ДОСТИГАЕМ ВМЕСТЕ,
РАЗВИВАЯ КАЖДОГО

Утвержден
БАРМ.00003-39 32 03-ЛУ

Система автоматизации процесса управления государственными и муниципальными закупками – Автоматизированный Центр Контроля – Государственный и муниципальный заказ («АЦК-Госзаказ»/«АЦК-Муниципальный заказ»)

Подсистема администрирования системы «АЦК-Госзаказ»/«АЦК-Муниципальный заказ» Электронная подпись

Руководство администратора

БАРМ.00003-39 32 03

Листов 179

АННОТАЦИЯ

подсистемы «Подсистема администрирования системы «АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» автоматизированного рабочего места системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»»

ГОСТ 19.503-79 «Единая система программной документации. РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА. Требования к содержанию и оформлению»

«Система автоматизации процесса управления государственными закупками - Автоматизированный Центр Контроля – Государственный заказ» («АЦК-Госзаказ») зарегистрирована в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам, Свидетельство № 2008610925 от 21 февраля 2008 г. «Система автоматизации процесса управления муниципальными закупками - Автоматизированный Центр Контроля - Муниципальный заказ» («АЦК-Муниципальный заказ») зарегистрирована в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам, Свидетельство № 2009615485 от 02 октября 2009 г.

ООО «БФТ» оставляет за собой право вносить изменения в программное обеспечение без внесения изменений в эксплуатационную документацию.

Оперативное внесение изменений в программное обеспечение отражается в сопроводительной документации к выпускаемой версии.

Документ соответствует версии системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» – 1.39.0. Последние изменения внесены 6/28/2019 г.

СОДЕРЖАНИЕ

1 Общие сведения о программе 7

1.1 Функции программы 8

2 Общие положения 9

2.1 Состав поставки программы 10

2.2 Ограничения текущей версии программы 10

3 Настройка и конфигурирование подсистемы 14

3.1 Настройка серверной части 15

3.2 Настройка клиентской части 15

3.3 Настройка режима работы подсистемы 16

4 Администрирование подсистемы 20

4.1 Импорт сертификатов в систему и привязка к пользователям 21

4.1.1 Автоматическая загрузка сертификатов в систему и привязка к учетным записям пользователей 21

4.1.2 Регистрация и привязка сертификатов к учетным записям пользователей в справочнике «Пользователи системы» 21

4.1.3 Пакетный импорт сертификатов 32

4.1.4 Настройка проверки объектных идентификаторов условий использования сертификатов 35

4.1.5 Настройка оповещения об истечении срока действия сертификата 38

4.2 Отзыв сертификатов пользователей 39

4.2.1 Автоматическая установка (обновление) списков отозванных сертификатов (CRL) 40

4.2.1.1 Управление точками распространения списков отзыва (CRL) 40

4.2.1.2 Алгоритм автоматической установки (обновления) списков отозванных сертификатов (CRL) 42

4.2.2 Отзыв сертификата пользователя администратором 44

4.3 Управление правами пользователя в рамках работы с ЭП 45

4.3.1 Настройка функциональной роли пользователя для работы с ЭП 46
4.3.2 Настройка права выгрузки документов с ЭП в электронный архив 47
4.4 Настройка документооборота 49
4.4.1 Требования к составу подписываемых полей (дайджесту) документов 49
4.4.2 Настройка сценариев обработки документов 49
4.4.2.1 Настройка правил подписания документов на статусах 50
4.4.2.2 Настройка правил проверки ЭП на статусах 62
4.4.3 Настройка подписываемых данных вложений 65
4.4.3.1 Привязка вложений к группам полей при присоединении подписываемых вложений к ЭД 65
5 Использование модуля подсистемы 69
5.1 Подписание электронных документов 70
5.1.1 Подписание документа в списке документов 70
5.1.2 Подписание документа в форме документа 77
5.1.3 Подписание нескольких документов 78
5.2 Проверка подписи электронных документов 81
5.3 Просмотр состава подписанных данных 85
5.4 Печать состава подписанных данных 86
5.5 Просмотр сертификата ЭП документа 86
5.6 Просмотр ЭП вложения в списке вложенных документов 87
5.7 Выгрузка документов с ЭП в электронный архив 88
5.7.1 Выгрузка документа из списка документов 88
5.7.2 Выгрузка документа из формы документа 90
5.7.3 Выгрузка нескольких документов 91
5.7.4 Автоматическая выгрузка документов с ЭП 92
5.7.5 Именование файлов в электронном архиве 95
5.7.6 Выгрузка вложений с ЭП 97
5.8 Удаление документов с ЭП 97
5.8.1 Удаление ЭП документа 98
5.8.2 Удаление ЭП документа в списке документов 99

5.8.3 Удаление ЭП нескольких документов в списке документов 101
5.8.4 Удаление ЭП документа в форме документа 102

6 Порядок контроля юридической значимости электронных документов 104

7 Приложения 106

7.1 Приложение 1. Подписание электронного документа УЭП 107
7.2 Приложение 2. Проверка УЭП электронного документа 107
7.3 Приложение 3. Подписание электронного документа УЭП с доказательствами подлинности 108
7.4 Приложение 4. Проверка УЭП с доказательствами подлинности электронного документа 109
7.5 Приложение 5. Алгоритм подписания ЭД УЭП в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» 111
7.6 Приложение 6. Алгоритм локальной проверки УЭП ЭД в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» 112
7.7 Приложение 7. Алгоритм серверной проверки УЭП ЭД в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» 113
7.8 Приложение 8. Место ЭП в документообороте 114
7.9 Приложение 9. Инструкция по установке КриптоПро CSP 114
7.10 Приложение 10. Инструкция по установке модуля поддержки УЭП 119
7.11 Приложение 11. Инструкция по настройке OCSP-клиента 123
7.12 Приложение 12. Инструкция по настройке TSP-клиента 126
7.13 Приложение 13. Инструкция по установке сертификатов цепочек доверия 129
7.14 Приложение 14. Инструкция по настройке взаимодействия ЭП-сервера с сервером приложений 132
7.15 Приложение 15. Получение сертификата ключа подписи в УЦ 135
7.16 Приложение 16. Инструкция по экспорту сертификата ключа подписи 140
7.17 Приложение 17. Инструкция по установке сертификата ключа подписи 144

7.18 Приложение 18. Инструкция по резервированию закрытых ключей ЭП 150
7.19 Приложение 19. Список диагностических сообщений 156
7.20 Приложение 20. Обобщенная спецификация формата электронного документа 162
7.21 Приложение 21. Инструкция по установке Сервиса ЭП АЦК 163
7.22 Приложение 22. Инструкция по настройке состава дайджеста для электронного документа 170
7.23 Приложение 23. ЭЦП АЦК под Linix 176

1

Общие сведения о программе

1.1 Функции программы

Подсистема администрирования системы «АЦК-Госзаказ»/«АЦК-Муниципальный заказ» включает следующие процедуры:

- настройка и конфигурирование подсистемы;
- администрирование подсистемы;
- использование подсистемы.

2

Общие положения

2.1 Состав поставки программы

Подсистема поставляется в составе Ядра платформы АЦК (версия Ядра АЦК 1.5.2.2 и выше).

- Программные компоненты АЦК:
  - **cades-win32.msi** или **cades-x64.msi** (в зависимости от разрядности ОС) – инсталляционный пакет модуля, который применяется для поддержания работы с усиленной ЭП (с доказательствами подлинности). Устанавливается как на стороне СП, так и на стороне клиента.
  - Серверная часть:
    - **cadessignverifyer.dll** – библиотека, реализующая функции проверки усиленной ЭП (с доказательствами подлинности) на ЭП-сервере, логику взаимодействия с криптопровайдером;
    - **cpsigner.dll** – библиотека, реализующая функции проверки ЭП на ЭП-сервере (поддержка обратной совместимости с версиями подсистемы ЭП, входившими в состав ядер платформы АЦК версий ниже 1.5.2.2);
    - **Server.jar** – java-архив, содержащий классы, реализующие основную логику работы с ЭП (также содержит java-классы, реализующие логику работы других подсистем АЦК).
  - Клиентская часть:
    - **bftlib.ocx** – компонент, реализующий общесистемную логику Ядра АЦК (в т.ч. клиентскую логику работы с ЭП);
    - **sign.ocx** – компонент, реализующий пользовательский интерфейс подсистемы ЭП;
    - **cadessigner.dll** – библиотека, реализующая логику поддержки усиленной ЭП (с доказательствами подлинности) клиентским приложением.

Примечание. *Функционал становится доступен только при пролитии специального xml-файла.*

2.2 Ограничения текущей версии программы

- **Требования к серверу ЭП**

Сервер электронной подписи (ЭП) – это сервер приложений АЦК, на который вынесены функции валидации электронных подписей, сформированных в системе. Вынесение данной функциональности на отдельный сервер способствует масштабированию и балансировке нагрузки на серверную часть системы, а также обеспечивает возможность использования на основном сервере приложений ОС семейства Unix при одновременном использовании ОС класса Windows на сервере ЭП. Это может быть особенно актуально при использовании Windows-версии средства криптографической защиты информации (СКЗИ). Ниже приведены системные требования к конфигурации и программному обеспечению сервера электронной подписи:

Таблица 1 – Системные требования к конфигурации сервера электронной подписи

Максимальное количество	Вид используемой ЭП	Рекомендуемая конфигурация

		CPU	RAM	Ethernet
до 5	Усиленная, Усиленная (XML), Усиленная (со штампом времени)	2 Cores 3GHz Intel Xeon 64 bit	4GB	1Gbit
	Усиленная (с доказательствами подлинности)	4 Cores 3GHz Intel Xeon 64 bit		
до 10	Усиленная, Усиленная (XML), Усиленная (со штампом времени)	4 Cores 3GHz Intel Xeon 64 bit		
	Усиленная (с доказательствами подлинности)	8 Cores 3GHz Intel Xeon 64 bit		
до 20	Усиленная, Усиленная (XML), Усиленная (со штампом времени)	8 Cores 3GHz Intel Xeon 64 bit		
	Усиленная (с доказательствами подлинности)	16 Cores 3GHz Intel Xeon 64 bit		

Примечание. *Для поддержки большего количества пользователей (свыше 20), одновременно выполняющих множественную проверку ЭП, рекомендуется развертывание дополнительного сервера ЭП.*

Таблица 2 – Системные требования к программному обеспечению сервера электронной подписи

Тип сервера	Тип ПО	Программное окружение
Сервер ЭП	ОС	MS Windows 2008/7/2012 R2(64) Oracle Enterprise Linux 5.5 и выше RH Linux AS 5.5 и выше SUSe Linux 10 SP2/11
	JDK (JRE)	Sun Java SE 8 update 40 и выше
	ЭП	При использовании ОС MS Windows: • КриптоПро CSP 3.0-4.0 (версия должна соответствовать установленной на сервере ОС согласно требованиям Компании «КРИПТО-ПРО»). Опционально: КриптоПро TSP Client, КриптоПро OCSP Client. • ViPNet CSP 3.2-4.2. При использовании ОС Linux, ОС MS Windows: • КриптоПро JCP 2.0.

Примечание. *При использовании видов ЭП: Усиленная, Усиленная (XML), Усиленная (со штампом времени).*

Примечание*. Инструкция по настройке взаимодействия ЭП-сервера с сервером приложений приведена в* *Приложении 14* 132 *к настоящему документу.*

- **Требования к клиентскому рабочему месту**
  - **Требования к программному окружению при использовании криптографических функций**

При использовании функций наложения ЭП и аутентификации по сертификату на компьютере должно быть установлено следующее программное обеспечение:

Таблица 3 – Требования к программному окружению при использовании криптографических функций

Минимальные требования			Рекомендуемые требования	
СКЗИ: КриптоПро CSP 3.0-4.0 (версия должна соответствовать установленной на сервере ОС согласно требованиям Компании «КРИПТО-ПРО»), КриптоПро ФКН CSP 3.9 Опционально: КриптоПро TSP Client, КриптоПро OCSP Client			СКЗИ: ViPNet CSP 3.2-4.2	
Windows-клиент				
ОС	Windows Vista/7/8/10		ОС	Windows Vista/7/10
Web-клиент				
ОС	Windows Vista/7/8/10	Scientific Linux 7.2	ОС	Windows Vista/7/10
Доп. ПО	Сервис ЭП АЦК 1.0.3.9	плагин nmsigner-1.0.9-1	Доп. ПО	Сервис ЭП АЦК 1.0.3.9

Примечание. *64х разрядная операционная система рекомендуется при оперативной памяти не меньше 4Gb.*

Примечание. *Сервис электронной подписи АЦК – программное окружение, обеспечивающее использование криптографических функций при работе в браузерах Google Chrome, Microsoft Edge, Mozilla Firefox и Internet Explorer под ОС Windows.*

Примечание. *Плагин – программное окружение, обеспечивающее использование криптографических функций при работе только в браузере Google Chrome под ОС Linux.*

Примечание. *При использовании функций наложения ЭП на прикрепленные к ЭД файлы (вложения) рекомендуемый размер подписываемого файла не должен превышать 20 Мб.*

- **Требования к программному окружению при использовании протокола HTTPS и алгоритмов шифрования ГОСТ**

При использовании криптографического протокола HTTPS в соответствии с требованиями ГОСТ к алгоритмам шифрования данных на компьютере должно быть установлено следующее программное обеспечение:

Таблица 4 – Требования к программному окружению при использовании протокола HTTPS и алгоритмов шифрования ГОСТ

При использовании СКЗИ КриптоПро	При использовании СКЗИ ViPNet
ОС: Windows Vista/7/8 СКЗИ: КриптоПро CSP 3.0-4.0 (версия должна соответствовать установленной на сервере ОС согласно требованиям Компании “КРИПТО-ПРО”), КриптоПро ФКН CSP 3.9 Опционально: КриптоПро TSP Client, КриптоПро OCSP Client Браузер: КрипроПро Fox 45.1, MS Internet Explorer 10.0, 11.0	ОС: Windows Vista/7 СКЗИ: ViPNet CSP 3.2-4.2 Браузер: MS Internet Explorer 10.0, 11.0

Примечание. *64х разрядная операционная система рекомендуется при оперативной памяти не меньше 4Gb.*

Примечание. *Для работы с ЭП в Google Chrome, Mozilla Firefox, Internet Explorer необходимо установить Сервис ЭП АЦК. Инструкция по установке Сервиса ЭП АЦК приведена в* *Приложении 21* 163 *к настоящему документу.*

3

Настройка и конфигурирование подсистемы

3.1 Настройка серверной части

Для настройки серверной части необходимо выполнить следующие действия:

- Установить/обновить сервер системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»».

Примечание. *Описание установки и обновления сервера системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» содержится в документации «».*

- Определить вариант использования сервера ЭП (инфраструктуру системы), будет ли он объединен с сервером приложений АЦК или будет вынесен отдельно.
- Если ЭП-сервер объединен с сервером приложений, то:
  - установить СКЗИ **КриптоПро CSP** (**Приложение 9** 114);
  - если планируется использование УЭП с доказательствами подлинности, то:
    - установить **Модуль поддержки УЭП** (**Приложение 10** 119);
    - если планируется добавлять штамп времени и цепочки отзыва сертификатов на сервере, то:
- произвести настройку OCSP-клиента (**Приложение 11** 123);
- произвести настройку TSP-клиента (**Приложение 12** 126).
    - если формирование УЭП с доказательствами подлинности производится полностью на клиенте, то настройку OCSP-клиента и TSP-клиента допустимо не производить (лицензии на OCSP-клиент и TSP-клиент не требуются).
  - установить сертификаты цепочек доверия, полученные от УЦ (**Приложение 13** 129).
- Если сервер ЭП вынесен отдельно, то на нем:
  - установить СКЗИ **КриптоПро CSP** (**Приложение 9** 114);
  - если планируется использование УЭП с доказательствами подлинности, то:
    - установить **Модуль поддержки УЭП** (**Приложение 10** 119);
    - если планируется добавлять штамп времени и цепочки отзыва сертификатов на сервере, то:
    - произвести настройку OCSP-клиента (**Приложение 11** 123);
    - произвести настройку TSP-клиента (**Приложение 12** 126).
  - установить сертификаты цепочек доверия, полученные от УЦ (**Приложение 13** 129);
  - настроить взаимодействие ЭП-сервера с сервером приложений (**Приложение 14** 132).
- Настроить документооборот в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» 49.

3.2 Настройка клиентской части

Для настройки клиентской части (клиентского АРМа) необходимо выполнить следующие действия:

- Установить/обновить приложение-клиент системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»».

Примечание. *Описание установки и обновления сервера системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» содержится в документации «».*

- Установить СКЗИ **КриптоПро CSP** (**Приложение 9** 114).
- Если планируется использование УЭП, то:
  - установить **Модуль поддержки УЭП** (**Приложение 10** 119);
  - если на настраиваемом клиентском рабочем месте планируется подписывать документы УЭП с доказательствами подлинности, то:
    - произвести настройку OCSP-клиента (**Приложение 11** 123);
    - произвести настройку TSP-клиента (**Приложение 12** 126).
  - если на настраиваемом рабочем месте не планируется подписывать документы УЭП с доказательствами подлинности (только проверять подписи, либо формирование доказательств подлинности производится на сервере), то допустимо не проводить настройку OCSP-клиента и TSP-клиента (лицензии на OCSP-клиент и TSP-клиент не требуются).
- Установить сертификаты цепочек доверия, полученные от УЦ (**Приложение 13** 129).
- Получить и установить сертификат ключа подписи:

○ если сертификат ключа подписи получается в процессе непосредственного соединения с УЦ (**Приложение 15** 135);
○ если сертификат получается в виде файла по электронной почте или лично в УЦ (**Приложение 17** 144).

Внимание! *Если планируется использование УЭП с доказательствами подлинности перед установкой сертификата необходимо убедиться, что он удовлетворяет следующим требованиям:*
- поле ***Назначение ключевой пары (KeyUsage)*** *ключа подписи содержит значение* ***Цифровая подпись****;*
- поле ***Доступ к информации о центрах сертификации (AIA)*** *содержит адреса доступных в сети OCSP-серверов (Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1));*
- поле ***Алгоритм подписи*** *содержит значение* ***ГОСТ Р 34.11/34.10-2012*** *(используются ГОСТ-алгоритмы).*
Если сертификат ключа подписи не содержит информации об адресе OCSP-службы, то допустимо указать полученный от поставщика сертификата ключа подписи адрес OCSP-службы в политиках безопасности OCSP-клиента.

3.3 Настройка режима работы подсистемы

Настройка режима работы подсистемы выполняется в пункте меню **Сервис→**, группа настроек :

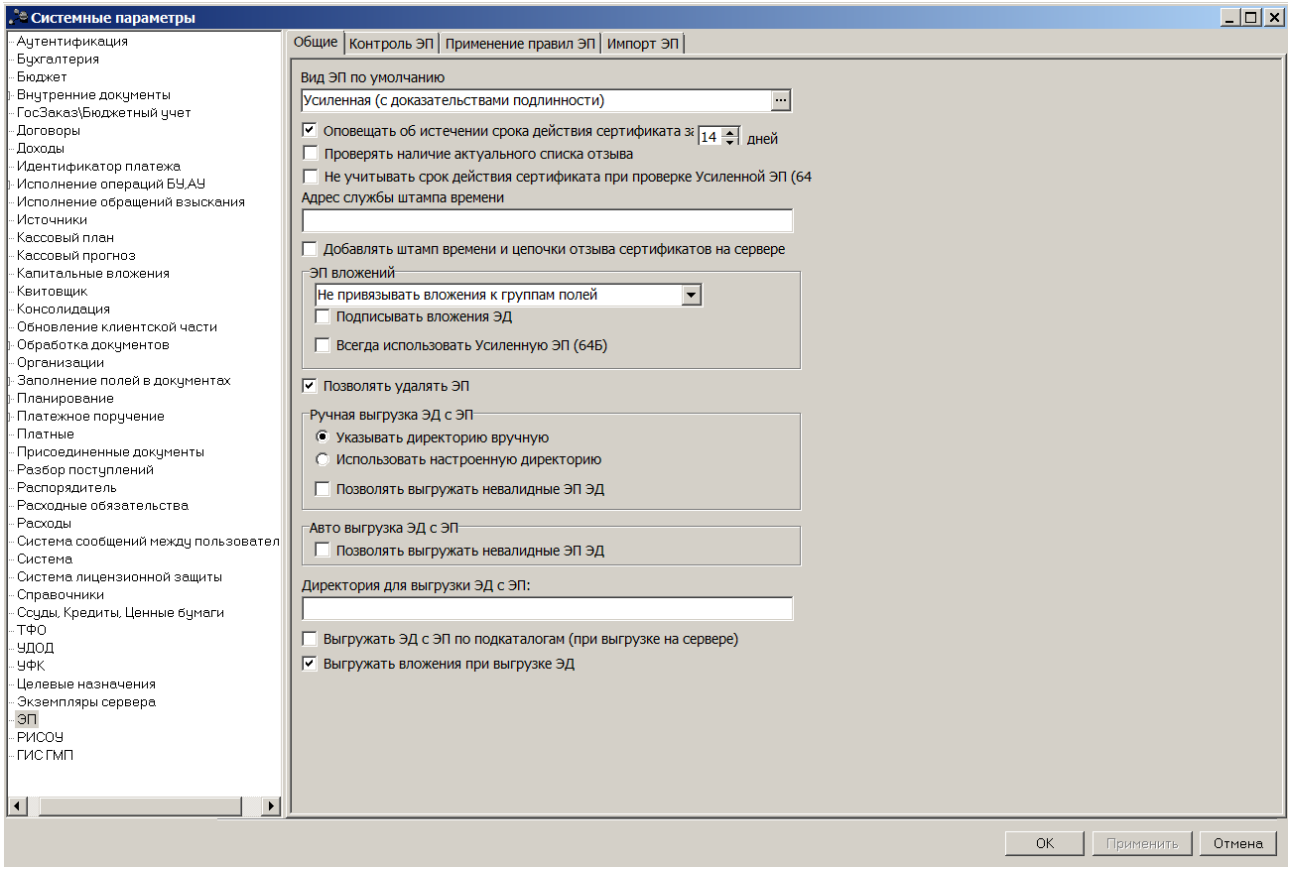

Рисунок 1 – Настройка системных параметров ЭП

Примечание. *Подробное описание настройки системных параметров работы с ЭП приведено в документации «».*

В системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» используются следующие виды ЭП:

- *Усиленная* – используется для формирования усиленной квалифицированной ЭП, содержащей подписываемые данные документа, атрибуты ЭП и текст подписи.

Примечание. *При выполнении процедур подписания и проверки ЭП вида* ***Усиленная*** *проверка наличия используемого для формирования ЭП сертификата пользователя в имеющемся списке отзыва (а также наличие и актуальность самого списка отзыва) и целостности и актуальности всей цепочки доверия для используемого сертификата осуществляется при включенном системном параметре* ***Проверять наличие актуального списка отзыва*** *(по умолчанию включен).*

Примечание. *При использовании ЭП вида* ***Усиленная*** *подписывается хэш-код, сформированный из дайджеста электронного документа/вложения электронного документа. При использовании видов ЭП, отличных от вида* ***Усиленная****, подписывается дайджест электронного документа/вложения электронного документа.*
Исходя из указанной специфики механизма наложения целесообразно использовать ЭП вида ***Усиленная*** *для подписания вложений электронных документов. Подписание вложений с использованием вида* ***Усиленная****, независимо от установленного в сертификате вида ЭП, настраивается с помощью системного параметра* ***Всегда использовать Усиленную ЭП (64Б)*** *группы параметров* ***ЭП вложений****.*

- *Усиленная (с доказательствами подлинности)* – используется для формирования усовершенствованной квалифицированной ЭП, содержащей подписываемые данные документа, атрибуты ЭП и текст подписи, а также подписываемый штамп времени, цепочку доверия и OCSP-ответы.
- *Усиленная (XML)* – предназначена для формирования усиленной квалифицированной ЭП в формате XMLDSig, накладываемой на электронные документы.

Примечание. *При выполнении процедур подписания и проверки ЭП вида* ***Усиленная (XML)*** *проверка наличия используемого для формирования ЭП сертификата пользователя в имеющемся списке отзыва (а также наличие и актуальность самого списка отзыва) и целостности и актуальности всей цепочки доверия для используемого сертификата осуществляется при включенном системном параметре* ***Проверять наличие актуального списка отзыва*** *(по умолчанию включен).*

- *Усиленная (со штампом времени)* – предназначена для формирования усовершенствованной квалифицированной ЭП в формате XAdES-T, накладываемой на электронные документы, в том числе выгружаемыев ГИС ГМП. Содержит подписываемый штамп времени.
- *Усиленная (с атрибутами)* – используется для формирования усиленной квалифицированной ЭП в формате CAdES-BES, накладываемой на электронные документы лицом, уполномоченным на проведение контроля в соответствии с ч. 5 ст. 99 Федерального закона от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

Задать по умолчанию вид ЭП для импортируемых в систему сертификатов пользователей позволяет системная настройка **Вид ЭП для новых сертификатов (по умолчанию)**. Значение системной настройки автоматически подставляется в поле **Вид ЭП формы создаваемых (импортируемых) сертификатов пользователей** 24. По умолчанию настройка имеет значение Усиленная (с доказательствами подлинности).

Значение системной настройки выбирается из справочника *Виды ЭП*:

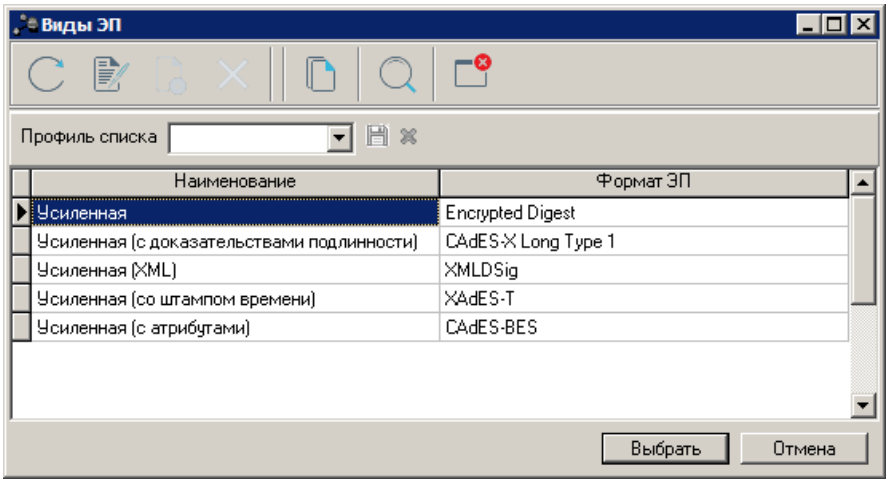

Рисунок 2 – Справочник «Виды ЭП»

Данные в справочнике представлены в табличной форме и имеют атрибуты:

- **Наименование** – наименование вида ЭП.
- **Формат ЭП** - формат ЭП из справочника *Форматы ЭП*.

Значения справочника заданы по умолчанию и доступны только для просмотра:

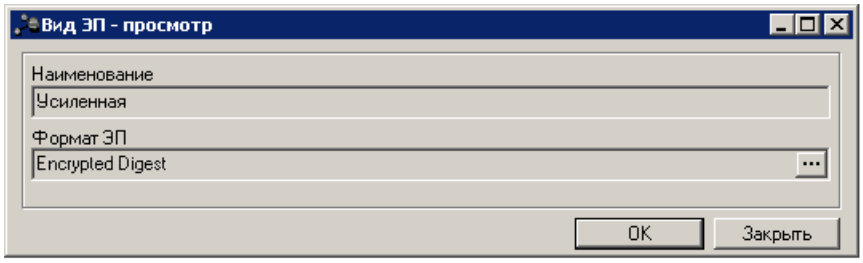

Рисунок 3 – Форма просмотра записи справочника «Виды ЭП»

4

Администрирование подсистемы

4.1 Импорт сертификатов в систему и привязка к пользователям

Для работы пользователя с ЭП необходимо импортировать в систему выданный ему в УЦ сертификат ключа подписи и осуществить привязку сертификата к учетной записи данного пользователя. Регистрация и привязка сертификатов к учетным записям пользователей производится в справочнике *Пользователи системы*. Регистрацию и привязку сертификатов к учетным записям пользователей через справочник *Пользователи системы* могут осуществлять пользователи, имеющие администраторские права и доступ к изменению пользовательской информации.

Внимание! *Для использования в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» сертификат пользователя должен отвечать требованиям, установленным следующими документами:*

– *Федеральный закон РФ от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи».*

– *Приказ ФСБ РФ от 27 декабря 2011 г. №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».*

– *Международный стандарт RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».*

– *Международный стандарт RFC 4491 «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile».*

4.1.1 Автоматическая загрузка сертификатов в систему и привязка к учетным записям пользователей

Автоматическая загрузка сертификатов в систему ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» и привязка сертификатов к учетным записям пользователей выполняется по заданию Планировщика *CertDownloader* (пункт меню). График запуска (периодичность выполнения) задания настраивается в справочнике *Расписание* (пункт меню **Планировщик→Расписание**).

Примечание. *Подробное описание настройки заданий Планировщика см. в документации:*

- «»;

- «».

4.1.2 Регистрация и привязка сертификатов к учетным записям пользователей в справочнике «Пользователи системы»

Регистрировать и привязывать сертификаты к учетным записям пользователей через справочник *Пользователи системы* могут пользователи с администраторскими правами и настроенным доступом к редактированию пользовательской информации. Для регистрации сертификата пользователя с помощью справочника *Пользователи системы* необходимо выполнить следующие действия:

1. Открыть справочник *Пользователи системы* (→**Пользователи системы**):

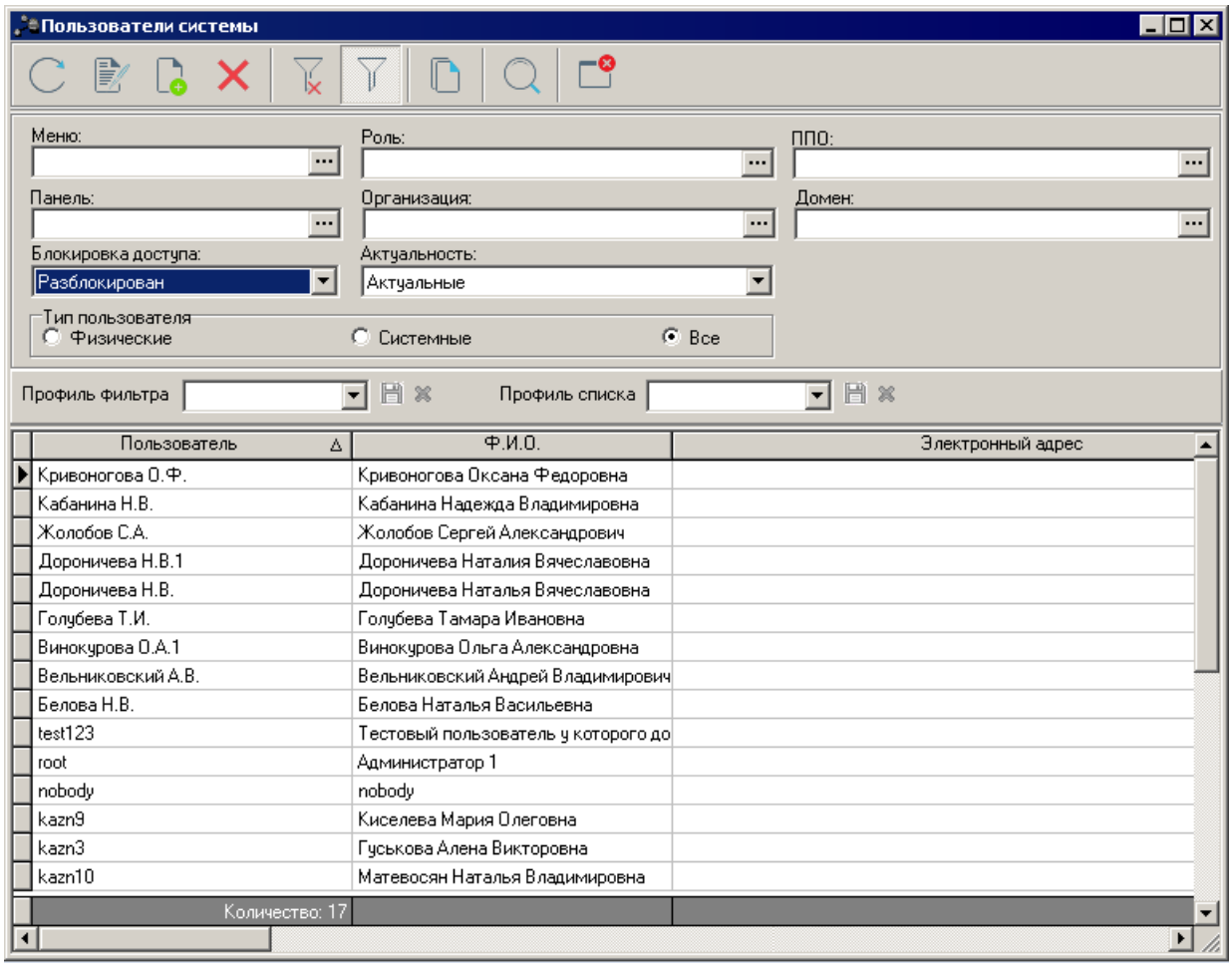

Рисунок 4 – Справочник «Пользователи системы»

2. Открыть на редактирование учетную запись пользователя, для которого регистрируется сертификат, с помощью кнопки  (**Редактировать**) панели инструментов формы или клавиши **<F4>** клавиатуры.
3. В открывшейся форме *Редактирование пользователя системы* на закладке **Сертификаты** содержится список сертификатов пользователя, которые используются при подписании документов ЭП:

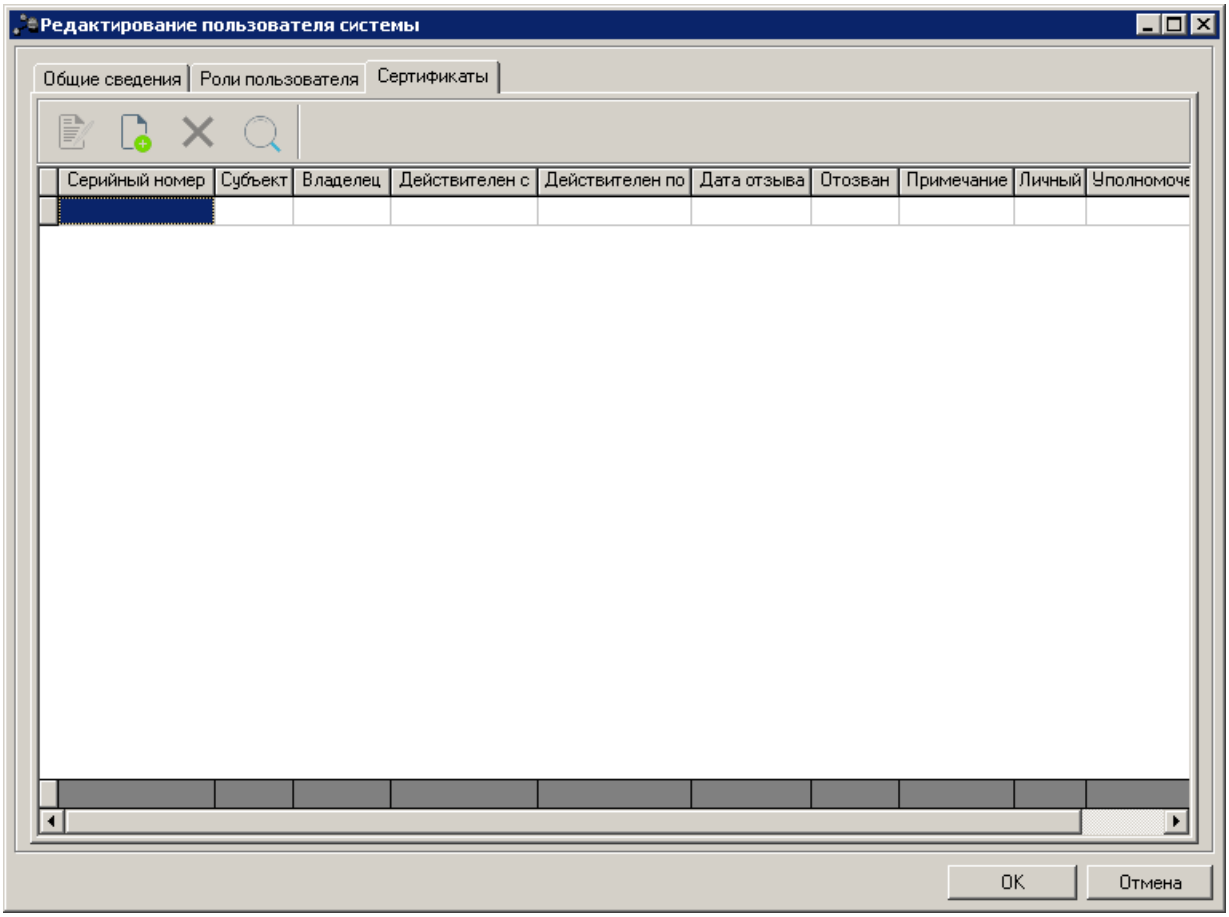

Рисунок 5 – Форма учетной записи пользователя, закладка «Сертификаты»

Над списком сертификатов находится панель инструментов. На ней располагаются стандартные функциональные кнопки, с помощью которых можно выполнить действия: добавить новый сертификат, отредактировать данные о сертификате, удалить и найти сертификат в списке.

4. Для добавления нового сертификата необходимо нажать кнопку  (**Новый**) панели инструментов окна или клавишу **<F9>**.
5. В открывшемся справочнике нажать кнопку  (**Новый**) на панели инструментов окна или клавишу **<F9>**:

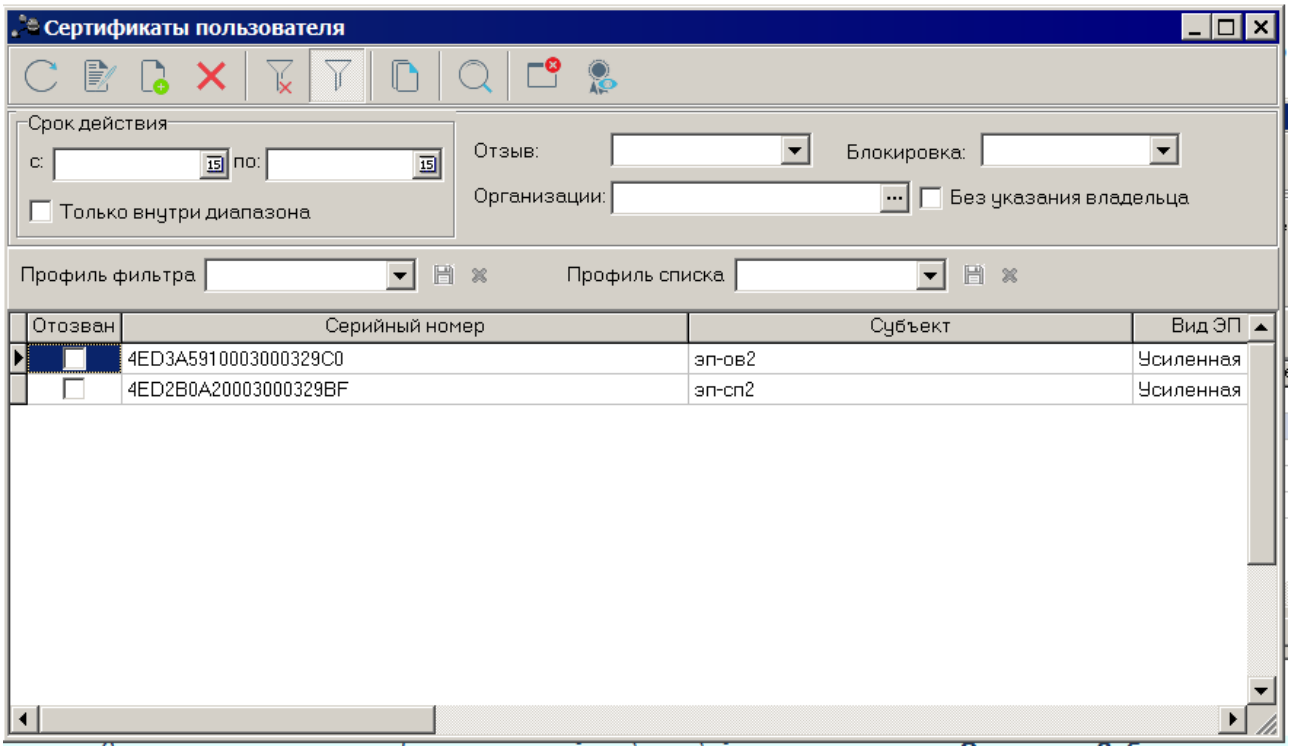

Рисунок 6 – Справочник «Сертификаты пользователей»

6. В открывшемся окне регистрации сертификата пользователя нажать кнопку **Импорт**:

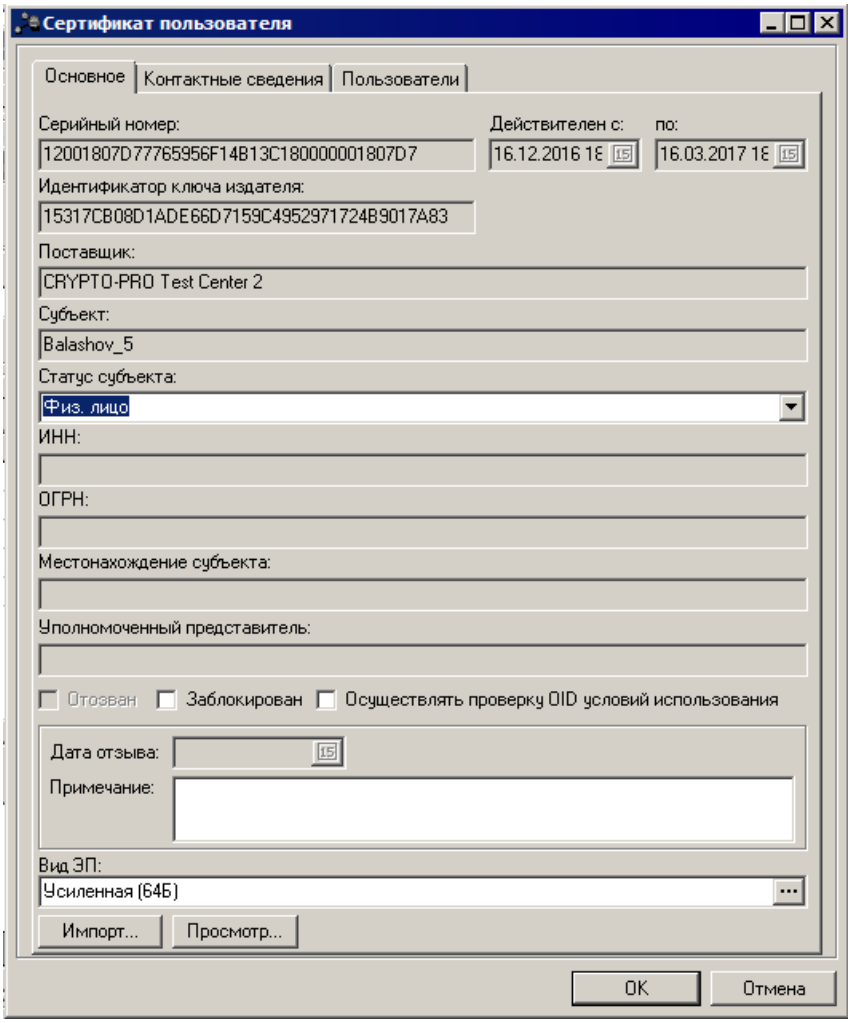

Рисунок 7 – Форма регистрации нового сертификата пользователя

7. С помощью стандартного диалогового окна Windows выбрать файл импортируемого сертификата:

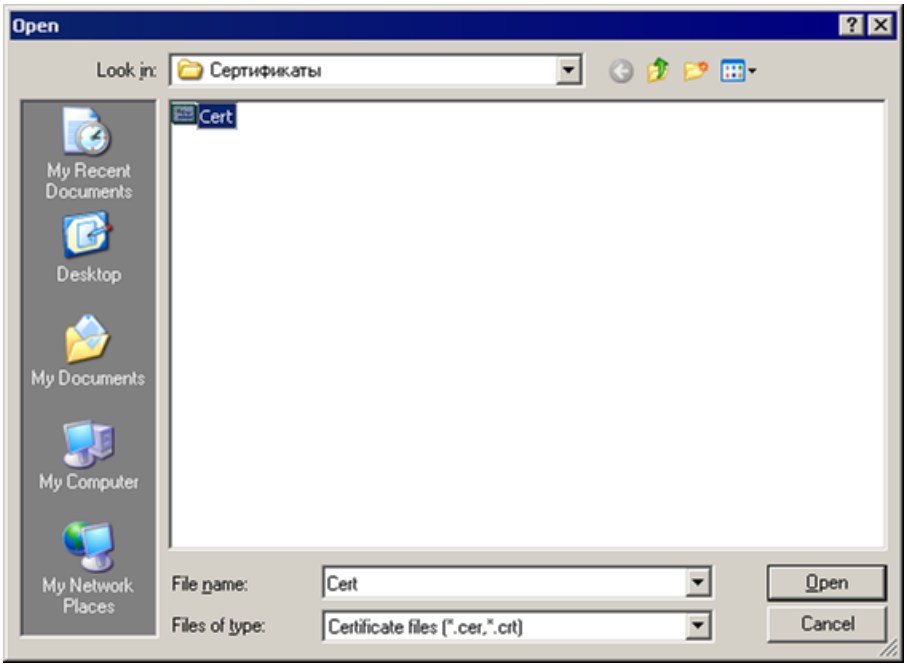

Рисунок 8 – Форма выбора сертификата

Импортируемый сертификат должен быть создан (получен) в системе «КриптоПро». Если импортируемый сертификат использует несоответствующий требованиям ГОСТ алгоритм подписи на экране появится сообщение:

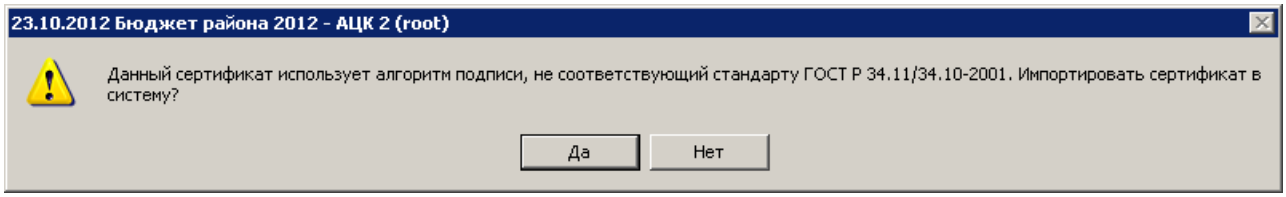

Рисунок 9 – Сообщение о несоответствии алгоритма подписи импортируемого сертификата требованиям ГОСТ

Чтобы продолжить процедуру регистрации сертификата, необходимо нажать кнопку **Да** в окне сообщения.
Форма сертификата содержит закладки **Контактные сведения** и **Пользователи**. Закладка **Контактные сведения** формы сертификата пользователя заполняется автоматически после выбора сертификата:

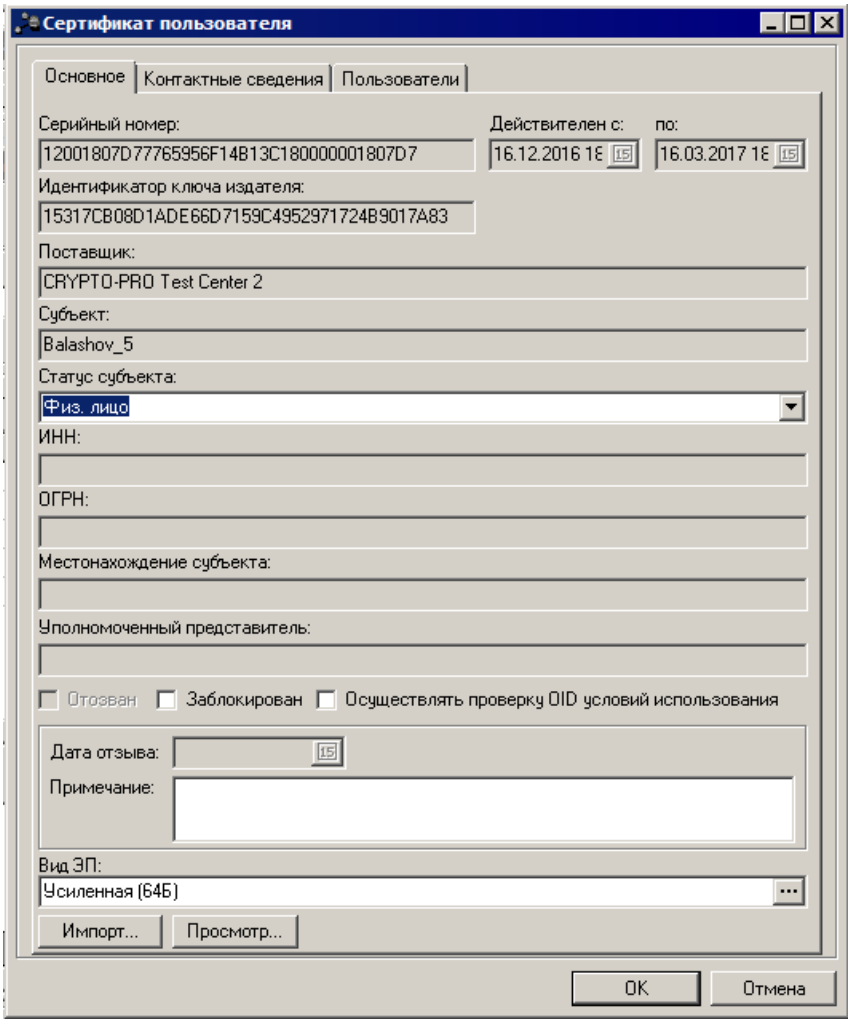

Рисунок 10 – Форма регистрации нового сертификата пользователя

На закладке **Основное** содержатся поля:

- **Серийный номер** – серийный номер сертификата пользователя. Заполняется автоматически данными из сертификата пользователя.
- **Действителен с ... по** – период действия сертификата. Заполняется автоматически данными из сертификата пользователя.
- **Идентификатор ключа изделия** – значение идентификатора ключа центра сертификатов. Заполняется автоматически данными из сертификата пользователя.
- **Поставщик** – название УЦ, который выдал сертификат ключа подписи. Заполняется автоматически данными из сертификата пользователя.
- **Субъект** – физическое лицо, на имя которого УЦ выдал сертификат ключа подписи и который владеет закрытым ключом ЭП. Заполняется автоматически данными из сертификата пользователя.
- **Статус субъекта** – заполняется автоматически при импорте нового сертификата в справочник и зависит от значения поля **ОГРН**. Если поле **ОГРН** не заполнено, указывается значение *Физ. лицо*. Если поле **ОГРН** заполнено, указывается значение *Юр. лицо*. Обязательное для заполнения. Доступное для редактирования.
- **ИНН** – ИНН субъекта сертификата. Заполняется автоматически данными из сертификата пользователя.
- **ОГРН** – ОГРН субъекта сертификата. Заполняется автоматически данными из сертификата пользователя.
- **Местонахождение** – местонахождение субъекта сертификата. Заполняется автоматически

данными из сертификата пользователя.

- **Уполномоченный представитель** – ФИО уполномоченного представителя владельца сертификата. Заполняется автоматически данными из сертификата пользователя.
- **Отозван** - параметр активируется автоматически при установке (обновлении) списка отозванных сертификатов, если сертификат входит в устанавливаемый список и имеет соответствующую точку распространения. Недоступен для редактирования.

Примечание. *Более подробно автоматический отзыв сертификатов при установке (обновлении) списков отзыва рассмотрен в разделе* ***Автоматическая установка списков отозванных сертификатов (CRL)*** 40

- **Заблокирован** – параметр используется администратором для отзыва сертификата в ручном режиме. Доступен для редактирования.

Примечание. *Более подробно отзыв сертификатов пользователей администратором в ручном режиме рассмотрен в разделе* ***Отзыв сертификата пользователя администратором*** 44

- **Осуществлять проверку OID условий использования** – параметр используется для настройки проверки объектных идентификаторов условий использования сертификата при наложении ЭП.

Примечание. *Более подробно работа параметра рассмотрена в разделе* ***Настройка проверки объектных идентификаторов условий использования сертификатов*** 35

- **Дата отзыва -** дата публикации установленного в системе списка отозванных сертификатов, в который входит данный сертификат. Заполняется автоматически значением поля **Дата публикации** соответствующей записи справочника *Точки распространения списков* отзыва при активации параметра **Отозван**. Обязательное для заполнения, если активирован параметр **Отозван**. Недоступно для редактирования.
- **Примечание** – причина отзыва сертификата. Обязательное для заполнения при активации параметра **Заблокирован**. Доступно для редактирования.
- **Вид ЭП** – вид электронной подписи. Поле заполняется автоматически при импорте сертификата значением настройки **Вид ЭП для новых сертификатов (по умолчанию)** (**Сервис→**, группа параметров , закладка **Общие**). Доступно для редактирования.

Для просмотра загруженного в систему сертификата используется кнопка **Просмотр**. При нажатии кнопки откроется форма загруженного сертификата:

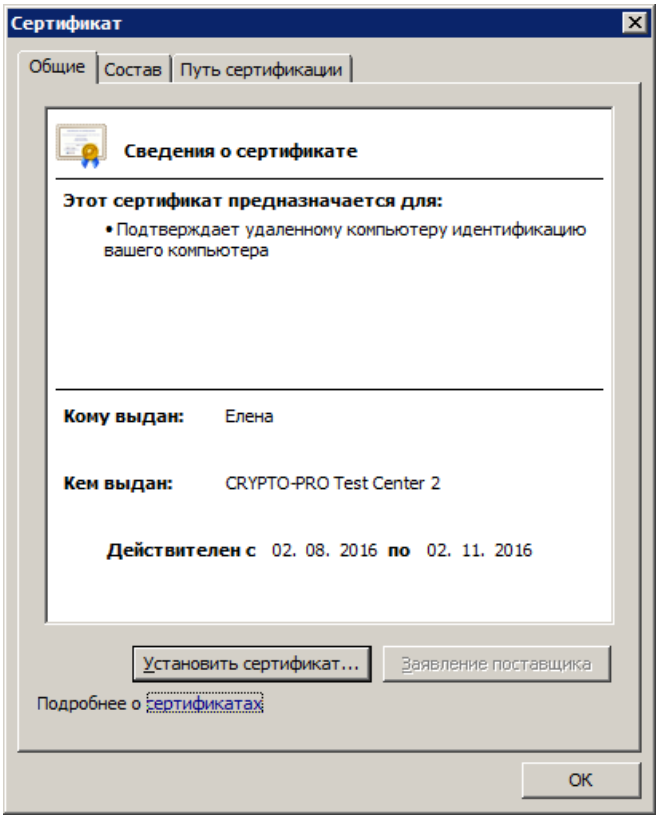

Рисунок 11 –Просмотр сертификата

На закладке **Контактные сведения** формы редактирования сертификата содержатся поля:

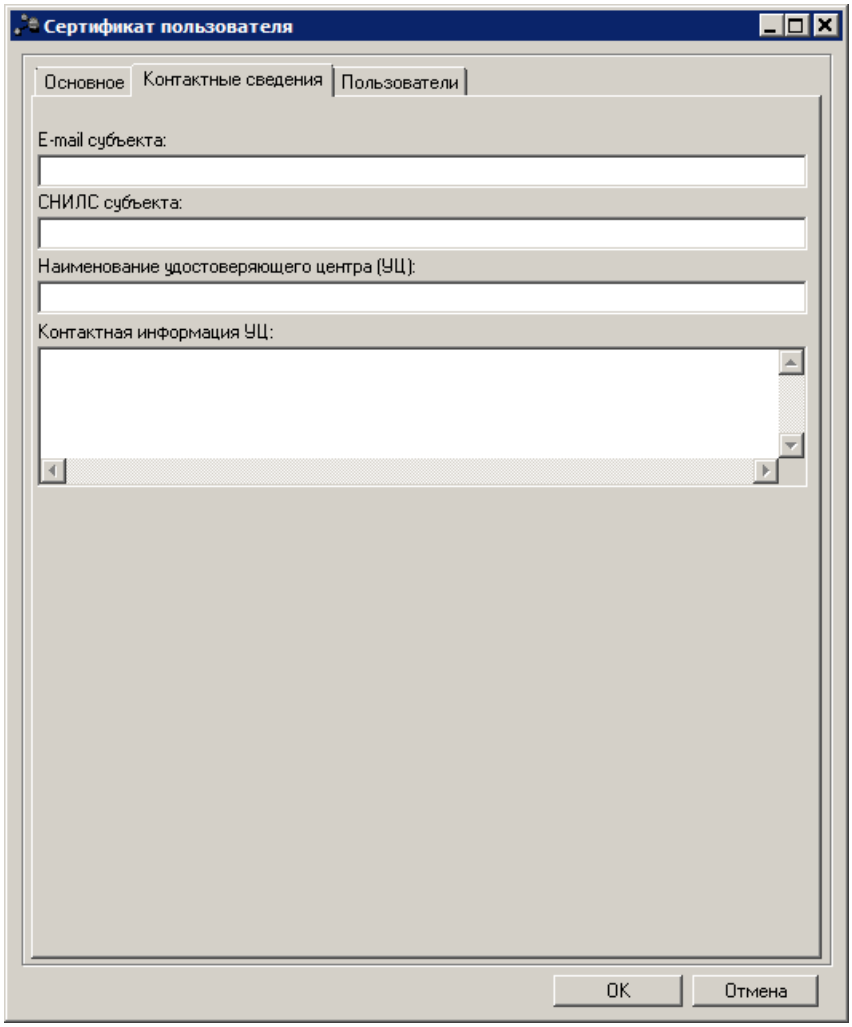

Рисунок 12 – Форма редактирования импортированного сертификата пользователя, закладка «Контактные сведения»

- **E-mail субъекта** – адрес электронной почты для связи с субъектом сертификата. Доступно для редактирования. Необязательное для заполнения.
- **СНИЛС субъекта** – СНИЛС субъекта сертификата для однозначной идентификации субъекта сертификата. Доступно для редактирования. Необязательное для заполнения.
- **Наименование удостоверяющего центра (УЦ)** – наименование аккредитованного удостоверяющего центра, выдавшего сертификат ключа подписи. Доступно для редактирования. Необязательное для заполнения.
- **Контактная информация УЦ** - местонахождение аккредитованного удостоверяющего центра, выдавшего сертификат ключа подписи, и контакты для получения открытых ключей и корневых сертификатов. Доступно для редактирования. Необязательное для заполнения.

На закладке **Пользователи** формы редактирования сертификата указывается владелец сертификата и формируется список пользователей, которые могут использовать его для подписания электронных документов:

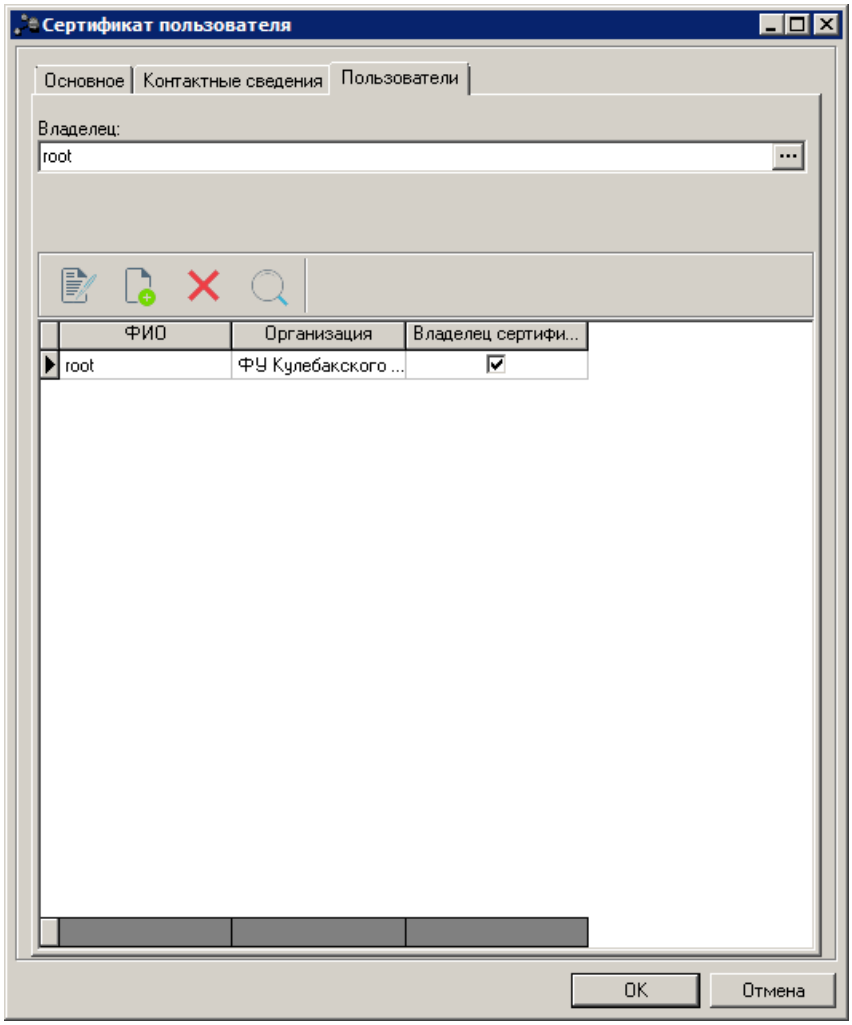

Рисунок 13 – Форма редактирования импортированного сертификата пользователя, закладка «Пользователи»

В поле **Владелец** указывается пользователь системы, на имя которого УЦ выдан сертификат ключа подписи. При импорте в систему нового сертификата с помощью справочника *Пользователи системы* в поле **Владелец** автоматически указывается пользователь, учетная запись которого редактируется в данный момент.

Список пользователей, к которым привязан сертификат, представлен в табличной форме с полями:

- **ФИО** – значение поля **ФИО** учетной записи пользователя в справочнике *Пользователи* системы.
- **Организация** – значение поля **Краткое наименование** из карточки организации, к которой принадлежит пользователь.
- **Владелец сертификата** - признак активируется автоматически для пользователя, указанного в поле **Владелец** и на имя которого выдан сертификат. Для других пользователей признак не активируется.

Над списком сертификатов находится панель инструментов. На ней располагаются стандартные функциональные кнопки, с помощью которых можно выполнить действия: добавить нового пользователя, редактировать учетную запись добавленного пользователя, удалить и найти пользователя в списке.

Для добавления нового пользователя в список используется кнопка  (**Новый**) на панели инструментов над списком или клавиша **<F9>**. При этом открывается справочник *Пользователи системы*, из которого выбирается нужный пользователь. При добавлении нового пользователя в список осуществляется привязка сертификата к учетной записи добавленного пользователя. Учетная запись пользователя, указанного в поле **Владелец**, добавляется в список автоматически с признаком

Владелец сертификата. При удалении из списка пользователя с включенным признаком **Владелец сертификата**, поле **Владелец очищается**.

8. Нажать кнопку **OK**, после чего сертификат пользователя добавится в список сертификатов.

4.1.3 Пакетный импорт сертификатов

В системе предусмотрена возможность одновременной загрузки группы сертификатов в справочник и их автоматической привязки к пользователям. Пакетный импорт сертификатов в системе осуществляется в справочнике :

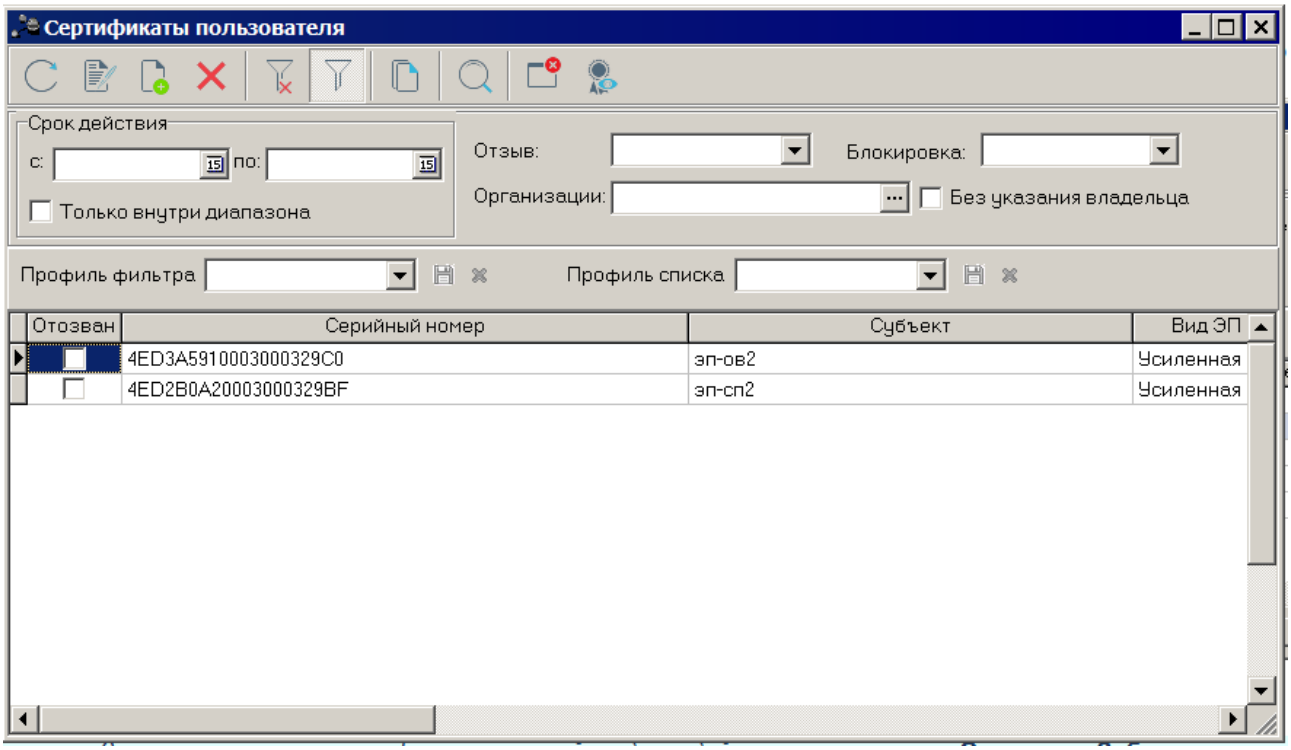

Рисунок 14 – Форма справочника сертификатов

Для одновременной загрузки группы сертификатов используется кнопка (**Импорт сертификатов**) на панели инструментов справочника. В результате нажатия данной кнопки открывается форма импорта сертификатов пользователей:

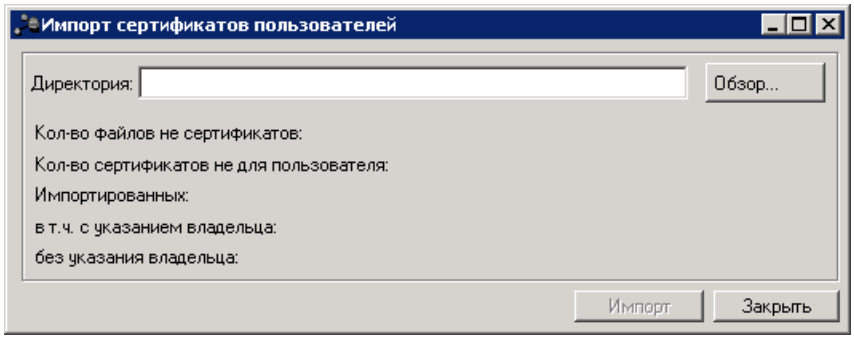

Рисунок 15 – Форма импорта сертификатов

В форме импорта сертификатов в поле **Директория** указывается директория доступа к папке с сертификатами, которые требуется загрузить в систему. Для указания директории нажимается кнопка **Обзор**. На экране появится окно *Обзор папок*:

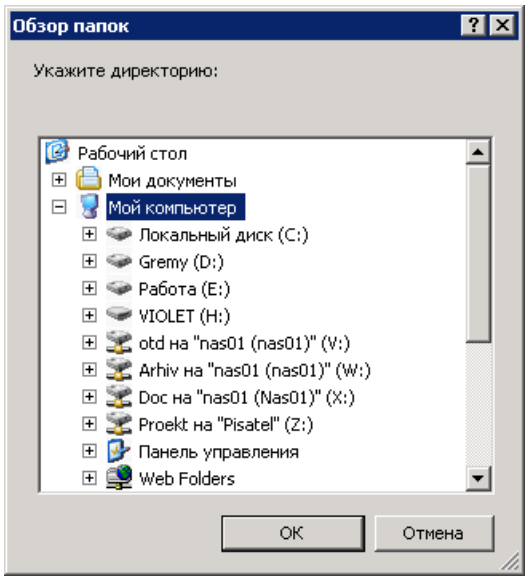

Рисунок 16 – Форма выбора папки

В окне выбирается нужная папка и нажимается кнопка **ОК**. Окно *Обзор* папок закрывается.

Процедура импорта сертификатов из указанной папки в справочник запускается нажатием кнопки **Импорт** в форме импорта сертификатов. В процессе импорта сертификатов осуществляется автоматическая привязка сертификатов к учетным записям пользователей по ФИО пользователей. При отсутствии в справочнике *Пользователи системы* учетных записей с указанным ФИО или нахождении более одной такой записи сертификат импортируется без привязки. После загрузки сертификатов на экране появляется сообщение о завершении процедуры импорта:

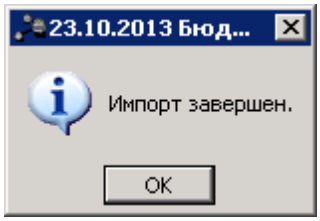

Рисунок 17 – Сообщение о завершении процедуры импорта

В форме сообщения нажимается кнопка **ОК**.

После завершения загрузки в форме импорта сертификатов выводится отчет о результатах выполнения процедуры импорта:

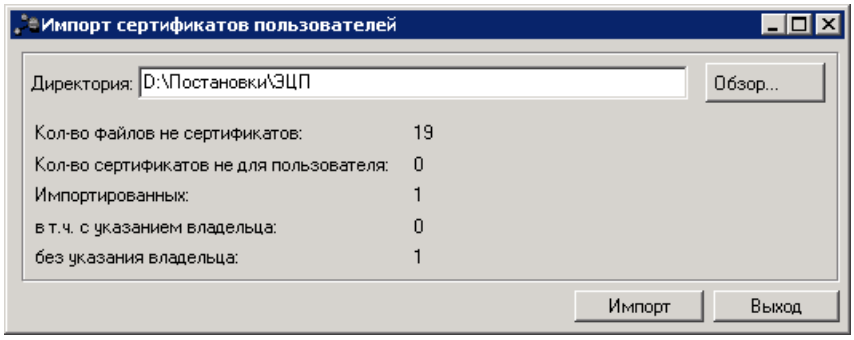

Рисунок 18 – Форма импорта сертификатов, отчет о результатах импорта

В форме импорта сертификатов выводятся следующие данные по результатам загрузки:

- **Количество файлов не сертификатов** – количество обнаруженных в директории импорта файлов, не являющихся сертификатами;
- **Количество сертификатов не для пользователей** – количество обнаруженных в директории импорта сертификатов, не предназначенных для пользователей;
- **Импортированных** – количество сертификатов, импортированных в систему;
- **в т.ч. с указанием владельца** – количество сертификатов, импортированных в систему и привязанных к учетным записям пользователей;
- **без указания владельца** – количество сертификатов, импортированных в систему без привязки к учетным записям пользователей.

После завершения процедуры импорта на панели фильтрации справочника автоматически включается параметр **Без указания владельца**. Записи справочника фильтруются по признаку отсутствия значения в поле **Владелец** (закладка **Пользователи**) формы сертификата, т.е. в форме справочника выводится список сертификатов пользователей, не привязанных к учетным записям пользователей.

4.1.4 Настройка проверки объектных идентификаторов условий использования сертификатов

В соответствии с положениями п.1 ст.6 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» ЭД с УЭП признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

Набор областей использования предоставляемого сертификата ключа подписи записывается с помощью объектных идентификаторов (OID) в расширении **Улучшенный ключ** сертификата ключа подписи. Состав полей и расширений сертификата ключа подписи представлен на закладке **Состав** формы просмотра сертификата:

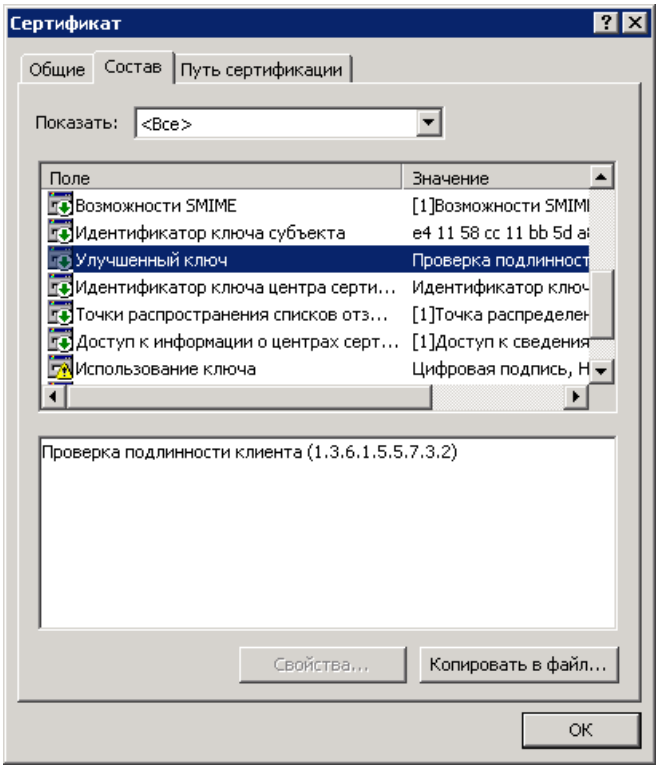

Рисунок 19 – Форма просмотра сертификата, закладка «Состав»

В целях спецификации условий использования сертификатов под собственные регламенты документооборота, а также осуществления дальнейшего контроля их использования при обработке документов в системе, организация может зарегистрировать в УЦ собственные объектные идентификаторы, которые будут указаны в расширении **Улучшенный ключ** сертификата ключа подписи. Данные объектные идентификаторы будут описывать цели, для которых сертификат может быть использован, и соответствовать требованиям к обработке ЭД, определенным в системе.

***Примечание**. Регистрация частного номера организации в российском сегменте мирового пространства объектных идентификаторов осуществляется Уполномоченным федеральным органом исполнительной власти РФ по применению ЭП (**www.reestr-pki.ru**). Перечень объектных идентификаторов, зарегистрированных и закрепленных за организацией, а также их значения и правила использования рекомендуется документально оформить и утвердить установленным в организации порядком.*

Таким образом, для осуществления контроля использования сертификатов в системе необходимо:

- разработать регламент обработки ЭД в системе, определить правила их подписания в справочнике *Правила подписания на статусах*;
- зарегистрировать в УЦ объектные идентификаторы, определяющие установленный в организации и настроенный в системе регламент обработки ЭД, поместить их в справочник *Объектные идентификаторы*;
- назначить зарегистрированные объектные идентификаторы правилам подписания документов в справочнике *Правила подписания на статусах*;
- установить в системе полученный от УЦ сертификат, содержащий объектные идентификаторы условий его использования;
- включить для сертификата проверку объектных идентификаторов условий его использования.

Проверка объектных идентификаторов условий использования сертификата настраивается с помощью опции **Осуществлять проверку OID условий использования** в форме редактирования сертификата в справочнике :

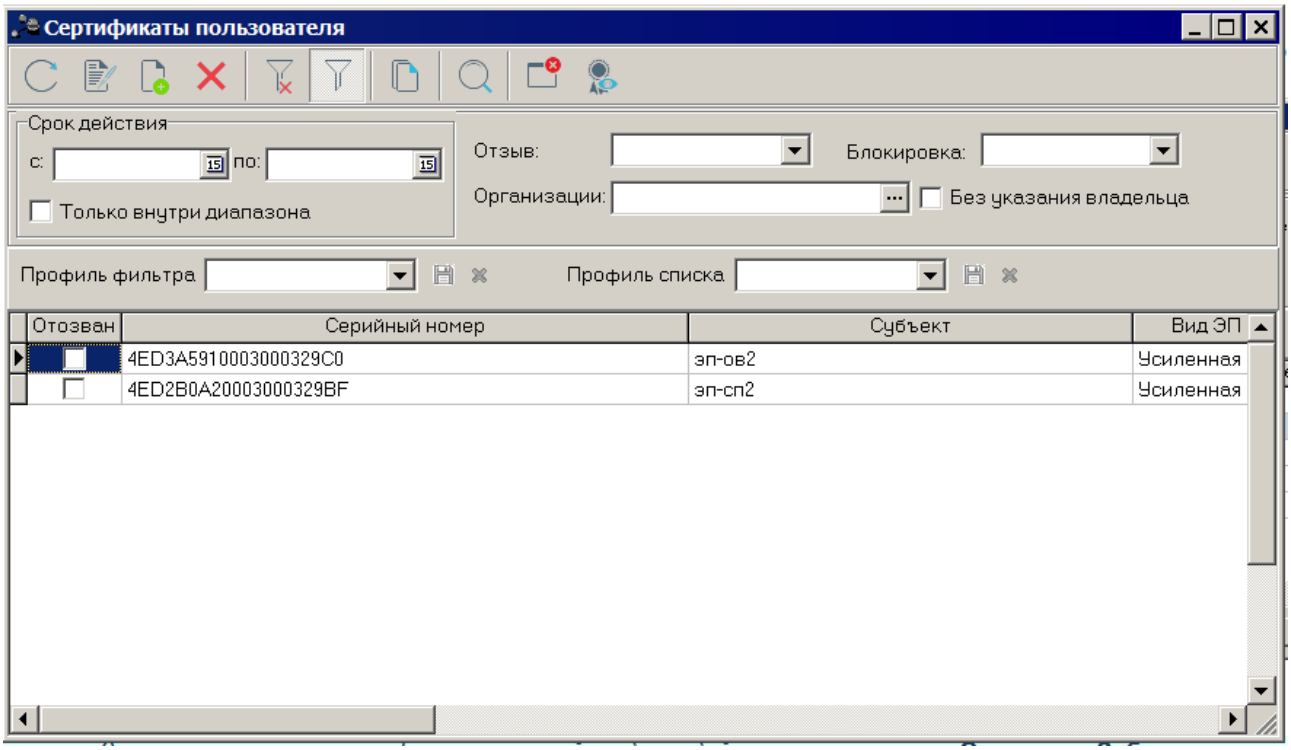

Рисунок 20 – Справочник «Сертификаты пользователей»

Состав полей для выделенного сертификата можно просмотреть, нажав кнопку **Редактировать** панели инструментов формы справочника или клавишу **<F4>** клавиатуры:

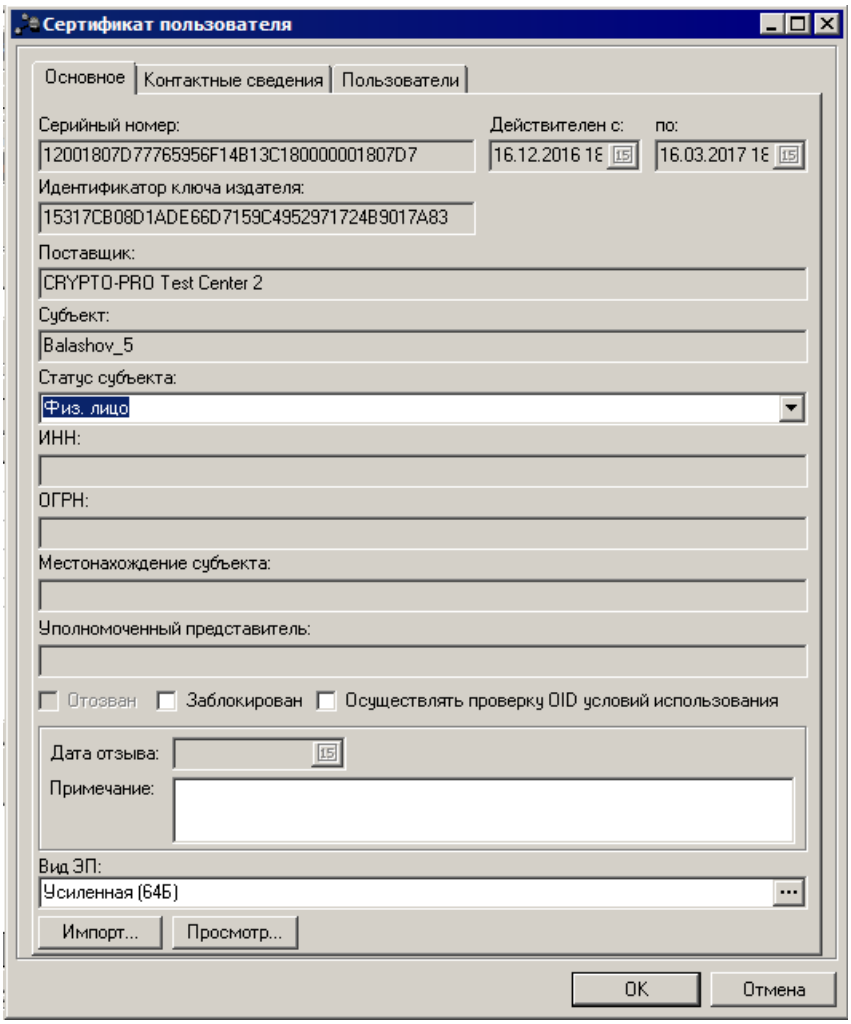

Рисунок 21 – Форма регистрации нового сертификата пользователя

Если для сертификата пользователя включена проверка OID'ов условий использования, то при попытке подписания документа с помощью данного сертификата будет производиться сравнение OID'ов правил подписания данного документа с OID'ами условий использования, содержащимися в сертификате. Подписание ЭД с помощью данного сертификата будет возможно только в случае вхождения OID'ов правил подписания подписываемых групп полей во множество значений OID'ов условий использования сертификата. В противном случае, если OID'ы правил подписания документа не соответствуют OID'ам условий использования сертификата, подписание документа с помощью данного сертификата будет невозможно.

Если для сертификата пользователя отключена проверка OID'ов условий использования, то контроль использования сертификата производиться не будет.

***Примечание**. С позиций юридической значимости ЭД, подписанных ЭП, не рекомендуется отключать опцию **Осуществлять проверку OID условий использования**. Использование сертификата ключа подписи при осуществлении отношений, не указанных в сертификате, не обеспечивает юридической значимости документов, подписанных сформированной с его помощью ЭП.*

4.1.5 Настройка оповещения об истечении срока действия сертификата

Для обеспечения своевременного обновления реестра используемых сертификатов в системе настраивается оповещение об истечении срока действия сертификата. Оповещение настраивается в пункте меню **Сервис→**, группа настроек , закладка **Общие**, параметр **Оповещать об истечении срока действия сертификата за ... дней**:

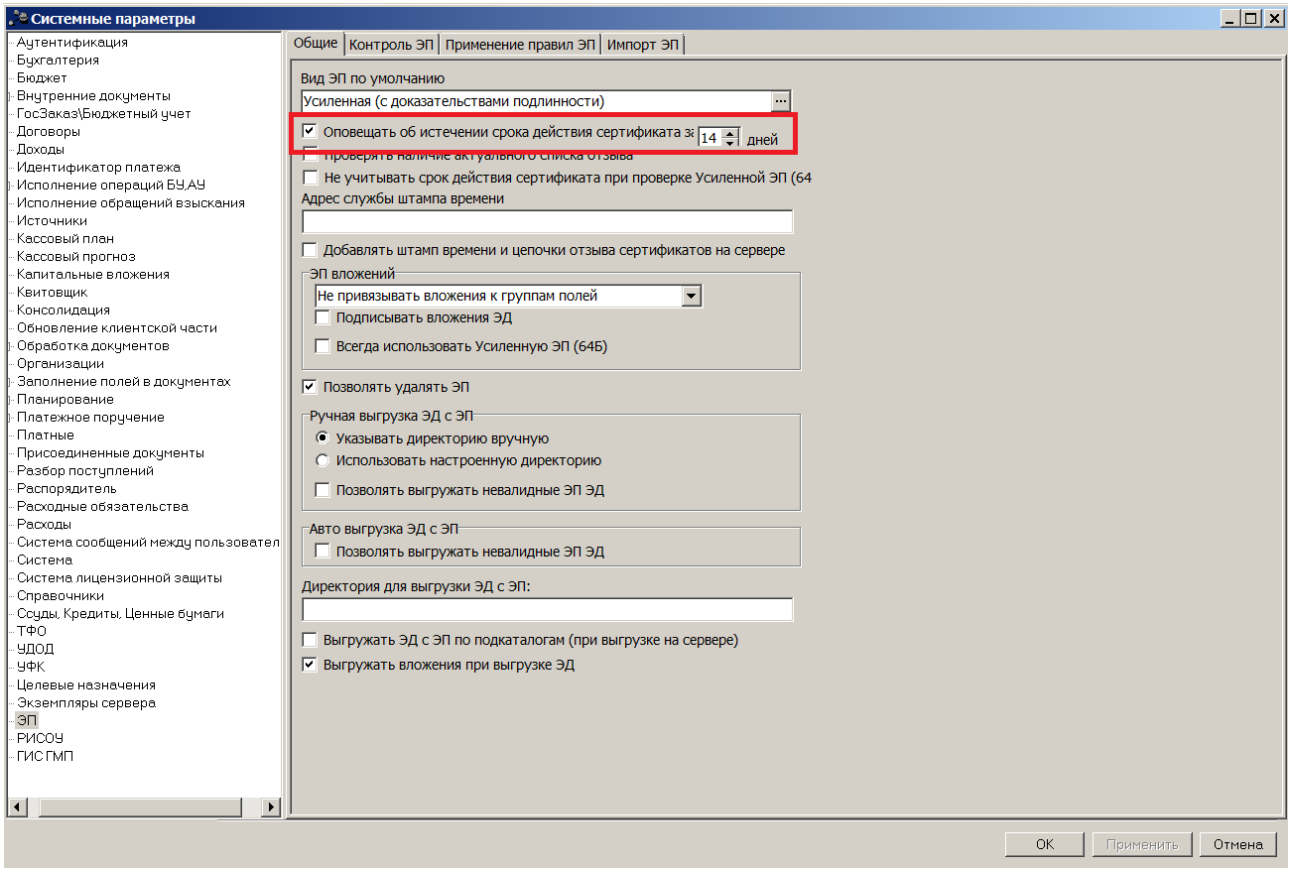

Рисунок 22 – Настройка оповещения об истечении срока действия сертификата

При включенной настройке **Оповещать об истечении срока действия сертификата за ... дней** в момент входа пользователя в систему осуществляется проверка всех сертификатов, в которых данный пользователь указан как владелец. По результатам проверки выводится сообщение, содержащее список сертификатов с датой окончания срока действия, попадающей в указанный в настройке диапазон, или истекшим сроком действия, кроме сертификатов, по которым пользователь отключил напоминание:

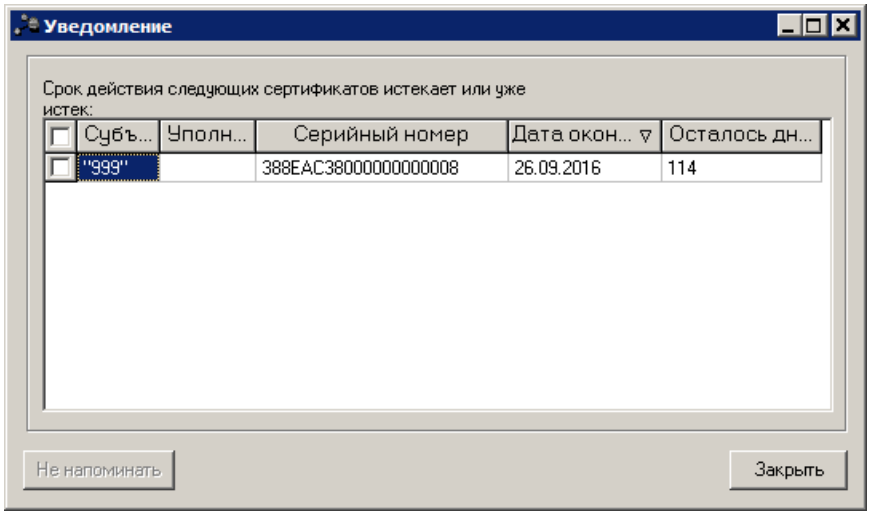

Рисунок 23 – Уведомление об истечении срока действия сертификата

Сертификаты, срок действия которых истекает или уже истек, представлены в виде таблицы с указанием даты окончания срока действия сертификатов и количества дней до истечения срока. Возможна сортировка данных по имени сертификата, дате окончания и количеству оставшихся дней.

Для отключения оповещения по сертификату необходимо выбрать в списке нужный сертификат, поставив отметку в поле рядом с ним, и нажать кнопку **Не напоминать**. При нажатии кнопки отключается дальнейшая проверка срока действия выбранного сертификата, и окно уведомления закрывается. Для сертификатов, у которых отключено напоминание об истечении срока их действия, при последующих входах в систему сообщение выдаваться не будет. Если в окне уведомления не выбрано ни одного сертификата, кнопка **Не напоминать** не активна. Для закрытия окна уведомления используется кнопка **Закрыть**.

По умолчанию настройка включена и оповещение производится за 14 дней до истечения срока действия сертификата.

4.2 Отзыв сертификатов пользователей

В системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» предусмотрена автоматическая поддержка актуальности реестра сертификатов пользователей, которая предполагает автоматический отзыв сертификатов пользователей в результате автоматической установки (обновления) списков отозванных сертификатов (CRL). Процедура автоматической установки (обновления) списков отозванных сертификатов (CRL) 40 выполняется по заданию Планировщика в соответствии с настроенной периодичностью и включает в себя:

- автоматическую проверку публикации списков отзыва (CRL) в точках их распространения для зарегистрированных в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» сертификатов;
- автоматическое скачивание списков отзыва (CRL) из точек их распространения для зарегистрированных в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»»

сертификатов;

- автоматическую установку списков отзыва (CRL) в хранилище сертификатов ОС сервера ЭП.

Администратор может производить *отзыв сертификатов пользователей вручную в справочнике Пользователи системы* 44.

При подписании электронных документов отозванные в автоматическом и ручном режиме сертификаты пользователей недоступны для выбора.

4.2.1 Автоматическая установка (обновление) списков отозванных сертификатов (CRL)

В системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» автоматическая установка (обновление) списков отозванных сертификатов (CRL) выполняется по заданию Планировщика *CRLDownloader* (пункт меню). График запуска (периодичность выполнения) задания настраивается в справочнике *Расписание* (пункт меню **Планировщик→Расписание**).

Внимание! *Задание Планировщика CRLDownloader поддерживает только протокол HTTP, то есть автоматическое скачивание списков отзыва (CRL) выполняется только из точек распространения списков отзыва (CRL), работающих по протоколу HTTP.*

Примечание. *Подробное описание настройки заданий Планировщика см. в документации:*
- «»;
- «».

4.2.1.1 Управление точками распространения списков отзыва (CRL)

Информация о точках распространения и времени обновления списков отзыва сертификатов содержится в справочнике Точки распространения списков отзыва (пункт меню **Справочники→Система→Точки распространения списков отзыва**):

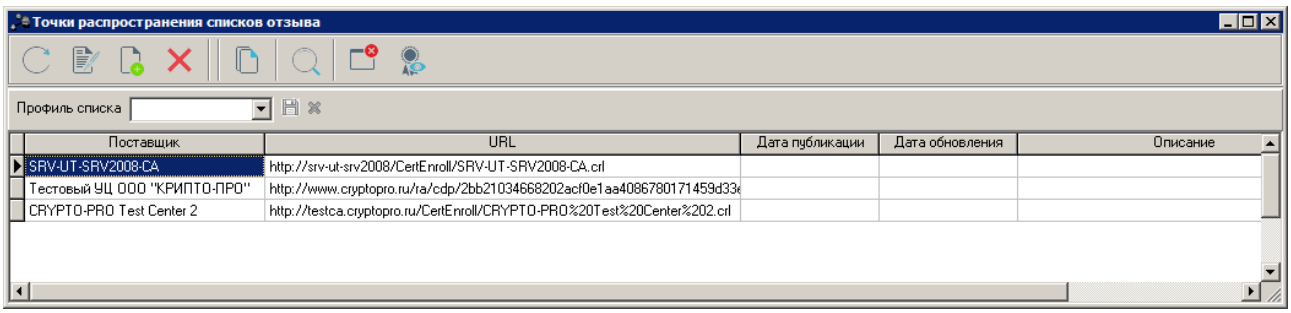

Рисунок 24 – Справочник «Точки распространения списков отзыва»

В верхней части справочника находится панель инструментов, на которой располагаются стандартные функциональные кнопки. С их помощью можно выполнить следующие действия: создать, редактировать, удалить, найти и обновить список записей.

Поле **Профиль списка** используется для хранения профилей настроек порядка следования и видимости колонок списка документов. Управление профилями пользовательских настроек осуществляется с помощью расположенных рядом с полем кнопок (**Сохранить профиль**) и (**Удалить профиль**). При выборе в поле профиля состав и последовательность колонок списка документов автоматически изменяется в соответствии с сохраненной настройкой профиля.

Для создания новой записи нажимается кнопка **Создать** **<F9>**. На экране появится форма:

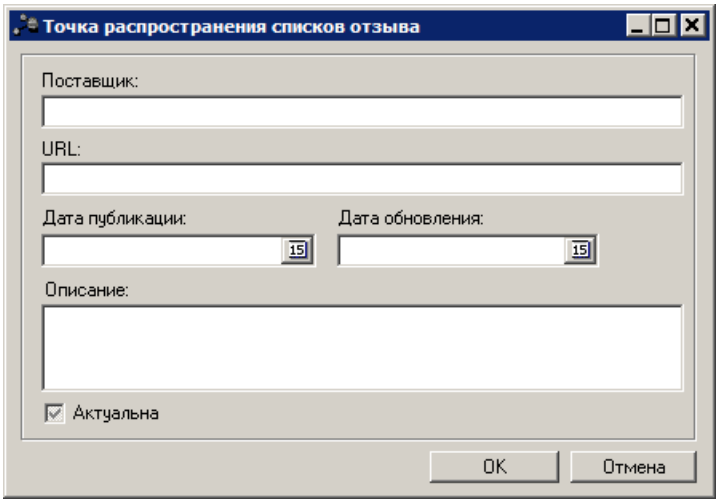

Рисунок 25 – Форма создания новой записи справочника «Точки распространения списков отзыва»

В форме новой записи справочника содержатся поля:

- **Поставщик** – название УЦ, который выдал сертификат ключа подписи. Обязательное для заполнения, доступно для редактирования.
- **URL** – полное имя точки распространения списков отзыва (URL-адрес, по которому публикуется список отзыва). Обязательное для заполнения, доступно для редактирования.

Примечание. *Добавляемая в справочник точка распространения списков отзыва (CRL) должна работать по протоколу HTTP (URL-адрес добавляемой точки распространения должен содержать протокол HTTP), иначе по данной точке распространения не будет производится автоматическая установка (обновление) списков отзыва (CRL).*

- **Дата публикации** – дата публикации списка отзыва. Обязательное для заполнения, доступно для редактирования.
- **Дата обновления** – дата обновления списка отзыва. Обязательное для заполнения, доступно для редактирования.

Примечание. *Информация о датах публикации и обновления списков отзыва вносится (обновляется) в справочнике в результате установки (обновления) списков отзыва, полученных из соответствующих точек распространения в результате выполнения задания Планировщика CRLDownloader. Более подробно см. в разделе* ***Алгоритм автоматической установки (обновления) списков отозванных сертификатов (CRL)*** 42

- **Описание** – описание точки распространения списков отзыва. Необязательное для заполнения, доступно для редактирования.
- **Актуальна** – признак актуальности точки распространения списков отзыва. Доступно для редактирования.

Для добавления/сохранения записи в справочник нажимается кнопка **OK**. Форма записи справочника закрывается.

Автоматически записи добавляются в справочник при регистрации в системе новых сертификатов пользователей. При регистрации в системе нового сертификата по каждой точке распространения, содержащейся в данном сертификате на момент его импорта, в справочнике *Точки распространения списков отзыва* автоматически формируется новая запись. Поля **Поставщик** и **URL** формы записи справочника автоматически заполняются данными из регистрируемого сертификата. Уникальность записей справочника определяется значением поля **URL**. Если в справочник уже внесена точка распространения списка отзыва, указанная в импортируемом сертификате, новая запись по данной точке распространения в справочнике не формируется.

Для единовременного автоматического добавления в справочник точек распространения сертификатов, содержащихся в файловой системе компьютера, используется кнопка  (**Импорт точек распространения**) на панели инструментов. При нажатии на данную кнопку открывается окно обзора файлов с расширениями **.cer* и **.crt*:

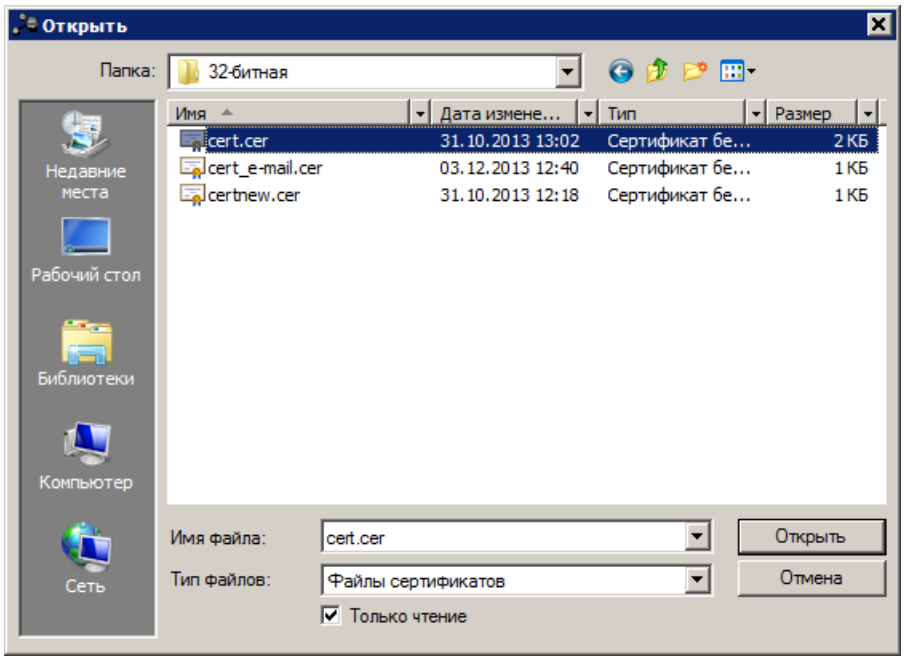

Рисунок 26 – Окно обзора файлов

В окне обзора выбирается один или несколько файлов сертификатов, точки распространения которых требуется загрузить в справочник, и нажимается кнопка **Открыть**. В результате в справочник загружаются точки распространения выбранных сертификатов.

4.2.1.2 Алгоритм автоматической установки (обновления) списков отозванных сертификатов (CRL)

Для актуализации реестра сертификатов пользователей при выполнении задания Планировщика *CRLDownloader* для каждой записи справочника *Точки распространения*

списков отзыва с включенным признакам **Актуальна** выполняется следующий алгоритм:

Внимание! *Задание планировщика «CRLDownloader» выполняется только для точек распространения списков отзыва (CRL), работающих по протоколу HTTP.*

- Если поле **Дата публикации** записи справочника не заполнено, производится установка списка отзыва:

1. По адресу, указанному в поле **URL** записи справочника, скачивается список отзыва.
2. Из соответствующих реквизитов списка отзыва заполняются поля **Дата публикации** и **Дата обновления** записи справочника.
3. Файл списка отзыва импортируется в систему.
4. В форме сертификатов, входящих в импортируемый список отзыва, автоматически включается параметр **Отозван**, поле **Дата отзыва** заполняется значением поля **Дата публикации** соответствующей записи справочника *Точки распространения списков отзыва*:

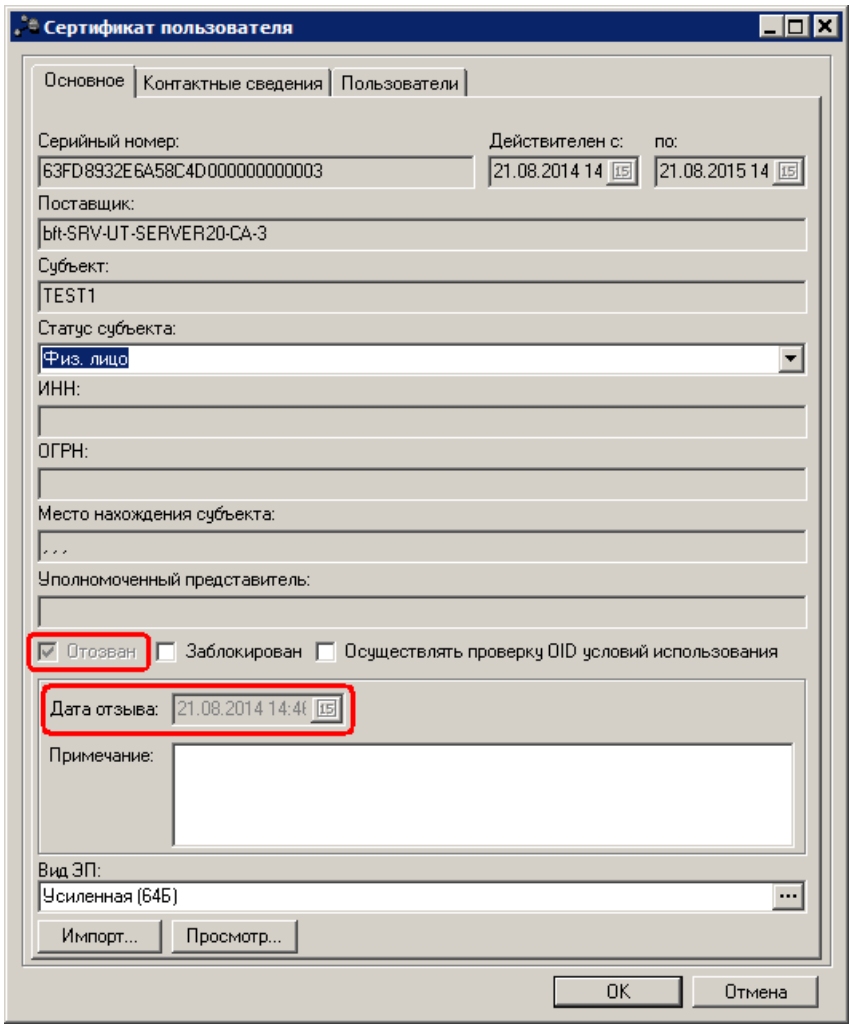

Рисунок 27 – Форма редактирования сертификата пользователя, отозванного в автоматическом режиме в результате установки (обновления) списка отзыва

Примечание. *Параметр* ***Отозван*** *и поле* ***Дата отзыва*** *формы сертификата недоступны для редактирования и заполняются (очищаются) только в автоматическом режиме при установке (обновлении) списка отзыва.*

5. Загруженный в систему список отзыва устанавливается в хранилище сертификатов ОС

сервера ЭП.

- Если поле **Дата публикации** записи справочника заполнено и значение текущей системной даты и времени больше значения указанного в поле **Дата обновления** записи справочника, производится обновление списка отзыва:

1. По адресу, указанному в поле **URL** записи справочника, скачивается список отзыва.
2. Значения полей **Дата публикации** и **Дата обновления** перезаписываются из соответствующих реквизитов списка отзыва.
3. Файл списка отзыва импортируется в систему.
4. В форме сертификатов, входящих в импортируемый список отзыва, автоматически включается параметр **Отозван**, поле **Дата отзыва** заполняется значением поля **Дата публикации** соответствующей записи справочника *Точки распространения списков отзыва*. Выполняется только для вновь отозванных сертификатов.
5. В форме ранее отозванных сертификатов, отсутствующих в импортируемом списке отзыва, автоматически выключается параметр **Отозван**, поле **Дата отзыва** очищается. Выполняется только для сертификатов, в которых указана данная точка распространения.
6. Список отзыва устанавливается в хранилище сертификатов ОС сервера ЭП.

4.2.2 Отзыв сертификата пользователя администратором

Администратору для отзыва сертификата пользователя в ручном режиме необходимо выполнить следующие действия:

1. Открыть справочник *Пользователи системы* (пункт меню →**Пользователи системы** 22).
2. Открыть на редактирование учетную запись пользователя, для которого необходимо отозвать сертификат, нажатием кнопки **Редактировать** на панели инструментов формы или клавиши **<F4>** клавиатуры.
3. В открывшейся форме *Редактирование пользователя системы* 23 перейти на закладку **Сертификаты**.
4. На закладке **Сертификаты** 23 выделить сертификат, который необходимо отозвать, и вызвать форму его редактирования нажатием кнопки **Редактировать** на панели инструментов окна или клавиши **<F4>** клавиатуры.
5. В открывшейся форме редактирования сертификата пользователя установить признак **Заблокирован**. При установке признака требуется в поле **Примечание** ввести причину отзыва сертификата:

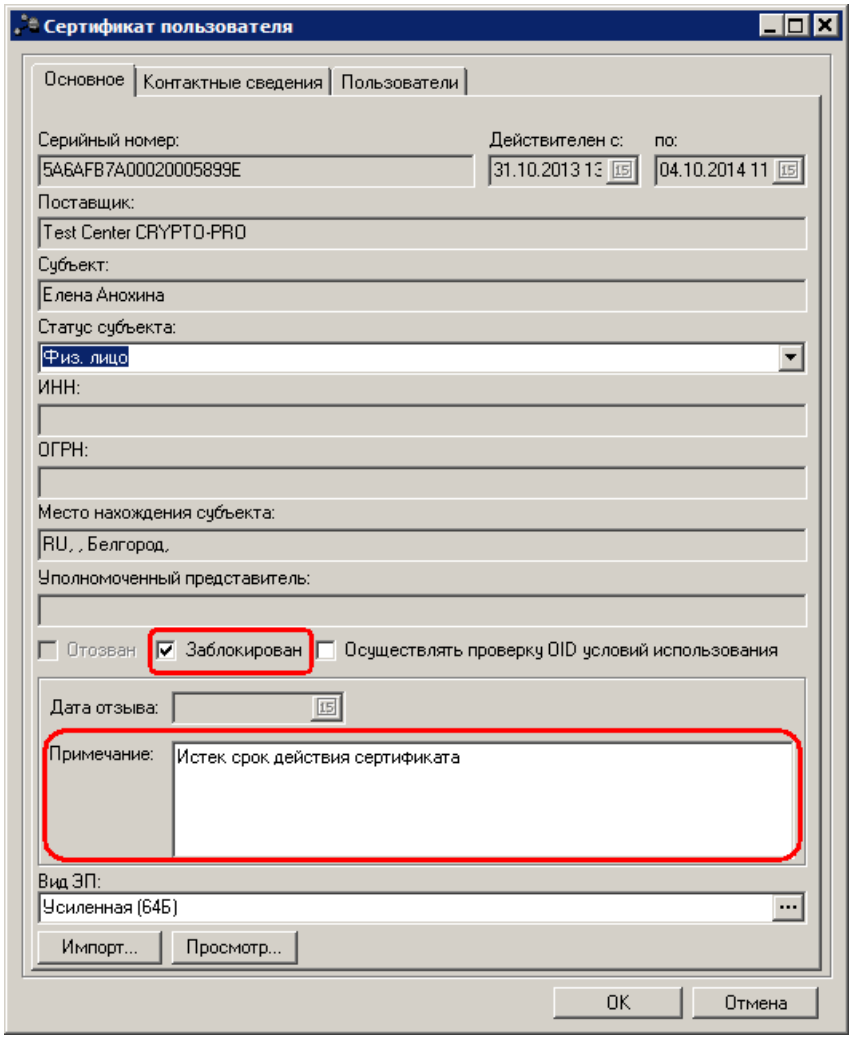

Рисунок 28 – Форма редактирования сертификата пользователя, отозванного администратором в ручном режиме

6. Нажать кнопку **OK**, форма редактирования сертификата пользователя закроется.

4.3 Управление правами пользователя в рамках работы с ЭП

Права пользователя по наложению ЭП на ЭД определяются доступом пользователя к ЭД и возможностью их подписания. Доступ пользователя к ЭД регулируется настройками его организационной роли, а возможность подписания – наличием функциональной ЭП-роли 46 .

***Примечание**. Правила настройки организационных ролей описаны в документации «».*

Для пользователей, которые в соответствии с регламентом обработки ЭД должны производить подписание ЭД и проверку ЭП ЭД, в системе создаются функциональные роли с признаком **Роль для ЭП**. Данные функциональные роли настраиваются и назначаются пользователям.

4.3.1 Настройка функциональной роли пользователя для работы с ЭП

Для обеспечения пользователя возможностью подписания ЭД, необходимо выполнить следующие действия:

1. Открыть справочник *Роли пользователей* (пункт меню **Справочники→Система→Роли пользователей** 59).
2. На панели фильтрации формы **Роли пользователей системы** установить с помощью переключателя значение *Функциональные* для отображения функциональных ролей пользователей.
3. Из списка ролей пользователей вызвать форму редактирования функциональной роли пользователя, для которого настраивается возможность использования ЭП, с помощью кнопки **Редактировать** панели инструментов окна или клавиши **<F4>** клавиатуры.
4. В форме редактирования функциональной роли пользователя, на закладке **Общие**, установить признак **Роль для ЭП**:

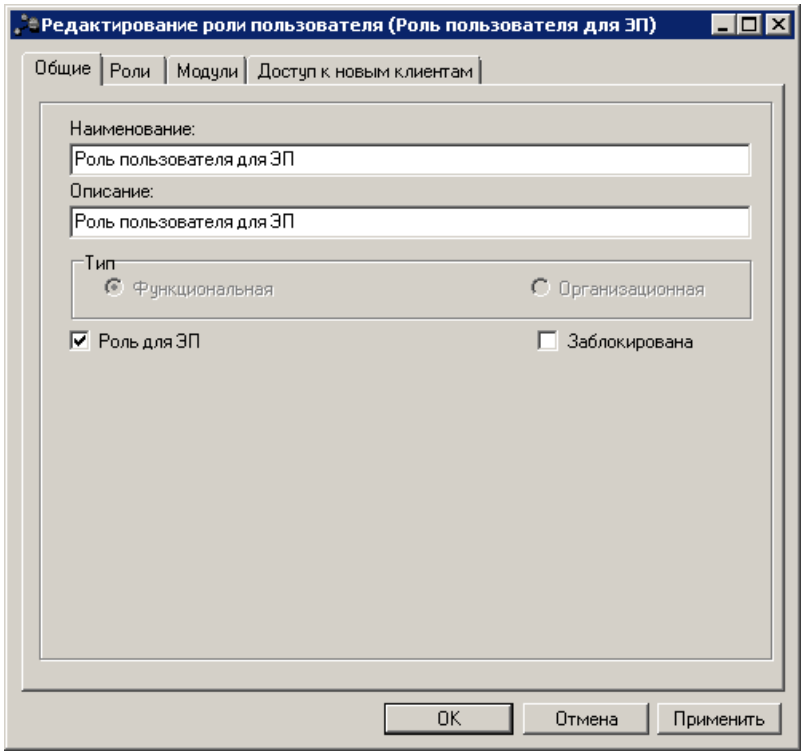

Рисунок 29 – Форма редактирования роли пользователя, закладка «Общие»

5. В случае необходимости, на закладке **Роли** можно назначить для роли специальные возможности (перенесением их из списка **Доступные** в список **Выбранные**):
   - **Позволять не контролировать ЭП** – возможность обрабатывать документы без функций ЭП.

Внимание! *Специальная возможность* ***Позволять не контролировать ЭП*** *используется отдельными объектами-пользователями системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»». Не рекомендуется использование возможности без необходимости.*

- **Позволять удалять подписанные документы** – возможность удаления подписанного ЭД.
- **Позволять удалять подписанные вложения в документах** – возможность удаления подписанного вложения к ЭД.
- **Позволять откладывать документ, подписанный ЭП другим пользователем** – возможность отмены обработки документа, подписанного ЭП другого пользователя.

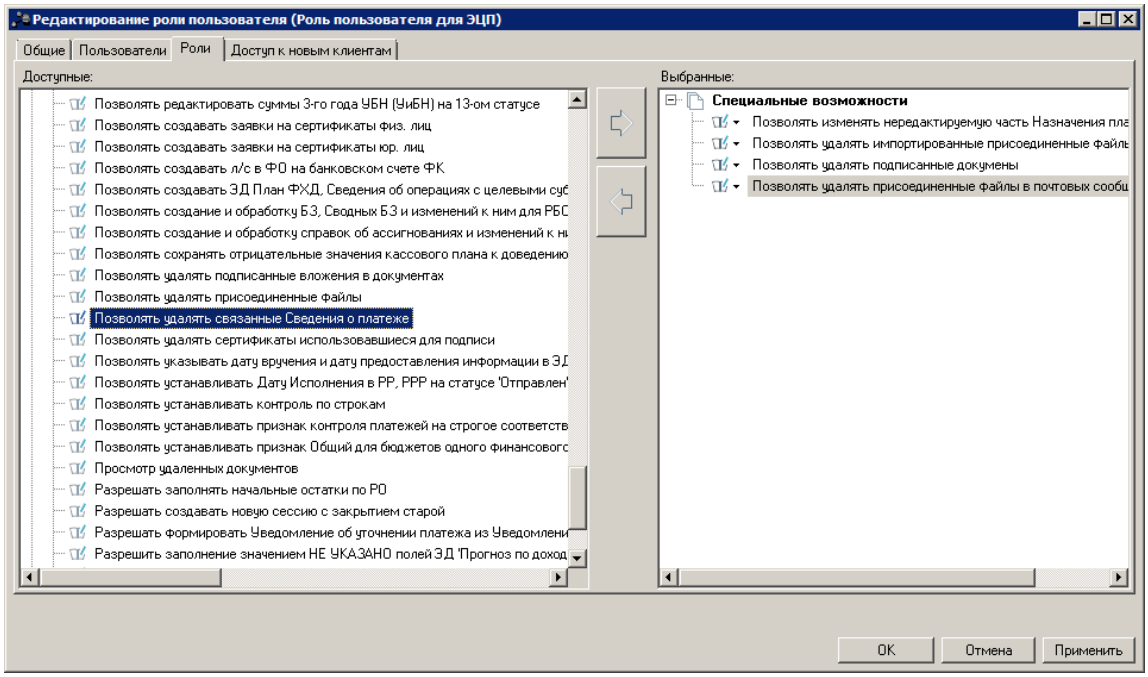

Рисунок 30 – Форма редактирования роли пользователя, закладка «Роли»

6. Нажать кнопку **ОК** для сохранения изменений функциональной роли.
7. В справочник *Реестр ролей пользователей* (меню) будет добавлена запись о назначении новой роли пользователю.

В системе осуществляется неигнорируемый контроль на наличие у пользователя-владельца сертификата ЭП-роли, используемой для подписания ЭД текущим пользователем. Если у владельца сертификата отсутствует ЭП-роль, подписание ЭД недоступно.

Примечание. *Контроль не осуществляется, если ФИО из сертификата = ФИО пользователя, подписывающего ЭД = ФИО пользователя-владельца сертификата.*

4.3.2 Настройка права выгрузки документов с ЭП в электронный архив

Настройка права выгрузки документов с ЭП производится через настройку специальной возможности функциональной роли пользователя. Для обеспечения пользователя правом выгрузки, необходимо выполнить следующие действия:

1. Открыть справочник *Роли пользователей* (меню **Справочники→Система→Роли**

пользователей).

2. На панели фильтрации формы справочника *Роли пользователей* 59 системы установить с помощью переключателя значение *Функциональные* для отображения функциональных ролей пользователей.
3. Из списка ролей пользователей вызвать форму редактирования функциональной роли пользователя, для которого настраивается право выгрузки документов с ЭП, с помощью кнопки **Редактировать** панели инструментов окна или клавиши **<F4>** клавиатуры (в случае создания отдельной функциональной роли, предназначенной для выгрузки документов с ЭП, необходимо нажать кнопку **Новый** панели инструментов окна или клавишу **<F9>** клавиатуры).
4. В форме редактирования (создания) функциональной роли пользователя 47, на закладке **Роли**, находятся два списка – **Доступные** и **Выбранные**:
   - **Доступные** – права, которые можно сделать доступными для роли. Права объединены в группы и оформлены в виде дерева. Первый уровень дерева – наименование группы прав, второй уровень – перечень прав, относящихся к данной группе.
   - **Выбранные** – права, включенные в роль. Список пополняется по мере переноса прав из списка **Доступные**. Права в списке объединяются в группы, аналогично списку **Доступные**.
5. Перенести специальную возможность **Выгрузка подписей документов** из списка **Доступные** в список **Выбранные**:

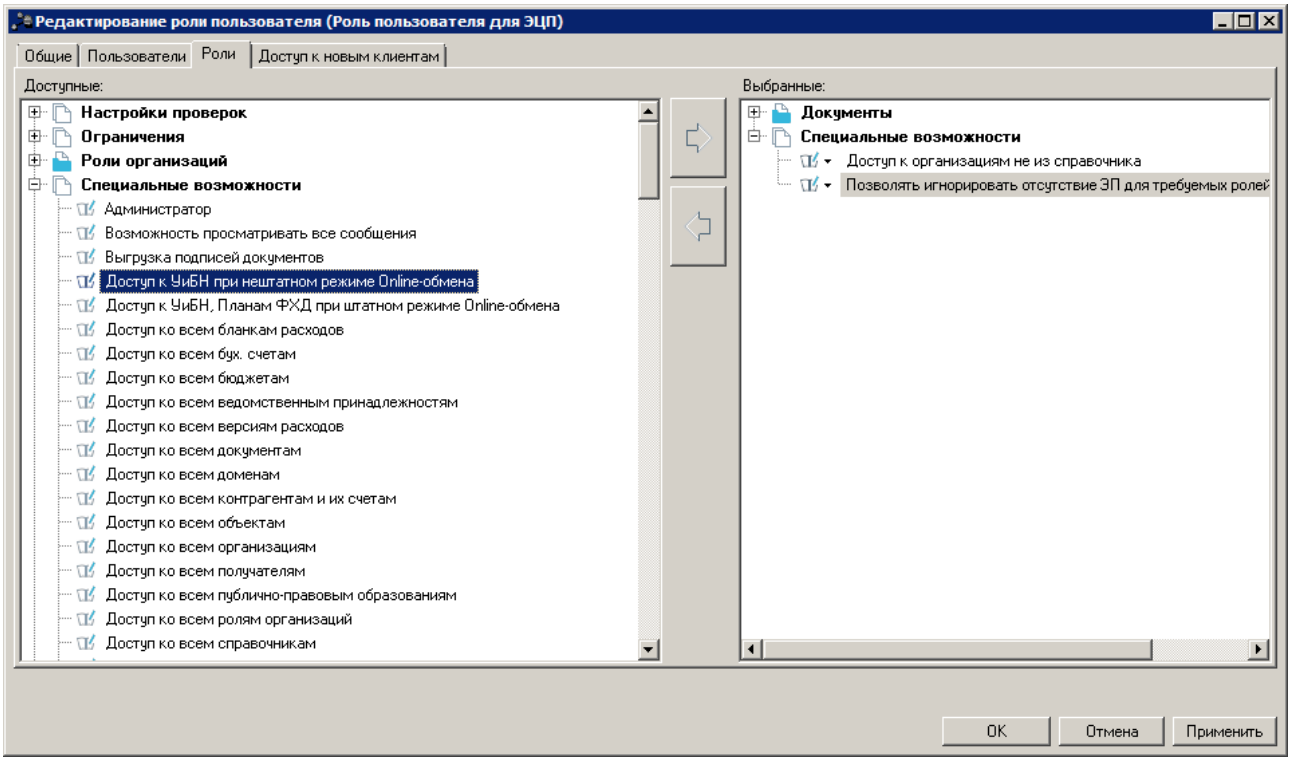

Рисунок 31 – Настройка специальных возможностей пользователя

6. Нажать кнопку **ОК**.

4.4 Настройка документооборота

4.4.1 Требования к составу подписываемых полей (дайджесту) документов

Состав подписываемых полей (дайджест) документов должен удовлетворять следующим условиям:

- в состав дайджеста не должна входить информация, меняющаяся от подписи к подписи (например, имя пользователя, наименование роли);
- в состав дайджеста не должна входить технологическая информация, описывающая структуру хранения документа в базе данных АЦК (например, ID, PARENT_ID, VERSION);
- в состав дайджеста должны входить только поля, представленные на печатной форме документа (должностное лицо, подписывая распечатанный на бумаге документ и/или дайджест документа в электронном виде, принимает ответственность за одинаковый (идентичный) объем/перечень информации);
- если рассматриваемый документ содержит семантически значимую ссылку на другой документ, то в состав дайджеста рассматриваемого документа должна быть включена семантически значимая информация, позволяющая установить документ, на который сделана эта ссылка (т.е. по распечаткам дайджестов одного и второго документа можно доказательно установить наличие связи между этими документами);
- в состав дайджеста должна быть включена семантически значимая регистрационная информация документа, позволяющая его однозначно идентифицировать по распечатке дайджеста (за пределами информационной системы АЦК, например, в электронном архиве);
- в состав дайджеста должны быть включены два блока информации:
  - блок семантически значимой информации, однозначно идентифицирующей документ;
  - блок информации, значимой с точки зрения бизнес-функций документа.
- формат дайджеста документа АЦК конкретного типа должен быть максимально стабилизирован; корректировки в формат дайджеста могут быть внесены только в случае изменений нормативов, регламентирующих состав полей документа (законодательство, местные нормативные акты).

4.4.2 Настройка сценариев обработки документов

Настройка регламента работы с ЭП может осуществляться в пользовательском дереве сценариев в соответствии с принятыми на объекте автоматизации политикой безопасности документооборота и регламентами обработки ЭД. В системе АЦК могут быть описаны правила подписания документов в статусах, а также порядок проверки ЭП с привязкой к конкретным статусам классов электронных документов.

Для описания и настройки регламента работы с ЭП администратор может

использовать справочники *Правила подписания на статусах* 50 (пункт меню **Справочники→Система→Правила подписания документов на статусах**) и *Правила проверки подписей на статусах* 62 (пункт меню **Справочники→Система→Правила проверки подписей на статусах**) системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»».

4.4.2.1 Настройка правил подписания документов на статусах

Регламент наложения ЭП на электронные документы настраивается в справочнике *Правила подписания на статусах*, доступном с помощью пункта меню **Справочники→Система→Правила подписания документов на статусах**:

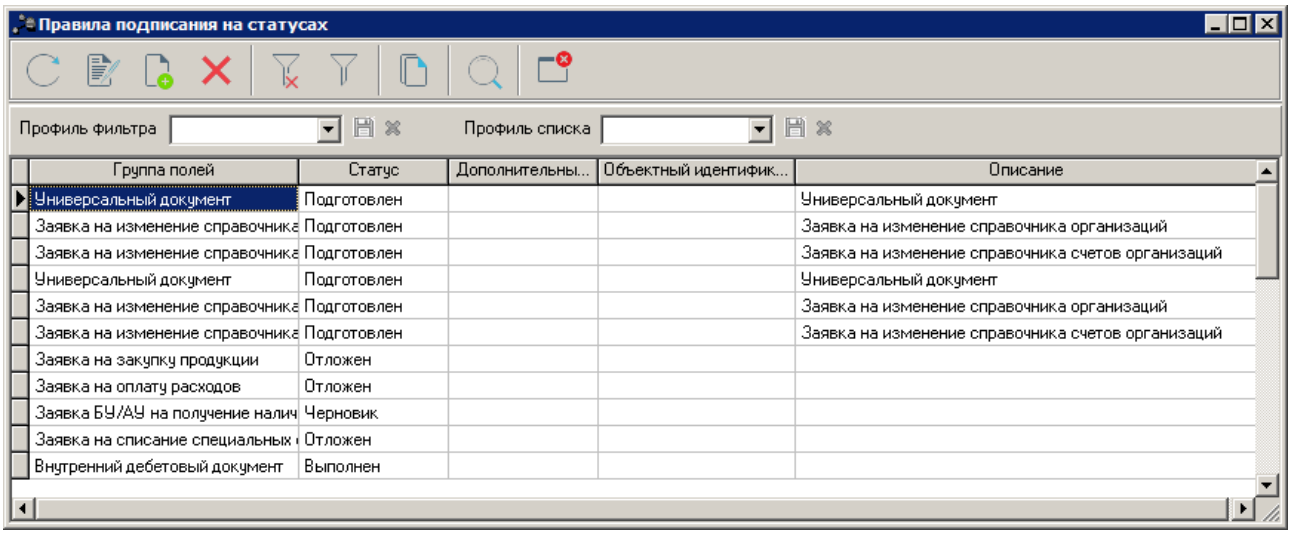

Рисунок 32 – Справочник «Правила подписания на статусах»

Данные этого справочника определяют возможность подписания ЭД (групп полей) на конкретных этапах их жизненного цикла (статусах) конкретными ЭП-ролями.

Примечание. *Правила подписания вложений электронных документов описываются в справочнике «Правила подписания документов на статусах» аналогичным образом.*

Внимание! *Данные справочника «Правила подписания документов на статусах» содержатся в xml-скрипте выполняемом единожды, при установке системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»». В дальнейшем, при обновлении системы АЦК, выполнение данного скрипта производиться не должно.*

В верхней части списка документов находится панель инструментов, на которой располагаются стандартные функциональные кнопки. С их помощью можно выполнить следующие действия: создать запись справочника, открыть форму редактирования или просмотра записи справочника, обновить список записей, скопировать список записей в буфер обмена и осуществить поиск записи в списке.

Панель фильтрации становится доступной при нажатии кнопки  . На панели фильтрации можно выбрать следующие параметры: **Класс документа**, **Группа полей**, **Статус**, **Роли**.

Для удаления выбранных параметров нажимается кнопка  .

Поле **Профиль фильтра** используется для хранения профилей параметров фильтрации списка документов, списка записей справочников, списка строк АРМ и редакторов. Поле **Профиль списка** используется для хранения профилей настроек порядка следования и видимости колонок в списках документов, списках записей справочников, списках строк АРМ и редакторов.

Каждое правило подписания определяет возможность подписания одного документа (группы полей) на одном статусе одной или несколькими ролями. При создании нового или изменении существующего правила указываются:

- **Группа полей** – группа полей ЭД, для которого настраивается правило подписания.
- **Базовый статус** – статус базового дерева сценариев обработки ЭД, на котором производится подписание.
- **Группа бюджетов** – группа бюджетов ЭД, для которого настраивается правило подписания.
- **Дополнительный статус** – статус дополнительного дерева сценариев обработки ЭД, на котором производится подписание.
- **Объектный идентификатор** – объектный идентификатор, назначенный правилу подписания документа.
- **Роли** – список ЭП-ролей, которыми производится подписание документа (группы полей).
- **Описание** – текстовое описание правила подписания документа (группы полей).
- **Скрипт** – название скрипта, описывающего условие выполнения правила подписания на статусах.
- **Вид ЭП** – наименование вида электронной подписи, которой производится подписание.

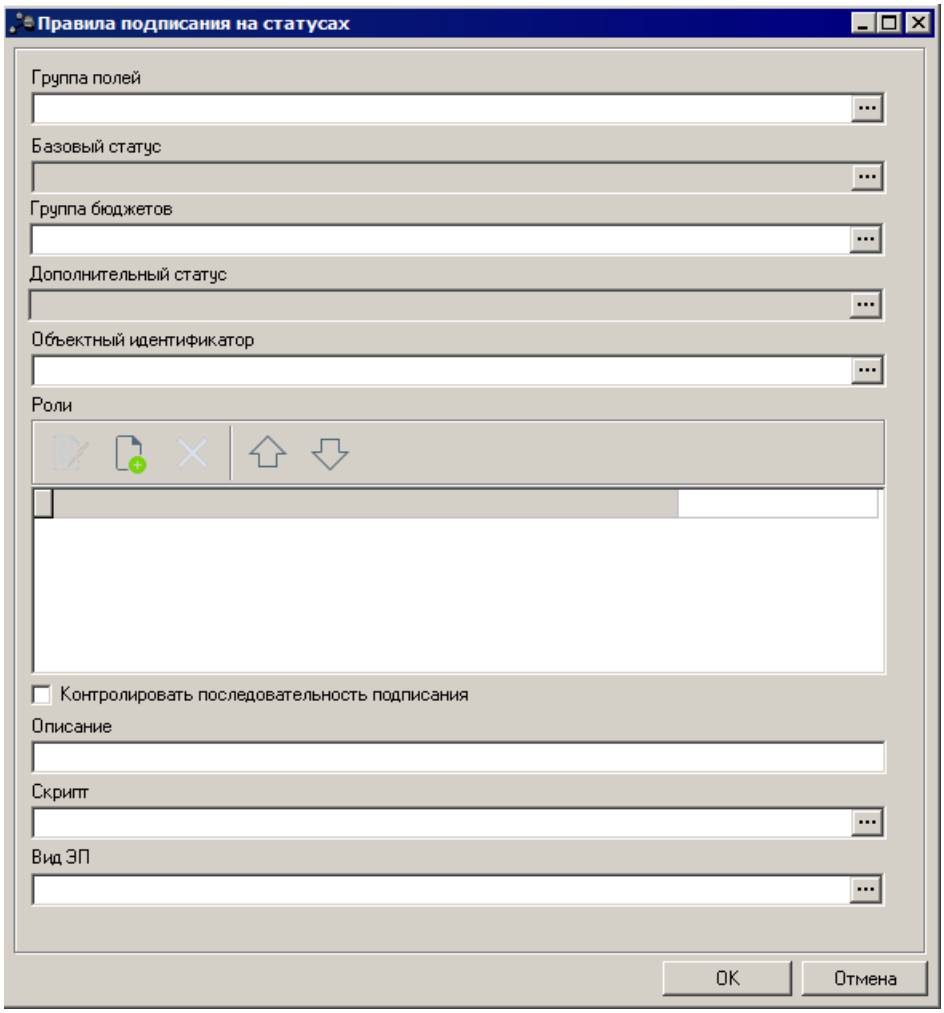

Рисунок 33 – Форма создания правила подписания на статусах

Выбор группы полей, для которой настраивается правило подписания, осуществляется пользователем из справочника *Группы полей*, который также доступен с помощью пункта меню **Справочники→Система→Группы полей**:

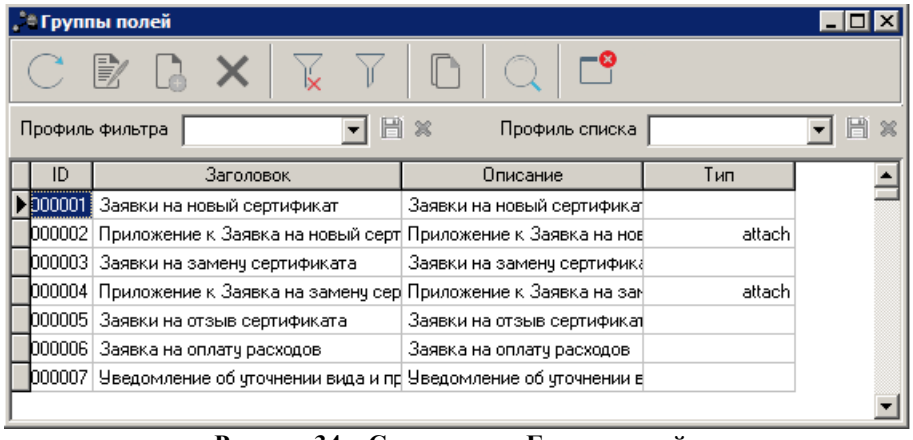

Рисунок 34 – Справочник «Группы полей»

Группы полей имеют следующие атрибуты: *Наименование*, *Заголовок*, *Описание*, *Тип* (для групп полей вложений принимает значение *attach*). Для просмотра выделенной группы

необходимо нажать кнопку  Редактировать на панели инструментов окна *Группы полей* или клавишу **<F4>** клавиатуры:

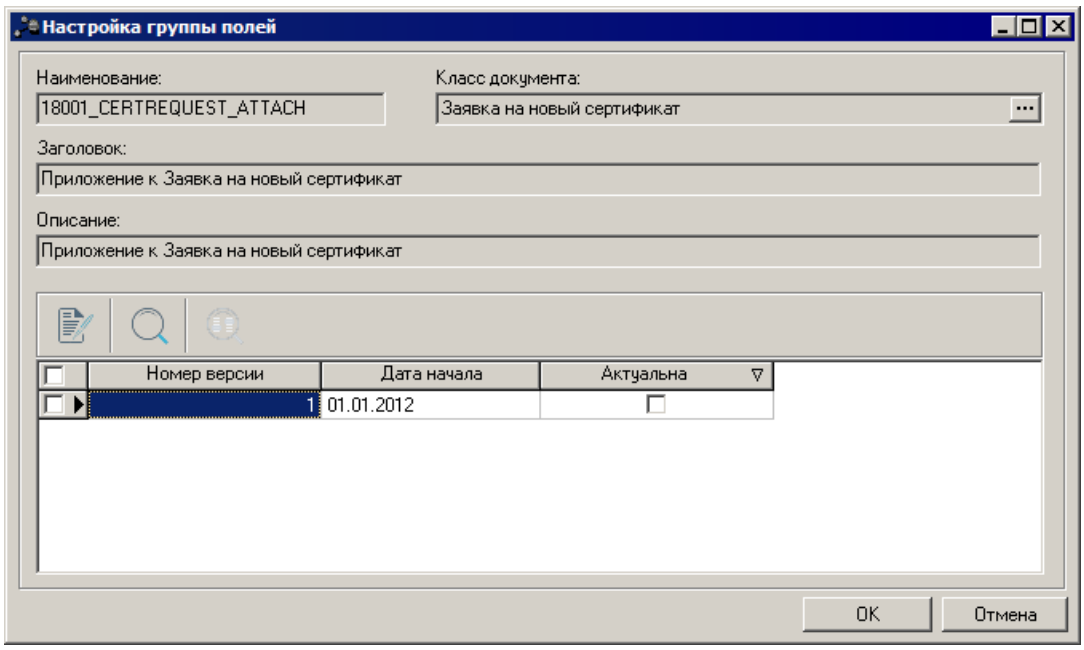

Рисунок 35 – Форма настройки группы полей

В форме новой записи справочника содержатся поля:

- **Наименование** – наименование группы полей
- **Заголовок** – уникальный заголовок группы полей.
- **Класс документа** – класс ЭД, к которому привязан заголовок группы полей.
- **Описание** – описание группы полей.

В нижней части формы расположен список версий группы полей с панелью инструментов для управления элементами списка.

Для открытия формы редактирования нажимается кнопка **Редактировать**  **<F4>**. На экране появится форма:

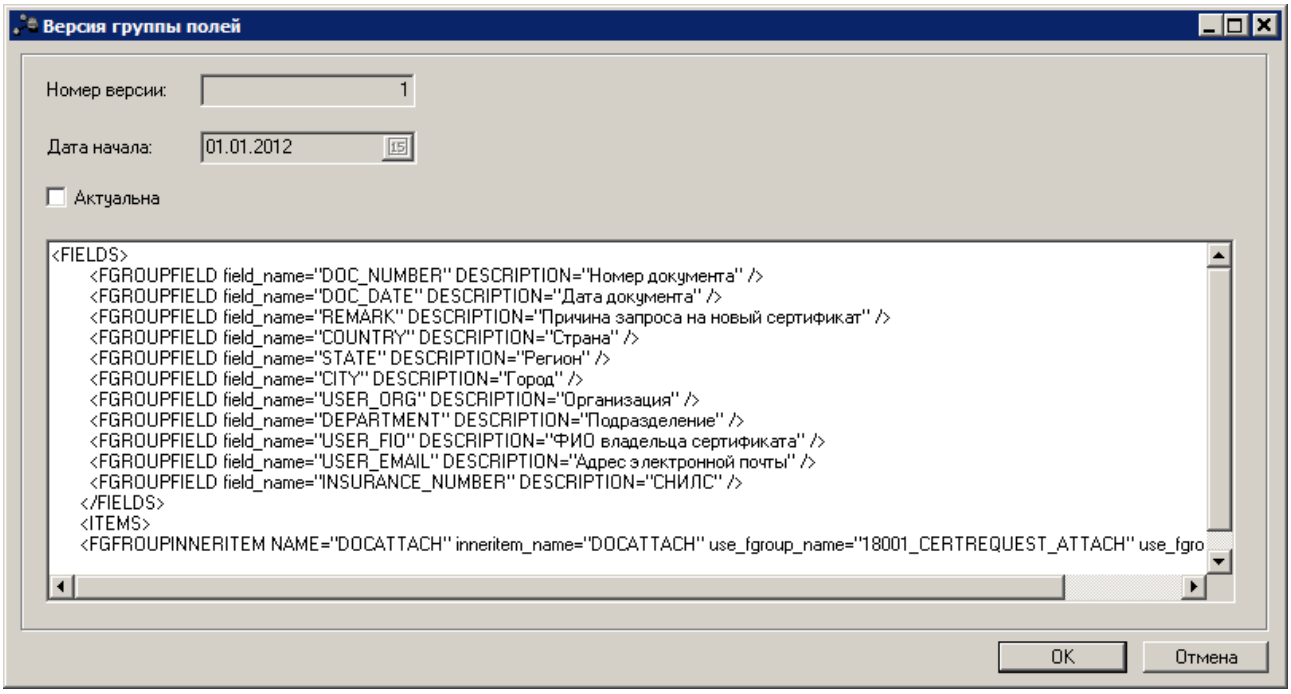

Рисунок 36 – Форма версии группы полей

В форме новой записи справочника содержатся поля:

- **Номер версии** – номер версии группы полей. Недоступно для редактирования.
- **Дата начала** – дата начала действия версии группы полей. Недоступно для редактирования.
- **Актуальна** – признак актуальности версии группы полей. Доступно для редактирования, необязательное для заполнения.

  Признак может быть включен только у одной версии в рамках группы или не включен ни у одной.

В нижней части формы расположено поле с XML-описанием версии группы полей, предназначенное для просмотра состава подписываемых полей версии группы полей.

Для сравнения версий в рамках одной группы полей с целью определения различий в составе подписываемых данных требуется в списке версий формы группы полей отметить сравниваемые версии и нажать кнопку  **Сравнить** (кнопка недоступна, если в списке не проставлены отметки рядом с версиями для сравнения). В результате на экране появится форма сравнения версий:

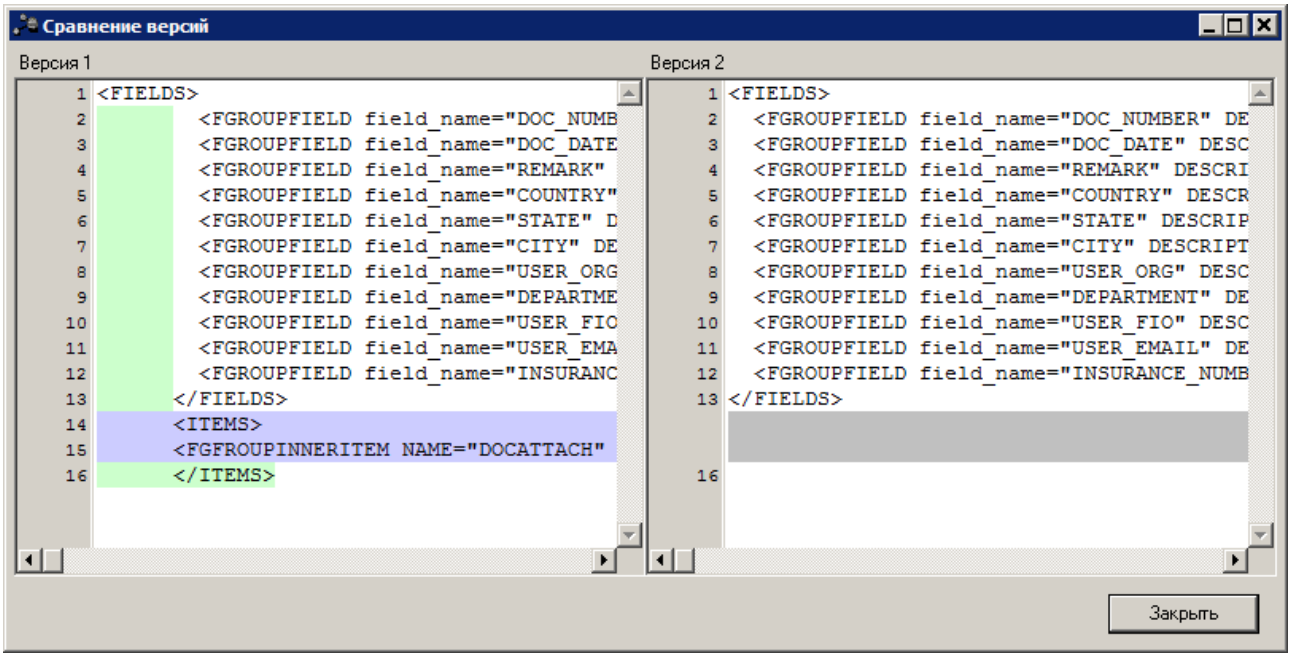

Рисунок 37 – Форма сравнения версий

Открывшаяся форма просмотра состоит из двух областей, содержащих XML-описание состава подписываемых полей сравниваемых версий. Отличающиеся строки XML-описания версий группы полей выделены цветом в обоих областях.

При наложении первой ЭП на документ используется версия выбранной группы полей, для которой включен признак **Актуальна**. Если признак **Актуальна** выключен для всех версий группы полей, выбор версии группы полей при наложении на документ первой ЭП осуществляется автоматически на основании даты подписываемого документа и даты версии группы полей. Выбирается версия группы полей, дата которой ближе всего к дате документа. Дата версии группы полей должна быть более ранней или равной дате подписываемого документа. Если не обнаружено ни одной версии, удовлетворяющей данному условию, на экран выводится сообщение: *«Не найдено групп полей, актуальных на дату документа»*.

Для формирования второй и последующих ЭП документа применяется версия группы полей, которая использовалась при наложении первой ЭП. При проверке ЭП применяется версия группы полей, которая использовалась при ее формировании.

При создании нового или изменении существующего правила обязательным является указание в форме правила статуса базового и/или дополнительного дерева сценариев обработки ЭД, на котором должно производиться подписание. Выбор статуса базового и/или дополнительного дерева сценариев обработки ЭД осуществляется в форме *Статусы документа*, вызываемой при заполнении полей **Базовый статус** и **Дополнительный статус** соответственно. При заполнении поля **Базовый статус** форма *Статусы документов* содержит перечень статусов базового дерева сценариев обработки ЭД, при заполнении поля **Дополнительный статус** – перечень статусов дополнительного дерева сценариев.

Примечание. *Поля* ***Базовый статус*** *и* ***Дополнительный статус*** *доступны для редактирования после заполнения поля* ***Группа полей****.*

Внимание! *В правиле подписания может одновременно указываться статус базового и статус дополнительного дерева сценариев обработки ЭД. Такое правило будет работать только для случаев, когда ЭД находится в заданном сочетании статусов базового дерева сценариев и дополнительного дерева сценариев.*

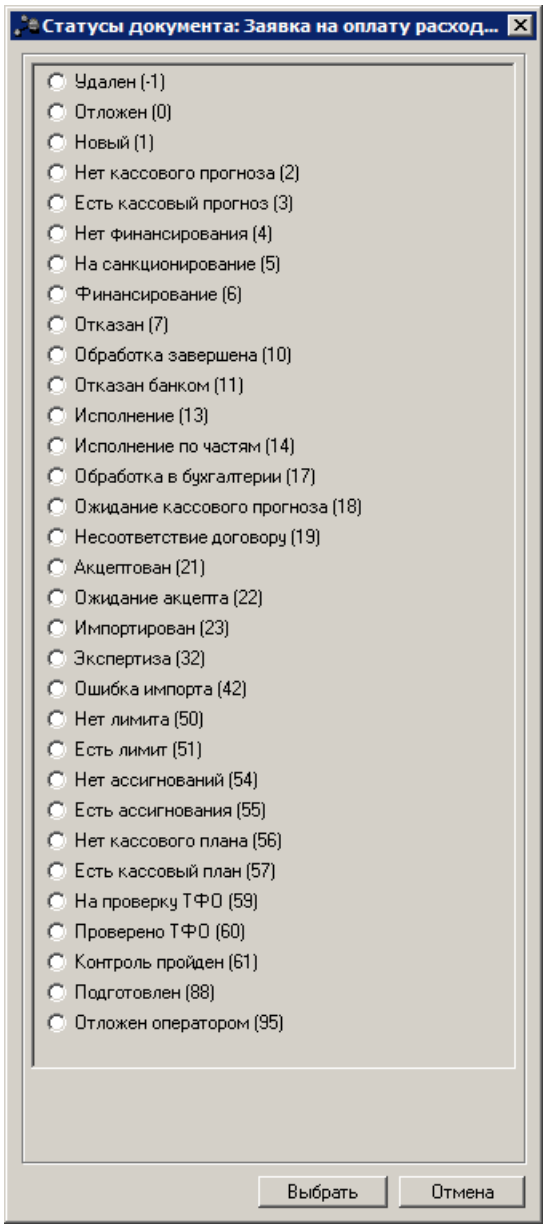

Рисунок 38 – Форма статусов документа

Назначение правилу подписания объектного идентификатора осуществляется выбором из справочника *Объектные идентификаторы*, который также доступен с помощью пункта меню **Справочники→Система→Объектные идентификаторы**:

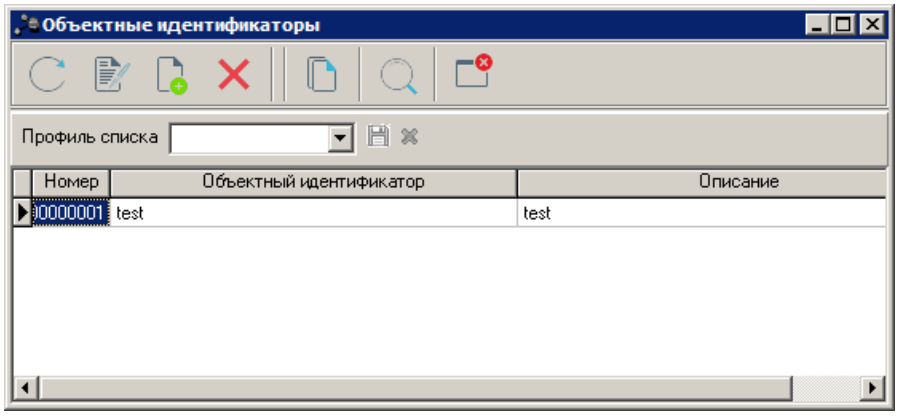

Рисунок 39 – Справочник «Объектные идентификаторы»

Примечание. ***Объектный идентификатор*** *– это числовая последовательность, разделенная точками, назначенная какому-либо объекту для его однозначной идентификации в мировом адресном пространстве объектных идентификаторов. С помощью объектных идентификаторов организация может специфицировать регламент обработки ЭД, подписываемых ЭП, для обеспечения его юридической значимости и осуществления контроля использования сертификатов ключей подписи в информационной системе. Для этого необходимо зарегистрировать объектные идентификаторы 35, определяющие установленный в организации и настроенный в системе регламент обработки ЭД, в УЦ.*

В списке *Роли* формируется перечень ЭП-ролей пользователей, которые должны подписать документ при достижении указанного в правиле статуса обработки. Для каждой ЭП-роли в списке предусмотрена возможность настройки автоматической обработки документа при его подписании:

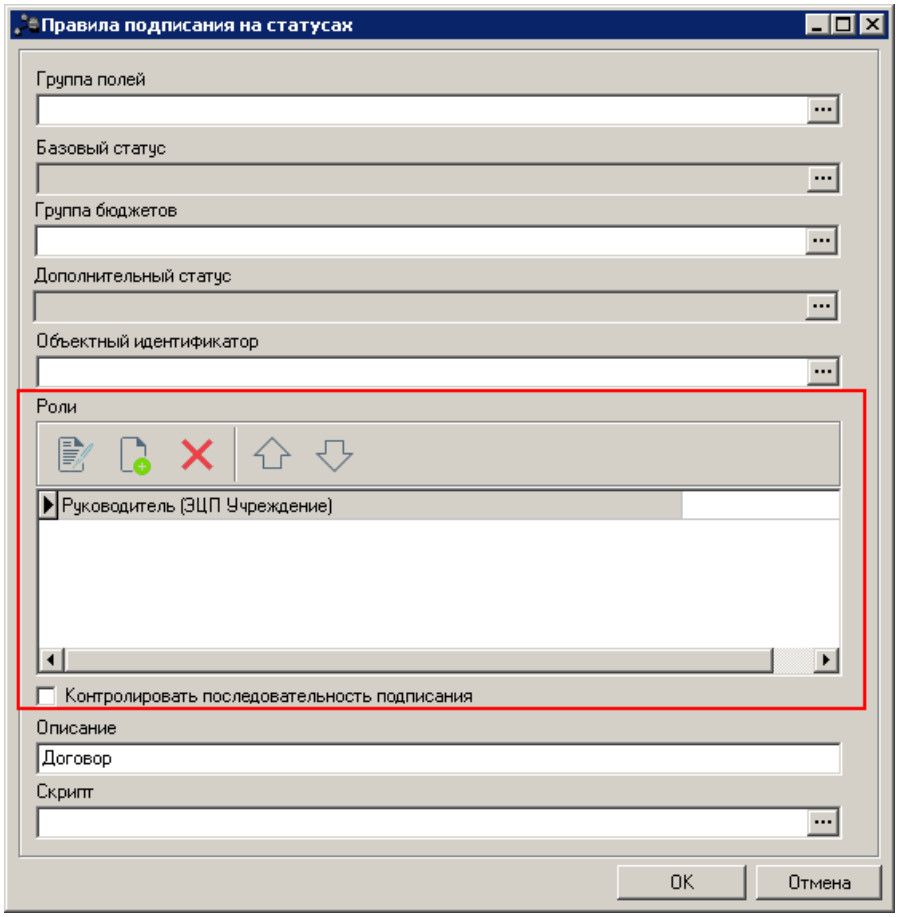

Рисунок 40 – Настройка ЭП-ролей в форме редактирования правила подписания на статусах

Управление списком ЭП-ролей, входящих в правило подписания документа, осуществляется с помощью кнопок на панели инструментов, расположенной непосредственно над списком ролей формы редактирования правила подписания на статусах 50. Форма редактирования строки списка открывается нажатием кнопки  **<F4>**. Чтобы удалить строку из списка, необходимо нажать кнопку  **<F8>**. Последовательность ролей в списке настраивается с помощью кнопок  и  . При включенном параметре **Контролировать последовательность подписания** срабатывает контроль последовательности наложения пользователями ЭП на документ в соответствии с заданной в списке последовательностью ролей. Контроль последовательности подписания осуществляется в разрезе группы полей, статуса документа и скрипта (поле **Скрипт**), содержащего условие выполнения правила, заданных в соответствующих полях формы редактирования правила подписания для данного класса документов.

Для создания новой записи справочника нажимается кнопка  <**F9**>. На экране появится форма записи справочника:

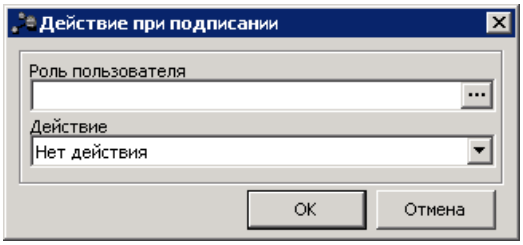

Рисунок 41 – Форма настройки действия при подписании

В форме новой записи справочника содержатся поля:

- **Роль пользователя** – ЭП-роль пользователя, который должен подписать документ в указанном в правиле статусе обработки. Поле доступно для редактирования. Значение выбирается из справочника *Роли пользователей системы* (справочник доступен также в пункте меню **Справочники→Система→Роли пользователей**), который открывается при нажатии кнопки вызова справочника. Записи справочника фильтруются по наличию признака **Роль ЭП**:

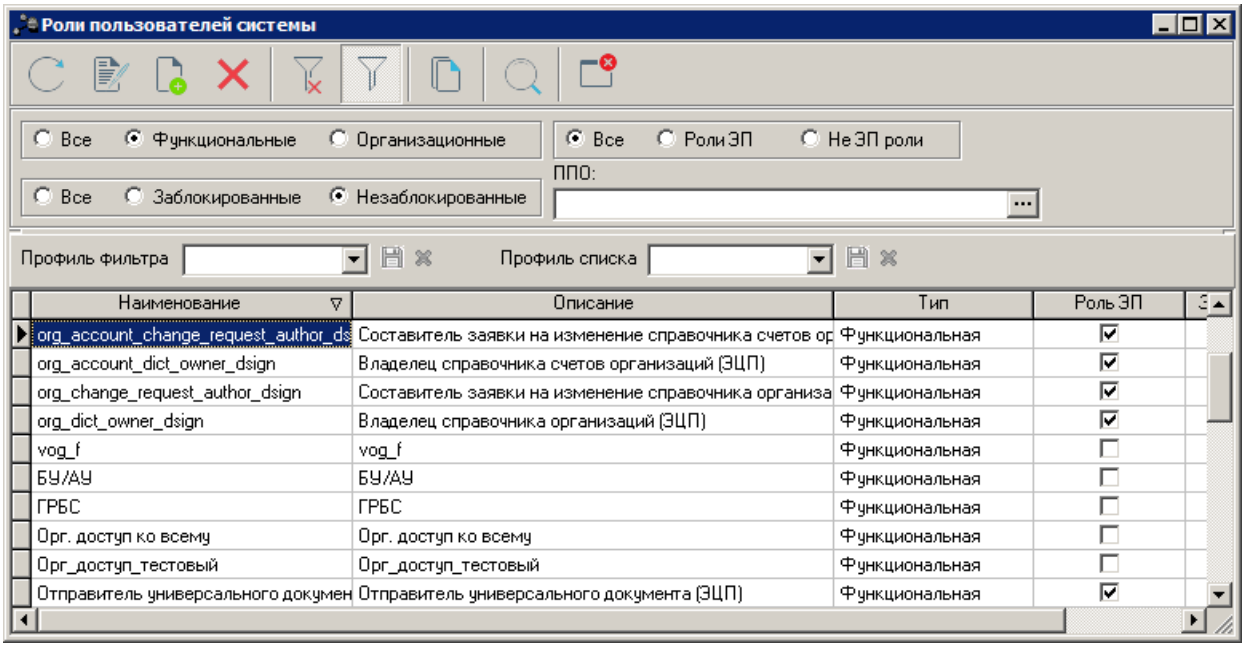

Рисунок 42 – Справочник «Роли пользователей системы»

- **Действие** – действие, которое должно быть автоматически выполнено над документом при подписании данного документа пользователем с указанной ЭП-ролью. Поле доступно для редактирования. Значение поля выбирается из раскрывающегося списка. В раскрывающемся списке содержится перечень действий, которые в соответствии с деревом обработки данного класса документов доступны в статусе обработки, указанном в правиле.
  Если при подписании документа ЭП-ролью не требуется производить автоматическую обработку документа, в поле выбирается значение *Нет действия*.

Примечание. *При удалении значений полей* ***Группа полей*** *и* ***Статус*** *формы правила настройка действий при подписании автоматически очищается.*

Для сохранения введенных настроек нажимается кнопка **ОК**, форма настройки действия при подписании закрывается и ЭП-роль добавляется в список входящих в правило ЭП-ролей.

Для настройки разветвленного регламента подписания документов со сложными процедурами согласования и большим количеством подписантов предусмотрена

возможность назначать правилам подписания документов условия выполнения, представляющие собой скриптовые конструкции. Скрипты позволяют настроить регламент подписания документов в зависимости от значений полей:

- документа, указанного в правиле, включая поля строк;
- связанных документов, включая поля строк;
- ЭП, наложенных на документ;
- ЭП связанных документов.

Скрипт назначается в форме редактирования правила подписания 50 в поле **Скрипт**. В поле указывается название скриптовой конструкции, описывающей условие выполнения правила. Значение поля выбирается в :

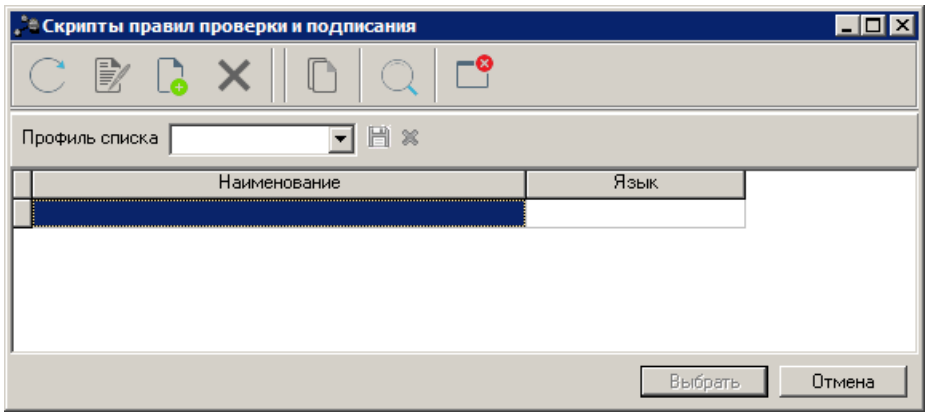

Рисунок 43 – Справочник скриптов подписания и проверки ЭП

Справочник содержит перечень скриптов, которые могут назначаться правилам подписания документов и правилам проверки ЭП. Каждому правилу может назначаться только один скрипт. Редактирование записей справочника и добавление новых скриптов осуществляется с помощью редактора скриптов:

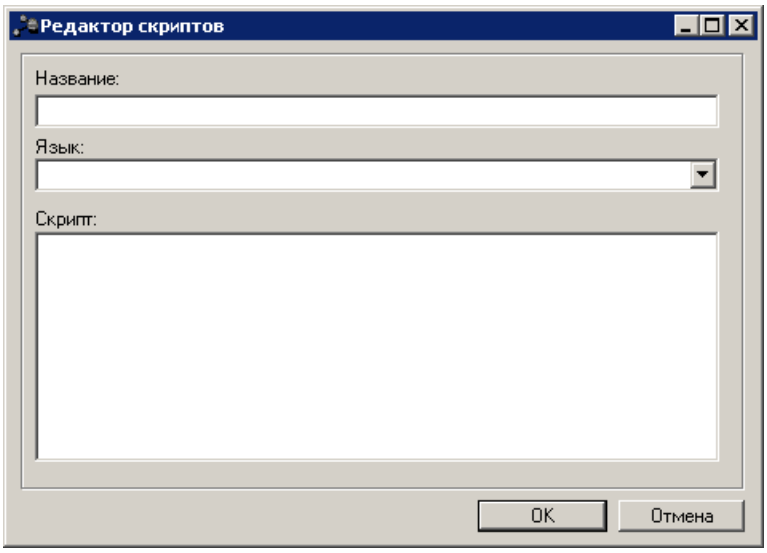

Рисунок 44 – Форма редактора скриптов

В форме новой записи справочника содержатся поля:

- **Название –** название скрипта.
- **Язык** - язык, на котором написан скрипт. Значение выбирается из раскрывающегося списка. Для написания скриптов используется язык программирования Groovy.
- **Скрипт** - поле для введения скриптовой конструкции.

Скрипт, назначенный конкретному правилу подписания, выполняется в момент подписания документа при нажатии кнопки **Подписать**. Процедура подписания документа в соответствии с настройками правила зависит от результатов выполнения назначенного скрипта (возвращенного значения). Если в результате выполнения скрипта возвращено значение «истина», осуществляется подписание электронного документа в соответствии с настройками правила. Если возвращено значение «ложь», подписание не производится. Если возвращенное значение отличается от значений «истина» или «ложь», подписание не производится. Выводится сообщение о том, что условие подписания составлено некорректно.

При попытке подписания документа производится проверка выполнения скриптов для всех групп полей, включая группы полей вложений, которые имеют настроенные правила подписания в данном статусе. Если в результате проверки установлена доступность операции подписания для группы полей ЭД и недоступность для группы полей вложения в ЭД, система позволяет подписать ЭД и не позволяет подписать вложение в ЭД. Если в результате проверки установлена недоступность операции подписания для группы полей ЭД и доступность для группы полей вложения в ЭД, система не позволяет подписать ЭД и позволяет подписать вложение в ЭД.

Ниже приведены примеры скриптовых конструкций, которые могут вводиться в справочник с помощью редактора скриптов и применяться к правилам подписания и проверки:

1. Всегда возвращать значение «истина»:

```
return  true;
```

2. Всегда возвращать значение «ложь»:

```
return false;
```

3. Настройка правил подписания и правил проверки ЭП конкретного документа по его идентификационному номеру:

```
return document.id.getLongValue() == <ID>;
```

В скрипт передается параметр *document*, обозначающий инстанс документа, к которому применяется правило.

4. Настройка правил подписания и правил проверки ЭП в документах по идентификационному номеру бюджета, к которому принадлежит документ:

```
return document.budget_id.getLongValue() == <ID>;
```

5. Настройка правил подписания и правил проверки ЭП в документах по идентификационному номеру бланка расходов, к которому принадлежит документ:

```
return document.expCodes.estimate_id.getLongValue()  == <ID>;
```

6. Настройка правил подписания и правил проверки ЭП в документах по идентификационному номеру бланка расходов, являющегося родительским по

отношению к бланку расходов, к которому принадлежит документ:

```
return com.bssys.azkserver.expense.EstimateObject.getParentEstimateID(con, document.expCodes.estimate_id.value) == <ID>;
```

7. Настройка различных правил подписания и правил проверки ЭП для одного и того же класса ЭД в зависимости от класса его родительского документа:

```
final com.bssys.server.docflow.DocumentObject parentDoc = document.getParentDoc(con, com.bssys.server.DataObject.LOCK_NONE);
return parentDoc != null && parentDoc.documentclass_id.value == <CLASS_ID>L;
```

Использование скриптов для определения условий выполнения правил подписания документов позволяет производить только чтение данных из БД, изменение данных при использовании скриптов недоступно.

4.4.2.2 Настройка правил проверки ЭП на статусах

Регламент проверки ЭП на статусах ЭД настраивается в справочнике *Правила проверки подписей на статусах*, доступном с помощью пункта меню **Справочники→Система→Правила проверки подписей на статусах**:

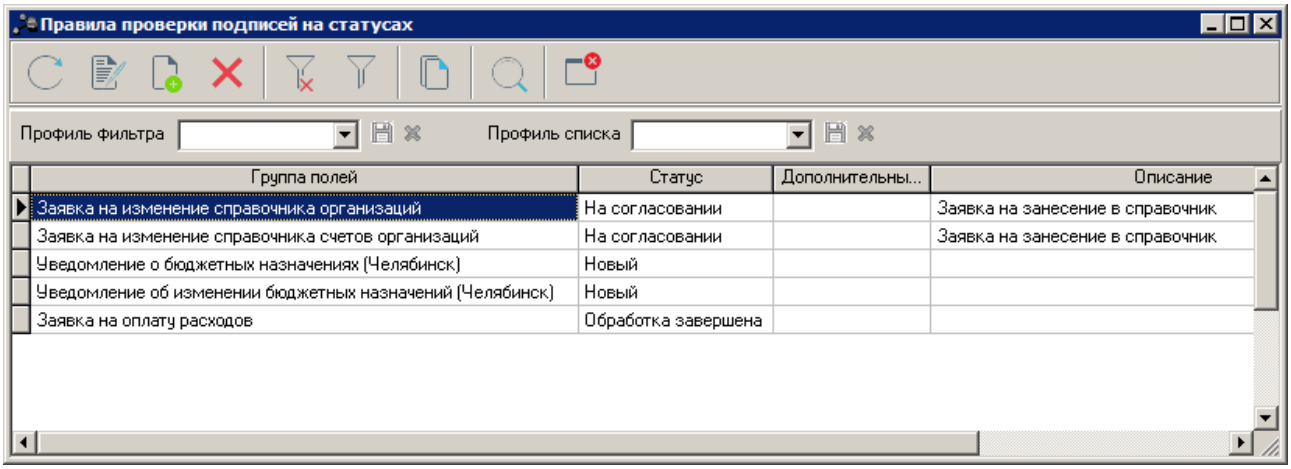

Рисунок 45 – Справочник «Правила проверки подписей на статусах»

Данные этого справочника определяют правила контроля наличия у электронных документов (групп полей) валидных ЭП определенных ролей на конкретных этапах жизненного цикла (статусах). Каждое правило проверки определяет возможность перевода ЭД на указанный в правиле статус при условии наличия у документа валидных ЭП указанных ролей.

***Примечание**. Применение правил ЭП настраивается в разрезе организаций, формирующих документы, в пункте меню **Сервис→Системные параметры→**, закладка **Применение правил** .*
*С помощью системного параметра **Не проверять для ЭД следующих организаций** настраивается список организаций-исключений, для документов которых не требуется проверять ЭП.*
Более подробно работа системных параметров рассмотрена в документации «».

В верхней части списка документов находится панель инструментов, на которой располагаются стандартные функциональные кнопки. С их помощью можно выполнить следующие действия: создать запись справочника, открыть форму редактирования или просмотра записи справочника, обновить список записей, скопировать список записей в буфер обмена и осуществить поиск записи в списке.

Панель фильтрации становится доступной при нажатии кнопки  . На панели фильтрации можно выбрать следующие параметры: **Класс документа**, **Группа полей**, **Статус**, **Роли**, **Активность**.

Поле **Профиль фильтра** используется для хранения профилей параметров фильтрации списка документов, списка записей справочников, списка строк АРМ и редакторов. Поле **Профиль списка** используется для хранения профилей настроек порядка следования и видимости колонок в списках документов, списках записей справочников, списках строк АРМ и редакторов.

Для удаления выбранных параметров нажимается кнопка  .

При создании нового или изменении существующего правила указываются:

- **Группа полей** – группа полей ЭД, для которого настраивается правило подписания. Выбирается из справочника *Группы полей* 52.
- **Статус** – статус базового дерева сценариев обработки ЭД, на котором производится проверка. Значение выбирается в форме *Статусы документа* 56, содержащей перечень статусов базового дерева сценариев обработки ЭД.
- **Группа бюджетов** – группа бюджетов ЭД, для которого настраивается правило подписания.
- **Дополнительный статус** – статус дополнительного дерева сценариев обработки ЭД, на котором производится проверка. Значение выбирается в форме *Статусы документа* 56, содержащей перечень статусов дополнительного дерева сценариев обработки ЭД.

***Примечание.** Поля **Статус** и **Дополнительный статус** доступны для редактирования после заполнения поля **Группа полей**.*

***Внимание!** В правиле проверки может одновременно указываться статус базового и статус дополнительного дерева сценариев обработки ЭД. Проверка ЭП производятся отдельно при обработке ЭД по статусам базового дерева сценариев и при обработке ЭД по статусам дополнительного дерева сценариев.*

- **Роли** – совокупность ЭП-ролей, которыми должен быть подписан документ (группа полей) для его перевода на указанный статус. Выбираются в справочнике *Роли пользователей* 59.
- **Описание** – текстовое описание правила проверки ЭП.
- **Правило активно** – признак активности правила проверки.
- **Скрипт** – название скрипта, описывающего условие выполнения правила проверки подписей на статусах.

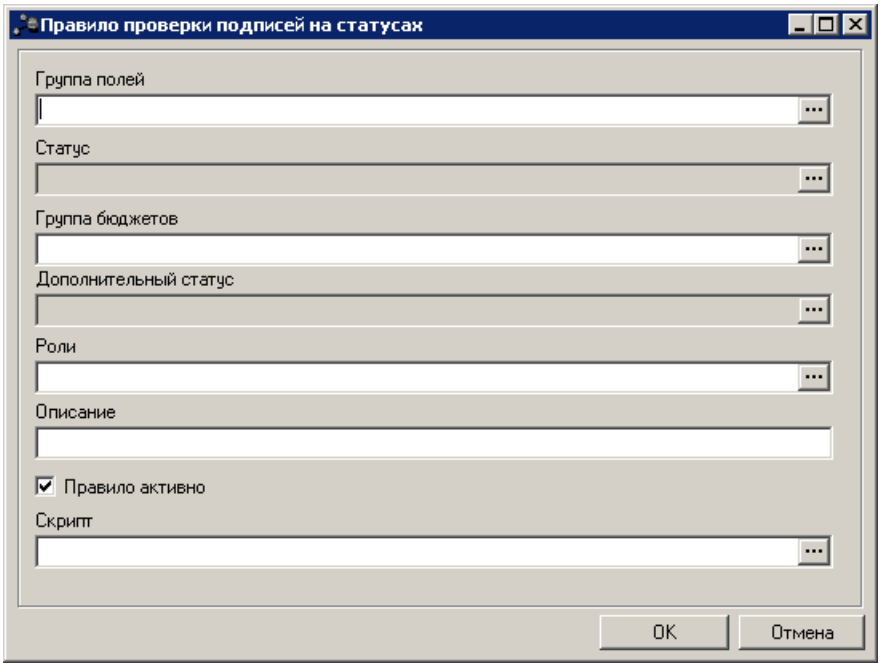

Рисунок 46 – Форма создания правила проверки подписей на статусах

Для настройки разветвленного регламента подписания документов со сложными процедурами согласования и большим количеством подписантов предусмотрена возможность назначать правилам проверки подписей документов условия выполнения, представляющие собой скриптовые конструкции. Скрипты позволяют настроить проверку соответствия ЭП документов регламенту подписания в зависимости от значений полей:

- документа, указанного в правиле, включая поля строк;
- связанных документов, включая поля строк;
- ЭП, наложенных на документ;
- ЭП связанных документов.

Скрипт назначается в форме редактирования правила проверки в поле **Скрипт**. В поле указывается название скриптовой конструкции, описывающей условие выполнения правила. Значение поля выбирается в .

***Примечание**. Параметры и порядок заполнения , а также примеры скриптов рассмотрены в разделе **Настройка правил подписания документов на статусах** 60*

Скрипт, назначенный конкретному правилу проверки ЭП, выполняется в момент перехода электронного документа в статус, для которого настроено данное правило. Процедура проверки ЭП в соответствии с настройками правила при обработке документа до заданного статуса зависит от результатов выполнения назначенного скрипта (возвращенного значения). Если в результате выполнения скрипта возвращено значение *«истина»*, проверка ЭП документа осуществляется в соответствии с настройками правила. Если возвращено значение *«ложь»*, проверка ЭП документа не производится, документ обрабатывается до заданного статуса. Если возвращенное значение отличается от значений *«истина»* и *«ложь»*, проверка ЭП документа не производится, документ возвращается в предыдущий статус. При этом на экран выводится сообщение о том, что условие проверки составлено некорректно.

Использование скриптов для определения условий выполнения правил проверки ЭП документов позволяет производить только чтение данных из БД, изменение данных при

использовании скриптов недоступно.

***Примечание**. Правила проверки ЭП вложений (соответствующих им групп полей) в статусах описываются аналогичным образом в справочнике «Правила проверки ЭП на статусах».*
Если электронный документ имеет вложения, привязанные к определенной группе полей, по которой настроено правило проверки ЭП, дальнейшая обработка документа возможна только при условии наличия и валидности ЭП всех вложений.

4.4.3 Настройка подписываемых данных вложений

Для обеспечения возможности подписания вложений ЭД, подписываемые вложения должны быть предварительно привязаны к специально настроенным группам полей, которые выступают своего рода «подписываемым контейнером» для файлов вложений.

Привязка вложений к группам полей производится в момент присоединения файла вложения к ЭД (при включенном системном параметре **Привязывать вложения к группам полей**), либо может быть осуществлена после присоединения 65, в форме привязки вложений к группам полей.

Процесс настройки групп полей для подписываемых вложений описан в **Приложении 19**.

4.4.3.1 Привязка вложений к группам полей при присоединении подписываемых вложений к ЭД

Для присоединения вложения к документу необходимо воспользоваться кнопкой (**Файлы**), расположенной в нижней части формы ЭД. При этом откроется форма списка вложенных документов:

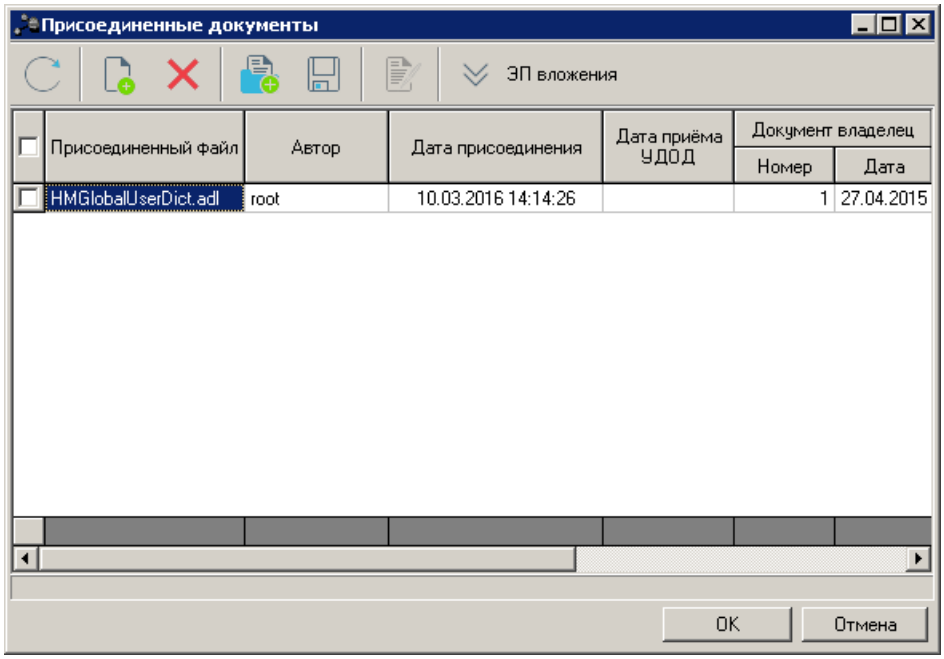

Рисунок 47 –Список вложенных документов

В форме новой записи справочника содержатся поля:

- **Присоединенный файл** – имя присоединенного файла;
- **Автор** – учетная запись пользователя, присоединившего файл;
- **Дата присоединения** – дата/время присоединения файла;
- **Дата приема УДОД** – дата/время приема УДОД;
- **Документ владелец/Номер** – номер документа, к которому присоединен файл;
- **Документ владелец/Дата** – дата документа, к которому присоединен файл;
- **Группа полей** – группа полей, к которой привязано вложение;
- **Количество ЭП** – количество ЭП, которыми подписано вложение;
- **Категории вложений** – категория вложения, присоединяемого к документу.

Примечание**. Для просмотра ЭП вложения необходимо выделить вложение в списке и нажать кнопку*  *на панели инструментов формы. В результате в нижней части формы отобразится список ЭП выбранного вложения. Более подробное описание приведено в разделе* ***Просмотр ЭП вложения в списке вложенных документов 87

Для присоединения файла к документу нажимается кнопка **Новый** панели инструментов окна или клавиша **<F9>** клавиатуры. В открывшемся окне выбирается файл вложения.

Если включен системный параметр **Автоматически привязывать вложения к группам полей**, привязка вложения к группам полей осуществляется автоматически в момент прикрепления вложения: к первой найденной группе полей с *GROUP_TYPE="attach"*, соответствующей классу ЭД, к которому происходит прикрепление вложения.

Просмотр и редактирование привязки вложения к группе полей осуществляется в окне, вызываемом нажатием кнопки  (**Привязать к группе полей...**) на панели

инструментов формы списка вложенных документов:

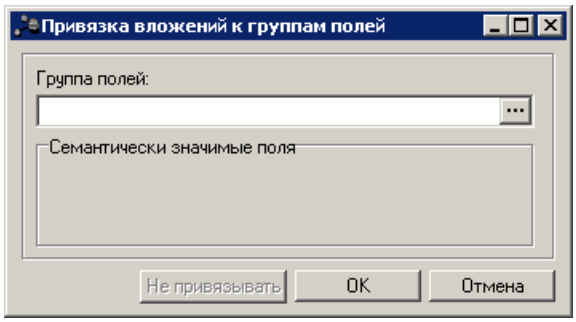

Рисунок 48 – Привязка вложений к группам полей

В поле **Группа полей** выбирается группа полей, к которой требуется привязать вложение. Поле заполняется путем выбора значения из справочника 52 *Группы полей* 52, отфильтрованного по классу документа, к которому прикреплено вложение. После выбора нужной группы полей нажимается кнопка **ОК**.

Примечание. *Кнопка* ***Не привязывать*** *не используется, т.к. осуществляется автоматическая привязка к группам полей*

Существует возможность настройки прав доступа пользователя на привязку вложений к группе полей в зависимости от класса и статуса ЭД. Для этого предназначен параметр **Привязывать вложения к группам полей в соответствии с доступом к категориям**. После активации параметра в окне привязки вложения к группе полей становятся доступными и отображаются для привязки только группы полей с полным уровнем доступа для данного пользователя и статуса ЭД.

Примечание*. Параметр* ***Привязывать вложения к группам полей в соответствии с доступом к категориям*** *включается/отключается выполнением соответствующего xml-скрипта –* ***sysparam.xml****. По-умолчанию параметр выключен.*

Для присоединения файла к документу нажимается кнопка **Новый** панели инструментов окна или клавиша **<F9>** клавиатуры. В открывшемся окне выбирается файл вложения.

Если включен системный параметр **Автоматически привязывать вложения к группам полей**, привязка вложения к группам полей осуществляется автоматически в момент прикрепления вложения: к первой найденной группе полей с *GROUP_TYPE="attach"*, соответствующей классу ЭД, к которому происходит прикрепление вложения.

Просмотр и редактирование привязки вложения к группе полей осуществляется в окне, вызываемом нажатием кнопки  (**Привязать к группе полей...**) на панели инструментов формы списка вложенных документов:

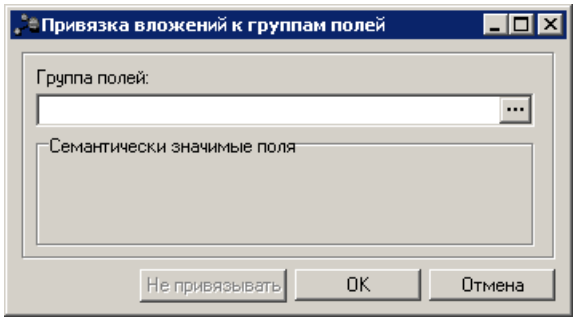

Рисунок 49 – Привязка вложений к группам полей

В поле **Группа полей** выбирается группа полей, к которой требуется привязать вложение. Поле заполняется путем выбора значения из справочника[52] *Группы полей*[52], отфильтрованного по классу документа, к которому прикреплено вложение. После выбора нужной группы полей нажимается кнопка **ОК**.

Примечание. *Кнопка* ***Не привязывать*** *не используется, т.к. осуществляется автоматическая привязка к группам полей*

Существует возможность настройки прав доступа пользователя на привязку вложений к группе полей в зависимости от класса и статуса ЭД. Для этого предназначен параметр **Привязывать вложения к группам полей в соответствии с доступом к категориям**. После активации параметра в окне привязки вложения к группе полей становятся доступными и отображаются для привязки только группы полей с полным уровнем доступа для данного пользователя и статуса ЭД.

Примечание*. Параметр* ***Привязывать вложения к группам полей в соответствии с доступом к категориям*** *включается/отключается выполнением соответствующего xml-скрипта –* ***sysparam.xml****. По-умолчанию параметр выключен.*

5

Использование модуля подсистемы

5.1 Подписание электронных документов

5.1.1 Подписание документа в списке документов

Для подписания документа в списке документов необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, который необходимо подписать.
3. Нажатием правой кнопки мыши вызвать контекстное меню для этого документа и выбрать пункт **Подписать**.

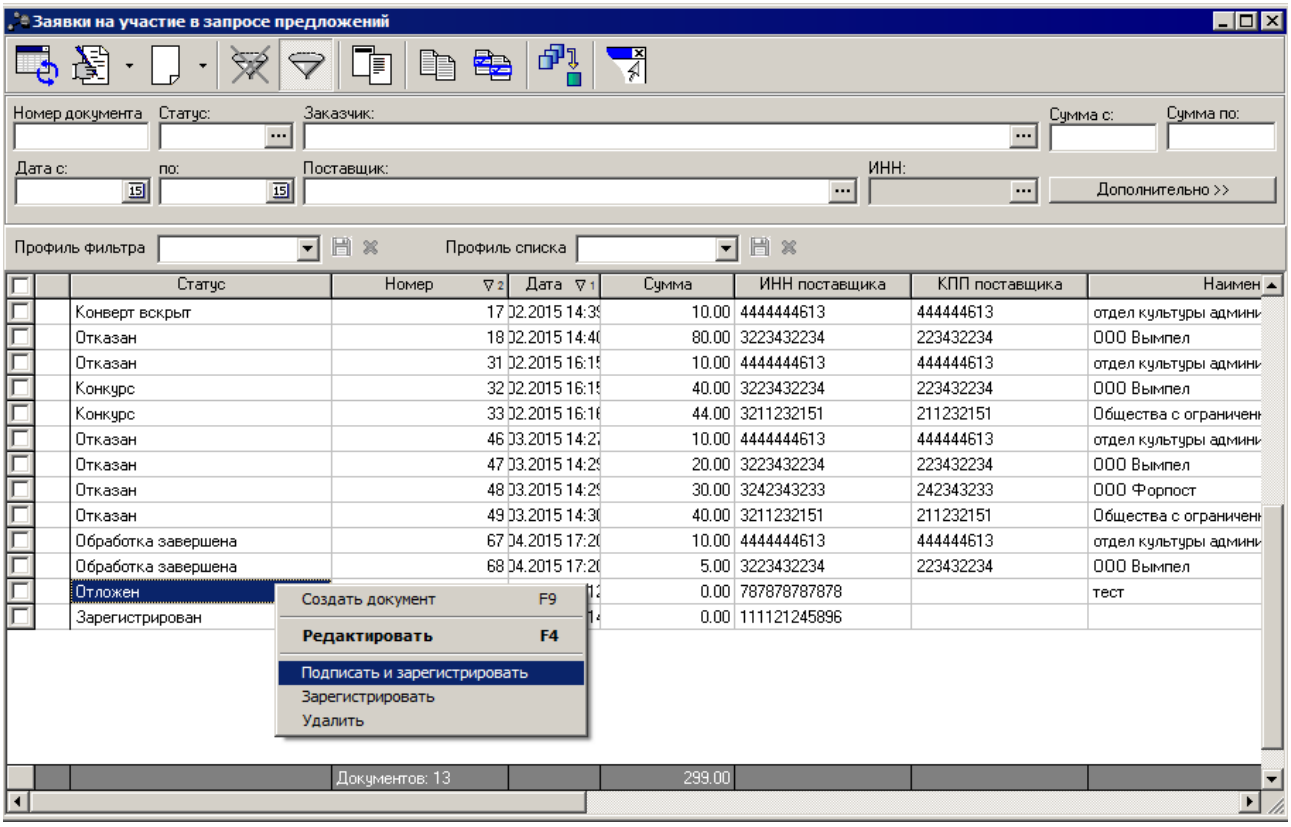

Рисунок 50 – Действие «Подписать» в контекстном меню списка докуменов

На экране появится окно Формирование электронной подписи (ЭП):

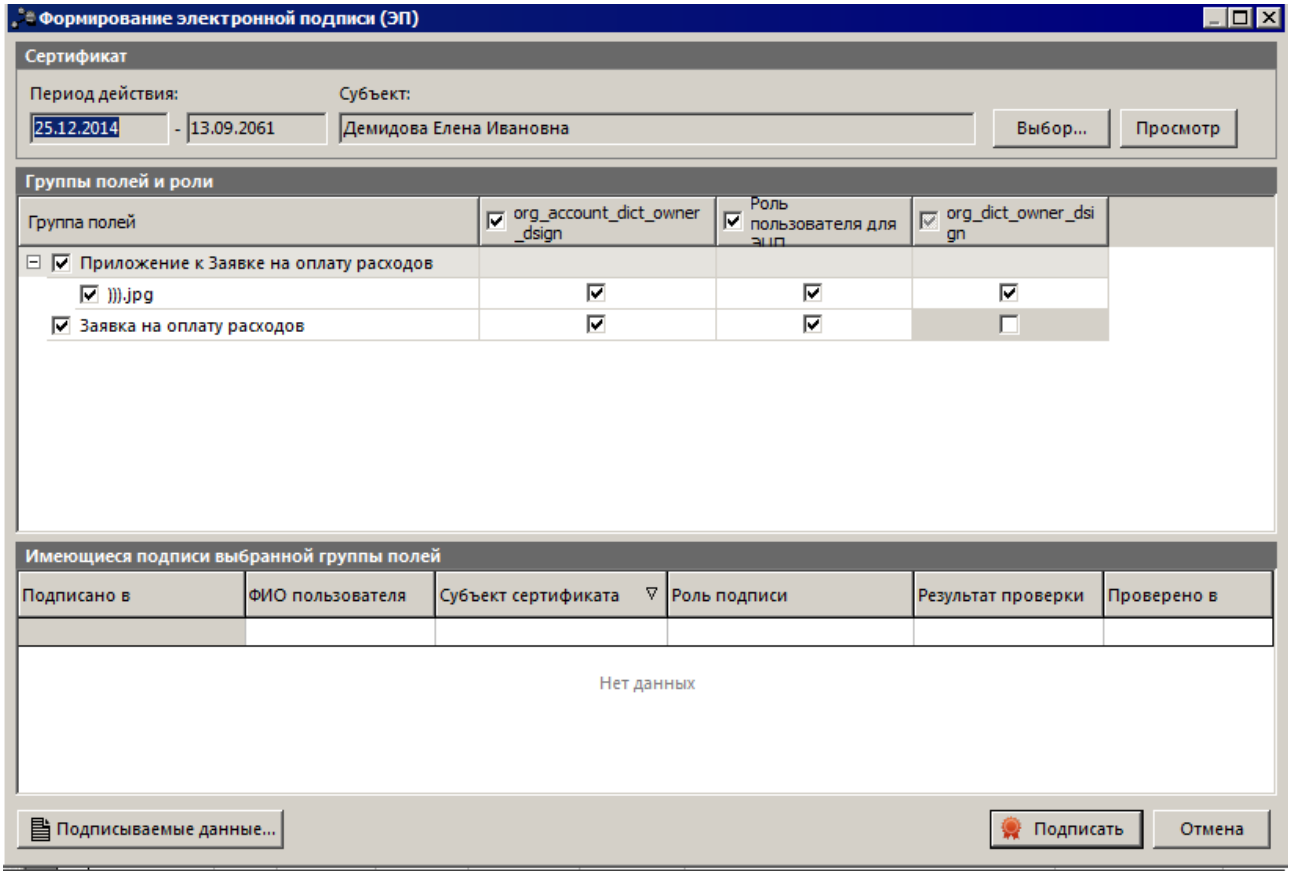

Рисунок 51 – Окно «Формирование электронной подписи (ЭП)»

Окно *Формирование электронной подписи (ЭП)* состоит из следующих элементов:

- группа полей **Сертификат** – в группе полей содержатся реквизиты сертификата, который используется для подписания документа/вложенного файла. Выбор сертификата осуществляется с помощью кнопки **Выбор**. В результате выбора сертификата автоматически заполняются поля:
  - **Период действия** – срок действия сертификата пользователя. Обязательное для заполнения, недоступно для редактирования.
  - **Субъект** – физическое лицо, на имя которого УЦ выдал сертификат и который владеет закрытым ключом ЭП. Обязательное для заполнения, недоступно для редактирования.

  Для просмотра выбранного сертификата нажимается кнопка **Просмотр**.
- таблица **Группы полей и роли** – в таблице определяется какие документы (группы полей) какими ролями пользователя должны быть подписаны с использованием выбранного сертификата. Таблица **Группы полей и роли** состоит из следующих элементов:
  - список *Группа полей* – иерархический список групп полей (документов и вложенных файлов), доступных для подписания. В списке *Группа полей* выбираются документы и вложенные файлы, которые требуется подписать с использованием выбранного сертификата.
  - группа колонок *ЭП-роли пользователя* – набор ЭП-ролей, каждой из которых соответствует отдельная колонка. ЭП-роль отображается в таблице, если она входит в правило подписания (справочник *Правила подписания документов на статусах*) хотя бы одного документа/вложенного файла из списка *Группа полей* и назначена пользователю, вызвавшему форму подписания. Для группы колонок доступны следующие действия контекстного меню:
    - **Выделить все** – при выборе действия на выделенной колонке Роли ЭП, если параметры в строках колонки не включены и доступны для изменения, то включить.
    - **Очистить все** – при выборе действия на выделенной колонке Роли ЭП, если параметры в строках колонки включены и доступны для изменения, то выключится.

Примечание. *Действия контекстного меню недоступны при подписании списка документов.*

- список **Имеющиеся подписи выбранной группы полей** – список ЭП, наложенных ранее на группу полей, выделенную в списке *Группа полей* таблицы **Группы полей и роли**. Список доступен только для просмотра.

4. В окне *Формирование подписи* для выбора сертификата нажать кнопку **Выбор**. В открывшейся форме *Сертификаты* отображается список всех сертификатов текущего пользователя, отфильтрованный по дате действия и признакам **Отозван** и **Заблокирован**. В списке выбтрается необходимый сертификат и нажимается кнопка **ОК**:

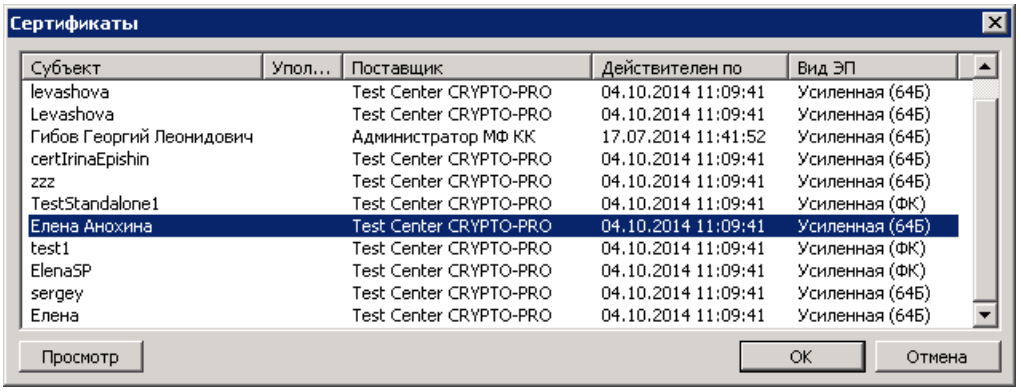

Рисунок 52 – Форма выбора сертификата пользователя

Информация о выбранном сертификате автоматически отобразится в группе полей **Сертификат** окна *Формирование электронной подписи (ЭП)*.

5. В таблице **Группы полей и роли** выбрать документы/вложенные файлы, которые требуется подписать с использованием выбранного сертификата, и ЭП-роли, которыми они должны быть подписаны.

   Документы/вложенные файлы, которые требуется подписать с использованием выбранного сертификата, выбираются в списке *Группа полей* таблицы **Группы полей и роли**. Для выбора требуется поставить отметки рядом с наименованиями нужных документов/вложенных файлов. По умолчанию в списке выбраны все доступные для подписания документы и вложенные файлы.

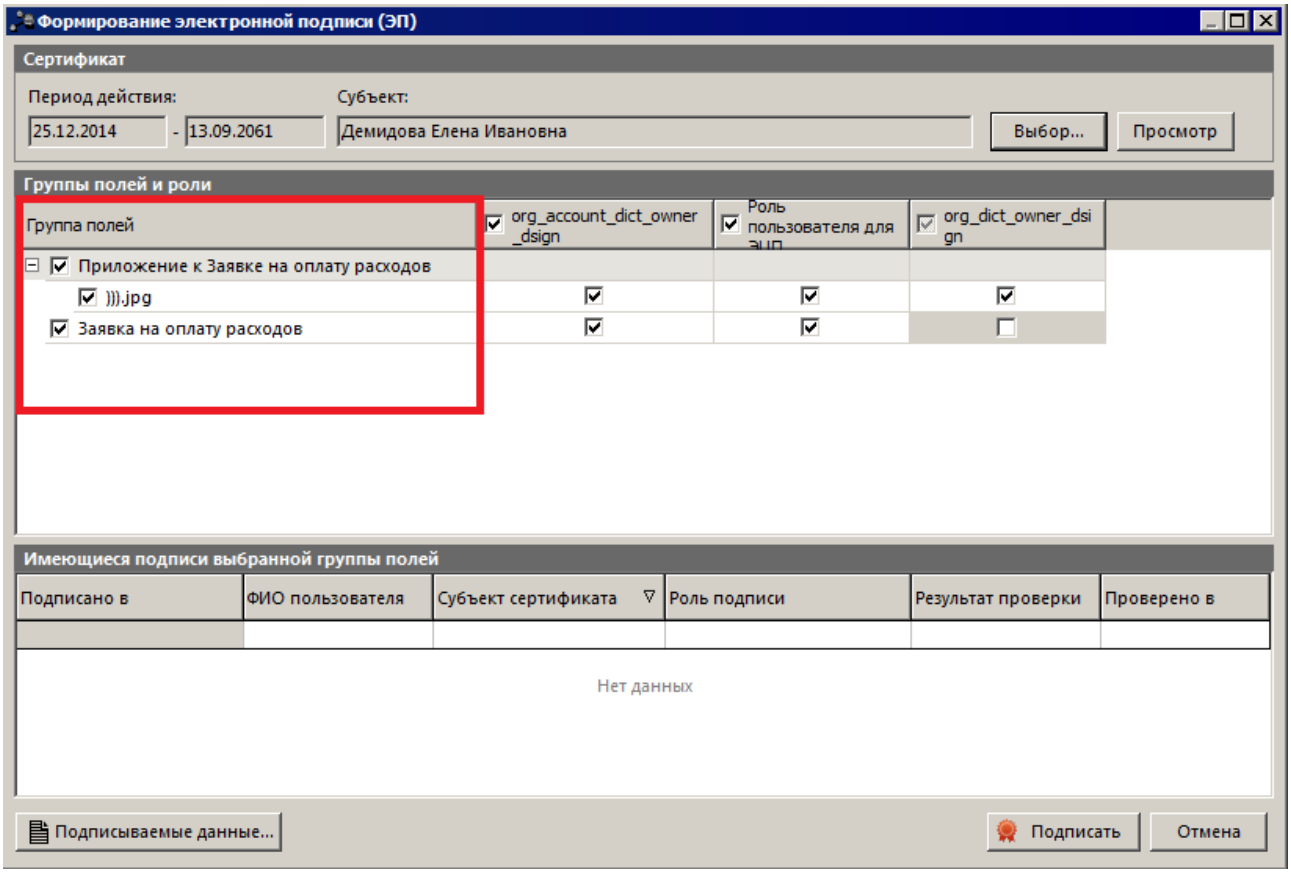

Рисунок 53 – Фрагмент окна «Формирование электронной подписи (ЭП)», список «Группа полей» таблицы «Группы полей и роли»

В группе колонок *ЭП-роли пользователя* таблицы **Группы полей и роли** для каждого документа/вложенного файла, выделенного в списке *Группа полей*, выбрать ЭП-роль, которой он должен быть подписан с использованием выбранного сертификата. Для этого напротив документа/вложенного файла поставить отметку в колонке ЭП-роли, которой требуется подписать документ/вложенный файл. По умолчанию отмечаются все ЭП-роли, входящие в правило подписания выбранного документа.

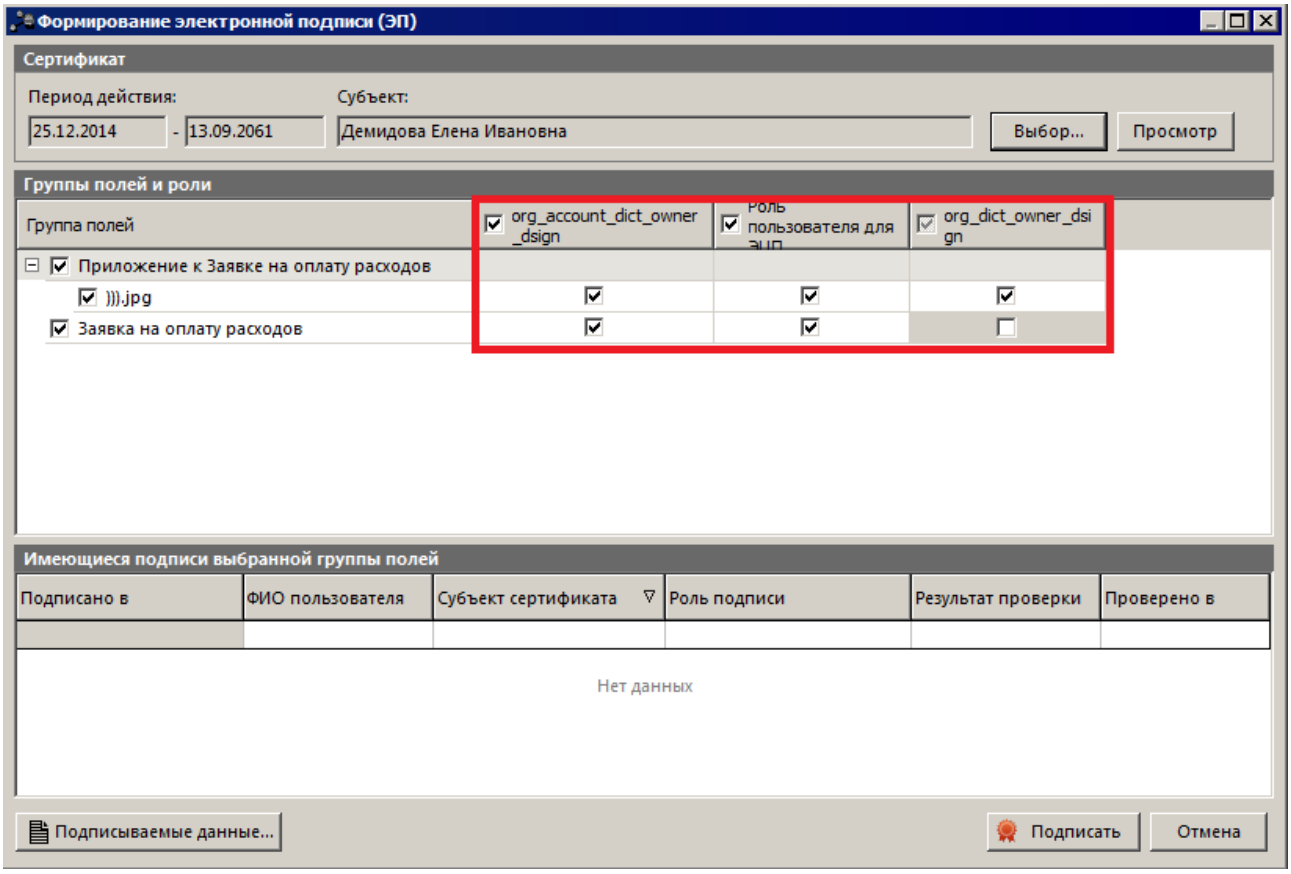

Рисунок 54 – Фрагмент окна «Формирование электронной подписи (ЭП)», группа колонок «ЭП-роли пользователя» таблицы «Группы полей и роли»

Проставление отметки в строках колонок ЭП-ролей недоступно, если документ/вложенный файл не выделен в списке *Группа полей* или ЭП-роль, указанная в наименовании колонки, не входит в правило подписания документа/вложенного файла, указанного в строке списка *Группа полей*.

6. Перед подписанием документа нажать кнопку **Подписываемые данные..**. окна *Формирование электронной подписи (ЭП)*. В открывшемся окне *Подписываемые данные* проверить правильность подписываемой информации (дайджеста) и нажать кнопку **Закрыть**.

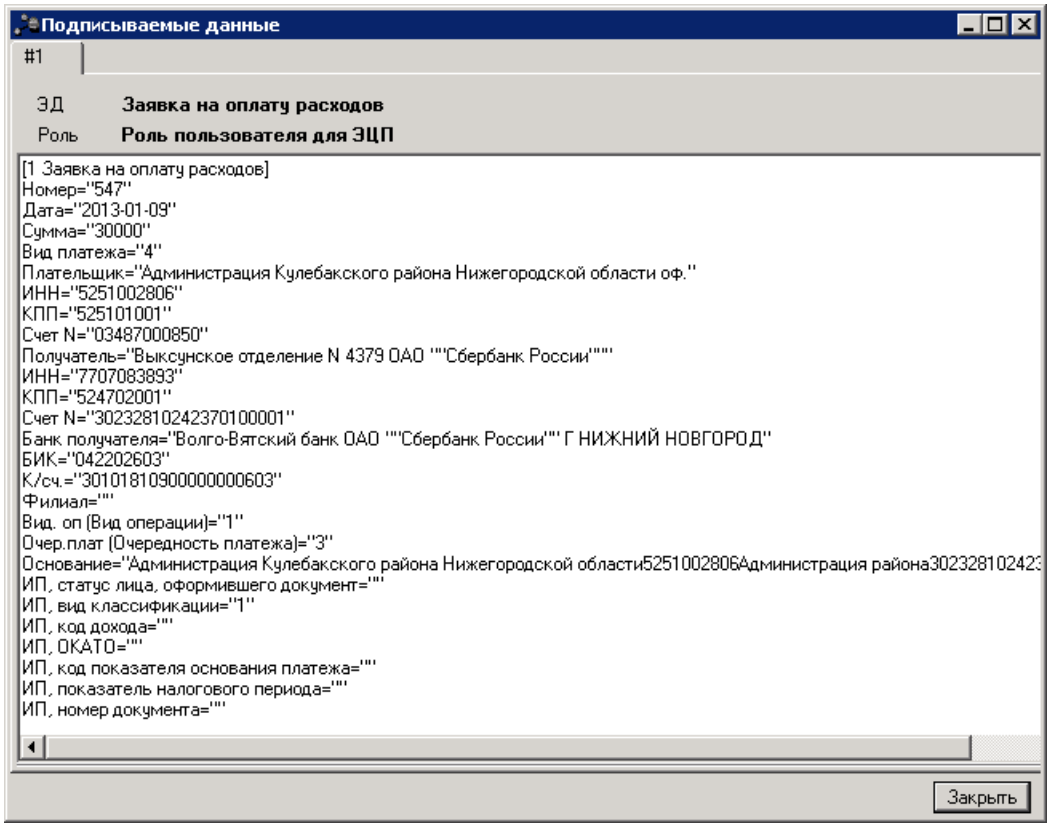

Рисунок 55 – Подписываемые данные электронного документа

7. Для подписания документа нажимается кнопка **Подписать** окна *Формирование электронной подписи (ЭП)*. Чтобы отменить действие, нажимается кнопка **Отмена**.
8. При подписании ЭД (нажатии на кнопку **Подписать**) осуществляются следующие контроли:

- Контроль последовательности подписания выполняется, если в правило подписания документа входит более одной роли и в форме правила включен параметр **Контролировать последовательность подписания**. Подписание документа становится недоступным, если в поле **Роль пользователя ЭП** окна формирования подписи выбрана роль, которая нарушает заданную в правиле последовательность подписания. На экране появится сообщение об ошибке с указанием ролей, валидные подписи которых должны быть наложены на документ перед подписанием документа выбранной ролью:

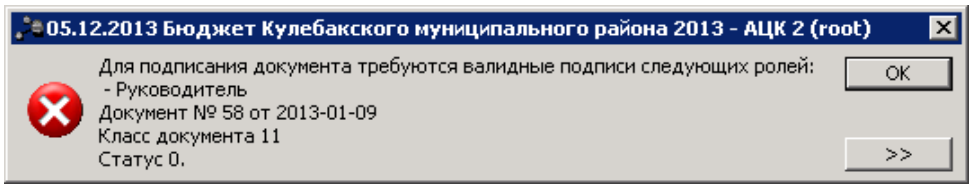

Рисунок 56 – Сообщение о непрохождении контроля последовательности подписания

- Если ЭД был изменен другим пользователем, ЭП не сохраняется. На экране появляется соответствующее сообщение об ошибке.

- Если в окне формирования подписи выбрано более одной роли и в правиле подписания для этих ролей настроены разные действия, на экране появиться предупреждающее сообщение:

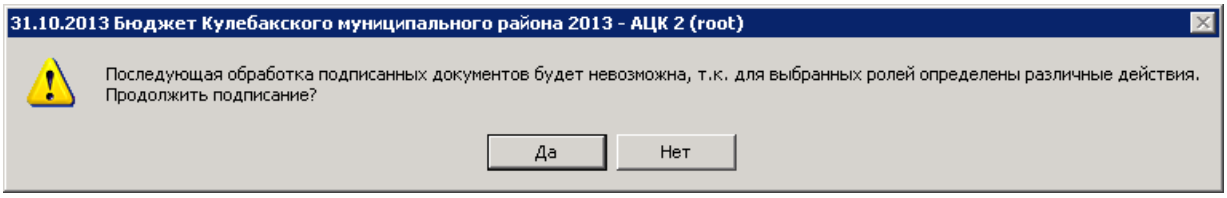

Рисунок 57 – Предупреждающее сообщение

Для отмены процедуры подписания и возврата к окну формирования подписи нажимается кнопка **Нет**.
Для выполнения процедуры подписания без последующей автоматической обработки документа нажимается кнопка **Да**.

9. По завершении процедуры формирования ЭП выдается сообщение с результатами процедуры подписания. Для закрытия формы сообщения с результатами процедуры подписания нажимается кнопка **Закрыть**:

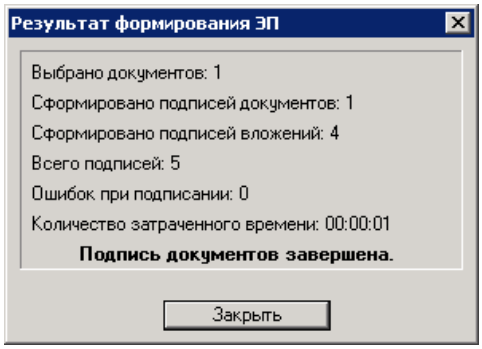

Рисунок 58 – Форма сообщения о результатах процедуры подписания

10. Если для ЭП-роли, которой произведено подписание документа, в соответствующем правиле подписания документа (справочник *Правила подписания документов на статусах*, пункт меню **Справочники→Система**) настроена автоматическая обработка при подписании, при закрытии формы сообщения с результатами подписания на экране появится запрос на обработку документа:

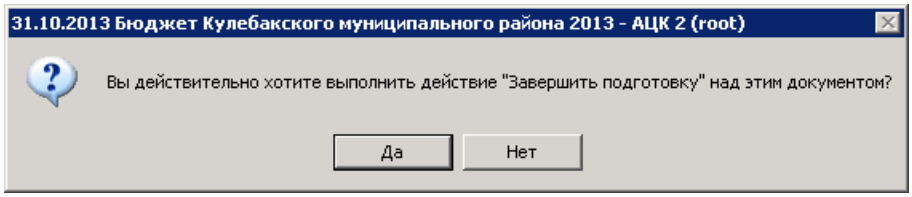

Рисунок 59 – Форма запроса на обработку документа

Для выполнения автоматической обработки документа и закрытия формы запроса нажимается кнопка **Да**. Для закрытия формы запроса без последующей обработки нажимается кнопка **Нет**.
Если автоматическая обработка документа при подписании не настроена, запрос на обработку не выводится.

Внимание! *Управление процессом подписания вложенных файлов осуществляется с помощью настроек* ***Подписывать вложения ЭД*** *и* ***Всегда использовать Усиленную ЭП (64Б)*** *(пункт меню* ***Сервис→****, закладка* ***Общие****).*
Функция подписания вложенных файлов электронных документов включается настройкой ***Подписывать вложения ЭД****.*
При включении настройки ***Всегда использовать Усиленную ЭП (64Б)*** *для подписания вложенных файлов электронных документов применяется вид подписи* ***Усиленная ЭП (64Б)****, независимо от установленного в сертификате вида подписи. Подпись вида* ***Усиленная ЭП (64Б)*** *накладывается на хэш-код дайджеста вложенного файла, что позволяет оперативно подписывать вложенные файлы больших размеров.*
Более подробное описание настройки системных параметров приведено в документации «».

Примечание. *Ограничения многократного подписания документов одной и той же ЭП-ролью на одном статусе и одним и тем же сертификатом на одном статусе настраиваются с помощью группы параметров* ***Контроль многократного подписания*** *(пункт меню* ***Сервис→****, закладка* ***Контроль ЭП****). В зависимости от выбранного режима выполнения контролей многократного подписания (Учитывать невалидные ЭП или Игнорировать невалидные ЭП), действие параметров распространяется на все ЭП ЭД или только на валидные ЭП ЭД.*

5.1.2 Подписание документа в форме документа

Для подписания документа в форме самого документа необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, который необходимо подписать, и нажатием кнопки **Редактировать** панели инструментов окна или клавиши **<F4>** вызвать форму его редактирования.
3. В форме редактирования документа, в меню действий, выбрать действие **Подписать**:

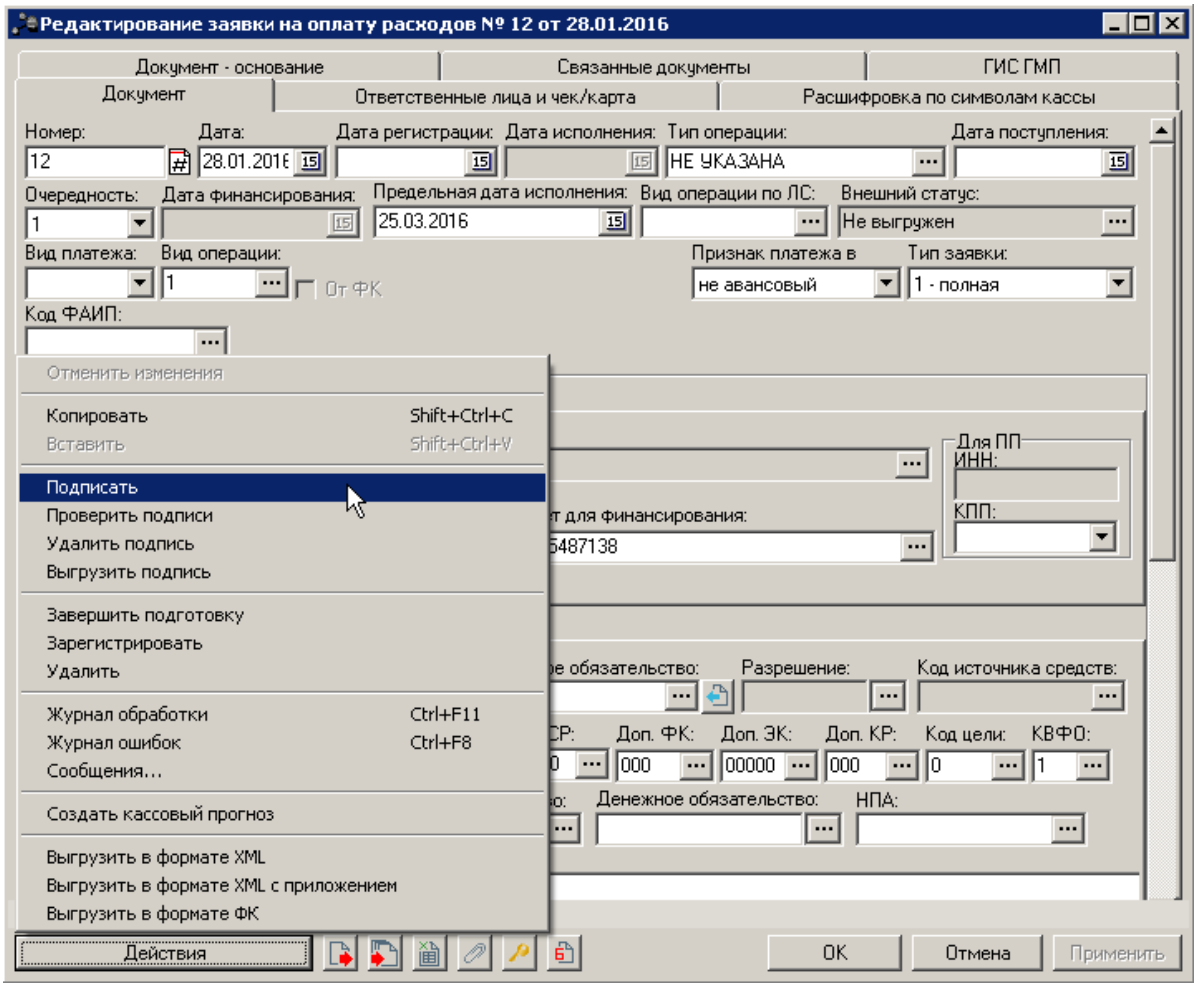

Рисунок 60 – Действие «Подписать» в меню действий формы документа

4. На экране появится окно Формирование электронной подписи (ЭП) (подробное описание окна формирования электронной подписи см. в разделе Подписание документа в списке документов 70).

5.1.3 Подписание нескольких документов

Для одновременного подписания нескольких документов необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить флажками документы, которые необходимо подписать.

Внимание! *Одновременно можно подписать несколько документов только одного класса, находящихся на одинаковом статусе. При попытке одновременного подписания документов, находящихся на разных статусах, будут подписаны только документы в статусе, соответствующем статусу первого выделенного в списке документа. Остальные документы подписаны не будут, но останутся выделенными и доступными для подписания.*
Выделение флажками подписываемых документов для удобства дальнейшей работы сохраняется независимо от результатов процедуры подписания.

3. Вызвать нажатием правой кнопки мыши контекстное меню произвольного выделенного документа и выбрать пункт **Подписать**:

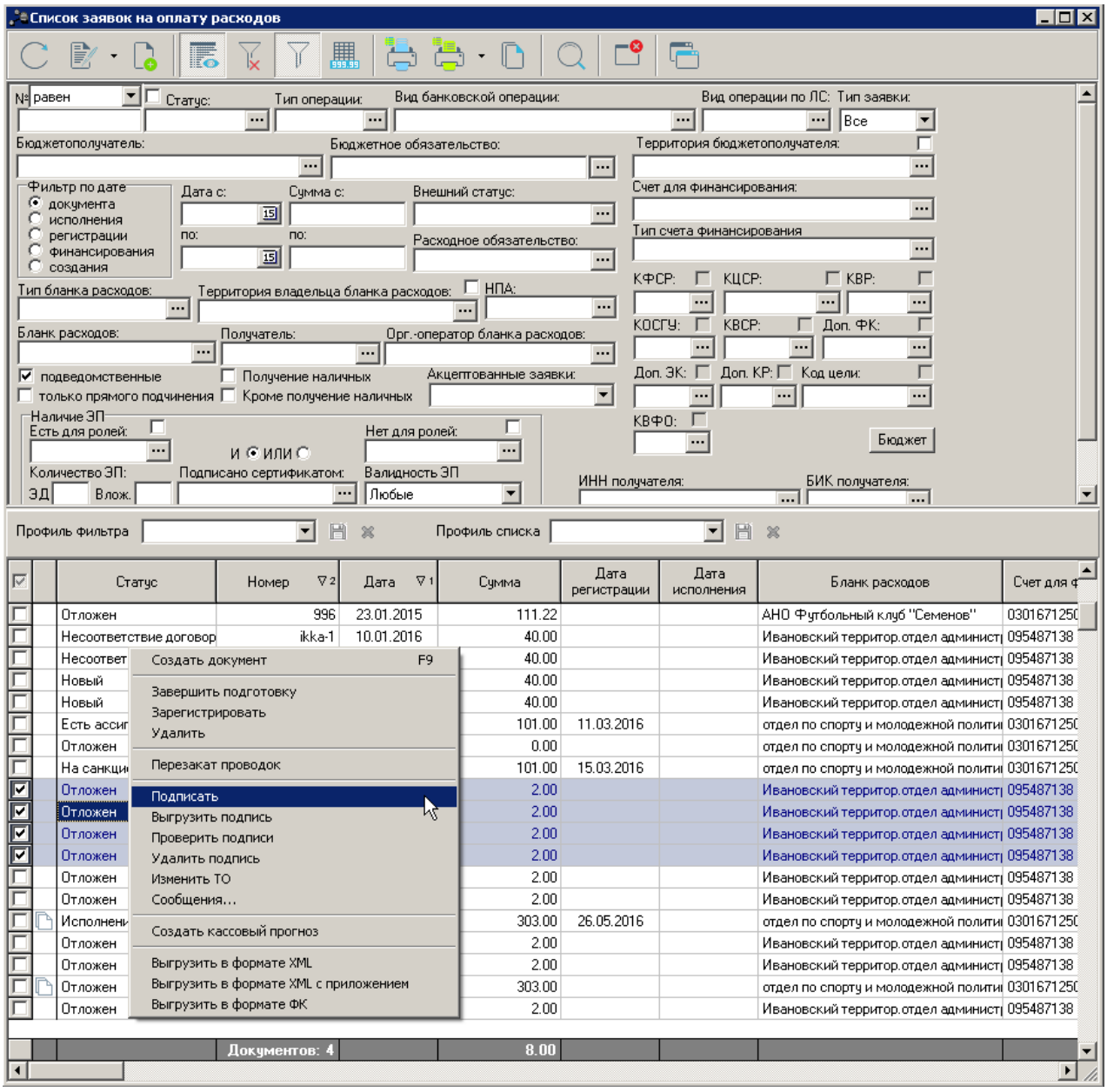

Рисунок 61 – Подписание нескольких документов в списке документов

4. Откроется окно формирования электронной подписи (подробное описание окна формирования электронной подписи см. в разделе Подписание документа в списке

документов[70]).

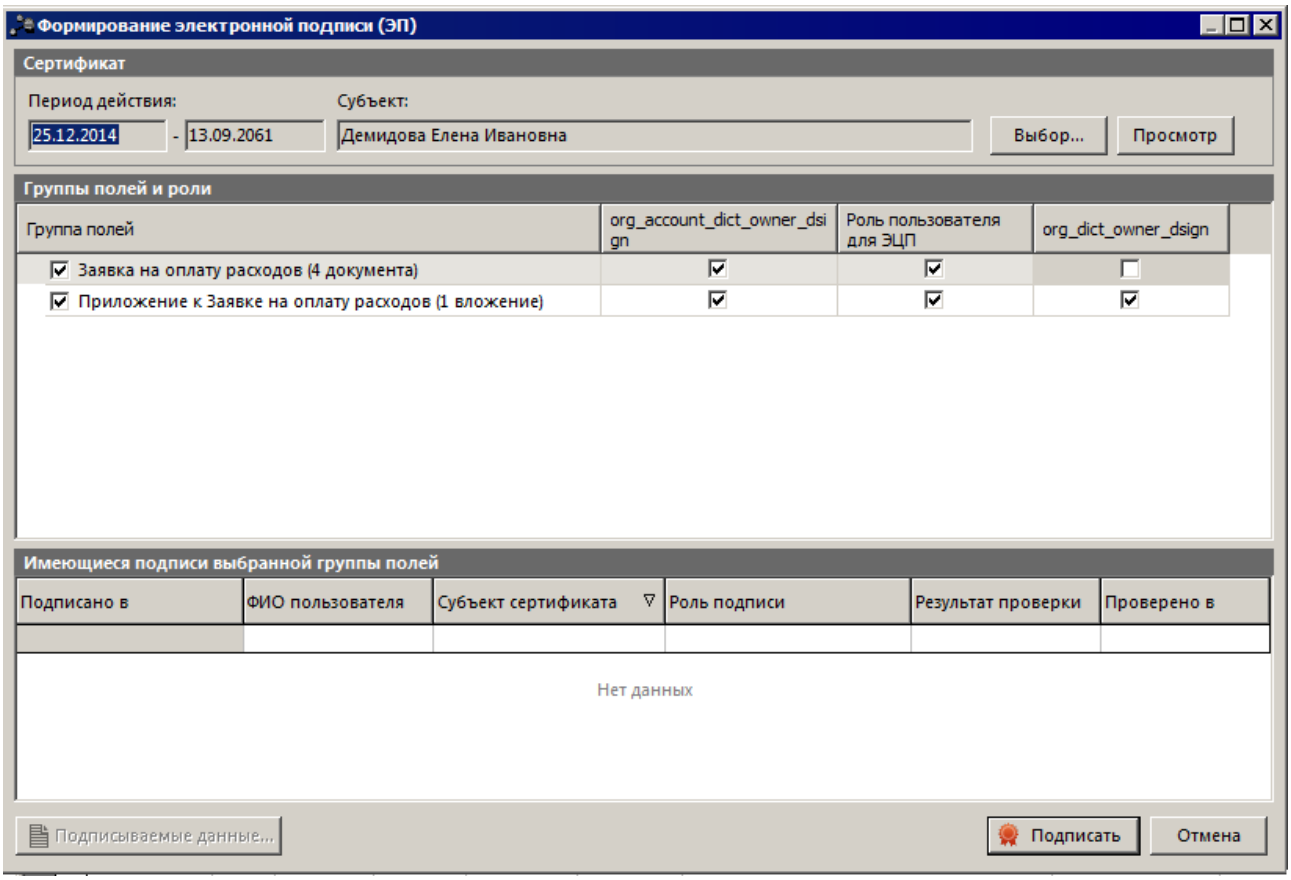

Рисунок 62 – Формирование подписи для нескольких документов

5. Для подписания документов нажать кнопку **Подписать** окна *Формирование электронной подписи*. Контроли, выполняемые при запуске процедуры подписания, описаны в разделе **Подписание документа в списке документов**[70].
6. По завершении формирования ЭП выдается сообщение с результатами процедуры подписания. Для закрытия формы сообщения с результатами процедуры подписания нажимается кнопка **Закрыть**:

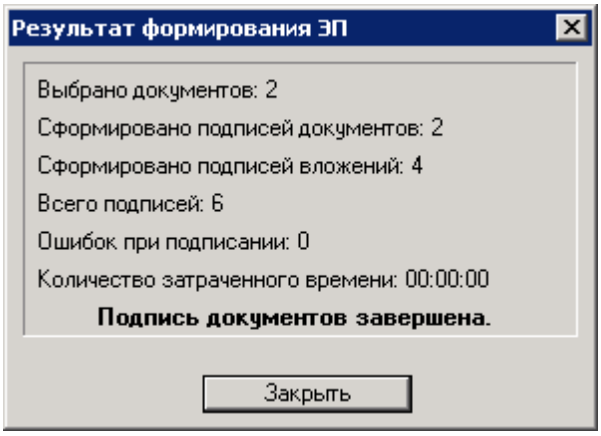

Рисунок 63 – Форма сообщения о результатах процедуры подписания

7. Если для ЭП-роли, которой произведено подписание документов, в соответствующем правиле подписания документа (справочник *Правила подписания документов на статусах*, пункт меню **Справочники→Система**) настроена автоматическая обработка при подписании, при закрытии формы сообщения с результатами подписания на экране появится запрос на обработку документов 76. Для выполнения автоматической обработки документов и закрытия формы запроса нажимается кнопка **Да**. Для закрытия формы запроса без последующей обработки нажимается кнопка **Нет**.

Если автоматическая обработка документа при подписании не настроена, запрос на обработку не выводится.

Подписание вложений электронных документов рассмотрено в разделе **Подписание документа в списке документов** 70.

5.2 Проверка подписи электронных документов

Количество ЭП, наложенных на электронный документ, отображается в поле **Количество ЭП** списка документов. Для фильтрации документов по данному признаку используется фильтр **Количество ЭП**.

Внимание! *Поле* ***Количество ЭП*** *отображает информацию о количестве всех подписей, наложенных на документ, вне зависимости от их валидности.*

Для проверки ЭП документа необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, у которого необходимо проверить ЭП, и нажатием кнопки **Редактировать** панели инструментов окна или клавиши **<F4>** вызвать форму его редактирования.
3. Чтобы просмотреть список подписей документа, необходимо нажать в форме данного документа кнопку  (**ЭП документа**):

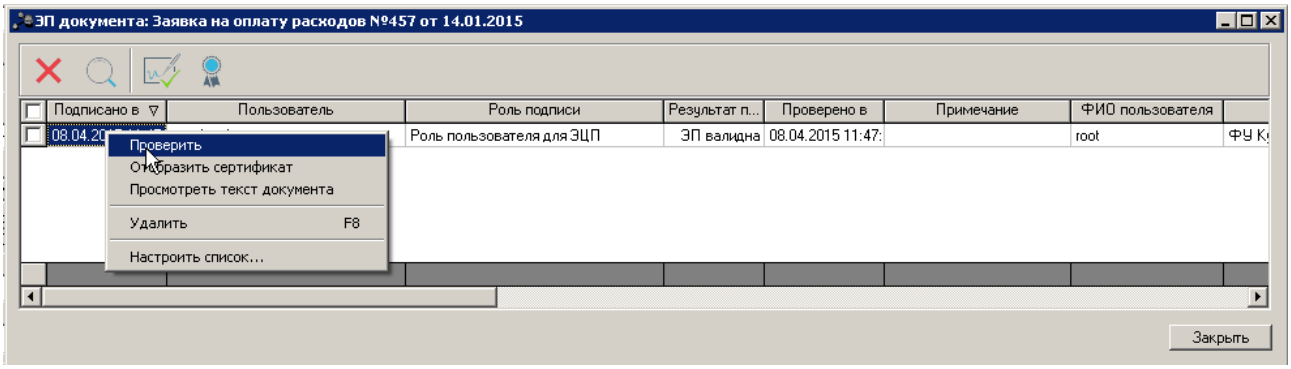

Рисунок 64 – Контекстное меню списка ЭП документа

В форме новой записи справочника содержатся поля:

- **Подписано в** – дата и время подписания документа.
- **Пользователь** – имя пользователя, подписавшего документ.
- **Роль подписи** – название ЭП-роли пользователя, с использованием которой был подписан документ.
- **Результат последней проверки** – состояние ЭП на момент последней проверки.
- **Проверено в** – дата и время проверки ЭП.
- **Примечание** – поле, предназначенное для информирования пользователя.
- **ФИО пользователя** – фамилия, имя, отчество пользователя, подписавшего документ.
- **Организация** – название организации, к которой принадлежит пользователь, подписавший документ.
- **Субъект сертификата** – название субъекта (организации, ответственного лица), которому выдан сертификат.
- **Уполномоченный представитель** – фамилия, имя, отчество уполномоченного представителя владельца сертификата (по умолчанию поле скрыто).
- **Примечание для пользователя** – краткий текстовый комментарий к ЭП.
- **Статус данных документа** – поле, указывающее на актуальность/неактуальность подписанных данных документа.
- **Вид ЭП** – вид электронной подписи. Для всех импортированных в БД сертификатов пользователей поле **Вид ЭП** заполняется значением *Усиленная*.
- **Подписанные данные** – значение поля зависит от типа подписанных данных. При наложении ЭП на электронный документ поле принимает значение ЭД. При наложении ЭП на вложение к электронному документу в поле указывается наименование подписанного файла вложения в следующем виде: <*наименование файла вложения.расширение*>.
- **Группа полей** – данные ЭП и электронного документа. Значение берется из поля **Заголовок** соответствующей записи справочника *Группы полей*.
- **Контроль последовательности** – наименование контроля последовательности.
- **Статус** – информация о базовом статусе, на котором находился ЭД в момент наложения ЭП.
- **Статус дополнительного сценария** – информация о статусе дополнительного сценария, на котором находился ЭД в момент наложения ЭП.

Для проверки ЭП документа в форме списка ЭП документа необходимо выделить одну или несколько ЭП, которые требуется проверить, и нажать на панели инструментов кнопку  (**Проверить**) или вызвать контекстное меню и выбрать пункт **Проверить**.

ЭП считается валидной при выполнении следующих условий:

- подтверждена подлинность ЭП (криптографическая проверка ЭП);

***Примечание**. При валидации ЭП вида «Усиленная (со штампом времени)» производится только криптографическая (математическая) проверка ЭП (включая штамп времени), прочих проверок не производится.*

- в значения записей справочников, которые подписаны в документе, не внесены изменения;
- сертификат ключа подписи, относящийся к проверяемой ЭП, не находится в списке отзыва;
- сертификаты цепочки доверия в наличии, действительны и не отозваны;
- списки отзыва для сертификата пользователя и для цепочки доверия в наличии и актуальны;

***Примечание**. Проверка актуальности списков отзыва осуществляется, если включен системный параметр **Проверять наличие актуального списка отзыва** (пункт меню **Сервис→**, закладка **Общие**).*

- сертификат ключа подписи, относящийся к этой ЭП, не утратил силу (действует) на момент проверки (для ЭП вида *Усиленная 64Б*) или на момент подписания электронного документа (для ЭП вида *Усиленная с доказательствами подлинности*);

***Внимание!** Если включен системный параметр **Не учитывать срок действия сертификата при проверке Усиленной (64Б)** (пункт меню **Сервис→**, закладка **Общие**), при проверке ЭП вида «Усиленная» не учитывается срок действия сертификата, с помощью которого сформирована проверяемая ЭП. То есть ЭП вида «Усиленная 64Б с сертификатом», у которого истек срок действия на момент проверки, признается валидной при единовременном соблюдении прочих перечисленных выше условий.*

1. Если ЭП валидна, на экране появится сообщение о том, что она верна:

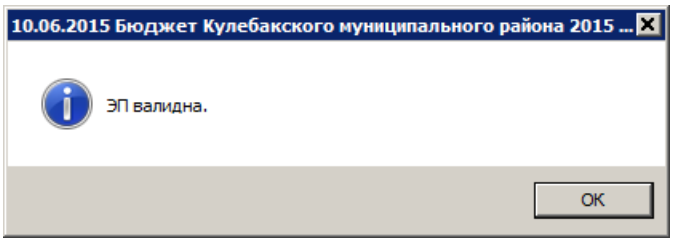

Рисунок 65 – Сообщение о валидности ЭП

После этого ЭП принимает статус «ЭП валидна».

2. Если ЭП невалидна, на экране появится соответствующее сообщение. В сообщении содержится заключение о невалидноси ЭП, диагностическая информация о криптографическом статусе ЭП и результатах проверки актуальности сертификата.

Например, если криптографическая проверка пройдена, но относящийся к ЭП сертификат утратил актуальность вследствие отзыва, выводится сообщение следующего вида:

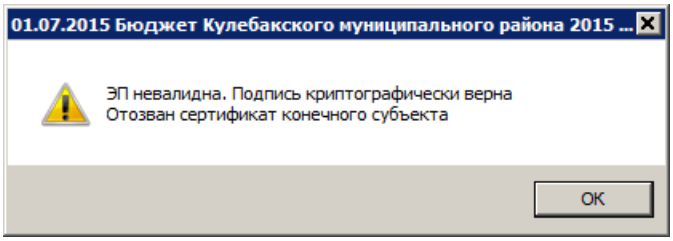

Рисунок 66 – Сообщение о невалидности ЭП: истек срок действи сертификата

Если криптографическая проверка не пройдена, выводится сообщение следующего вида:

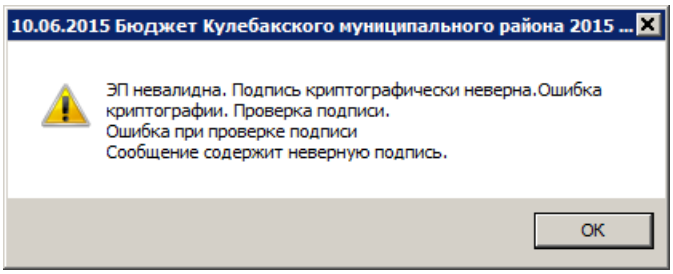

Рисунок 67 – Сообщение о невалидности ЭП: не пройдена криптографическая проверка

После этого ЭП принимает статус *«ЭП невалидна»*.

Диагностическая информация о результатах проверки автоматически указывается в поле **Примечание** формы списка ЭП документа.

Если документ, имеющий валидные ЭП, был изменен, при его сохранении на экране появится предупреждающее сообщение:

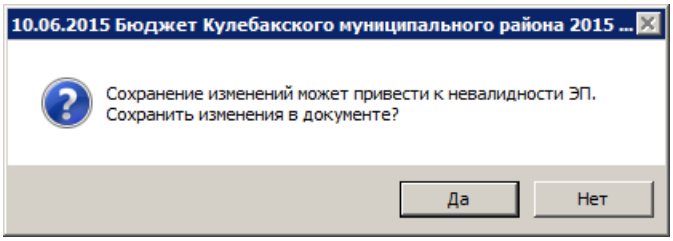

Рисунок 68 – Сообщение о возможной невалидности ЭП вследствие сохранения изменений в документе

При подтверждении сохранения в документе осуществляется проверка ЭП на предмет валидности. При отрицательном ответе документ возвращается в режим редактирования без сохранения.

Примечание. *Проверка валидности ЭП при сохранении изменений в документе производится при включенном системном параметре* ***Проверять ЭП при сохранении документа*** *(пункт меню* ***Сервис→****, закладка* ***Контроль ЭП****). Результат проверки отражается в полях* ***Результат последней проверки****,* ***Проверено в****,* ***Статус данных документа****,* ***Примечание*** *(в случае наличия диагностической информации) списка «ЭП документа».*
Если пользователю назначена специальная возможность «Позволять не контролировать , проверка валидности ЭП при сохранении измененного документа и при переходе документа по статусам не производится.

5.3 Просмотр состава подписанных данных

Для просмотра состава подписанных данных необходимо выполнить следующие действия:

1. В форме электронного документа открыть список наложенных на него подписей, нажав кнопку (**ЭП документа**).
2. Выделить необходимую ЭП и вызвать контекстное меню, щелкнув по ней правой кнопкой мыши.
3. В контекстном меню выбрать пункт **Просмотреть текст документа**.
4. Открывшееся окно просмотра текста документа состоит из следующих областей:

- **Деревья дайджестов и ЭП документа** – отображают хронологически упорядоченную совокупность дайджестов ЭД и ЭП, которыми эти дайджесты были подписаны.
- **Области с подписываемыми данными документа** – отображают содержимое выделенных дайджестов ЭД с цветовым выделением имеющихся различий между ними.

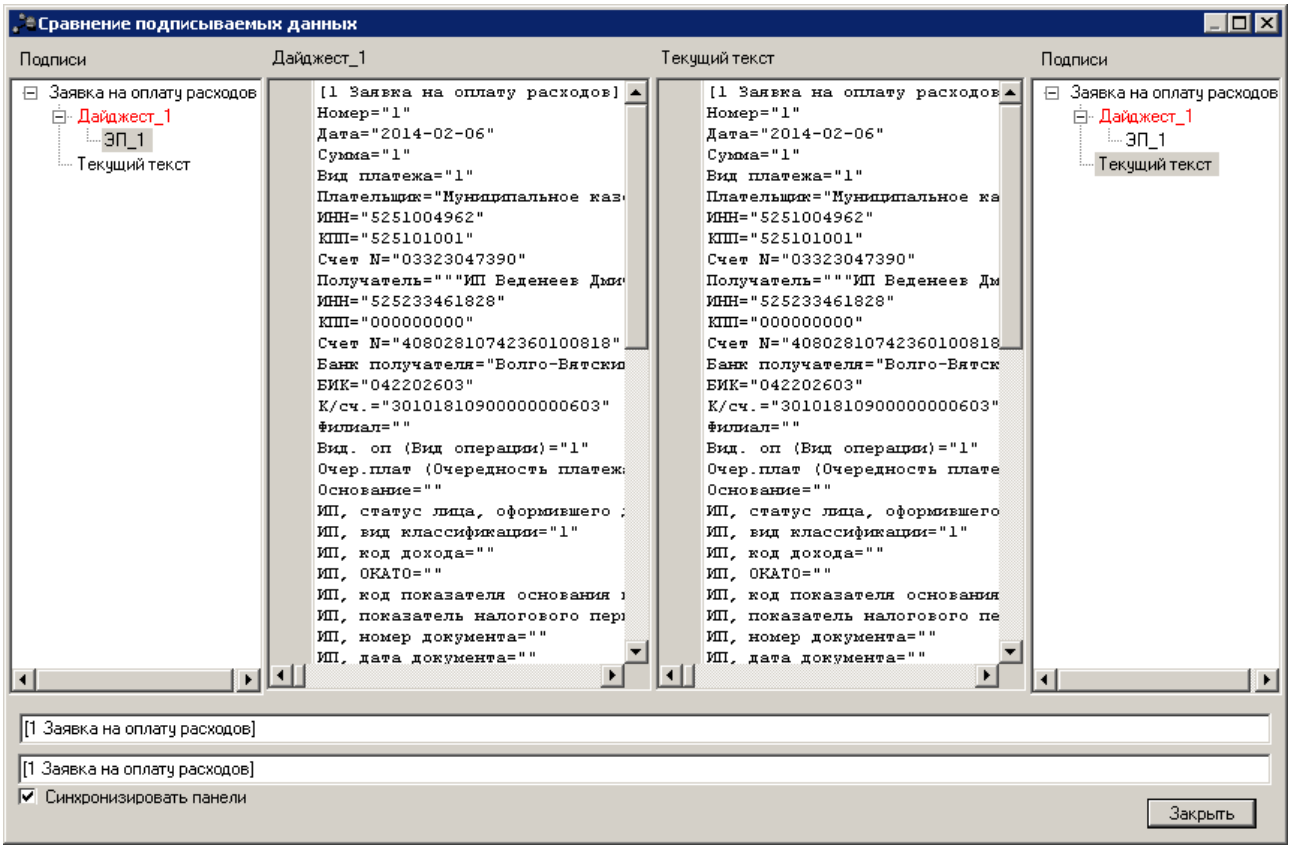

Рисунок 69 – Окно просмотра текста документа

***Примечание**. В дереве дайджестов и ЭП документа актуальный (последний подписанный) дайджест выделяется красным цветом, а текст документа, соответствующий текущему состоянию, отображается как **Текущий текст**.*

5. После просмотра состава подписанных данных закрыть окно *Сравнение подписываемых данных* нажатием кнопки **Закрыть**.

В случае если документ имеет подписанные вложения, они также отображаются в

форме *Сравнение подписываемых данных*. В ней доступна информация о наименованиях вложений документа, группах полей, к которым они привязаны, а также о количестве сформированных ЭП

5.4 Печать состава подписанных данных

Печать состава подписанных данных документа осуществляется нажатием кнопки (**Печать**) в форме документа при включенном отчетном параметре **Выводить дайджесты на печать** (). Информация о дайджестах отображается на отдельных листах, следующих за листом с печатной формой документа. Ниже информации о дайджесте располагается информация об ЭП.

Примечание. *Настройка печати ЭП рассмотрена в разделе* ***Настройка вывода на печать реквизитов ЭП и сертификатов****.*

Примечание. *Подробное описание настройки отчетных параметров см. в документации «БАРМ.00003-39 32 01-5 <%32_01-5%>».*

5.5 Просмотр сертификата ЭП документа

Для просмотра сертификата ЭП документа необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов открыть документ, подписанный ЭП.
3. В форме редактирования документа нажать кнопку (**ЭП документа**), откроется список наложенных на документ электронных подписей:

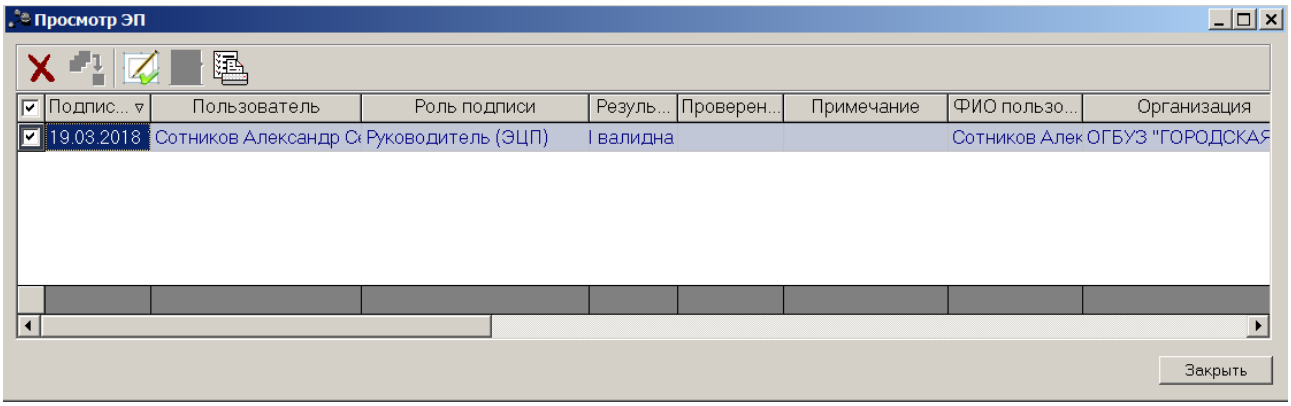

Рисунок 70 – Форма просмотра ЭП документа

4. В списке необходимо выделить ЭП, сертификат которой требуется просмотреть, и нажать кнопку (**Отобразить сертификат**). Кнопка просмотра сертификата

недоступна, если в списке выбрано более одной ЭП. При нажатии кнопки открывается сертификат, с использованием которого была сформирована ЭП:

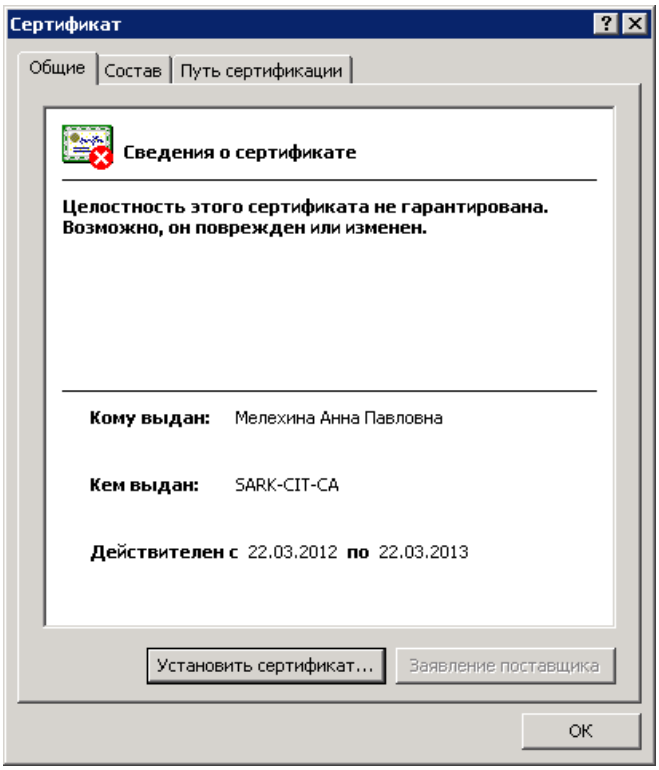

Рисунок 71 – Просмотр сертификата ЭП

5. Для печати списка наложенных на документ ЭП нажимается кнопка  (**Печать универсального списка выделенных документов**). В отчетную выводятся видимые колонки списка ЭП:

Финансовое управление администрации Володарского района
(наименование органа, исполняющего бюджет)

ЭП документа: Заявка на оплату расходов №10007 от 13.01.2017

Дата печати: 25.01.2018

Подписано в	Пользователь	Роль подписи	Результат последней проверки	Проверено в	Примечание	ФИО пользователя	Организация	Субъект сертификата	Примечание для пользователя	Статус данных документа	Вид ЭП	Подписанные данные	Группа полей	Контроль последовательности	Статус	Статус дополнительного сценария
18.09.2017 15:17:53	Администратор 1 (root)	Роль пользовате	1			Администратор 1	Володарское райфинуправлени	Balashov_9		1	1	ЭД	Заявка на оплату	0	Отложен	

Рисунок 72 – Универсальный список выделенных документов

5.6 Просмотр ЭП вложения в списке вложенных документов

Для просмотра ЭП вложения в списке вложенных документов необходимо открыть список вложенных документов текущего ЭД с помощью кнопки  (**Файлы**). В открывшейся форме *Присоединенные документы* в списке вложенных документов необходимо выделить нужное вложение и нажать на панели инструментов кнопку  . В результате в нижней части формы отобразится список ЭП выбранного вложения (по умолчанию при открытии

формы Присоединенные документы список ЭП вложения не отображается):

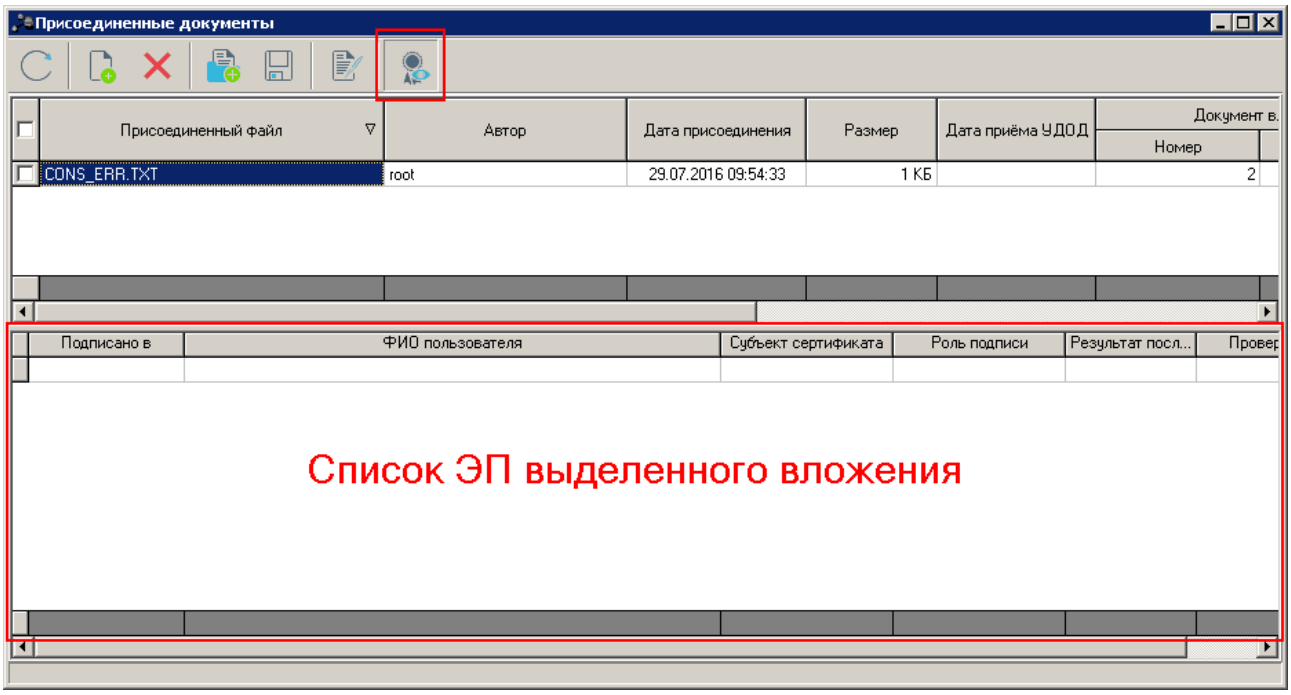

Рисунок 73 – Просмотр ЭП вложения в форме «Присоединенные документы»

В форме новой записи справочника содержатся поля:

- **Подписано в** – дата и время подписания вложенного документа.
- **ФИО пользователя** – ФИО пользователя, подписавшего вложенный документ.
- **Субъект сертификата** – название субъекта (организации, ответственного лица), которому выдан сертификат.
- **Роль пользователя** – название ЭП-роли пользователя, с использованием которой был подписан вложенный документ.
- **Результат проверки** – валидность ЭП вложенного документа на момент последней проверки.
- **Проверено в** – дата и время проверки ЭП вложенного документа .

Поля списка ЭП вложения заполняются автоматически из одноименных полей формы списка ЭП текущего ЭД 81. Список ЭП вложений доступен только для просмотра.

Если выбранное вложение не имеет ЭП, список ЭП для данного вложения не содержит записей.

5.7 Выгрузка документов с ЭП в электронный архив

5.7.1 Выгрузка документа из списка документов

Для выгрузки документа в электронный архив из списка документов необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, который необходимо выгрузить.

3. Нажатием правой кнопки мыши вызвать контекстное меню для этого документа и выбрать пункт **Выгрузить подпись**:

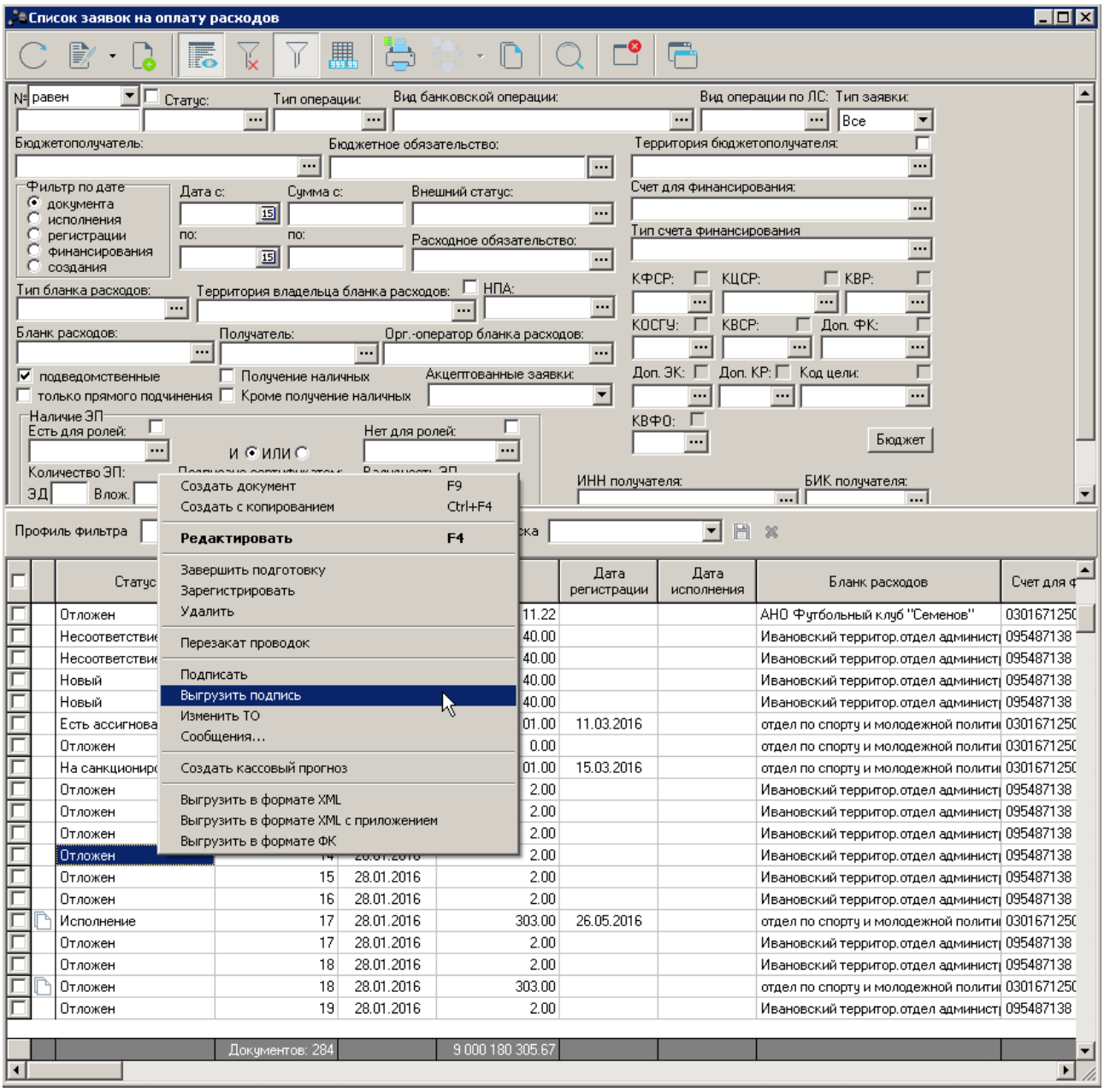

Рисунок 74 – Действие «Выгрузить подпись» в контекстном меню списка документов

В случае если в настройках системы установлен параметр **Указывать директорию вручную**, для осуществления выгрузки документа необходимо указать полный путь к электронному архиву:

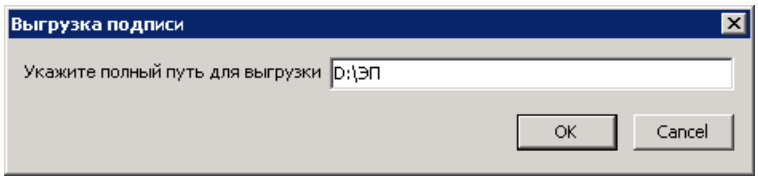

Рисунок 75 – Окно выбора полного пути для выгрузки подписи

По результатам выгрузки выдается соответствующее подтверждение:

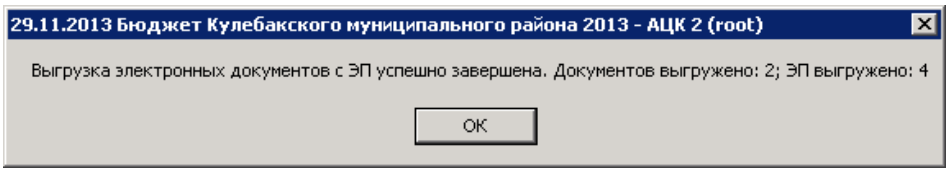

Рисунок 76 – Окно подтверждения выгрузки ЭД с ЭП

Внимание! *Выгрузка невалидных ЭП доступна, если установлен системный параметр* ***Позволять выгружать невалидные ЭП ЭД*** *(**Сервис→**, группа параметров , закладка* ***Общие****). При выгрузке невалидных ЭП на экране появляется предупреждающее сообщение:*

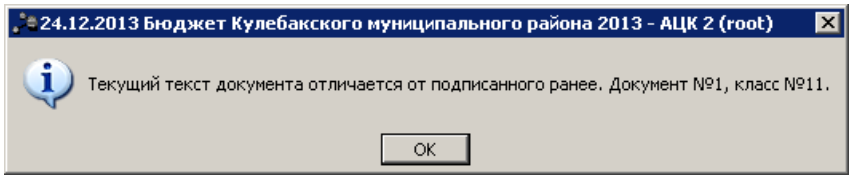

Рисунок 77 – Предупреждающее сообщение о невалидности выгружаемой ЭП

Для выполнения процедуры выгрузки ЭП требуется нажать кнопку ***ОК*** *в форме сообщения.*
Если системный параметр ***Позволять выгружать невалидные ЭП ЭД*** *не установлен, выгрузка невалидных ЭП недоступна.*

5.7.2 Выгрузка документа из формы документа

Для выгрузки документа в электронный архив из формы самого документа необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, который необходимо выгрузить, и нажатием кнопки **Редактировать** панели инструментов окна или клавиши <**F4**> вызвать форму его редактирования.
3. В форме редактирования документа, в меню действий, выбрать действие **Выгрузить подпись**:

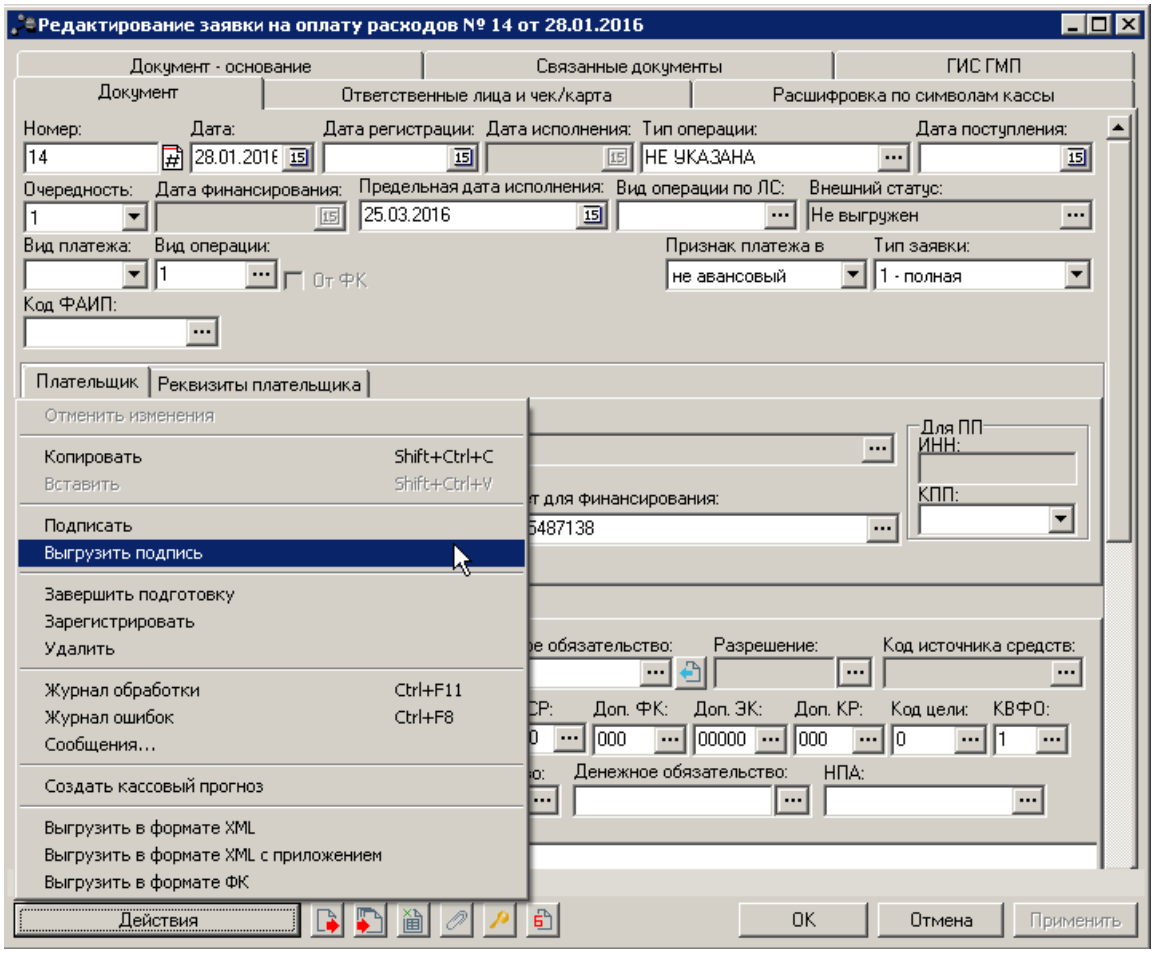

Рисунок 78 – Действие «Выгрузить подпись» в меню действий формы документа

Если в настройках системы установлен параметр **Указывать директорию вручную**, для осуществления выгрузки документа необходимо указать полный путь к электронному архиву[89].

По результатам выгрузки выдается соответствующее подтверждение[90].

5.7.3 Выгрузка нескольких документов

Для одновременной выгрузки нескольких документов в электронный архив необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить галочками документы, которые необходимо выгрузить.
3. Вызвать нажатием правой кнопки мыши контекстное меню произвольного выделенного документа и выбрать пункт **Выгрузить подпись**:

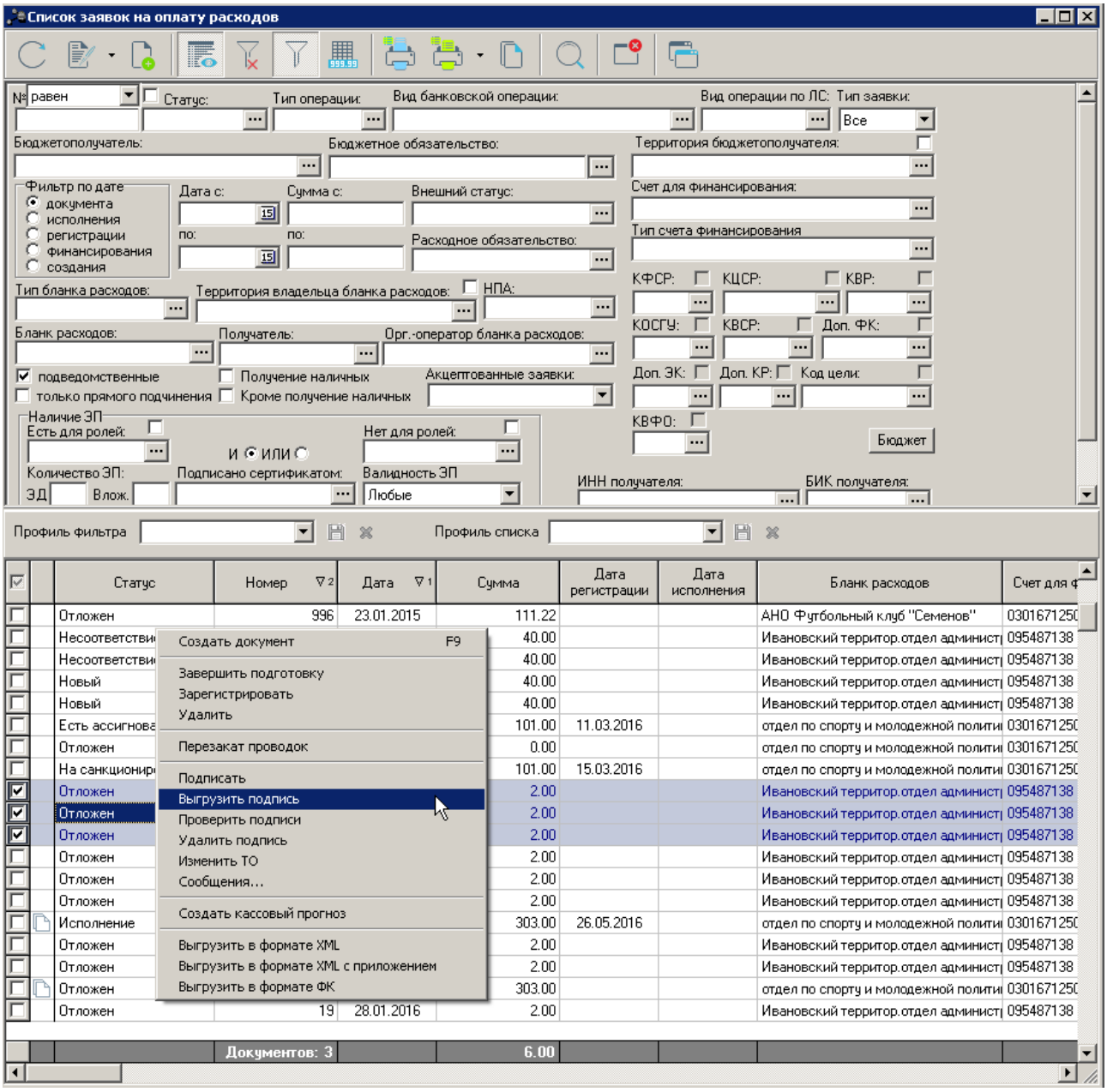

Рисунок 79 – Выгрузка подписей нескольких документов в списке документов

В случае если в настройках системы установлен параметр **Указывать директорию вручную**, для осуществления выгрузки документа необходимо указать полный путь к электронному архиву 89.

По результатам выгрузки выдается соответствующее подтверждение 90.

5.7.4 Автоматическая выгрузка документов с ЭП

Автоматическая выгрузка документов с ЭП осуществляется с помощью задания планировщика *SchExpDocs*, настройка которого доступна с помощью пункта меню →**Планировщик**→**Расписание**, через создание нового задания **SchExpDocs**:

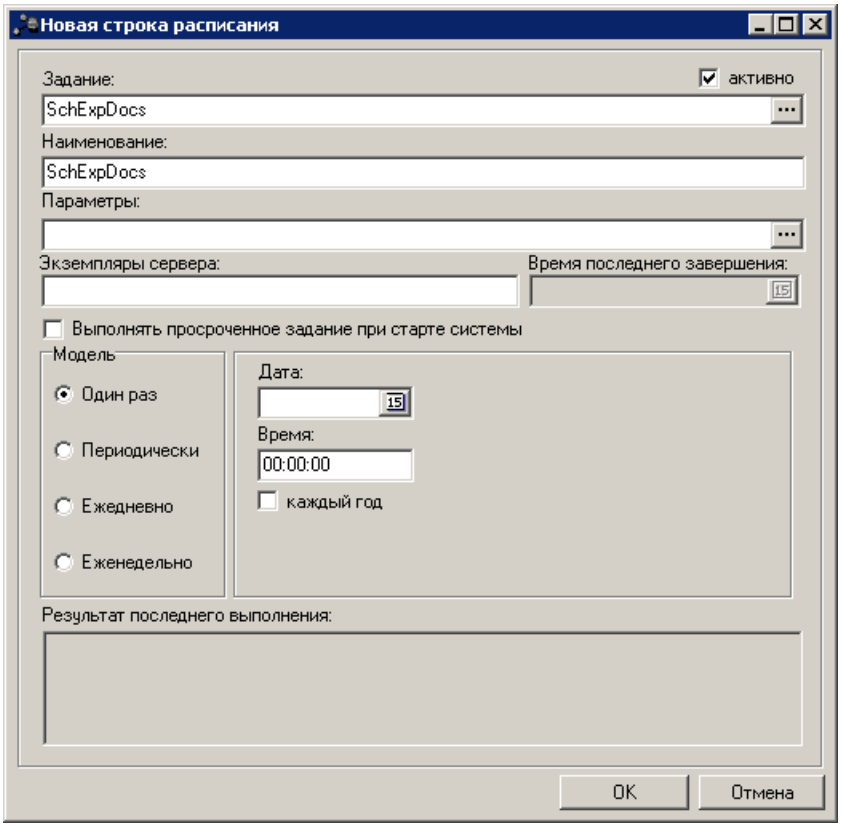

Рисунок 80 – Редактирование строки расписания SchExpDocs

Задание на выгрузку ЭД с ЭП **SchExpDocs** имеет следующие параметры:

- **export_code (необязательный)** – код варианта выгрузки из справочника *Документы с ЭП, выгружаемые по расписанию*. Если параметр не указан, выгружаются все документы из справочника *Документы с ЭП*, выгружаемые *по расписанию*;
- **-except_exported (необязательный)** – не выгружать уже выгруженные документы (проверка производится по журналу выгрузки). Если параметр не указан, выгружаются все документы, определенные параметром **export_code**, в том числе выгружаемые ранее;
- **-except_exported; max_documents (необязательный)** – параметр определяет максимальное количество документов, которое может быть выгружено за один запуск задания; уже выгруженные документы не выгружаются (проверка производится по журналу выгрузки). Если параметр не указан, выгружаются все документы, определенные параметром **export_code**, в том числе выгружаемые ранее.

Шаблон настройки параметров задания можно просмотреть/выбрать в окне *Параметры задания*:

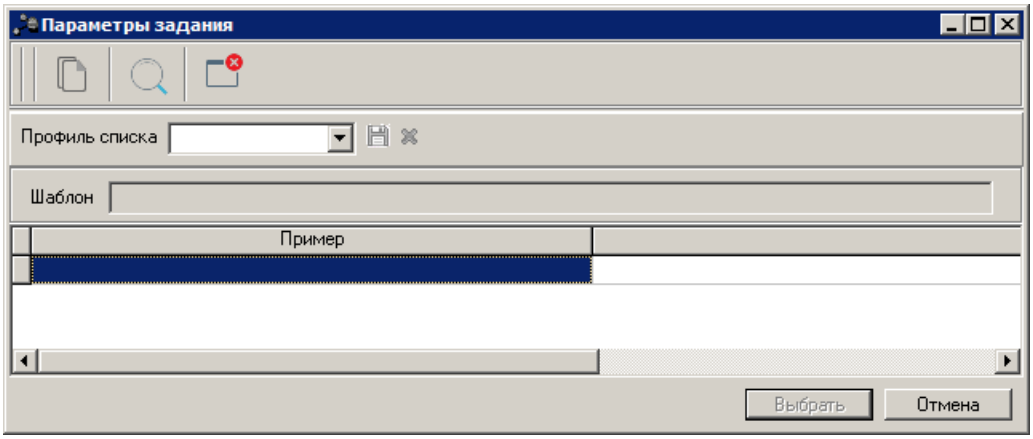

Рисунок 81 – Форма параметров задания

Варианты выгрузки (параметр **export_code**) создаются и настраиваются в справочнике *Документы с ЭП*, выгружаемые по расписанию, доступном с помощью пункта меню **Справочники→Система→Документы с ЭП, выгружаемые по расписанию**:

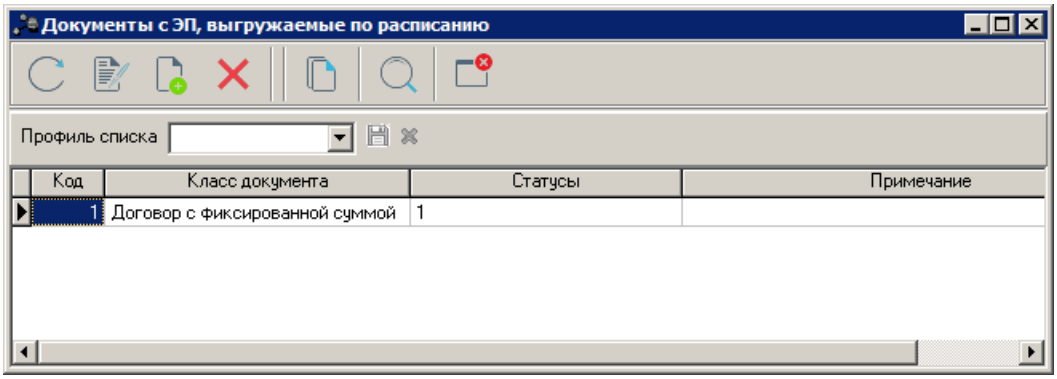

Рисунок 82 – Справочник «Документы с ЭП, выгружаемые по расписанию»

Вариант выгрузки документов с ЭП представляет собой информацию о том, документы какого класса, подписанные какими ЭП-ролями и на каких статусах, будут выгружаться. При создании/редактировании варианта выгрузки документов с ЭП возможно указание перечисленных параметров:

- **Код** – код варианта выгрузки. Обязательное для заполнения.
- **Класс документа** – класс выгружаемых документов. Обязательное для заполнения.
- **Статусы** – документы, подписанные на каких статусах, будут выгружены. Обязательное для заполнения.
- **Роли** – документы, подписанные какими ролями, будут выгружены. Обязательное для заполнения.
- **Примечание** – описание варианта выгрузки. Необязательное для заполнения.

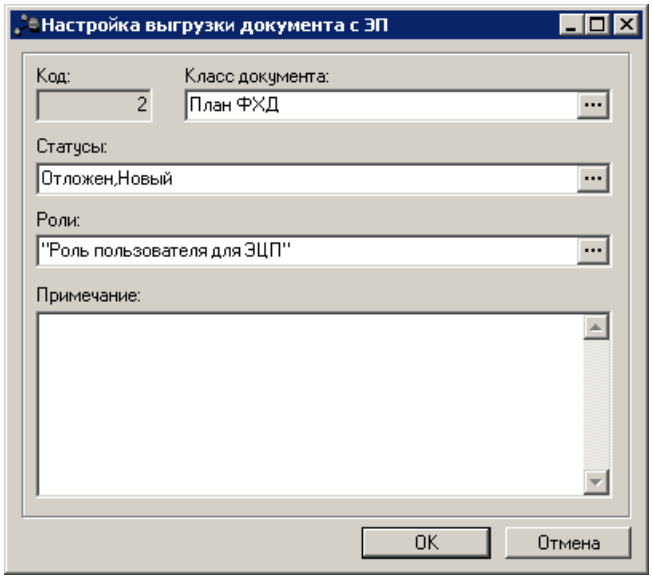

Рисунок 83 – Настройка выгрузки документов

Выгрузка документов с ЭП осуществляется в директорию, указанную в системном параметре **Директория для выгрузки ЭД с ЭП (Сервис→**, группа настроек , закладка **Общие**).

Примечание. Более подробную информацию по работе с Планировщиком см. в документации «».

5.7.5 Именование файлов в электронном архиве

Электронный документ, подписанный ЭП, выгружается в каталог, указываемый вручную в момент выгрузки либо преднастроенный в системном параметре **Директория для выгрузки ЭД с ЭП (Сервис→**, группа настроек , закладка **Общие**), в виде:

- текстового файла с подписанными данными документа (актуальным дайджестом);
- файлов с ЭП по количеству подписей, относящихся к актуальному дайджесту.

При этом для формирования имен файлов используются следующие маски:

- Маска, используемая для формирования имен файлов с дайджестами выгружаемых документов:

<№_кл>_<ид_док>_<имя_гп>.txt,

где:

- **<№_кл>** – номер класса документа;
- **<ид_док>** – идентификатор документа;
- **<имя_гп>** – имя группы полей.

- Маска, используемая для формирования имен файлов с ЭП, которыми подписаны выгружаемые документы:

<№_кл>_<ид_док>_<имя_гп>_<№пп_ЭП>.txt.sig,

где:

- **<№_кл>** – номер класса документа;
- **<ид_док>** – идентификатор документа;
- **<имя_гп>** – имя группы полей;
- **<№пп_ЭП>** – порядковый номер ЭП.

Вложение электронного документа, подписанное ЭП, выгружается в каталог, указываемый вручную в момент выгрузки либо преднастроенный в системном параметре **Директория для выгрузки ЭД с ЭП** (**Сервис→**, группа настроек , закладка **Общие**), в виде:

- файла вложения;
- файлов с ЭП по количеству относящихся к вложению подписей.

При этом для формирования имен файлов используются следующие маски:

- Маска, используемая для формирования имен выгружаемых подписанных вложений:

<№_кл>_<ид_док>_<имя_гп>_<имя_атт>.<расш_атт>,

где:

- **<№_кл>** – номер класса документа;
- **<ид_док>** – идентификатор документа;
- **<имя_гп>** – имя группы полей;
- **<имя_атт>** – имя прикрепленного файла;
- **<расш_атт>** – расширение прикрепленного файла.

- Маска, используемая для формирования имен файлов с ЭП, которыми подписаны выгружаемые вложения:

<№_кл>_<ид_док>_<имя_гп>_<имя_атт>_<№пп_ЭП>.<расш_атт>.sig,

где:

- **<№_кл>** – номер класса документа;
- **<ид_док>** – идентификатор документа;
- **<имя_гп>** – имя группы полей;
- **<имя_атт>** – имя прикрепленного файла;
- **<№пп_ЭП>** – порядковый номер ЭП;
- **<расш_атт>** – расширение прикрепленного файла.

Если включен системный параметр **Выгружать ЭД с ЭП по подкаталогам (при выгрузке на сервере)** (**Сервис→**, группа настроек , закладка **Общие**), выгрузка документов и вложений с ЭП осуществляется в автоматически создаваемые для каждого класса документов каталоги, имеющие корневой директорией ту, которая указана в настройке **Директория для выгрузки ЭД с ЭП** системных параметров. При этом имена каталогов формируются в соответствии со следующей маской:

<№_кл>_<имя_кл>,

где:

- **<№_кл>** – номер класса документа;
- **<имя_кл>** – физическое имя класса документа.

Внимание! *При совпадении имен файлов выгружаемых ЭД, вложений и подписей с именами файлов, уже хранящихся в каталоге выгрузки, происходит перезапись старых файлов на новые.*

5.7.6 Выгрузка вложений с ЭП

В системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» вместе с документами по умолчанию выгружаются подписанные вложения.

Выгрузка подписанных вложений документов настраивается с помощью системного параметра **Выгружать вложения при выгрузке ЭД**. Данный параметр по умолчанию включен и доступен в пункте меню **Сервис→**, группа настроек , закладка **Общие**.

Для настройки выгрузки документов без вложений необходимо отключить параметр **Выгружать вложения при выгрузке ЭД**.

5.8 Удаление документов с ЭП

При переводе документов в статус *«удален»* осуществляются следующие неигнорируемые контроли:

- Контроль наличия ЭП для документов и их вложений. Если документ или его вложения имеют хотя бы одну ЭП, выдается сообщение об ошибке;
- Контроль наличия ЭП для вложений документа. Если вложения документа имеют хотя бы одну ЭП, выдается сообщение об ошибке.

Примечание. *Для перевода документа в статус «удален» или удаления вложений документа предварительно необходимо осуществить* *удаление всех имеющихся ЭП* 98
.

Примечание. *Игнорировать контроль наличия ЭП для документов может только пользователь, для которого настроена специальная возможность* ***Позволять удалять подписанные документы*** *(пункт меню* ***Справочники→Система→Роли пользователей****). Игнорировать контроль наличия ЭП для вложений документов может только пользователь, для которого настроена специальная возможность* ***Позволять удалять подписанные вложения в документах*** *(пункт меню* ***Справочники→Система→Роли пользователей****).*

5.8.1 Удаление ЭП документа

Внимание! *Функция удаления ЭП доступна, если включена системная настройка* ***Позволять удалять ЭП*** *(**Сервис→**, группа настроек , закладка* ***Общие****). При отключенной настройке кнопка* ***(Удалить)*** *на панели инструментов и соответствующий пункт контекстного меню недоступны пользователям.*

Для удаления ЭП документа необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов открыть документ, у которого необходимо удалить подпись.
3. В форме редактирования документа нажать кнопку (**ЭП документа**), откроется список электронных подписей.
4. Вызвать нажатием правой кнопки мыши контекстное меню нужной подписи документа и выбрать пункт **Удалить**, либо нажать кнопку на панели инструментов:

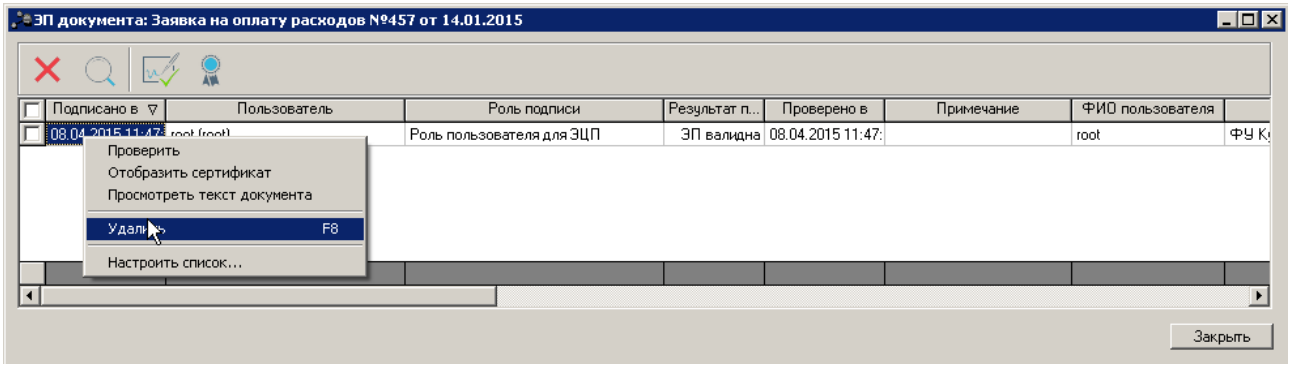

Рисунок 84 – Удаление ЭП

На экране появится окно подтверждения удаления:

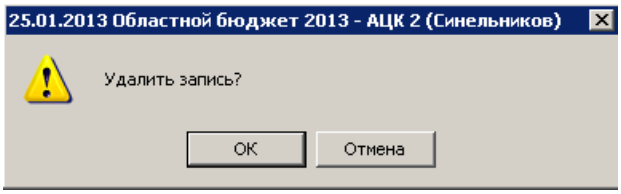

Рисунок 85 – Форма подтверждения удаления ЭП

Для удаления ЭП нажимается кнопка **Да**. Если ЭП невозможно удалить, выдается сообщение об ошибке.

Внимание! *ЭП невозможно удалить при следующих условиях:*
- если пользователь, производящий удаление подписи, не является пользователем, сформировавшим удаляемую подпись;
- если статус, в котором производится удаление подписи, не совпадает со статусом, в котором она была сформирована;
- если удаляемая подпись имеет дату/время формирования более позднюю, чем дата/время остальных подписей, наложенных на ту же группу полей;
- если под группой полей, подписанной удаляемой подписью, имеются подписи с более поздними датой/временем формирования и они сформированы на статусе, отличном от статуса формирования удаляемой подписи;
- если под группой полей, подписанной удаляемой подписью, имеются подписи с более поздними датой/временем формирования, они сформированы на статусе, соответствующем статусу формирования удаляемой подписи и в удаляемой подписи включен параметр «Контроль последовательности подписания».

5.8.2 Удаление ЭП документа в списке документов

Для удаления ЭП документа в списке документов необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, в котором необходимо удалить подпись.
3. Нажатием правой кнопки мыши вызвать контекстное меню для этого документа и выбрать пункт **Удалить подпись**.

Внимание! *Действие доступно если включен параметр* ***Позволять удалять ЭП (Сервис→Системные параметры*** *раздел* ***ЭП*** *закладка* ***Общие****).*

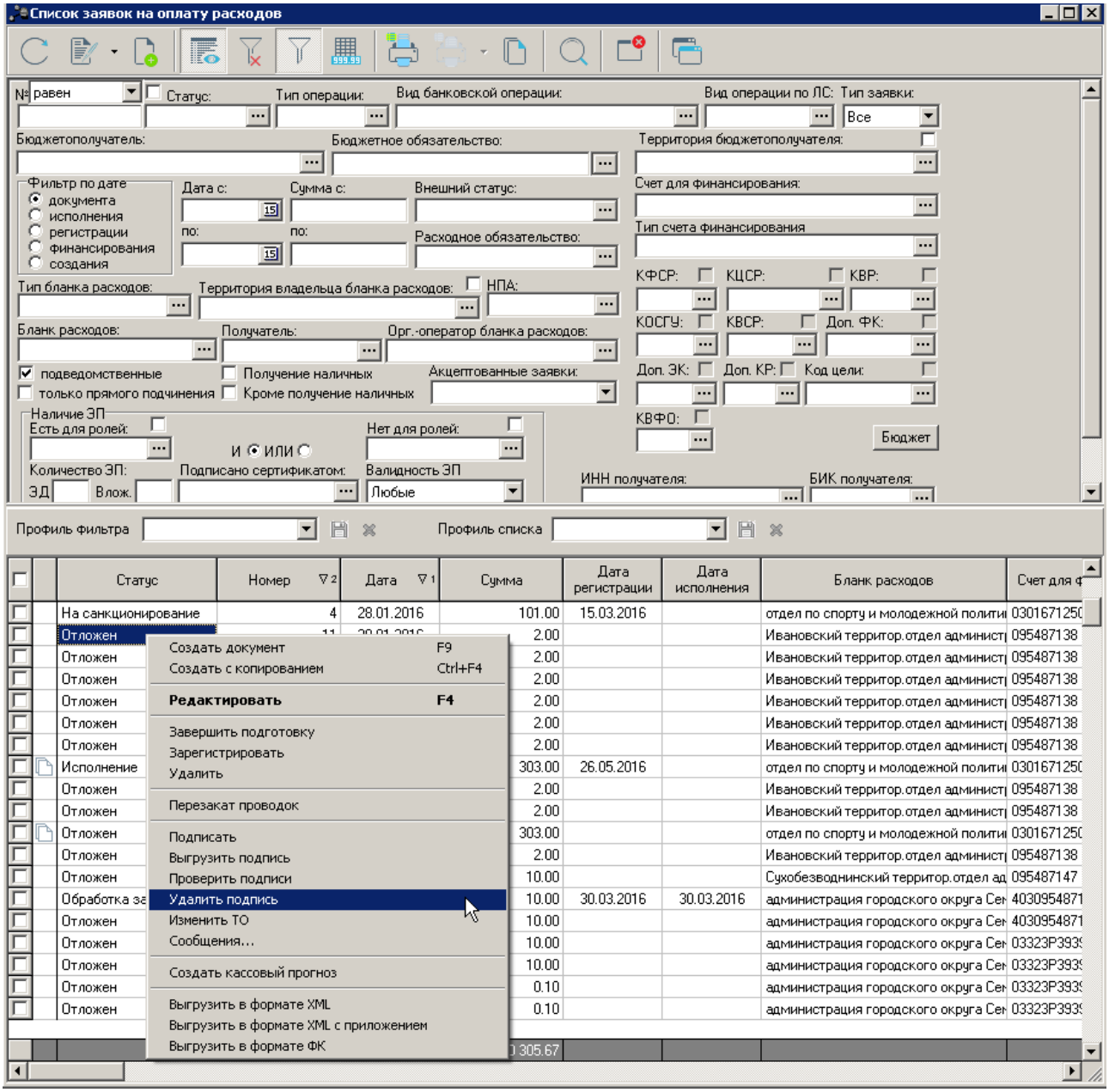

Рисунок 86 – Действие «Удалить подпись» в контекстном меню списка документов

На экране появится окно подтверждения удаления подписей документа. Если удаление необходимо - нажимается кнопка **ОК**, иначе – **Отмена**.

При выполнении удаления для каждой ЭП каждого документа выполняются контроли, определяющие возможность удаления этой ЭП:

- Проверка совпадения пользователя, производящего удаление ЭП и пользователя, наложившего ЭП. Если пользователи не совпадают, удаление ЭП не доступно.
- Сочетание базового статуса и допстатуса при наложении ЭП должно совпадать с текущим состоянием ЭД. Если при наложении ЭП допстатус не использовался или не известен, текущий допстатус ЭД при выполнении проверки не учитывается.
- Удаляемая ЭП должна иметь дату/время формирования более поздние, чем

дата/время остальных ЭП, наложенных на ту же группу полей с учетом сочетания базового статуса и допстатуса.

- Группа полей должна иметь ЭП с более поздними датой/временем формирования и эти ЭП должны быть сформированы с тем же сочетанием базового статуса и допстатуса, соответствующих условиям формирования удаляемой ЭП и в настройке **Правила подписания** для удаляемой ЭП признак **Контролировать последовательность подписания** должен быть выключен.

Если все контроли для ЭП пройдены успешно, то:

- удалению подлежат все ЭП документа, наложенные пользователем вызвавшим действие удаления, вне зависимости от роли, которой наложены эти ЭП.
- Если пользователем на документ наложено несколько ЭП, то все ЭП этого пользователя удаляются из документа последовательно, в хронологическом порядке, начиная с ЭП, наиболее поздней по дате/времени наложения.

После удаления откроется информационное окно:

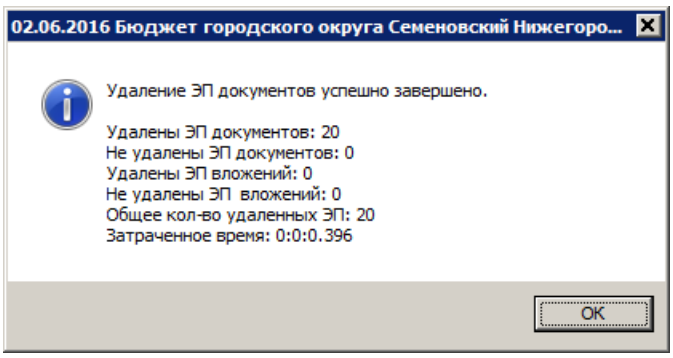

Рисунок 87 – Форма результатов удаления ЭП

Если хотя бы один из контролей не пройден, удаление ЭП становится недоступным.

5.8.3 Удаление ЭП нескольких документов в списке документов

Для одновременного удаления ЭП нескольких документов в списке документов необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документы, в которых необходимо удалить подпись.
3. Нажатием правой кнопки мыши вызвать контекстное меню и выбрать пункт **Удалить подпись**.

Внимание! *Действие доступно если включен параметр* ***Позволять удалять ЭП (Сервис→Системные параметры*** *раздел* ***ЭП*** *закладка* ***Общие****).*

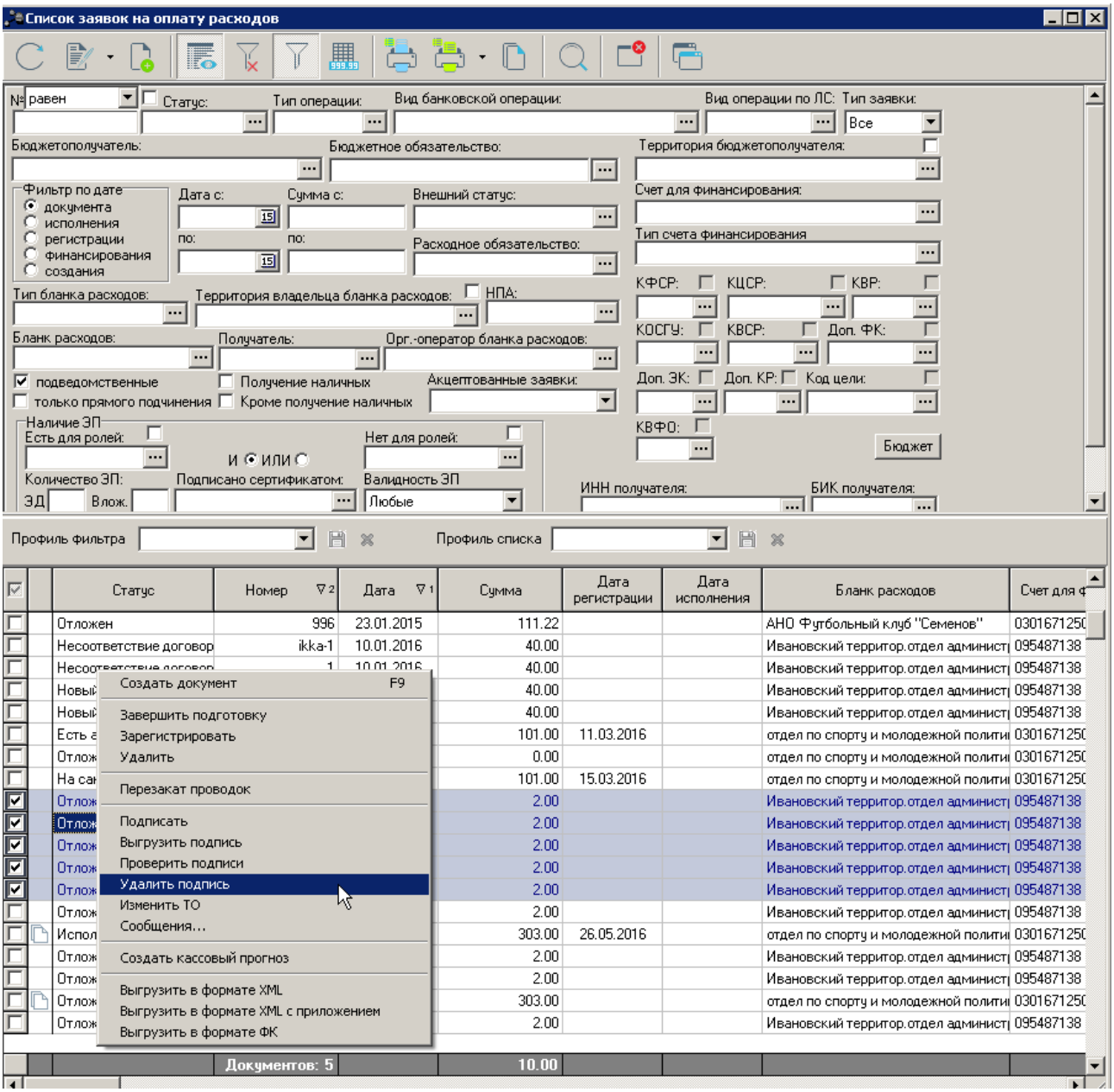

Рисунок 88 – Действие «Удалить подпись» в контекстном меню списка документов

На экране появится окно подтверждения удаления подписей документа. Если удаление необходимо - нажимается кнопка **ОК**, иначе – **Отмена**.

При выполнении удаления для каждой ЭП каждого документа выполняются контроли, определяющие возможность удаления этой. Подробнее см. раздел Удаление ЭП документа в списке документов 99.

5.8.4 Удаление ЭП документа в форме документа

Для удаления ЭП документа в форме документов необходимо выполнить следующие действия:

1. Открыть список документов.
2. В списке документов выделить документ, в котором необходимо удалить подпись, и нажатием кнопки **Редактировать** панели инструментов окна или клавиши <**F4**> вызвать форму его редактирования.
3. В форме редактирования документа, в меню действий, выбрать действие **Удалить подпись**:

Внимание! *Действие доступно если включен параметр* ***Позволять удалять ЭП*** *(****Сервис→Системные параметры*** *раздел* ***ЭП*** *закладка* ***Общие****).*

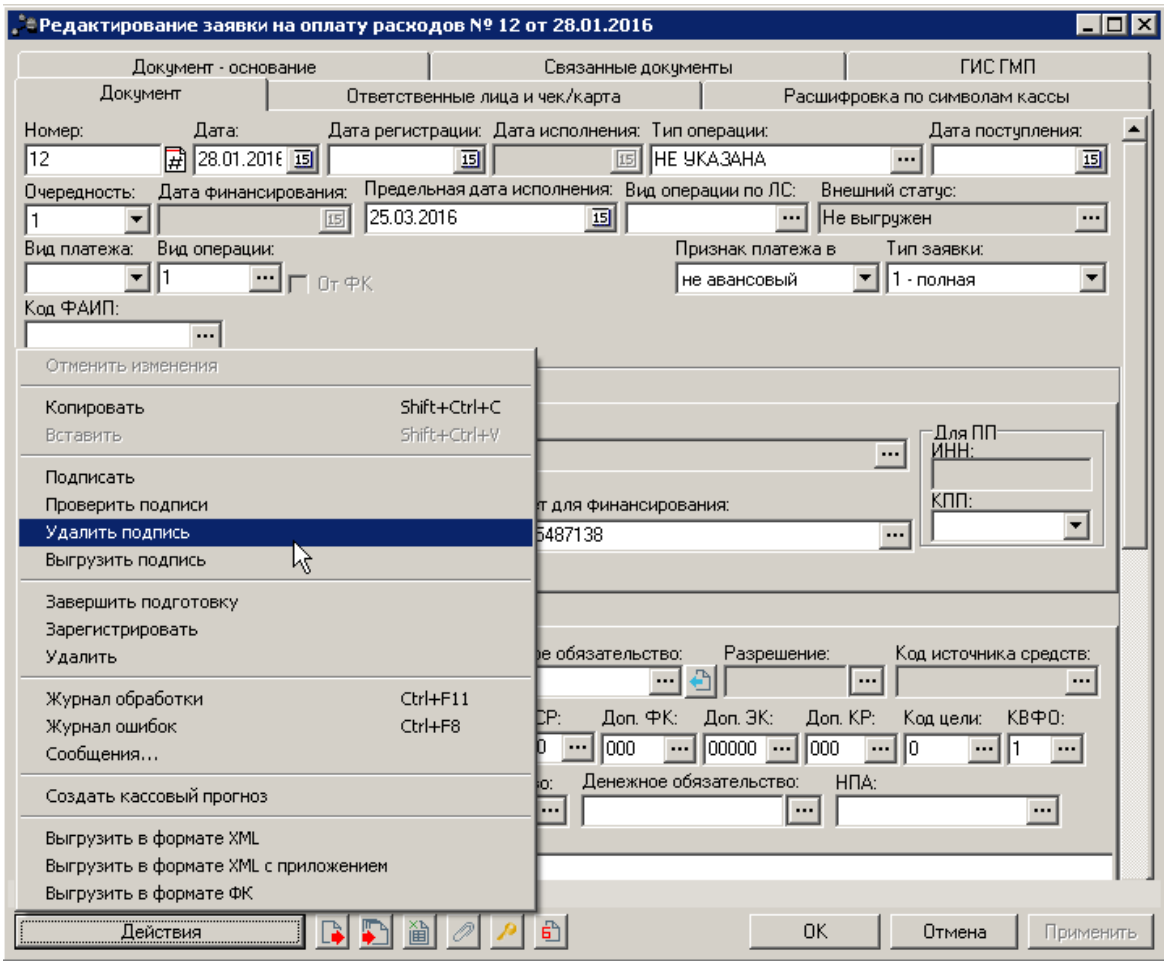

Рисунок 89 – Действие «Удалить подпись» в контекстном меню формы документа

На экране появится окно подтверждения удаления подписей документа. Если удаление необходимо - нажимается кнопка **ОК**, иначе – **Отмена**.

При выполнении удаления для каждой ЭП документа выполняются контроли, определяющие возможность удаления этой ЭП. Подробнее см. раздел Удаление ЭП документа в списке документов 99.

6

Порядок контроля юридической значимости электронных документов

Текущая реализация функций подписания ЭД и выгрузки документов с ЭП не позволяет контролировать юридическую значимость подписываемых и выгружаемых документов. Возможность подписания и выгрузки документов пользователями должна регулироваться в организационном порядке, в соответствии с внутренними регламентами обработки ЭД, принятыми на объекте автоматизации. Управление правами подписания ЭД и выгрузки документов с ЭП осуществляется посредством настройки функциональных ролей пользователей.

7

Приложения

7.1 Приложение 1. Подписание электронного документа УЭП

Для подписания электронного документа УЭП необходимо наличие:

- СКЗИ (ГОСТ 34.11-2012 и 34.10-2012);
- сертификата ключа подписи, для которого имеется закрытый ключ УЭП;
- закрытого ключа УЭП;
- подписываемого УЭД.

Схема подписания электронного документа УЭП:

Рисунок 90 – Схема подписания электронного документа УЭП

7.2 Приложение 2. Проверка УЭП электронного документа

Для проверки электронной подписи электронного документа необходимо наличие:

- СКЗИ (ГОСТ 34.11-2012 и 34.10-2012);

- сертификата ключа подписи, использованного для подписания ЭД;
- ЭД, подписанного УЭП.

Схема проверки УЭП электронного документа:

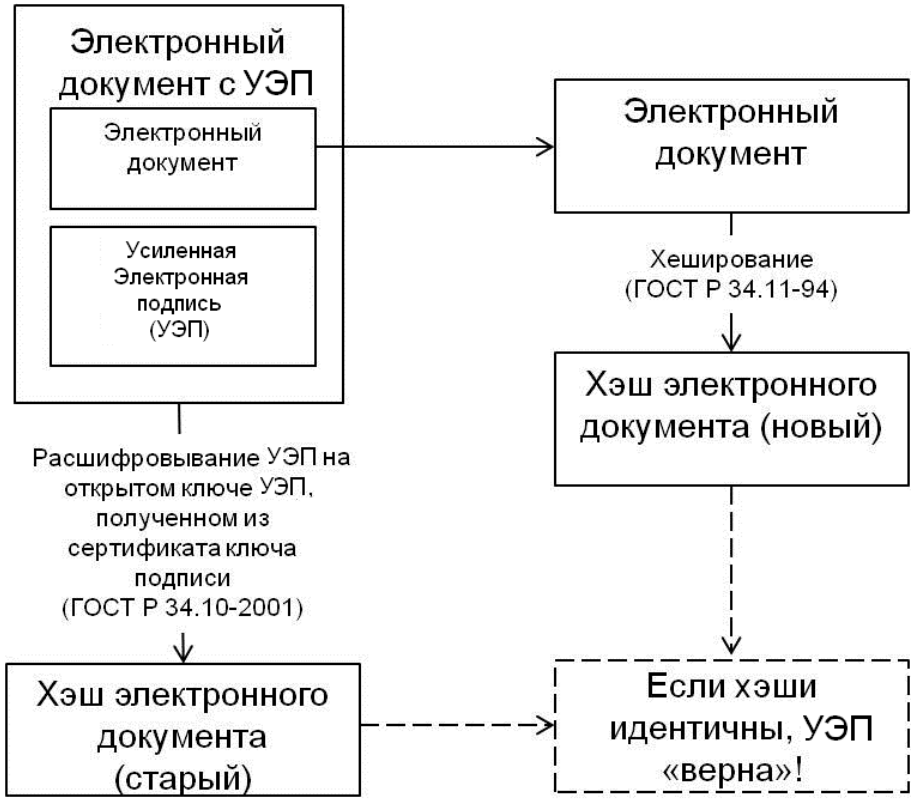

Рисунок 91 – Схема проверки УЭП электронного документа

7.3 Приложение 3. Подписание электронного документа УЭП с доказательствами подлинности

Процесс подписания электронного документа УЭП с доказательсвами подлинности состоит из следующих этапов:

- создание ЭП;
- получение штампа времени на документ и ЭП;
- сбор доказательств подлинности ЭП и присоединение их хеш-кодов к подписанному документу;
- получение штампа времени на доказательства подлинности;
- присоединение доказательств подлинности к ЭП.

Схема подписания электронного документа УЭП с доказательсвами подлинности:

Рисунок 92 – Схема подписания электронного документа УЭП с доказательсвами подлинности

7.4 Приложение 4. Проверка УЭП с доказательствами подлинности электронного документа

Проверка УЭП с доказательсвами подлинности предполагает выполнение следующих операций:

- подтверждение подлинности ЭП в ЭД;

- подтверждение принадлежности ЭП в документе владельцу сертификата ключа подписи;
- подтверждение отсутствия искажений в подписанном данной цифровой подписью документе;
- подтверждение момента подписания документа ЭП;
- подтверждение действительности сертификата ключа подписи на момент подписания документа ЭП.

Схема проверки УЭП с доказательсвами подлинности:

Рисунок 93 – Схема проверки УЭП с доказательсвами подлинности электронного документа

7.5 Приложение 5. Алгоритм подписания ЭД УЭП в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»»

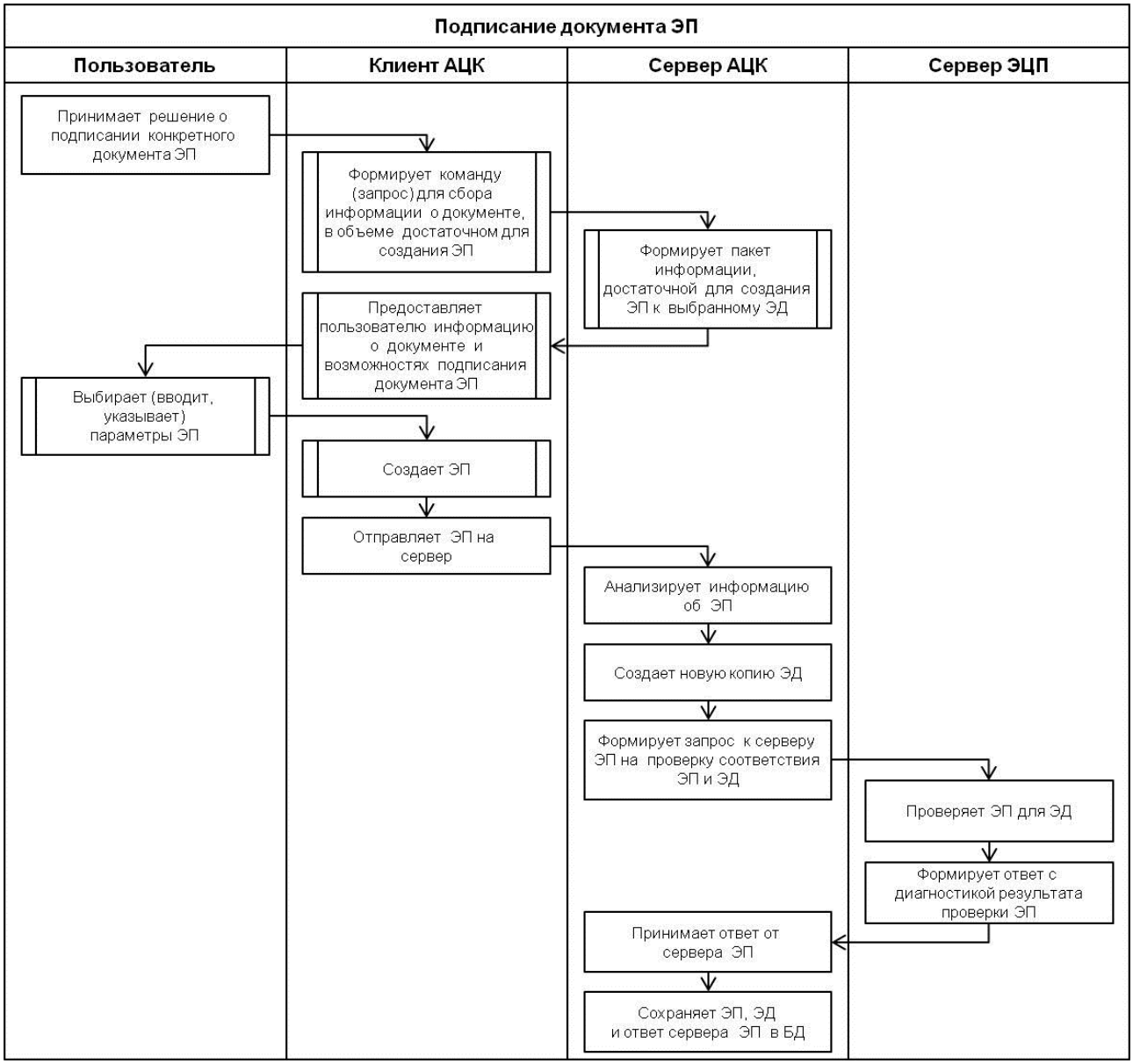

Рисунок 94 – Схема алгоритма подписания ЭД УЭП в «АЦК-Госзаказ»/«АЦК-Муниципальный заказ»

7.6 Приложение 6. Алгоритм локальной проверки УЭП ЭД в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»»

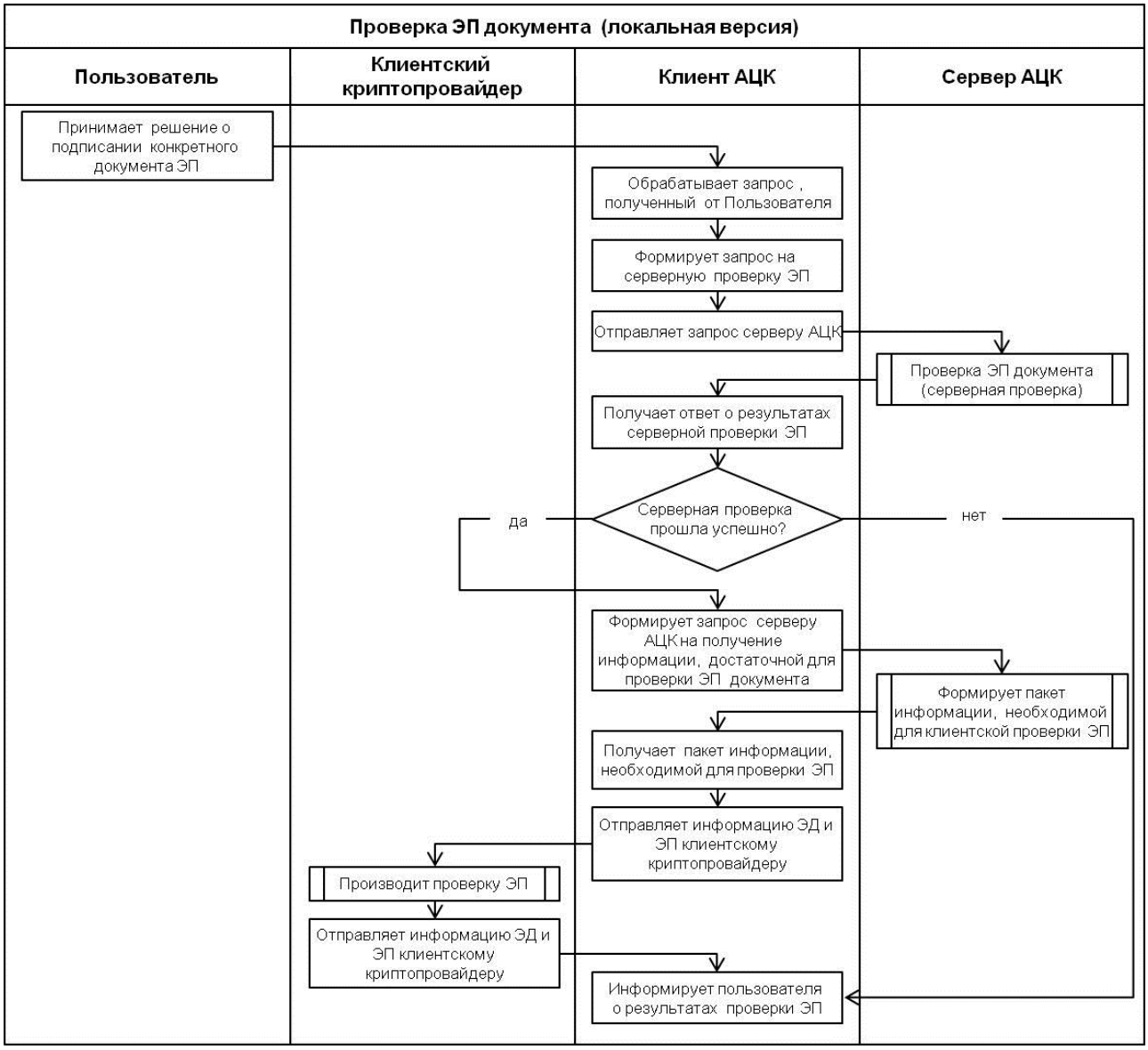

Рисунок 95 – Схема алгоритма локальной проверки УЭП ЭД в «АЦК-Госзаказ»/«АЦК-Муниципальный заказ»

7.7 Приложение 7. Алгоритм серверной проверки УЭП ЭД в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»»

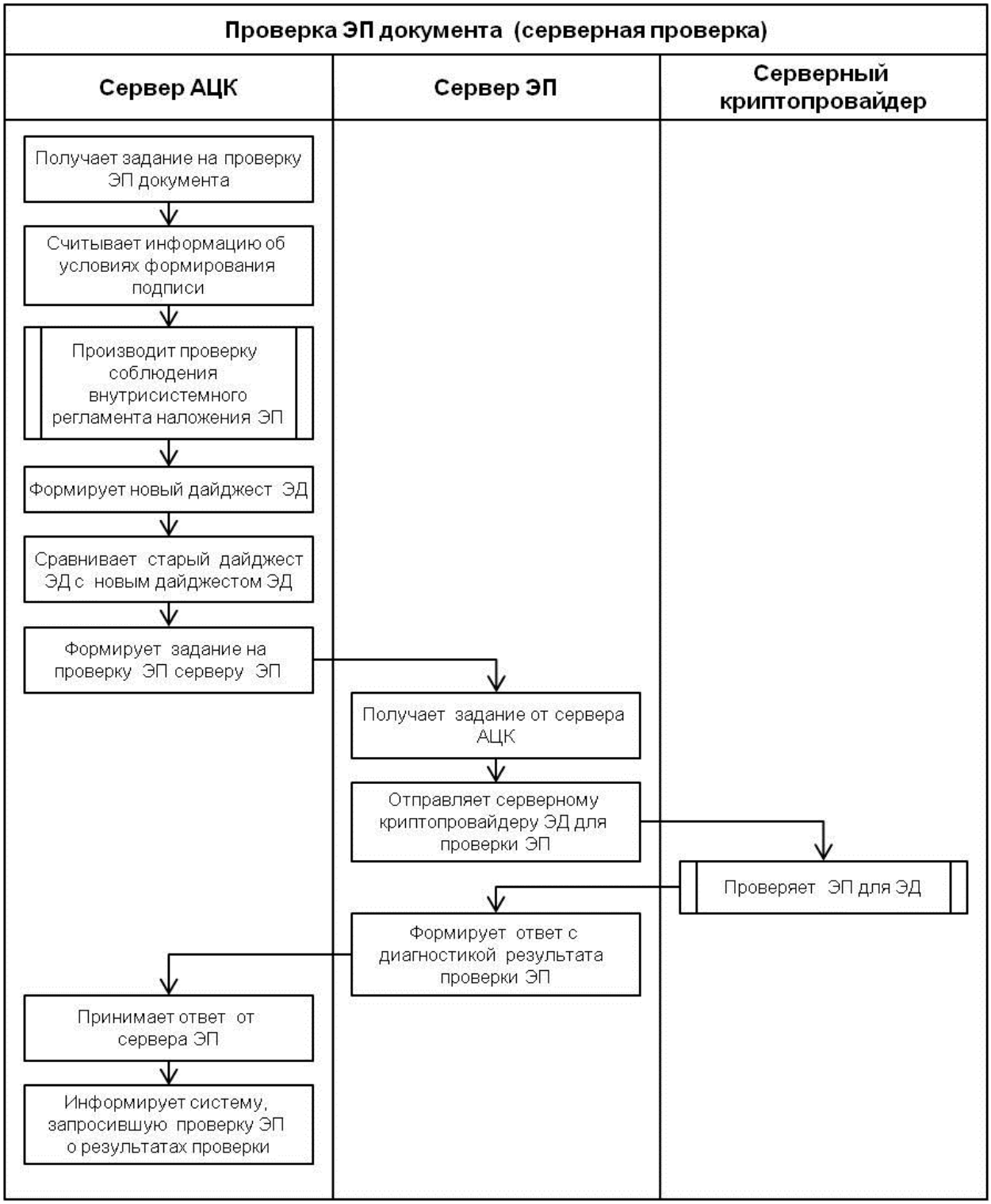

Рисунок 96 – Схема алгоритма серверной проверки УЭП ЭД в «АЦК-Госзаказ»/«АЦК-Муниципальный заказ»

7.8 Приложение 8. Место ЭП в документообороте

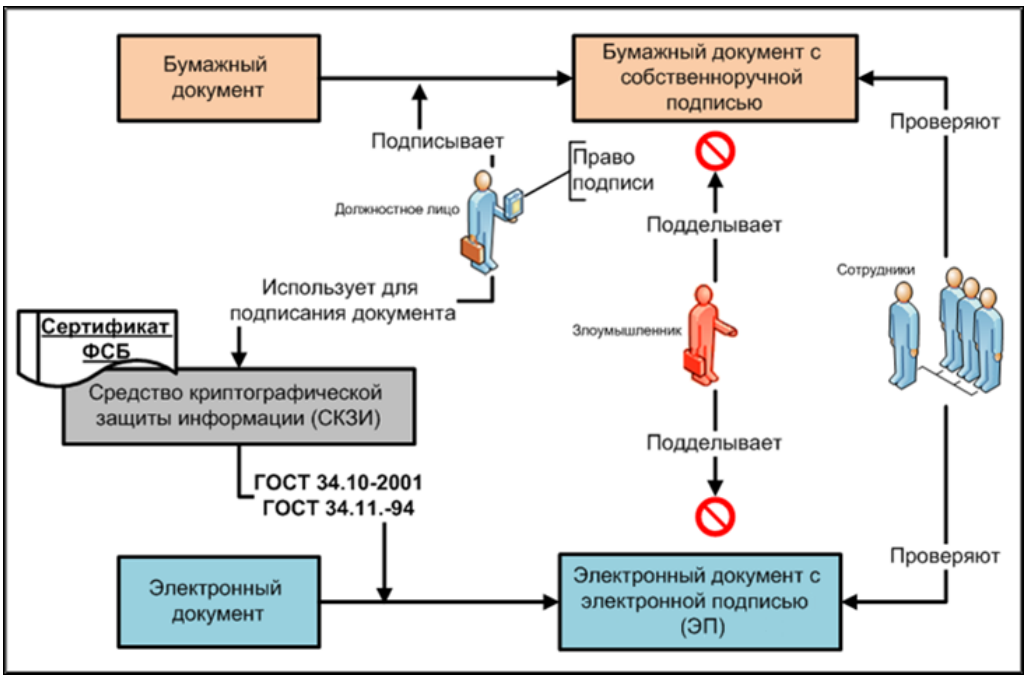

Рисунок 97 – Место электронной подписи (ЭП) в документообороте

7.9 Приложение 9. Инструкция по установке КриптоПро CSP

Внимание! *Данная инструкция написана на основании документации компании* ***КриптоПро****. Для получения актуальной информации смотри последнюю версию документации, поставляемой компанией.*

1. ТРЕБОВАНИЯ К СИСТЕМЕ

ПО СКЗИ КриптоПро CSP предназначено для использования в ОС Windows 2000/XP/2003/Vista/2008/7 на ПЭВМ типа IBM PC с процессором Pentium и выше.

В состав дополнительных аппаратных средств ПЭВМ может входить средство для обеспечения контроля целостности ПО и предотвращения загрузки ОС с нештатных носителей.

2. КОНТРОЛЬ ЦЕЛОСТНОСТИ ДИСТРИБУТИВА

Программа **CPVERIFY.EXE** поставляется вместе с дистрибутивом и предназначена для контроля целостности дистрибутивов, изготовленных организацией-разработчиком ПО. Контроль целостности файлов осуществляется при загрузке файла на исполнение (и периодически во время выполнения) или при ручном запуске программы контроля целостности (см. опцию *-rv* ниже).

Примечание*. Программа* ***CPVERIFY.EXE*** *является средством проверки целостности дистрибутива и не заменяет собой средства контроля целостности уже установленного ПО.*

Синтаксис командной строки для запуска программы **CPVERIFY.EXE** выглядит следующим образом:

- Проверка целостности заданного файла с использованием значения хеш-функции:

cpverify.exe filename hashvalue

где:

- **filename** – имя проверяемого файла;
- **hashvalue** – ранее вычисленное значение хеш-функции, 64 символа.

При проверке целостности дистрибутивного файла, значение хеш-функции вводится из лицензионного бланка.

В случае успешного завершения проверки программа выдает сообщение **File filename has been verified** (где *filename* – имя проверяемого файла) и возвращает ненулевой код возврата.

Нулевой код возврата и вывод сообщения **File filename was corrupted** на экран обозначает несоответствие значения хеш-функции, вычисленной разработчиком для дистрибутива, и свидетельствует об изменениях исходного файла. В данном случае процесс установки дистрибутива ПО СКЗИ КриптоПро CSP должен быть прерван.

3. УСТАНОВКА ДИСТРИБУТИВА ПО СКЗИ КриптоПро CSP

Установка дистрибутива должна производиться пользователем, имеющим права администратора.

Перед установкой дистрибутива ПО СКЗИ КриптоПро CSP удалите все ранее существующие версии устанавливаемого ПО. Для этого используете пункты основного меню Windows **Пуск→Настройка→Панель управления→Установка и удаление программ**:

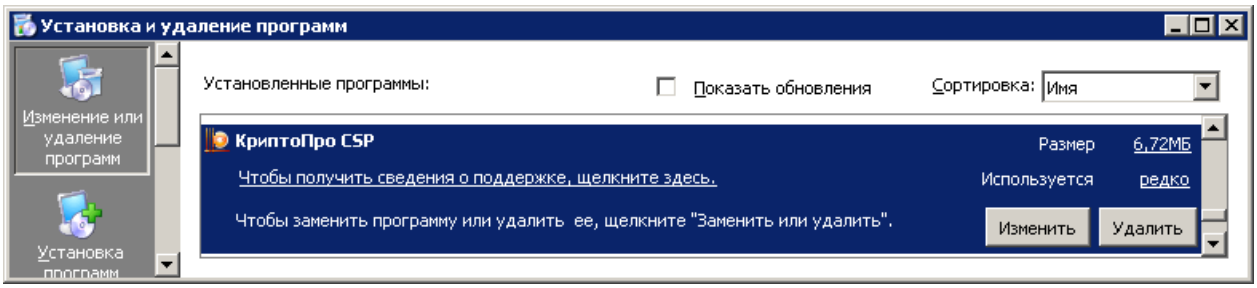

Рисунок 98 – Окно «Установка и удаление программ»

Установка программного обеспечения производится путем запуска программы **CPCSP.EXE** (или программы **SETUP.EXE**, находящейся на первом диске дистрибутива, если дистрибутив записан на несколько магнитных носителей – дискет). Для запуска программы используете пункты **Пуск→Выполнить** главного окна Windows:

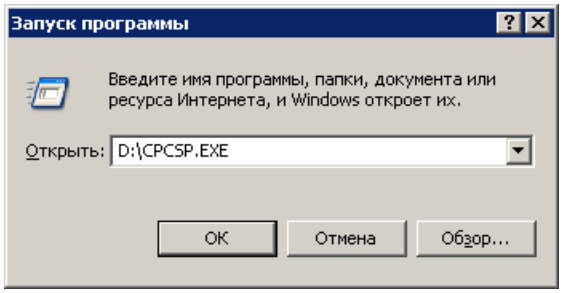

Рисунок 99 – Окно «Выполнить»

При установке дистрибутива дальнейшая установка производится в соответствии с сообщениями, выдаваемыми ПО установки.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

4. ИЗМЕНЕНИЕ НАБОРА УСТРОЙСТВ ХРАНЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Программа установки по умолчанию устанавливает все модули, обеспечивающие работу с различными поддерживаемыми устройствами хранения ключевой информации, но при этом настойки СКЗИ КриптоПро CSP допускают использовать в качестве ключевого носителя только дискету 3,5». Если для работы с ПО СКЗИ необходимы дополнительные типы устройств работы с ключевыми носителями, выберите режим изменения их состава.

Для этого откройте панель управления компьютером, используя пункты меню **Пуск→Настройка→Панель управления**, и в окне панели управления выберите значок **КриптоПро CSP**:

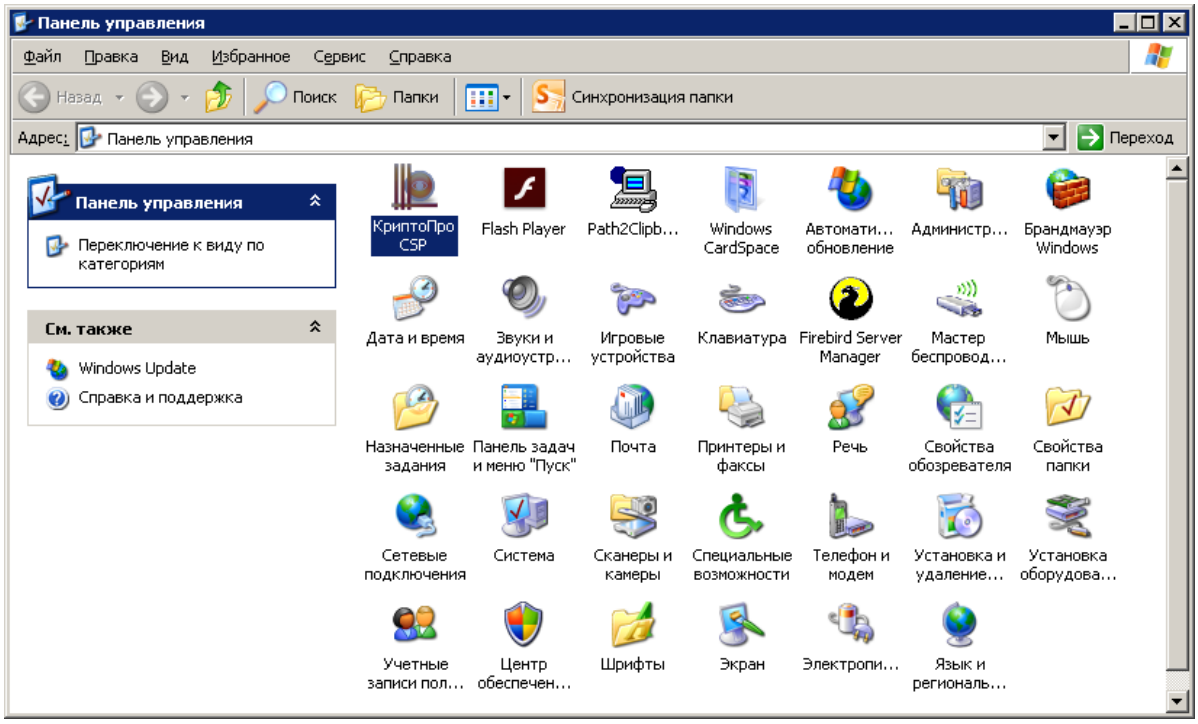

Рисунок 100 – Окно панели управления

В форме настройки СКЗИ КриптоПро CSP выберите закладку **Оборудование** и нажмите кнопку **Настроить считыватели**:

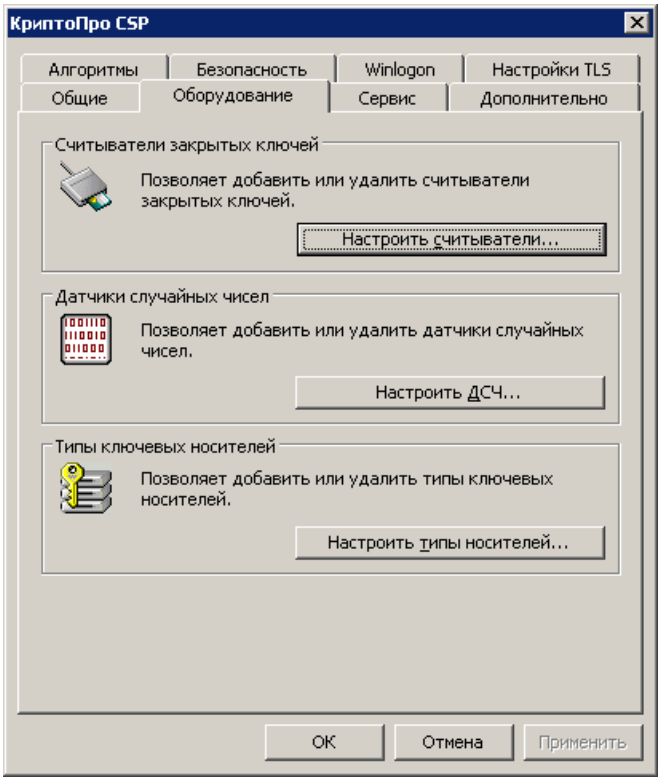

Рисунок 101 – Форма настройки КриптоПро CSP, закладка «Оборудование»

В окне мастера настройки считывателя добавьте или удалите из списка те устройства, которые будут использованы в качестве считывателей ключевой информации.

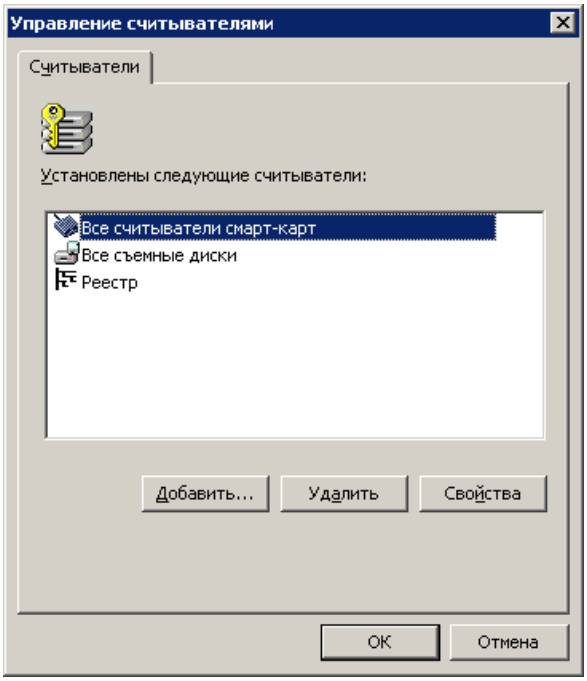

Рисунок 102 – Окно мастера настройки считывателя

***Примечание**. В состав дистрибутива СКЗИ КриптоПро CSP не входят драйверы и другие модули третьих производителей, обеспечивающие взаимодействие СКЗИ с аппаратной частью. Для их установки нужно воспользоваться программой установки, поставляемой производителями таких устройств, либо получить их с сервера разработчика СКЗИ КриптоПро CSP по адресу **www.cryptopro.ru/CryptoPro/moduls.html**. Например, если CSP уже установлен и нужно использовать новые устройства, необходимо установить поддерживающие драйверы и другие модули от производителей этих устройств.*

Программное обеспечение СКЗИ КриптоПро CSP распространяется с ограниченным сроком использованием – 30 дней. До истечения этого срока пользователь должен ввести серийный номер и код активации с Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (Дилера).

На закладке **Общие** формы настройки СКЗИ КриптоПро CSP нажмите кнопку **Ввод лицензии** и введите **серийный номер (License serial number)** с бланка Лицензии:

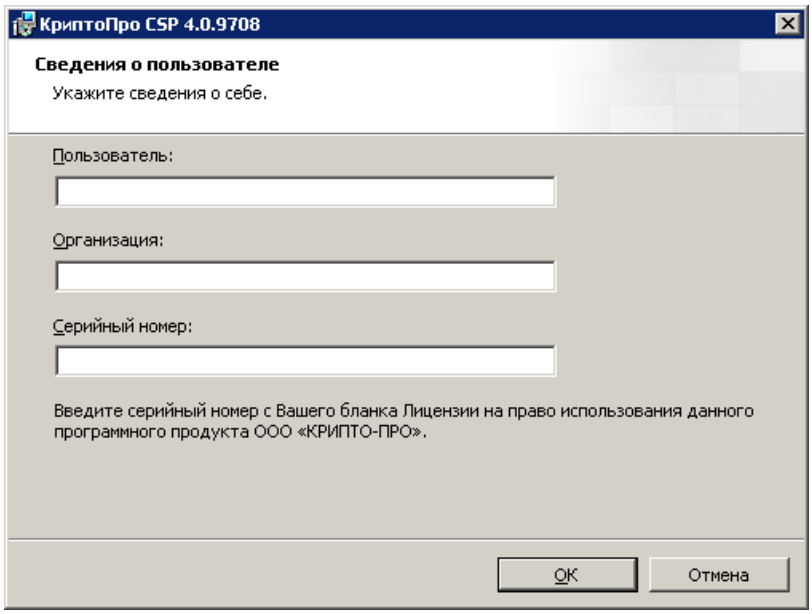

Рисунок 103 – Окно ввода информации о лицензии

После завершения программы установки рекомендуется зарегистрировать установленное ПО СКЗИ КриптоПро CSP у организации-разработчика. Для этого откройте панель управления компьютером, используя пункты меню, **Пуск→Настройка→Панель управления**, и в окне панели управления выберите значок **КриптоПро CSP**.

В панели настройки СКЗИ КриптоПро CSP выберите пункт **Регистрация** и выполните регистрацию.

5. НАСТРОЙКА ПО СКЗИ

СКЗИ КриптоПро CSP может функционировать и хранить ключевую информацию в двух режимах:

- в памяти приложения;
- в «Службе хранения ключей», которая реализована в виде системного сервиса.

При выборе параметра **в памяти приложений** или **в «Службе хранения ключей»** с

выключенной настройкой **Включить кеширование** для подписи всегда требуется носитель закрытого ключа. При выборе параметра **в «Службе хранения ключей»** с включенной настройкой **Включить кеширование** после одного использования ключа носитель можно будет удалить – подписывать этим ключом можно будет без носителя до тех пор, пока служба хранения ключей не будет перезапущена, или ключ не будет вымещен из кэша другими ключами.

Функционирование СКЗИ КриптоПро CSP в **Службе хранения ключей** обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на ПЭВМ, но может незначительно снизить производительность.

Для изменения режима функционирования СКЗИ откройте форму настроек СКЗИ КриптоПро CSP, как описано в предыдущем пункте, выберите закладку **Безопасность** и выберите необходимый режим:

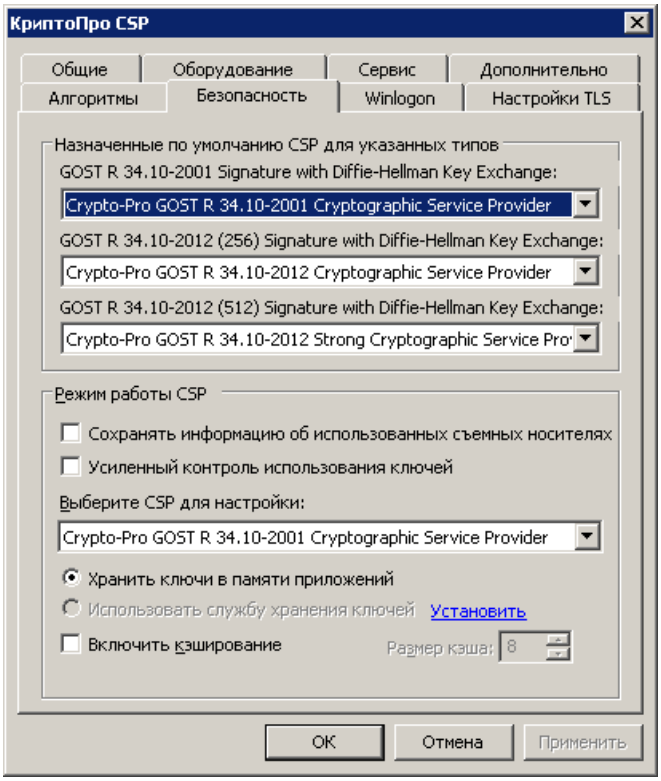

Рисунок 104 – Форма настройки КриптоПро CSP, закладка «Безопасность»

7.10 Приложение 10. Инструкция по установке модуля поддержки УЭП

Для установки модуля поддержки УЭП необходимо выполнить следующие действия:

1. Запустить на выполнение установочный файл модуля **cades-win32.msi**, после чего выполнить установку следуя указаниям программы **КриптоПро ЭЦП Runtime**:
   - В открывшемся окне мастера установки нажать кнопку **Далее**:

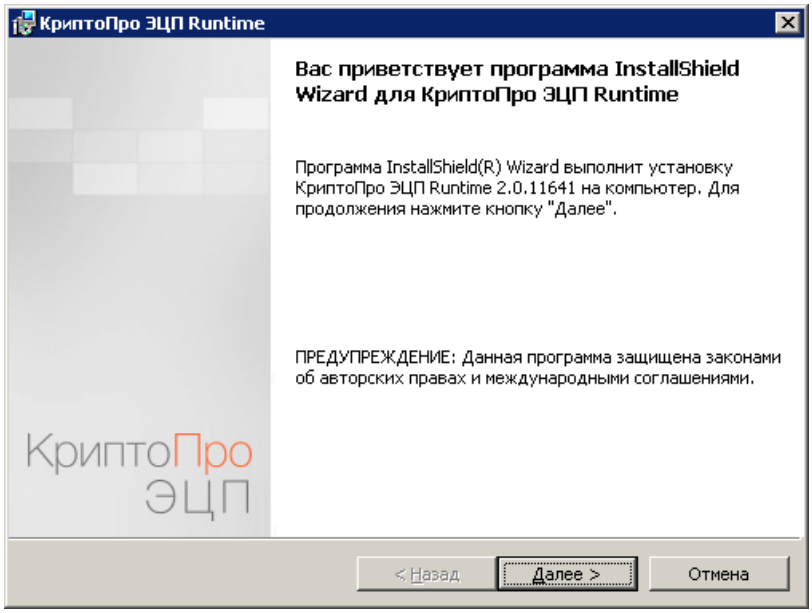

Рисунок 105 – Мастер установки КриптоПро ЭЦП Runtime, шаг 1

- В следующем окне выбрать пункт **Я принимаю условия лицензионного соглашения** и нажать кнопку **Далее**:

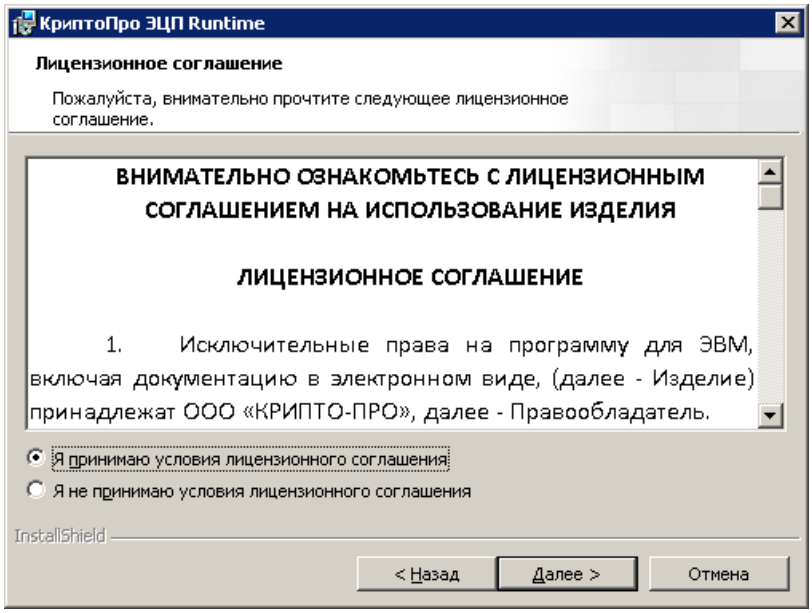

Рисунок 106 – Мастер установки КриптоПро ЭЦП Runtime, шаг 2

- В новом окне заполнить поля **Пользователь** и **Организация** и нажать кнопку **Далее**:

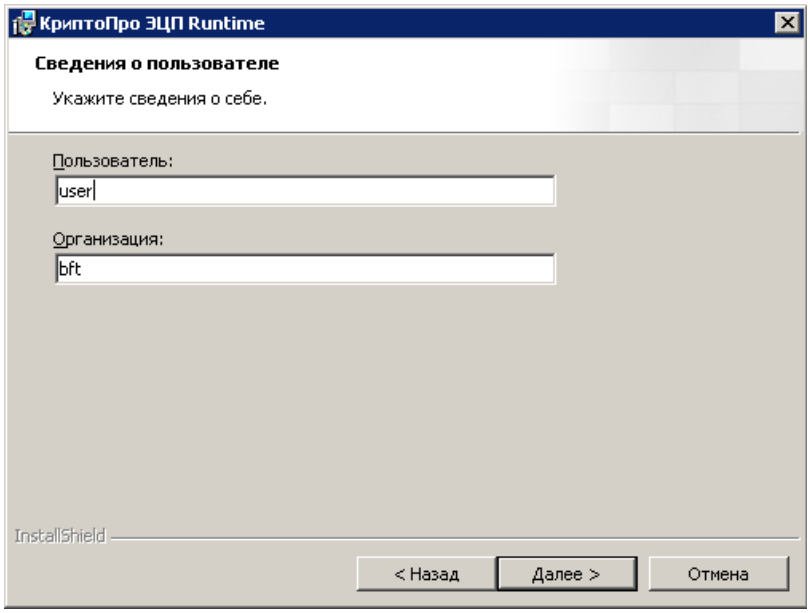

Рисунок 107 – Мастер установки КриптоПро ЭЦП Runtime, шаг 3

- В открывшемся нажать кнопку **Установить**:

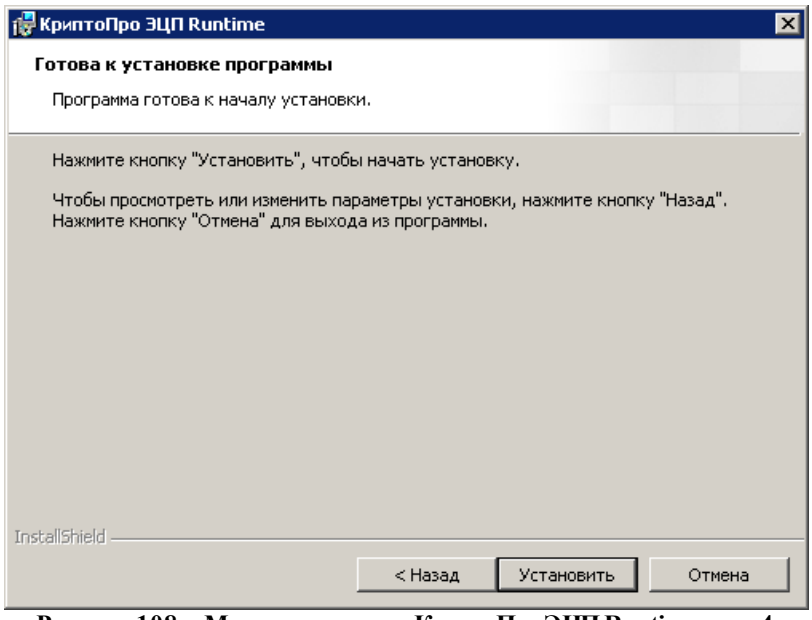

Рисунок 108 – Мастер установки КриптоПро ЭЦП Runtime, шаг 4

- В следующем окне показан ход установки **КриптоПро ЭЦП Runtime**:

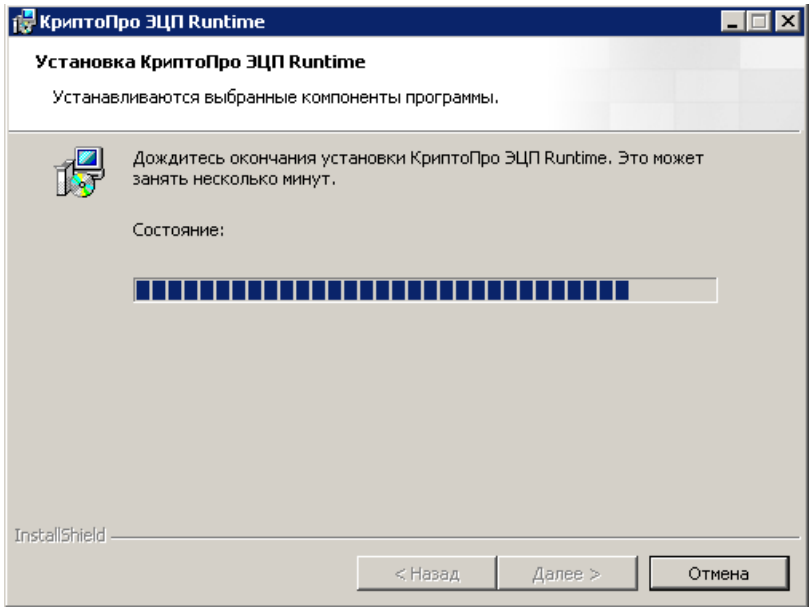

Рисунок 109 – Мастер установки КриптоПро ЭЦП Runtime, шаг 5

- В открывшемся окне нажать кнопку **Готово**:

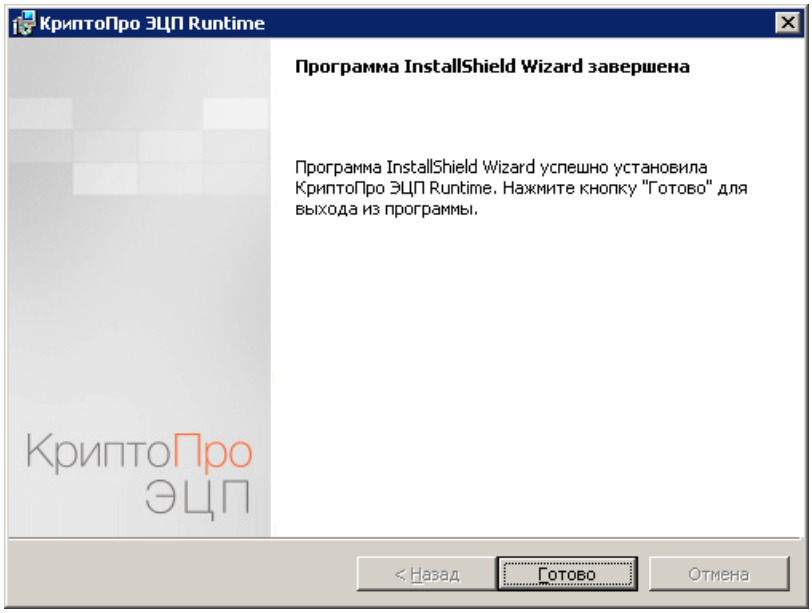

Рисунок 110 – Мастер установки КриптоПро ЭЦП Runtime, шаг 6

2. По окончании установки модуля проверить наличие в меню **Пуск→Программы** группы **Крипто-Про**, содержащей элементы:

- **КриптоПро PKI** для доступа к настройкам OCSP- и TSP-клиентов;
- **Сертификаты** для управления сертификатами, установленными на компьютере;
- **Управление лицензиями КриптоПро PKI** для управления лицензиями, установленными на компьютере.

7.11 Приложение 11. Инструкция по настройке OCSP-клиента

OCSP-клиент КриптоПро предназначен для обращения к службам актуальных статусов сертификатов по протоколу OCSP поверх HTTP, для работы с OCSP-запросами и OCSP-ответами.

Для настройки OCSP-клиента необходимо выполнить следующие действия:

1. Ввести лицензию на OCSP-клиент КриптоПро в оснастке консоли **КриптоПро PKI (Пуск→Программы→КриптоПро→КриптоПро PKI)**.
   - В контекстном меню раздела **Управление лицензиями→КриптоПро OCSP Client** выбрать пункт **Все задачи→Ввести серийный номер...**:

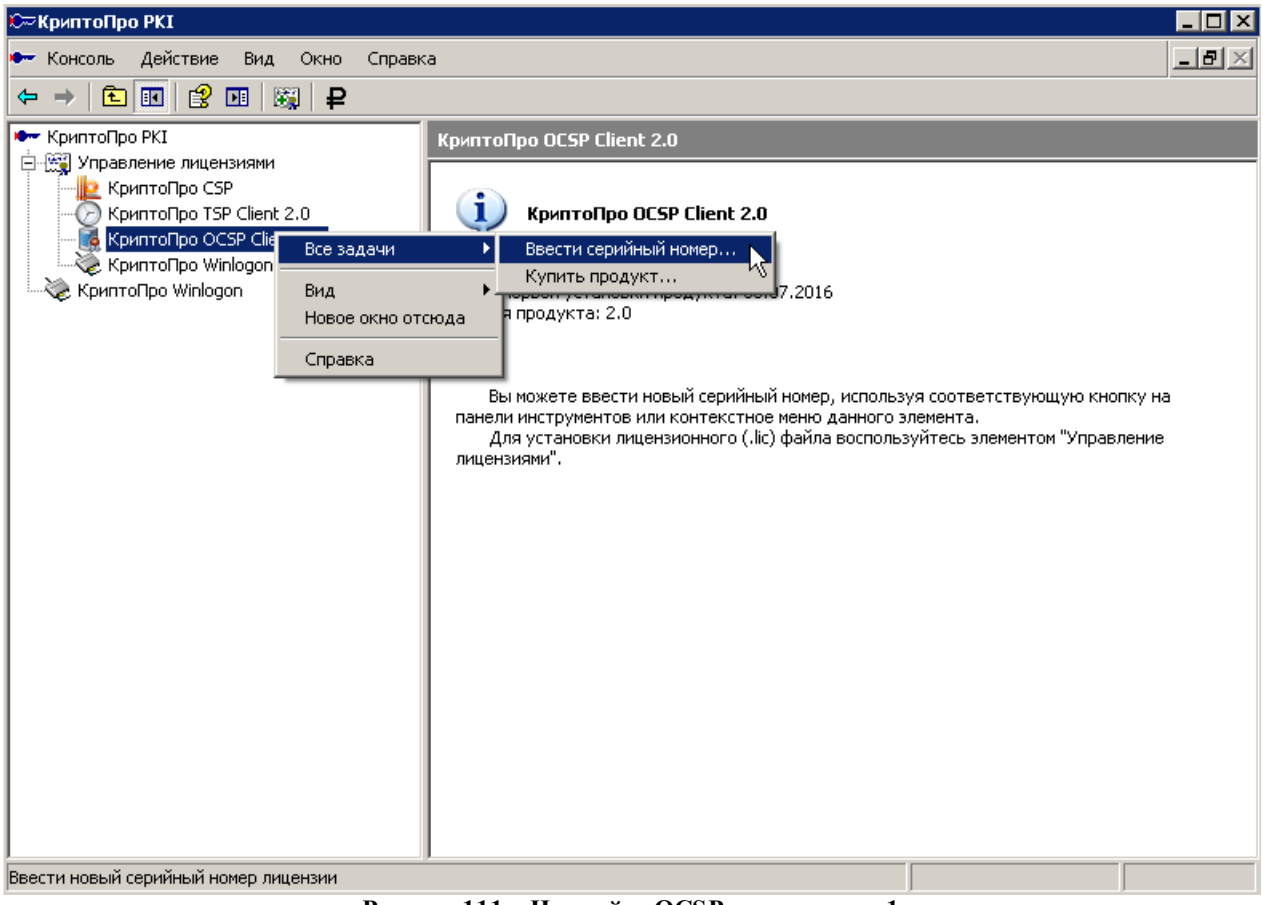

Рисунок 111 – Настройка OCSP-клиента, шаг 1

   - В открывшейся форме ввода лицензии ввести серийный номер в виде последовательности символов **0AXXX-XXXXX-XXXXX-XXXXX-XXXXX**. Если оставить поле ввода серийного номера лицензии пустым, **КриптоПро OCSP Client** будет работать в ознакомительном режиме в течение 30 дней с момента первой установки.

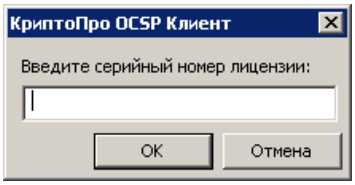

Рисунок 112 – Форма ввода серийного номера лицензии

2. Открыть консоль настройки групповых политик (**Пуск→Выполнить→gpedit.msc**).
3. В зависимости от того, на уровне пользователя или на уровне компьютера настраивается OCSP-клиент, выбрать раздел **Политика «Локальный компьютер»→Конфигурация компьютера→Административные шаблоны→КриптоПро→КриптоПро OCSP Client** или **Политика «Локальный компьютер»→Конфигурация пользователя→Административные шаблоны→КриптоПро→КриптоПро OCSP Client** настроек.

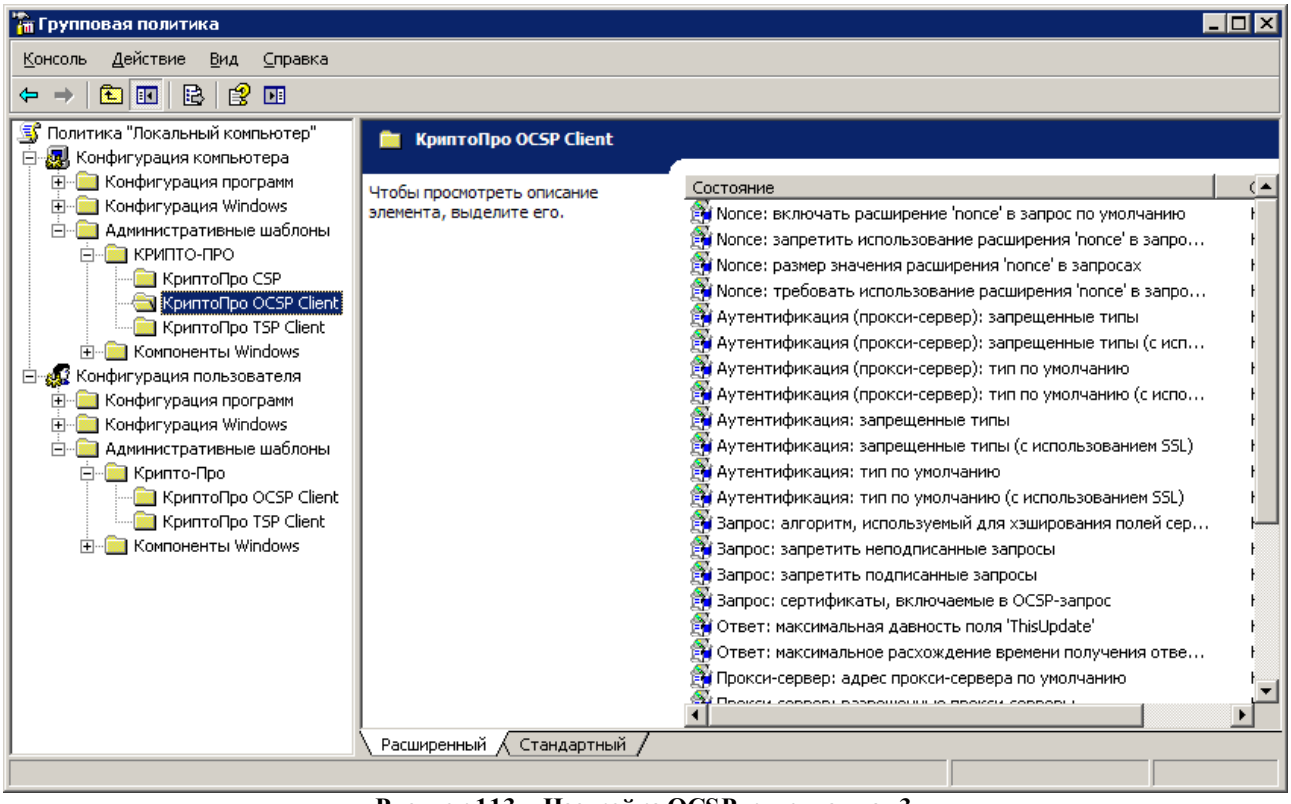

Рисунок 113 – Настройка OCSP-клиента, шаг 3

4. Открыть двойным щелчком мыши настройку **Прокси-сервер: адрес прокси-сервера по умолчанию** и ввести адрес прокси-сервера в формате:

<protocol>://<username>:<password>@<host>:<port>

Например:

http://ivanov:12345@proxy.myhost.com:8080

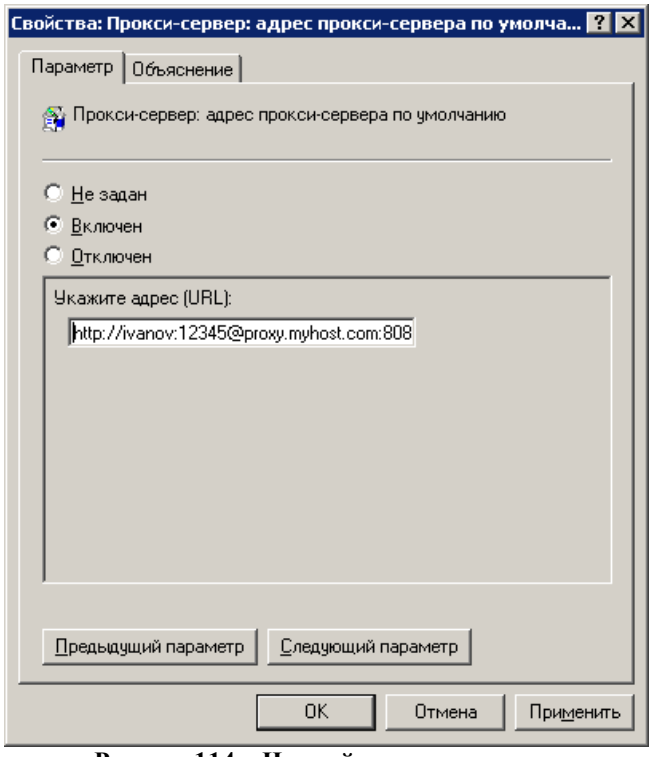

Рисунок 114 – Настройка прокси-сервера

Нажать кнопку **ОК**.

5. Открыть двойным щелчком мыши настройку **Аутентификация (прокси-сервер): тип по умолчанию** и ввести тип аутентификации **Обычная**:

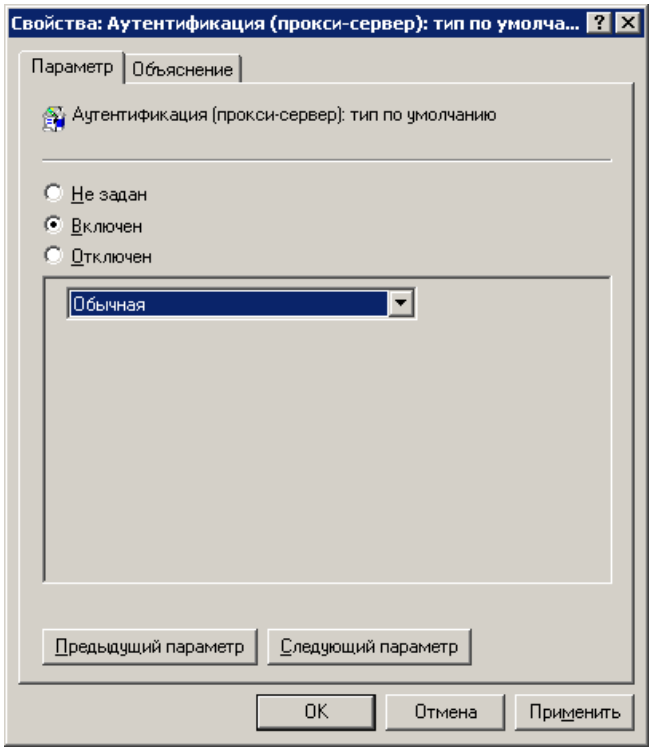

Рисунок 115 – Аутентификация прокси-сервера

Нажать кнопку **ОК**.

6. Закрыть консоль настройки групповых политик.

7.12 Приложение 12. Инструкция по настройке TSP-клиента

TSP-клиент КриптоПро предназначен для обращения к серверам штампов времени по протоколу TSP поверх HTTP, для работы с запросами на штампы и с самими штампами времени.

Для настройки TSP-клиента необходимо выполнить следующие действия:

1. Ввести лицензию на TSP-клиент КриптоПро в оснастке консоли **КриптоПро PKI** (**Пуск→Программы→КриптоПро→КриптоПро PKI**).
   - В контекстном меню раздела **Управление лицензиями→КриптоПро TSP Client** выбрать пункт **Все задачи→Ввести серийный номер...**:

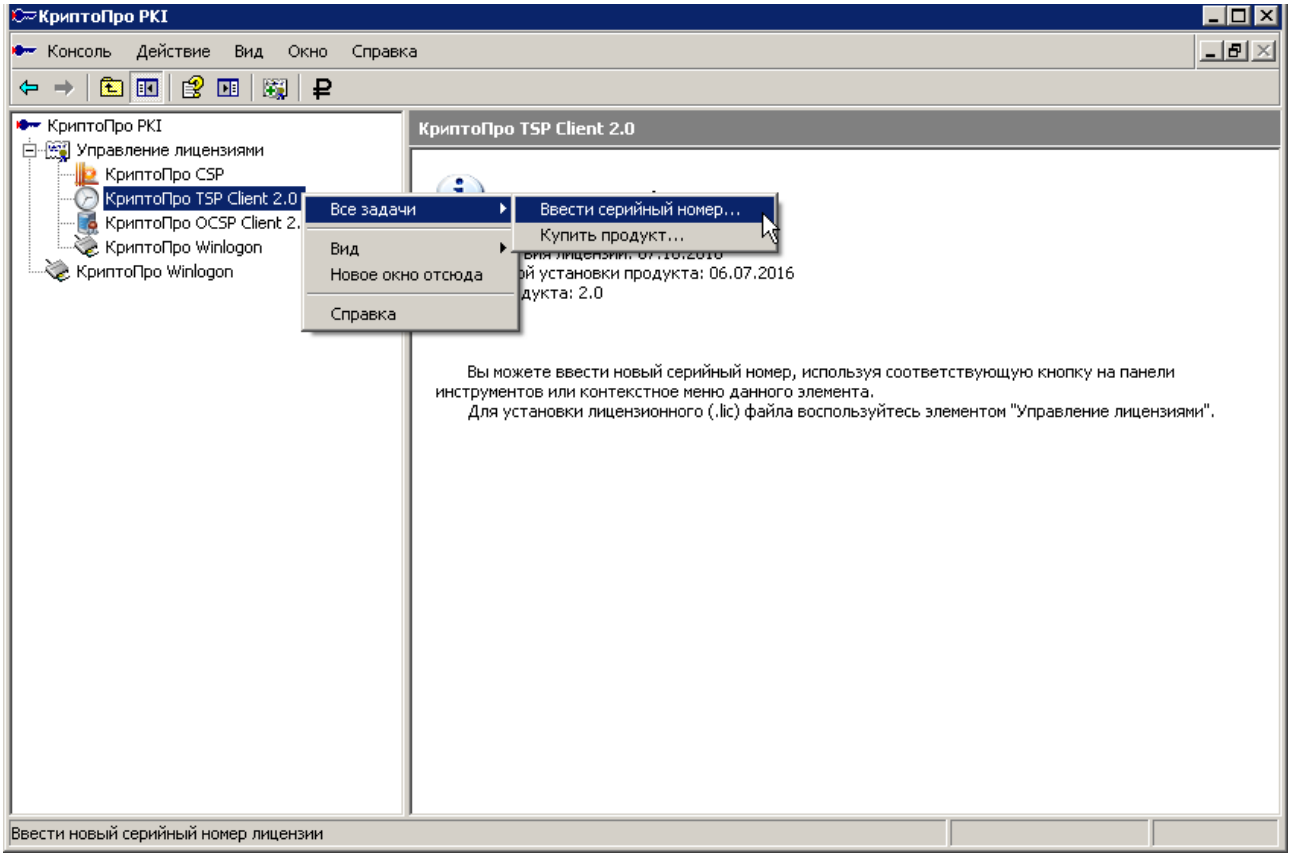

Рисунок 116 – Настройка TSP-клиента, шаг 1

   - В открывшейся форме ввода лицензии ввести серийный номер в виде последовательности символов TA*XXX*-**XXXXX-XXXXX-XXXXX-XXXXX**. Если оставить поле ввода серийного номера лицензии пустым, КриптоПро TSP Client будет работать в ознакомительном режиме в течение 30 дней с момента первой установки:

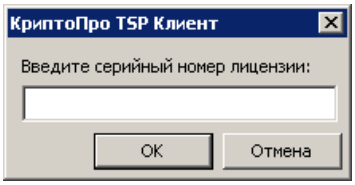

Рисунок 117 – Окно ввода серийного номера лицензии

2. Открыть консоль настройки групповых политик (**Пуск→Выполнить→gpedit.msc**).
3. В зависимости от того, на уровне пользователя или на уровне компьютера настраивается TSP-клиент, выбрать раздел **Политика «Локальный компьютер»→Конфигурация компьютера→Административные шаблоны→КриптоПро→КриптоПро TSP Client** или **Политика «Локальный компьютер»→Конфигурация пользователя→Административные шаблоны→КриптоПро→КриптоПро TSP Client** настроек:

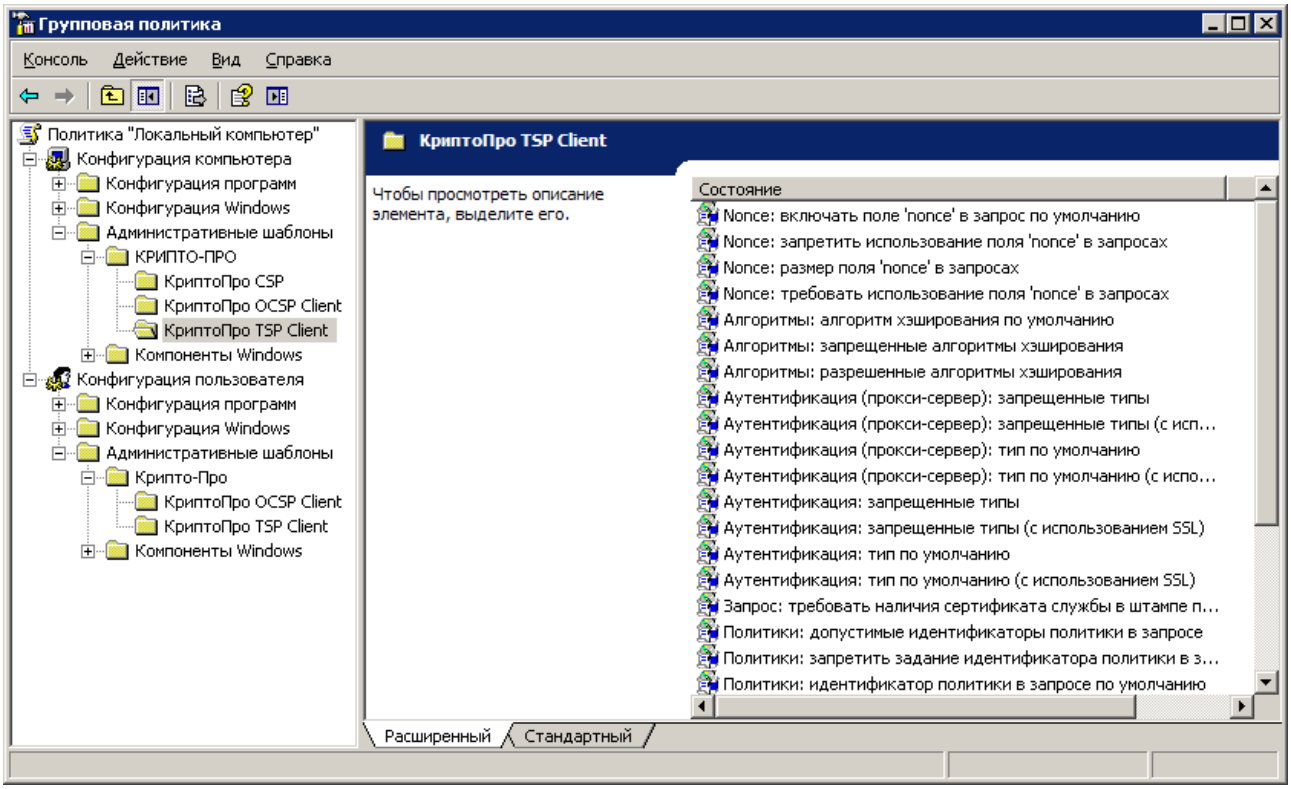

Рисунок 118 – Настройка TSP-клиента, шаг 3

4. Открыть двойным щелчком мыши настройку **Службы штампов: адрес службы штампов времени по умолчанию** и ввести адрес службы штампов времени:

http://www.cryptopro.ru/tsp/tsp.srf

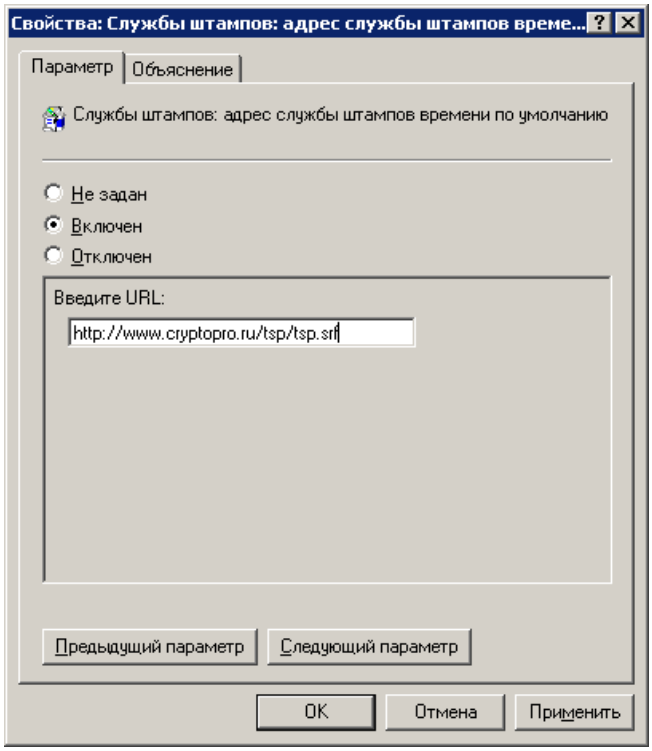

Рисунок 119 – Служба штампов

Нажать кнопку **ОК**.

5. Открыть двойным щелчком мыши настройку **Прокси-серверы: адрес прокси-сервера по умолчанию** 125 и ввести адрес прокси-сервера в формате:

```
<protocol>://<username>:<password>@<host>:<port>
```

Например:

```
http://ivanov:12345@proxy.myhost.com:8080
```

Нажать кнопку **ОК**.

6. Открыть двойным щелчком мыши настройку **Аутентификация (прокси-сервер): тип по умолчанию** 125 и ввести тип аутентификации **Обычная**. Нажать кнопку **ОК**.

7. Если требует технологический процесс, аналогично описанным способом включить настройку **Запрос: требовать наличия сертификата службы в штампе по умолчанию**.

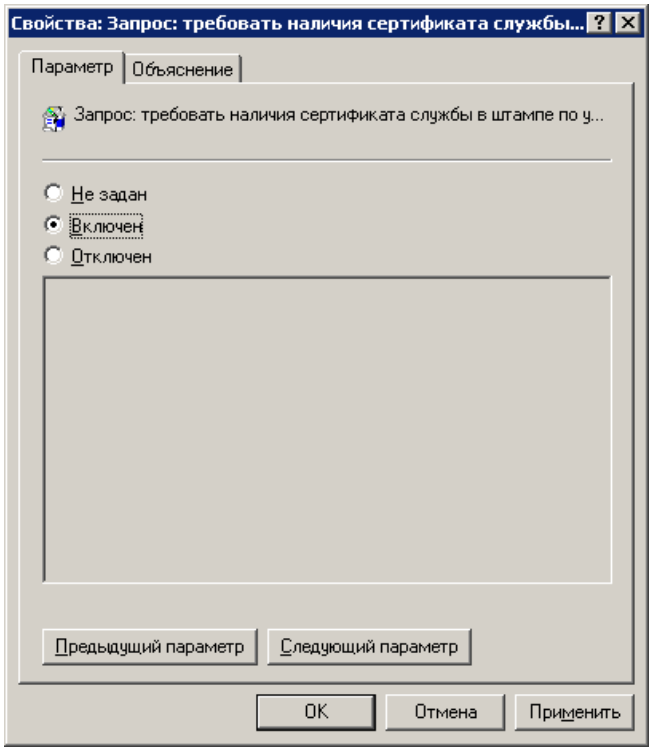

Рисунок 120 – Запрос

8. Закрыть консоль настройки групповых политик.

7.13 Приложение 13. Инструкция по установке сертификатов цепочек доверия

Для установки сертификатов цепочек доверия, полученных от УЦ, необходимо проверить содержимое сертификатов на соответствие информации из документов, полученных вместе с сертификатами, и выполнить следующие действия:

1. В контекстном меню файла сертификата цепочек доверия выбрать пункт **Установить сертификат**.
2. В открывшемся окне мастера импорта сертификатов нажать кнопку **Далее**:

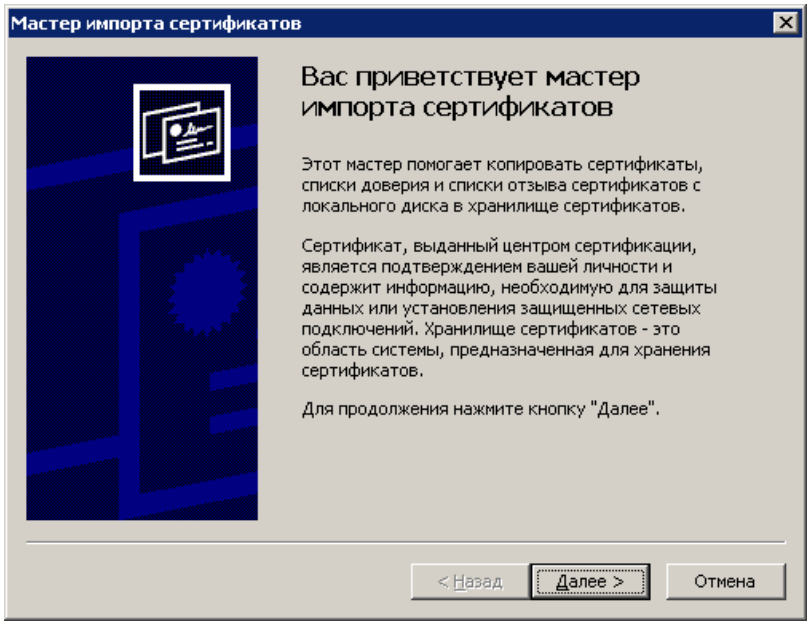

Рисунок 121 – Мастер импорта сертификатов, шаг 1

3. В следующем окне мастера выбрать пункт **Автоматически выбрать хранилище на основе типа сертификата** и нажать кнопку **Далее**:

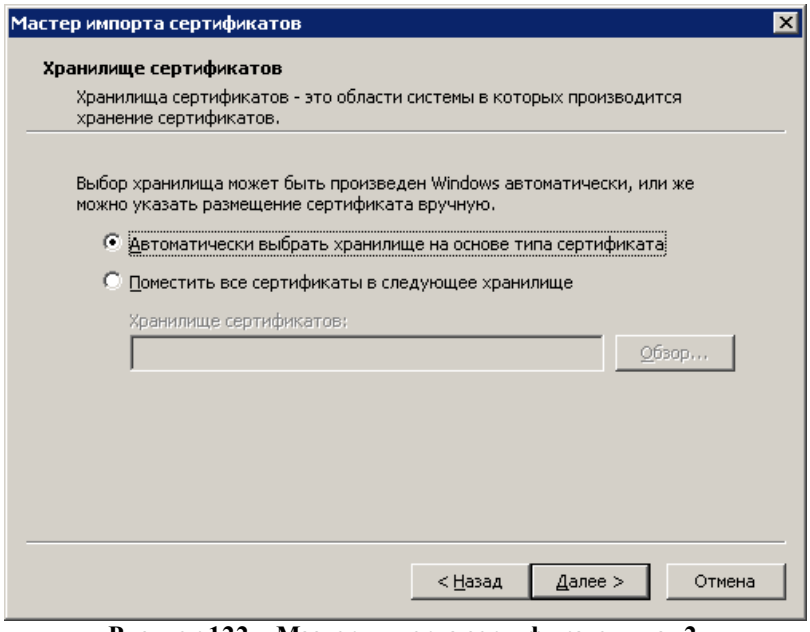

Рисунок 122 – Мастер импорта сертификатов, шаг 2

4. В последнем окне мастера нажать кнопку **Готово**:

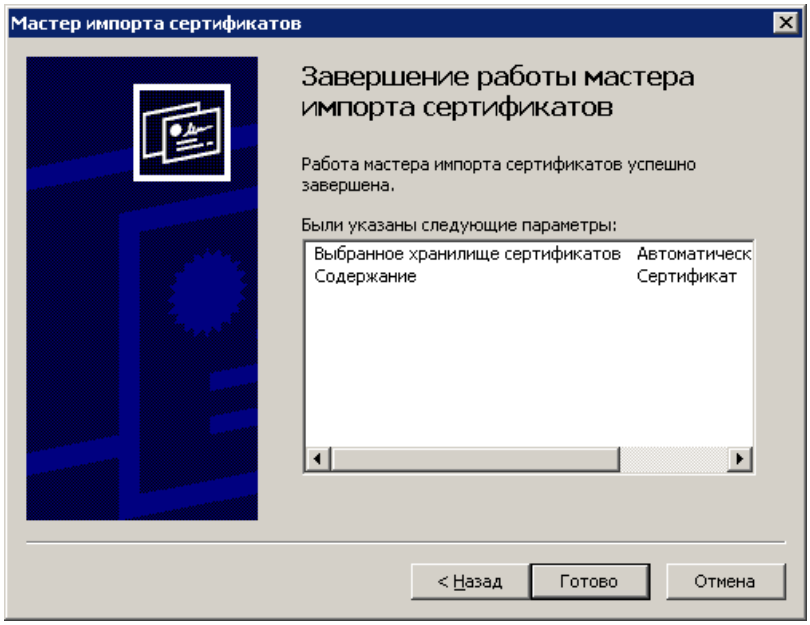

Рисунок 123 – Мастер импорта сертификатов, шаг 3

5. В открывшемся сообщении системы безопасности с запросом на подтверждение установки сертификата нажать кнопку **Yes**:

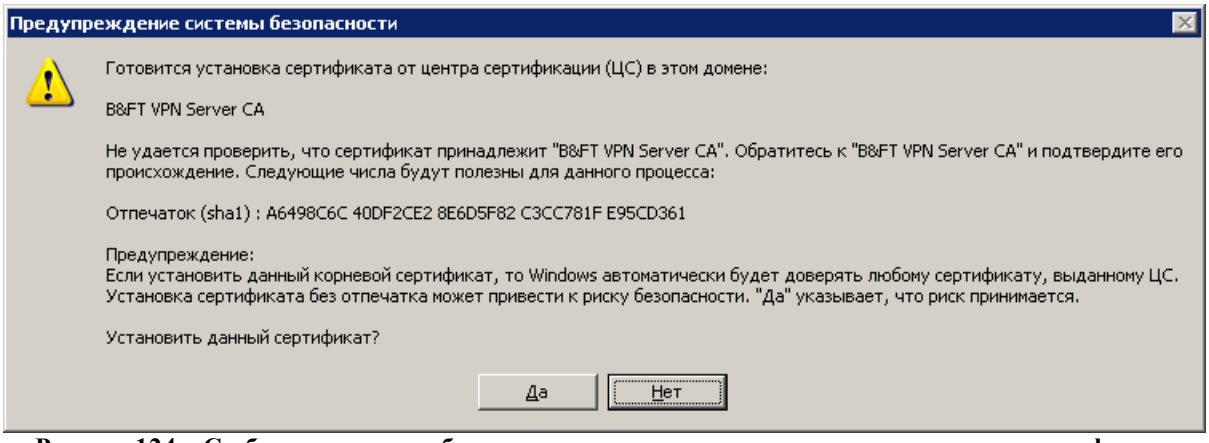

Рисунок 124 – Сообщение системы безопасности с запросом подтверждения установки сертификата

После этого будет выдано сообщение об успешной установке сертификата:

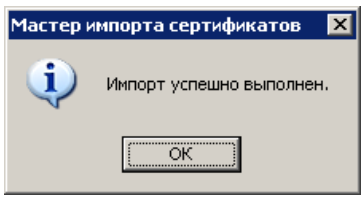

Рисунок 125 – Сообщение об успешной установке сертификата

6. Проверить наличие установленного сертификата в консоли Сертификаты, доступной посредством меню **Пуск→Программы→Крипто-Про→Сертификаты**:

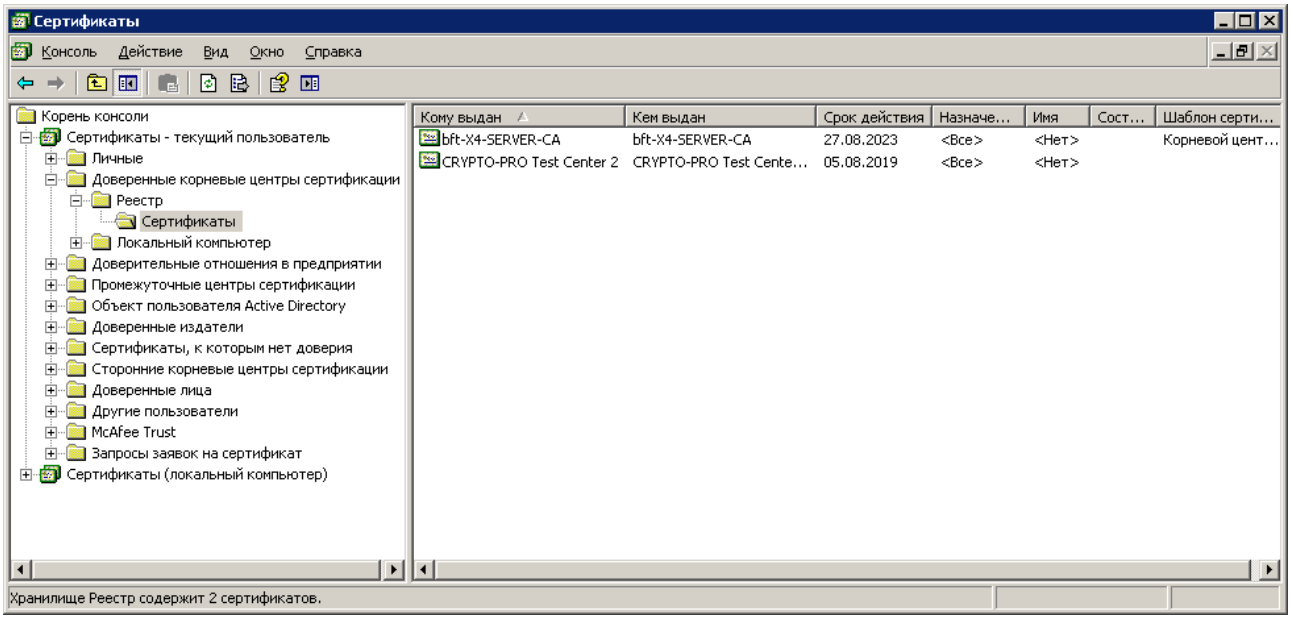

Рисунок 126 – Консоль «Сертификаты»

После этого требуется аналогичным образом установить сертификат TSP, полученный у поставщика услуг TSP, и проверить его установку в разделе **Промежуточные центры сертификации** консоли **Сертификаты**, доступной посредством меню **Пуск→Программы→Крипто-Про→Сертификаты**.

7.14 Приложение 14. Инструкция по настройке взаимодействия ЭП-сервера с сервером приложений

1. В инфраструктуре информационной системы выберите два физических сервера (считается, что **Сервер БД** уже настроен и работает):
   - высокопроизводительный сервер – **Сервер №1**;

Примечание. *Системными параметрами не предусмотрено ограничений по типу используемой ОС для управления основным сервером приложений (**Сервер №1**). При высокой нагрузке на **Сервер №1** рекомендуется использовать ОС семейств Linux/Unix, при малой нагрузке может использоваться ОС семейства Windows.*

   - сервер средней производительности, работающий под управлением ОС семейства Windows, – **Сервер №2**.
2. Убедитесь, что имеющиеся каналы связи обеспечивают обмен данными между **Сервером №1** и **Сервером №2**.
3. Убедитесь, что имеющиеся каналы связи обеспечивают обмен данными между **Сервером №1** и **Сервером БД.**
4. Убедитесь, что имеющиеся каналы связи обеспечивают обмен данными между **Сервером №2** и **Сервером БД**.
5. Установите основной сервер приложений на **Сервер №1**, настройте его взаимодействие с **Сервером БД**.

6. Установите в ОС **Сервера №2** СКЗИ, настройте СКЗИ в соответствии с требованиями к режиму его работы (установка сертификатов ключей подписей пользователей в локальное хранилище не требуется).
7. Установите сервер приложений, предназначенный для проверки ЭП на **Сервер №2**.
8. Настройте в конфигурационном файле основного сервера приложений (на **Сервере №1**) параметры:
   - **azk.sign.hostname** – адрес **Сервера №2** (сервера приложений, предназначенного для проверки ЭП);
   - **azk.sign.port** – порт сервера приложений, предназначенного для проверки ЭП;
   - **azk.sign.user** – имя учетной записи пользователя, которая будет использоваться при проверке ЭП;
   - **azk.sign.pswd** – пароль пользователя, осуществляющего проверку ЭП.

Пример:

```
# --------------------------------
#          ПАРАМЕТРЫ ЭП
# --------------------------------
# Адрес сервера, который осуществляет проверку ЭП. Если не указано, то
# сервером выступает текущий сервер
azk.sign.hostname=172.33.1.21
# Порт сервера, который осуществляет проверку ЭП
azk.sign.port=2002
# Пользователь, под которым осуществляется проверка ЭП
azk.sign.user=es_user
# Пароль пользователя указанного в параметре azk.sign.user
azk.sign.pswd=es_password
```

9. Запустите основной сервер приложений (на **Сервере №1**), проверьте корректность его работы (проверка наличия связи с сервером, предназначенным для проверки ЭП в момент старта основного сервера, **не производится**).
10. Запустите сервер приложений, предназначенный для проверки ЭП (на **Сервере №2**).
11. Сконфигурируйте клиентские приложения для работы с основным сервером приложений.
12. Проверьте работу механизма удаленной проверки ЭП:
    - запустите клиентское приложение;
    - осуществите вход в систему;
    - выберите любой документ, ранее подписанный ЭП (или подпишите документ);
    - откройте этот документ для просмотра/редактирования;
    - откройте список подписей документа (кнопка **ЭП документа**);
    - выберите одну из подписей документа и вызовите контекстное меню, предназначенное для работы с подписью;
    - выберите пункт меню **Проверить локально** (начнется процесс проверки подписи: сначала на сервере, а затем локально);
    - дождитесь диалогового окна с текстом сообщения **Подпись верна**;

- убедитесь, что в log-файле сервера приложений, предназначенного для проверки ЭП, появился запрос на запуск процессора **DOCSIGN** и XML-задание:

```
<SIGN.DOCSIGN action=«verify_signature»>
```

13. Определите сервер, на котором будет производиться добавление штампов времени и цепочек отзыва сертификатов при использовании УЭП.

Внимание! *Данный пункт требуется выполнять, если включен системный параметр* ***Добавлять штамп времени и цепочки отзыва сертификатов на сервере*** *(пункт меню* ***Сервис→Системные параметры****, группа параметров* ***ЭП****). В этом случае наложение УЭП осуществляется следующим образом: формирование простой ЭП производится на клиенте, а добавление штампов времени и цепочек отзыва сертификатов на сервере.*

Добавление штампов времени и цепочек отзыва сертификатов может производиться на **Сервере №2** или на отдельно выделенном для этого сервере – **Сервере №3**.

Для добавления штампов времени и цепочек отзыва сертификатов на **Сервере №3** настройте в конфигурационном файле основного сервера приложений (на **Сервере №1**) параметры:

- **azk.sign.enhance.hostname** – адрес **Сервера №3** (сервера приложений, предназначенного для расширения ЭП до УЭП);
- **azk.sign.enhance.port** – порт сервера приложений, предназначенного для расширения ЭП до УЭП;
- **azk.sign.user** – имя учетной записи пользователя, которая будет использоваться при расширении ЭП (аналогично имени учетной записи, используемой при проверке ЭП);
- **azk.sign.pswd** – пароль пользователя, осуществляющего расширение ЭП (аналогичен паролю пользователя, осуществляющего проверку ЭП).

Пример:

```
# Адрес и порт сервера, который осуществляет "расширение" подписи – добавление
# штампов времени и подтверждение достоверности сертификатов.
# Используются пользователь и пароль, указанные в параметрах azk.sign.user и
# azk.sign.pswd
# Если параметры azk.sign.enhance.hostname и azk.sign.enhance.port не указаны, то
# расширение подписи осуществляется на сервере указанном в параметрах
azk.sign.hostname и azk.sign.port
azk.sign.enhance.hostname=172.33.1.22
azk.sign.enhance.port=2003
```

Для добавления штампов времени и цепочек отзыва сертификатов на **Сервере №2** закомментируйте в конфигурационном файле основного сервера приложений (на **Сервере №1**) указанные выше параметры. Если параметры **azk.sign.enhance.hostname** и **azk.sign.enhance.port** закомментированы/не указаны, расширение подписи осуществляется на сервере, указанном в параметрах **azk.sign.hostname** и **azk.sign.port**, т.е. на **Сервере №2**.

***Примечание**. Также в конфигурационных файлах серверов приложений могут быть настроены:*

*– количество запускаемых параллельно процессов сохранения подписей (на основном сервере приложений) – параметр **azk.sign.task.parallel.count**;*

*– количество запускаемых параллельно процессов проверки подписи (на проверяющем сервере приложений) – параметр **azk.sign.verify.threads.count**;*

*– количество запускаемых параллельно процессов расширения подписи (на сервере приложений, производящем расширение подписи) – параметр **azk.sign.enhance.threads.count**.*

7.15 Приложение 15. Получение сертификата ключа подписи в УЦ

Перед получением ключей нужно загрузить сертификат Удостоверяющего центра.

1. В окне «Тестовый Удостоверяющий Центр ООО "КРИПТО-ПРО"» щелкнуть по ссылке *Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов*.

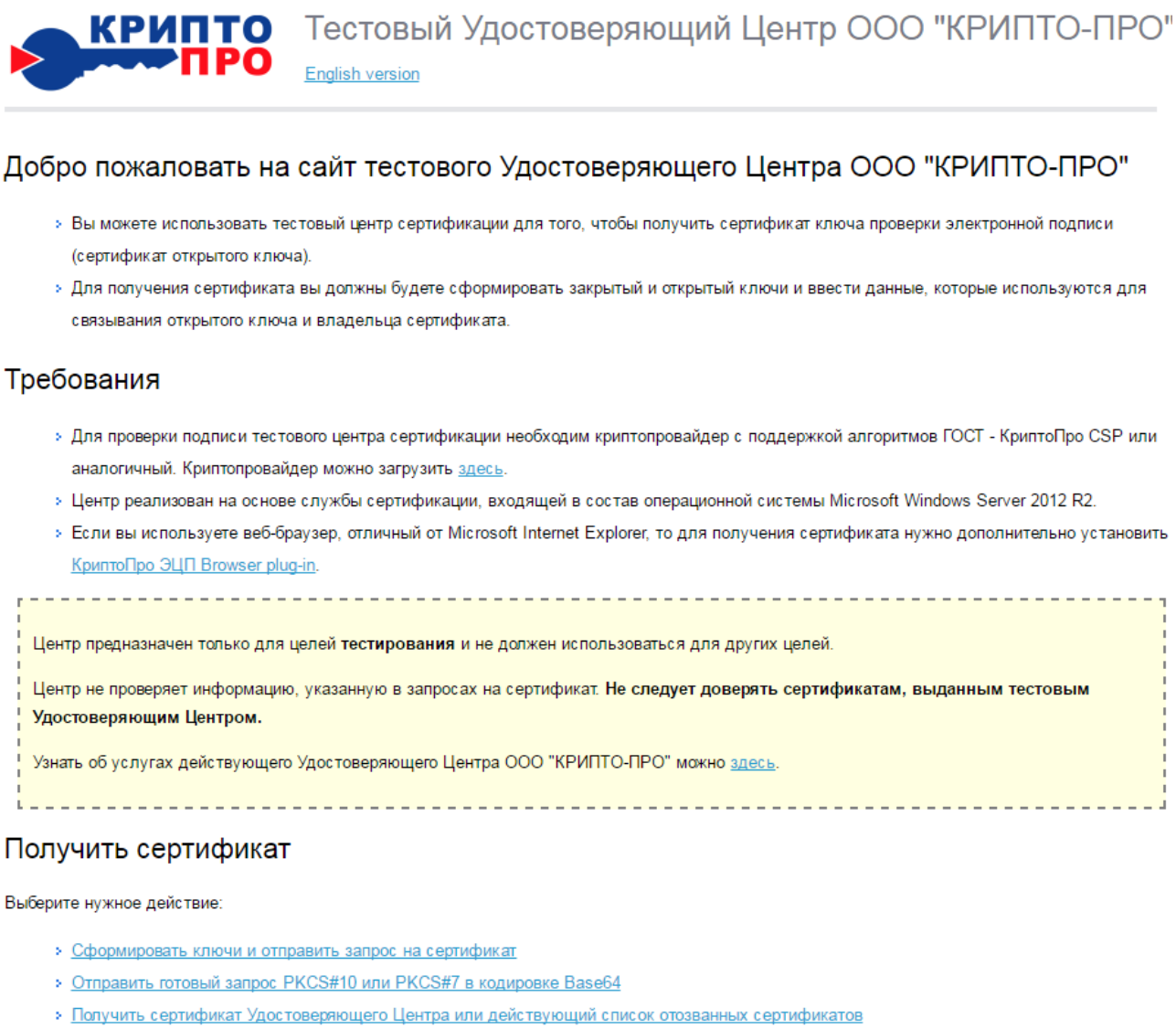

Рисунок 127 – Тестовый Удостоверяющий Центр ООО "КРИПТО-ПРО"

2. В открывшемся окне выбрать **метод шифрования** *Base 64* и щелкнуть по ссылке *Загрузка цепочки сертификатов ЦС*:

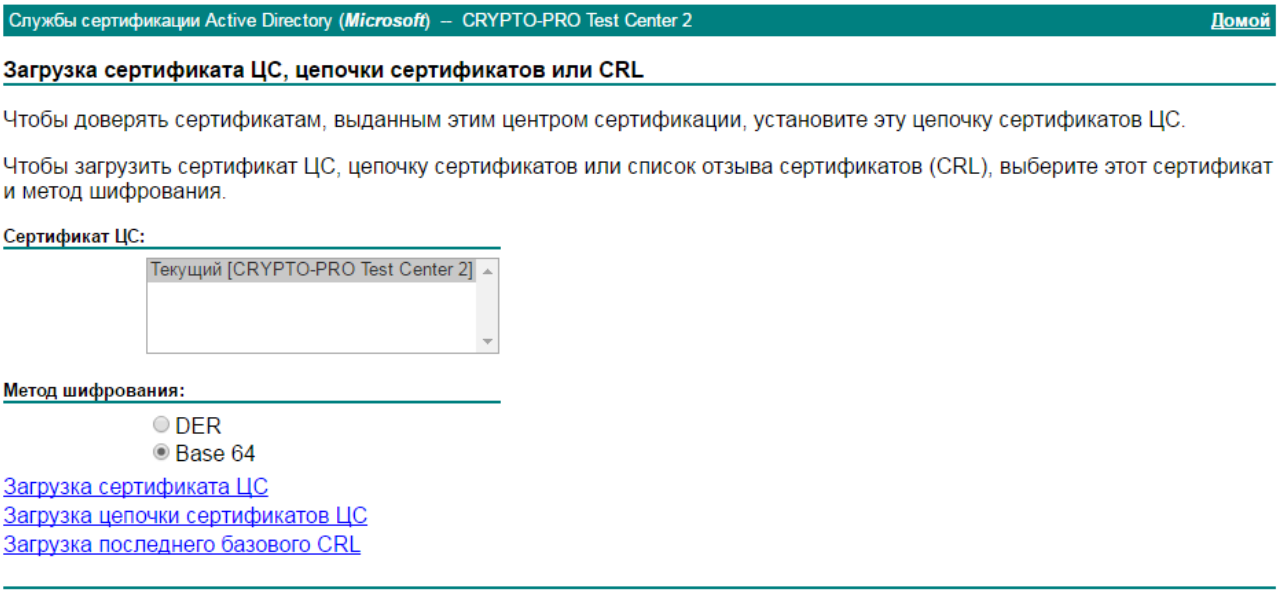

Рисунок 128 –Форма загрузки сертификата ЦС

После нажатия на ссылку осуществляется загрузка файла **certnew.p7b**.

3. Скачанный сертификат необходимо установить. Для этого необходимо выделить файл, правой кнопкой мыши вызвать контекстное меню и выбрать **Установить сертификат**. С помощью **Мастера импорта сертификатов** установить корневой сертификат.

4. Для получения ключа подписи окне «Тестовый Удостоверяющий Центр ООО "КРИПТО-ПРО"» щелкнуть по ссылке *Сформировать ключи и отправить запрос на сертификат*.

***Примечание**. Для корректного формирования формы получения ключа рекомендуется использовать браузер Intetnet Explorer.*

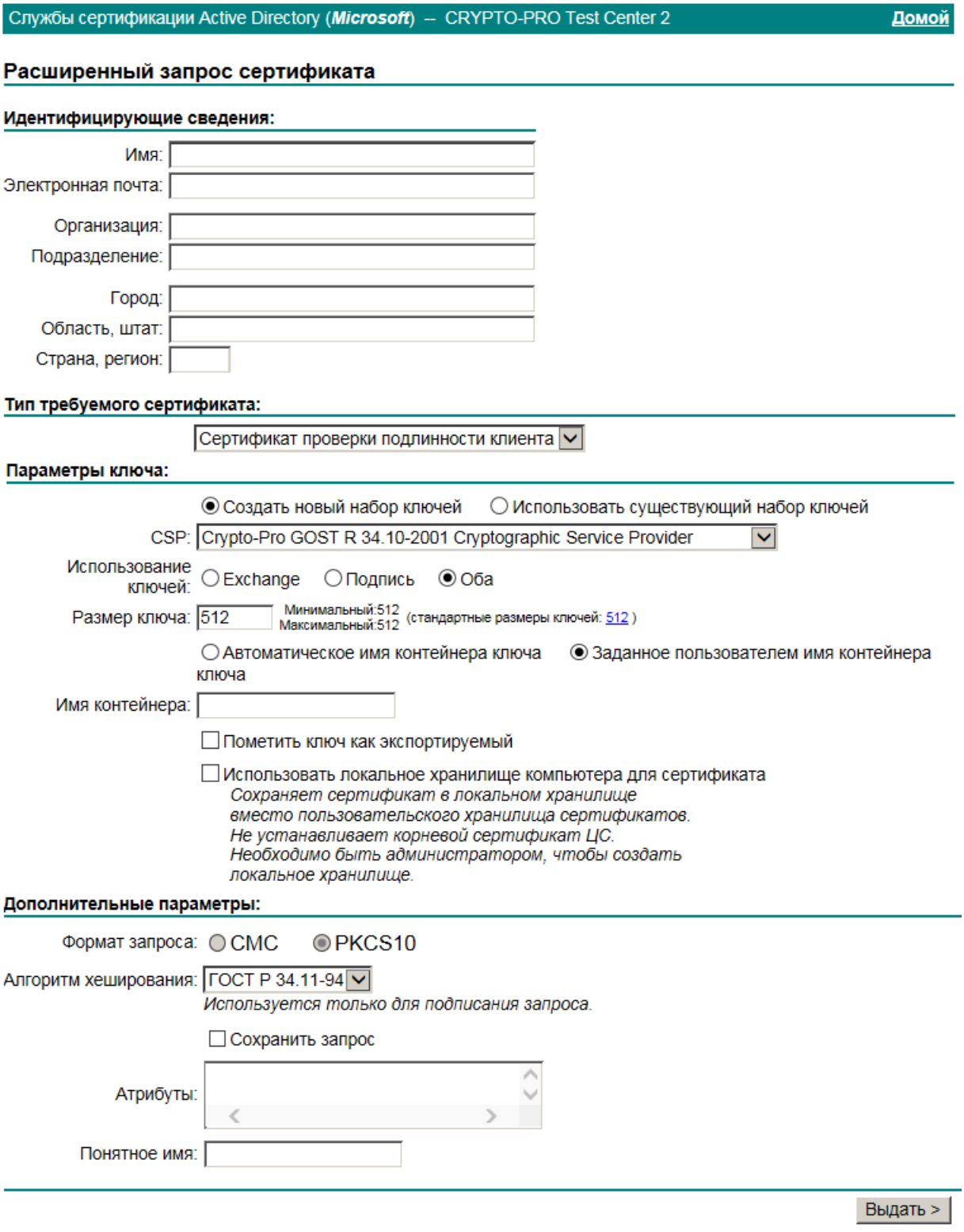

Рисунок 129 – Получение сертификата ключа подписи в УЦ, шаг 1

5. В открывшейся форме указать необходимую информацию. В качестве криптобиблиотеки (поле **CSP**) указать **Crypto-Pro Cryptographic Service Provider**.

***Примечание**. Имя контейнера и адрес электронной почты должны совпадать.*

6. Нажать кнопку **Выдать**.

7. В открывшемся окне указать ключевой носитель (если в настройках **КриптоПро** не установлен признак **Всегда использовать значение по умолчанию**)

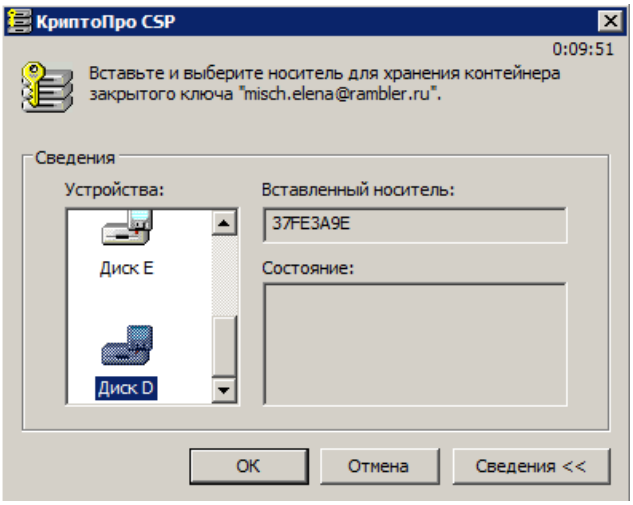

Рисунок 130 – Получение сертификата ключа подписи в УЦ, шаг 2

8. Нажать кнопку **ОК**, после чего должен отработать биологический датчик случайных чисел:

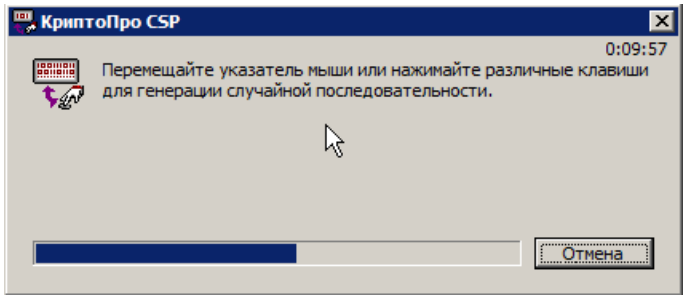

Рисунок 131 – Получение сертификата ключа подписи в УЦ, шаг 3

9. Далее нужно задать пароль для контейнера (если при подписи документа нужно указывать пароль):

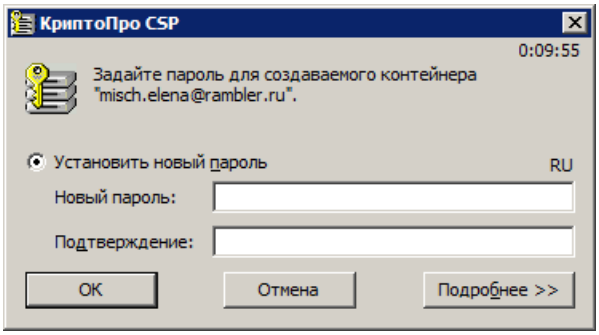

Рисунок 132 – Получение сертификата ключа подписи в УЦ, шаг 4

10. В открывшемся окне выполнить действие **Установить этот сертификат**:

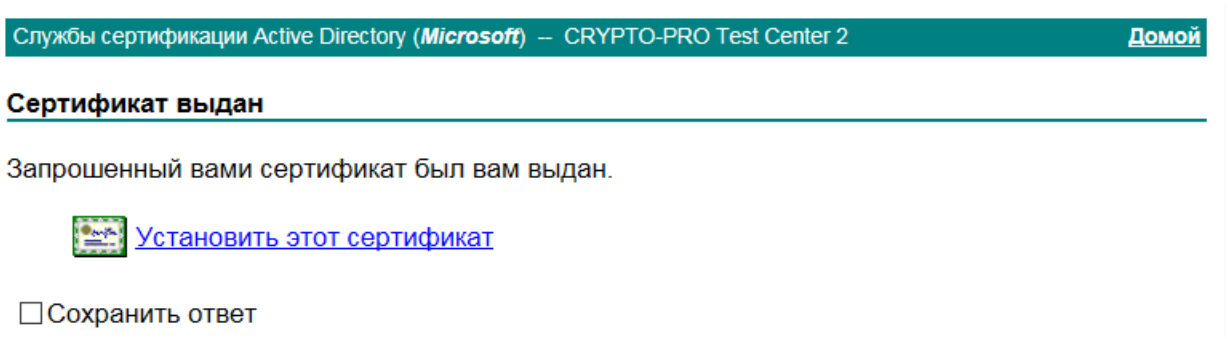

Рисунок 133 – Получение сертификата ключа подписи в УЦ, шаг 5

11. В открывшейся форме следует задать пароль от контейнера и нажать кнопку **ОК**.

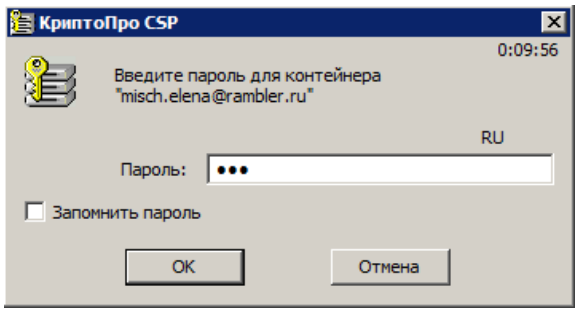

Рисунок 134 – Получение сертификата ключа подписи в УЦ, шаг 6

12. После этого будет выдано сообщение о завершении установки сертификата:

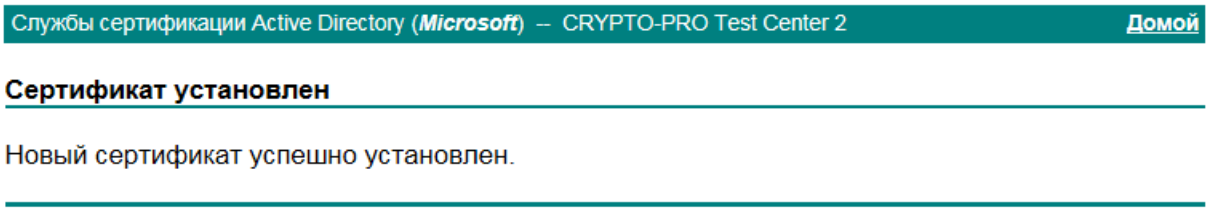

Рисунок 135 – Получение сертификата ключа подписи в УЦ, шаг 7

7.16 Приложение 16. Инструкция по экспорту сертификата ключа подписи

Для экспорта сертификата ключа подписи необходимо выполнить следующие действия:

1. Открыть **Панель управления** (**Пуск→Настройка→Панель управления**).
2. Открыть двойным щелчком мыши значок **Свойства браузера**.
3. На закладке **Содержание** нажать кнопку **Сертификаты**.
4. В открывшемся окне **Сертификаты**, на закладке **Личные**, выбрать сертификат для экспорта и нажать кнопку **Экспорт**:

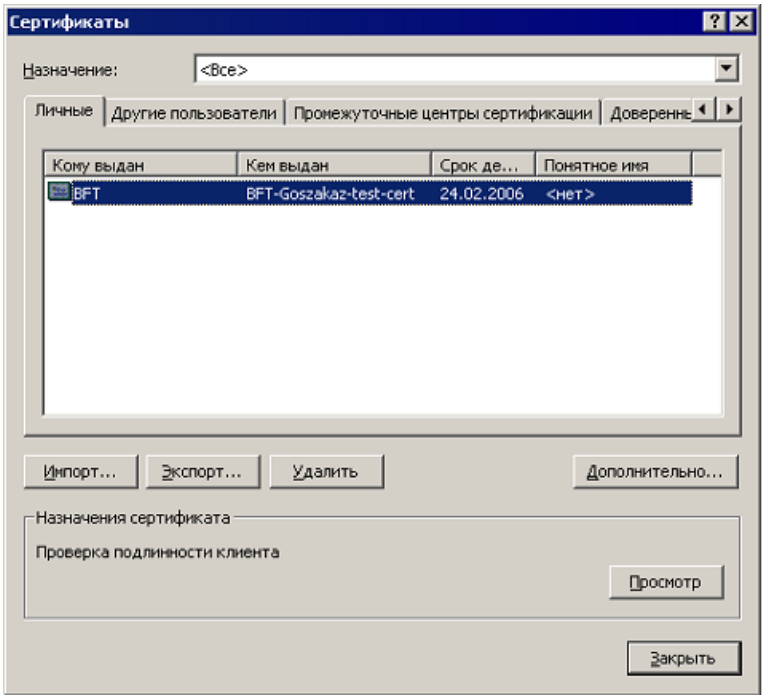

Рисунок 136 – Окно сертификатов

5. В открывшемся окне мастера экспорта сертификатов нажать кнопку **Далее**:

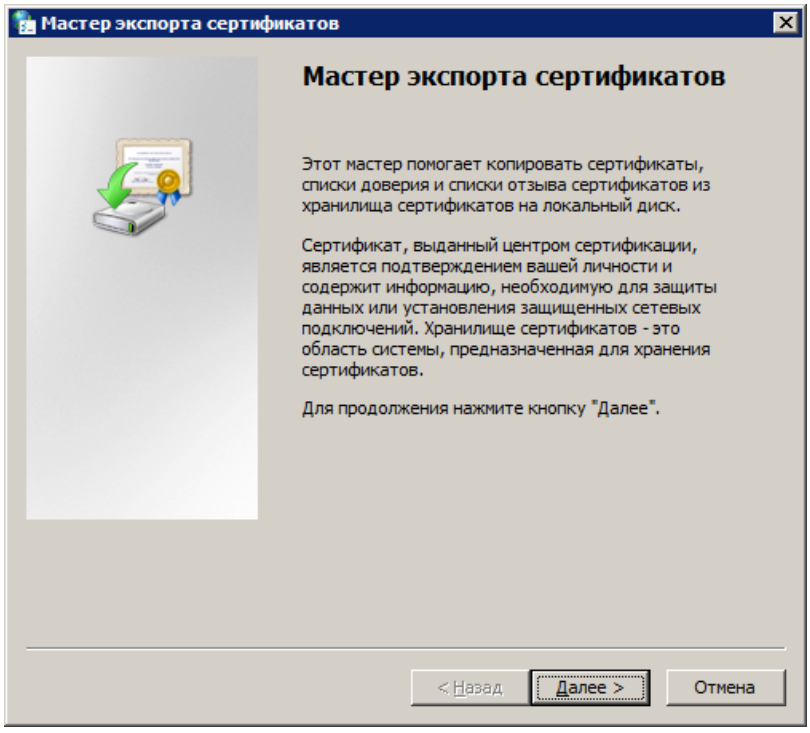

Рисунок 137 – Мастер экспорта сертификатов, шаг 1

6. Выбрать опцию **Нет, не экспортировать закрытый ключ** и нажать кнопку **Далее**:

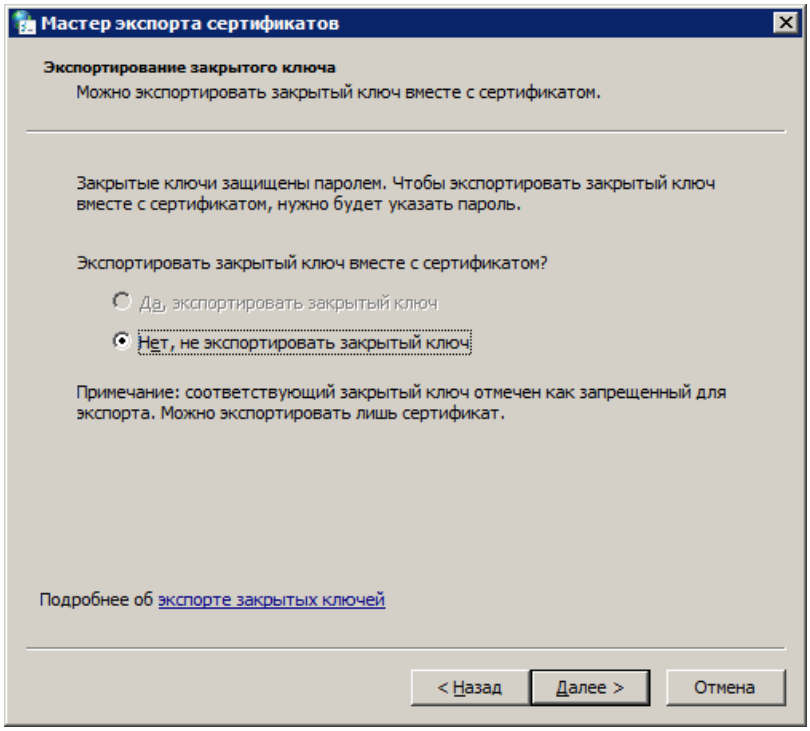

Рисунок 138 – Мастер экспорта сертификатов, шаг 2

7. Выбрать опцию **Файлы в Base64-кодировке X.509 (.CER)** и нажать кнопку **Далее**:

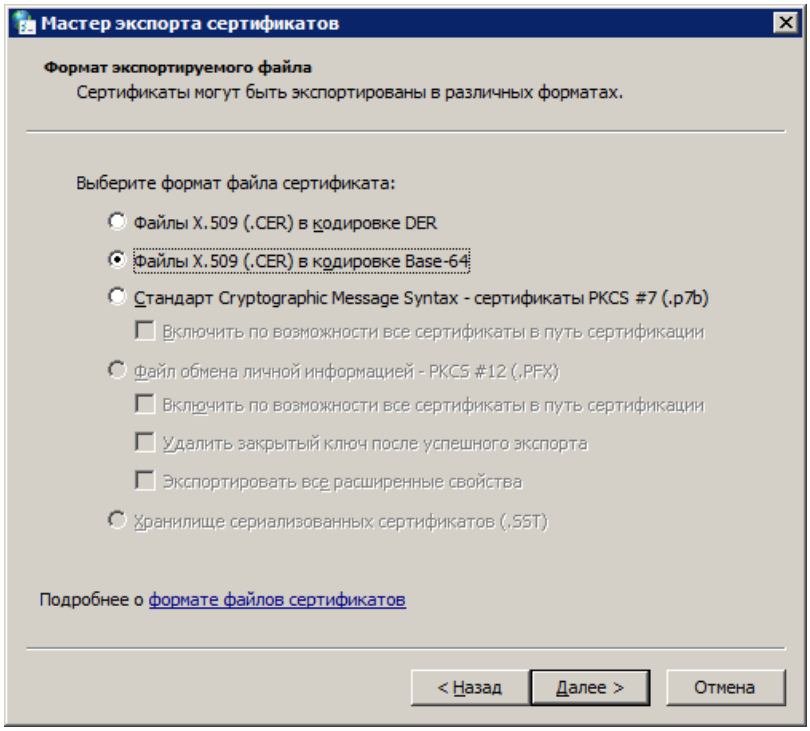

Рисунок 139 – Мастер экспорта сертификатов, шаг 3

8. Указать путь к файлу экспорта сертификата и нажать кнопку **Далее**:

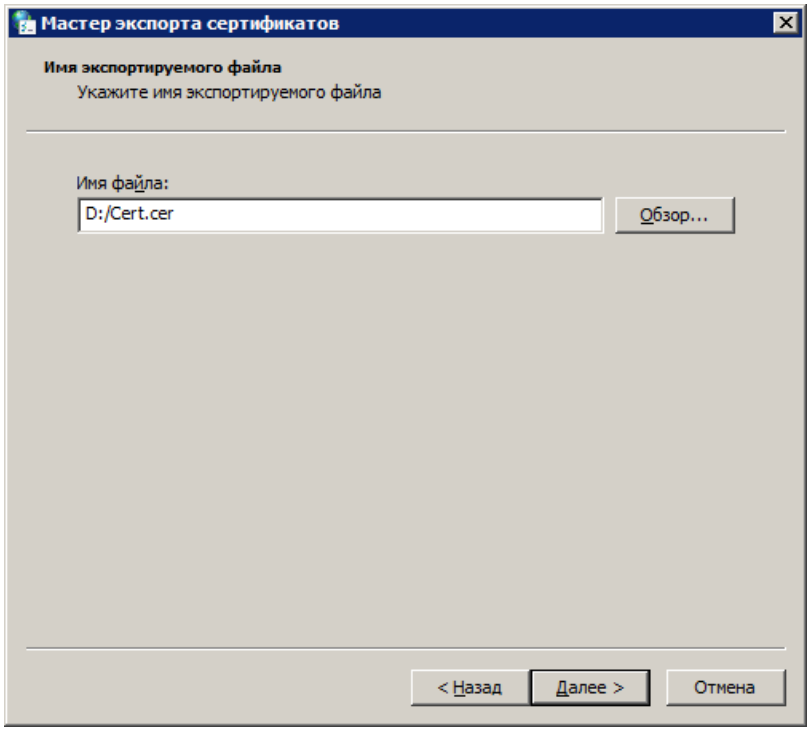

Рисунок 140 – Мастер экспорта сертификатов, шаг 4

9. В последнем окне мастера экспорта сертификата нажать кнопку **Готово**:

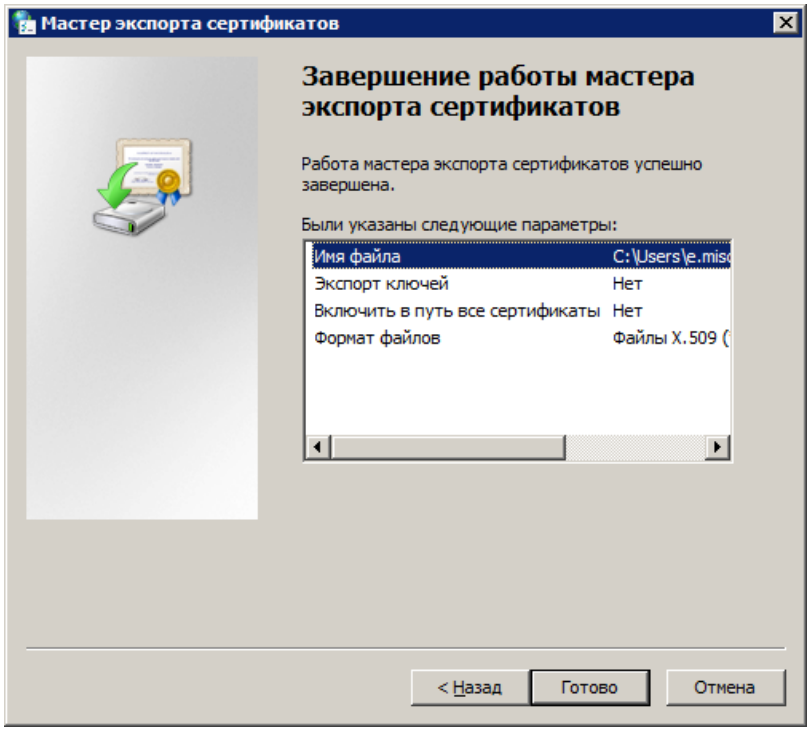

Рисунок 141 – Мастер экспорта сертификатов, шаг 5

Будет выдано сообщение об успешном выполнении экспорта сертификата:

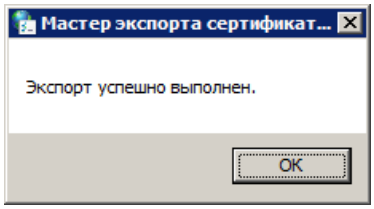

Рисунок 142 – Сообщение о выполнении экспорта сертификата

7.17 Приложение 17. Инструкция по установке сертификата ключа подписи

Для установки личного сертификата ключа подписи необходимо выполнить следующие действия:

1. Открыть свойства **КриптоПро CSP** двойным щелчком по соответствующему значку в **Панели управления** (**Пуск→Настройка→Панель управления**[116]).
2. Перейти на закладку **Сервис** и нажать кнопку **Установить личный сертификат**:

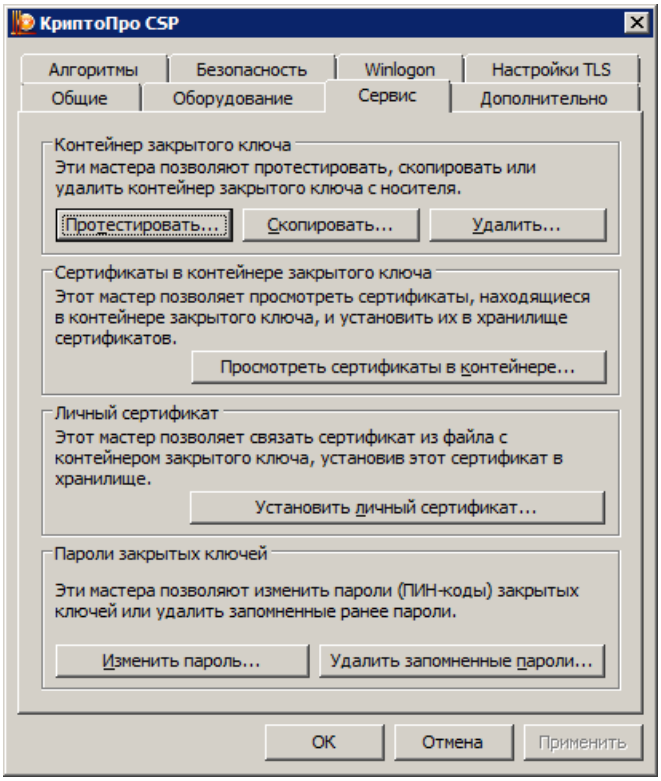

Рисунок 143 – Форма свойств CryptoPro CSP, закладка «Сервис»

3. В открывшемся окне указать с помощью кнопки **Обзор** месторасположение сертификата ключа подписи и нажать кнопку **Далее**:

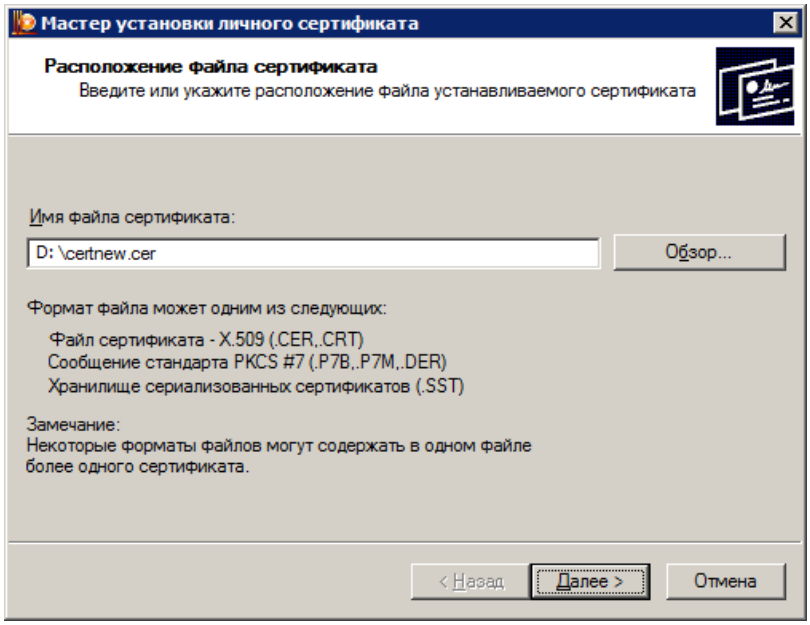

Рисунок 144 – Мастер установки личного сертификата, шаг 2

4. В новом окне мастера, содержащем информацию из устанавливаемого сертификата, нажать кнопку **Далее**:

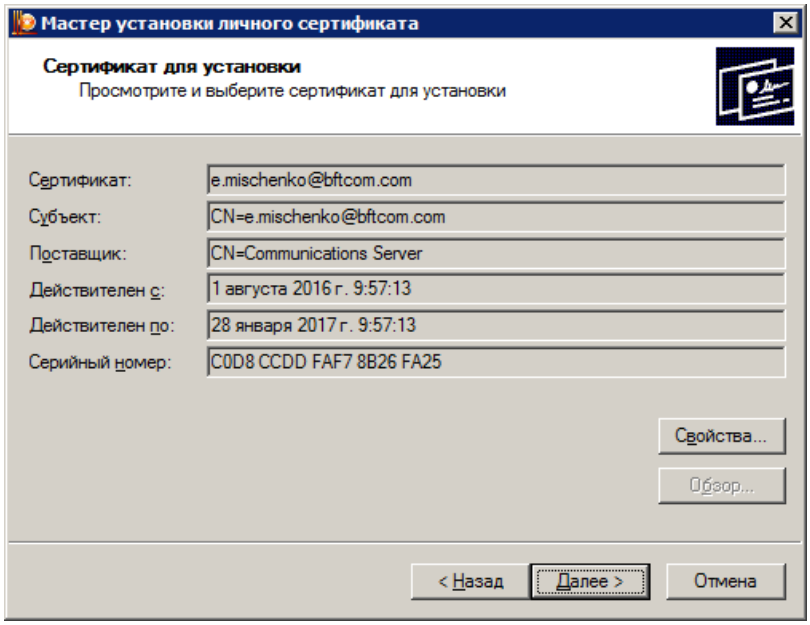

Рисунок 145 – Мастер установки личного сертификата, шаг 3

5. В следующем окне нажать кнопку **Обзор** для указания контейнера ключа.

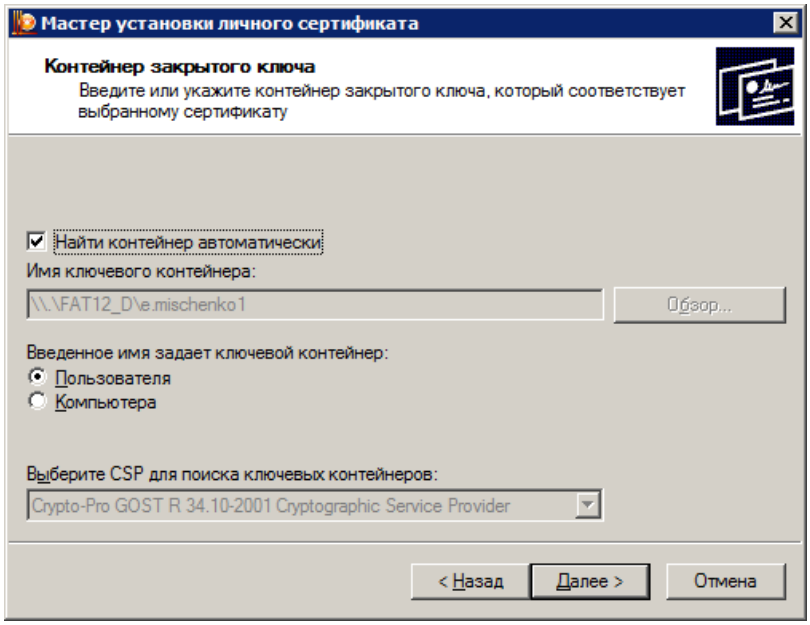

Рисунок 146 – Мастер установки личного сертификата, шаг 4

6. В открывшемся окне выбрать из списка нужный контейнер и нажать кнопку **ОК**:

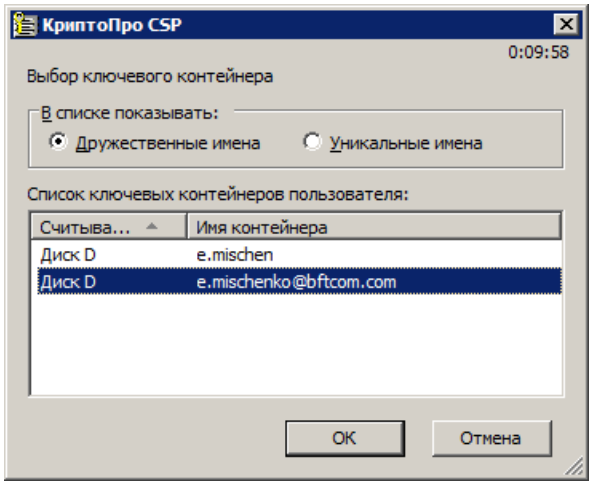

Рисунок 147 – Окно выбора контейнера

7. В окне мастера установки сертификата нажать кнопку **Далее**:

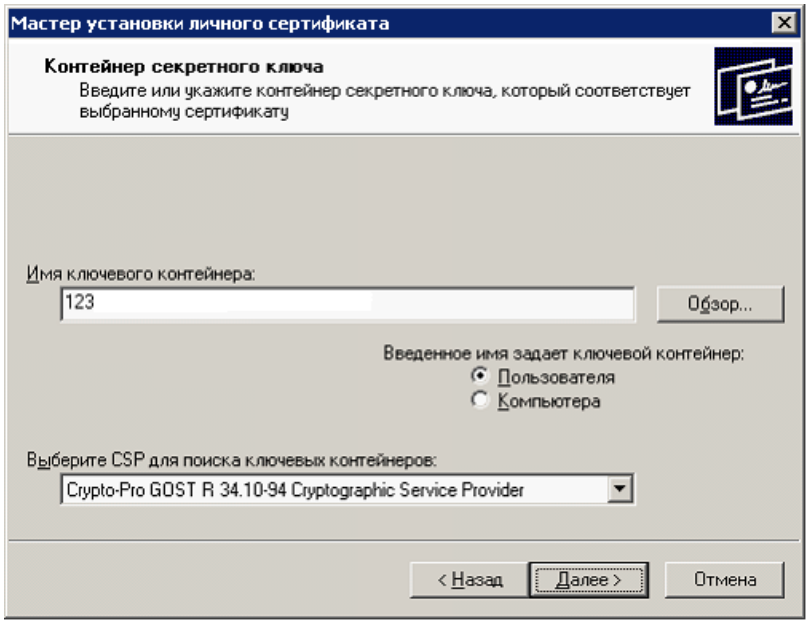

Рисунок 148 – Мастер установки личного сертификата, шаг 6

8. Указать пароль для доступа к ключевому контейнеру и нажать кнопку **OK**.

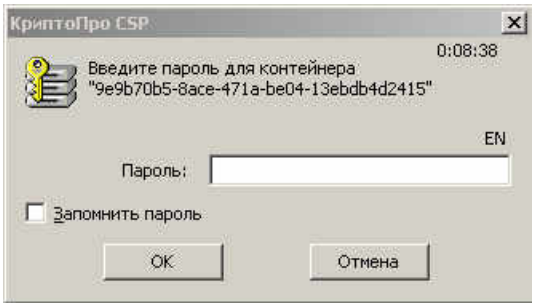

Рисунок 149 – Окно ввода пароля для контейнера

9. В новом окне мастера нажать кнопку **Обзор** для указания хранилища, в которое будет установлен сертификат.

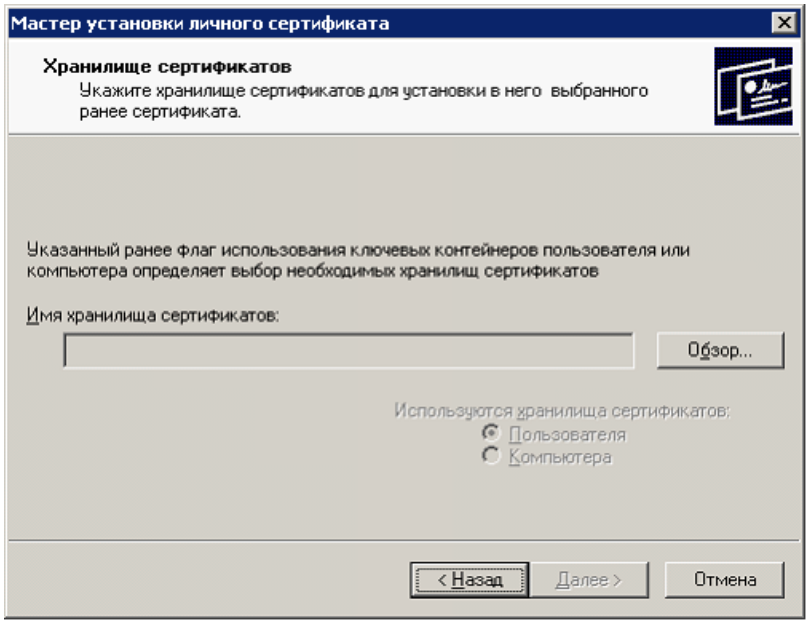

Рисунок 150 – Мастер установки личного сертификата, шаг 8

10. В открывшейся форме выбрать необходимое хранилище (**Личные**) и нажать кнопку **ОК**:

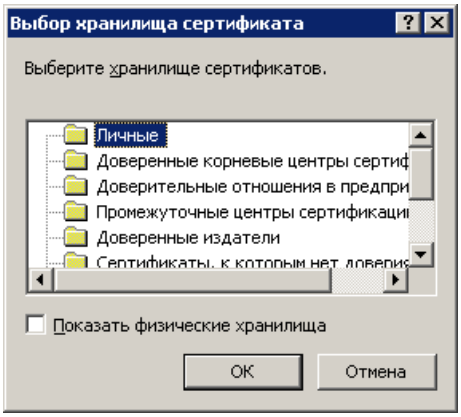

Рисунок 151 – Форма выбора хранилища

11. В окне мастера установки сертификата нажать кнопку **Далее**:

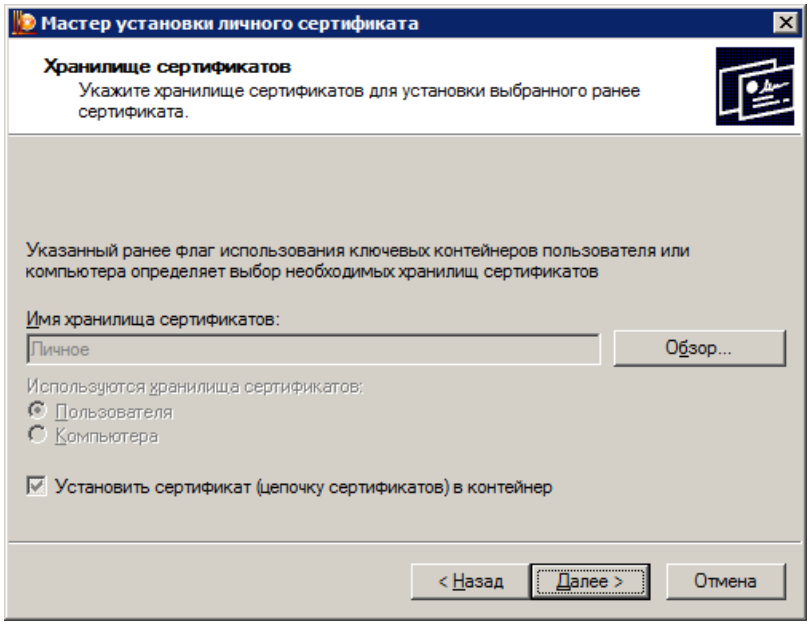

Рисунок 152 – Мастер установки личного сертификата, шаг 10

12. В итоговом окне мастера установки сертификата нажать кнопку **Готово**:

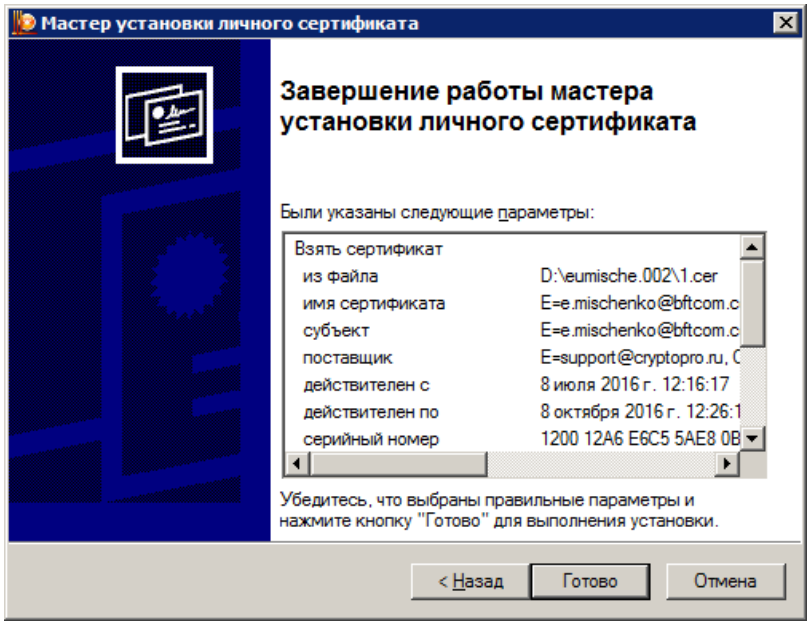

Рисунок 153 – Мастер установки личного сертификата, шаг 11

13. Проверить наличие установленного сертификата в консоли **Сертификаты**, доступной посредством меню **Пуск→Программы→Крипто-Про→Сертификаты**:

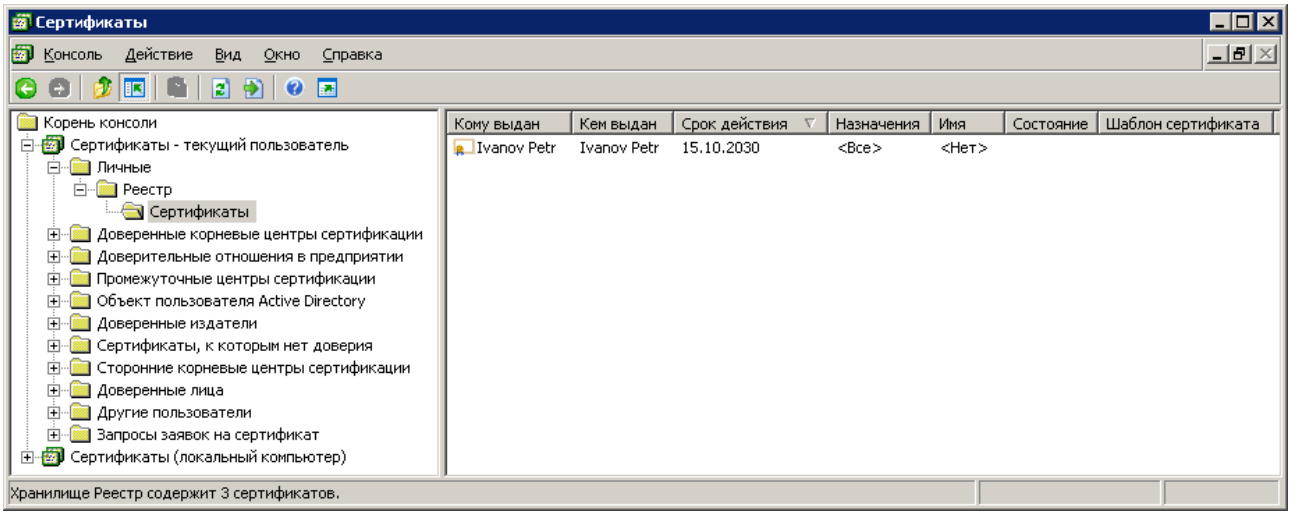

Рисунок 154 – Консоль «Сертификаты», хранилище сертификатов «Личные»

7.18 Приложение 18. Инструкция по резервированию закрытых ключей ЭП

Резервирование закрытых ключей ЭП осуществляется переносом ключей из контейнера в контейнер методами системы «КриптоПро». Для переноса ключа из одного контейнера в другой можно воспользоваться внутренним механизмом системы.

Для переноса ключа из одного контейнера в другой необходимо соблюдение следующих правил:

- При генерации ключа ЭП, если планируется его перенос или копирование, должен быть активен признак **Пометить ключ как экспортируемый**:

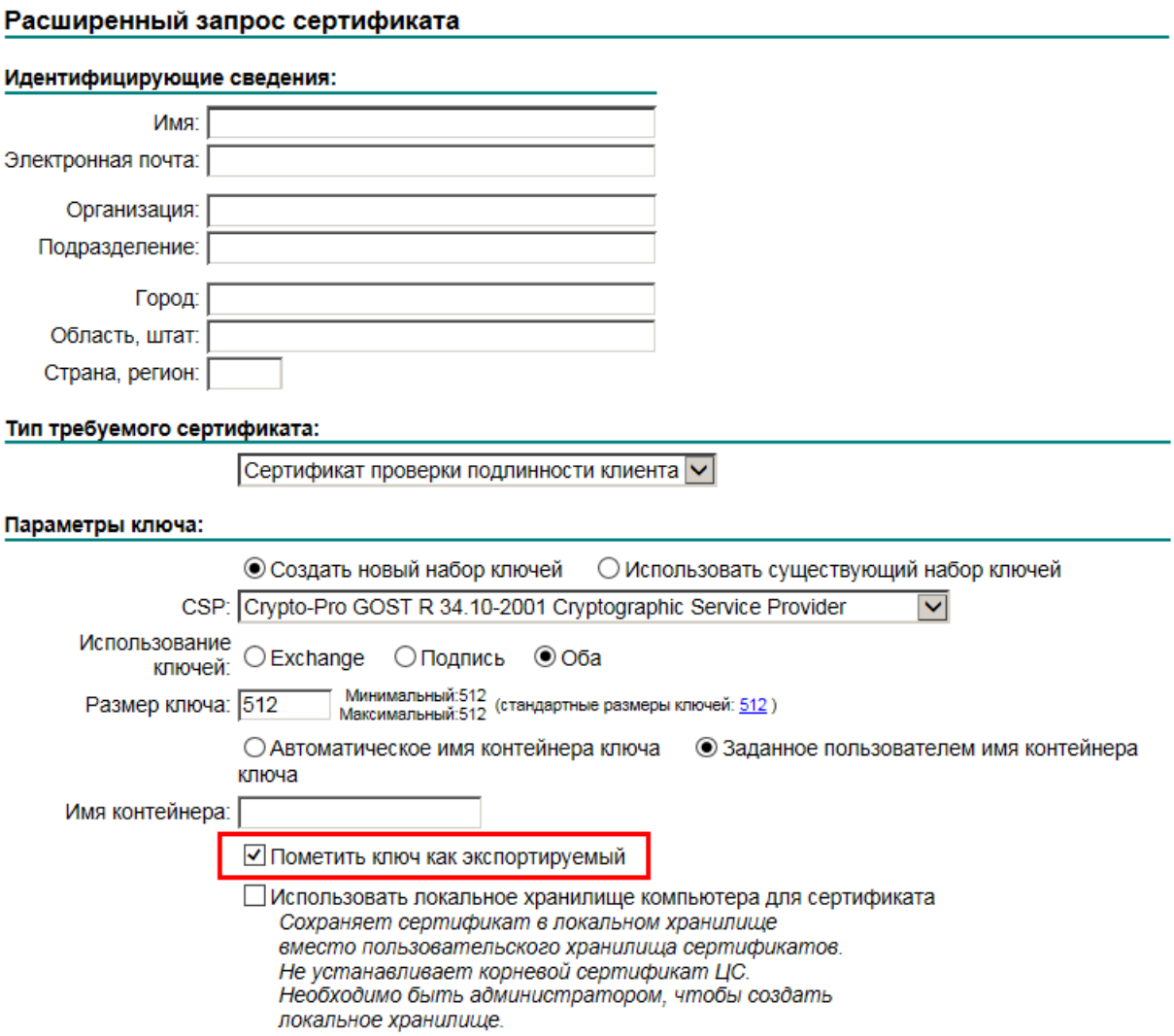

Рисунок 155 – Генерация ключа ЭП

В противном случае при копировании ключа средствами «КриптоПро» появится сообщение об ошибке:

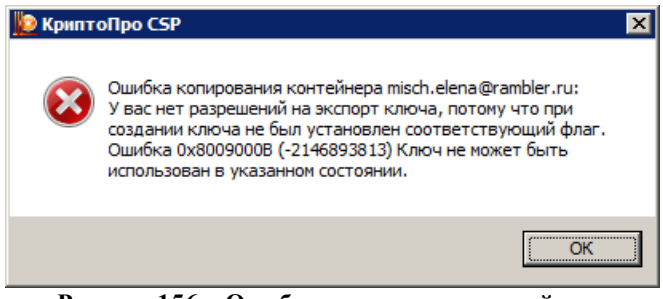

Рисунок 156 – Ошибка копирования контейнера

- Для копирования ключа необходимо иметь 2 ключевых контейнера. В одном из них располагается сам ключ, во второй будет осуществляться перенос.

Для копирования закрытого ключа из одного контейнера в другой требуется выполнить следующие действия:

- Необходимо зайти в пункт меню **Пуск→Панель управления→КриптоПро CSP**.

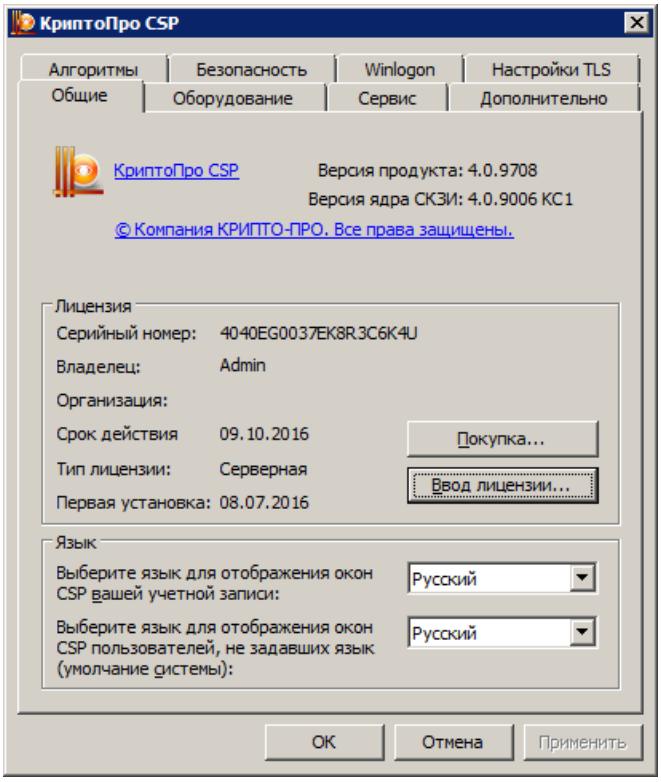

Рисунок 157 – Свойства: КриптоПро CSP

- В открывшемся окне свойств *КриптоПро CSP* перейти на закладку **Сервис** и нажать кнопку **Скопировать …**:

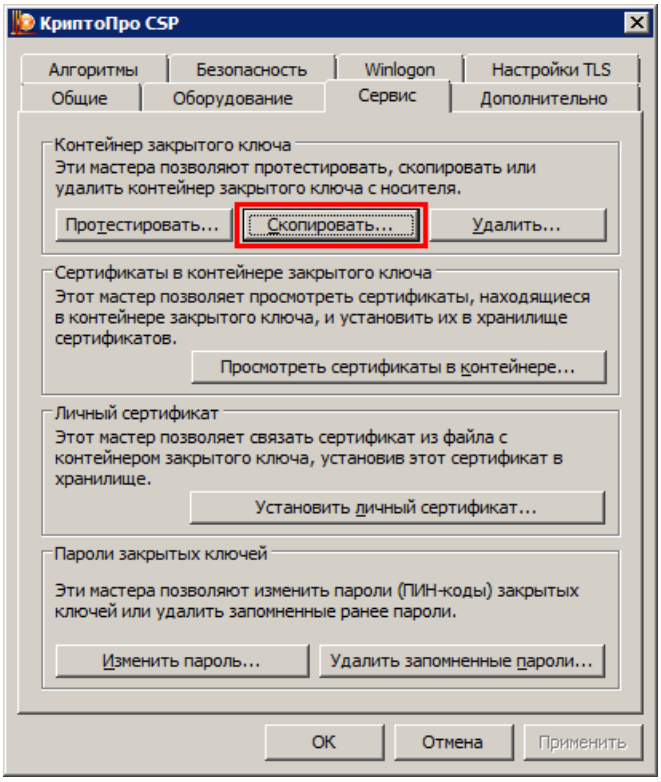

Рисунок 158 – Свойства: КриптоПро CSP, закладка «Сервис»

- В открывшемся окне копирования контейнера закрытого ключа нажать кнопку **Обзор**:

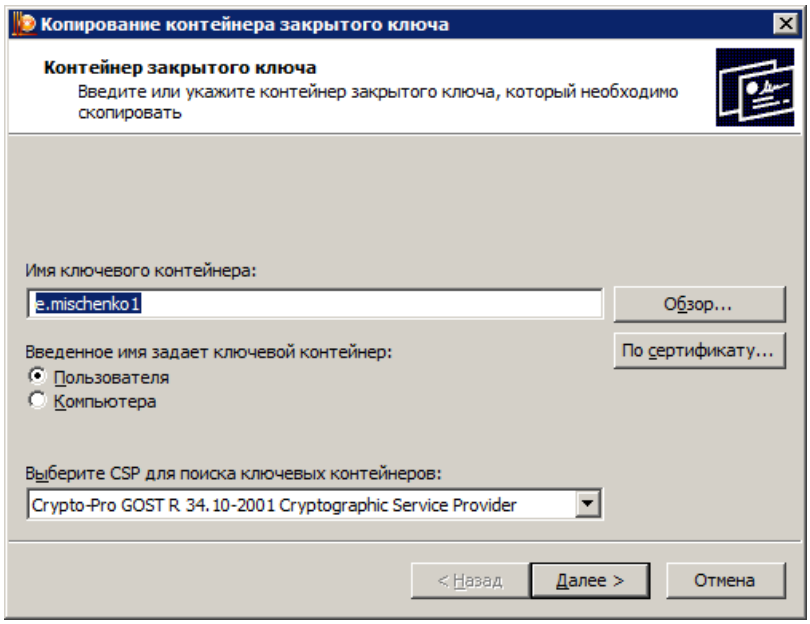

Рисунок 159 – Свойства: КриптоПро CSP, копирование контейнера закрытого ключа

Выбрать ключ, который необходимо скопировать:

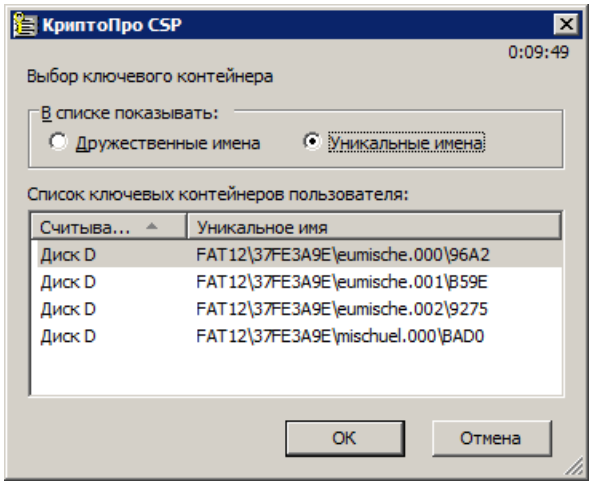

Рисунок 160 – Окно выбора ключевого контейнера

- Нажать кнопку **Далее**. В следующем окне в поле **Имя ключевого контейнера** требуется указать имя для нового контейнера.

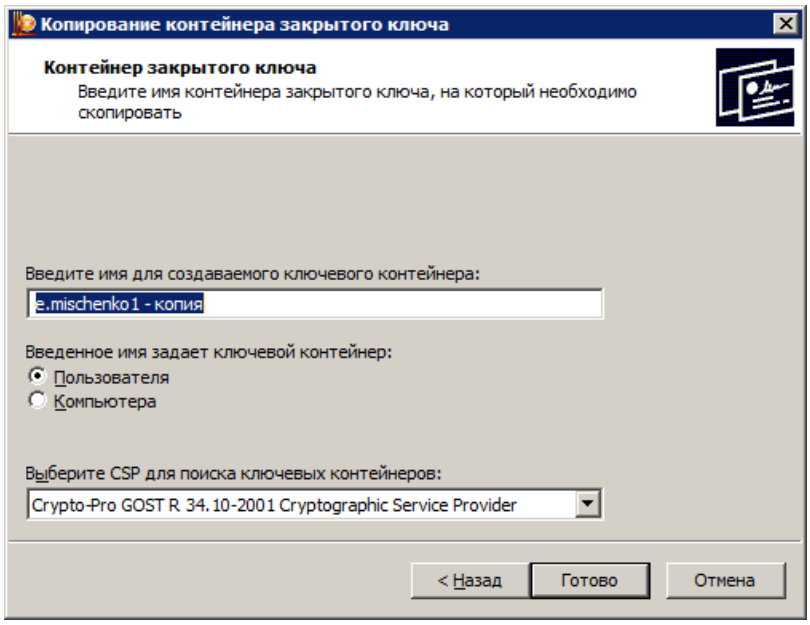

Рисунок 161 – Свойства: КриптоПро CSP, копирование контейнера закрытого ключа

- Нажать кнопку **Готово**.

Для усиления режима безопасности можно ввести пароль, который будет запрашиваться при подписи.

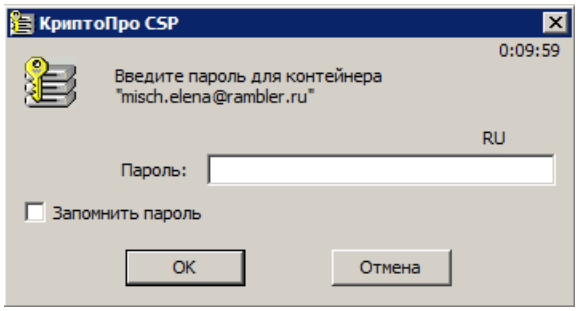

Рисунок 162 – Ввод пароля

Если контейнеров несколько, будет предложено выбрать в какой из них скопировать ключ.

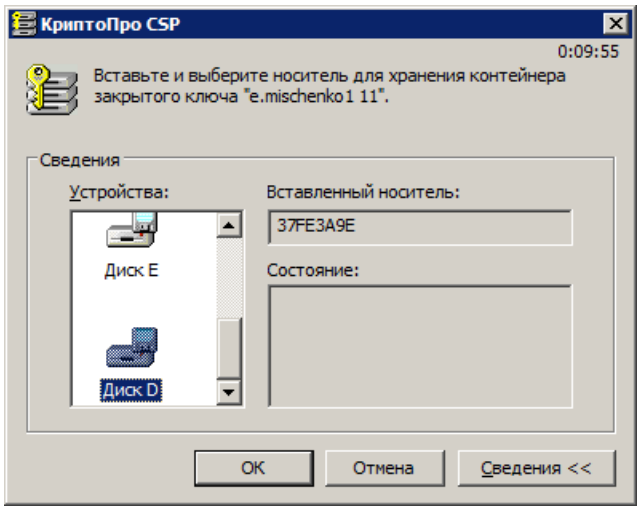

Рисунок 163 – Выбор носителя ключа

Ключ копируется в новый ключевой контейнер (съемный носитель данных и т.д.) и его можно посмотреть.

После выполнения процедуры копирования данный ключ может использоваться как со старого ключевого контейнера (другой съемный носитель данных, реестр и т.д), так и с нового.

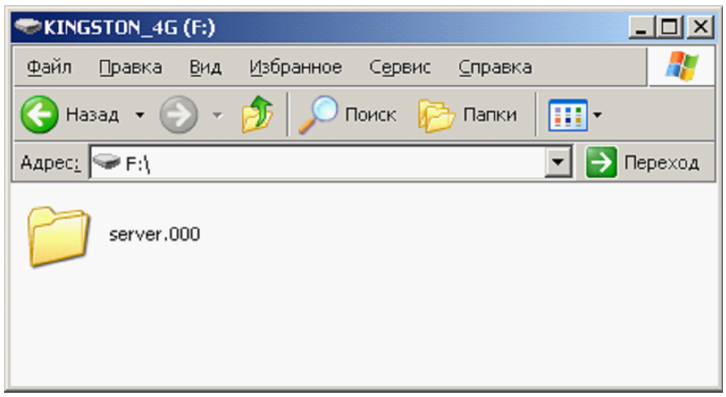

Рисунок 164 – Папка с ключами

В дальнейшем копировать закрытый ключ еще проще. Папка с закрытым ключом может быть перенесена стандартными средствами ОС в другую директорию и использоваться уже там.

***Примечание**. Данный метод касается только версий ключей старше 1.X.*

7.19 Приложение 19. Список диагностических сообщений

Диагностические сообщения отображаются системой в трех местах:

- диалоговое окно сообщения, появляющееся при локальной проверке подписи из списка подписей;
- колонка **Статус** на форме просмотра списка подписей (соответствует полю **ISVALID** таблицы **OBJECTSIGN** в базе данных);
- колонка **Примечание** на форме просмотра списка подписей (соответствует полю **REMARK** таблицы **OBJECTSIGN** в базе данных).

Результаты диагностики ЭП выводятся пользователю в следующем виде:

- Если ЭП верна:
  - на экран выводится диалоговое сообщение **Подпись валидна**;
  - в колонке **Статус данных документа** на форме просмотра списка подписей выводится текст **соответствует**;
  - колонка **Примечание** на форме просмотра списка подписей остается не заполненной.
- Если ЭП не верна:
  - на экран выводится диалоговое сообщение сервера с диагностикой;
  - в колонке **Статус данных документа** на форме просмотра списка подписей выводится текст **не соответствует**;
  - в колонке **Примечание** на форме просмотра списка подписей выводится диалоговое сообщение сервера с диагностикой.

Таблица 5 – Сообщения сервера

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
УЭП с доказательствами подлинности	CHECK_PARAMETERS__ERROR_NO_DATA	Не найдены данные для проверки.	Переданные для проверки данные невозможно проверить (данные имеют нулевую длину).	Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
УЭП с доказательствами подлинности	CHECK_PARAMETERS__ERROR_NO_SIGNATURE	Подпись не найдена.	Переданную для проверки подпись невозможно проверить (подпись имеет нулевую длину).	Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	CHECK_PARAMETERS__ERROR_CHECK_SIGNATURE	Подпись повреждена или имеет неверный формат.	Переданная для проверки подпись повреждена или имеет неверный формат.	Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	CADES__VERIFY_INVALID_REFS_AND_VALUES	Доказательства подлинности отсутствуют или имеют неверный формат.	Отсутствуют или имеют неправильный формат атрибуты со ссылками и значениями доказательств подлинности: 1. Возможна попытка подлога проверяемой ЭП. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	CADES__VERIFY_SIGNER_NOT_FOUND	Не найден сертификат ключа подписи.	1. Возможна попытка подлога проверяемой ЭП. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	CADES__VERIFY_NO_VALID_SIGNATURE_TIMESTAMP	Не найден действительный штамп времени на подпись.	1. Возможна попытка подлога проверяемой ЭП. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново,

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
				предварительно убедившись в работоспособности и доступности сервера штампов времени (TSP). В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	CADES__VERIFY_REFS_AND_VALUES_NO_MATCH	Доказательства подлинности и ссылки на них не соответствуют друг другу.	Значения ссылок на доказательства подлинности и сами доказательства, вложенные в сообщение, не соответствуют друг другу: 1. Возможна попытка подлога проверяемой ЭП. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	CADES__VERIFY_NO_CHAIN	Не удалось построить цепочку доверия для сертификата ключа подписи.	–	–
УЭП с доказательствами подлинности	CADES__VERIFY_END_CERT_REVOCATION	Не удалось проверить статус конечного сертификата ключа подписи.	–	–
УЭП с доказательствами подлинности	CADES__VERIFY_CHAIN_CERT_REVOCATION	Не удалось проверить статус сертификата цепочки доверия.	Ошибка проверки сертификата цепочки на отзыв.	–

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
УЭП с доказательствами подлинности	CADES__VERIFY_BAD_SIGNATURE	Подпись невалидна.	Сообщение содержит неверную подпись.	–
УЭП с доказательствами подлинности	CADES__VERIFY_NO_VALID_CADES_C_TIMESTAMP	Не найден действительный штамп времени на доказательства подлинности.	1. Возможна попытка подлога проверяемой ЭП. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново, предварительно убедившись в работоспособности и доступности сервера штампов времени (TSP). В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	–	Подпись принадлежит не ЭП-роли.	1. Преднамеренные или непреднамеренные искажения в реестре ролей пользователей системы. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести аудит действий пользователей системы в части внесения изменений в реестр ролей пользователей. 1.2. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП с доказательствами подлинности	–	На момент подписания пользователь не обладал ЭП-ролью, которой принадлежит проверяемая подпись.	1. Преднамеренные или непреднамеренные искажения в журнале назначения ролей пользователям системы. 2. Системный сбой при формировании проверяемой ЭП.	1. 1.1. Провести аудит действий пользователей системы в части внесения изменений в журнал назначения ролей пользователям. 1.2. Провести проверку соблюдения внутренних регламентов обеспечения уровня доступа в части предотвращения несанкционированных действий с информационной системой. 2. 2.1. Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП,

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
				обратиться к разработчикам.
УЭП с доказательствами подлинности	–	Текущий текст ЭД отличается от подписанного ранее текста.	Подписанные ЭП данные были изменены.	Способ разрешения данной ситуации определяется регламентом электронного документооборота, принятым в организации.
УЭП с доказательствами подлинности	–	Ошибка проверки ЭП. Причина неизвестна.	–	Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП (64Б)	–	Ошибка проверки ЭП: Нет данных для проверки.	Переданы данные нулевой длины.	Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам.
УЭП (64Б)	–	Ошибка проверки ЭП: Нет подписи для проверки.	Передана подпись нулевой длины.	Если позволяет регламент, подписать ЭП электронный документ заново. В противном случае, а также в случае повторения данной ошибки при проверке вновь созданной ЭП, обратиться к разработчикам
УЭП (64Б)	–	Ошибка проверки ЭП: Неверный серийный номер.	Значение серийного номера сертификата ключа подписи не совпадает с зарегистрированным в базе данных АЦК (**Serialnumber**).	Переустановить сертификат в информационной системе АЦК. Если после переустановки сертификата ошибка повторяется, обратиться к разработчикам.
УЭП (64Б)	–	Ошибка проверки ЭП: Неверный поставщик сертификата.	Значение поставщика сертификата ключа подписи не совпадает с зарегистрированным в базе данных АЦК (**Issuer**).	Переустановить сертификат в информационной системе АЦК. Если после переустановки сертификата ошибка повторяется, обратиться к разработчикам.
УЭП (64Б)	–	Ошибка проверки ЭП: Неверное поле **Субъект**.	Значение имени пользователя сертификата ключа подписи не совпадает с зарегистрированным в базе данных АЦК.	Переустановить сертификат в информационной системе АЦК. Если после переустановки сертификата ошибка повторяется, обратиться к разработчикам.

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
УЭП (64Б)	–	Ошибка проверки ЭП: Серийный номер не задан.	В базе данных АЦК для выбранного сертификата не заполнено поле **Серийный номер** (**Serialnumber**).	Переустановить сертификат в информационной системе АЦК. Если после переустановки сертификата ошибка повторяется, обратиться к разработчикам.
УЭП (64Б)	–	Ошибка проверки ЭП: Поставщик сертификата не задан.	В базе данных АЦК для выбранного сертификата не заполнено поле **Поставщик** (**Issuer**).	Переустановить сертификат в информационной системе АЦК. Если после переустановки сертификата ошибка повторяется, обратиться к разработчикам.
УЭП (64Б)	–	Ошибка проверки ЭП: Субъект сертификата не задан.	В базе данных АЦК для выбранного сертификата не заполнено поле **Пользователь** (**Subject**).	Переустановить сертификат в информационной системе АЦК. Если после переустановки сертификата ошибка повторяется, обратиться к разработчикам.
УЭП (64Б)	–	Не найден актуальный список отзыва сертификатов.	1. Для сертификата не найден список отзыва. 2. Список отзыва неактуален.	–
УЭП (64Б)	–	Сертификат пользователя был отозван.	Сертификат пользователя отозван (содержится в списке отзыва).	–
УЭП (64Б)	–	Целостность цепочки доверия нарушена.	Не найден хотя бы один сертификат из цепочки доверия.	–
УЭП (64Б)	–	В цепочке доверия имеются истекшие сертификаты.	Хотя бы один сертификат из цепочки доверия неактуален (истёк срок действия).	–
УЭП (64Б)	–	Не найден актуальный список отзыва для одного из сертификатов цепочки доверия.	1.Для одного из сертификатов цепочки доверия не найден список отзыва. 2. Список отзыва хотя бы для одного сертификата цепочки доверия неактуален.	–

Тип ЭП	Код	Сообщение	Описание возможных причин	Способ устранения/разрешения
УЭП (64Б)	–	В цепочке доверия имеются отозванные сертификаты.	Хотя бы один сертификат цепочки доверия отозван.	–

В процессе работы с подсистемой ЭП на экран могут выводиться диагностические сообщения, отсутствующие в списке. Описания таких сообщений см. в документации к другим подсистемам АЦК, документации к **КриптоПро CSP** или документации **Microsoft CryptoAPI** и др. (в соответствии со спецификой диагностического сообщения).

7.20 Приложение 20. Обобщенная спецификация формата электронного документа

Обобщенная структура дайджеста ЭД имеет следующий вид:

[описание_документа]

описания_полей_документа

описания_подчиненных_документов (необязательная часть)

[завершение_описания_документа]

где:

- **[описание_документа]** – строка вида **[(номер_раздела_документа)(пробел)(наименование_раздела_документа)]**,

где:

- **(номер_раздела_документа)** – порядковый номер раздела, который присваивается разделу документа автоматически по мере формирования дайджеста (по мере добавления в дайджест документа новых разделов);
- **(пробел)** – разделительный символ (код: 20);
- **(наименование_раздела_документа)** – значение атрибута **DESCRIPTION** соответствующей группы полей.

- **описания_полей_документа** – набор строк вида **(наименование_поля)(=)(«)(значение_поля)(«)**, где:

- **(наименование_поля)** – наименование поля документа, определяемое атрибутом **DESCRIPTION** тэга **FGROUPFIELD** (уникальный ключ поля документа в пределах раздела);
- **(=)** – обязательный символ (разделитель наименования поля и значения поля);
- **(«)** – обязательный символ (код: 22);
- **(значение_поля)** – значение поля документа (текстовая строка);
- **(«)** – обязательный символ (код: 22).

- **описания_подчиненных_документов** – совокупность блоков строк вида:

[(номер_раздела_документа)(пробел)(наименование_раздела_документа)]

описания_полей_документа

описания_подчиненных_документов (необязательная часть)

[(номер_раздела_документа)]

где подчиненные документы (например, строки) описываются в том же формате, что и родительский документ. Разделы описаний подчиненных документов размещаются внутри раздела описания родительского документа, после описаний его полей.

- **[завершение_описания_документа]** – строка вида **[(номер_раздела_документа)]**,

где:

- **(номер_раздела_документа)** – порядковый номер раздела, соответствующий значению **(номер_раздела_документа)**, строки **[описание_документа]** (см. выше).

7.21 Приложение 21. Инструкция по установке Сервиса ЭП АЦК

Для установки Сервиса ЭП АЦК (далее – Сервис) необходимо:

Примечание. *Для корректной работы Сервиса ЭП АЦК на ОС Windows XP необходимо перед инсталляцией Сервиса скачать и установить пакет обновления Administration Tools Pack, доступный по адресу: https://www.microsoft.com/en-us/download/details.aspx?id=16770.*

1. Запустить файл Мастера установки ***setup.exe*** 

.
2. В открывшемся окне выбрать язык, который будет использоваться в процессе установки Сервиса, и нажать кнопку **ОК**:

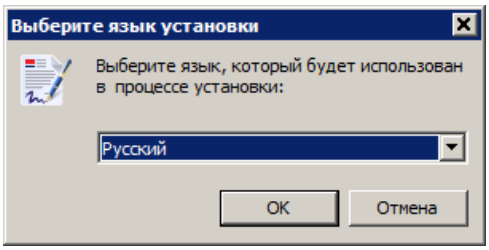

Рисунок 165 – Окно выбора языка установки

3. В окне приветствия Мастера установки нажать кнопку **Далее**:

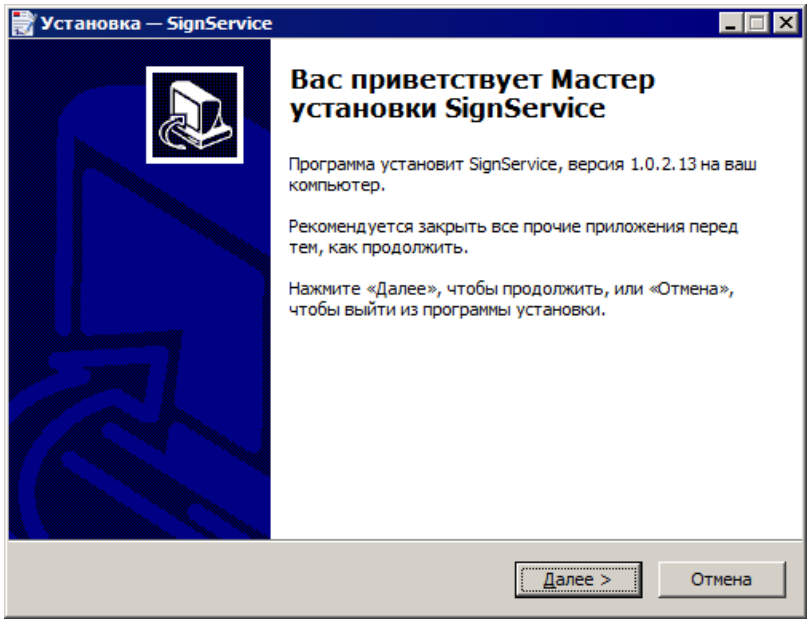

Рисунок 166 – Окно приветствия Мастера установки

4. В окне с информацией об установке нажать кнопку **Далее**:

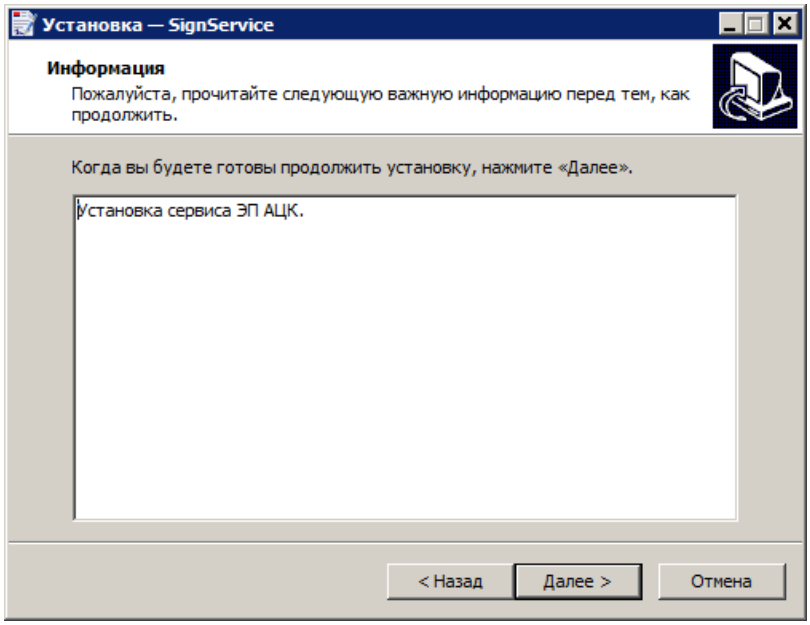

Рисунок 167 – Информационное окно Мастера установки

5. В окне выбора папки для установки с помощью кнопки **Обзор** выбрать папку, в которую необходимо произвести установку Сервиса:

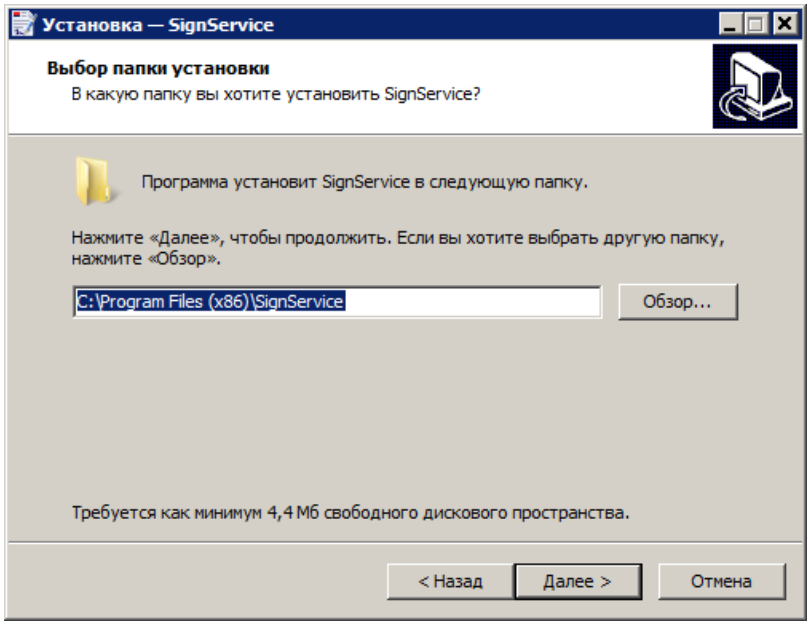

Рисунок 168 – Окно выбора папки установки

После выбора папки для установки необходимо нажать кнопку **Далее**.

6. В следующем окне с помощью кнопки **Обзор** необходимо выбрать папку меню **Пуск**, в которой будут созданы ярлыки запуска и удаления Сервиса:

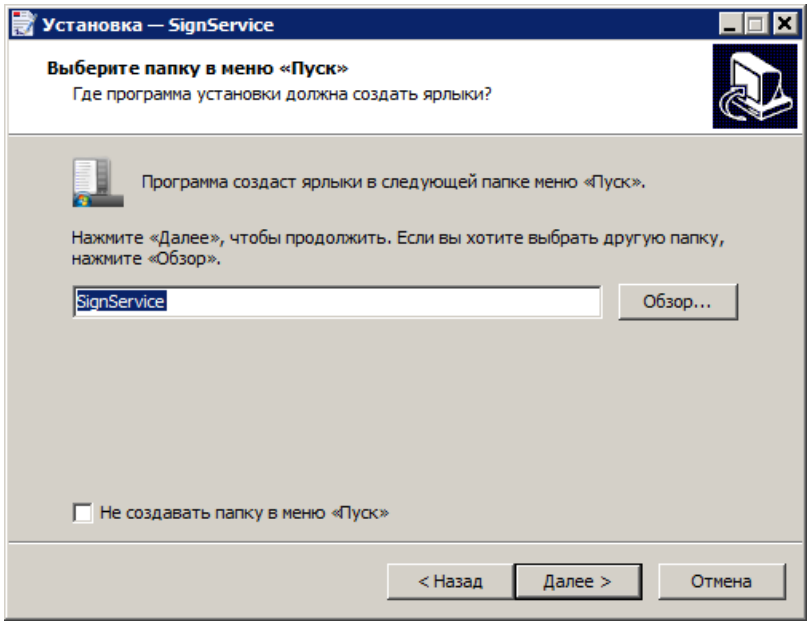

Рисунок 169 – Окно выбора папки в меню «Пуск»

После выбора папки для создания ярлыков необходимо нажать кнопку **Далее**.

7. В следующем информационном окне необходимо проверить правильность путей установки Сервиса и его ярлыков, после проверки нажать кнопку **Установить**:

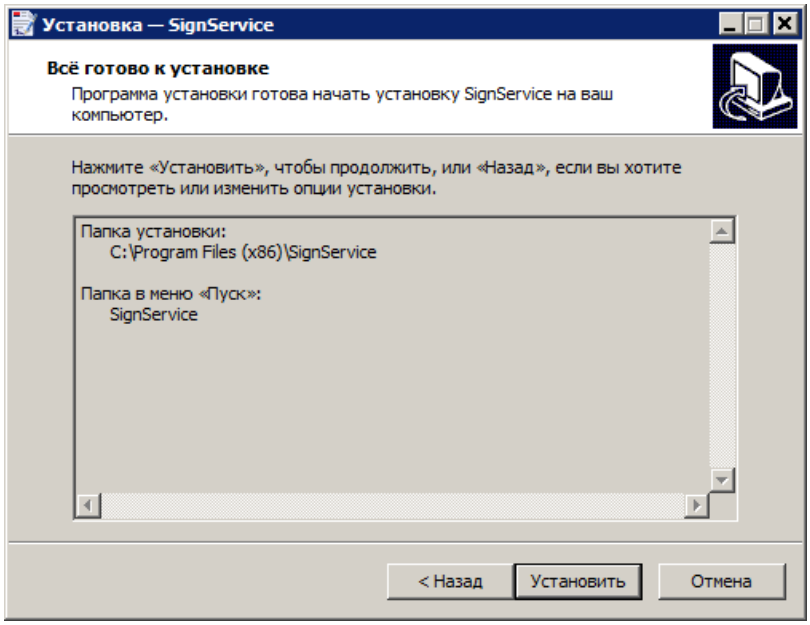

Рисунок 170 – Информационное окно Мастера установки

8. После произведенных операций запустится процесс установки Сервиса:

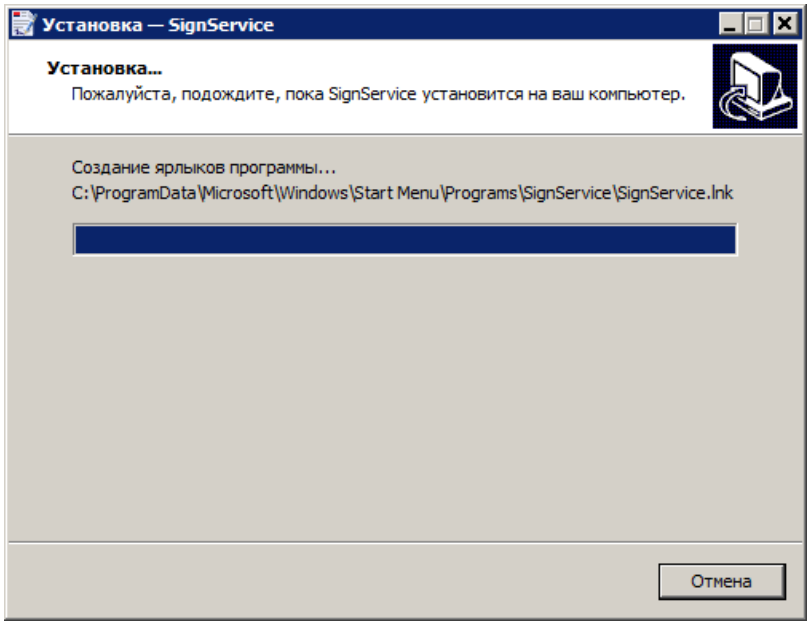

Рисунок 171 – Окно Мастера установки, отображающее ход процесса установки

9. В процессе инсталляции выдается запрос на установку сертификата издателя, необходимого для поддержки работы Сервиса через протокол HTTPS:

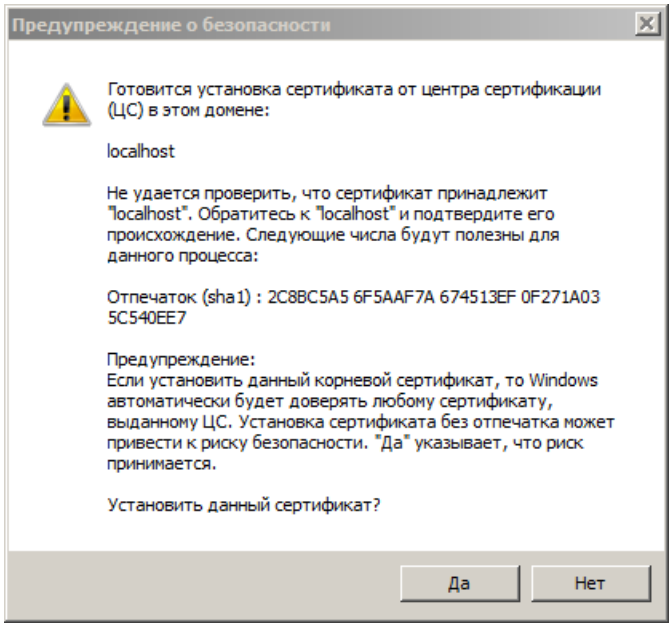

Рисунок 172 – Окно предупреждения о безопастности

Для продолжения инсталляции необходимо нажать кнопку **Да**.

10. По окончании процесса инсталляции на экране появится окно завершения Мастера установки Сервиса ЭП с включенным параметром **Запустить SignService**:

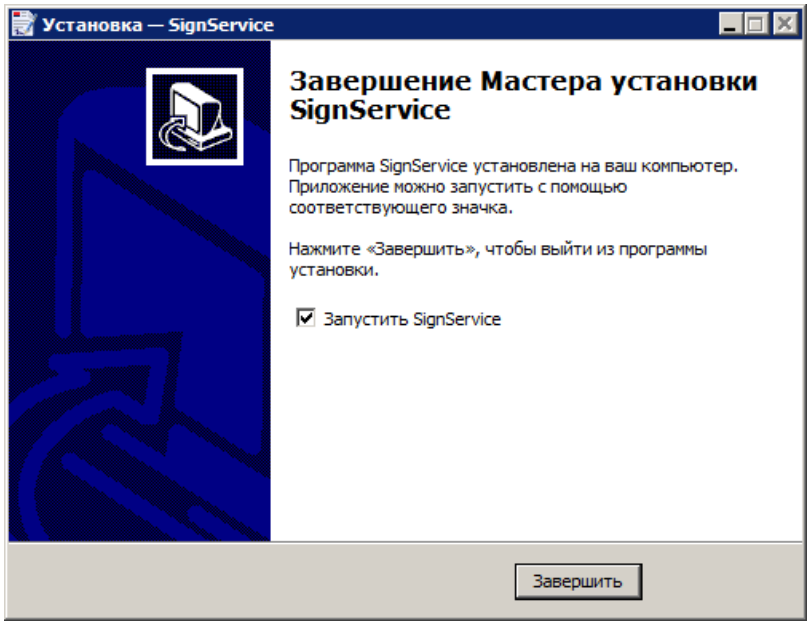

Рисунок 173 – Окно, информирующее о завершении установки Сервиса

Для завершения работы Мастера установки и запуска Сервиса необходимо нажать кнопку **Завершить**.

11. После установки Сервиса, в меню **Пуск** будет создана группа ярлыков **SignService**:

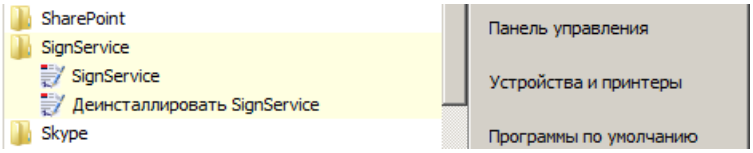

Рисунок 174 – Группа ярлыков «SignService» в меню «Пуск»

12. Факт запуска и работы Сервиса, а также его версию можно проверить посредством соответствующего значка в области уведомлений панели задач:

Рисунок 175 – Значок Сервиса в области уведомлений панели задач

Примечание. *Для работы через протоколы HTTP и HTTPS Сервис использует порты 50003 и 50004 соответственно. Для исправной работы Сервиса перед его запуском необходимо убедится в том, что данные порты не заняты сторонними приложениями.*

Для удаления Сервиса необходимо:

1. В меню **Пуск→Все программы→SignService** выбрать пункт **Деинсталлировать SignService**:

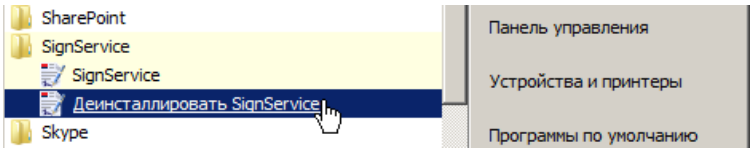

Рисунок 176 – Пункт «Деинсталлировать SignService» в группе ярлыков «SignService» в меню «Пуск»

2. В открывшемся диалоговом окне подтвердить остановку работающего сервиса, нажав кнопку **Да**:

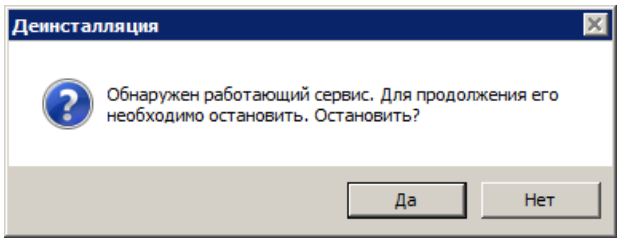

Рисунок 177 – Окно подтверждения остановки работающего Сервиса

3. Подтвердить удаление Сервиса и всех его компонентов, нажав кнопку **Да**:

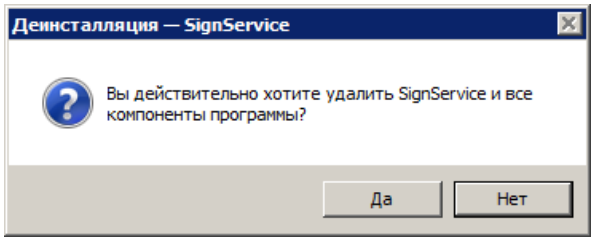

Рисунок 178 – Окно подтверждения удаления Сервиса

4. По окончании процесса удаления Сервиса в информационном окне завершения деинсталляции нажать кнопку **ОК**:

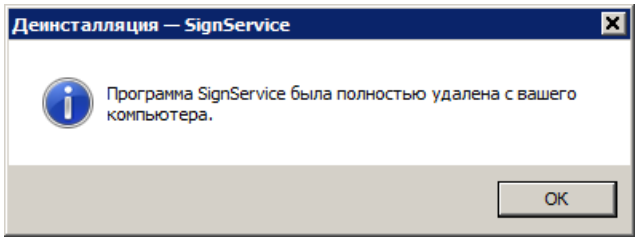

Рисунок 179 – Окно завершения деинсталляции

Для обновления (установки новой версии) Сервиса необходимо:

1. Запустить файл Мастера установки, соответствующий новой версии Сервиса. В открывшемся диалоговом окне подтвердить остановку старой версии Сервиса, нажав кнопку **Да**:

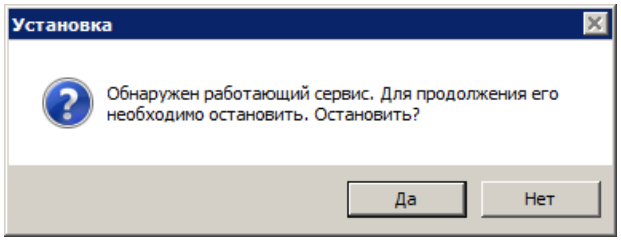

Рисунок 180 – Окно подтверждения остановки старой версии работающего Сервиса

2. Произвести дальнейшую установку новой версии Сервиса в соответствии с приведенной инструкцией установки Сервиса[163].

На персональном компьютере с установленным и запущенным Сервисом ЭП АЦК в браузере Mozilla FireFox необходимо выполнить следующее:

1. Открыть **Настройки→Дополнительные→Сертификаты→Просмотр сертификатов**.
2. В открывшемся окне *Управление сертификатами* перейти на закладку **Серверы** и нажать на кнопку **Добавить исключение...**.
3. В открывшемся окне в поле **Адрес** ввести значение: *https://localhost:50004*.
4. Нажать на кнопку **Получить сертификат**:

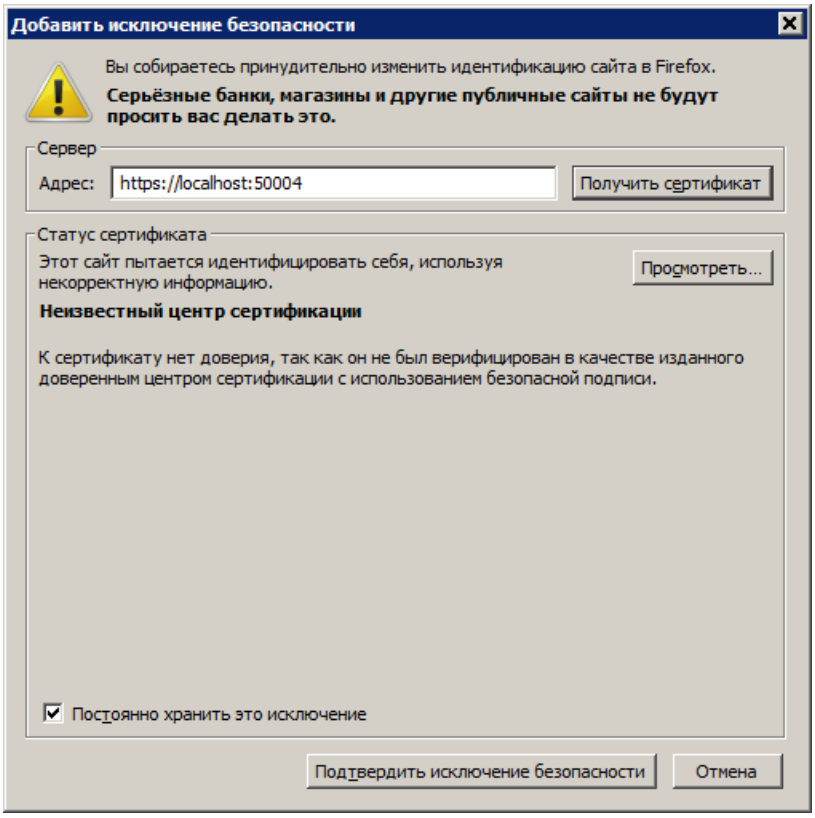

Рисунок 181 – Окно добавления исключения безопасности в FireFox

5. Нажать на кнопку **Подтвердить исключение безопасности**.
6. В окне *Управление сертификатами* нажать кнопку **Ок**.

7.22 Приложение 22. Инструкция по настройке состава дайджеста для электронного документа

Для создания описания состава дайджеста необходимо:

1. Создать xml-файл ***user_fgroups.xml***, расположив его в каталоге **XML** сервера приложений.

Файл должен быть в кодировке Windows-1251, т.е. в начале файла должна присутствовать строка:

‘<?xml version="1.0" encoding="windows-1251"?>’.

Далее обязательно должен присутствовать тэг:

<REFERENCE ref_name="FGROUPHEADER" SUBSYSTEM="0" action="synchronize">

</REFERENCE>

Внутри этого тэга должны находиться все описания дайджестов.

Для подписи документов определенного класса необходимо описать группу полей для этого класса документа. Группы полей описывают с помощью тэга **FGROUPHEADER**:

```
<FGROUPHEADER DOCUMENTCLASS_ID="19" NAME="USER_19_INCORDER" CAPTION="Распоряжение на зачисление в доходы" GROUP_TYPE="" DESCRIPTION="Распоряжение на зачисление в доходы">
```

где:

- значение атрибута **FGROUPHEADER** – группа полей;
- значение атрибута **DOCUMENTCLASS_ID** – ID класса документа;
- значение атрибута **NAME** – уникальное имя группы полей. Обязательно для этого поля использовать префикс **USER_**;
- значение атрибута **CAPTION** – заголовок группы полей, отображается в поле **Заголовок** в форме редактирования Группы полей. Рекомендуется в начале заголовка добавить определенное словосочетание, по которому легко можно будет найти пользовательскую группу в списке групп полей;
- значение атрибута **GROUP_TYPE** – тип группы полей (либо пустая строка, либо *attach*);
- значение атрибута **DESCRIPTION** – описание заголовка группы полей.

Группа полей содержит одну или несколько версий группы полей. Нельзя изменять версию группы полей, если этой группой полей уже подписывали документы. Если необходимо внести изменения в версию группы полей, нужно добавлять новую версию, а не вносить изменения в существующую версию. Внесение изменений в существующую версию группы полей приведет к невалидности подписей, сделанных с помощью этой версии группы полей.

Версия группы полей описывается с помощью тэга **FGROUP**:

```
<FGROUP FG_VERSION="1" FG_DATE="2008-01-01" OBJECT_NAME="INCORDER" CLASSNAME=" ">
```

где:

- значение атрибута **FGROUP** – версия группы полей;
- значение атрибута **FG_VERSION** – номер версии группы полей;
- значение атрибута **FG_DATE** – дата начала использования версии. По данному полю при подписании определяется версия, актуальная на дату документа;
- значение атрибута **OBJECT_NAME** – наименование объекта;
- значение атрибута **CLASSNAME** – наименования класса для преобразования дайджестов. Не заполняется;
- значение атрибута **BODY** – описание полей для формирования дайджеста.

В поле **BODY** содержатся описания подписываемых полей и строк документа в блоках **<FIELDS>** и **<ITEMS>** соответственно. Описание подписываемого поля содержится в тэге **< FGROUPFIELD >**:

```
<FIELDS>
<FGROUPFIELD DESCRIPTION="Номер" field_name="DOC_NUMBER" is_key="1"/>
<FGROUPFIELD DESCRIPTION="Дата" field_name="DOC_DATE" is_key="1"/>
<FGROUPFIELD DESCRIPTION="Сумма выписки" field_name="AMOUNT"/>
</FIELDS>
```

```
<ITEMS>
<FGFROUPINNERITEM NAME="USER_INCORDER_LINES" inneritem_name="LINES" use_fgroup_name="USER_INCORDER_LINES.19" use_fgroup_version="1"/>
</ITEMS>
```

где:

- значение атрибута **field_name –** наименование подписываемого поля базы данных;
- значение атрибута **DESCRIPTION** – описание подписываемого поля;
- **Is_key** – признак использования поля для формирования атрибута ЭП **Семантически значимые поля заголовка документа** (1.2.643.2.44.1.1.1.3.1, используется для проверки взаимного соответствия подписи и электронного документа при разборе конфликтных ситуаций, в этот атрибут записываются поля, позволяющие однозначно идентифицировать документ вне системы ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»»). Если параметр **is_key** отсутствует или равен 0, информация из настоящего поля не помещается в атрибут ЭП.

В тэге **< FGFROUPINNERITEM >** содержатся сведения о группе полей, используемой для подписи строк документа:

```
<FGFROUPINNERITEM NAME="_INCORDER_LINES" inneritem_name="LINES" use_fgroup_name="USER_INCORDER_LINES.19" use_fgroup_version="1"/>
```

где:

- значение атрибута **NAME** – наименование блока строк в дайджесте;
- значение атрибута **inneritem_name** – наименование блока строк;
- значение атрибута **use_fgroup_name** – наименование группы полей, используемое для описания дайджеста строк документа. В этом поле указывается уникальное имя (**NAME**) из описания той группы полей, которую пользователь хочет использовать для подписания строк документа;
- значение атрибута **use_fgroup_version** – версия группы полей, используемая для описания дайджеста строк документа. В этом поле указывается версия (**FG_VERSION**) из описания той группы полей, которую пользователь хочет использовать для подписания строк документа.

Таким образом, если требуется создать группу полей для подписи одного документа, который содержит один тип строк, требуется описать две группы полей. Одну группу полей для шапки документа и одну группу для строки документа. В первой группе в разделе **<FGFROUPINNERITEM>** необходимо указать данные второй группы полей, а именно наименование и версию группы.

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>
<REFERENCE ref_name="FGROUPHEADER" SUBSYSTEM="0" action="synchronize">
<FGROUPHEADER DOCUMENTCLASS_ID="19" NAME="USER_19_INCORDER" CAPTION="Распоряжение на зачисление в доходы" GROUP_TYPE="" DESCRIPTION="Распоряжение на зачисление в доходы">
  <FGROUP>
```

```
<FGROUP old_name="19" FG_VERSION="1" FG_DATE="2008-01-01" OBJECT_NAME="INCORDER" CLASSNAME=" ">
<BODY><![CDATA[
<FIELDS>
<!-- Общая информация -->
<FGROUPFIELD DESCRIPTION="Номер" field_name="DOC_NUMBER" is_key="1"/>
<FGROUPFIELD DESCRIPTION="Дата" field_name="DOC_DATE" is_key="1"/>
<FGROUPFIELD DESCRIPTION="Сумма выписки" field_name="AMOUNT"/>
<FGROUPFIELD DESCRIPTION="Тип дохода" field_name="KDT_CODE"/>
<FGROUPFIELD DESCRIPTION="Тип операции" field_name="OPERTYPE_CAPTION" />
<FGROUPFIELD DESCRIPTION="Невыясненные поступления прошлых лет" field_name="UNKNOWN_LAST_YEAR_FLAG"/>
<FGROUPFIELD DESCRIPTION="Основание" field_name="DESCRIPTION"/>
</FIELDS>
<ITEMS>
<FGFROUPINNERITEM NAME="_INCORDER_LINES" inneritem_name="LINES" use_fgroup_name="USER_INCORDER_LINES.19" use_fgroup_version="1"/>
</ITEMS>
]]></BODY>
</FGROUP>
<FGROUP old_name="19" FG_VERSION="2" FG_DATE="2015-09-01" OBJECT_NAME="INCORDER" CLASSNAME=" ">
<BODY><![CDATA[
<FIELDS>
<!-- Общая информация -->
<FGROUPFIELD DESCRIPTION="Номер" field_name="DOC_NUMBER" is_key="1"/>
<FGROUPFIELD DESCRIPTION="Дата" field_name="DOC_DATE" is_key="1"/>
<FGROUPFIELD DESCRIPTION="Сумма выписки" field_name="AMOUNT"/>
<FGROUPFIELD DESCRIPTION="Тип дохода" field_name="KDT_CODE"/>
```

```
                    <FGROUPFIELD DESCRIPTION="Тип операции" field_name="OPERTYPE_CAPTION"/>
    <FGROUPFIELD DESCRIPTION="Невыясненные поступления прошлых лет" field_name="UNKNOWN_LAST_YEAR_FLAG"/>
 <FGROUPFIELD DESCRIPTION="Основание" field_name="DESCRIPTION"/>
</FIELDS>
<ITEMS>
<FGFROUPINNERITEM NAME="_INCORDER_LINES" inneritem_name="LINES" use_fgroup_name="USER_INCORDER_LINES.19" use_fgroup_version="2"/>
</ITEMS>
    ]]></BODY>
    </FGROUP>
  </FGROUP>
 </FGROUPHEADER>
  <FGROUPHEADER DOCUMENTCLASS_ID="" NAME="USER_INCORDER_LINES.19" CAPTION="Строка распоряжения на зачисление в доходы" GROUP_TYPE="" DESCRIPTION="Строка распоряжения на зачисление в доходы">
  <FGROUP>
                    <FGROUP FG_VERSION="1" FG_DATE="2008-01-01" OBJECT_NAME="INCORDER" CLASSNAME="">
     <BODY><![CDATA[
<FIELDS>
 <!-- Доходная классификация-->
        <FGROUPFIELD DESCRIPTION="Администратор (Гл.Администратор)" field_name="KADMD_CODE"/>
 <FGROUPFIELD DESCRIPTION="КВД" field_name="KD_CODE"/>
 <FGROUPFIELD DESCRIPTION="КОСГУ" field_name="KESD_CODE"/>
 <FGROUPFIELD DESCRIPTION="Доп. КД" field_name="KDD_CODE"/>
 <FGROUPFIELD DESCRIPTION="КВФО" field_name="FSD_ID"/>
```

```
<FGROUPFIELD DESCRIPTION="Сумма" field_name="AMOUNT"/>
</FIELDS>
]]></BODY>
</FGROUP>
<FGROUP FG_VERSION="2" FG_DATE="2015-09-01" OBJECT_NAME="INCORDER" CLASSNAME="">
<BODY><![CDATA[
<FIELDS>
<!-- Доходная классификация-->
<FGROUPFIELD DESCRIPTION="Администратор (Гл.Администратор)" field_name="KADMD_CODE"/>
<FGROUPFIELD DESCRIPTION="КВД" field_name="KD_CODE"/>
<FGROUPFIELD DESCRIPTION="КОСГУ" field_name="KESD_CODE"/>
<FGROUPFIELD DESCRIPTION="Доп. КД" field_name="KDD_CODE"/>
<FGROUPFIELD DESCRIPTION="КВФО" field_name="FSD_ID"/>

<FGROUPFIELD DESCRIPTION="Сумма" field_name="AMOUNT"/>
<FGROUPFIELD DESCRIPTION="Основание строки" field_name="DESCRIPTION_LINES"/>
</FIELDS>
]]></BODY>
</FGROUP>
</FGROUP>
</FGROUPHEADER>
</REFERENCE>
```

2. Для регистрации пользовательской группы полей в системе ««АЦК-Госзаказ»/«АЦК-Муниципальный заказ»» необходимо выполнить файл ***user_fgroups.xml*** с помощью утилиты ***xml.cmd***. Для этого необходимо запустить сервер приложений АЦК.
3. В командной строке серверного каталоге **XML** выполнить команду:

```
..\XML>xml.cmd user_fgroups.xml.
```

После регистрации в системе АЦК пользовательская группа полей:

- появится в справочнике *Группы полей*;
- будет доступна при создании правил подписания ЭД и проверки ЭП на статусах;
- будет доступна для подписания (при настроенных правилах) в окне формирования подписи.

7.23 Приложение 23. ЭЦП АЦК под Linix

1. ТРЕБОВАНИЯ К СИСТЕМЕ

КриптоПро JCP – средство криптографической защиты информации, реализующее российские криптографические стандарты, разработанное в соответствии со спецификацией JCA (Java Cryptography Architecture).

ПО СКЗИ КриптоПро JCP предназначено для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечение аутентичности, конфиденциальности и имитозащиты соединений TLS;
- контроля целостности, системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Системные требования для функционирования КриптоПро JCP:

- виртуальная машина, удовлетворяющая спецификации Sun Java 2 ™ Virtual Machine;
- Java 2 Runtime Environment версии 1.4.2, 1.5.0 для версии JCP 1.0.46, Java 6 и выше для 1.0.54 (для этой версии – Java до 1.7.0_25) и 2.x.

2. Установка и настройка ПО СКЗИ для АЦК

Для настройки ЭП на продуктах АЦК требуется:

- Java SE (версия jdk1.8.0_77).
- Крипто Про JCP (версия jcp-2.0.39014).

***Примечание**. Скачать Крипто Про JCP можно по адресу http://www.cryptopro.ru/products/csp/jcp/downloads (для возможности скачивания необходимо зарегистрироваться на сайте).*

- Корневой сертификат УЦ.
- Система АЦК.

С помощью команды sudo mkdir /opt создается папка opt:

Рисунок 182 – Создание папки Otp

Затем осуществляется:

2.1 Установка Java SE

Архив Java (jdk-8u77-linux-x64.tar.gz) копируется в папку opt.

С помощью команды sudo tar –xzvf jdk-8u77-linux-x64.tar.gz происходит распаковка архива:

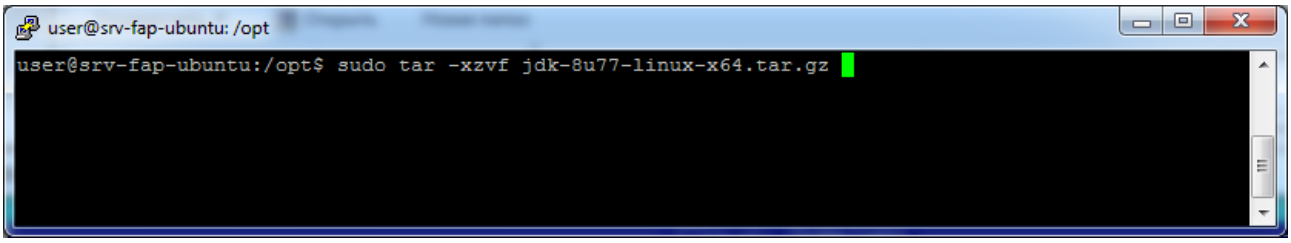

Рисунок 183 – Распаковка архива с помощью команды

Затем прописывается JAVA_HOME и путь к JAVA:

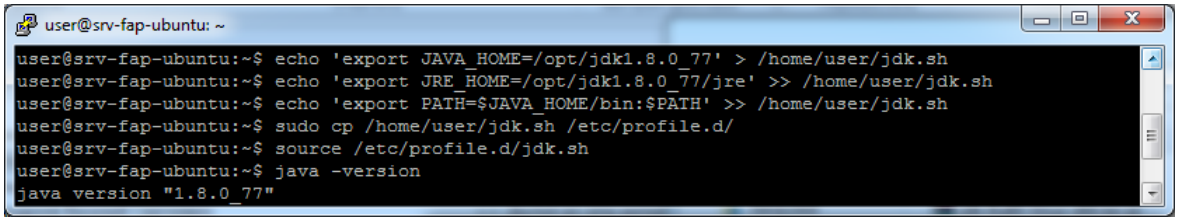

Рисунок 184 – Java_Home и путь к Java

2.2 Установка Крипто Про JCP

Архив Крипто Про JCP (jcp-2.0.39014.zip) копируется в папку opt.

С помощью команды sudo unzip jcp-2.0.39014.zip происходит распаковка архива:

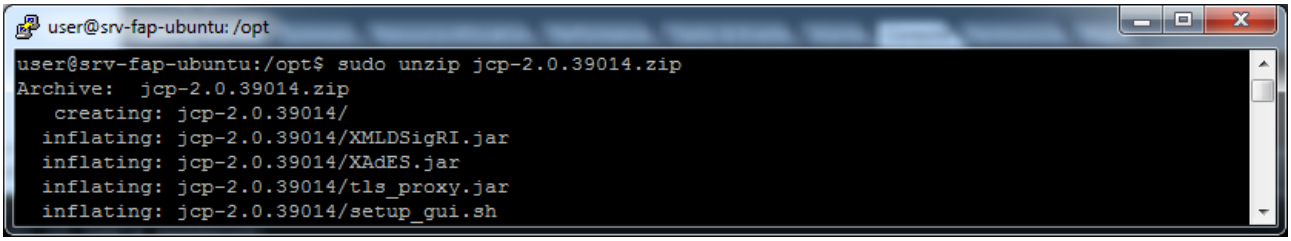

Рисунок 185 – Распаковка архива jcp-2.0.39014.zip с помощью команды

Далее переходим в папку /opt/jcp-2.0.39014:

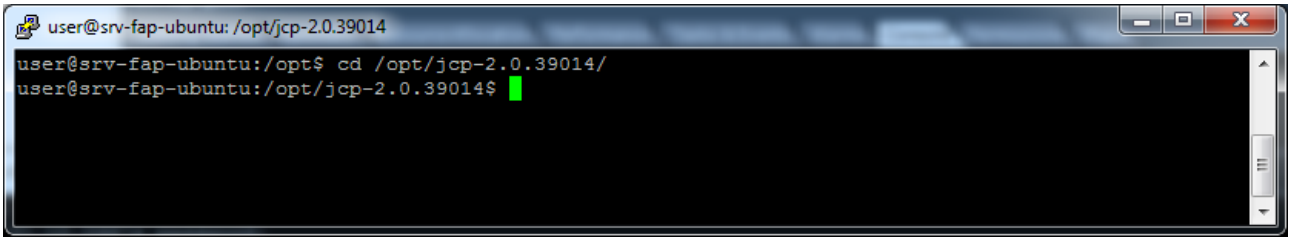

Рисунок 186 – Перход в папку otp

В консоли вводится команда sudo chmod +x *.sh:

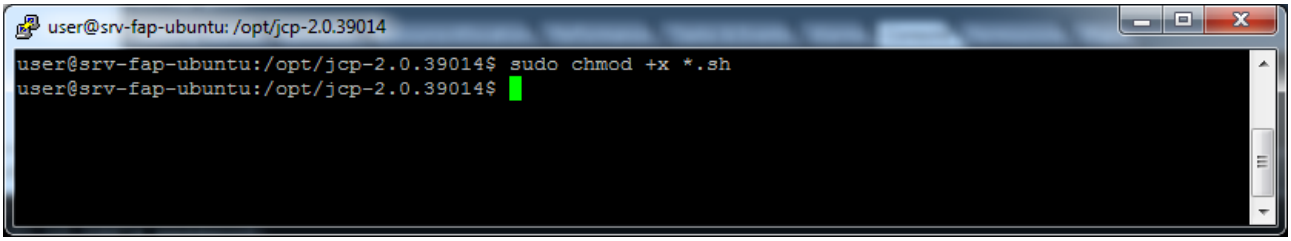

Рисунок 187 – Ввод команды sudo chmod +x *.sh

Далее, с помощью команды sudo ./setup_console.sh /opt/jdk1.8.0_77/, происходит установка КриптоПро JCP. В процессе установки в ответ на все вопросы системы нажимается кнопка **Enter**.

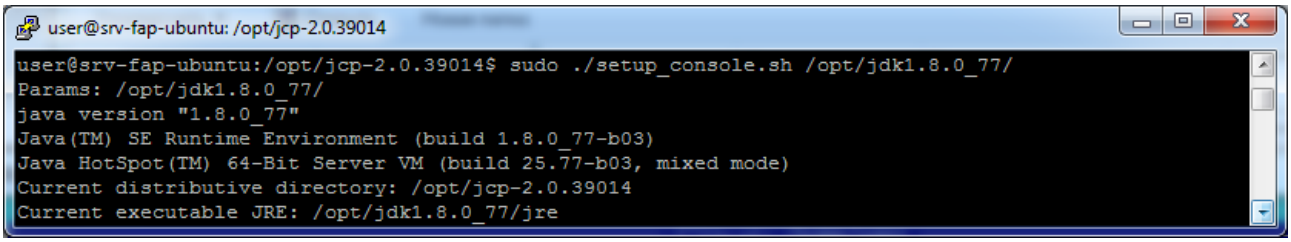

Рисунок 188 – Установка JCP

2.3 Импорт корневого сертификата УЦ

Для импорта корневого сертификата УЦ необходимо перейти в папку с jre (/opt/jdk1.8.0_77/jre/lib/security/) и выполнить команду:

sudo /opt/jdk1.8.0_77/jre/bin/keytool -importcert -alias jcpca.cer -file /opt/jcpca.cer -keystore cacerts

Примечание. *В случае, если система запрашивает ввод пароля, необходимо ввести пароль пользователя.*

Далее вводится пароль *«changeit»:*

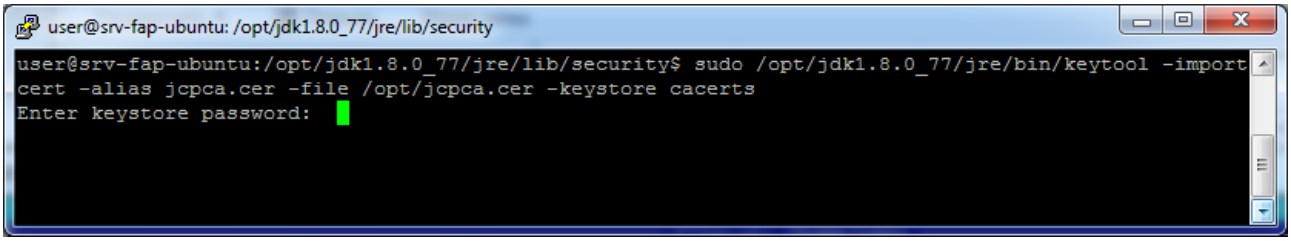

Рисунок 189 – Ввод пароля

Затем вводится значение *«yes»:*

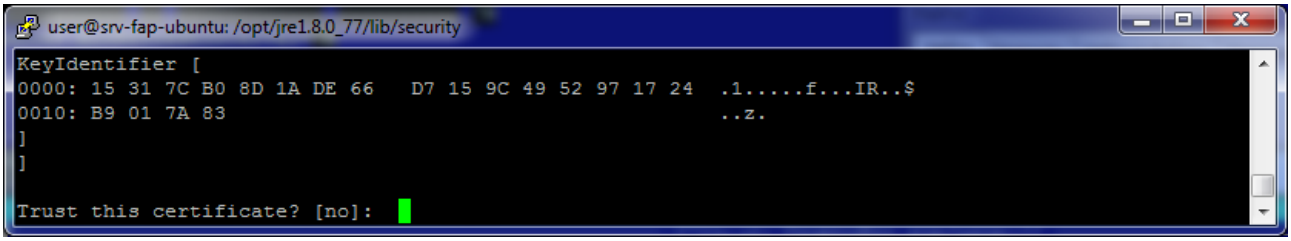

Рисунок 190 – Подтверждение ввода пароля

2.4 Установка АЦК

Установка АЦК представляет собой набор следующих действий:

- Папка со стендом копируется в каталог /opt.
- В папке со стендом (/opt/stand_2.43.0) необходимо исправить файл Azk2Server.properties следующим образом:
  - изменить параметры azk.native.cryptoprovider = false, также в параметре azk.crl.path указать путь к папке с CRL-файлами (azk.crl.path=/opt/crl).

Важно! *В папке с CRL-файлами не должно быть файлов с расширением.*

- Далее запускается стенд.

Примечание. *Вход в систему может также осуществляться по сертификату.*

НАШИ КОНТАКТЫ

Звоните:
(495) 784-70-00

Пишите:
bft@bftcom.com

Будьте с нами online:
www.bftcom.com

Приезжайте:
127018, Москва, ул. Складочная, д.3, стр.1

Дружите с нами в социальных сетях:

vk.com/bftcom

facebook.com/companybft

twitter.com/bftcom

instagram.com/bftcom