

ПО «КриптоПро **DSS Lite**»

ТЕСТОВЫЙ СЕРВИС ЭЛЕКТРОННОЙ ПОДПИСИ

Инструкция Пользователя DSS Lite

ООО «КРИПТО-ПРО»

Аннотация

Настоящая инструкция предназначена для Пользователей тестового сервиса электронной подписи ООО «КРИПТО-ПРО» на базе ПО «КриптоПро DSS Lite» (далее – DSS Lite), обслуживаемых Оператором DSS Lite, и определяет порядок использования Веб-интерфейса DSS Lite для выполнения операций по созданию запросов на управление сертификатами ключей проверки электронной подписи, созданию и проверке электронной подписи, шифрованию и расшифрованию электронных документов.

Информация о Сервисе электронной подписи и разработчике ПО «КриптоПро DSS Lite»:

ООО «КРИПТО-ПРО»

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

Телефон: (495) 995 4820

<http://www.CryptoPro.ru>

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

E-mail: info@CryptoPro.ru

Содержание

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.....	22
5. СОЗДАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ ДОКУМЕНТА	23
6. ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ И СЕРТИФИКАТА.....	31
6.1. ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ С ИСПОЛЬЗОВАНИЕМ «СЛУЖБЫ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ» В СОСТАВЕ СЭП.	31
6.2. ПРОВЕРКА СЕРТИФИКАТА, ПОЛУЧЕННОГО ОТ ДРУГОГО ПОЛЬЗОВАТЕЛЯ	37
7. ШИФРОВАНИЕ ФАЙЛОВ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ	38
8. РАСШИФРОВЫВАНИЕ ФАЙЛОВ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ	43
ПРИЛОЖЕНИЕ 1. НАСТРОЙКА ИНТЕРНЕТ-БРАУЗЕРА.....	48
Настройка Google Chrome.....	48
Настройка Internet Explorer IE9 и выше.....	49
Настройка Mozilla Firefox 4.0 и выше.....	52
ПЕРЕЧЕНЬ РИСУНКОВ.....	55

1. Общие положения.

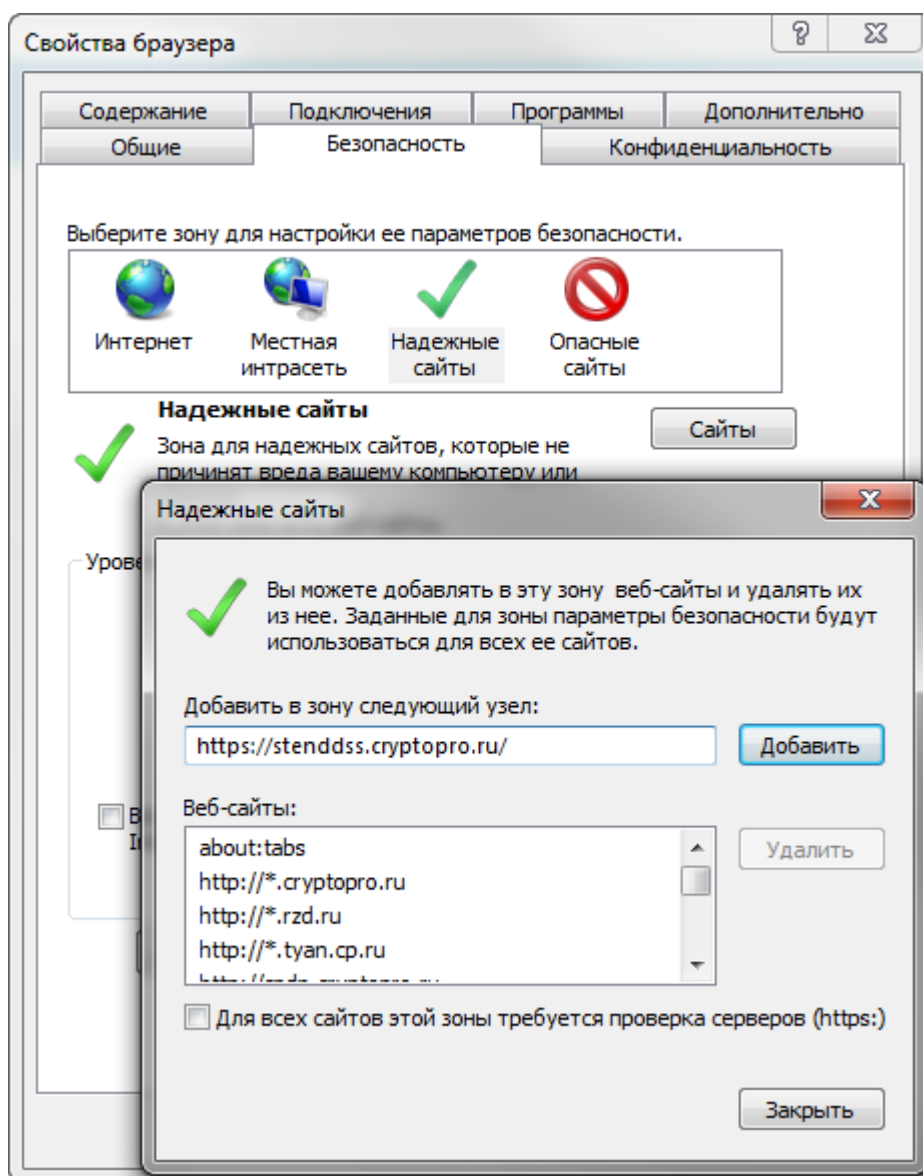
Тестовый сервис электронной подписи на базе ПО «КриптоПро DSS Lite» (далее – DSS Lite) предназначен для демонстрации операций создания и хранения ключей электронной подписи, формирования запросов на создание и управление сертификатами ключей проверки электронной подписи для Тестового удостоверяющего центра КриптоПро, выполнение операций по созданию и проверке электронной подписи различного формата, шифрования и расшифрования электронных документов.

Доступ к DSS Lite получают все авторизованные Пользователи, зарегистрированные Оператором DSS Lite.

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

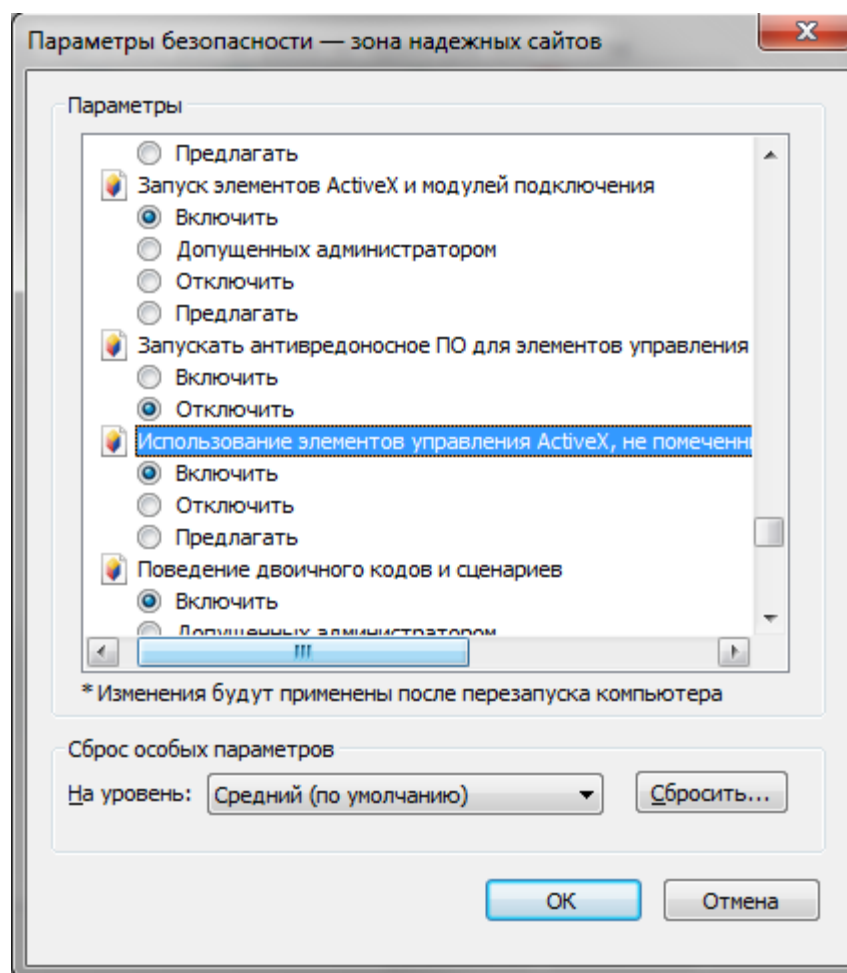
На рабочем месте Пользователя под управлением MS Windows 7 или выше должен быть установлен [СКЗИ «КриптоПро CSP» версии 4.0](#) или выше и [КриптоПро ЭЦП Browser plug-in версии 2.0](#).

Для корректной работы с DSS Lite необходимо добавить адрес в доверенные сайты в настройках браузера. Для этого в свойствах браузера выберите вкладку Безопасность, в список надежных сайтов добавьте узел <https://stenddss.cryptopro.ru/> и сохраните изменения свойств.



В разделе "Элементы ActiveX и модуле подключения" проверить состояние настройки "Использование элементов управления ActiveX, не помеченных как безопасные для использования" - должно быть "Включить".

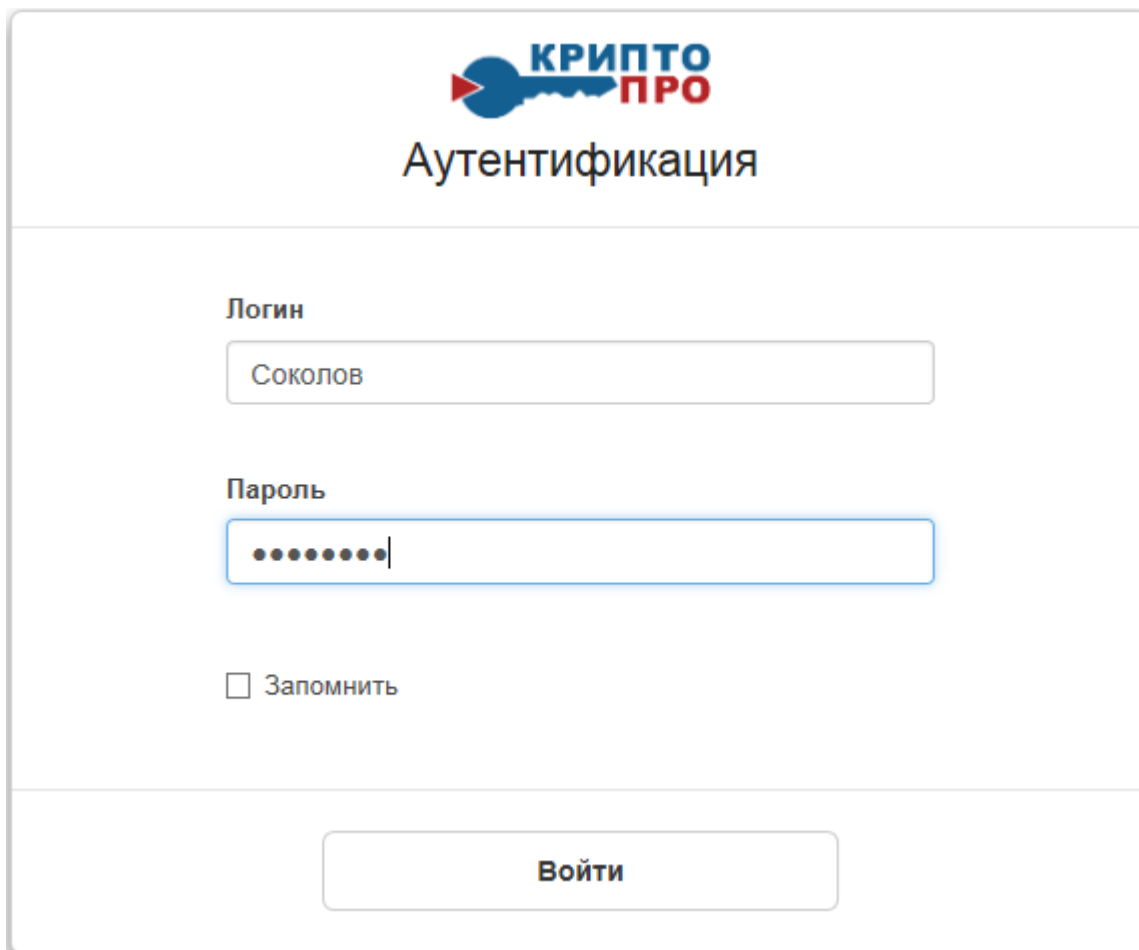
Для этого нужно зайти в Internet Explorer меню Сервис - Свойства обозревателя - Безопасность - для зоны "Надежные узлы" нажать кнопку "Другой"



1. 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 <https://stenddss.cryptopro.ru/OperLite/>, 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 адрес подключения к СЭП <https://stenddss.cryptopro.ru/OperLite/>, в открывшемся окне аутентификации ввести полученный от Оператора логин и пароль, нажать кнопку «**Войти**» (см. Рисунок 1):

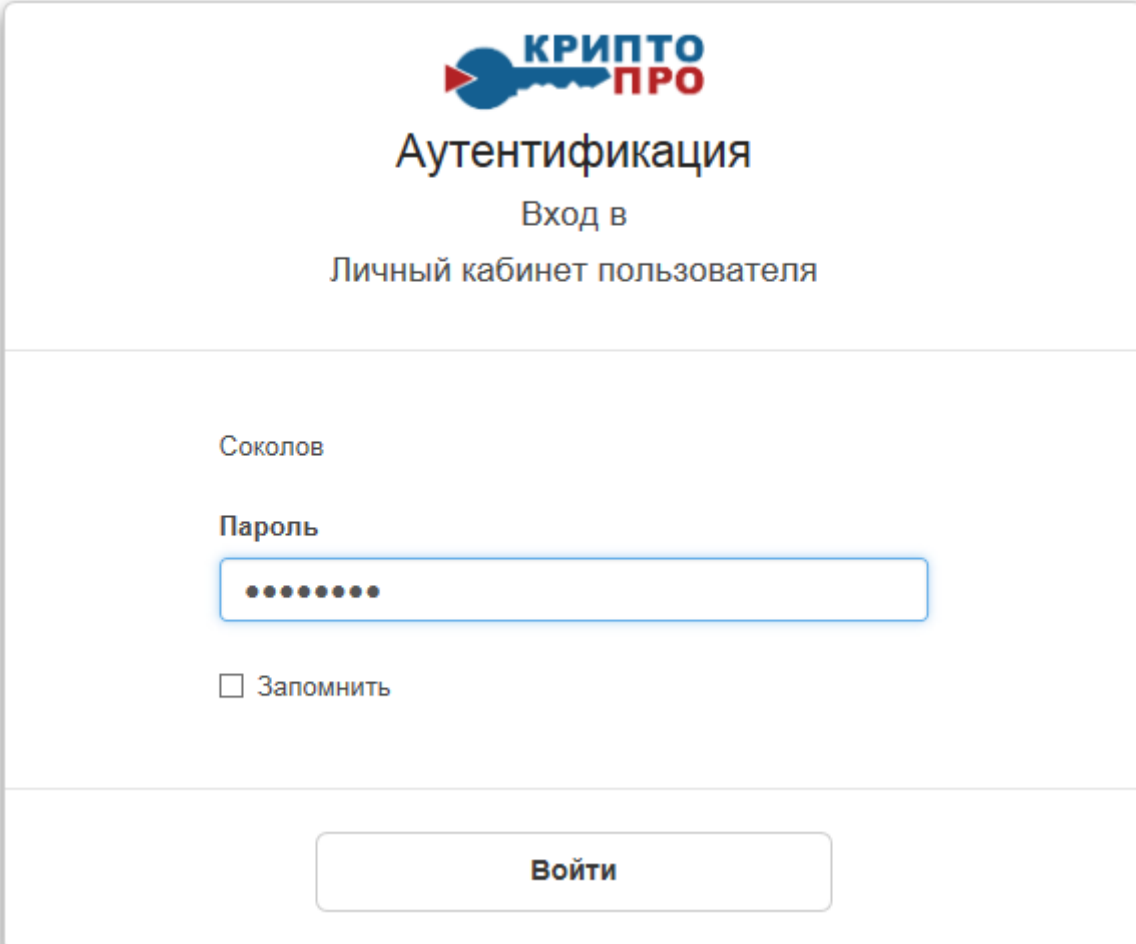


The screenshot shows a web-based authentication interface. At the top, there is a logo consisting of a blue key icon and the text 'КРИПТО ПРО' in blue and red. Below the logo, the word 'Аутентификация' (Authentication) is displayed in a large, black, sans-serif font. The main area contains two input fields: the first is labeled 'Логин' (Login) and contains the text 'Соколов'; the second is labeled 'Пароль' (Password) and contains ten dots, indicating a masked password. Below these fields is a checkbox labeled 'Запомнить' (Remember). At the bottom of the form is a large button labeled 'Войти' (Login).

Рисунок 1. Окно аутентификации пользователя

4. 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.

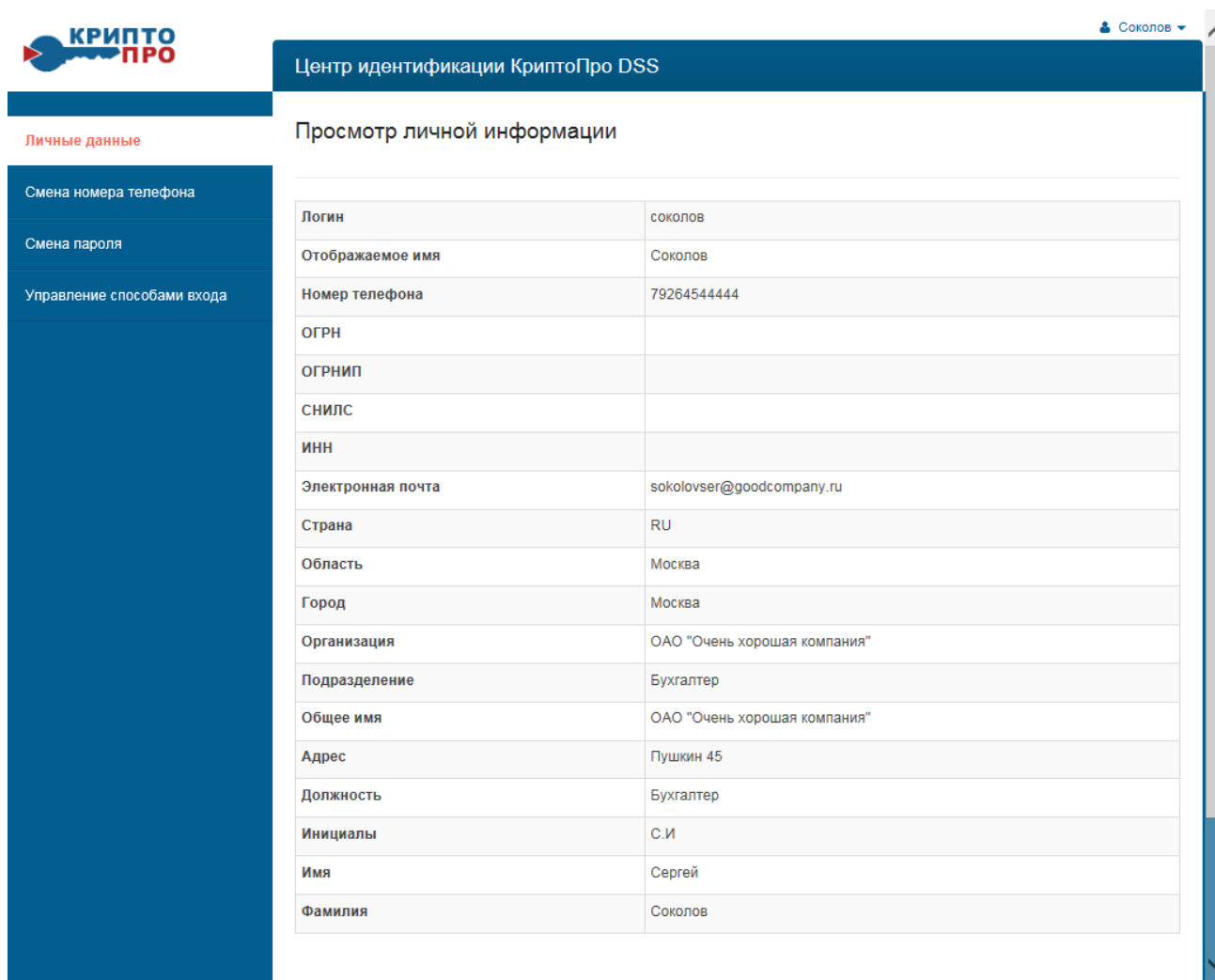
5. Для того, чтобы сменить временный пароль, необходимо зайти в личный кабинет Пользователя по адресу <https://stenddss.cryptopro.ru/OperLiteidp/Users/>, ввести текущий логин и пароль (см. Рисунок 2):



The screenshot shows a login window titled 'Аутентификация' (Authentication) with the subtitle 'Вход в Личный кабинет пользователя' (Login to the user's personal cabinet). The window features the 'КРИПТО ПРО' logo at the top. Below the title, there are input fields for the username 'Соколов' and the password 'Пароль'. The password field is currently filled with ten dots. A checkbox labeled 'Запомнить' (Remember) is located below the password field. At the bottom of the window is a large button labeled 'Войти' (Login).

Рисунок 2. Окна аутентификации Пользователя в личный кабинет

6. Откроется окно с регистрационной информацией Пользователя (см. Рисунок 3):



КриптоПРО

Соколов

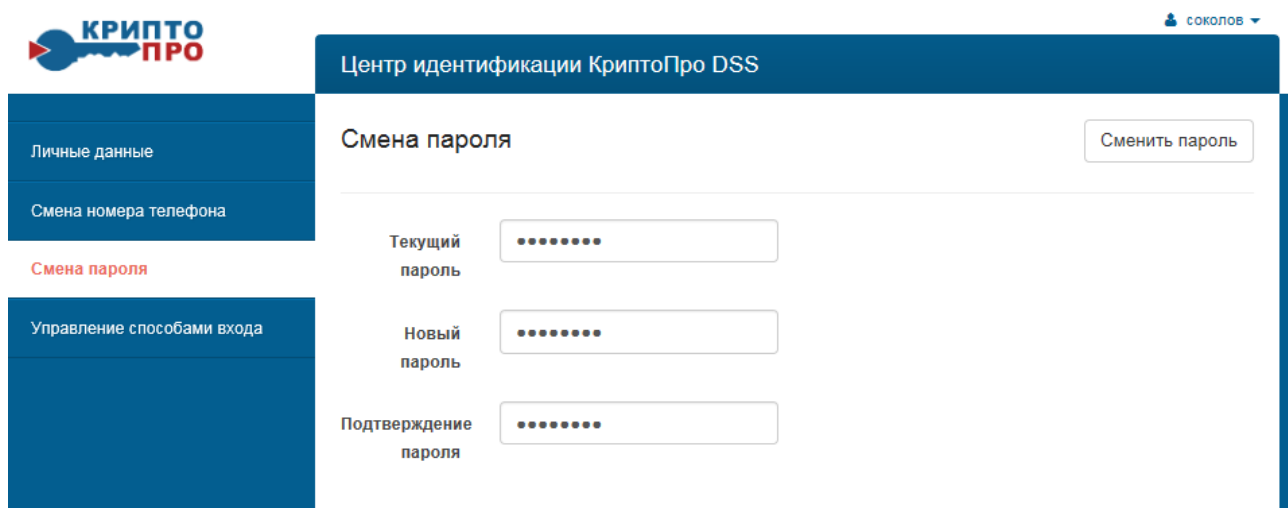
Центр идентификации КриптоПро DSS

Просмотр личной информации

Логин	соколов
Отображаемое имя	Соколов
Номер телефона	79264544444
ОГРН	
ОГРНИП	
СНИЛС	
ИНН	
Электронная почта	sokolovser@goodcompany.ru
Страна	RU
Область	Москва
Город	Москва
Организация	ОАО "Очень хорошая компания"
Подразделение	Бухгалтер
Общее имя	ОАО "Очень хорошая компания"
Адрес	Пушкин 45
Должность	Бухгалтер
Инициалы	С.И
Имя	Сергей
Фамилия	Соколов

Рисунок 3. Личная информация пользователя

7. 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 4](#)):



КриптоПРО

Соколов

Центр идентификации КриптоПро DSS

Смена пароля

Сменить пароль

Текущий пароль

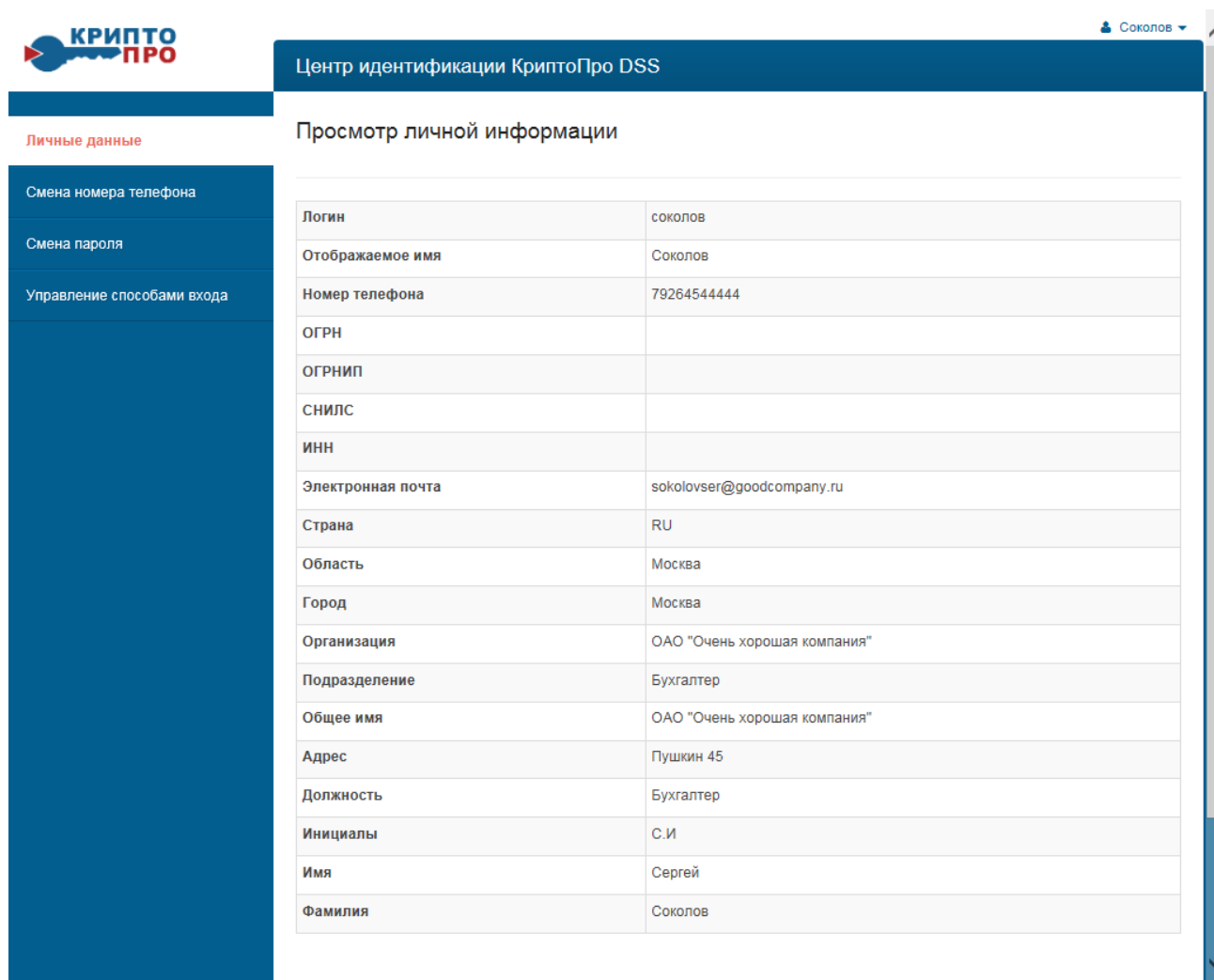
Новый пароль

Подтверждение пароля

Рисунок 4. Смена пароля

Новый пароль должен состоять не менее чем из 5 цифр и сохраняться втайне от прочих лиц.

8. Для просмотра личной информации нажать на ссылку «**Личные данные**» (см. Рисунок 5). Для того, что бы сменить Личные данные пользователя, необходимо обратиться к Оператору СЭП.



КРИПТОПРО

Соколов

Центр идентификации КриптоПро DSS

Личные данные

Просмотр личной информации

Логин	соколов
Отображаемое имя	Соколов
Номер телефона	79264544444
ОГРН	
ОГРНИП	
СНИЛС	
ИНН	
Электронная почта	sokolovser@goodcompany.ru
Страна	RU
Область	Москва
Город	Москва
Организация	ОАО "Очень хорошая компания"
Подразделение	Бухгалтер
Общее имя	ОАО "Очень хорошая компания"
Адрес	Пушкин 45
Должность	Бухгалтер
Инициалы	С.И
Имя	Сергей
Фамилия	Соколов

Рисунок 5. Окно просмотр личной информации

9. Для того, чтобы выйти из личного кабинета, в правом верхнем углу на имени пользователя открыть выпадающее меню и нажать «**Выход**» и закрыть Интернет-Браузер (см. Рисунок 6):

Личные данные

Просмотр личной информации

Смена номера телефона

Смена пароля

Логин	соколов сергей
Отображаемое имя	
Номер телефона	75557744455
Общее имя	ОАО "Очень хорошая компания"
Электронная почта	sokolovser@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	Соколов

3. Получение первого или внеплановая смена сертификата



 СОКОЛОВ ▾

Сервер электронной подписи КриптоПро DSS

Сертификаты

[+ Создать запрос на сертификат](#)

 Установить сертификат

Сертификаты отсутствуют.

Подписать

Зашифровать

Расшифровать

Проверить подпись

[Проверить сертификат](#)

Сертификаты

10

2. Нажать **«Создать запрос на сертификат»**, Откроется окно для подтверждения операции с цифровым сертификатом от имени пользователя, нажать **«ДА»** (см. Рисунок 8):

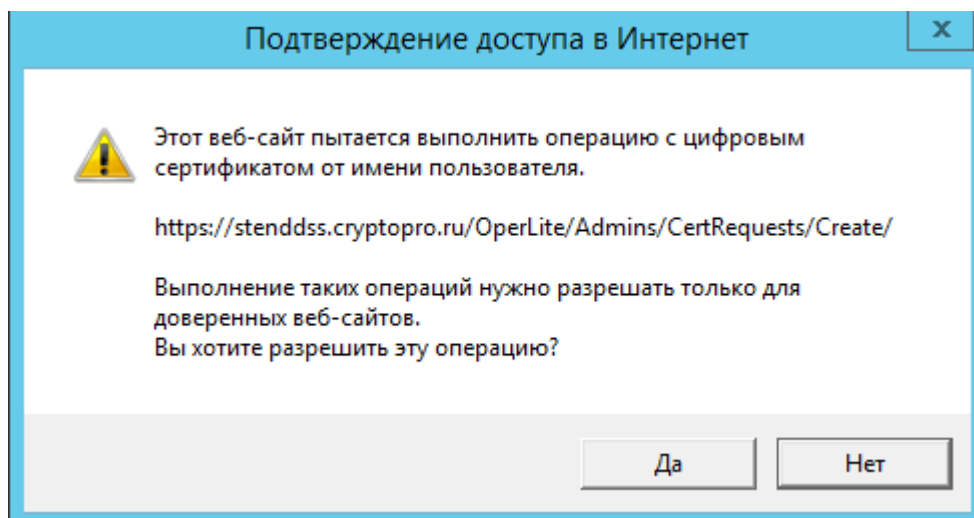


Рисунок 8. Подтверждения операции с цифровым сертификатом

3. Заполнить форму запроса в соответствии по данной заявкой на выдачу сертификата согласно Регламенту деятельности Удостоверяющего центра (УЦ), выбрать Тестовый УЦ КриптоПро, выбрать шаблон сертификата «Сертификат пользователя УЦ», нажать **«Создать запрос»** (см. Рисунок 9):

Подписать

Зашифровать

Расшифровать

Проверить подпись

Проверить сертификат

Сертификаты

Создание запроса на сертификат

Выберите УЦ, к которому будет направлен запрос на сертификат

КриптоПро УЦ 1.5 R2
▼

Заполните необходимые компоненты имени

Фамилия (SN)

Имя (G)

Должность/звание (T)

Неструктурированное имя
(1.2.840.113549.1.9.2)

Адрес (2.5.4.9)

Общее имя (CN)*

Подразделение (OU)

Организация (O)

Город (L)

Область (S)

Страна/регион (C)

Электронная почта (E)

ИНН (INN)

ОГРН (ОГРН)

СНИЛС (СНИЛС)

ОГРНИП (ОГРНИП)

Выберите шаблон сертификата

Сертификат пользователя DSS
▼

Создать запрос

Рисунок 9. Форма запроса на сертификат

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

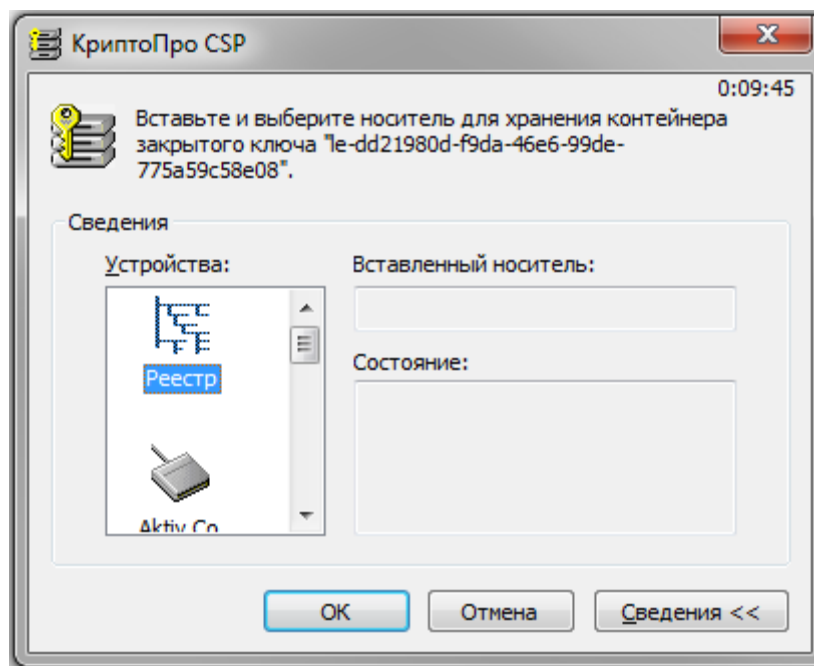


Рисунок 10. Выбор ключевого носителя

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

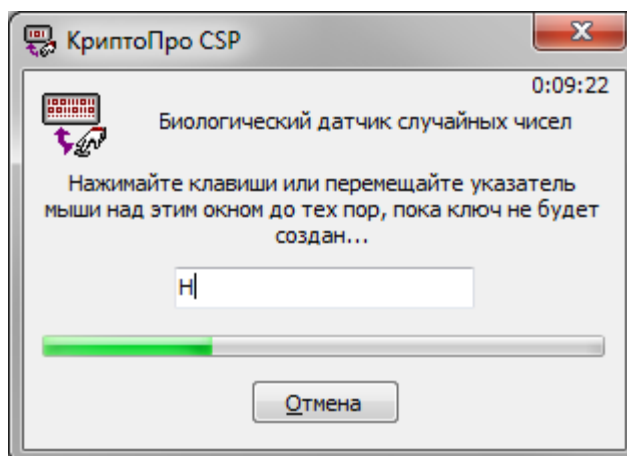


Рисунок 11. Биологический датчик случайных чисел

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

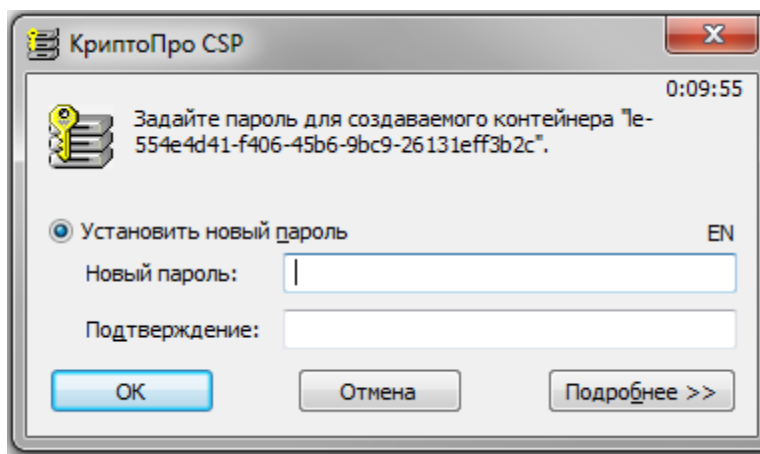


Рисунок 12. Ввод пароля на доступ к закрытому ключу

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.

7. Откроется окно с информацией о статусе сертификата (см. [Рисунок 13](#)):

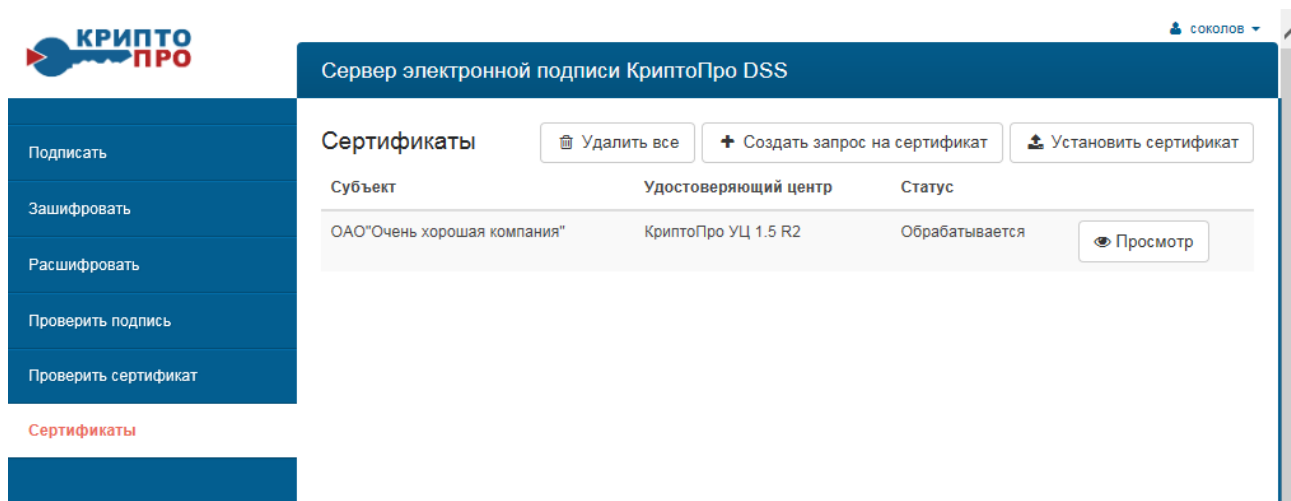


Рисунок 13. Информация о статусе имеющихся сертификатов

8. Справа нажать кнопку **«Просмотр»**, отобразится окно с запросом на сертификат и статусом **«Обрабатывается»** (см. [Рисунок 14](#)):

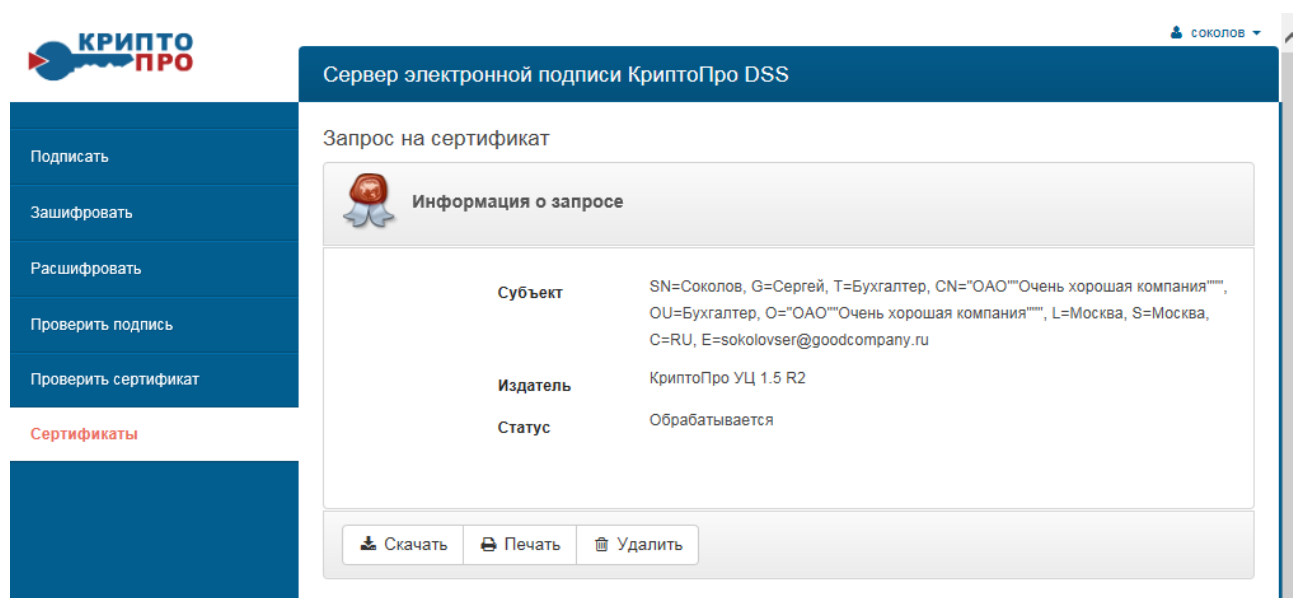


Рисунок 14. Информация о запросе на сертификат

9. Нажать кнопку «Печать», откроется форма запроса на сертификат для печати (см. Рисунок 15):

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, T = Бухгалтер, STREET = Пушкин 45, CN = ОАО"Очень хорошая компания", OU = Бухгалтер, O = ОАО"Очень хорошая компания", L = Москва, S = Москва, C = RU, E = sokolovser@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 5c ba 77 a0 a4 bc 5a 2a 8f 26 67 3b 99 23 d9 a2 d9 90 5b 67 7b 1d 7a af a9 55 fe c7 57 4a 3e be 48 25 a3 f9 65 f2 59 22 4a 8e c8 26 9c 3c ff 9c e1 50 c7 48 5c b5 d2 e1 ba 21 ec 48 32 9a 93 59

Атрибуты запроса на сертификат X.509

Название: Расширения сертификатов

Расширения сертификата X.509

1. Расширение

Название: Улучшенный ключ

Значение: 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), Проверка сервера лицензий (1.3.6.1.4.1.311.10.6.2)

2. Расширение (критическое)

Название: Использование ключа

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

3. Расширение

Название: Идентификатор ключа субъекта

Значение: 72 fb 42 c6 f0 12 2d 90 18 82 7b 49 f8 44 8d ae 0e 0a 8c fa

Название: CSP подачи заявок

Сведения о провайдере

Название провайдера : Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider

Подпись провайдера :

Название: Версия ОС

Значение: 6.3.9600.2

Название: Сведения о клиенте

Значение: 30 3e 02 01 05 0c 08 73 74 65 6e 64 64 73 73 0c 25 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 53 69 67 6e 53 65 72 76 65 72 0c 08 77 33 77 70 2e 65 78 65

Подпись запроса:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2001

Значение: BA 7C 02 41 9A B3 18 43 69 6A F3 96 AF 7D 3E EF BD 0E 77 FA BD E9 FE 80 49 46 13 2A AD A9 C3 91 DE 9C 4D 8A 8E 65 0C F3 3E BD A2 1D E4 FC CF 35 B6 85 9C F8 47 24 71 DC A4 6A C8 30 81 E4 54 16

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, XXXXXXXXXXXXXXXXXXXX
Администратору информационной безопасности.

Рисунок 15. Печатная форма запроса на сертификат

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

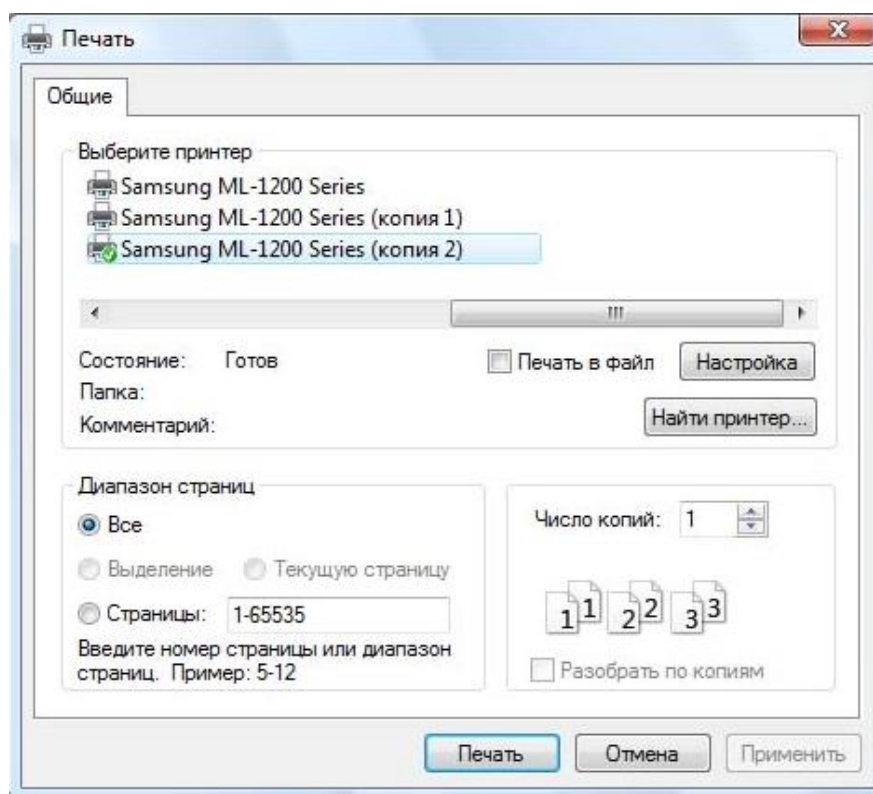


Рисунок 16. Выбор принтера для печати запроса на сертификат

Распечатанный запрос подписать, отсканировать и отправить на адрес электронной почты Оператора СЭП.

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

12. 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 17](#)):

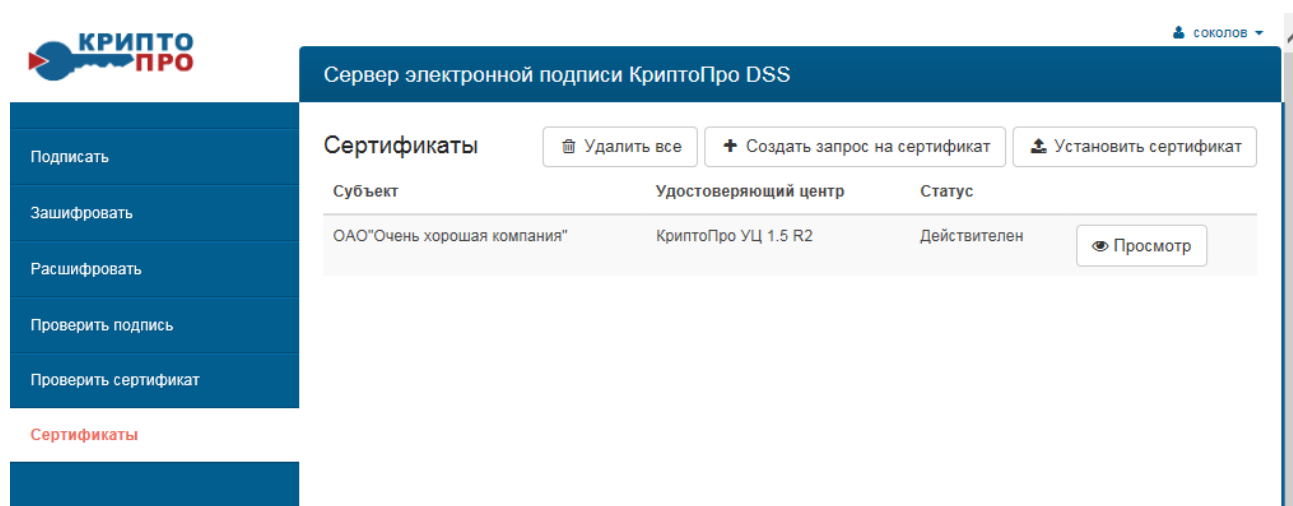


Рисунок 17. Перечень полученных сертификатов и их статус

13. Справа нажать кнопку «**Просмотр**», откроется окно с информацией о сертификате и меню управления сертификатом (см. Рисунок 18):

Информация о сертификате

Субъект	SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, O="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolovser@goodcompany.ru
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 05.10.2015 15:53:00 по 05.01.2017 16:03:00
Отпечаток	E4467FB697AE59F81D4BA080B344AECAB1DCBEBC
Серийный номер	42E818B9000000000004B
Алгоритм	1.2.643.2.2.19 (ГОСТ Р 34.10-2001)
открытого ключа	

Скачать
Печать
Установить в хранилище
Удалить

Отозвать
Приостановить
Возобновить
Обновить

☐ Назначить сертификатом по умолчанию

Запрос на сертификат

Субъект	Издатель	Статус	Действия
SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, O="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolovser@goodcompany.ru	Тест УЦ DSS	Принят	<div>Скачать</div> <div>Печать</div> <div>Удалить</div>

Рисунок 18. Информация о сертификате и меню управления сертификатом

14. Нажать кнопку «**Установить в хранилище**», сертификат установится в хранилище «Личные» текущего пользователя с привязкой к закрытому ключу.

15. Выбрать «**Печать**», откроется печатная форма копии сертификата (см. Рисунок 19):

**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 05.10.2015 15:53:00 по 05.01.2017 16:03:00

Версия: 3 (0x2)**Серийный номер:** 42E818B9000000000048**Издатель сертификата:** CN = Тестовый УЦ для DSS, O = ООО "КРИПТО-ПРО", L = Москва, S = 77 г. Москва, C = RU, STREET = ул. Суворовский вал, д. 18, ИНН = 007712345678, ОГРН = 1007712345678**Срок действия:**

Действителен с: 05.10.2015 15:53:00

Действителен по: 05.01.2017 16:03:00

Владелец сертификата: 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 = sokolovser@goodcompany.ru**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 ea 05 39 b0 e5 00 33 51 71 90 08 76 15 00 5f af d2 93 37 a5 f8 cf 43 ef 73 c2 38 54 c2 19 0e 75 c2 60 67 f0 12 54 6a 60 9e dc 69 0e ef 15 24 b5 9e 45 7d fc 06 67 29 cd fd 9d 52 a6 51 ed cb 68

Расширение сертификата X.509

1. Расширение

Название: Улучшенный ключ

Значение: Неизвестное использование ключа (1.2.643.2.2.34.33), 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)

2. Расширение (критическое)

Название: Использование ключа

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

3. Расширение

Название: Идентификатор ключа субъекта

Значение: d2 fa eb 88 08 0b dd 52 64 11 ca dc 50 e3 e0 9e 74 4e 3a b0

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. Суворовский вал, д. 18", ИНН=007712345678, ОГРН=1007712345678, Серийный номер сертификата=3d 4b 95 91 f0 c1 e1 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 5 октября 2015 г. 15:53:00 по 5 января 2017 г. 15:53:00

8. Расширение

Название: Политики сертификата

Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП KC1, [2]Политика сертификата:Идентификатор политики=Класс средства ЭП KC2

9. Расширение

Название: Средство электронной подписи владельца

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

10. Расширение

Название: Средство 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: DB 22 7F DC 17 A9 F4 9D 51 92 1C 10 20 D1 BD F0 EE FB AA 88 89 27 5E B9 FF 0D 4F D8 8C AA 83 88 FB 07 E8 BE E9 CD E4 76 B0 4F 2B C6 AD 97 70 CA A2 36 DF BF 3F 0D 34 A1 D1 82 00 BE BC A9 27 68

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, XXXXXXXXXXXXXXXXXXXX

Администратору информационной безопасности.

Рисунок 19. Печатная форма запроса на сертификат

2. Выгрузка сертификата

- 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 0) слева нажать «Сертификаты» (см. Рисунок 13), 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 20):

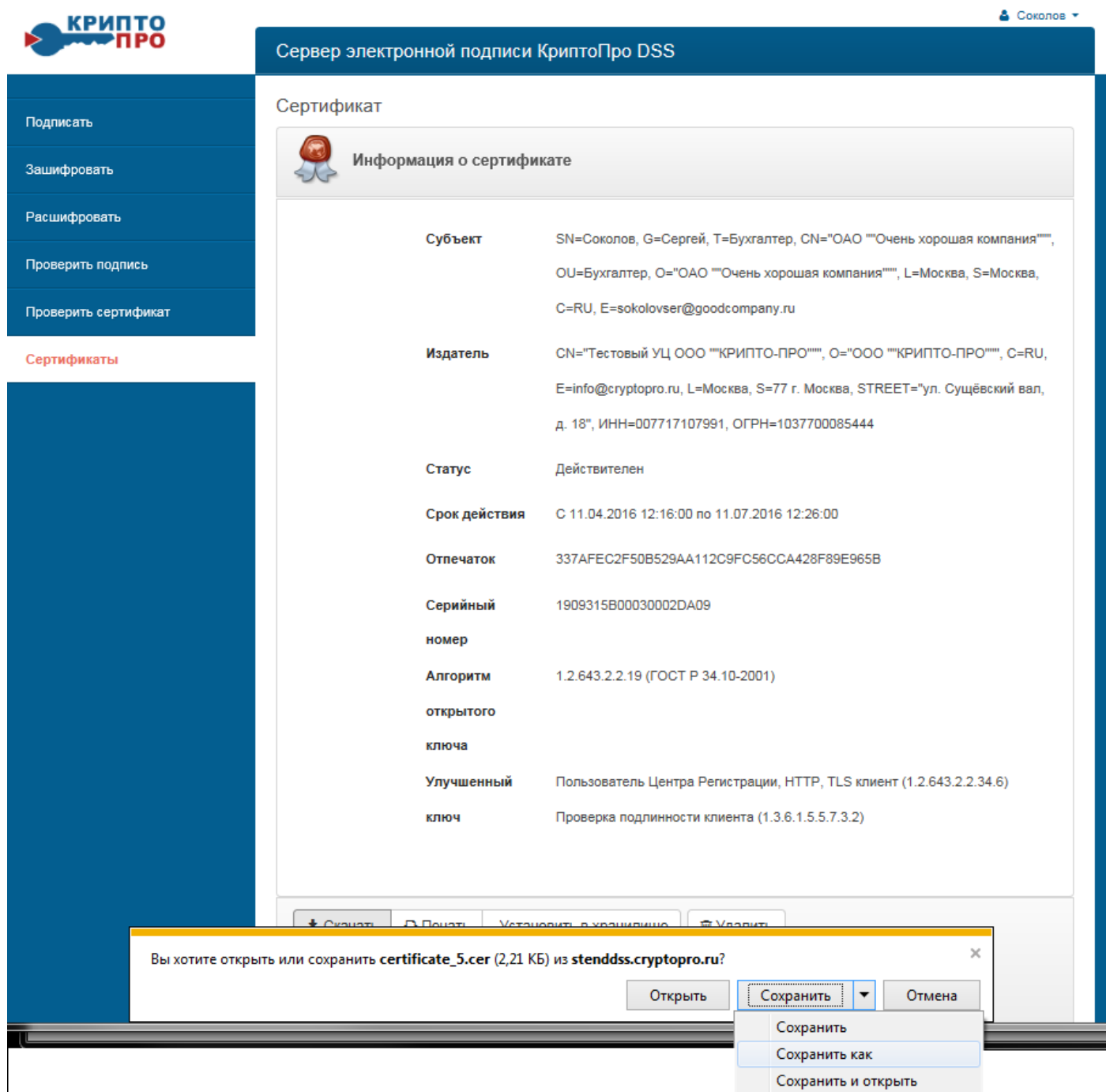


Рисунок 20. Выгрузка сертификата

2. Далее выбрать папку и нажать **«Сохранить»** (см. Рисунок 21):

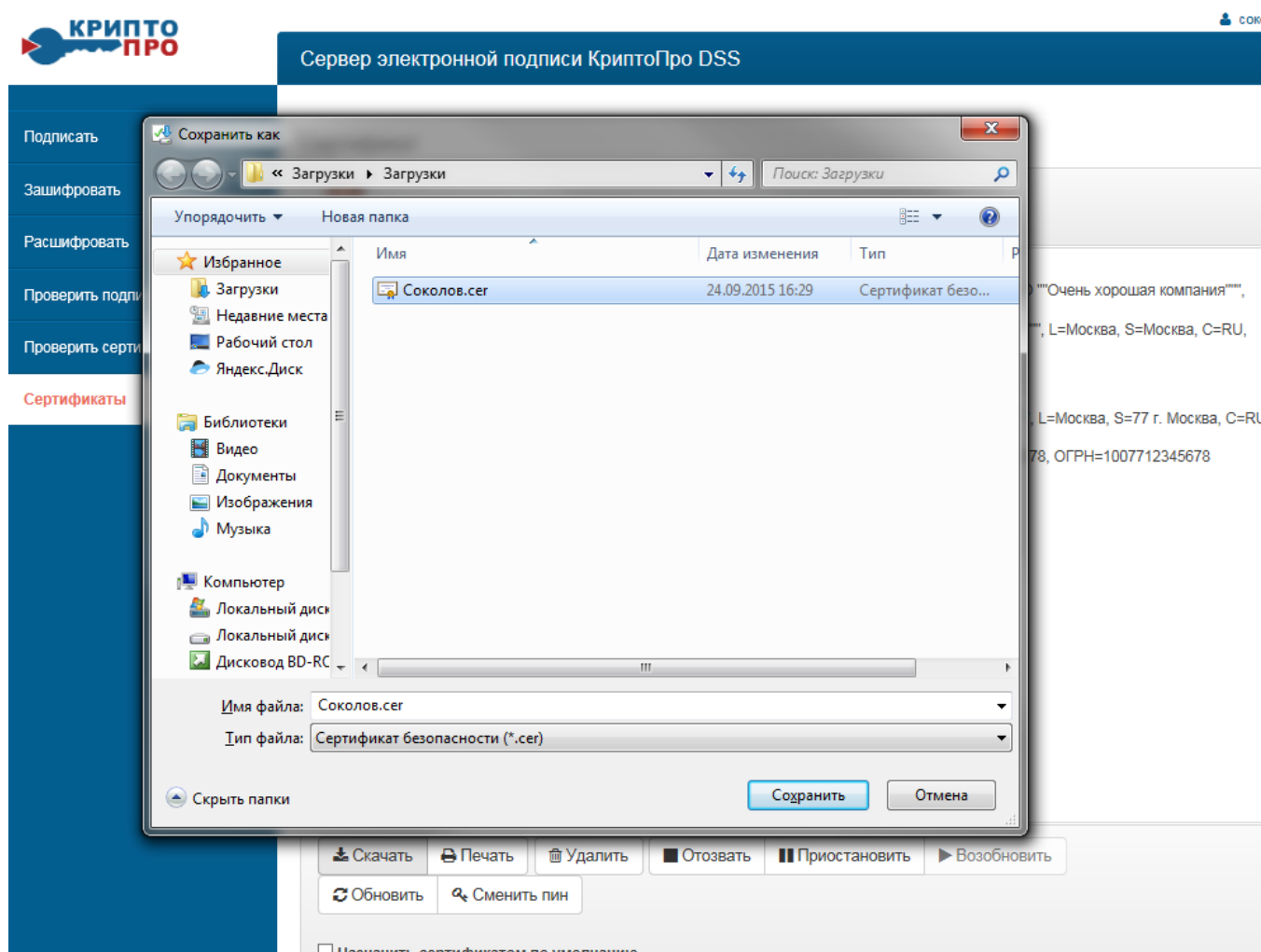


Рисунок 21. Выбор папки для сохранения сертификата

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

3. 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.13 Раздела 3).
3. Нажать «**Обновить**», откроется окно для выбора шаблон сертификата, выбрать шаблон «**Сертификат пользователя DSS**», нажать «**ОК**».
4. Нажать слева на кнопку «**Сертификаты**». Справа нажать кнопку «**Просмотр**», отобразится окно с запросом на сертификат и статусом «Обрабатывается» (см. п.8 Раздел 3)

5. После получения запроса на сертификат выполнить процедуру (в соответствии п.8-15 Раздела 3).

4. 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 22):

The screenshot shows the 'КриптоПро DSS' web application. On the left is a blue sidebar menu with the following items: 'Подписать' (highlighted in red), 'Зашифровать', 'Расшифровать', 'Проверить подпись', 'Проверить сертификат', and 'Сертификаты'. The main content area has a dark blue header 'Сервер электронной подписи КриптоПро DSS' and a user profile 'соколов'. Below the header, the title 'Создание подписи' is displayed. A 'Подписать' button is in the top right. The main form contains several sections: a document selection dropdown currently showing 'Документ' and 'Не задан'; a message 'Документ будет отправлен на сервер.' with a progress bar and an 'Обзор...' button; a 'Формат подписи' dropdown set to 'Простая электронная подпись'; a 'Параметры подписи' dropdown set to 'Подпись данных'; and a 'Сертификат' dropdown showing detailed certificate information: 'SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, О="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolov@goodcompany.ru, ОГРН=1024567890678, СНИЛС=11223344565, ОГРНИП=106784566656787'.

Рисунок 22. Выбор документа для создания электронной подписи

2. Далее – **«Обзор»**, выбрать нужный файл и нажать кнопку **«Открыть»** (см. Рисунок 23):

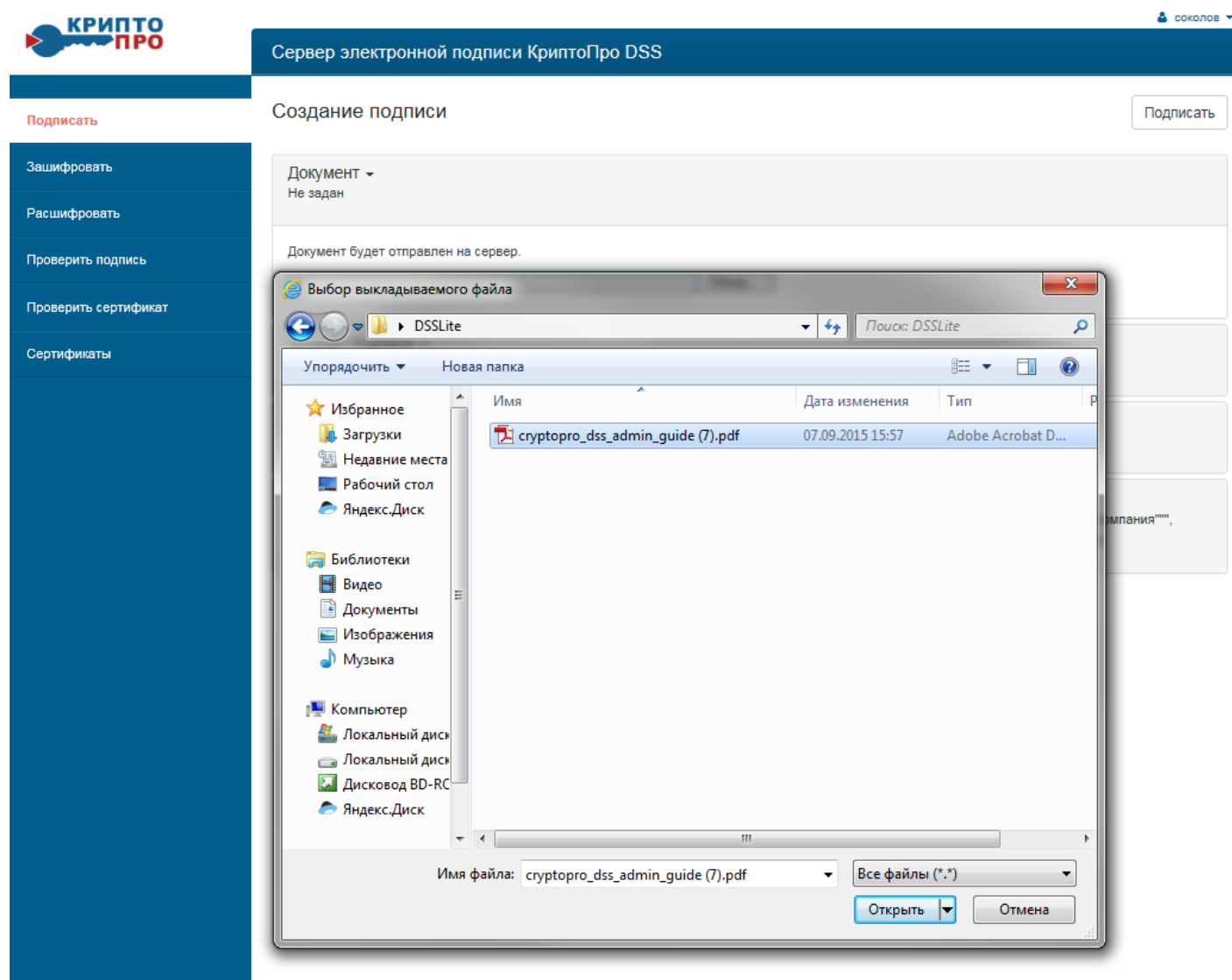


Рисунок 23. Выбор файла электронного документа для загрузки

3. Нажимая кнопку «Вперед» просмотреть отображаемое содержание подписываемого электронного документа (см. Рисунок 24):

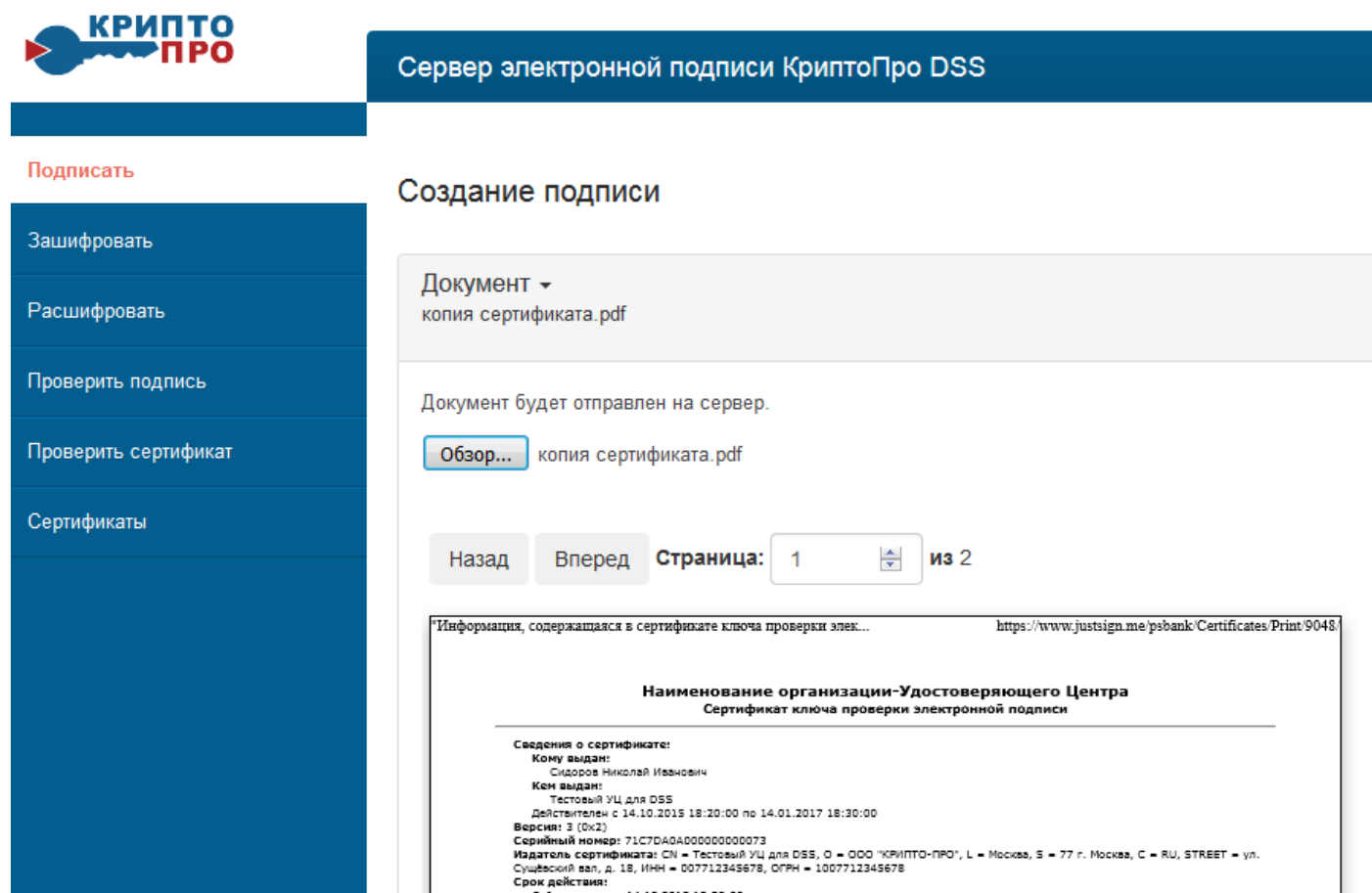


Рисунок 24. Просмотр содержания электронного документа

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 25):

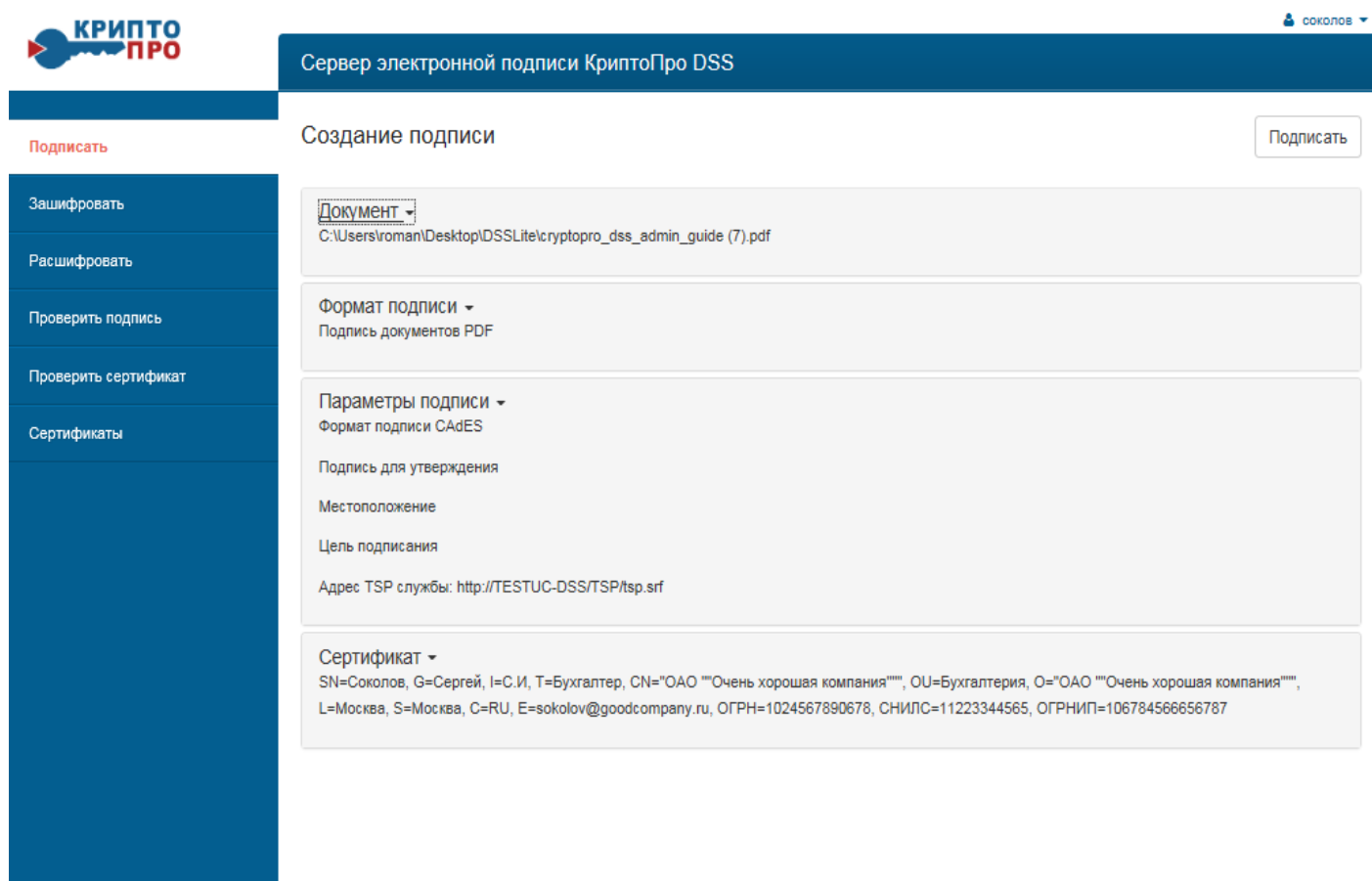


Рисунок 25. Выбор формата и параметров электронной подписи

«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 26):

КриптоПРО

Сервер электронной подписи КриптоПро DSS

Подписать

Создание подписи

Подписать

Зашифровать

Расшифровать

Проверить подпись

Проверить сертификат

Сертификаты

Документ ▾
C:\Users\roman\Desktop\тестовые файлы\cryptopro_dss_admin_guide (7).pdf

Формат подписи ▾
Подпись документов PDF

Параметры подписи ▾
Формат подписи CAdES

Подпись для утверждения

Местоположение

Цель подписания

Адрес TSP службы: http://cryptopro.ru/tsp/tsp.srf

☐ Формат подписи CMS

☒ Формат подписи CAdES

Местоположение

Цель подписания

Адрес службы штампов времени

TestTSP ▾

☒ Подпись для утверждения

☐ Сертифицирующая подпись, после сертификации изменения запрещены

☐ Сертифицирующая подпись, после сертификации разрешено заполнение полей форм и использование цифровых подписей

☐ Сертифицирующая подпись, после сертификации разрешены комментарии, заполнение полей форм и использование цифровых подписей

Сертификат ▾
SN=Соколов, G=Сергей, T=Бухгалтер, CN="ОАО""Очень хорошая компания"", OU=Бухгалтер, O="ОАО""Очень хорошая компания"", L=Москва, S=Москва, C=RU, E=sokolovser@goodcompany.ru

Рисунок 26. Выбор параметров электронной подписи CAdES

5. Выбрать действующий сертификат (см. Рисунок 27):

КРИПТОПРО

Сервер электронной подписи КриптоПро DSS

Подписать

Создание подписи

Подписать

Документ ▾
C:\Users\roman\Desktop\DSSLite\cryptopro_dss_admin_guide (7).pdf

Формат подписи ▾
Подпись документов PDF

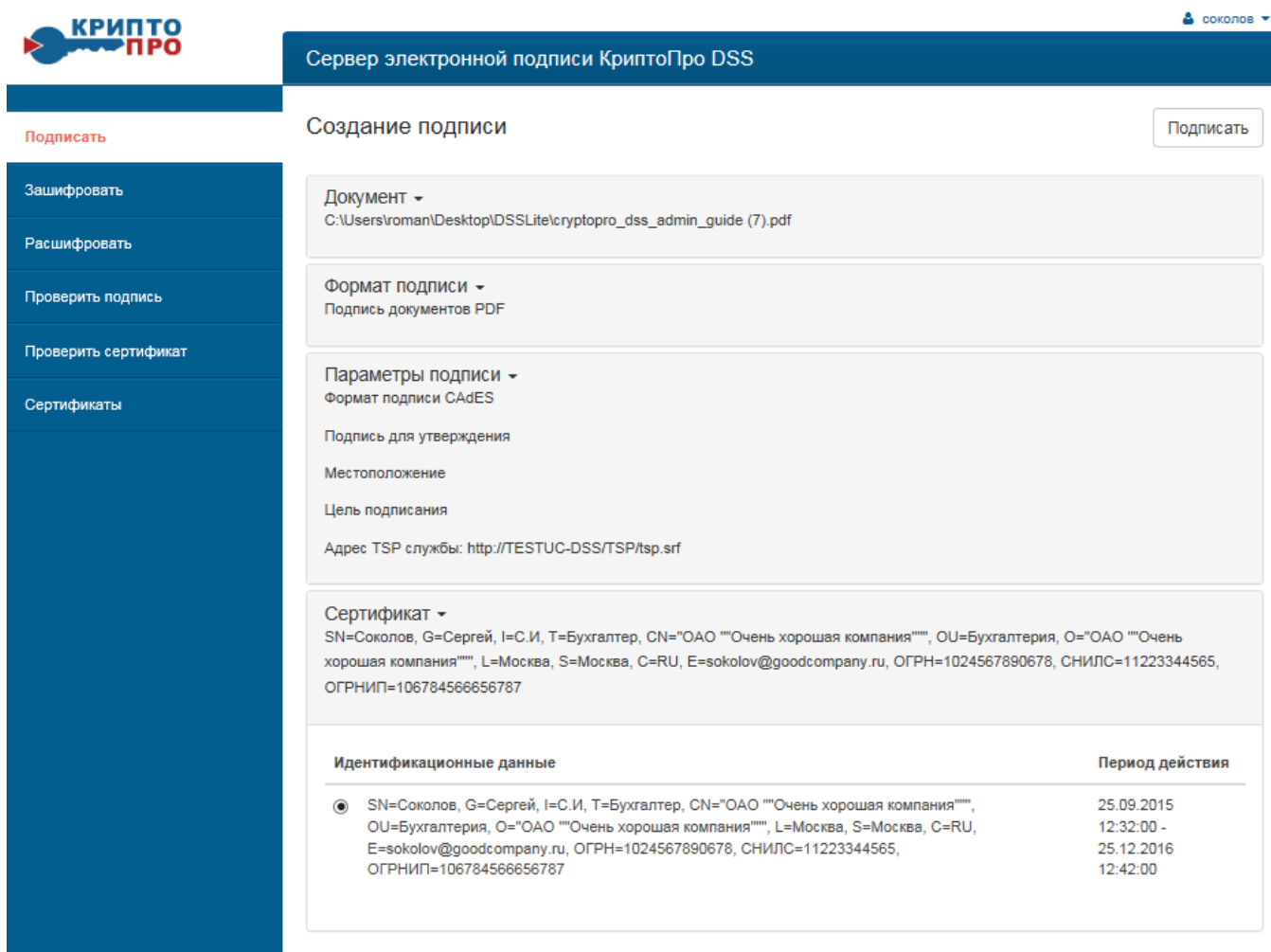
Параметры подписи ▾
Формат подписи CAdES
Подпись для утверждения
Местоположение
Цель подписания
Адрес TSP службы: http://TESTUC-DSS/TSP/tsp.srf

Сертификат ▾
SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, О="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolov@goodcompany.ru, ОГРН=1024567890678, СНИЛС=11223344565, ОГРНИП=106784566656787

Идентификационные данные	Период действия
<input checked="" type="radio"/> SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, О="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolov@goodcompany.ru, ОГРН=1024567890678, СНИЛС=11223344565, ОГРНИП=106784566656787	25.09.2015 12:32:00 - 25.12.2016 12:42:00

Рисунок 27. Выбор сертификата

6. После того как все параметры заданы, нажать сверху справа кнопку «Подписать» (см. Рисунок 28):



КРИПТОПРО

Сервер электронной подписи КриптоПро DSS

Подписать

Создание подписи

Документ
C:\Users\roman\Desktop\DSSLite\cryptopro_dss_admin_guide (7).pdf

Формат подписи
Подпись документов PDF

Параметры подписи
Формат подписи CAdES
Подпись для утверждения
Местоположение
Цель подписания
Адрес TSP службы: http://TESTUC-DSS/TSP/tsp.srf

Сертификат
SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, О="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolov@goodcompany.ru, ОГРН=1024567890678, СНИЛС=11223344565, ОГРНИП=106784566656787

Идентификационные данные	Период действия
<input checked="" type="radio"/> SN=Соколов, G=Сергей, I=С.И, Т=Бухгалтер, CN="ОАО ""Очень хорошая компания""", OU=Бухгалтерия, О="ОАО ""Очень хорошая компания""", L=Москва, S=Москва, C=RU, E=sokolov@goodcompany.ru, ОГРН=1024567890678, СНИЛС=11223344565, ОГРНИП=106784566656787	25.09.2015 12:32:00 - 25.12.2016 12:42:00

Рисунок 28. Подготовка документа к подписанию

1. В открывшемся окне отобразит окно ввода пароля на доступ к закрытому ключу выбранного контейнера (см. Рисунок 29). Введите указанный пароль и нажмите кнопку «ОК».

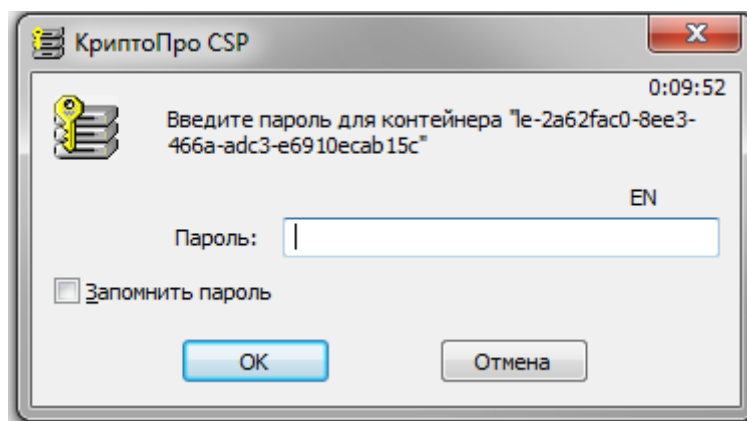


Рисунок 29. Ввод пароля на доступ

2. Документ будет подписан, после чего в низу открывшегося окна нажать стрелку, далее - «Сохранить как» (см. Рисунок 30):

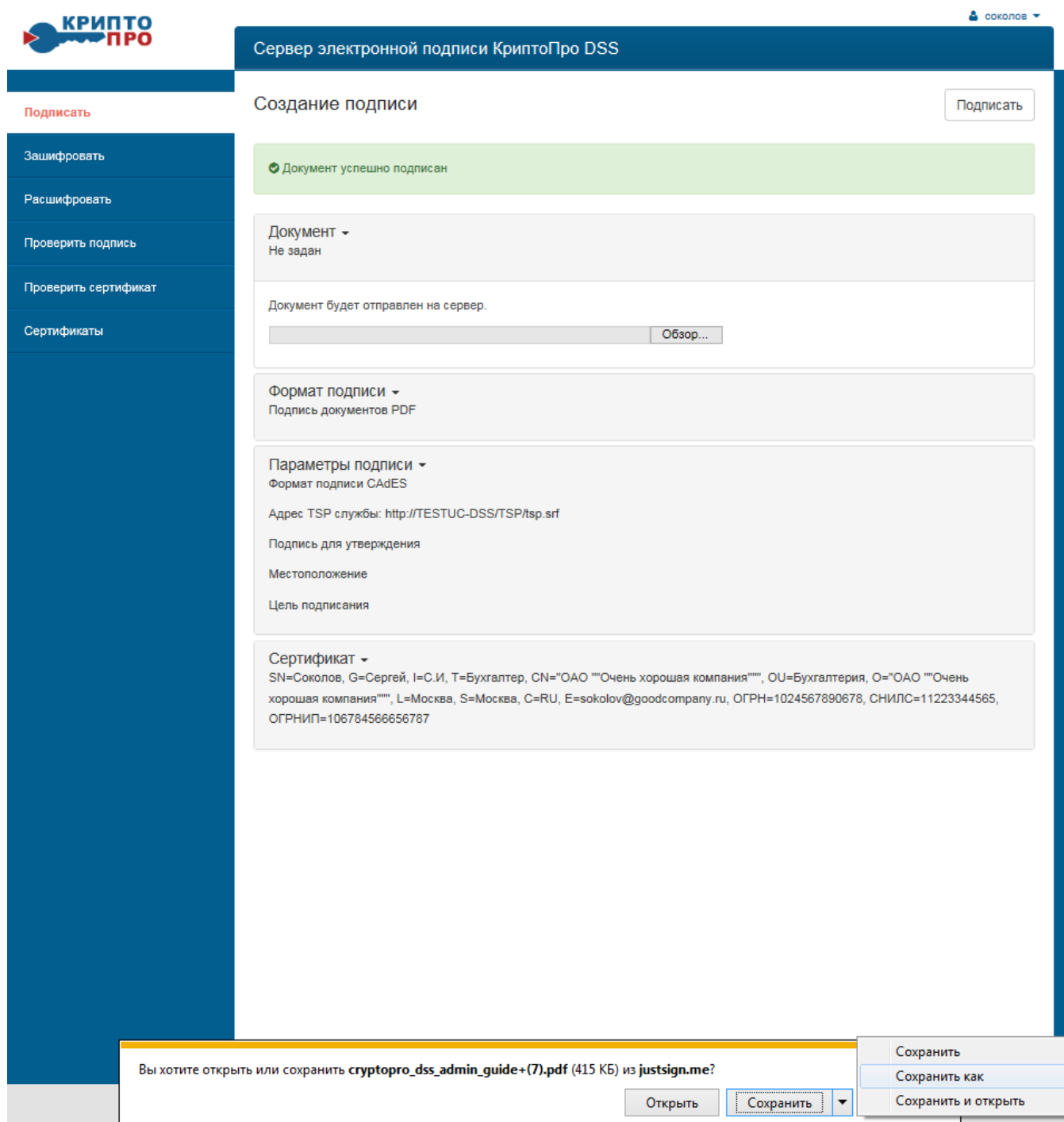


Рисунок 30. Сохранение подписанного электронного документа

3. Выбрать каталог и название файла для подписанного электронного документа (см. Рисунок 31):

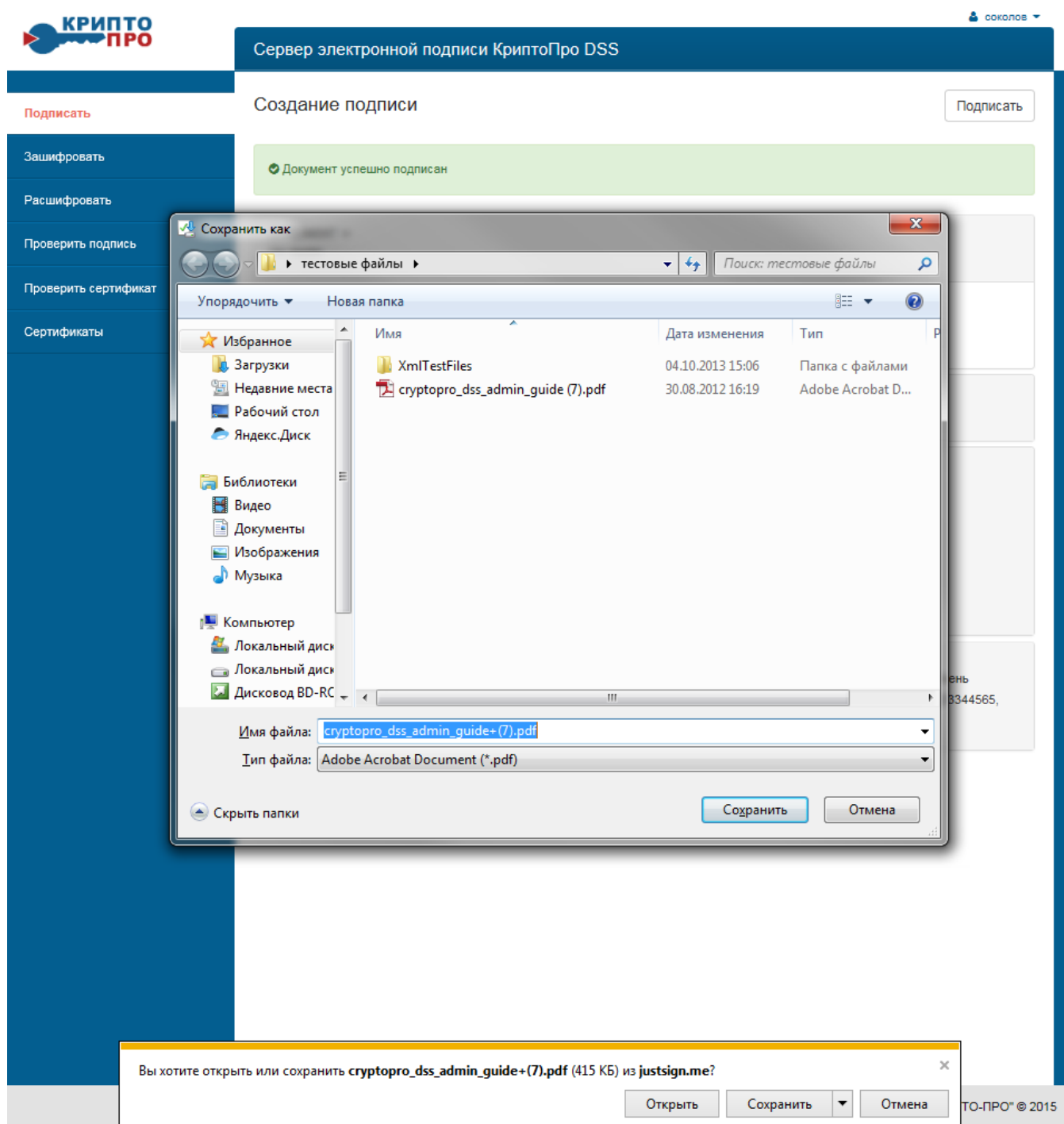


Рисунок 31. Выбор папки и названия файла для сохранения подписанного электронного документа

5. Проверка электронной подписи и сертификата

5.1. 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://dss.cryptopro.ru/verify> и в меню слева нажать на кнопку «**Проверить подпись**», откроется окно «**Проверка подписи**» (см. Рисунок 32):

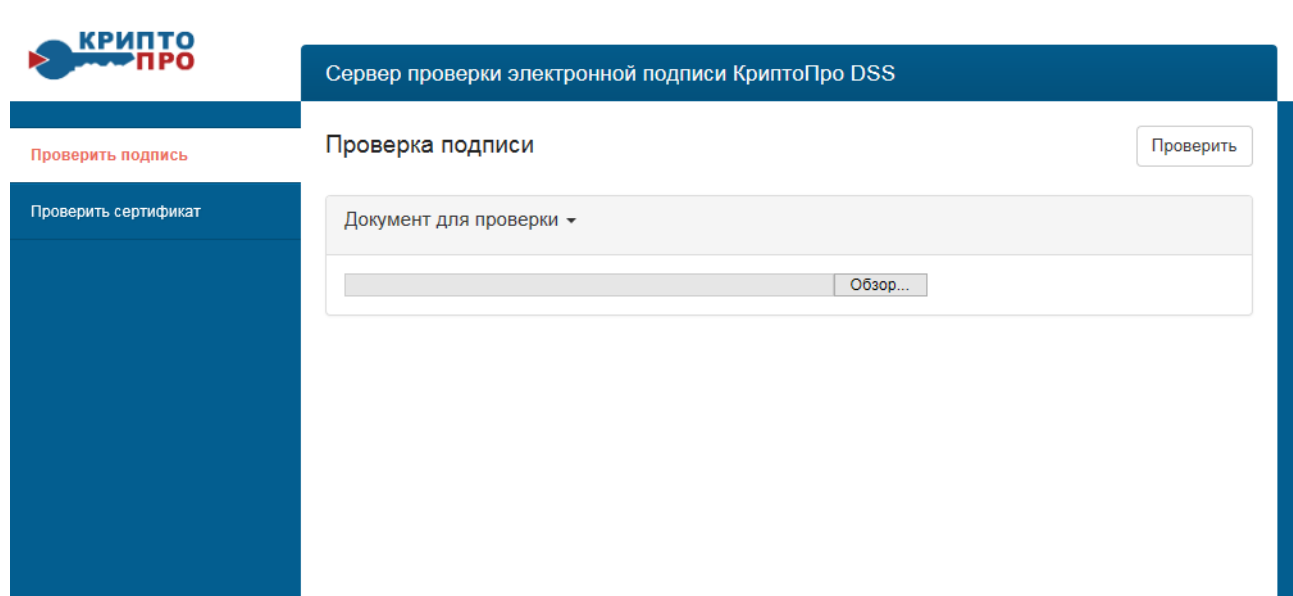


Рисунок 32. Окно проверка подписи

Нажать «**Обзор**» откроется окно, выбрать подписанный документ (с расширением .sig) и нажать «**Открыть**» (см. Рисунок 33):

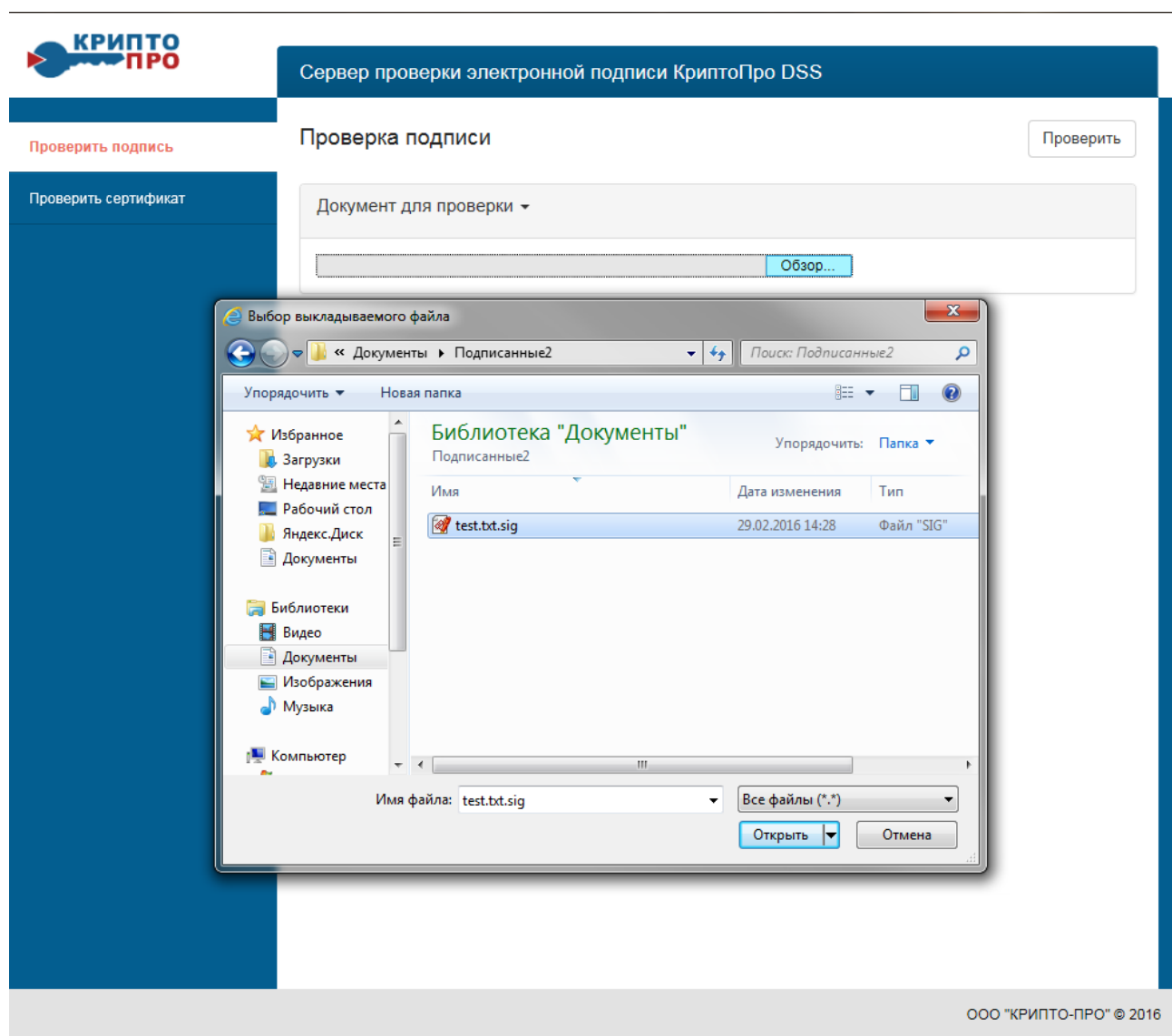


Рисунок 33. Выбор файла для проверки присоединенной электронной подписи (в составе электронного документа)

2. Формат подписи определится автоматически, после нажать кнопку «Проверить» (см. Рисунок 34):

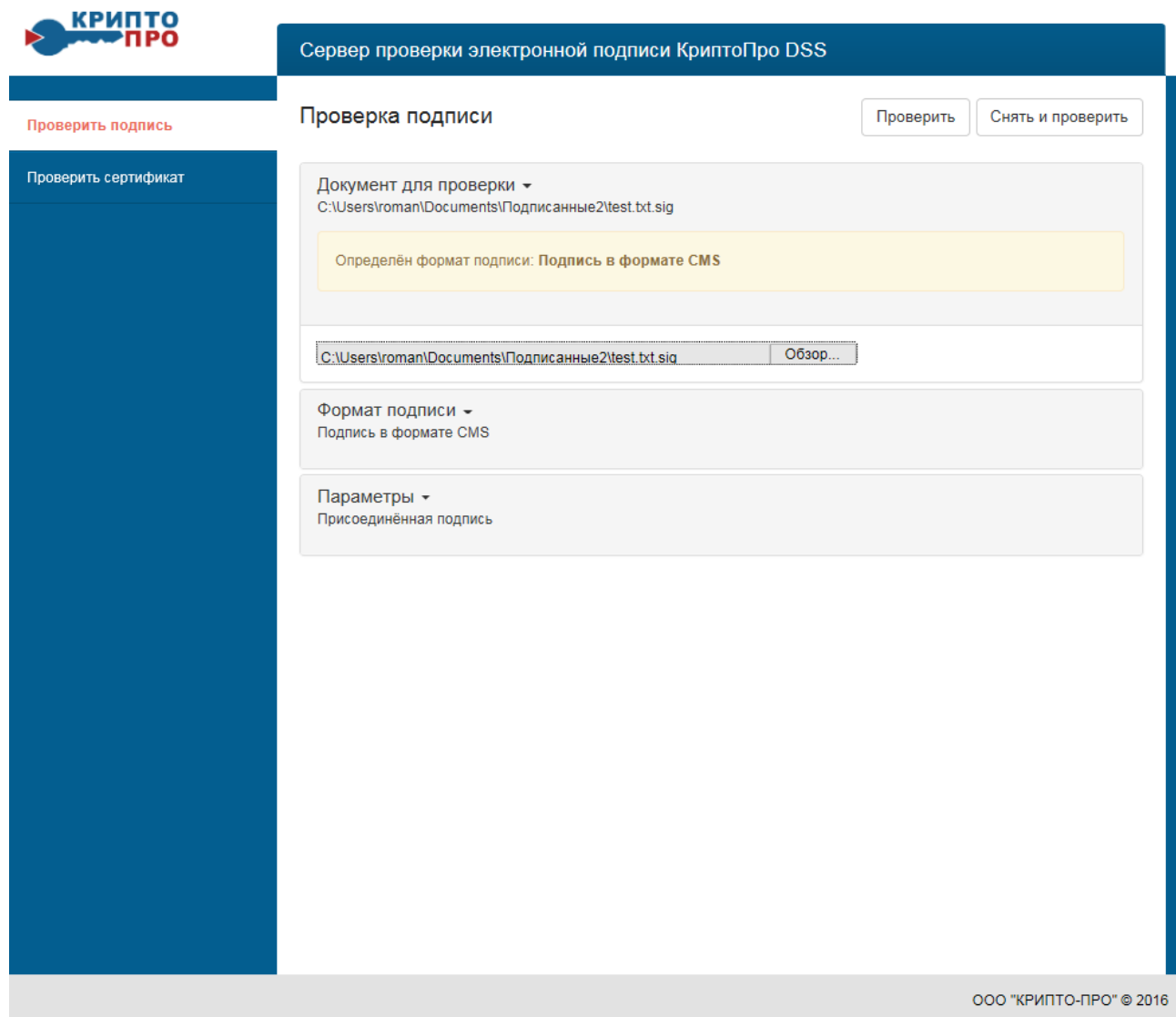
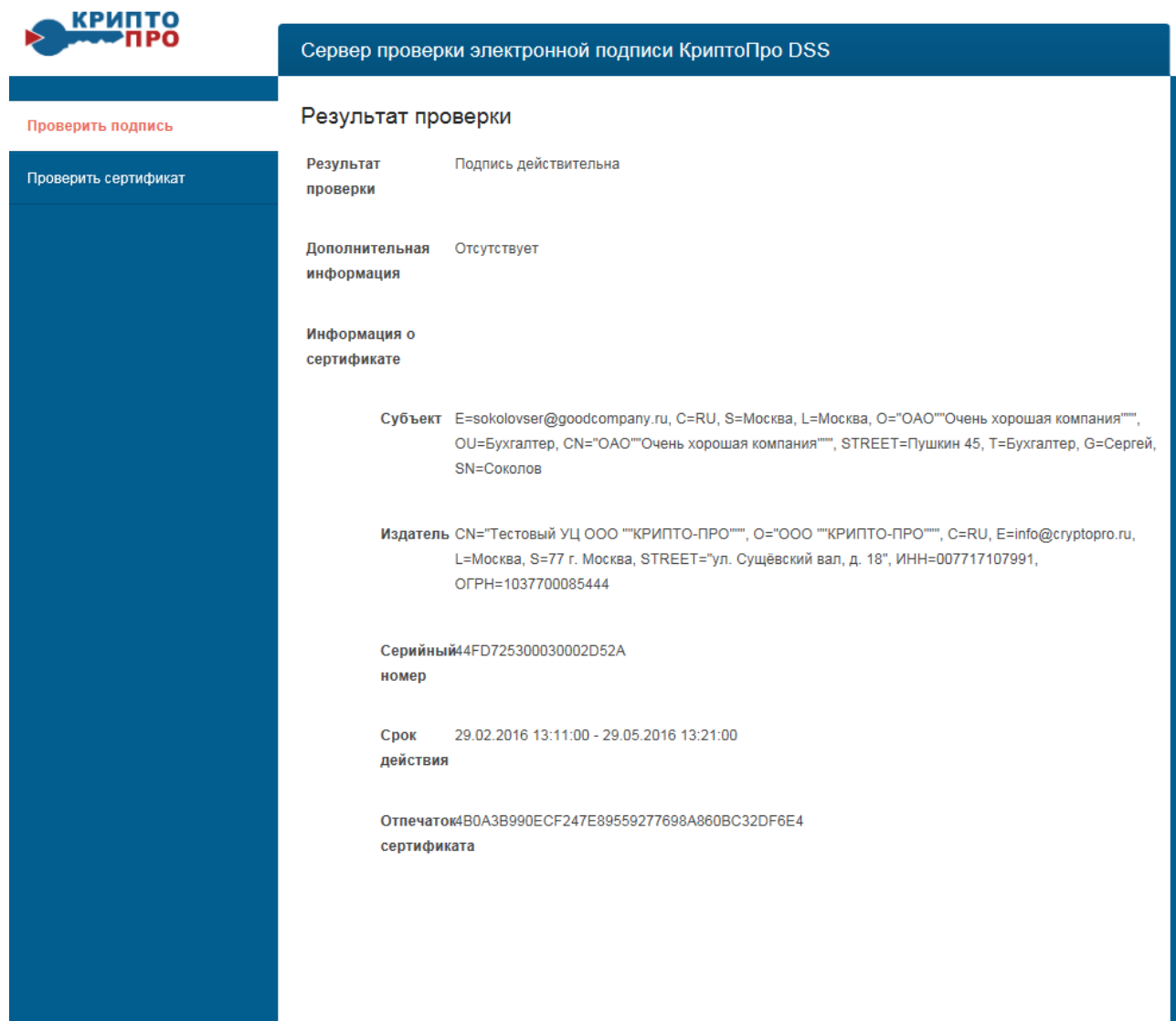


Рисунок 34. Параметр присоединённой подписи

3. Будет выполнено действие проверки электронной подписи документа и откроется окно с результатом (см. Рисунок 35):



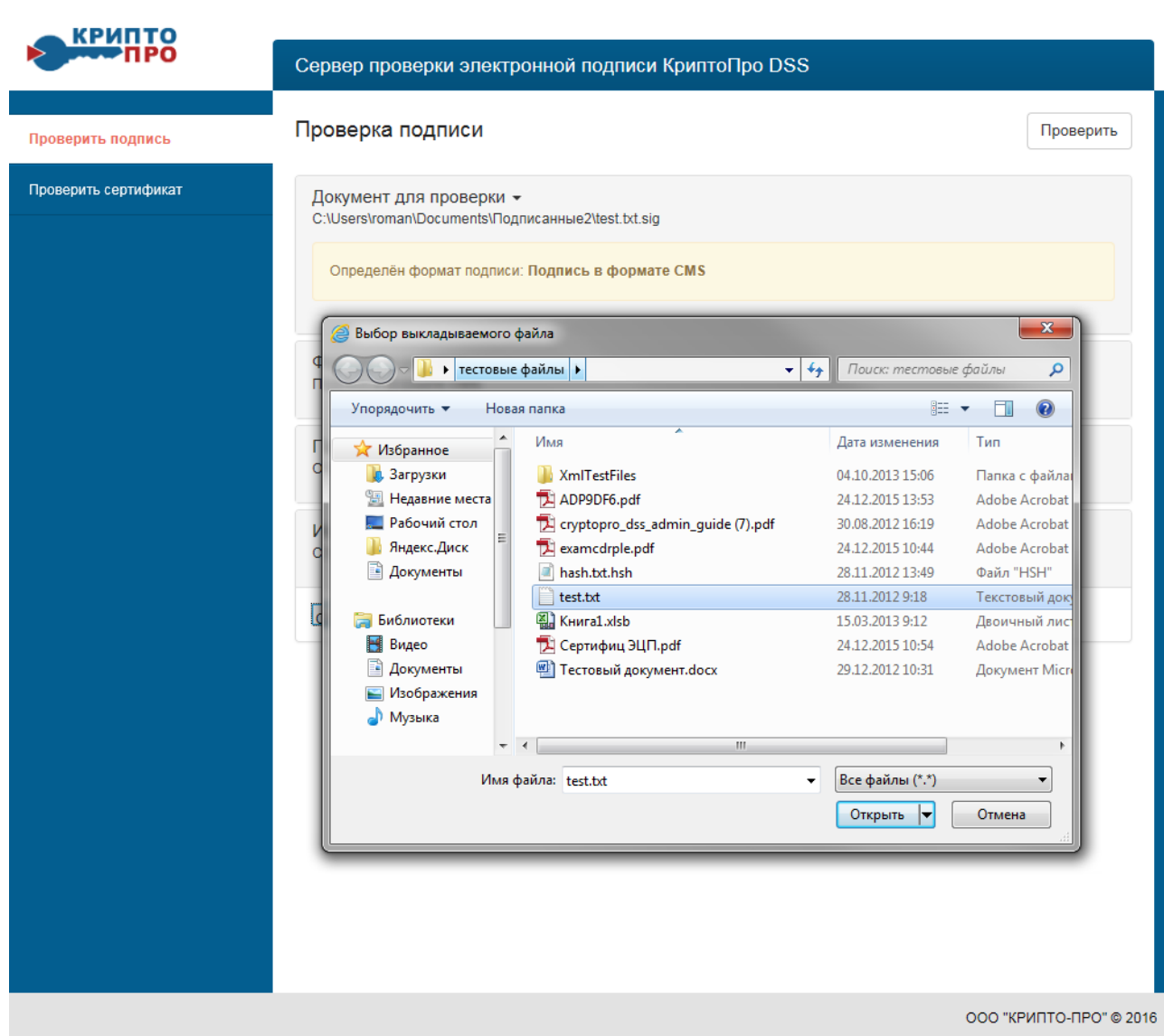


Рисунок 36. Выбор файла первоначального документа для проверки отсоединенной электронной подписи

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.

5.2. 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 **6**) осуществляется с использованием «Службы проверки электронной подписи». Доступ к Службе проверки осуществляется из личного кабинета Пользователя СЭП или по адресу <https://dss.cryptopro.ru/verify> в меню слева нажать кнопку «**Проверить сертификат**» (см. Рисунок 37):

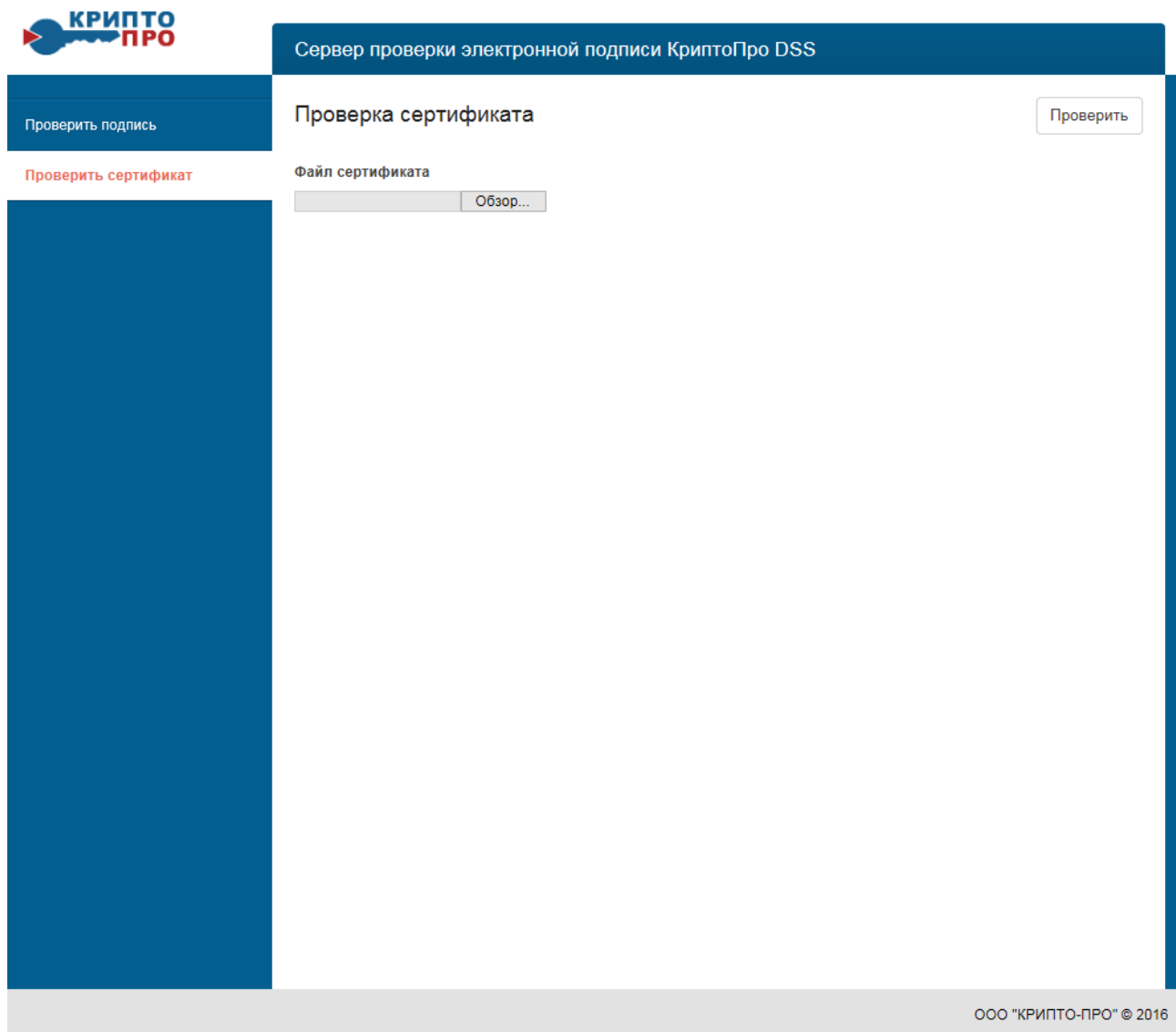
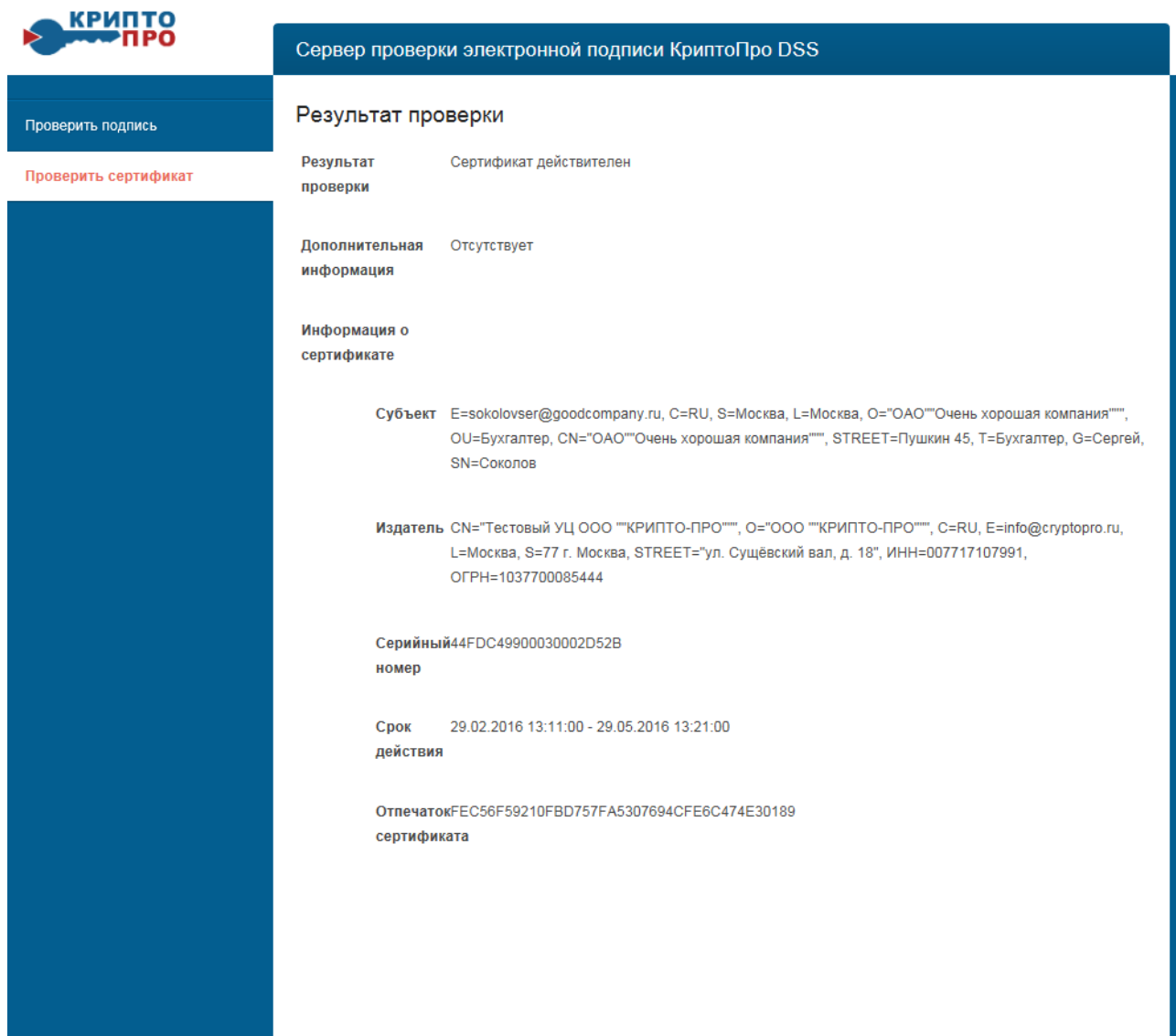


Рисунок 37. Проверка сертификата

2. Далее нажать на «**Обзор**» и выбрать ранее полученный от контрагента сертификат, нажать «**Проверить**», откроется окно с результатом проверки (см. Рисунок 38):



The screenshot displays the 'КРИПТОПРО' logo on the left and the title 'Сервер проверки электронной подписи КриптоПро DSS' at the top. The main content area is titled 'Результат проверки' (Verification Result). It shows the following details:

- Результат проверки** (Verification Result): Сертификат действителен (Certificate is valid).
- Дополнительная информация** (Additional information): Отсутствует (Absent).
- Информация о сертификате** (Certificate information):
 - Субъект** (Subject): E=sokolovser@goodcompany.ru, C=RU, S=Москва, L=Москва, O="ОАО""Очень хорошая компания"", OU=Бухгалтер, CN="ОАО""Очень хорошая компания", STREET=Пушкин 45, Т=Бухгалтер, G=Сергей, SN=Соколов
 - Издатель** (Issuer): CN="Тестовый УЦ ООО ""КРИПТО-ПРО"", O="ООО ""КРИПТО-ПРО"", C=RU, E=info@cryptopro.ru, L=Москва, S=77 г. Москва, STREET="ул. Суцёвский вал, д. 18", ИНН=007717107991, ОГРН=1037700085444
 - Серийный номер** (Serial number): 44FDC49900030002D52B
 - Срок действия** (Validity period): 29.02.2016 13:11:00 - 29.05.2016 13:21:00
 - Отпечаток сертификата** (Certificate fingerprint): FEC56F59210FBD757FA5307694CFE6C474E30189

Рисунок 38. Результат проверки сертификата

6. 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 39):

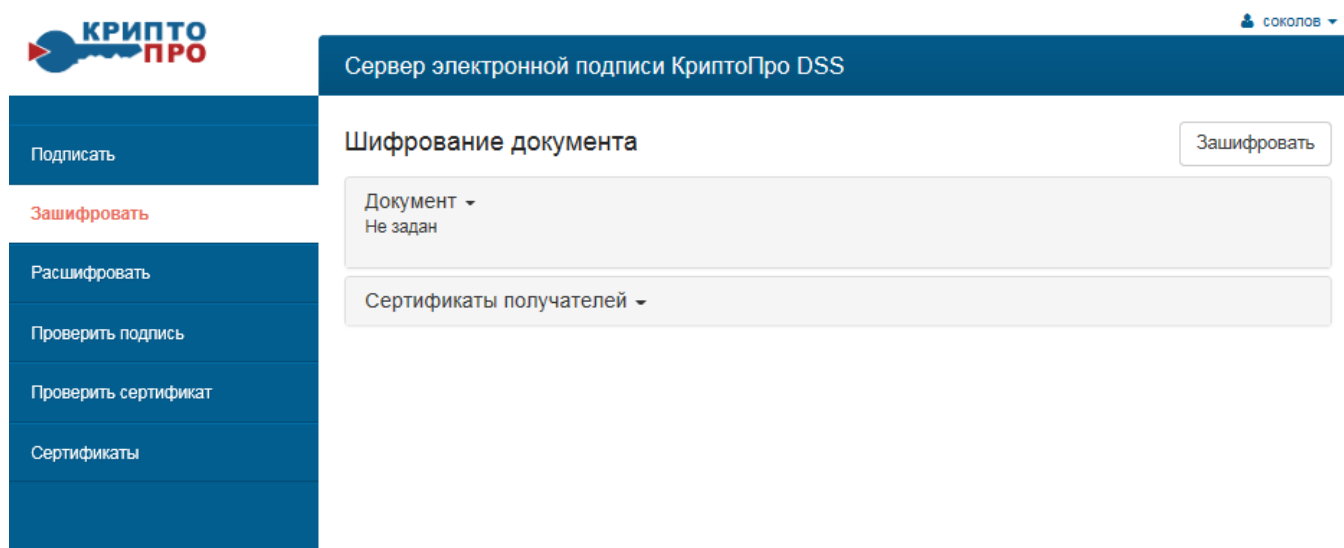


Рисунок 39. Шифрование документа

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 40):

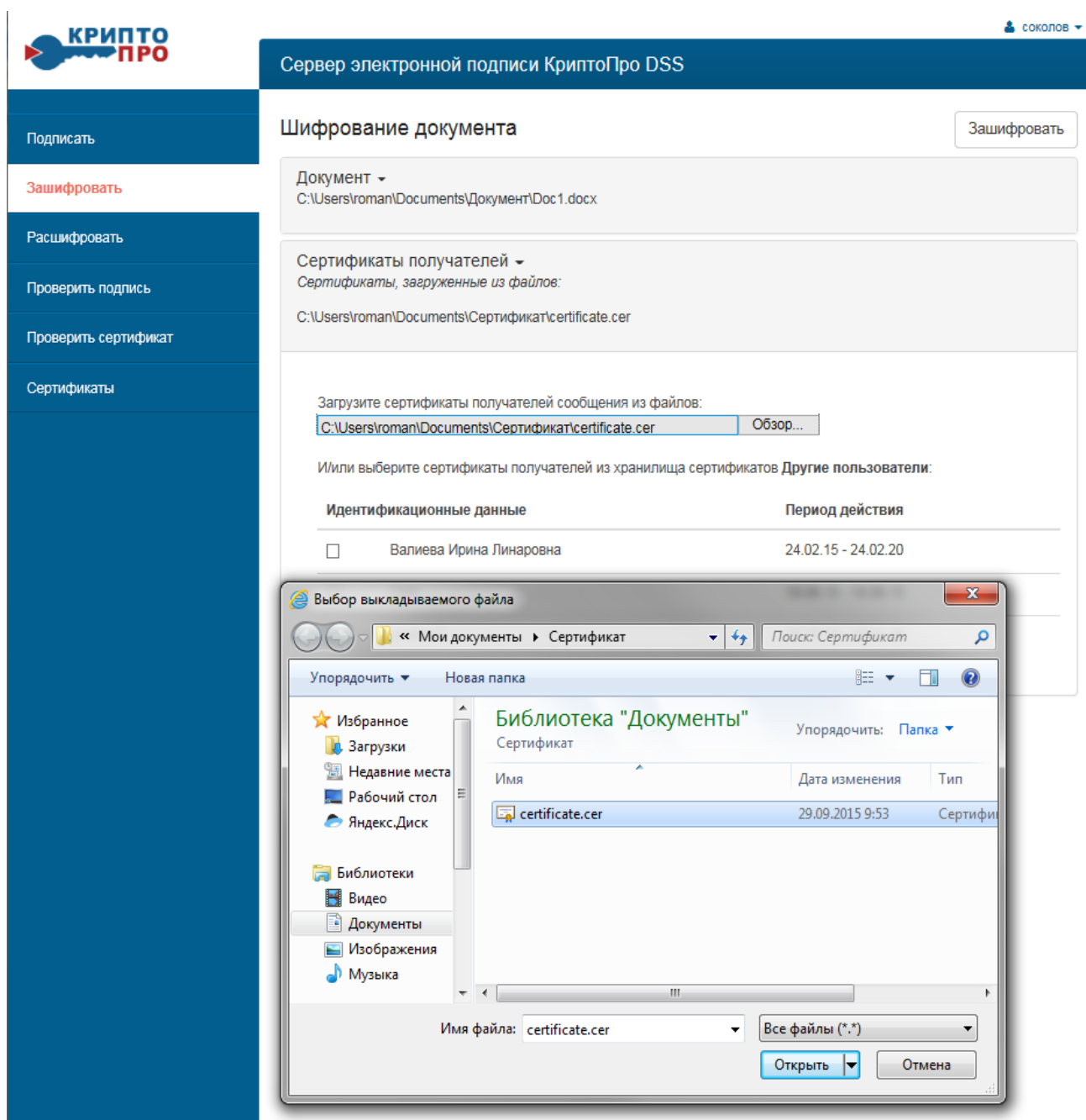


Рисунок 40. Выбор сертификата пользователя

- Нажать кнопку «Обзор» выбрать документ для шифрования (см. Рисунок 41):

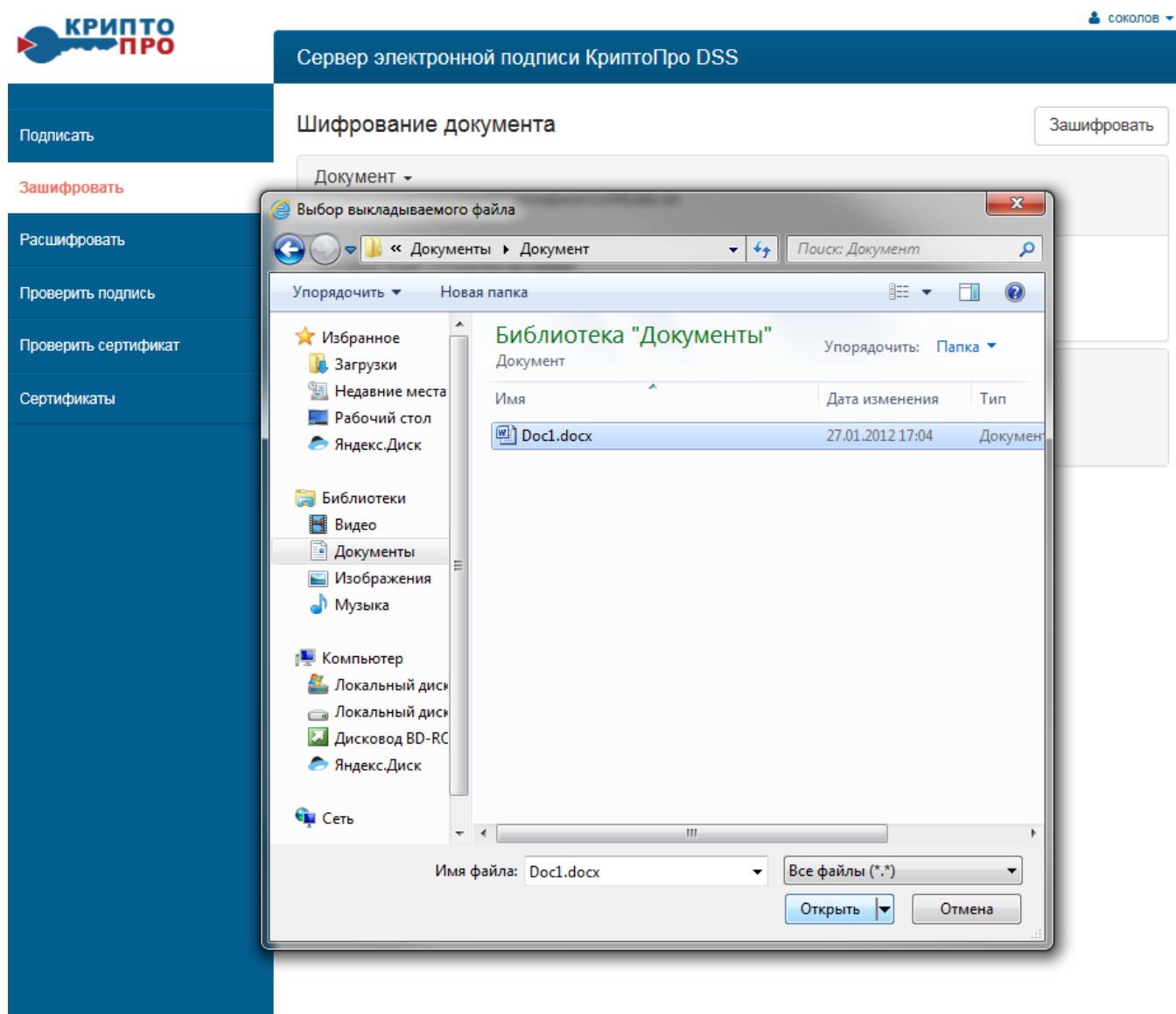


Рисунок 41. Выбор документа для шифрования

4. Нажать кнопку «Зашифровать» откроется окно с результатом действия «Документ зашифрован» и будет предложено его сохранить, нажать «Сохранить как» (см. [Рисунок 42](#) и [Рисунок 43](#)):

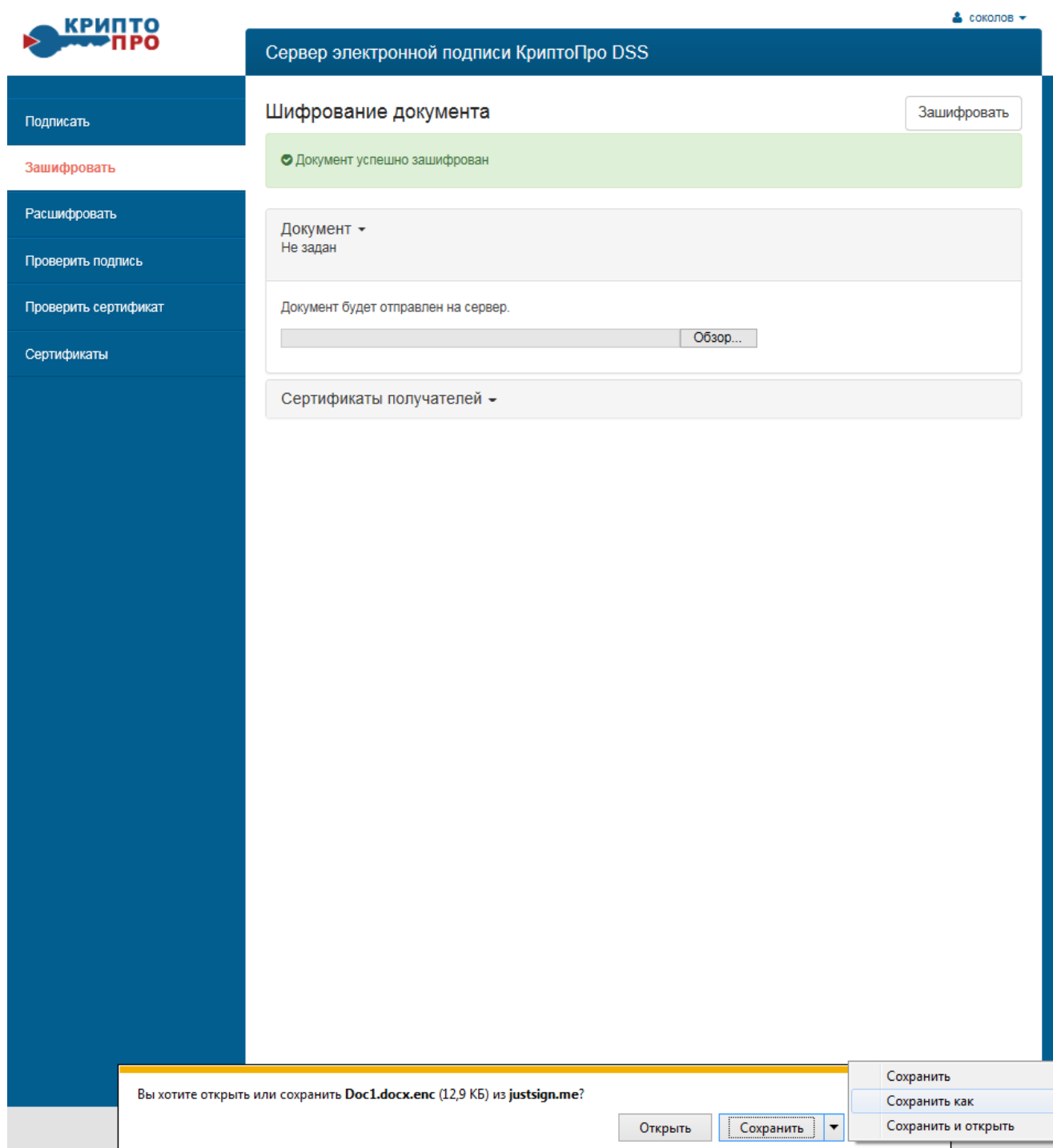


Рисунок 42. Завершение операции шифрования документа

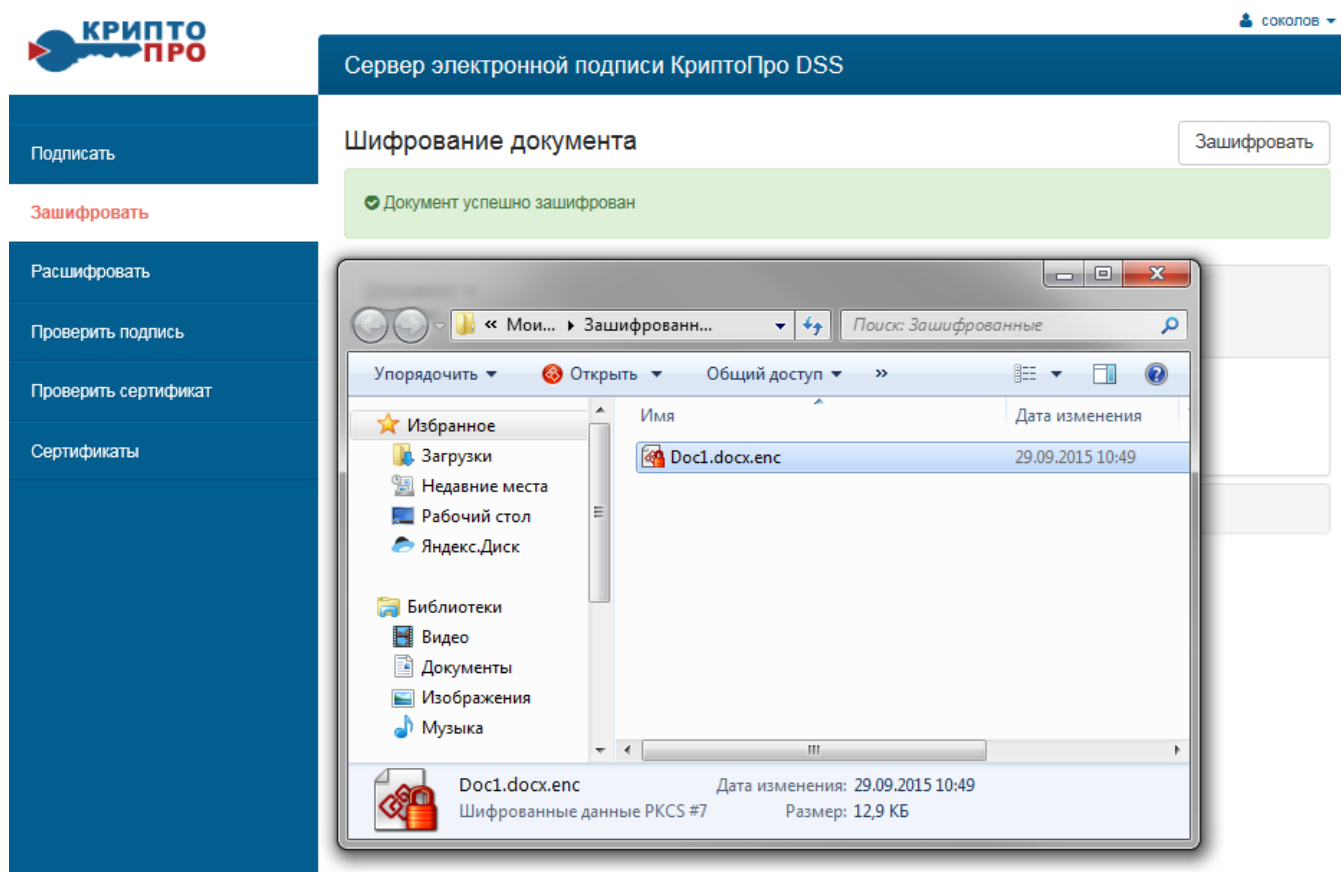


Рисунок 43. Сохранение зашифрованного документа

5. Для шифрования своих документов предварительно выгрузить с СЭП свой сертификат (см. Раздел 2). Далее шифрование, выполнить, как описано в текущем разделе.

7. 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 44):

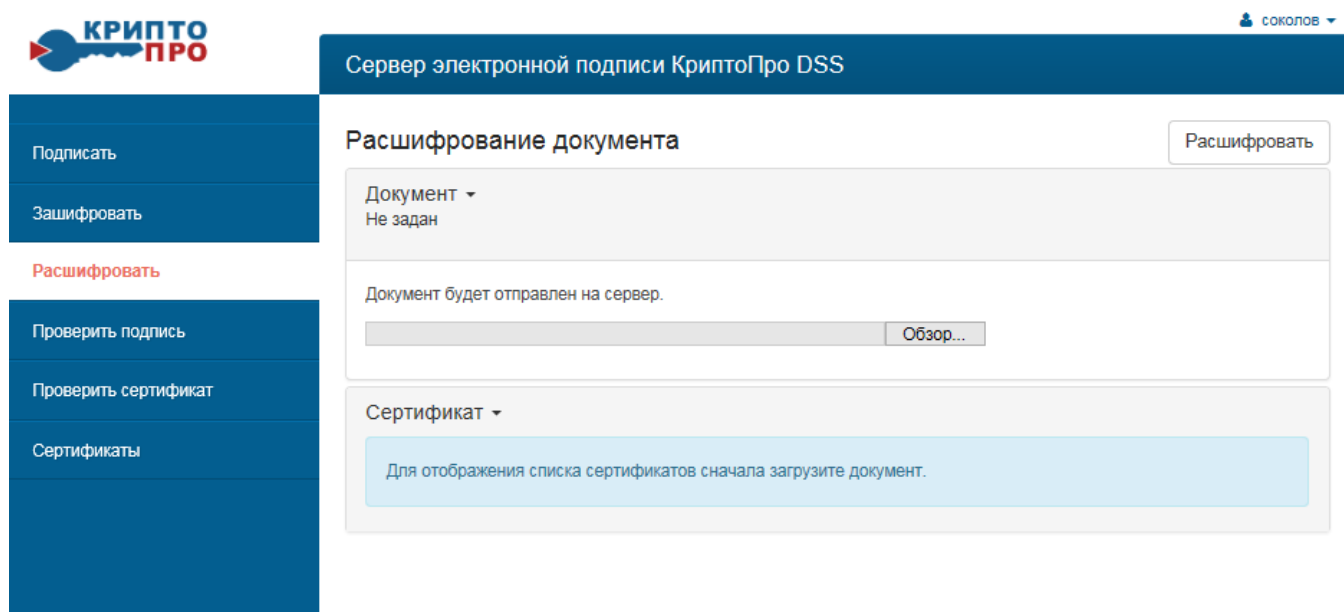


Рисунок 44. Расшифровывание документа

2. Нажать кнопку «**Обзор**» выбрать документ для расшифровывания, нажать кнопку «**Открыть**» (см. [Рисунок 45](#)):

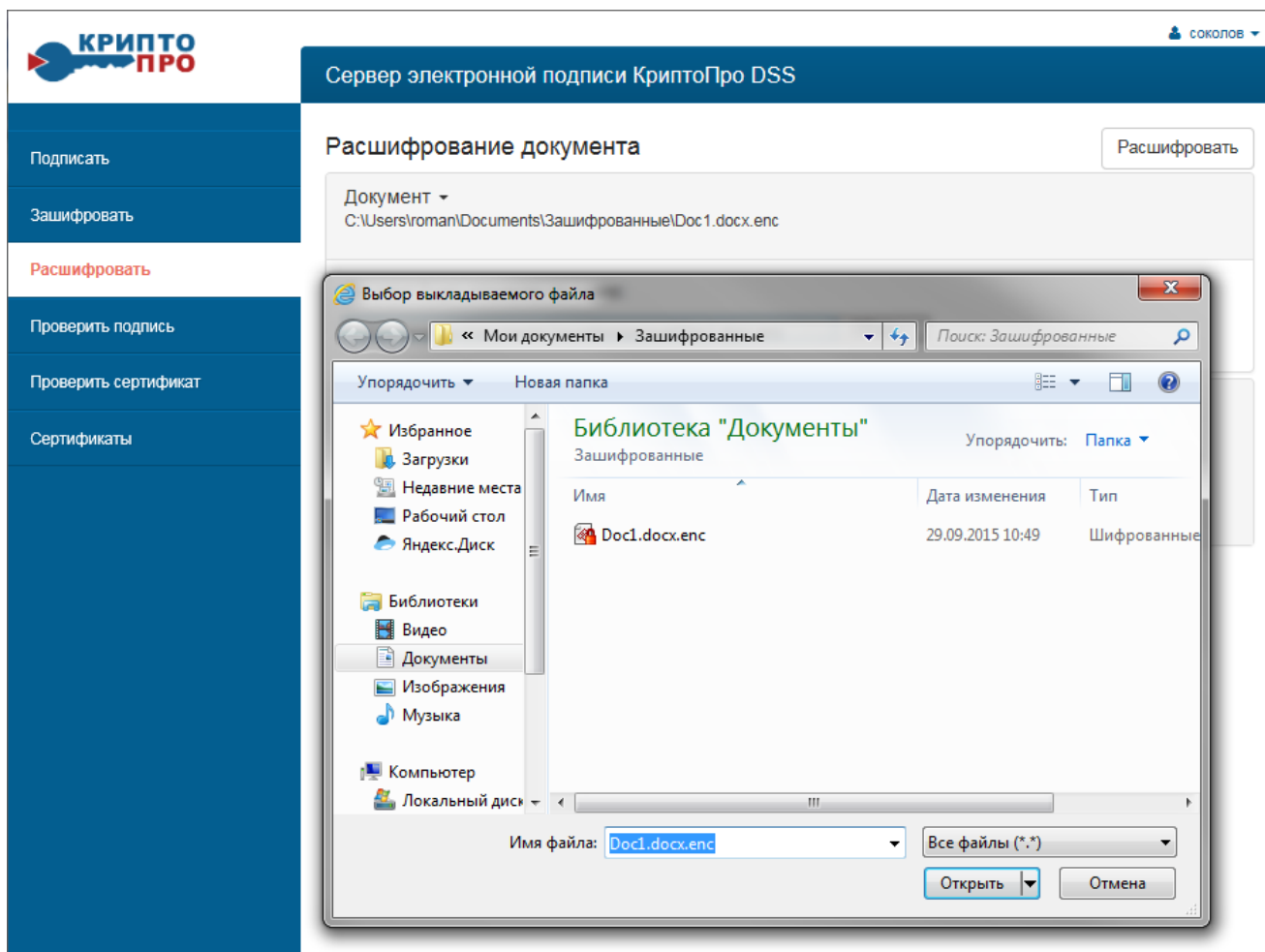


Рисунок 45. Выбор документа для расшифровывания

3. Далее будет автоматически произведена проверка используемого сертификата и отображены его сведения (см. Рисунок 46):

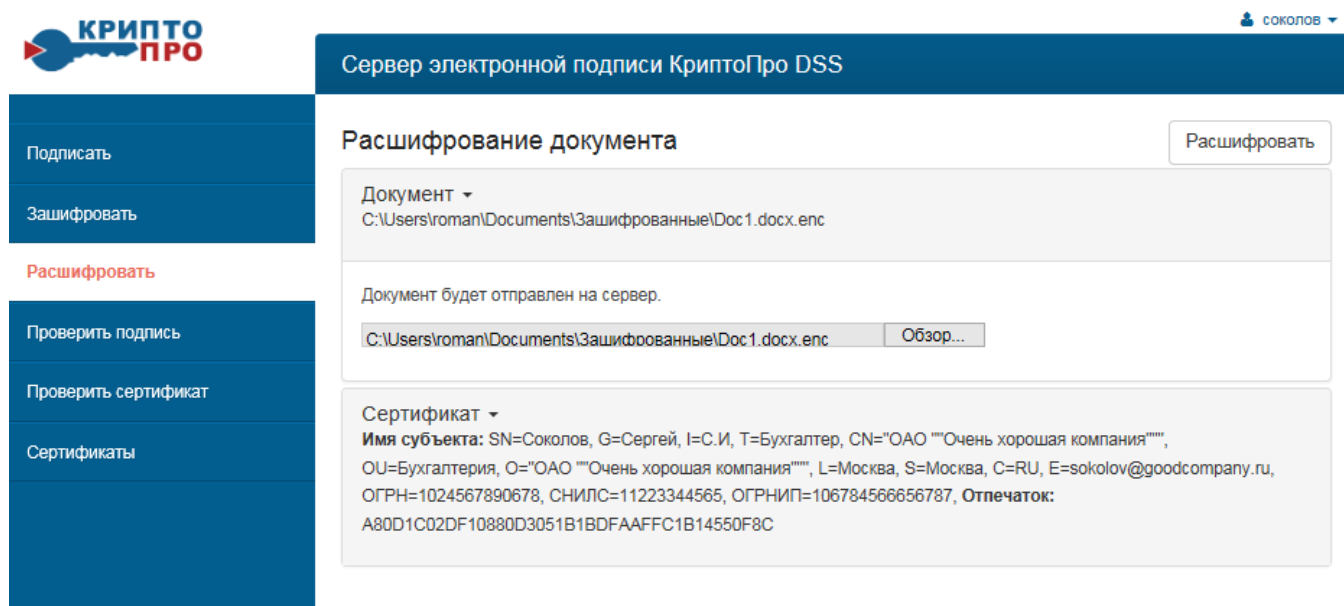


Рисунок 46. Вывод информации об используемом сертификате

4. Если сертификат недействительный, то отобразится соответствующее сообщение (см. Рисунок 47):

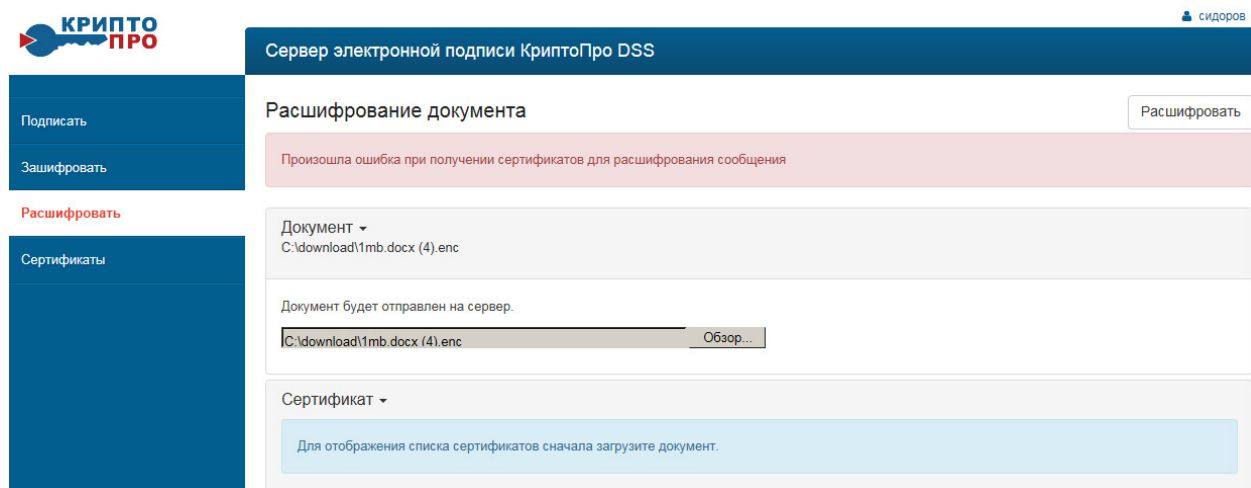


Рисунок 47. Отрицательный результат проверки сертификата

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 48):

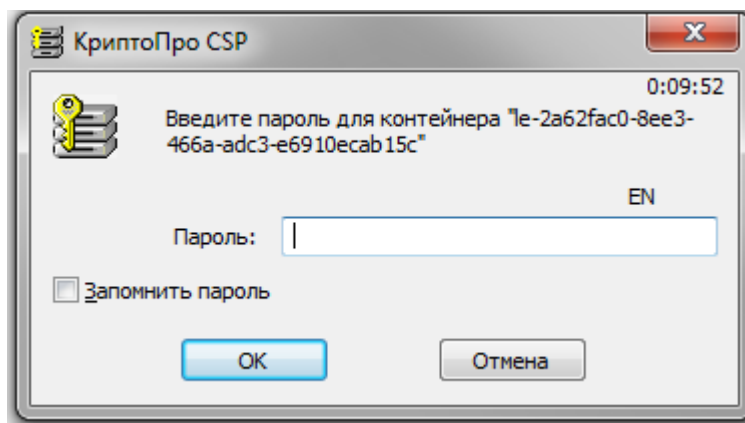


Рисунок 48. Окно для ввода ПИН-кода доступа к закрытому ключу

6. Откроется окно «Документ успешно расшифрован» и будет предложено его сохранить, нажать «**Сохранить как**» (см. Рисунок 49):

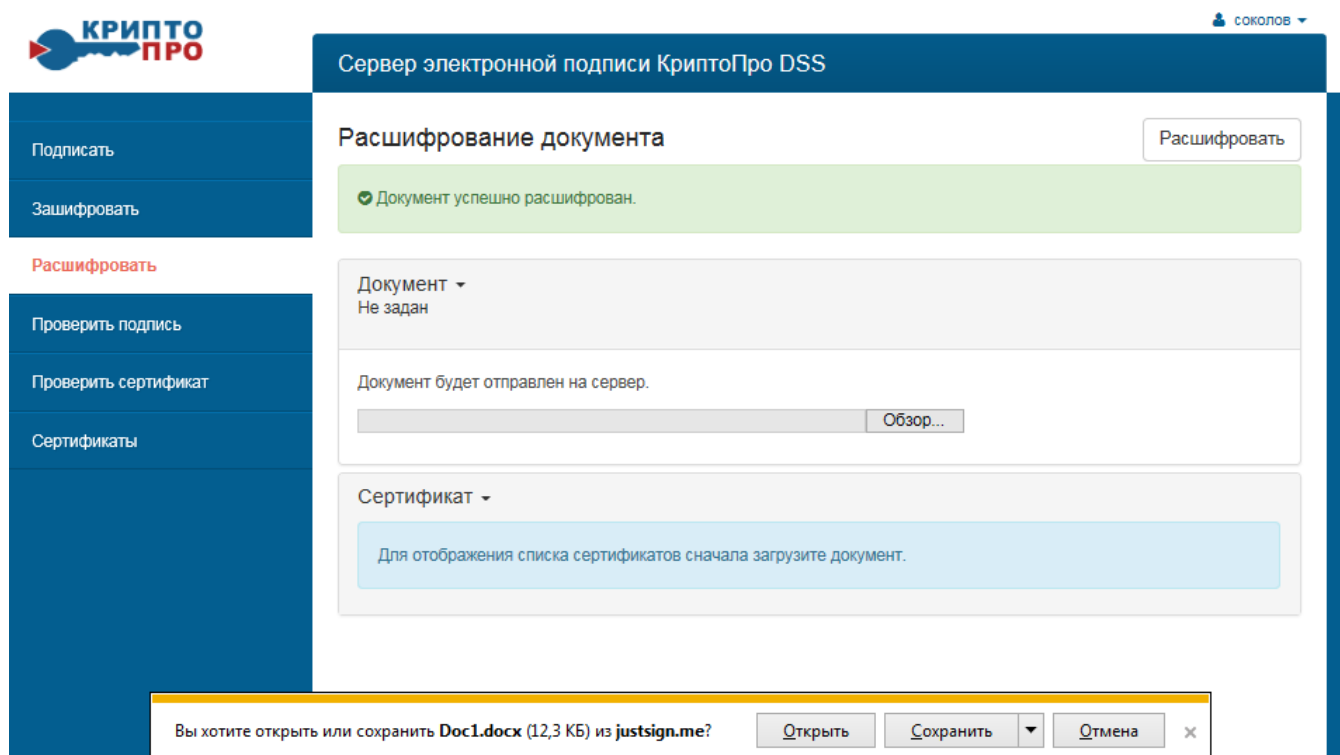


Рисунок 49. Сохранение расшифрованного документа

7. Откроется окно, ввести имя расшифрованного документа и нажать «**Сохранить**» (см. Рисунок 50):

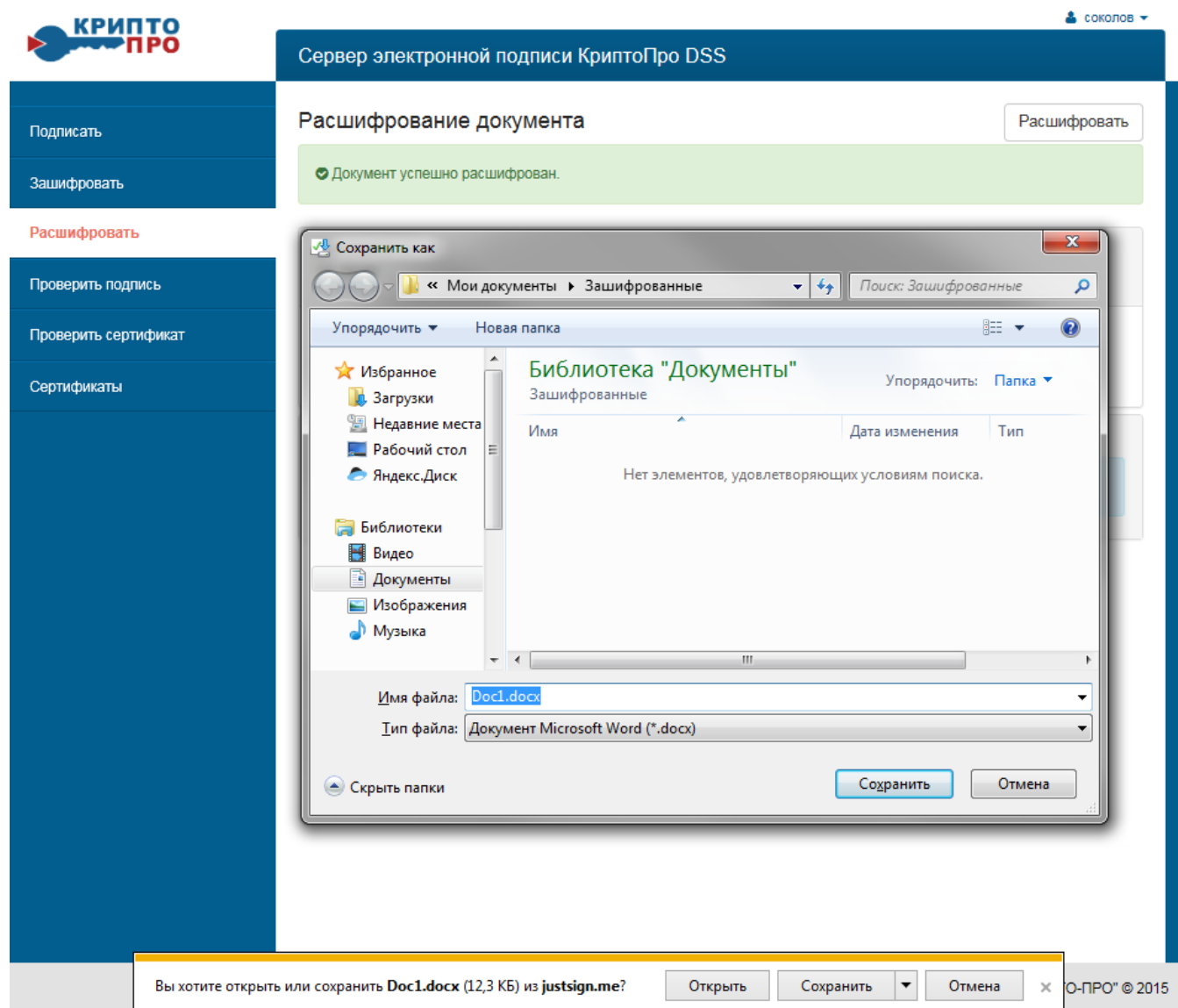


Рисунок 50. Выбор папки для сохранения расшифрованного документа

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 51 и Рисунок 52):

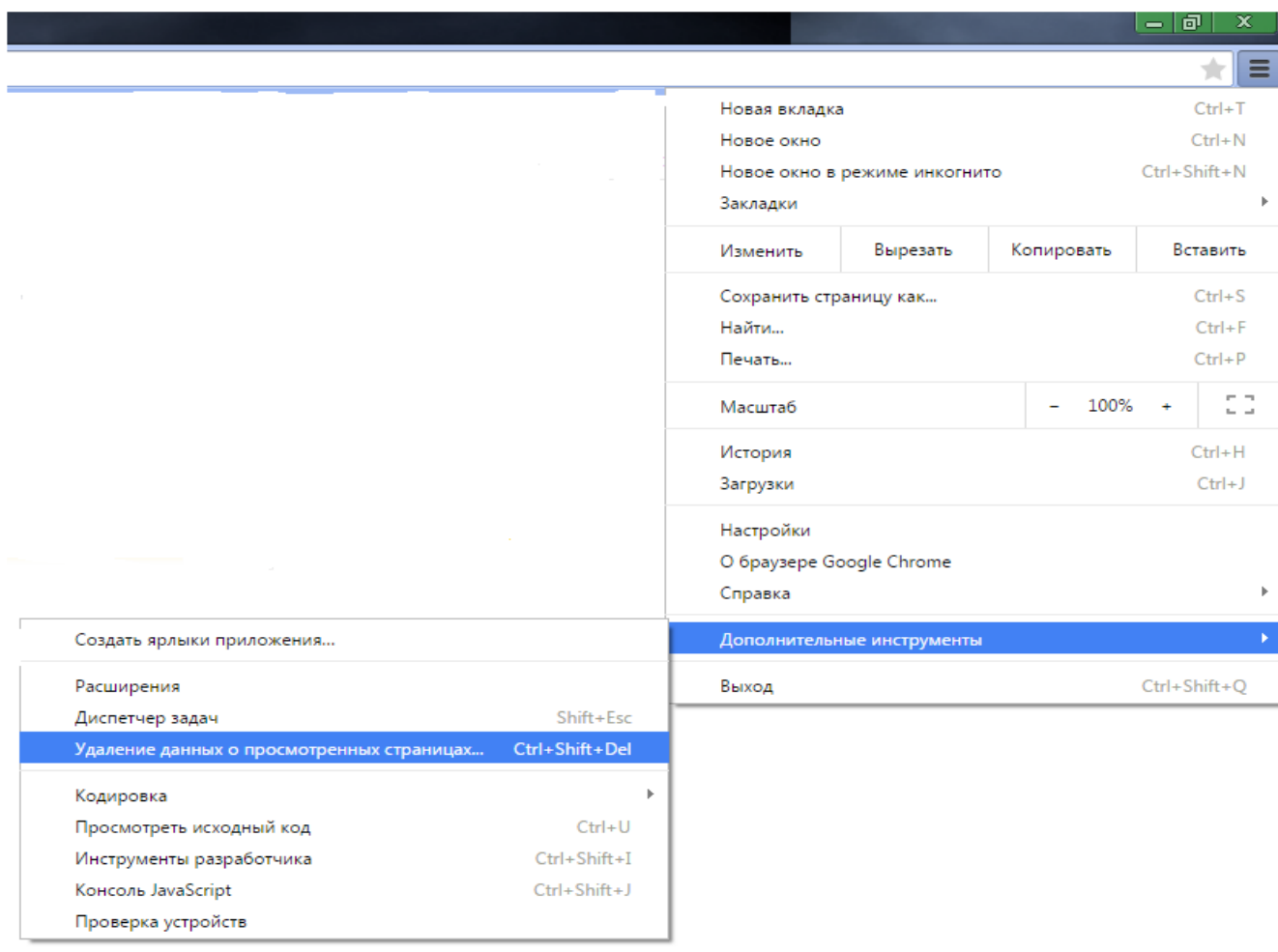


Рисунок 51. Удаление данных

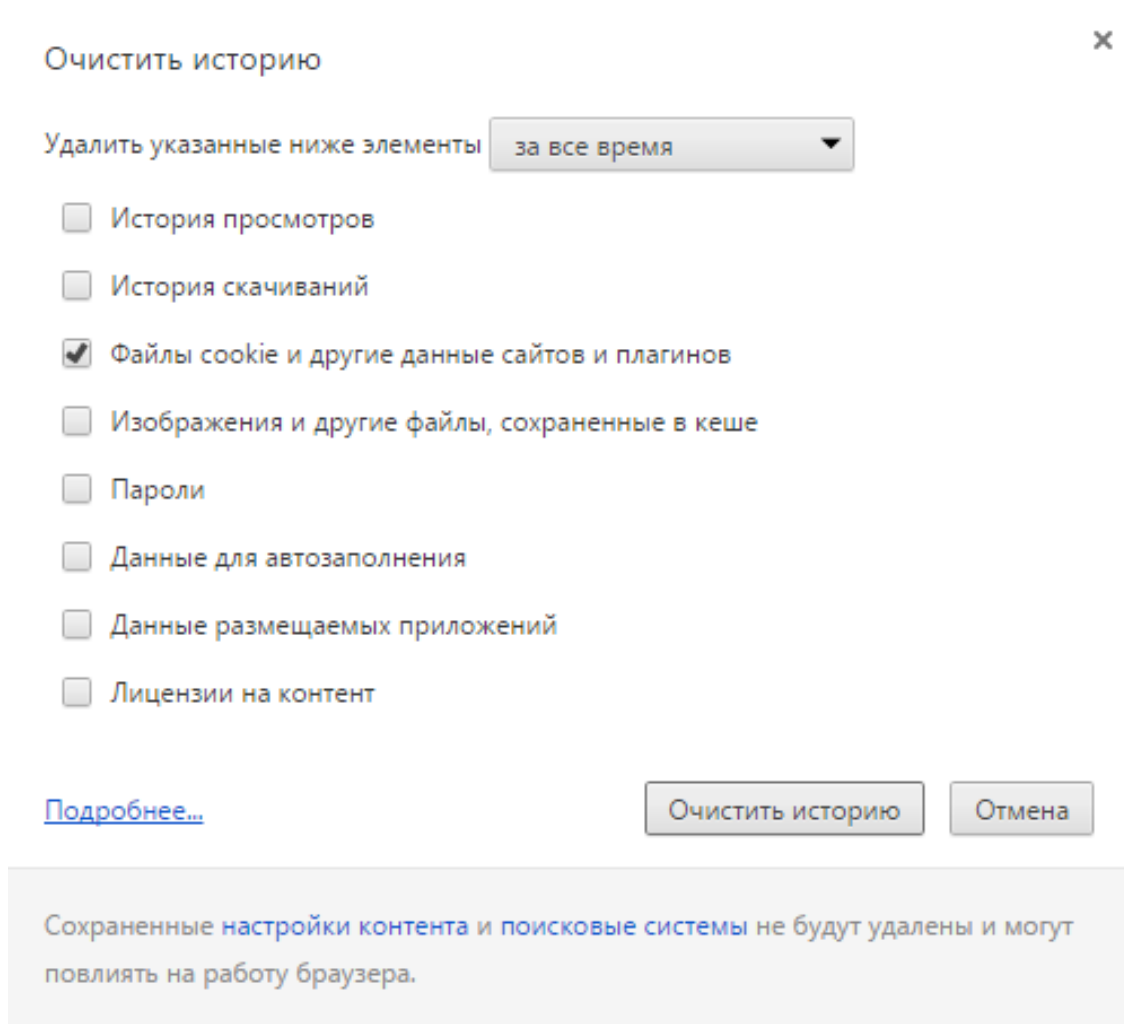


Рисунок 52. Очистка историй

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 53 и Рисунок 54):

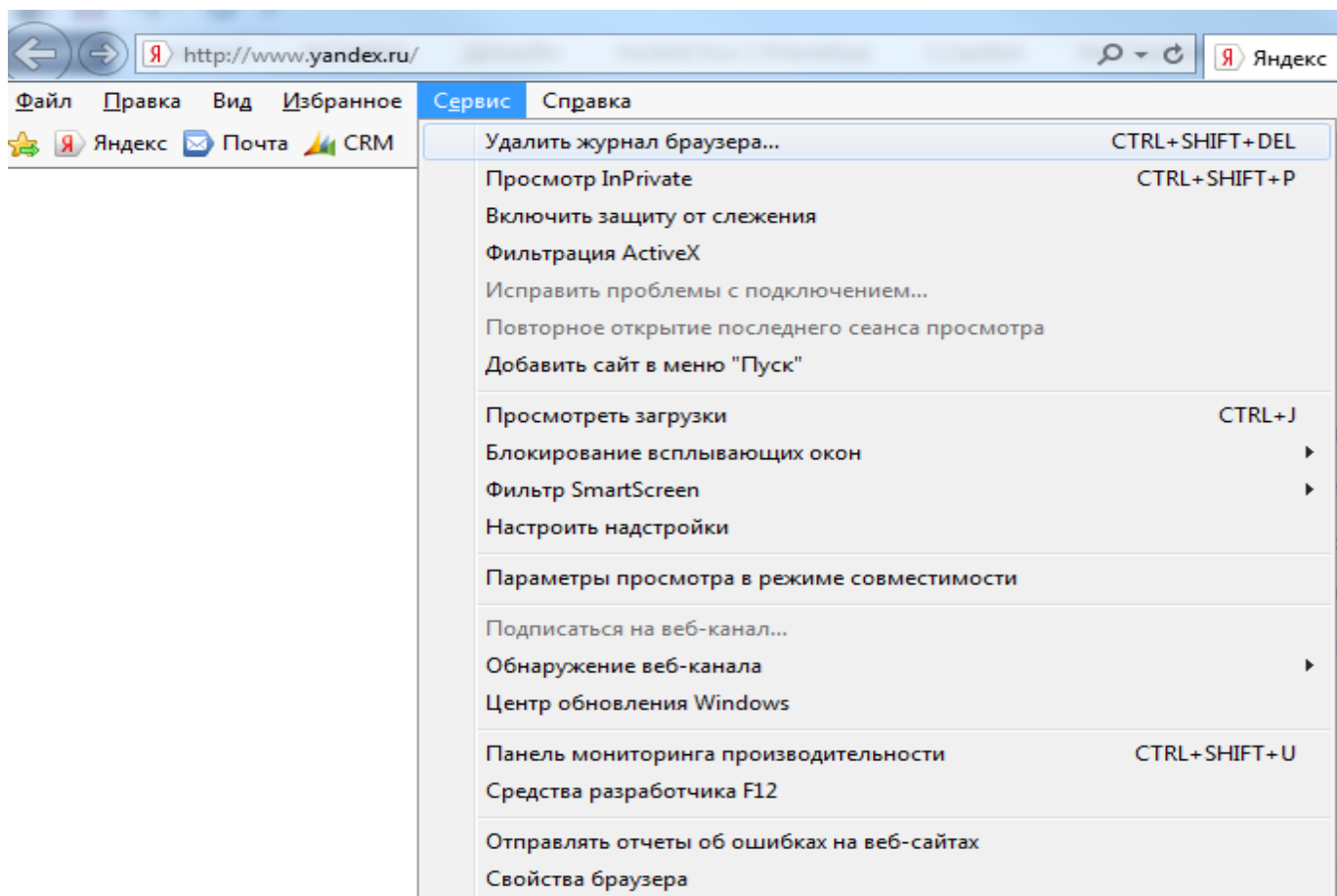


Рисунок 53. Удаление журнала браузера

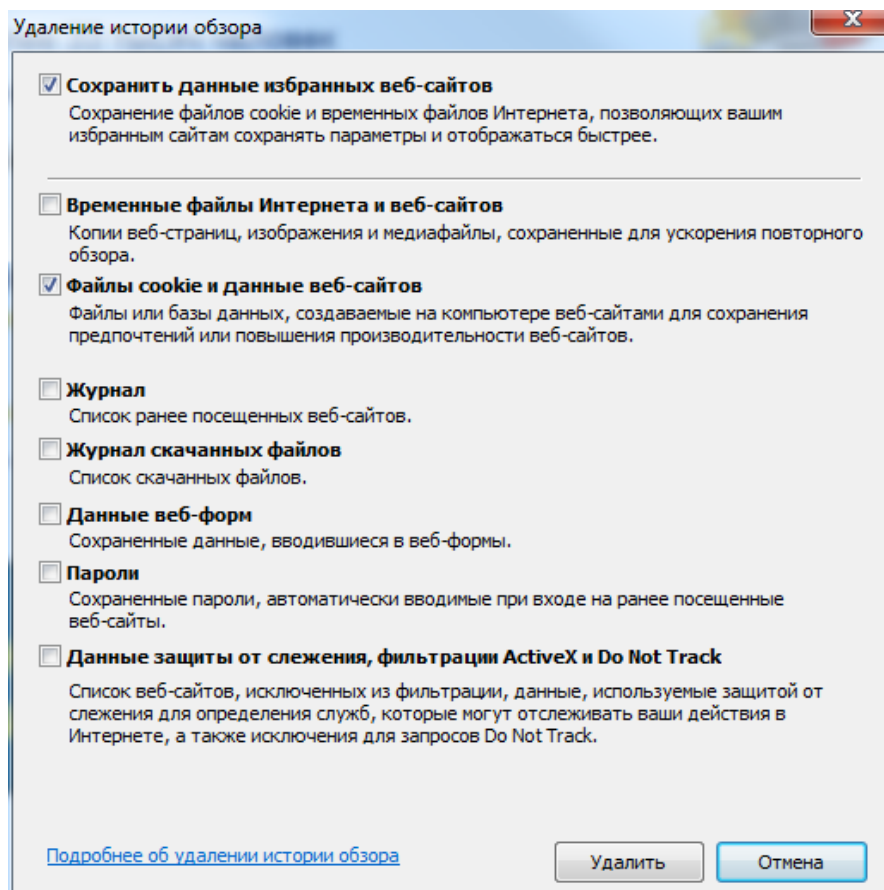


Рисунок 54. Удаление истории обзора

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://stenddss.cryptopro.ru/> и сохраните изменения (см. Рисунок 55):

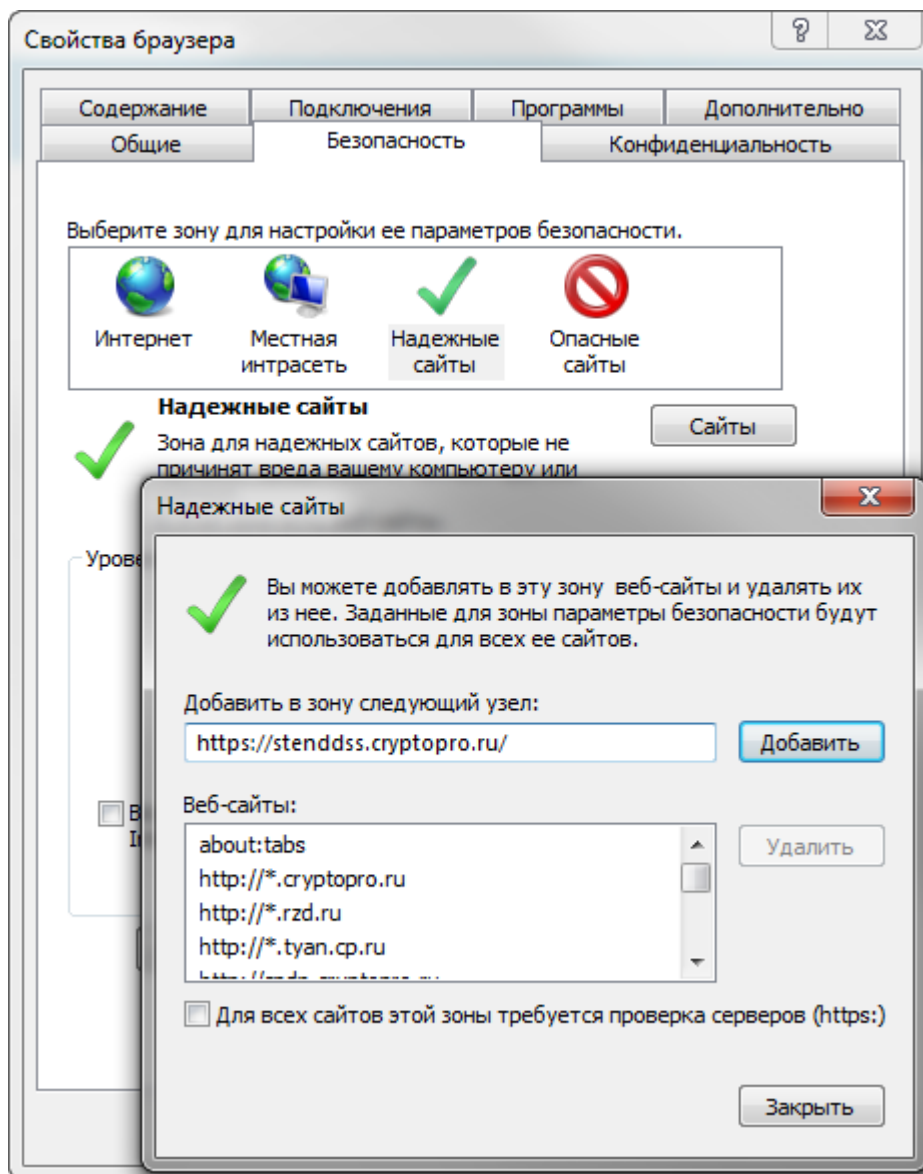


Рисунок 55. Добавление безопасного узла

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 56).

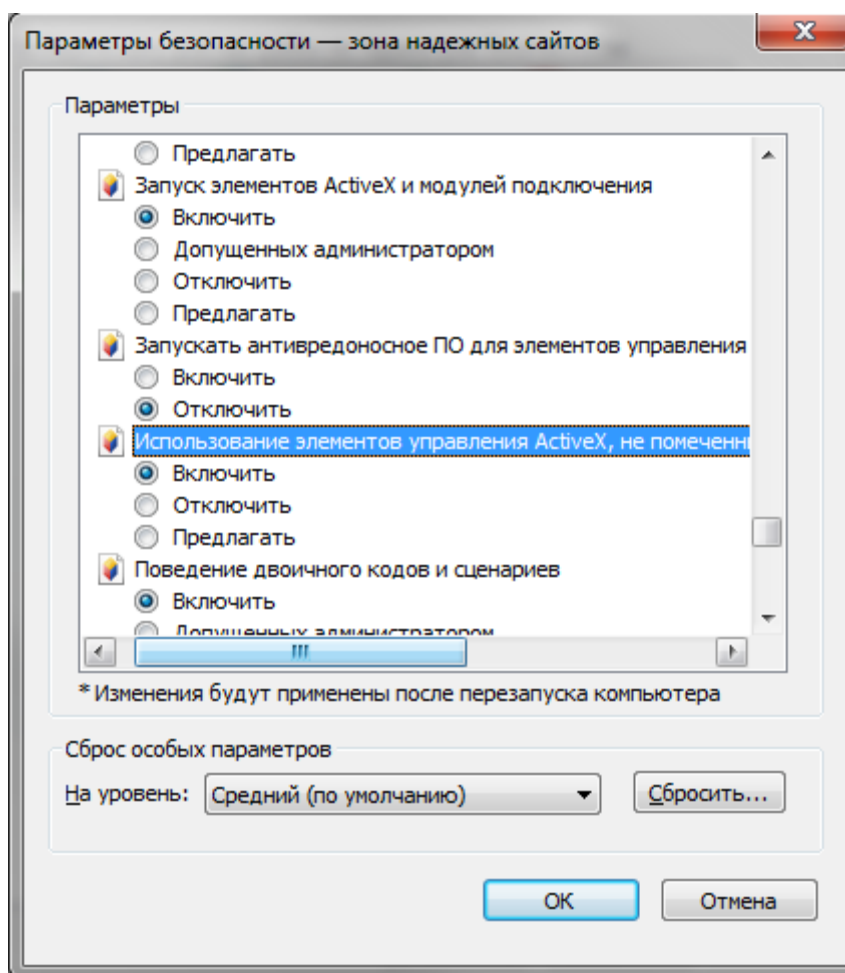


Рисунок 56. Включение элементов ActiveX

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 57, Рисунок 58 и Рисунок 59):

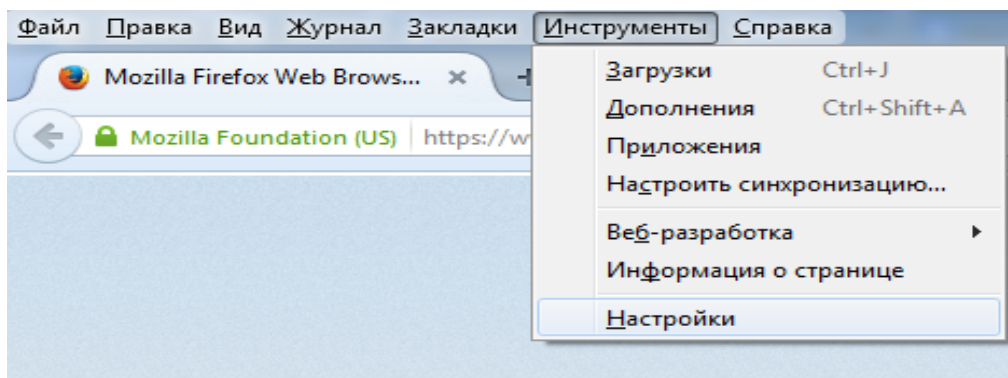


Рисунок 57. Настройки

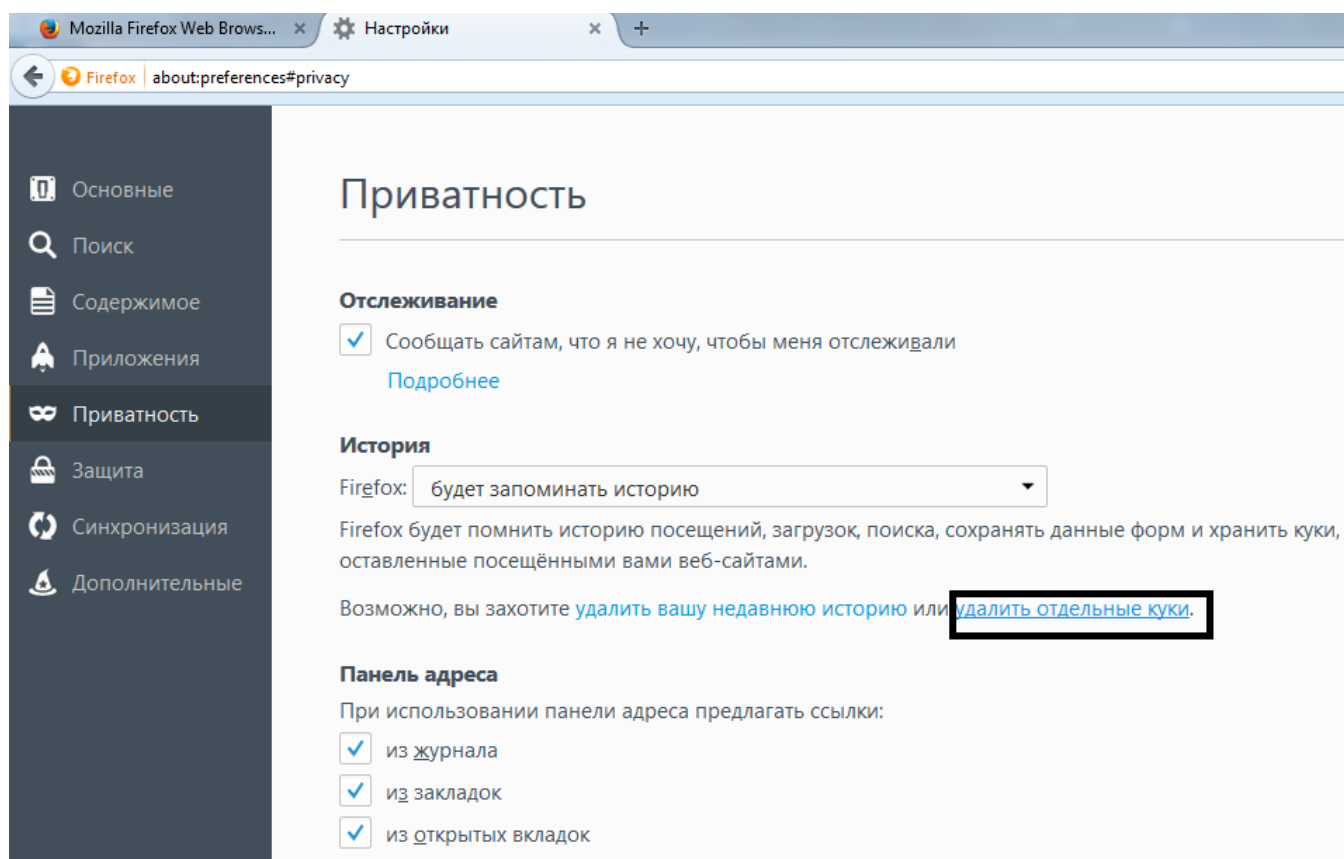


Рисунок 58. Приватность

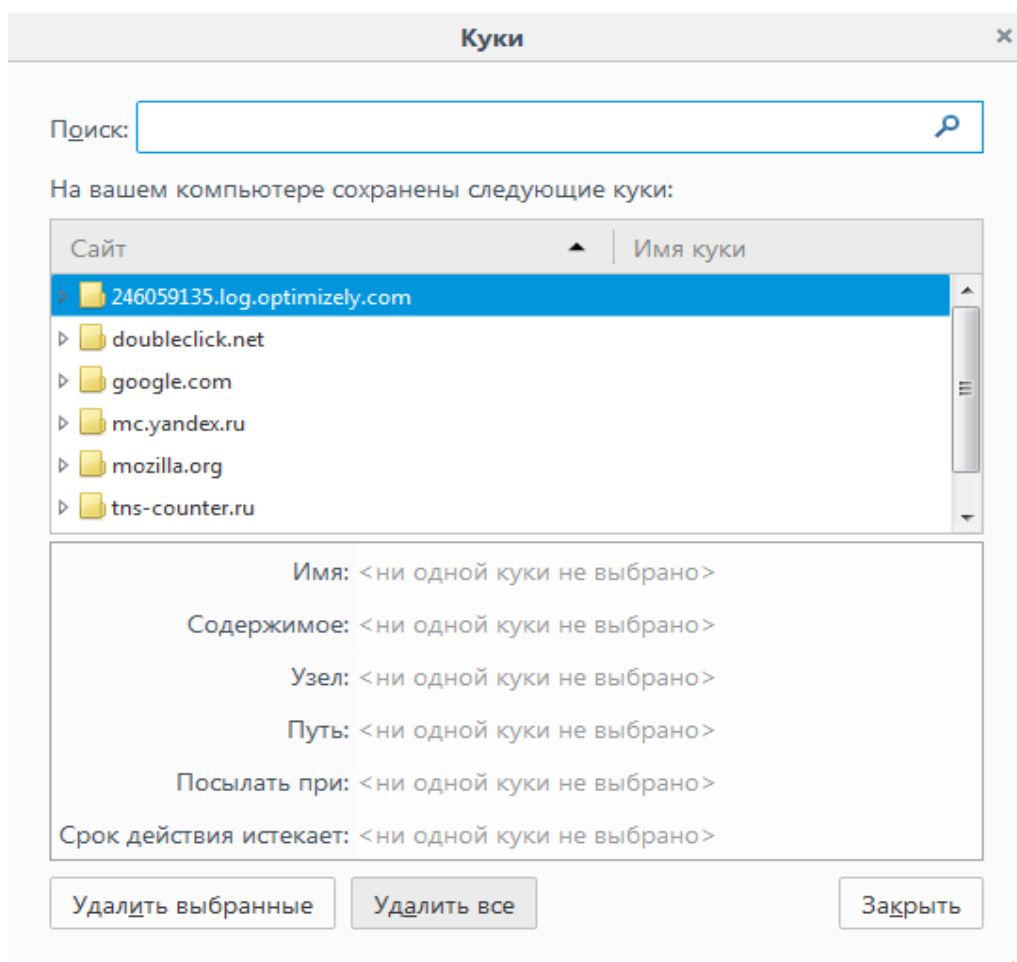


Рисунок 59. Куки

Перечень рисунков

Рисунок 1. Окно аутентификации пользователя	6
Рисунок 2. Окна аутентификации Пользователя в личный кабинет	7
Рисунок 3. Личная информация пользователя	8
Рисунок 4. Смена пароля	9
Рисунок 5. Окно просмотр личной информации	9
Рисунок 6. Завершение редактирования личных данных	10
Рисунок 7. Сертификаты в личном кабинете пользователя СЭП	10
Рисунок 8. Подтверждения операции с цифровым сертификатом	11
Рисунок 9. Форма запроса на сертификат	12
Рисунок 10. Выбор ключевого носителя	13
Рисунок 11. Биологический датчик случайных чисел	13
Рисунок 12. Ввод пароля на доступ к закрытому ключу	14
Рисунок 13. Информация о статусе имеющихся сертификатов	14
Рисунок 14. Информация о запросе на сертификат	15
Рисунок 15. Печатная форма запроса на сертификат	16
Рисунок 16. Выбор принтера для печати запроса на сертификат	17
Рисунок 17. Перечень полученных сертификатов и их статус	18
Рисунок 18. Информация о сертификате и меню управления сертификатом	19
Рисунок 19. Печатная форма запроса на сертификат	20
Рисунок 20. Выгрузка сертификата	21
Рисунок 21. Выбор папки для сохранения сертификата	22
Рисунок 22. Выбор документа для создания электронной подписи	23
Рисунок 23. Выбор файла электронного документа для загрузки	24
Рисунок 24. Просмотр содержания электронного документа	25
Рисунок 25. Выбор формата и параметров электронной подписи	26
Рисунок 26. Выбор параметров электронной подписи CAdES	27
Рисунок 27. Выбор сертификата	28
Рисунок 28. Подготовка документа к подписанию	29
Рисунок 29. Ввод пароля на доступ	29
Рисунок 30. Сохранение подписанного электронного документа	30
Рисунок 31. Выбор папки и названия файла для сохранения подписанного электронного документа	31
Рисунок 32. Окно проверка подписи	32
Рисунок 33. Выбор файла для проверки присоединенной электронной подписи (в составе электронного документа)	33
Рисунок 34. Параметр присоединённой подписи	34
Рисунок 35. Результат проверки электронной подписи	35
Рисунок 36. Выбор файла первоначального документа для проверки отсоединенной электронной подписи	36
Рисунок 37. Проверка сертификата	37
Рисунок 38. Результат проверки сертификата	38
Рисунок 39. Шифрование документа	39
Рисунок 40. Выбор сертификата пользователя	40
Рисунок 41. Выбор документа для шифрования	41
Рисунок 42. Завершение операции шифрования документа	42
Рисунок 43. Сохранение зашифрованного документа	43
Рисунок 44. Расшифровывание документа	44
Рисунок 45. Выбор документа для расшифровывания	44
Рисунок 46. Вывод информации об используемом сертификате	45
Рисунок 47. Отрицательный результат проверки сертификата	45
Рисунок 48. Окно для ввода ПИН-кода доступа к закрытому ключу	46
Рисунок 49. Сохранение расшифрованного документа	46
Рисунок 50. Выбор папки для сохранения расшифрованного документа	47
Рисунок 51. Удаление данных	48
Рисунок 52. Очистка истории	49
Рисунок 53. Удаление журнала браузера	50
Рисунок 54. Удаление истории обзора	50
Рисунок 55. Добавление безопасного узла	51
Рисунок 56. Включение элементов ActiveX	52
Рисунок 57. Настройки	53
Рисунок 58. Приватность	53
Рисунок 59. Куки	54

