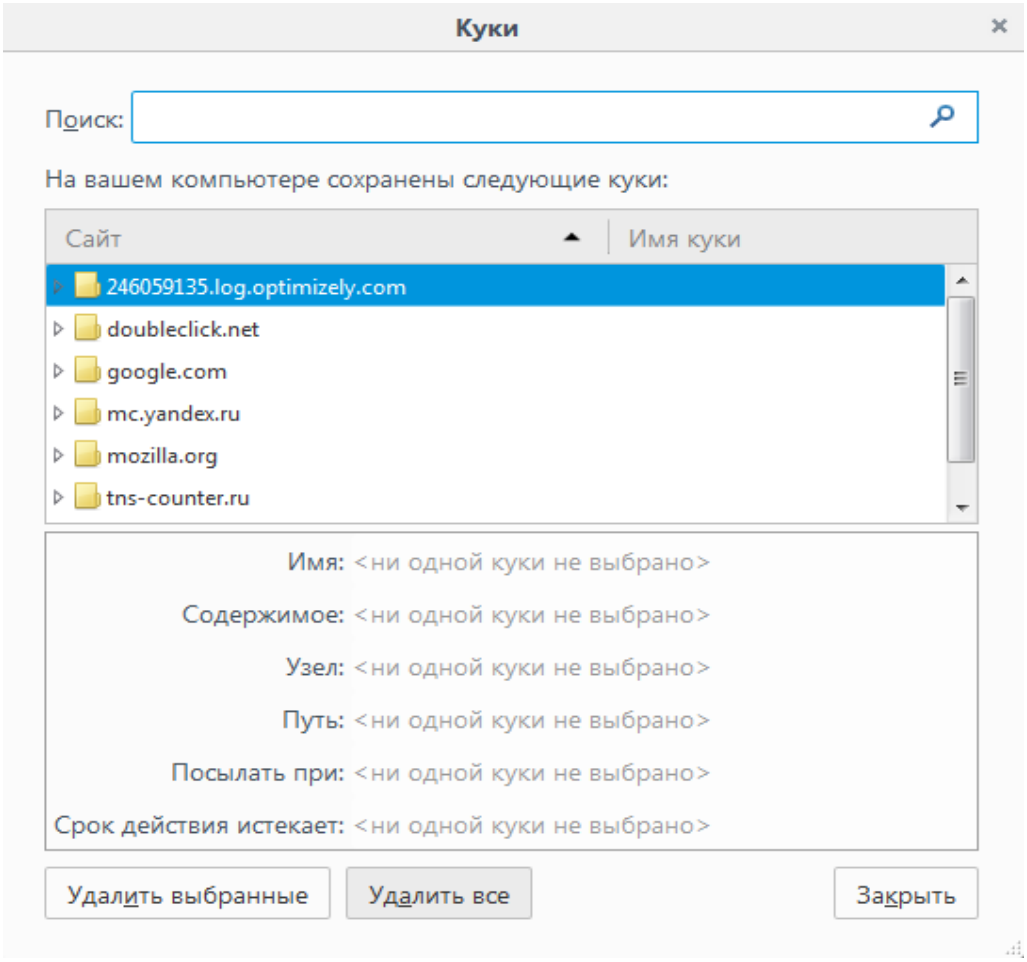


Рисунок 65. Куки

Перечень рисунков

Рисунок 1. Окно аутентификации пользователя 4
Рисунок 2. Ввод одноразового пароля 4
Рисунок 3. Личный кабинет пользователя СЭП 5
Рисунок 4. Личная информация пользователя 6
Рисунок 5. Смена пароля 7
Рисунок 6. Окно редактирования личной информации 8
Рисунок 7. Окно регистрации номера телефона 9
Рисунок 8. Смена телефонного номера 9
Рисунок 9. Завершение редактирования личных данных 10
Рисунок 10. Сертификаты в личном кабинете пользователя СЭП 11
Рисунок 11. Форма запроса на сертификат 12
Рисунок 12. Запрос ПИН-кода для доступа к закрытому ключу 13
Рисунок 13. Ввод одноразового пароля для подтверждения операции 13
Рисунок 14. Информация о статусе имеющихся сертификатов 14
Рисунок 15. Информация о запросе на сертификат 14
Рисунок 16. Печатная форма запроса на сертификат 15
Рисунок 17. Выбор принтера для печати запроса на сертификат 16
Рисунок 18. Перечень полученных сертификатов и их статус 17
Рисунок 19. Информация о сертификате и меню управления сертификатом 18
Рисунок 20. Печатная форма копии сертификата 19
Рисунок 21. Выгрузка сертификата 20
Рисунок 22. Выбор папки для сохранения сертификата 21
Рисунок 23. Формирование запроса на обновление сертификата 22
Рисунок 24. Подтверждение операции одноразовым паролем 22
Рисунок 25. Печать копии сертификата в файл формата PDF 23
Рисунок 26. Выбор документа для создания электронной подписи 24
Рисунок 27. Выбор файла электронного документа для загрузки 25
Рисунок 28. Просмотр содержания электронного документа 26
Рисунок 29. Выбор формата и параметров электронной подписи 27
Рисунок 30. Выбор параметров электронной подписи CAdES 28
Рисунок 31. Выбор сертификата 29
Рисунок 32. Подготовка документа к подписанию 30
Рисунок 33. Ввод ПИН-кода к закрытому ключу электронной подписи 30
Рисунок 34. Ввод одноразового пароля для подтверждения операции 31
Рисунок 35. Сохранение подписанного электронного документа 32
Рисунок 36. Выбор папки и названия файла для сохранения подписанного электронного документа 33
Рисунок 37. Окно проверка подписи 34
Рисунок 38. Выбор файла для проверки присоединенной электронной подписи (в составе электронного документа) 35
Рисунок 39. Параметр присоединённой подписи 36
Рисунок 40. Результат проверки электронной подписи 36
Рисунок 41. Выбор файла первоначального документа для проверки отсоединенной электронной подписи 37
Рисунок 42. Проверка сертификата 38
Рисунок 43. Результат проверки сертификата 38
Рисунок 44. Шифрование документа 39
Рисунок 45. Выбор сертификата пользователя 40
Рисунок 46. Выбор документа для шифрования 41
Рисунок 47. Завершение операции шифрования документа 42
Рисунок 48. Сохранение зашифрованного документа 43

Рисунок 49. Расшифровывание документа 44
Рисунок 50. Выбор документа для расшифровывания 44
Рисунок 51. Вывод информации об используемом сертификате 45
Рисунок 52. Отрицательный результат проверки сертификата 45
Рисунок 53. Окно для ввода ПИН-кода доступа к закрытому ключу 46
Рисунок 54. Ввод одноразового пароля для подтверждения операции 46
Рисунок 55. Сохранение расшифрованного документа 47
Рисунок 56. Выбор папки для сохранения расшифрованного документа 48
Рисунок 57. Удаление данных 49
Рисунок 58. Очистка историй 50
Рисунок 59. Удаление журнала браузера 51
Рисунок 60. Удаление истории обзора 51
Рисунок 61. Добавление безопасного узла 52
Рисунок 62. Включение элементов ActiveX 53
Рисунок 63. Настройки 54
Рисунок 64. Приватность 54
Рисунок 65. Куки 55