УТВЕРЖДЕН

РБ.ЮСКИ.08003-02 34 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС

«ПЕРСОНАЛЬНЫЙ МЕНЕДЖЕР СЕРТИФИКАТОВ АВЕСТ»

AvPCM

Руководство оператора

РБ.ЮСКИ.08003-02 34 01

Листов 81

Подп. и дата	
Инв.№ дубл	
Взам. инв.№	
Подп. и дата	
Инв.№	

2013

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта РБ.ЮСКИ.08003-02 «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» (далее – ПК AvPCM). В документе содержится информация и приведена последовательность действий оператора при установке и использовании AvPCM. А также приведены процедуры общения оператора с ПК AvPCM в процессе функционирования ПК AvPCM.

ПК AvPCM является элементом инфраструктуры открытых ключей (ИОК) и предоставляет пользователю ИОК сервисы управления криптографическими ключами, сертификатами открытых ключей (далее – СОК) и списками отозванных сертификатов (далее – СОС) в соответствии с ТНПА Республики Беларусь.

СОДЕРЖАНИЕ

1.НАЗНАЧЕНИЕ ПРОГРАММЫ

ПК AvPCM функционирует на персональном компьютере конечного субъекта - пользователя ИОК и предоставляет пользователю ИОК сервисы управления криптографическими ключами, сертификатами открытых ключей (далее – СОК) и списками отозванных сертификатов (далее – СОС).

ИОК – это технологическая инфраструктура, сервисы и процедуры, обеспечивающие необходимый уровень доверия и безопасности информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

ИОК обеспечивает сервисы, необходимые для непрерывного управления ключами в распределенной системе, связывает открытые ключи с владельцами соответствующих личных ключей и позволяет пользователям проверять подлинность этих связей.

Цель ИОК состоит в управлении криптографическими ключами, СОК и СОС, посредством которого поддерживается надежная сетевая среда. ИОК позволяет использовать криптографические сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, использующих криптографические алгоритмы с открытыми ключами.

В качестве программного средства криптографической защиты информации (ПСКЗИ), реализующего криптографические алгоритмы и протоколы в соответствии с ТНПА Республики Беларусь ПК AvPCM использует криптопровайдер компании ЗАО «АВЕСТ».

В состав ПК AvPCM входят следующие ПСКЗИ, предоставляющих криптографические сервисы ЭЦП и шифрования:

- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP» AvCSP (РБ.ЮСКИ.08000-02);
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BEL» AvCSPBEL (РБ.ЮСКИ.12004-01);
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BIGN» AvCSPBIGN (РБ.ЮСКИ.12005-01), использующий криптографические сервисы изделия ИЯТА.467532.003 «Устройства программно-аппаратные электронной цифровой подписи и шифрования AvBign».

Примечание: Варианты установки см. ниже.

ПК AvPCM предоставляет пользователю ИОК следующие сервисы:

– генерация с помощью криптопровайдеров личных и открытых ключей ЭЦП и шифрования по ГОСТ 28147-89 оператора ОО удовлетворяющих требованиям СТБ 1176.2-99, СТБ 1176.1-99, СТБ 34.101.31-2011, СТБ П 34.101.45-2011 и проекта РД РБ «Банковские технологии. Протоколы формирования общего ключа» (ПФОК);

– формирование запроса на сертификат к удостоверяющему центру в соответствии с требованиями СТБ 34.101.17-2012 (PKCS#10);

– формирование карточки открытого ключа в соответствии с требованиями СТБ 34.101.49-2012;

– поддержка СОК и СОС, удовлетворяющих требованиям РД РБ 07040.1206-2004 и СТБ 34.101.19-2012 (X.509);

– поддержка форматов параметров криптографических алгоритмов согласно СТБ 34.101.23-2012 (PKCS#7);

– регистрацию объектов информационных технологий согласно СТБ П 34.101.50-2012;

– использование реестра сертификатов, размещенного в локальной файловой системе, хранилищах Microsoft Crypto API (системный реестр Windows) или базе данных;

– хранение списка доверенных корневых удостоверяющих центров с контролем целостности в случае использования файлового хранилища СОК и СОС;

– использование реестра сертификатов УЦ и РЦ;

– информирование пользователя об ошибке при любых некорректных действиях пользователя или сбоях компонентов программного комплекса;

– визуализация сертификата для просмотра атрибутов его владельца и назначения сертификата;

– проверка действительности СОК и СОС;

– ведение журнала работы ПК AvPCM с обеспечением контроля целостности файла журнала.

Взаимодействие ПК AvPCM с криптопровайдером AvCSP осуществляется с использованием открытых стандартизированных криптографических интерфейсов: Microsoft Cryptographic Application Programming Interface (CryptoAPI) версий 1.0 и 2.0

ПК AvPCM обеспечивает выполнение криптографических сервисов ЭЦП, шифрования, управления ключами, СОК и СОС абонента ИОК в соответствии со следующими нормативными актами и документами:

1) ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая.

Алгоритм криптографического преобразования»;

2) СТБ 1176.1-99 «Информационная технология. Защита информации. Процедура хэширования»;

3) СТБ 1176.2-99 «Информационная технология. Защита информации. Процедура выработки и проверки электронной цифровой подписи»;

4) СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»

5) СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»

6) СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией»;

7) СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

8) СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»;

9) СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»;

10) СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (раздел 6.2).

11) СТБ 34.101.49-2012 «Информационные технологии и безопасность. Формат карточки открытого ключа»

12) Проект Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа»

13) СТБ П 34.101.45-2011 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых»;

14) СТБ П 34.101.50-2012 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий».

2.УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

ПК AvPCM предназначен для работы на персональном компьютере общего назначения, функционирующим под управлением ОС MS Windows:

- Windows 2003 Server (x32, x64) SP1 или выше;
- Windows XP SP3 (x32);
- Windows XP SP2 (x64);
- Windows Vista SP1/SP2 (x32, x64);
- Windows 7 (x32, x64);
- Windows 8 (x32, x64);
- Windows 8.1 (x32, x64);
- Windows 2008 R1 Server (x32, x64);
- Windows 2008 R2 Server (x64);
- Windows 2012 Server (x64);
- Windows Windows 2012 R1 Server (x64);

Требуется также наличие установленного Microsoft Internet Explorer версии 6.0 и выше.

Для использования ПК AvPCM в операционных системах Windows XP, Windows 2003, Windows Vista, Windows 7 Windows 2008 и Windows 8 пользователь должен иметь права «Administrator (Администратор)» либо «PowerUser (Опытный пользователь)».

Для установки и работы программы требуется персональный IBM – совместимый компьютер, имеющий оперативную память не менее 128 Мбайт, жесткий диск, содержащий не менее 450 Мбайт свободного пространства, монитор с установленным разрешением не менее чем 800x600 и цветовой палитрой не менее 256 цветов.

Для хранения личных ключей пользователя ИОК ПК AvPCM использует отчуждаемые носители ключевой информации (НКИ).

На компьютере должен быть установлен один из типов криптопровайдера AvCSP.

3.ВЫПОЛНЕНИЕ ПРОГРАММЫ И СООБЩЕНИЯ ОПЕРАТОРУ

ПК AvPCM является интерактивным приложением, выполняющимся в среде 32 либо 64-разрядной операционной системы Microsoft Windows. Для выполнения программы необходимо использовать средства, предоставляемые данным семейством операционных систем. Взаимодействие с оператором, осуществляется посредством обращения к пунктам меню и ввода данных в поля диалоговых форм. Сообщения оператору, а также информация об актуальном состоянии базы данных отображается в диалоговых окнах графического пользовательского интерфейса.

В разделах, приведенных далее, описываются диалоговые окна, выводимые ПК AvPCM, и действия оператора по управлению ПК AvPCM.

4.УСТАНОВКА ПРОГРАММЫ

Перед установкой ПК AvPCM необходимо проверить, установлен ли на компьютере, на котором будет произведена установка программы, криптопровайдер Avest CSP («Пуск»⇒ «Настройка»⇒ «Панель управления»⇒ «Установка и удаление программ») и подключен ли свободный носитель для записи личных ключей пользователя. В случае, если криптопровайдер еще не был установлен, произвести его установку.

ПК AvPCM поддерживает 3 варианта установки в зависимости от использования типа хранилища СОК и СОС:

- установка с сетевой базой данных сертификатов;
- установка с файловой базой данных сертификатов;
- установка с базой данных в реестре Windows.

Для использования ПК AvPCM с криптопровайдером Avest CSP X.X.X.XXX в качестве файла настроечных данных нужно использовать AvCmED_Main.zip

Для использования ПК AvPCM с криптопровайдером Avest CSP BEL X.X.X.XXX в качестве файла настроечных данных нужно использовать:

AvCmED_Main_Bel2.zip – для старых объектных идентификаторов (OID) – ов;

AvCmED_Main_Bel1.zip – для новых OID – ов.

Для использования ПК AvPCM с криптопровайдером Avest CSP BIGN X.X.X.XXX в качестве файла настроечных данных нужно использовать AvCmED_Bign.zip

Выбор варианта установки программы зависит от необходимости использования различных криптографических алгоритмов и OID.

4.1.Установка с сетевой БД

Действия по установке ПК AvPCM:

1) Запустить с дистрибутива программу AvPCM_DB_setup.exe (AvPCMEx_DB_setup.exe).

   Для запуска программы воспользуйтесь пунктом «Выполнить» в основном меню Windows «Пуск», либо сделайте это с помощью возможностей стандартного приложения Windows «Проводник».

   В начале установки выводится стандартное окно с информацией о предполагаемом к установке программном обеспечении (см. **Рисунок 1**).

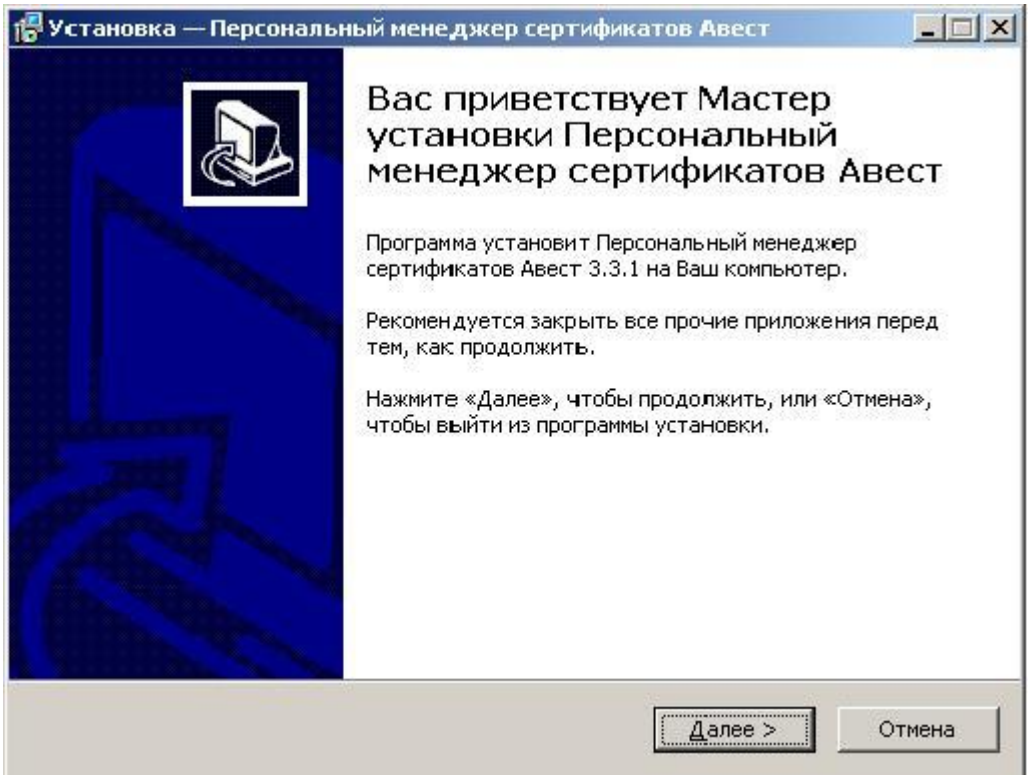

Рисунок 1. Заставка начала инсталляции ПК AvPCM

В следующем окне установки ПК AvPCM оговариваются условия лицензионного соглашения. Для продолжения процедуры инсталляции надо принять условия лицензионного соглашения и нажать кнопку «Далее».

Если Вы не согласны с условиями лицензионного соглашения, нажмите кнопку «Отмена» для выхода из программы.

2) Определить основной каталог, в котором будут расположены устанавливаемые компоненты (см. Рисунок 2).

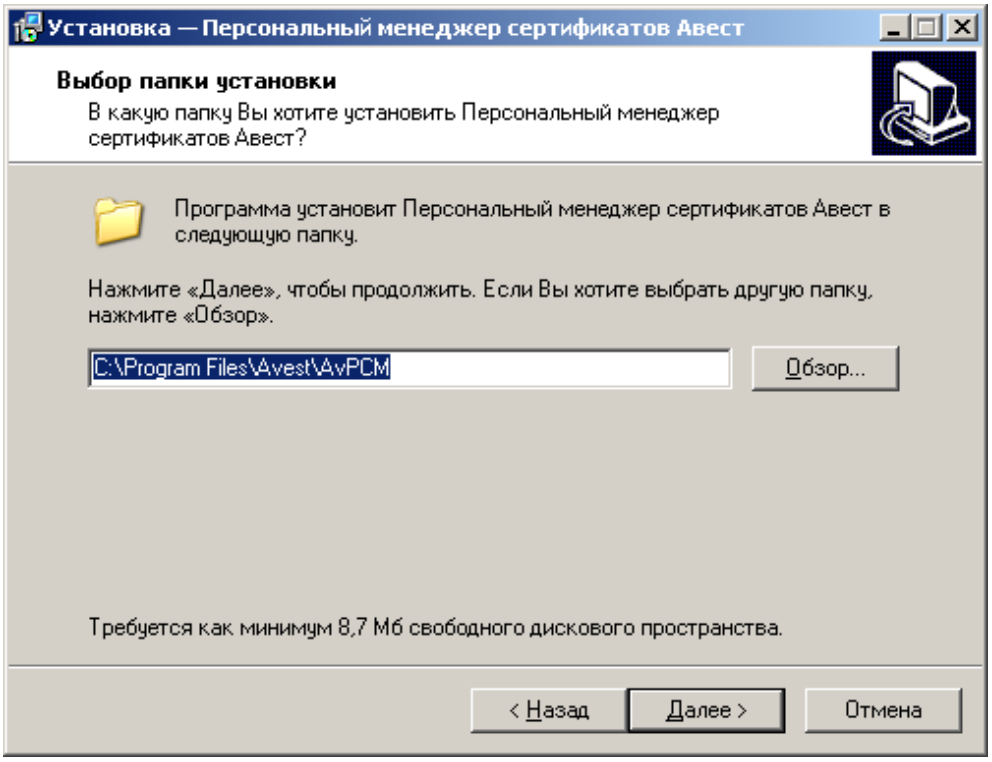

Рисунок 2. Выбор каталога установки программы

3) Определить тип установки ПК AvPCM. В окне «Выбор компонентов» требуется выбрать из встроенного списка тип установки программы – «Инсталляция с сетевой базой данных», выбрать используемую базу данных и нажать кнопку «Далее» (см. Рисунок 3).

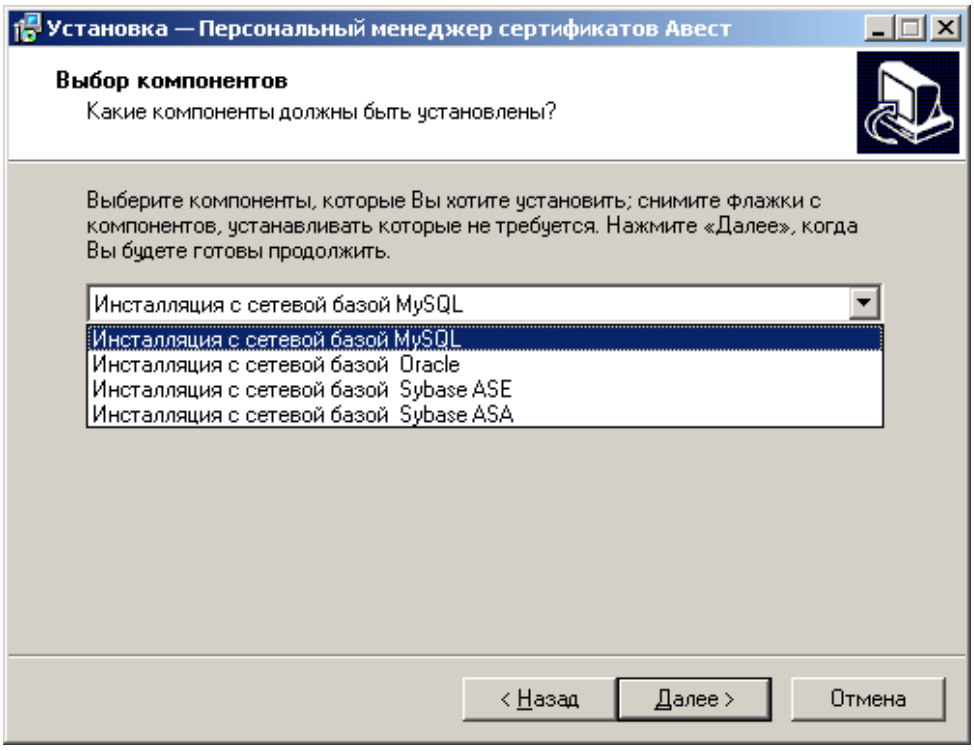

Рисунок 3. Выбор компонентов

Следующая страница мастера установки проинформирует о том, что все готово к установке ПК AvPCM, а в окне параметров установки будут указаны: путь к месту хранения ПК AvPCM на компьютере, тип установки, выбранные компоненты. Для установки ПК AvPCM здесь надо нажать кнопку «Установить» (см. **Рисунок 4**).

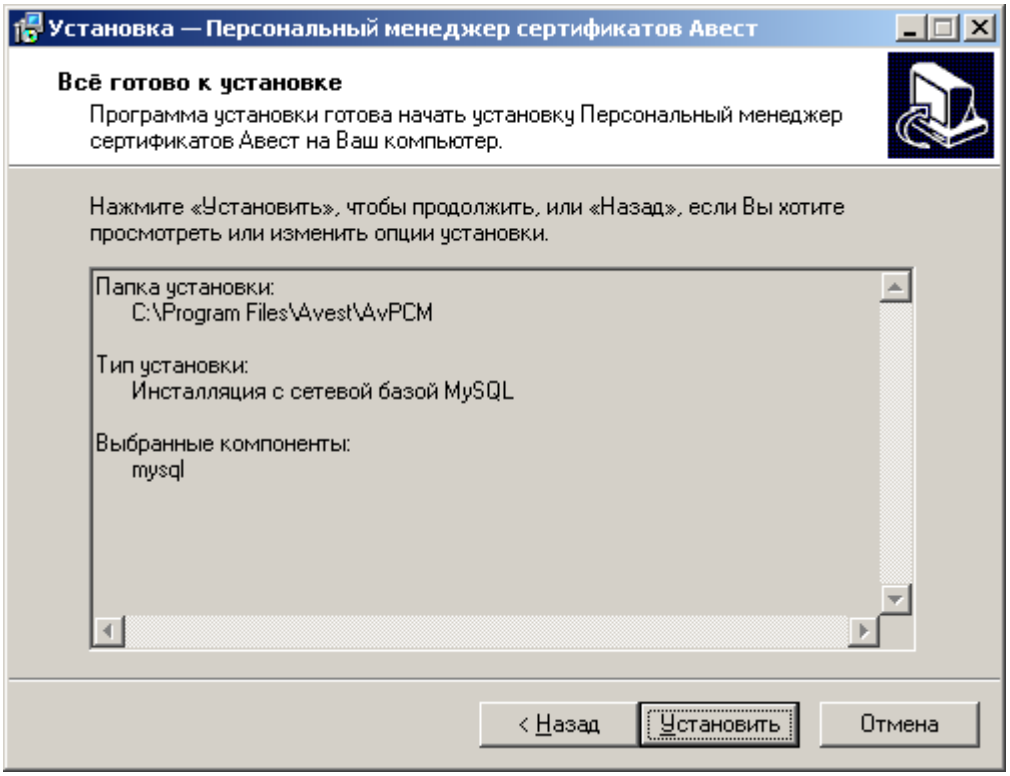

Рисунок 4. Параметры установки программы

ПК AvPCM произведет распаковку и копирование файлов программного обеспечения.

В последнем окне мастера установки ПК AvPCM включены флажки «Настройка сетевого подключения к БД» и «Запустить менеджер сертификатов». Если Вы хотите перейти к настройке сетевого подключения и открыть ПК AvPCM для создания запроса на сертификат, рекомендуется не снимать флажки и нажать кнопку «Завершить» для выхода из мастера установки ПК AvPCM.

Если Вы хотите произвести настройку позже и выйти из мастера установки, то снимите все флажки и нажмите кнопку «Завершить».

4) Затем следует произвести настройку сетевого доступа к базе данных справочников сертификатов (см. **Рисунок 5**):

– в группе «База данных сертификатов» указать источник данных (ODBC), имя базы данных Удостоверяющего центра, имя администратора БД и пароль доступа администратора к ней и нажать кнопку «Проверить подключение»;

Внимание: Перед проверкой подключения при установке ПК AvPCM следует убедиться, что запущена программа удостоверяющего центра «Центр цифровых сертификатов Авест» к базе данных, которого производится подключение.

– в группе «Пользователь БД» ввести, или выбрать из существующих имя пользователя, используемое при подключении к базе данных и ввести его пароль;
– Если было введено новое имя пользователя, то требуется ввести его пароль доступа и нажать последовательно кнопки «Создать пользователя БД» и «Проверить подключение»;
– Нажать кнопку «Сохранить» для сохранения настроек сетевого подключения.

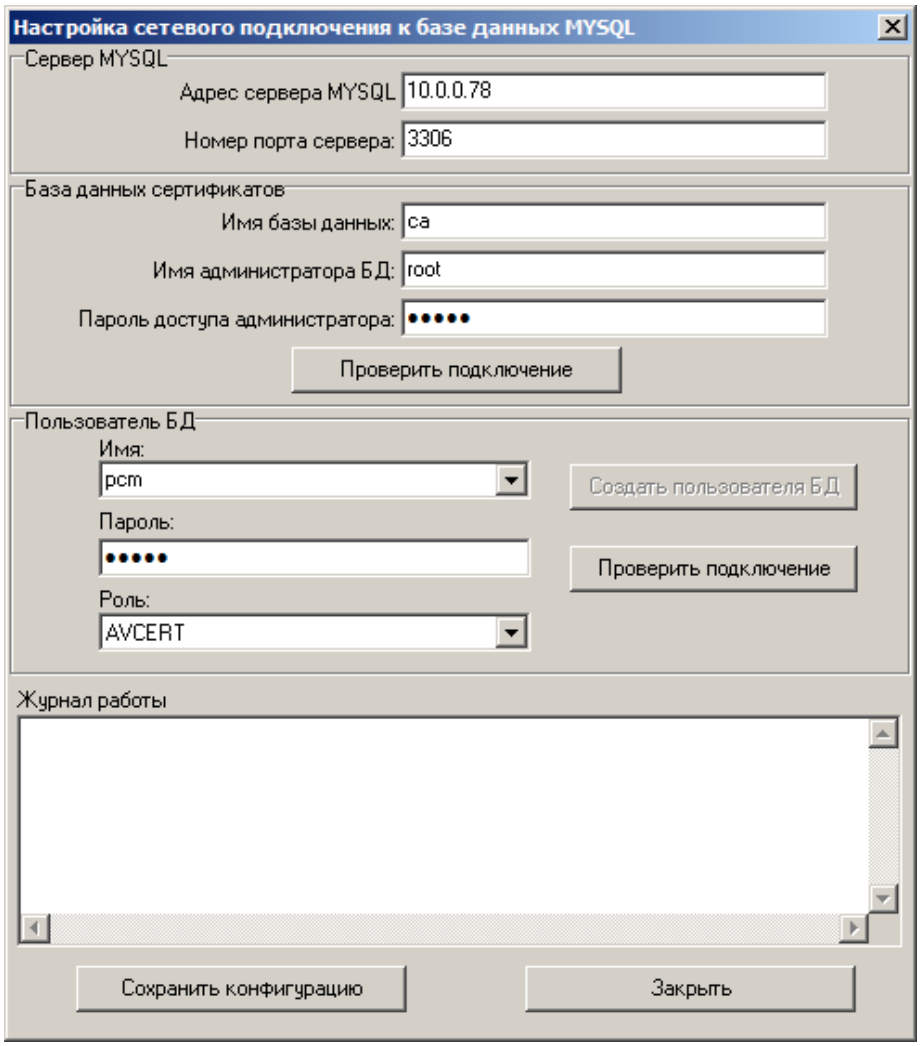

Рисунок 5. Настройка сетевого подключения к БД

Процесс установки ПК AvPCM завершен.

После завершения установки ПК AvPCM раздел «Программы» в основном меню Windows «Пуск» будет дополнен подразделом «Авест» – AvPCM, а на рабочем столе появится ярлык для быстрого запуска ПК AvPCM.

4.2. Установка с файловой базой данных (с базой данных в реестре)

Установка ПК AvPCM с файловой базой данных или базой данных сертификатов в системном реестре Windows производится аналогично установке с сетевой базой данных. Основное отличие в том, что используются установочные файлы AvPCM_setup.exe (AvPCMEx_setup.exe), и в окне «Выбор компонентов» требуется указать «Инсталляция с файловой базой данных сертификатов» или «Инсталляция с базой данных сертификатов в реестре» (см. **Рисунок 6**).

Данный вариант установки не предусматривает подключение к сетевой базе данных УЦ, поэтому пункты, касающиеся настройки сетевого подключения к базе данных здесь не рассматриваются.

В случае успешного завершения установки ПК AvPCM на экране появится окно с сообщением о выполненной инсталляции с предложением запустить ПК AvPCM, для чего требуется включить имеющийся в данном окне флажок. Для выхода из программы надо нажать кнопку «Завершить» (см. **Рисунок 7**).

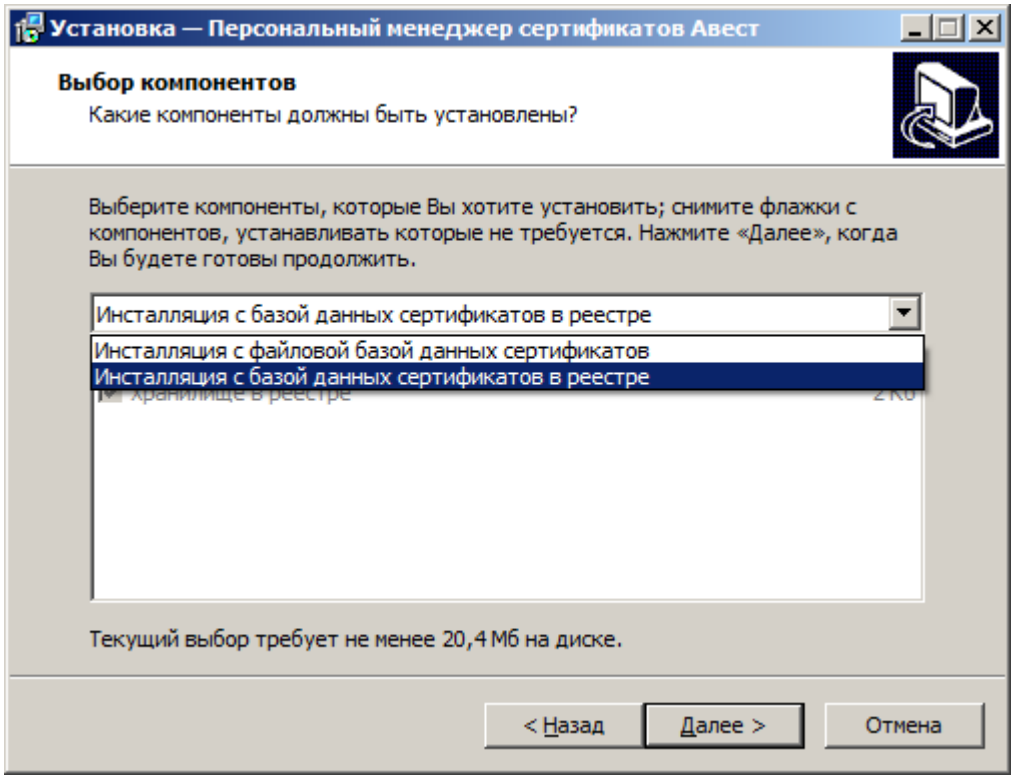

Рисунок 6. Выбор компонентов

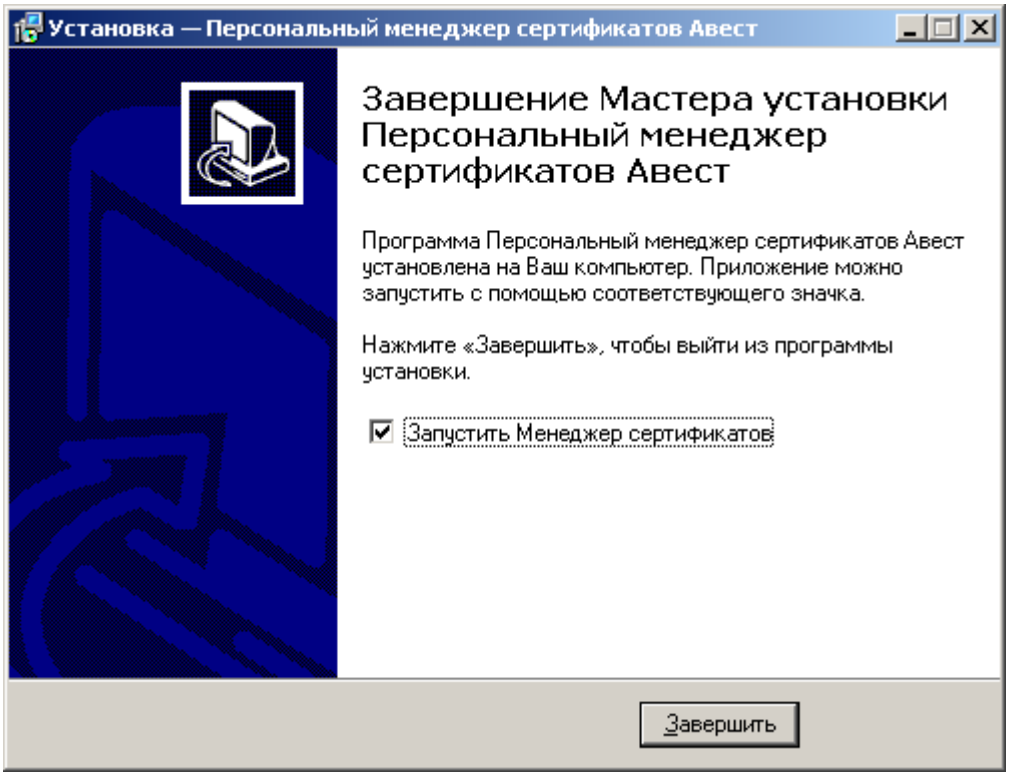

Рисунок 7. Завершение работы мастера установки программы

После завершения программы установки раздел «Программы» в основном меню *Windows* «Пуск» будет дополнен подразделом «Авест», который включает в себя следующие пункты:

– «Персональный менеджер сертификатов Авест»;
– «Создать запрос на сертификат»;
– «Импорт сертификатов».

На рабочем столе появится ярлык для быстрого запуска ПК AvPCM.

5. ЗАПУСК ПРОГРАММЫ

Запуск ПК AvPCM может производиться 2 способами:

- Из основного меню Windows: «Пуск»→«Программы»→«Авест»→ «Персональный менеджер сертификатов Авест»;
- Щелкнув по ярлыку ПК AvPCM, находящемся на вашем Рабочем столе после инсталляции.

Вход в систему осуществляется через авторизацию пользователя, для этого в окне авторизации необходимо выбрать идентификатор ключевого контейнера соответствующий личному ключу пользователя, после чего ввести пароль доступа к нему (см. **Рисунок 8**).

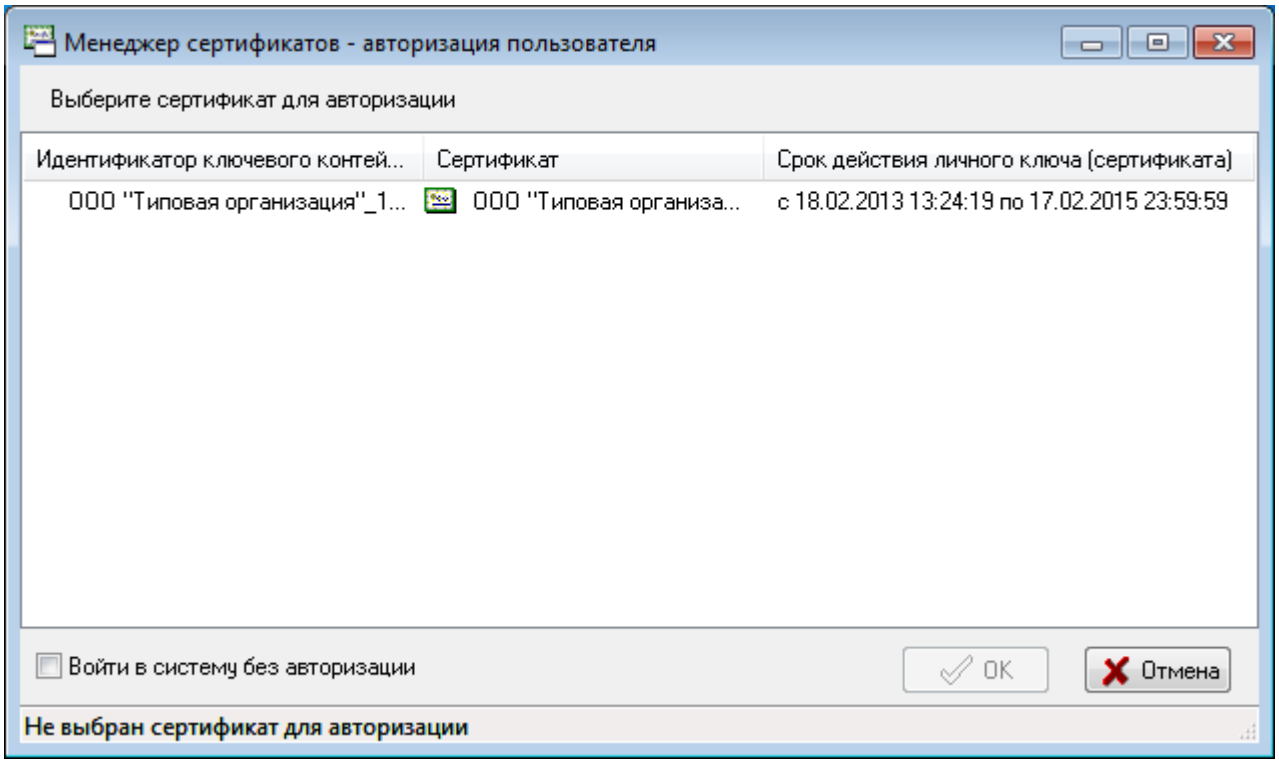

Рисунок 8. Авторизация пользователя

6. РАБОТА С ПРОГРАММОЙ

6.1. Создание запроса на сертификат

Процедура генерации новой пары ключей и создания запроса на сертификат – это первая процедура, которую нужно выполнить пользователю после инсталляции ПК AvPCM на компьютер.

Её выполнение необходимо для того, чтобы впоследствии можно было использовать ПК AvPCM для отправки и приема защищенных и подписанных сообщений в автоматизированной системе.

Пара ключей состоит из: личного ключа подписи/шифрования (доступ к которому имеет только владелец и который будет помещен на его носитель ключей в защищенном виде) и открытого ключа проверки подписи/шифрования (который владелец может свободно распространять вместе с его карточкой открытого ключа среди тех, с кем он собирается вести электронную переписку).

Действия при создании запроса на сертификат:

1) Выбрать из основного меню Windows: «Пуск»→«Программы»→«Авест»→ «Персональный менеджер сертификатов»→«Создать запрос на сертификат»;
2) В появившемся окне мастера создания запроса на сертификат выбрать шаблон для создания сертификата (см. Рисунок 9);

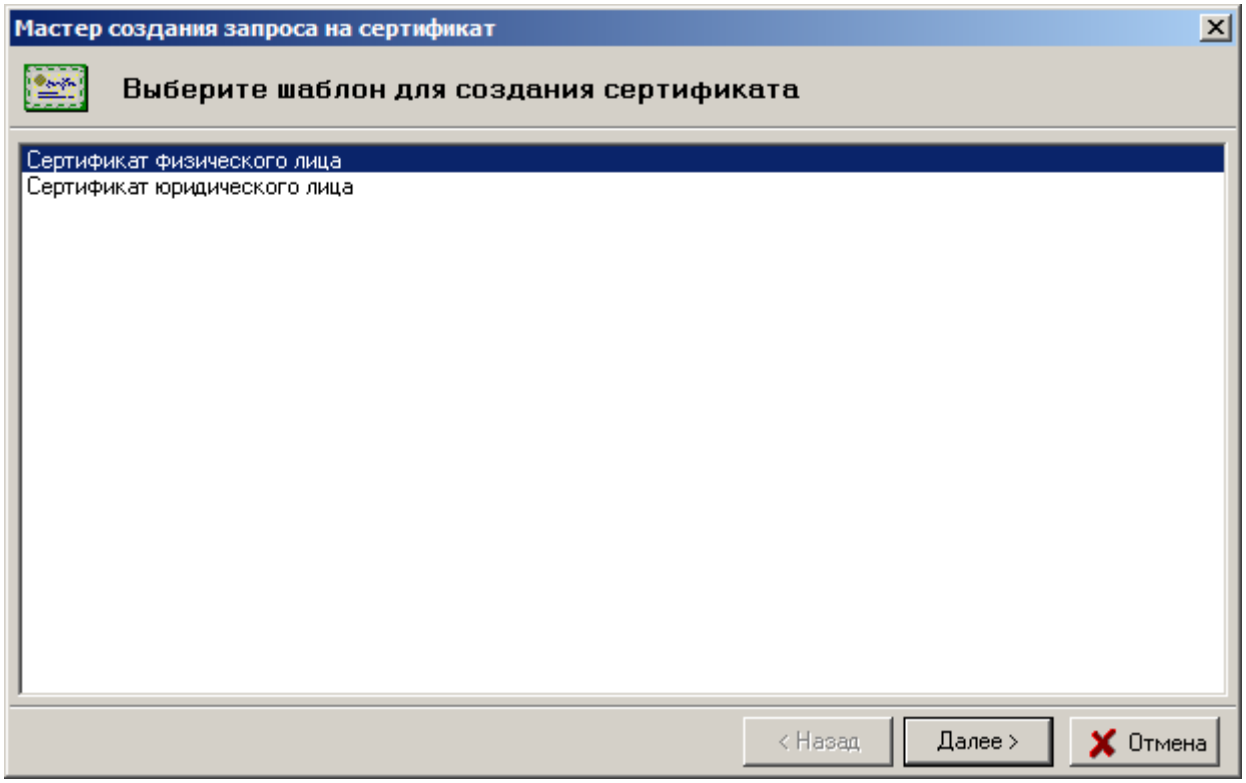

Рисунок 9. Выбор шаблона для создания сертификата

3) В следующем диалоговом окне надо задать атрибуты будущего владельца сертификата для карточки открытого ключа, включаемые в запрос на сертификат (см. **Рисунок 10**);

Обязательными полями для заполнения являются:

– «Наименование организации владельца открытого ключа» – полное наименование организации, на имя которой будет выпущен сертификат;
– «Страна» – двухбуквенный международный код страны, в которой зарегистрирована организация, в которой работает будущий владелец сертификата;
– «Населенный пункт» – наименование населенного пункта, в котором зарегистрирована организация, в которой работает будущий владелец сертификата;
– «Адрес» – юридический адрес организации, в которой работает будущий владелец сертификата.

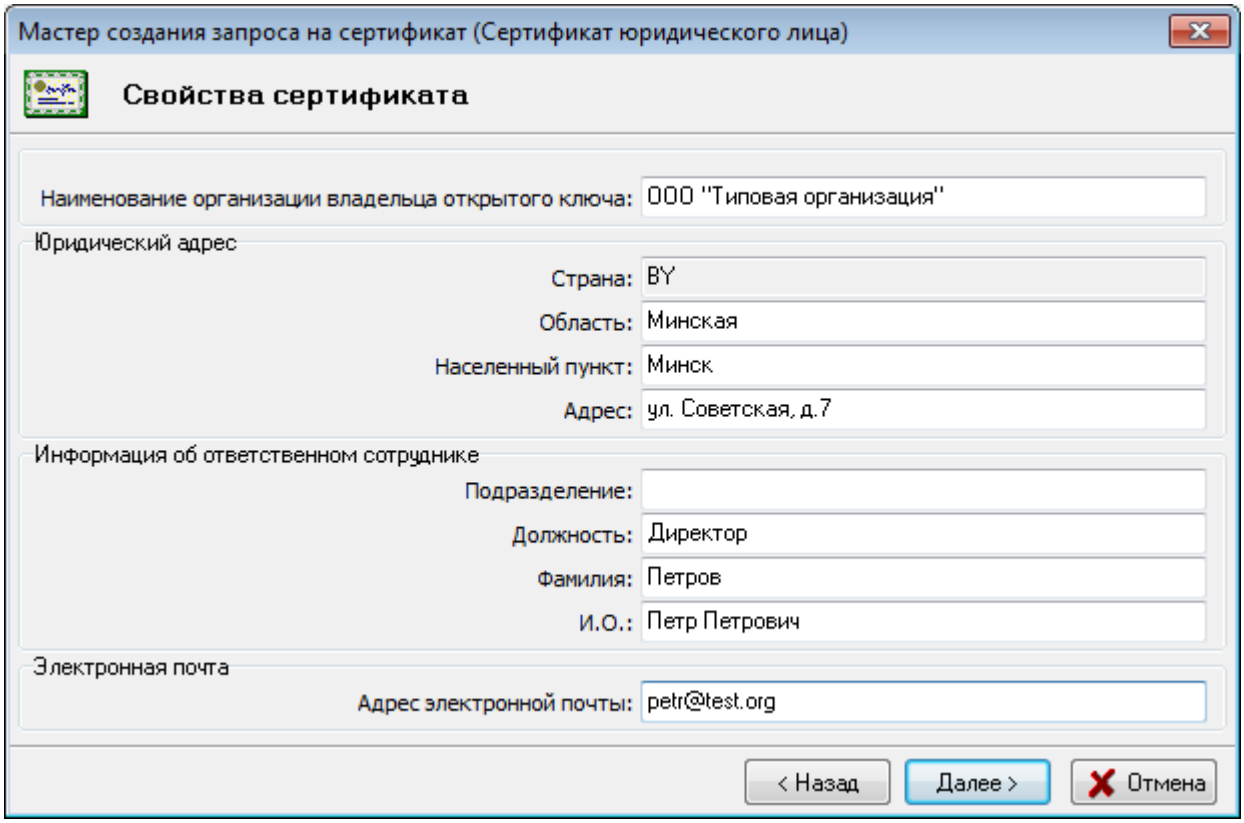

Рисунок 10. Заполнение атрибутов владельца сертификата

Необязательными для заполнения полями являются:

- «Подразделение» – наименование подразделения, в котором работает будущий владелец сертификата;
- «Должность» – должность лица, ответственного за работу с криптографическими ключами;
- «Фамилия» – фамилия лица, ответственного за работу с криптографическими ключами;
- «И.О.» – имя и отчество лица, ответственного за работу с криптографическими ключами.
- «Область» – наименование административно-территориальной единицы деления страны, в которой зарегистрирована организация владельца сертификата;
- «Адрес электронной почты» – адрес электронной почты, по которому можно будет связаться с администрацией организации или сотрудниками, ответственными за использование ключей, при возникновении проблем или для получения дополнительных разъяснений.

Внимание: Эти атрибуты в дальнейшем изменять не рекомендуется. В связи с этим обращаем особое внимание на тщательность выполнения первой генерации личного ключа и заполнения атрибутов пользователя.

В случае если, какое-либо из обязательных атрибутов не заполнен и была нажата кнопка «Далее», то программа сообщит об ошибке и предложит заполнить его значение.

Затем появится окно, в котором будет указано применение личного ключа пользователя (см. **Рисунок 11**).

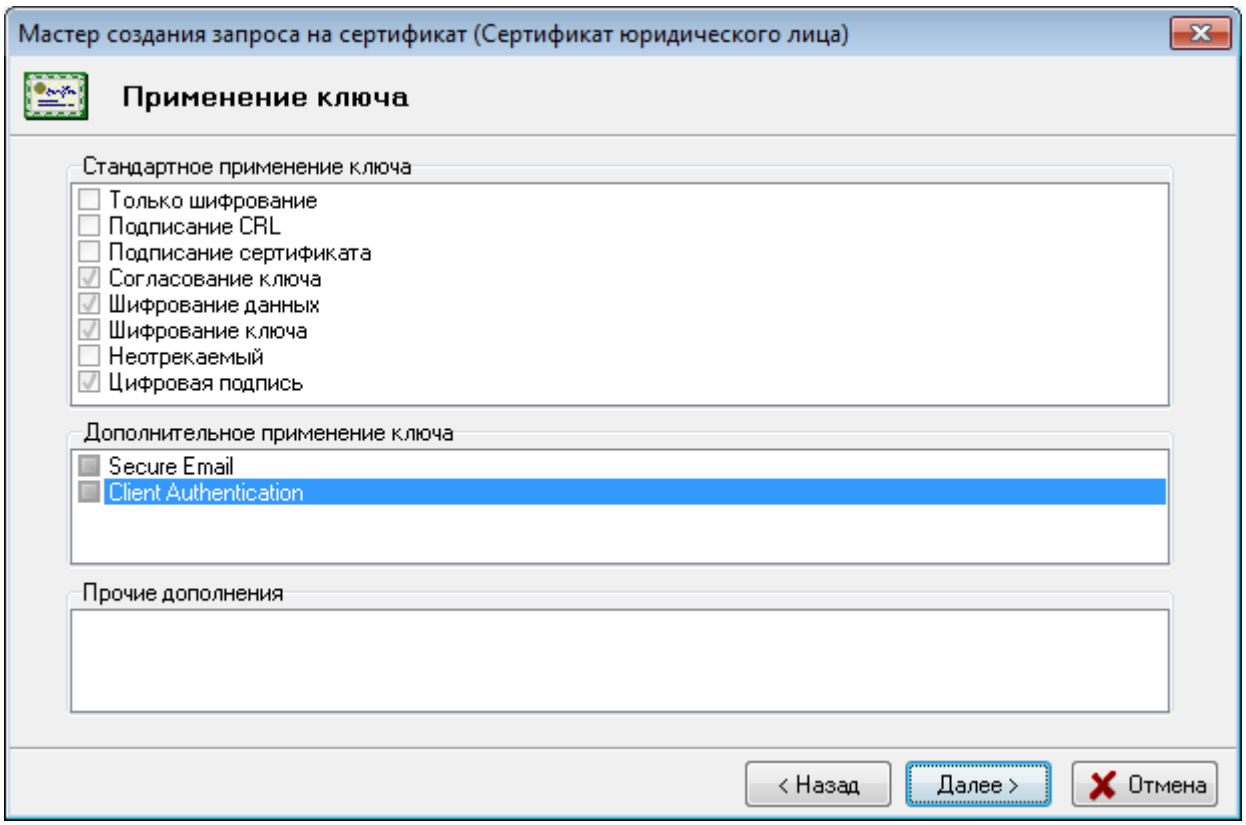

Рисунок 11. Применение личного ключа

4) В следующем диалоговом окне надо определить срок действия сертификата пользователя (см. **Рисунок 12**);

По умолчанию включен флажок «Срок действия сертификата задается удостоверяющим центром» и поля «действителен с» и «действителен по» заполнены значениями «0».

Если Вы хотите указать другой срок действия сертификата, то выключите флажок «Срок действия сертификата задается удостоверяющим центром» и введите нужный срок действия.

Если срок действия сертификата задается Удостоверяющим центром, то дата начала действия сертификата будет равна текущему времени обработки Вашего запроса в Удостоверяющем центре.

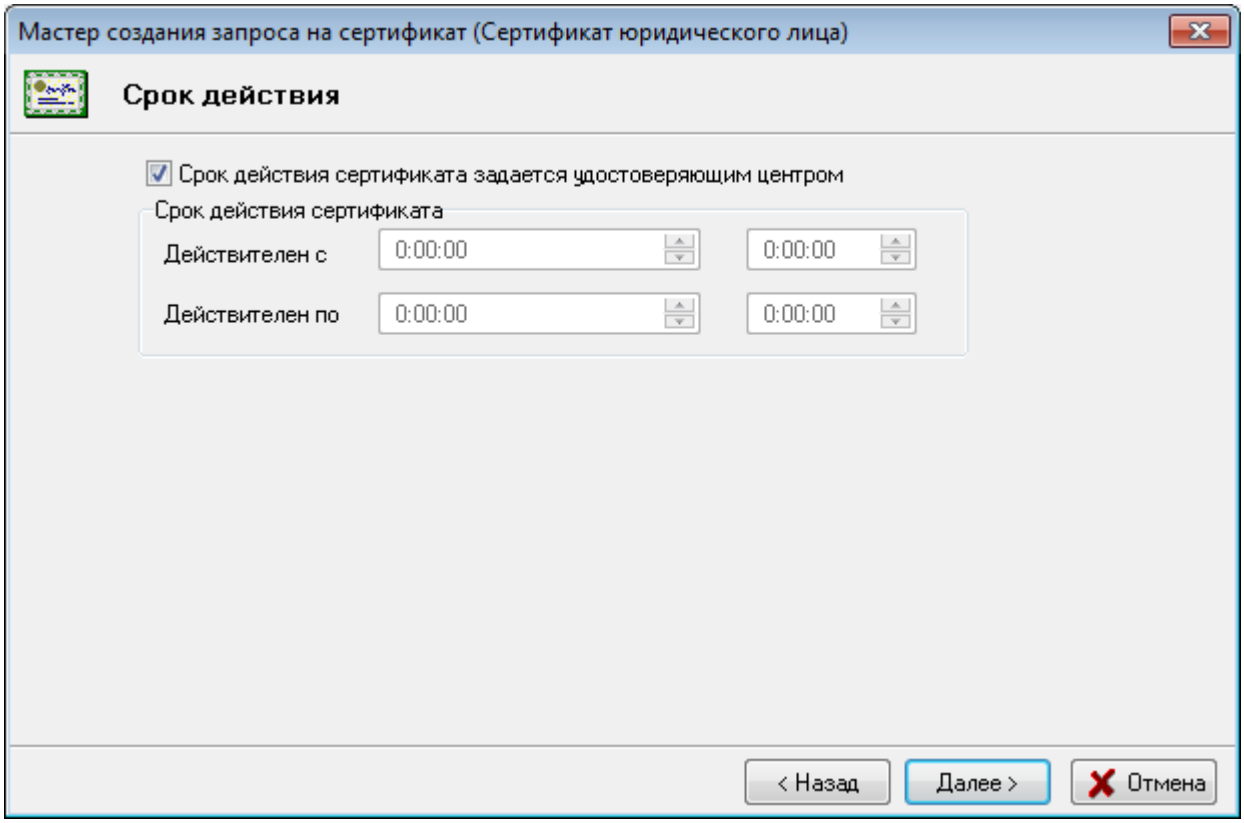

Рисунок 12. Ввод сроков действия сертификата

5) Затем, в появившемся окне, надо задать имя контейнера, в который будет помещен ваш личный ключ (см. **Рисунок 13**).

По умолчанию программа создаст контейнер личных ключей с именем « [Наименование организации владельца открытого ключа]_дд_мм_гг_чч_мм», где «дд_мм_гг_чч_мм»- это время генерации ключей.

Внимание: Обращаем внимание на то, что на этом этапе задается только логическое имя контейнера и оно никак не связано с реальными физическими устройствами. Рекомендуем не менять имя, задаваемое по умолчанию.

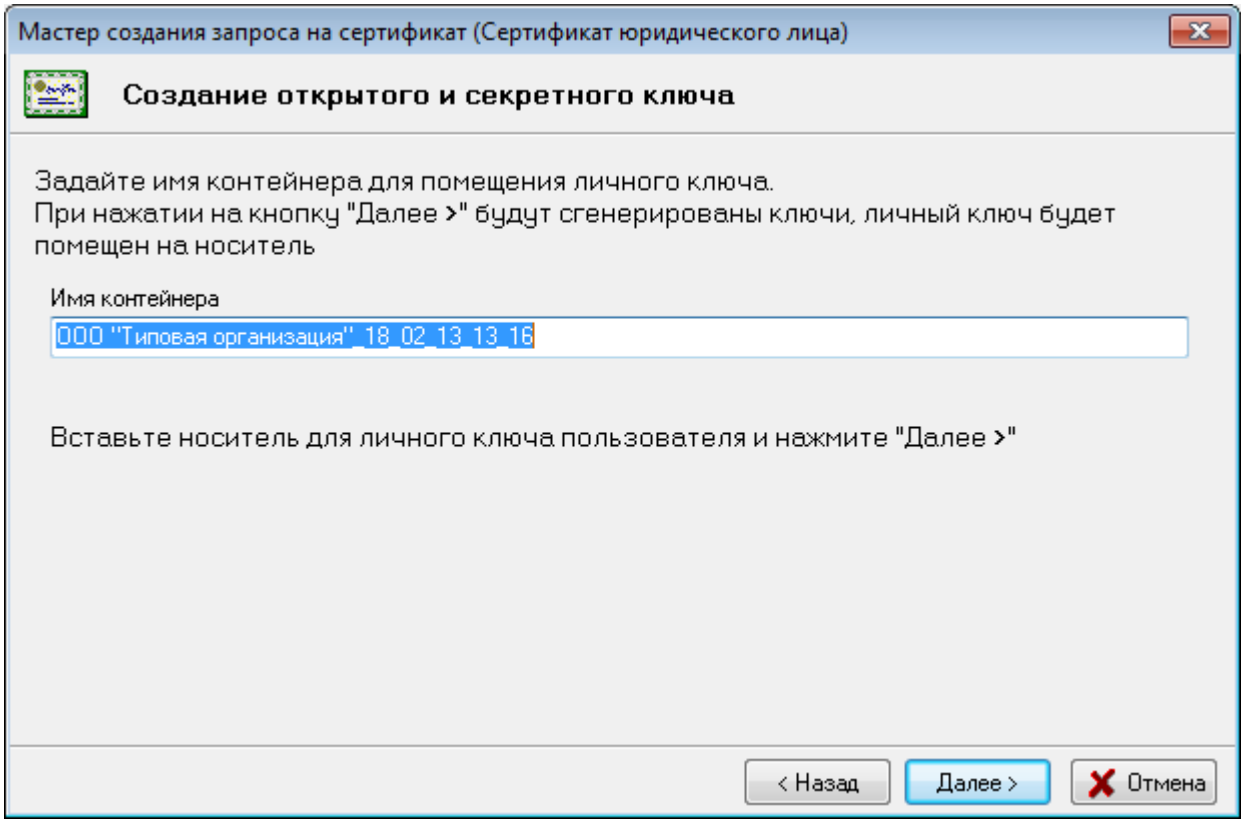

Рисунок 13. Инициализация носителя личного ключа

6) Для инициализации контейнера личных ключей в появившемся далее диалоговом окне необходимо выбрать из списка физический носитель ключей, ввести в соответствующих полях пароль и его подтверждение (см. **Рисунок 14**);

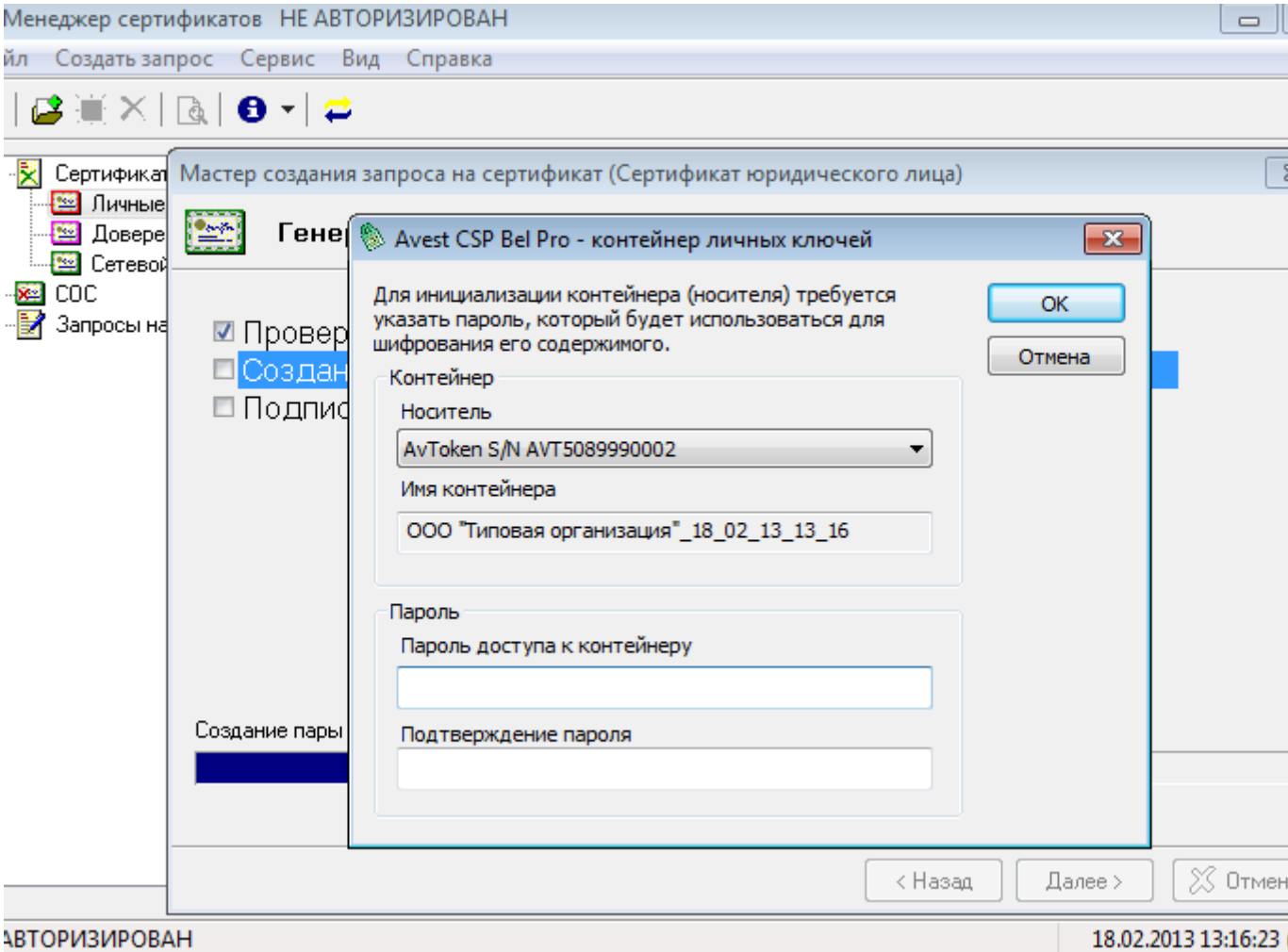

Рисунок 14. Выбор физического носителя личного ключа

7) Для создания личных ключей программе требуется некоторое количество случайных данных, поэтому подвигайте курсором мыши в пределах появившегося окна до полного заполнения полосы индикации (см. **Рисунок 15**);

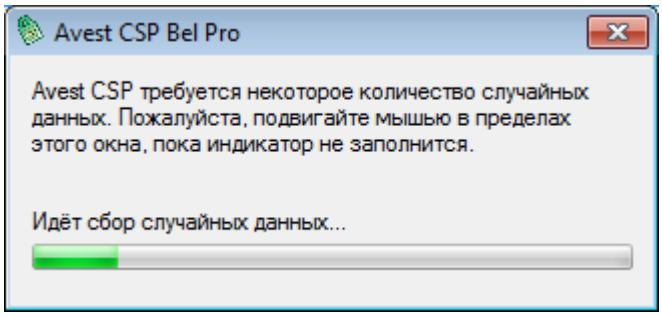

Рисунок 15. Окно «сбор случайных данных»

Информация о личном ключе хранится на носителе в криптоконтейнере в зашифрованном виде. Для доступа к ключу при его создании необходимо указать пароль, который в дальнейшем будет использоваться для доступа к ключу, например, при выработке электронной цифровой подписи документов. Пароль должен быть в длину не менее 8 символов и не может состоять из одинаковых символов.

Примечания:

1. Носители личных ключей некоторых производителей, например, Aladdin eToken имеют по умолчанию личный пароль с возможностью аппаратной блокировки доступа к носителю средствами самого носителя после некоторого количества попыток ввода неправильного пароля (см. документацию производителя). В силу этого все контейнеры на данных носителях личных ключей имеют одинаковый пароль, такой же, как пароль самого носителя, а количество попыток ввода пароля на доступ к контейнеру ограничено параметрами носителя при его форматировании.
2. В случае утраты личного ключа пользователя или пароля доступа к нему, следует произвести новую процедуру генерации пары ключей потому, что восстановление утерянного личного ключа и пароля к нему невозможно.
3. При использовании носителя AvToken в режиме AvToken strong семи попыток ввода неправильного пароля на доступ к личным ключам на носителе, происходит автоматическое удаление контейнера с личными ключами на носителе.
4. ПК AvPCM обеспечивает работу со всеми типами носителей ключей, которые поддерживает криптопровайдер AvCSP Bel.

8) После этого будет сформирована карточка открытого ключа, которую требуется распечатать (см. **Рисунок 16**).

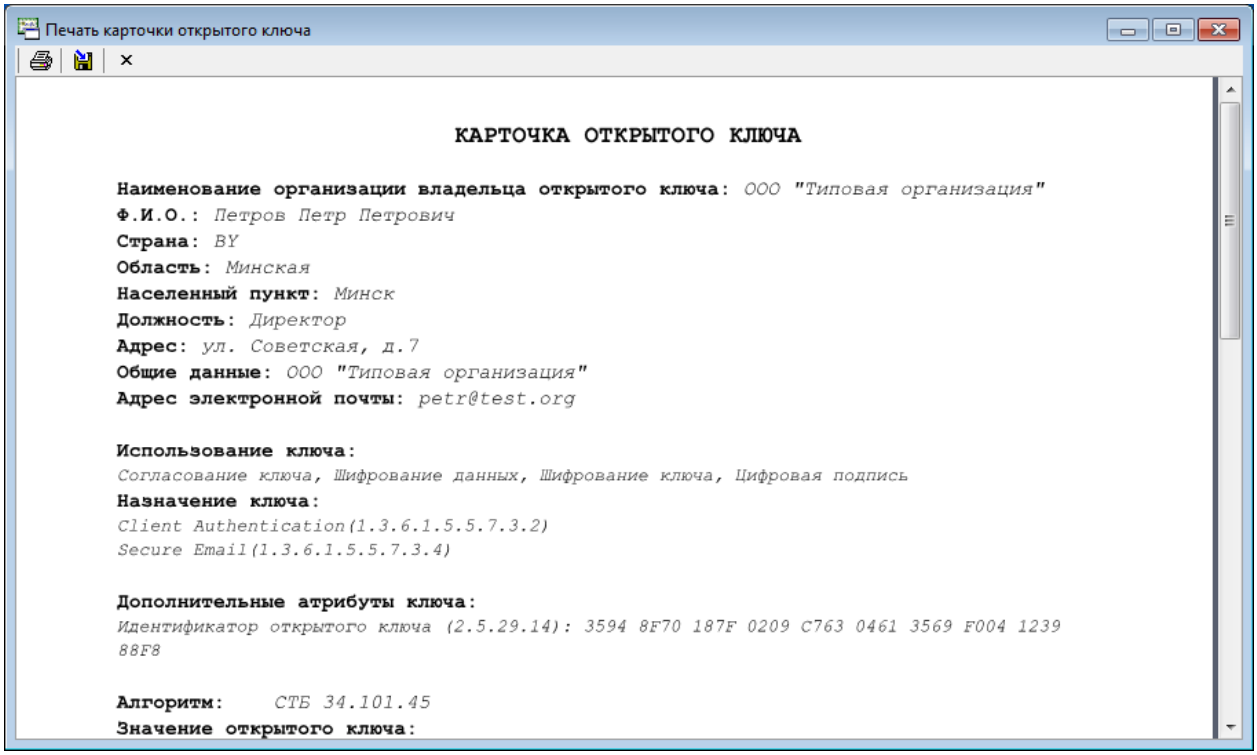

Рисунок 16. Карточка открытого ключа

Дальнейшие действия зависят от того, какой тип установки производился.

Если при инсталляции была выбрана установка с сетевой базой данных, то можно не экспортировать полученный запрос в файл, т.к. запрос автоматически пропадает в базу данных Удостоверяющего центра.

Если при инсталляции была выбрана установка с файловой базой данных, то в окне «Экспорт запроса в файл» мастера создания запроса на сертификат надо включить флажок «Экспортировать запрос в файл» и указать имя файла (см. Рисунок 17).

Имя файла можно ввести как вручную, так и с помощью кнопки «Обзор», для того, чтобы выбрать файл с использованием средств просмотра файловой системы Microsoft Windows.

С помощью кнопки «Просмотр» можно просмотреть запрос, который будет экспортирован в файл.

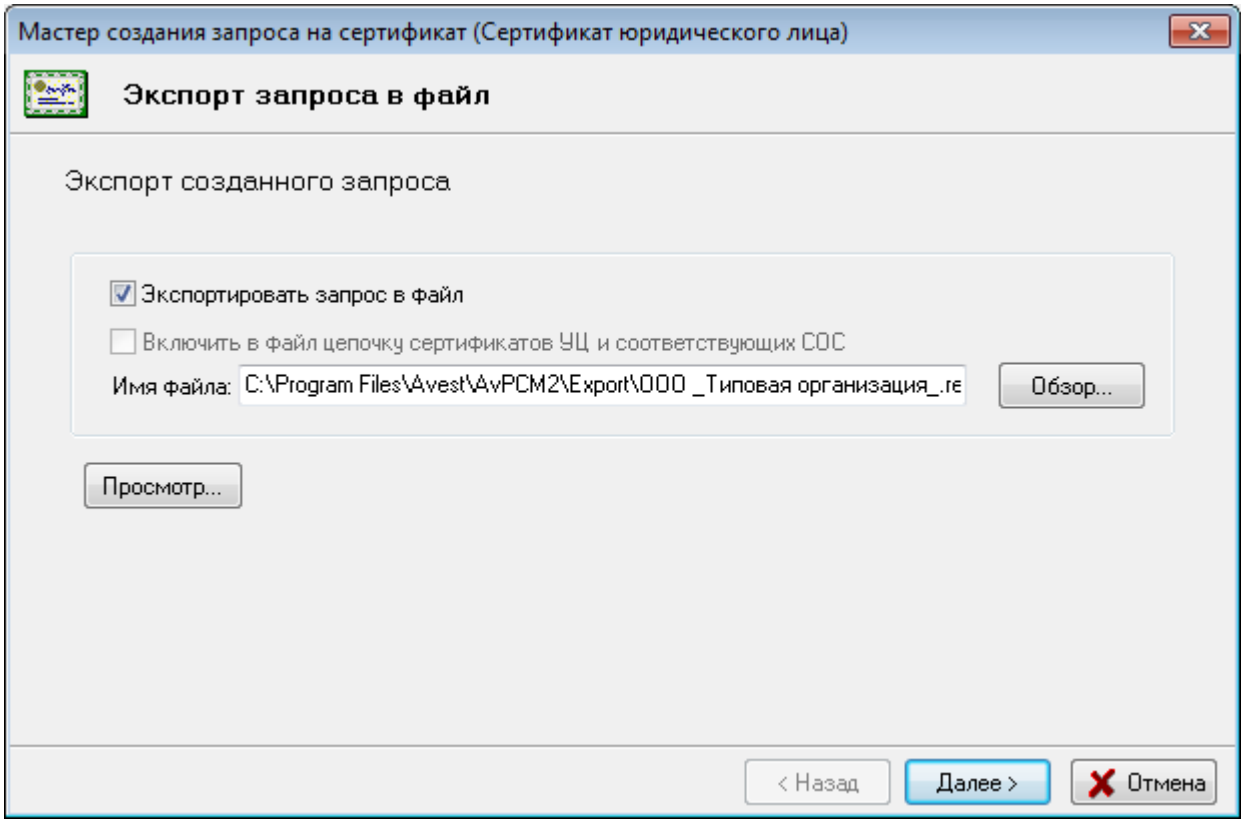

Рисунок 17. Сохранение запроса

В финальном окне мастер создания запроса на сертификат информирует о том, что запрос на сертификат создан. Для окончания работы с мастером сертификатов надо нажать кнопку «Закрыть».

Созданный запрос на сертификат, экспортированный в файл, и карточка открытого ключа, удостоверенная установленным образом, передаются в Удостоверяющий центр для получения на их основании сертификата пользователя.

6.2. Создание запроса на атрибутный сертификат

Предварительно следует авторизоваться в ПК AvPCM под тем сертификатом, на основании которого будет создаваться запрос на атрибутный сертификат.

Выбрать из основного меню пункт «Создать запрос» ⇒ «На атрибутный сертификат».

1) В окне мастера создания запроса на сертификат указать тип шаблона (см. Рисунок 18);

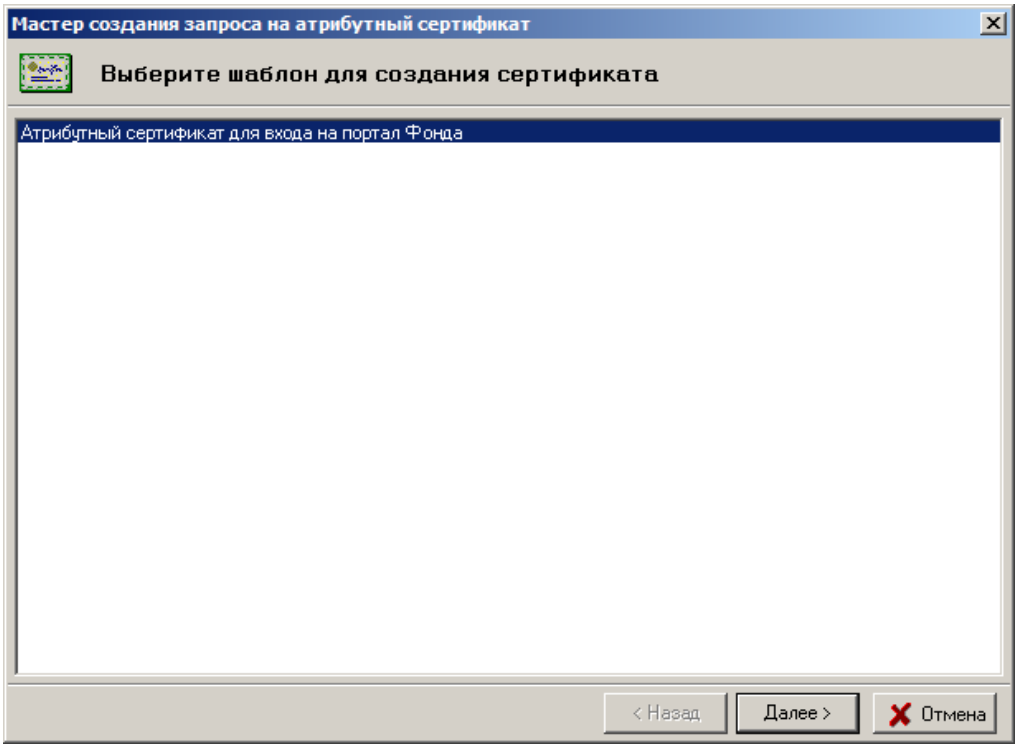

Рисунок 18. Выбор шаблона создания атрибутного сертификата

2) Далее будут выведены сведения о сертификате пользователя, на основании которого будет сформирован атрибутный сертификат (см. Рисунок 19);

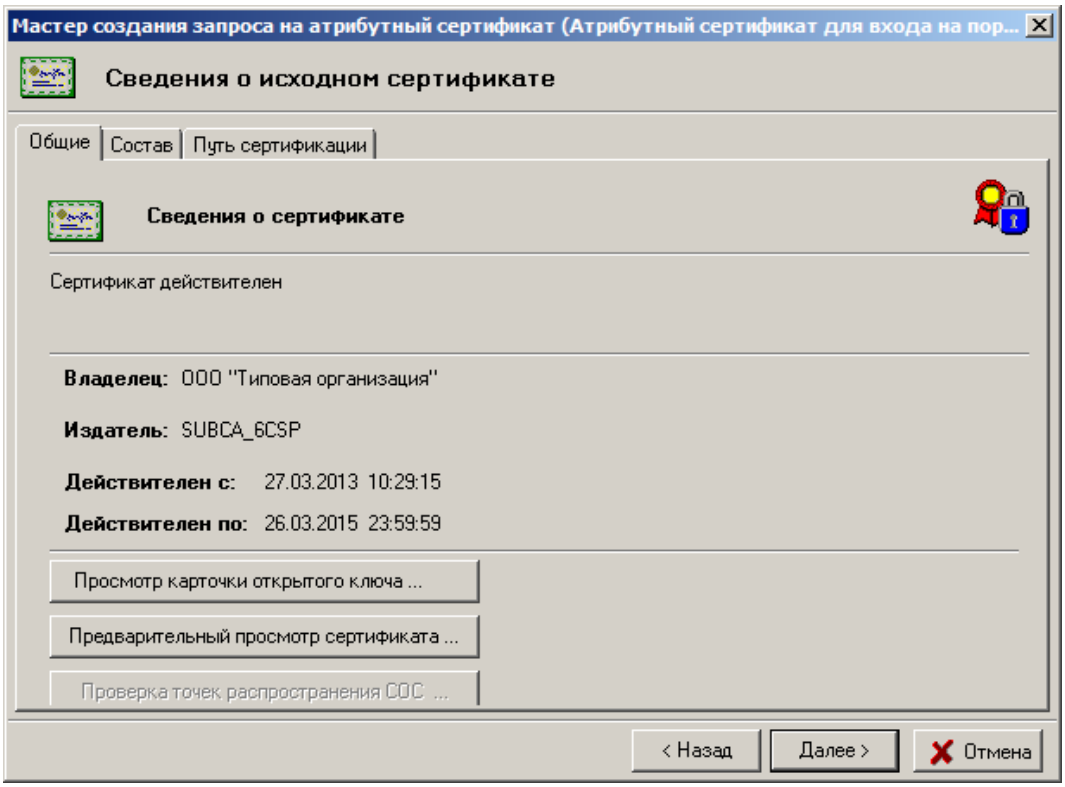

Рисунок 19. Сведения об исходном сертификате

В этом окне также можно просмотреть и распечатать карточку открытого ключа пользователя для этого надо нажать на кнопку «Просмотр карточки открытого ключа…» и информацию о сертификате, нажав на кнопку «Предварительный просмотр сертификата…».

3) В следующем окне следует указать данные по применению, которые будут включены в атрибутный сертификат (см. **Рисунок 20**).

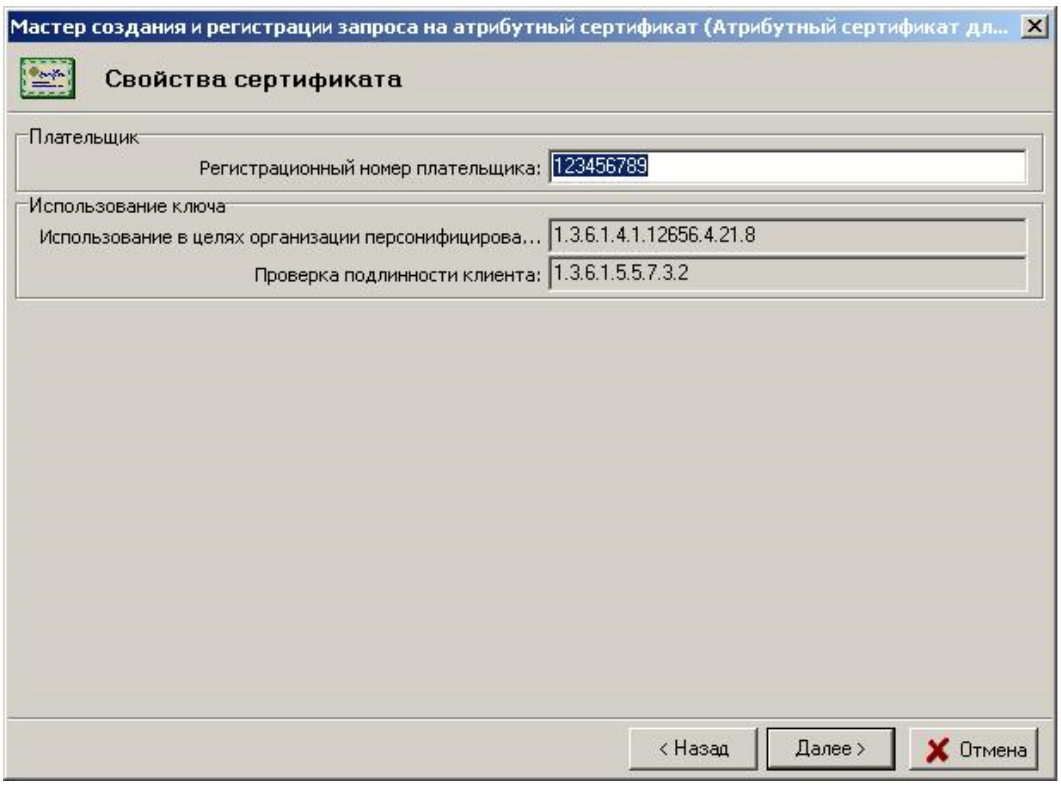

Рисунок 20. Заполнение свойств атрибутного сертификата

4) Затем необходимо определить срок действия сертификата пользователя (см. **Рисунок 12**);

5) В окне «Экспорт запроса на атрибутный сертификат в файл» следует надо включить флажок «Экспортировать запрос на атрибутный сертификат в файл» и указать имя файла (см. Рисунок 21).

Имя файла можно ввести как вручную, так и с помощью кнопки «Обзор», для того, чтобы выбрать файл с использованием средств просмотра файловой системы Microsoft Windows.

С помощью кнопки «Просмотр» можно просмотреть запрос, который будет экспортирован в файл.

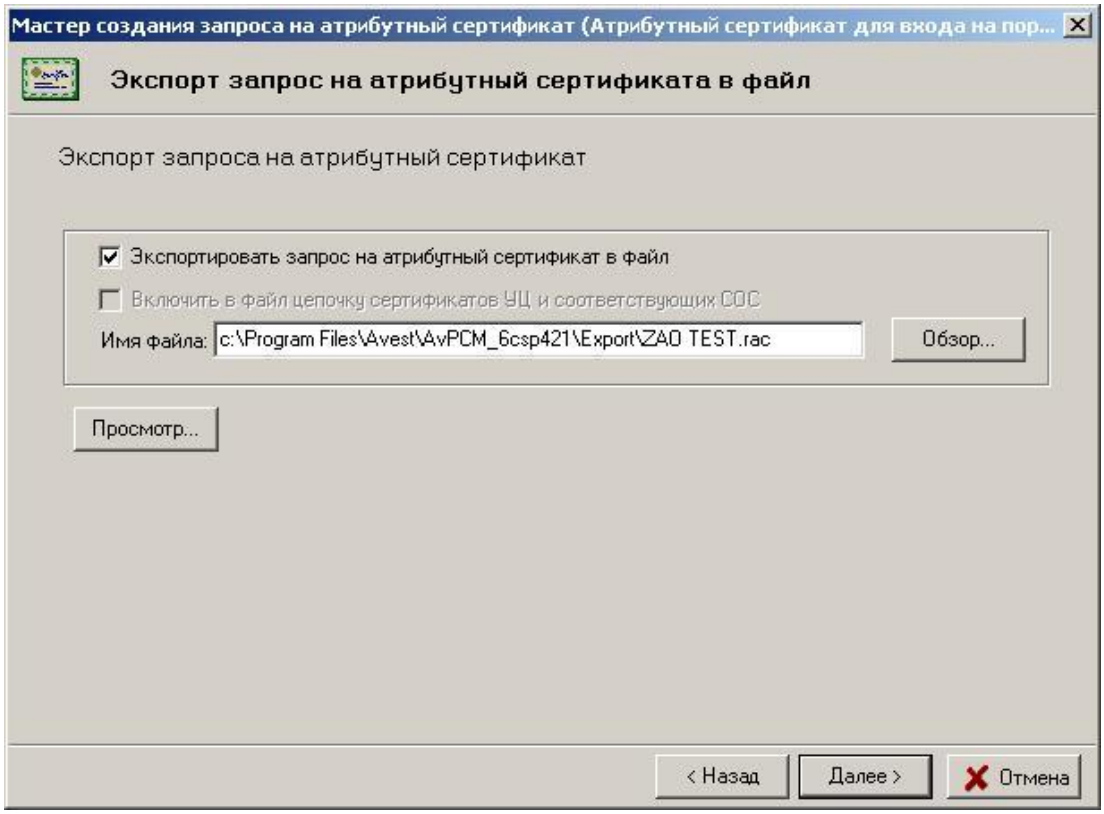

Рисунок 21. Сохранение запроса на атрибутный сертификат

6.3. Создание запроса на обновление личного сертификата

Обновление сертификата пользователя рекомендуется проводить до истечения срока действия текущего сертификата пользователя.

Действия по созданию запроса на обновление личного сертификата:

Выбрать из основного меню пункт «Создать запрос» ⇒ «На обновление личного сертификата».

Дальнейшие действия по созданию запроса на обновление личного сертификата аналогичны описанным при создании первого запроса на сертификат. Особенностью данного создания запроса является то, что информация о будущем владельце сертификата заполняется автоматически на основании той, которая указанна в текущем (активном в настоящее время) сертификате, находящемся в справочнике «Личные».

Сгенерированный таким образом новый запрос на сертификат можно передать в Удостоверяющий центр и продолжать работать со старыми личными ключами и сертификатом до операции импорта в базу данных программы нового (обновленного) личного сертификата.

После того как из Удостоверяющего центра получен новый личный сертификат, необходимо импортировать его в программу ПК AvPCM.

Процедура импорта в программу обновленного личного сертификата пользователя описана в следующем пункте данного документа.

6.4. Подключение личного сертификата при инсталляции с сетевой базой данных

После того, как в Удостоверяющем центре, в соответствии с установленным регламентом, пользователю будут переданы: личный сертификат пользователя, сертификаты корневого и подчиненного УЦ, необходимые для работы карточки открытого ключа УЦ и СОС корневого УЦ, – он должен произвести их импорт в программу ПК AvPCM.

Особенностью подключения личного сертификата при инсталляции программы с сетевой базой данных является то, что личный сертификат пользователя не импортируется в базу данных, потому, что он уже там находится.

Действия при подключении личного сертификата при инсталляции с сетевой базой данных:

1) Из основного меню Windows выбрать поочередно: «Пуск»→«Программы»→«Авест»→ «Персональный менеджер сертификатов»→«Импорт сертификатов»;
2) В диалоговом окне мастера импорта сертификатов, надо указать имя каталога, из которого будет производиться импорт: личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и СОС, выпущенных УЦ;
3) В появившемся далее окне в виде таблицы будут отражены все объекты, которые входят в импортируемый файл и могут быть подключены для работы.

   Выделив соответствующий объект в таблице, можно просмотреть информацию, содержащуюся в файле, для этого надо нажать кнопку «Просмотр».

   Для продолжения процедуры импорта после выбора импортируемых объектов надо нажать кнопку «Далее» (см. **Рисунок 22**).

   Внимание: В окне с таблицей импортируемых объектов не выделен ни один объект, т.е. не включена галочка в столбце «Субъект», т.к. импортируемые сертификаты и СОС уже находятся в базе данных программы.

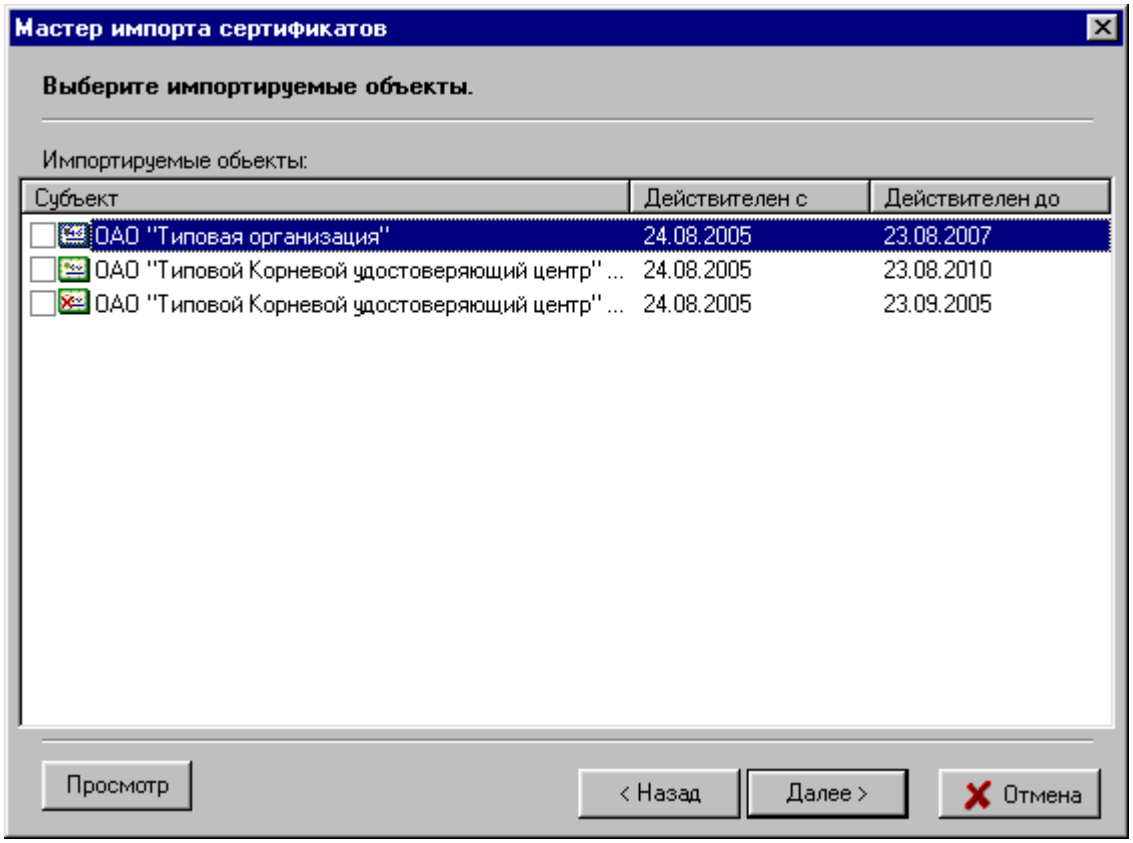

Рисунок 22. Информация об импортируемых объектах

4) В следующем окне содержится информация о количестве импортированных объектов и предложено поместить личный сертификат в персональный справочник. Т.к. импортируемые сертификаты и СОС уже находятся в базе данных программы, то в информации о количестве импортированных сертификатов будет указан «0» (см. **Рисунок 23**).

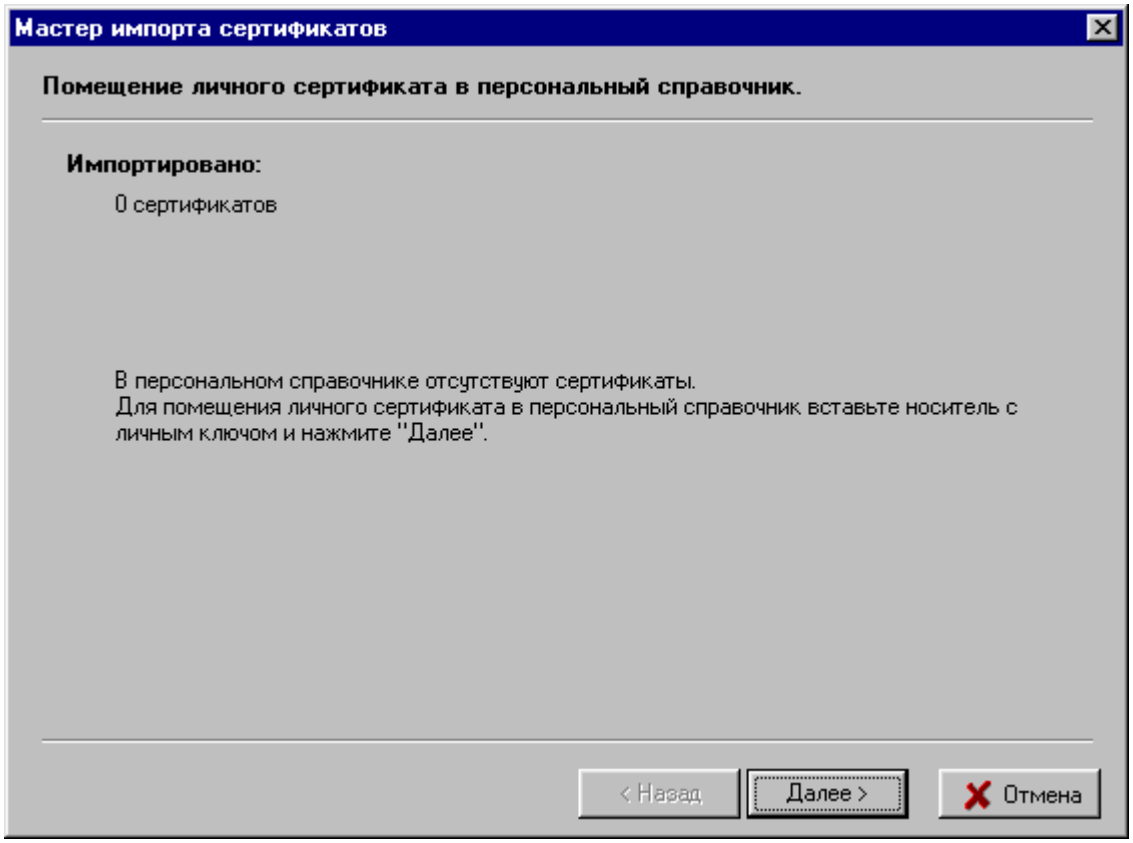

Рисунок 23. Помещение личного сертификата в персональный справочник

Для помещения личного сертификата в персональный справочник необходимо вставить носитель с Вашим личным ключом подписи/шифрования в считывающее устройство и нажать кнопку «Далее».

Будет проведена проверка носителя ключей и в появившемся окне будет выведена информация обо всех находящихся на данном носителе личных ключах.

Для продолжения процедуры помещения личного сертификата в персональный справочник надо из данного списка выбрать контейнер личного ключа, который соответствует личному сертификату, и нажать кнопку «Далее».

5) Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» необходимо ввести пароль, который Вы вводили при генерации личных ключей.

6) Следующим шагом является установка доверия к корневому сертификату Удостоверяющего центра. Для этого в появившемся окне надо включить флажок «Установить доверие сертификату корневого УЦ» (см. Рисунок 24).

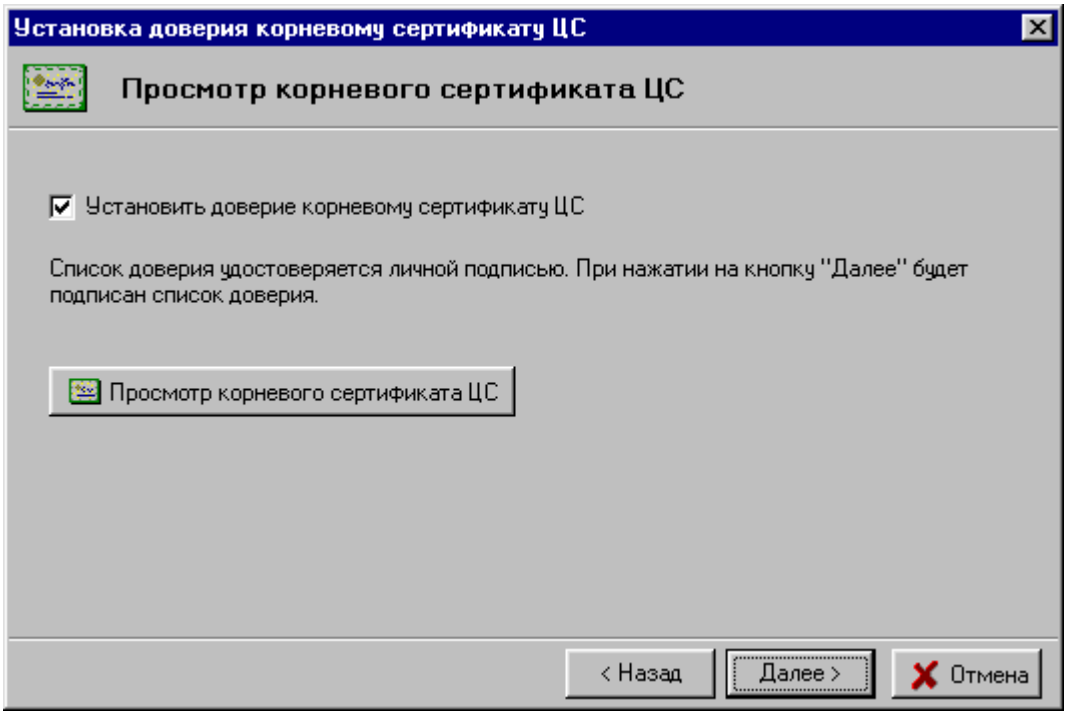

Рисунок 24. Просмотр корневого сертификата УЦ

В следующем окне программа сообщит о помещении корневого сертификата УЦ в список доверия. Здесь надо нажать на кнопку «Закрыть».

6.5. Импорт личного сертификата при инсталляции с файловой базой данных

Действия по импорту личного сертификата при инсталляции с файловой базой данных:

1) Из основного меню Windows выбрать поочередно: «Пуск»→«Программы»→«Авест»→ «Персональный менеджер сертификатов»→«Импорт сертификатов»;
2) В диалоговом окне мастера импорта сертификатов, надо указать имя каталога, из которого будет производиться импорт: личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и СОС, выпущенных УЦ (см. **Рисунок 25**);

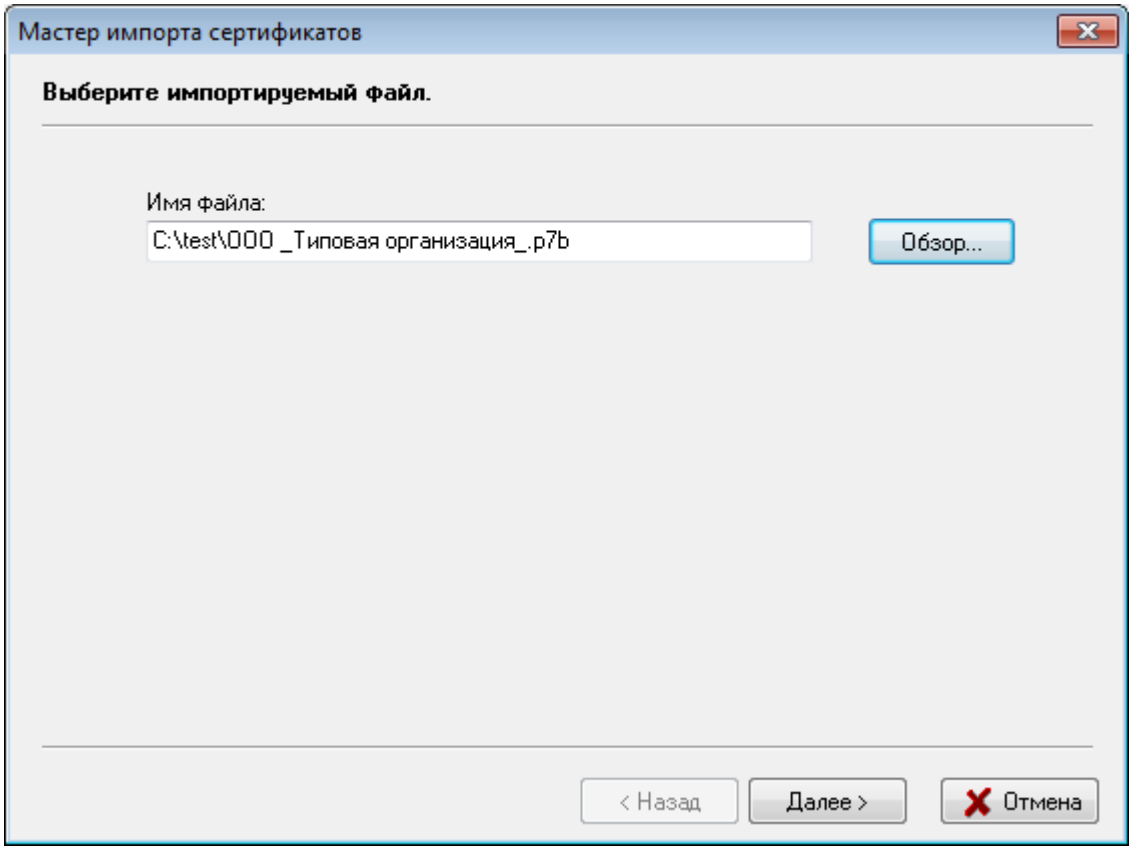

Рисунок 25. Выбор файла импортируемых данных

3) В появившемся окне в виде таблицы будут отражены все объекты, которые входят в импортируемый файл и могут быть подключены для работы (см. **Рисунок 26**).

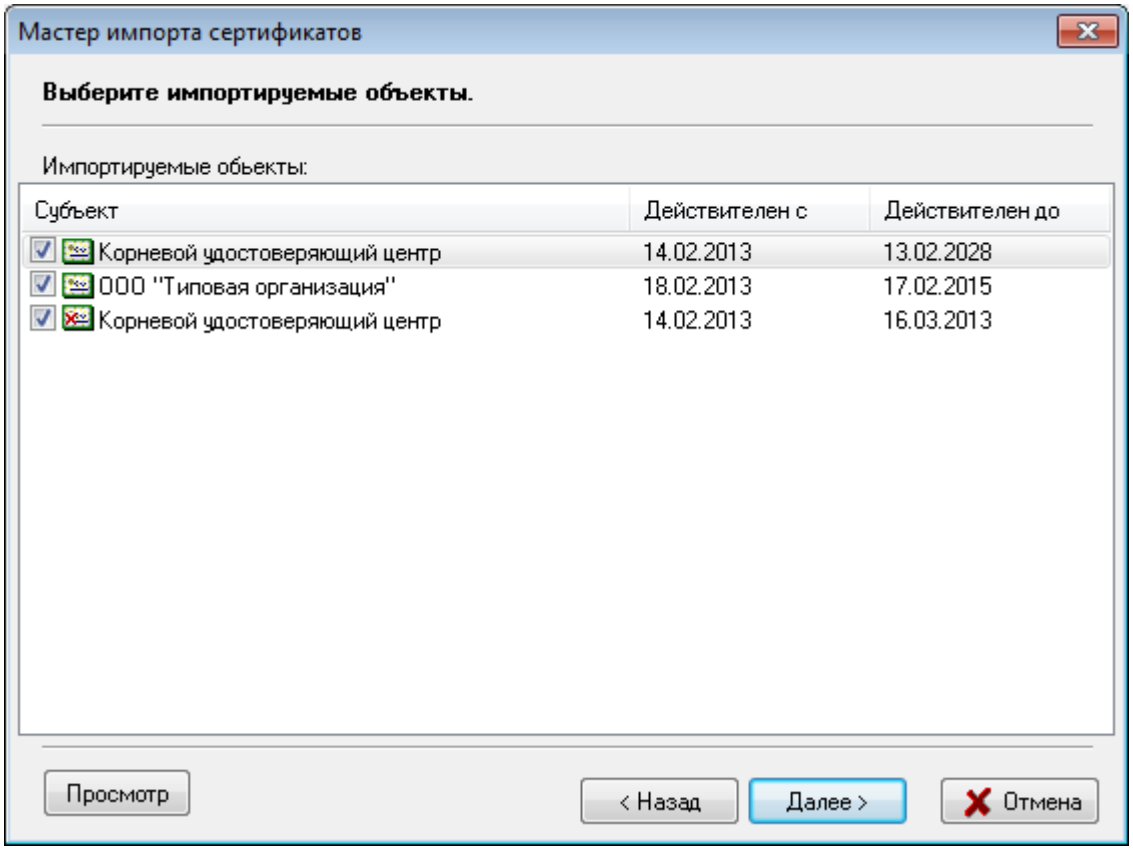

Рисунок 26. Информация об импортируемых объектах

Выделив соответствующий объект в таблице, можно просмотреть информацию, содержащуюся в файле, для этого надо нажать кнопку «Просмотр».

Убедившись в соответствии информации содержащейся в файле той, что представлена в карточке открытого ключа (для сертификата УЦ), Вы можете принять решение об установке элемента в своей системе (снять или установить «галочку» в столбце «Субъект»).

Для продолжения процедуры импорта после выбора импортируемых объектов надо нажать кнопку «Далее».

Внимание: При импорте своего личного сертификата в первый раз рекомендуем выделить и импортировать все отображаемые в данном окне объекты.

4) В следующем окне содержится информация о количестве импортированных объектов и предложено поместить личный сертификат в персональный справочник (см. **Рисунок 27**).

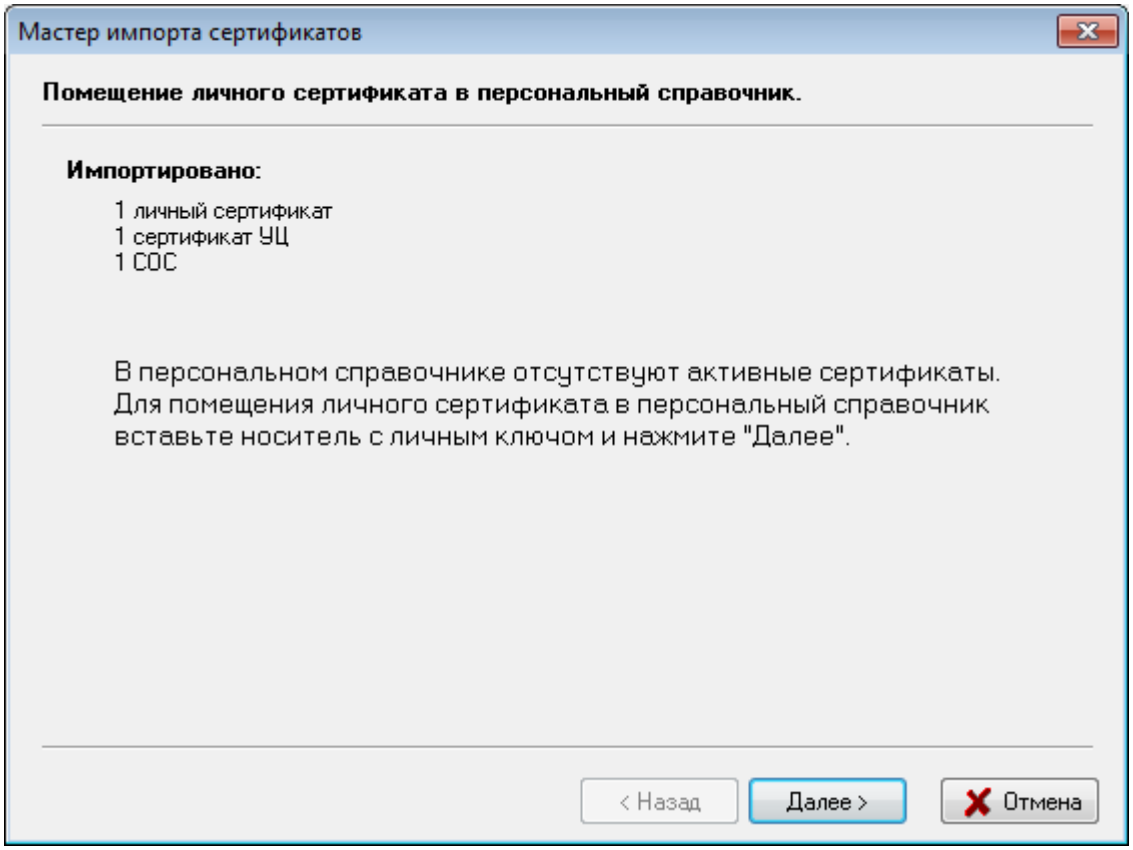

Рисунок 27. Помещения личного сертификата в персональный справочник

Т.к. это Ваш первый импорт личного сертификата в программу ПК AvPCM, то в персональном справочнике сертификатов он отсутствует. Поэтому, для помещения личного сертификата в персональный справочник необходимо вставить носитель с Вашим личным ключом подписи/шифрования в считывающее устройство и нажать кнопку «Далее».

Будет проведена проверка носителя ключей и в появившемся окне будет выведена информация обо всех находящихся на данном носителе личных ключах.

Для продолжения процедуры помещения личного сертификата в персональный справочник надо из данного списка выбрать контейнер личного ключа, который соответствует личному сертификату и нажать кнопку «Далее» (см. **Рисунок 28**).

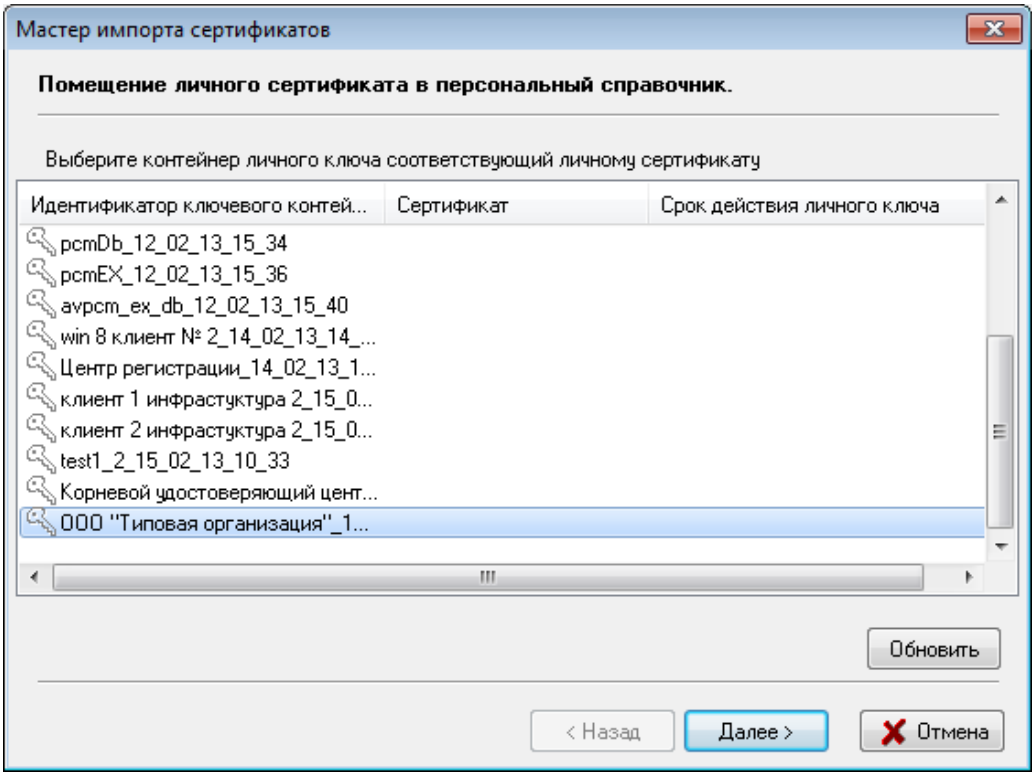

Рисунок 28. Выбор контейнера личного ключа соответствующего личному сертификату

Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» необходимо ввести пароль, который Вы вводили при генерации личных ключей (см. **Рисунок 29**).

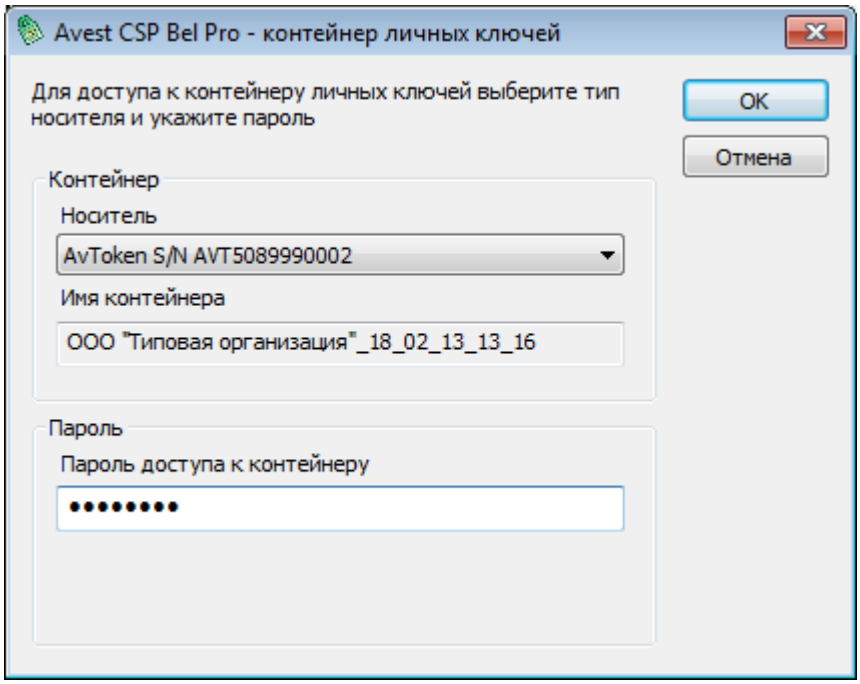

Рисунок 29. Ввод пароля доступа к контейнеру личного ключа

На этом процесс добавления вашего личного сертификата в персональный справочник сертификатов «Персонального менеджера сертификатов Авест» завершен.

5) Для полнофункциональной работы программы необходимо установить доверие к корневому сертификату УЦ. Для этого в следующем окне надо включить флажок «Установить доверие сертификату корневого УЦ» (см. **Рисунок 30**).

Внимание: Для того чтобы убедиться в том, что карточка открытого ключа Удостоверяющего центра переданная пользователю соответствует сертификату корневого УЦ надо нажать на кнопку «Просмотр сертификата корневого УЦ».

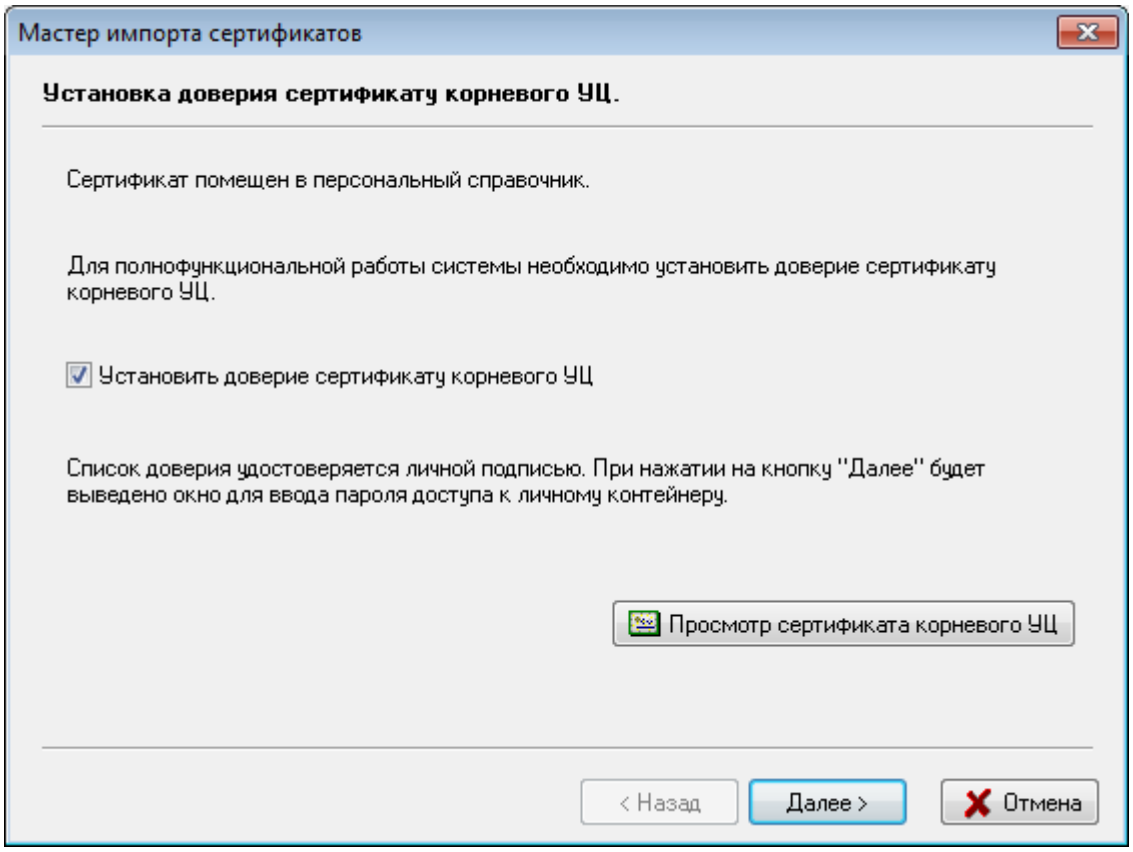

Рисунок 30. Установка доверия сертификату корневого УЦ

После этого будет выведено сообщение о том, что корневой сертификат УЦ помещен в список доверия и мастер импорта сертификатов завершил работу (см. **Рисунок 31**).

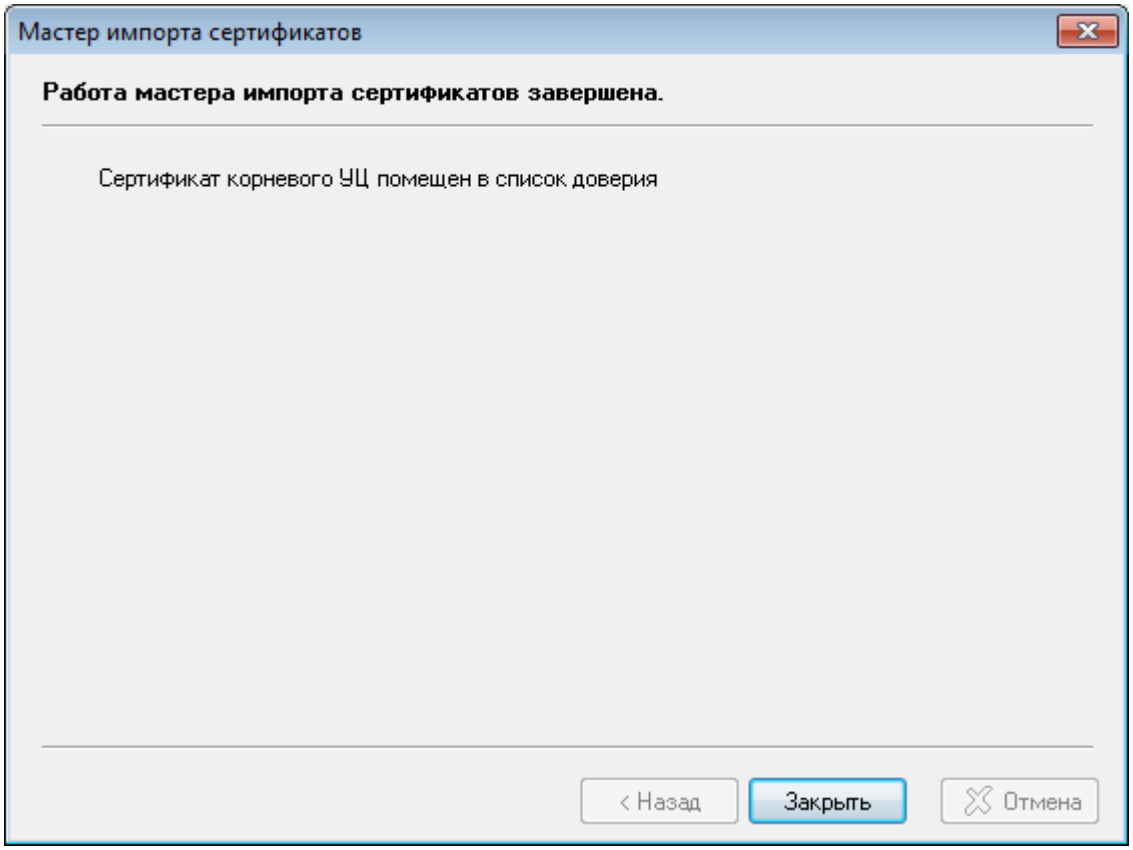

Рисунок 31. Завершение работы мастера импорта сертификатов

6.6. Главное окно программы

После запуска программы ПК AvPCM и прохождения процедуры авторизации на экране появится главное окно программы (см. **Рисунок 32**).

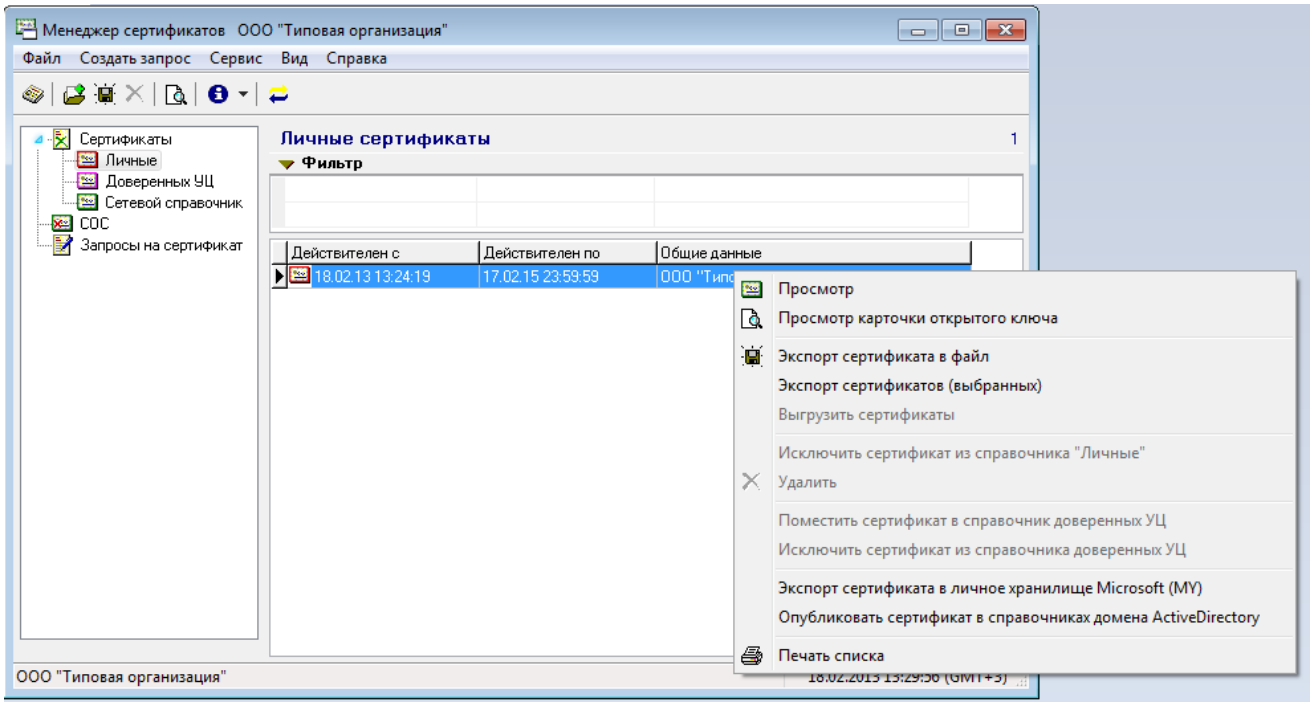

Рисунок 32. Интерфейс программы ПК AvPCM

Используя стандартные средства пользовательского интерфейса, такие как главное меню, панели инструментов и контекстные меню, пользователь может выполнять все операции, связанные с генерацией личных ключей подписи и шифрования, формированием запроса на сертификат, просмотром журнала событий и т.п.

Главное окно программы разделено на две половины для визуализации базы данных сертификатов пользователя.

В левой половине располагается дерево справочников, в которых хранится информация по сертификатам, спискам отозванных сертификатов и запросам на сертификат.

В правой половине главного окна отражается детализация информации, хранящейся в справочниках (сертификаты, списки отозванных сертификатов, запросы на сертификат).

Если в левой половине выбран конкретный объект, то в правой половине окна отображается содержание этого объекта.

Каждый объект, хранящийся в базе данных, представлен в Главном окне программы в виде иконки.

Например:

– – список отозванных сертификатов (СОС);

– – запрос на сертификат;

–  – сертификат, находящийся в базе данных недействителен в данный момент (отозван, срок действия сертификата ещё не наступил);

–  – срок действия сертификата, находящегося в базе данных программы, временно приостановлен;

–  – сертификат, находящийся в базе данных программы действителен;

–  – сертификат действителен и был использован при входе в программу.

С помощью фильтра, расположенного в правой половине окна, можно осуществлять поиск сертификатов по разным параметрам (наименование организации владельца открытого ключа, серийный номер и др.).

Для этого надо щелкнуть по значку ►рядом со словом «Фильтр». Появиться дополнительное окошко для поиска нужной информации и значок изменит свою форму на ▼ «Фильтр». В появившемся дополнительном окошке надо стать курсором в графу с тем параметром, по которому будет проводиться отбор, и ввести одно из значений интересующего Вас сертификата. В нижнем окошке появятся все сертификаты соответствующие заданному параметру.

Параметры, по которым может производиться поиск сертификата:

– поиск только по начальным буквам, если после них установлен знак «%»;
– поиск по указанному сочетанию букв, если указана, какая либо буква или сочетание букв;
– поиск по диапазону, если в верхней строке указан начальный атрибут, а в нижней конечный, то будут отражены все сертификаты атрибуты, которых входят в заданный диапазон;
– поиск по любому символу, если в поле для поиска стоит знак «_»,

Например, если в столбце «Адрес» ввести буквы адреса держателя сертификата, то в нижнем окне будут отражены все сертификаты владельцы, которых имеют в своем адресе эти буквы.

В программе ПК AvPCM предусмотрена возможность вывода на печать списка сертификатов, находящихся в базе данных.

Можно печатать как полный список сертификатов со всеми параметрами сертификатов, так и только с нужными вам колонками и строками. Добавление и скрытие полей выводимых на печать описано в подразделе «Просмотр содержимого справочников».

Для печати сертификатов необходимо выполнить приведенные ниже шаги:

1) Выбрать справочник, из которого сертификаты должны попасть в реестр;
2) В правой панели Главного окна программы щелкнуть правой клавишей мыши по сертификату и во всплывающее меню выбрать пункт «Печать списка»;

3) В появившемся окне можно просмотреть список сертификатов, и нажав на соответствующую пиктограмму в меню распечатать (см. **Рисунок 33**).

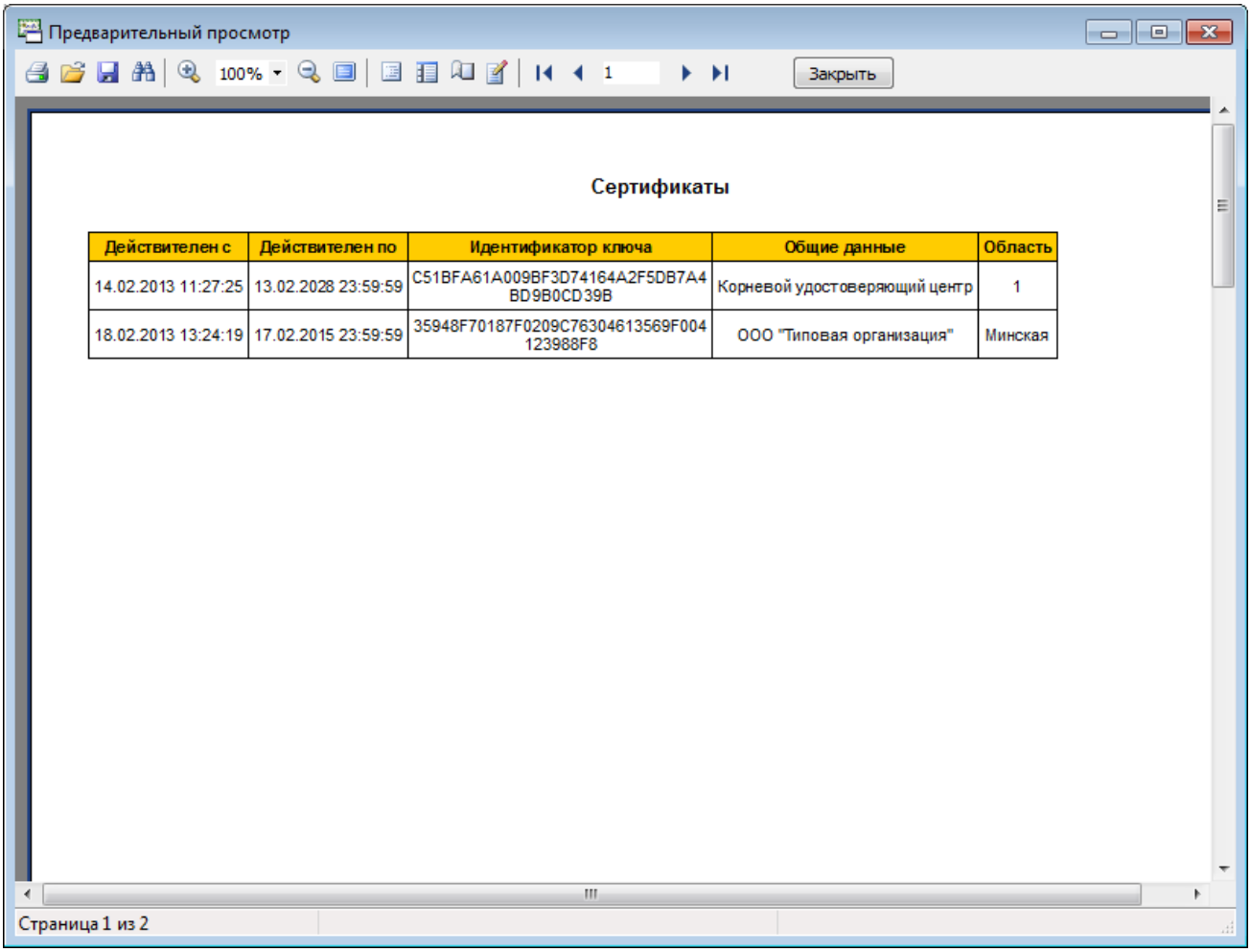

Рисунок 33. Список сертификатов

Основное меню Главного окна программы для наглядности представим в виде таблицы, в которой будут указаны все элементы, входящие в него (см. Таблица 1).

Таблица 1.

Пункт основного меню	**Пункт подменю**	**Пояснение**
Файл		Основные функции работы с файлами. Выход из программы
	Экспорт сертификата в файл (Экспорт СОС в файл/ Экспорт запроса в файл)	Позволяет сохранить в файл данные выбранного в окне программы объекта (сертификата/ СОС/ запроса на сертификат в зависимости от выбранного справочника).

Пункт основного меню	Пункт подменю	Пояснение
	Импорт сертификата/СОС	Позволяет установить для использования сертификаты и/или СОС из определенного пользователем каталога.
	Открыть запрос на сертификат	Позволяет просмотреть содержимое файла с запросом на сертификат.
	Удалить	Удаляет установленный в системе сертификат. Удаление из любого справочника разрешено только в случае если срок действия объекта истек.
	Печать списка	Позволяет произвести печать реестра сертификатов хранящихся в базе данных.
	Параметры печати	Позволяет произвести настройку печати.
	Выход	Осуществляет выход из программы.
Создать запрос		Реализует функции для получения сертификата.
	Подготовить запрос на сертификат	Позволяет сгенерировать новую пару ключей, сформировать карточку открытого ключа пользователя, поместить в файл запрос на выпуск нового сертификата для передачи в Удостоверяющий центр.
	Используя данные сертификата (запроса)	Позволяет сгенерировать новую пару (личный/открытый ключ), сформировать карточку открытого ключа пользователя, поместить в файл запрос на обновление любого сертификата (запроса), который находится в базе данных, для передачи в Удостоверяющий центр.
	Используя данные личного сертификата	Позволяет сгенерировать новую пару (личный/открытый ключ), сформировать карточку открытого ключа пользователя, поместить в файл запрос на выпуск сертификата, созданного на основании личного сертификата, для передачи в Удостоверяющий центр.
	На атрибутный	Сформировать и поместить в файл запрос на выпуск

Пункт основного меню	Пункт подменю	Пояснение
	сертификат	атрибутного сертификата для передачи в Центр атрибутных сертификатов.
	На обновление личного сертификата	Позволяет сгенерировать новую пару (личный/открытый ключ), сформировать карточку открытого ключа пользователя, поместить в файл запрос на обновление личного сертификата для передачи в Удостоверяющий центр.
Сервис		
	Журнал работы	Позволяет вести работу с журналом для программы (просматривать, делать архивную копию).
	Список ключей на носителе	Позволяет пользователю увидеть список личных ключей на носителе, установленном в считывателе.
	Контроль точек распределения СОС	Проверка точек распределения СОС на наличие актуальных списков отозванных сертификатов.
	Настройки	Определяет основные настройки работы программы.
	Вывод информационных окон	Позволяет включать или выключать определенные окна при создании запроса.
	Сроки действия	Позволяет настроить срок действия сертификата и напоминания о завершении срока действия личного ключа/СОС.
Вид		
	Динамический фильтр	Автоматически отображает сертификаты, соответствующие критерию отбора
	Фильтр по нажатию Enter	Отображает сертификаты, соответствующие критерию отбора после нажатия клавиши Enter
	Очистить фильтр	Очищает фильтр
	Показывать количество строк	Отображает количество выводимых в окне записей
	Автоформат таблицы	Автоматически изменяет отображение колонок
Справка	О программе	Выводит общую информацию о программе

6.7. Работа со справочниками

В программе ПК AvPCM используются справочники, в которые помещена информация по сертификатам, спискам отозванных сертификатов УЦ.

Полный список существующих справочников следующий:

- Личные;
- Доверенных Удостоверяющих центров;
- Сетевой справочник;
- Списков отозванных сертификатов (СОС);

Внимание: Сертификаты и СОС можно удалить из любого справочника, при условии, если срок действия указанного объекта истек.

6.7.1. Просмотр содержимого справочников

Содержимое справочников отображается в виде таблицы, в которой выводятся основные поля объектов (сертификат, СОС, запрос на сертификат). Пользователь имеет возможность настроить видимые поля объектов по своему усмотрению. Управление отображением полей осуществляется при помощи подменю управления таблицей, которое вызывается нажатием правой клавиши мыши на шапке таблицы. Для скрытия ненужного поля необходимо вызвать подменю управления таблицей на этом поле и выбрать пункт «Спрятать колонку». Для вывода невидимого поля необходимо вызвать подменю управления таблицей и выбрать пункт с названием требуемого поля.

Содержимое справочников может быть отсортировано по любому видимому полю. Для сортировки по какому-то полю необходимо нажать левой клавишей мыши на шапке таблицы в зоне требуемого поля, повторное нажатие по этому же полю приводит к сортировке по убыванию. Поля - отсортированные по возрастанию отмечаются знаком  , по убыванию знаком  .

6.7.2. Справочник «Личные»

В этом разделе хранятся личные сертификаты пользователя.

Информация в этом справочнике пополняется в момент подключения пользователем личного сертификата, выпущенного УЦ по подготовленному ранее запросу.

Действующим сертификатом пользователя может быть только корректный рабочий сертификат пользователя.

Процедура проверки корректности сертификата пользователя может быть описана следующим образом:

- Проверяется, что текущая дата попадает в срок действия проверяемого сертификата;
- В разделе «Доверенных УЦ» ищется сертификат УЦ, которым выдан проверяемый сертификат, проверяется корректность его периода действия и самоподпись;
- Производится проверка корректности подписи УЦ в проверяемом сертификате пользователя;
- Ищется список отозванных сертификатов (СОС), выпущенный указанным выше УЦ и являющийся действительным (проверяется, что текущая дата входит в период действия СОС), проверяется корректность подписи УЦ под ним;
- Проверяется, не указан ли номер сертификата пользователя в списке найденного и проверенного СОС.

6.7.3. Справочник «Доверенных Удостоверяющих центров»

В этом справочнике хранятся все сертификаты корневых УЦ, подлинность которых (имеется в виду «сертификатов») гарантирована, т.е. пользователь убедился в подлинности информации, содержащейся в сертификате, сравнив ее с той, которая находится в карточке открытого ключа и идентификационных документах владельцев сертификатов, загруженных в этот раздел.

Справочник может пополняться следующими способами:

- При выполнении оператором процедуры установки (импорта) сертификата, когда сертификат является самоподписанным сертификатом УЦ;
- Добавление из Сетевого справочника.

Процедура «Добавления сертификата в список доверенных УЦ» из Сетевого справочника осуществляется следующим образом:

1) Найти в Сетевом справочнике сертификатов сертификат того УЦ, который мы хотим поместить в справочник «Доверенных Удостоверяющих центров»;
2) Подвести курсор к этому сертификату, и, нажав правую клавишу мыши вызвать всплывающее меню, в котором выбираем пункт «Поместить сертификат в справочник доверенных УЦ»;
3) Появится окно, в котором надо ввести серийный номер помещаемого в список доверия сертификата УЦ (см. **Рисунок 34**).

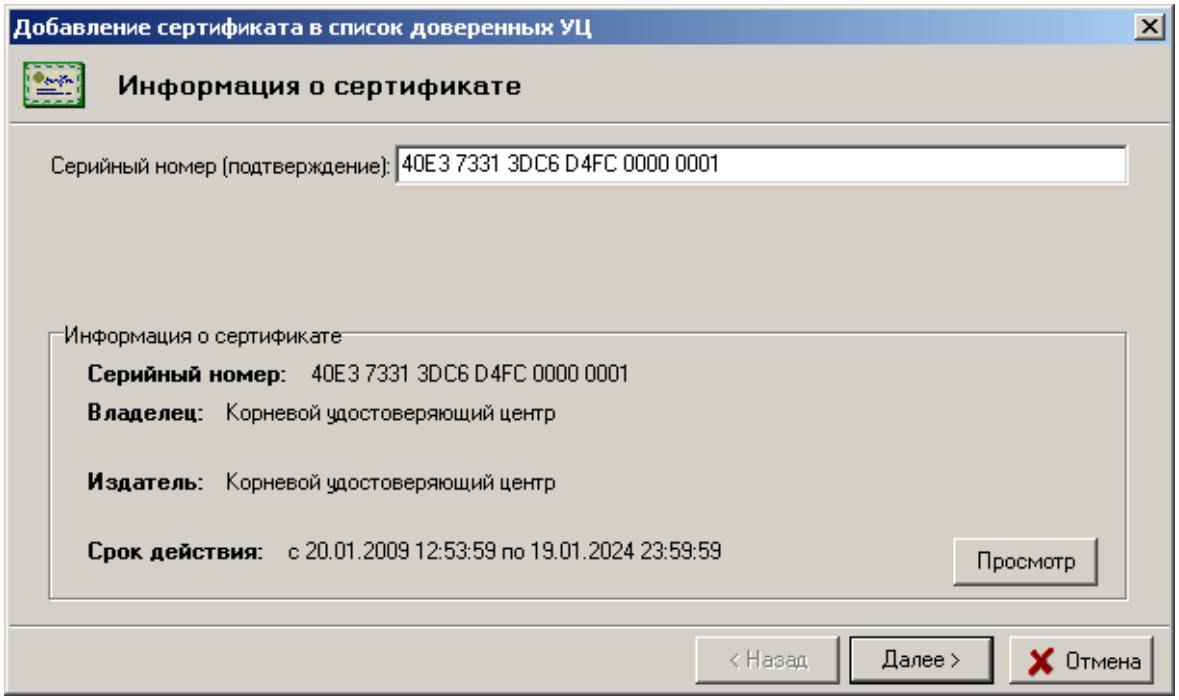

Рисунок 34. Информация о сертификате, помещаемом в список Доверенных УЦ

4) В следующем окне отражается уже существующий список доверяемых Удостоверяющих центров, в который будет помещен сертификат УЦ. Здесь надо только нажать кнопку «Далее» (см. **Рисунок 35**).

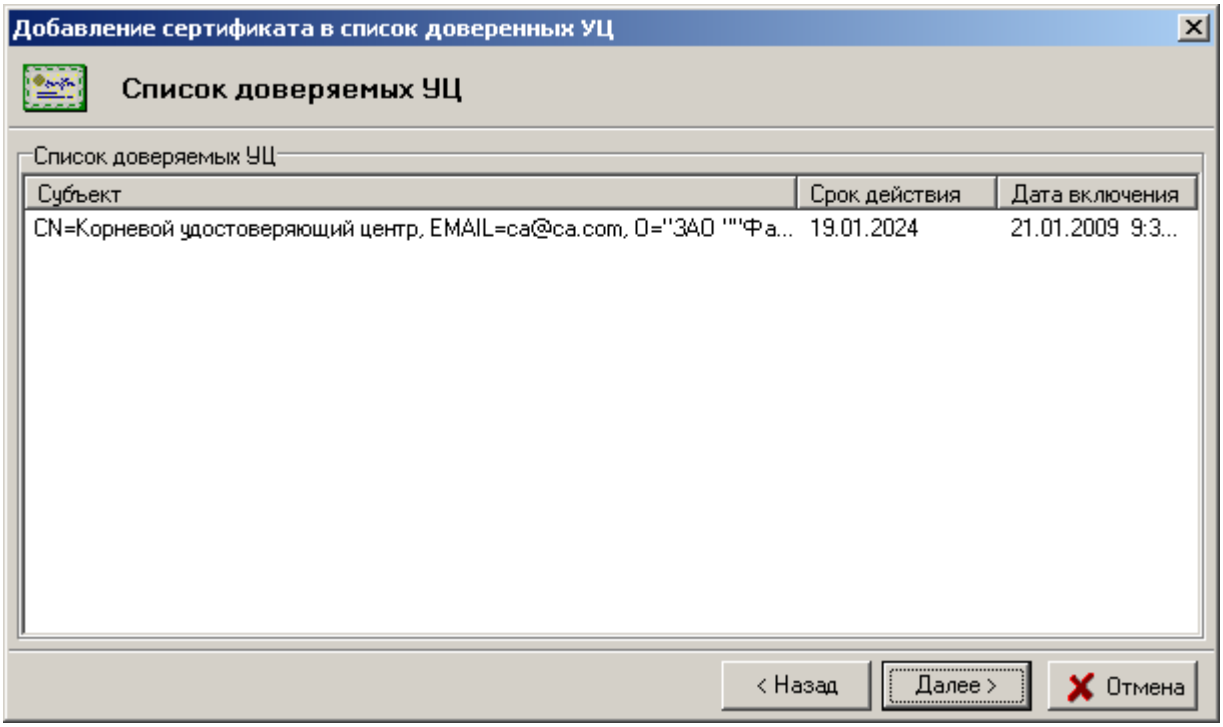

Рисунок 35. Список доверяемых Центров сертификации

5) Затем надо вставить носитель личного ключа в считыватель и в появившемся окне ввести пароль доступа к контейнеру с личным ключом пользователя (см. Рисунок 36).

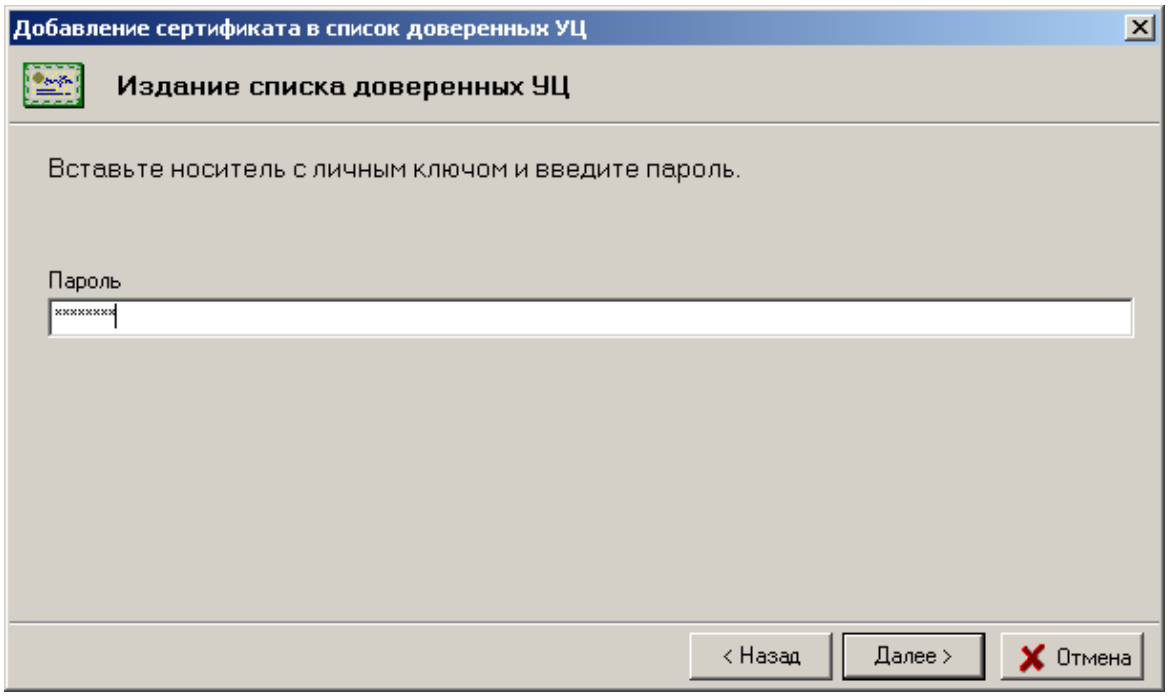

Рисунок 36. Издание списка Доверенных Центров сертификации

6) В последнем окне программа сообщит о том, что Список доверенных Удостоверяющих центров издан и помещен в сетевой справочник (см. Рисунок 37).

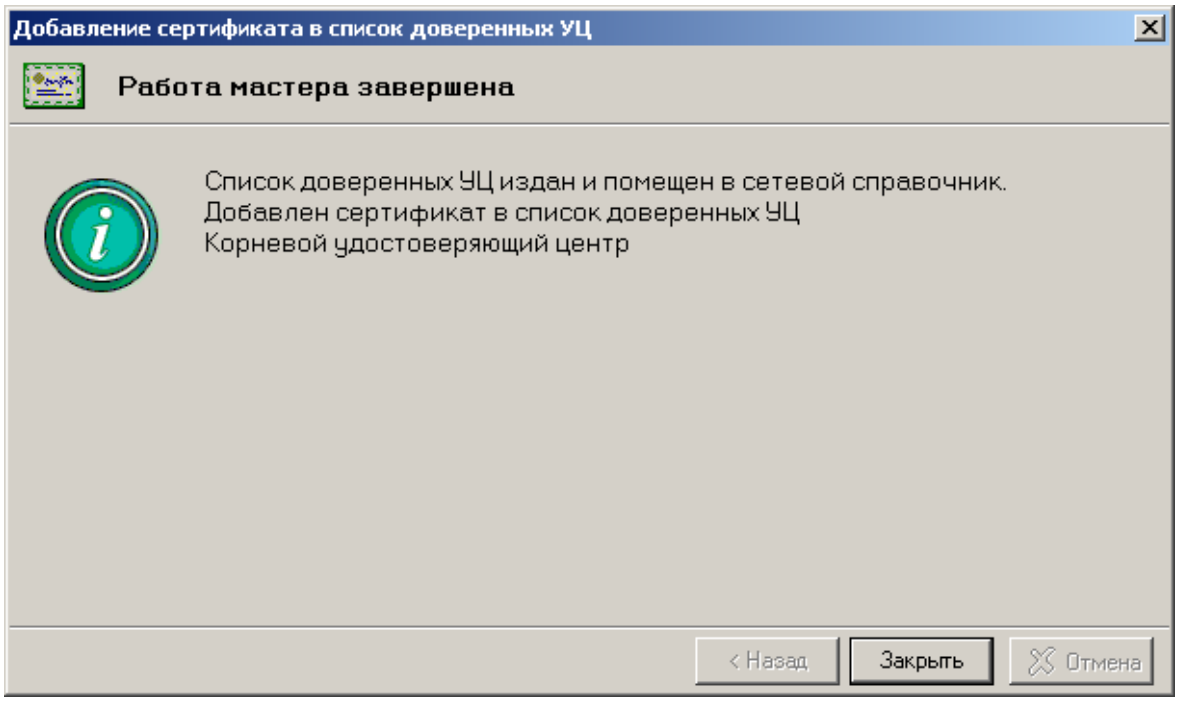

Рисунок 37. Завершение работы мастера «Добавление сертификатов в список доверенных УЦ»

Из справочника «Доверенных УЦ» можно удалить любой сертификат, если ему нет доверия или у него закончился срок действия.

В случае утраты доверия к любому из сертификатов доверенных УЦ, например, в случае его компрометации, необходимо удалить данный сертификат из справочника «Доверенных Удостоверяющих центров».

Действия при исключении сертификата УЦ из списка Доверенных УЦ:

1) В справочнике «Доверенных УЦ» надо стать курсором на нужный сертификат;
2) Щелкнуть по нему правой клавишей мыши и во всплывающем меню выбрать пункт «Исключить сертификат из справочника доверенных УЦ»;
3) В появившемся окне надо указать серийный номер и нажать кнопку «Далее» (см. **Рисунок 38**).

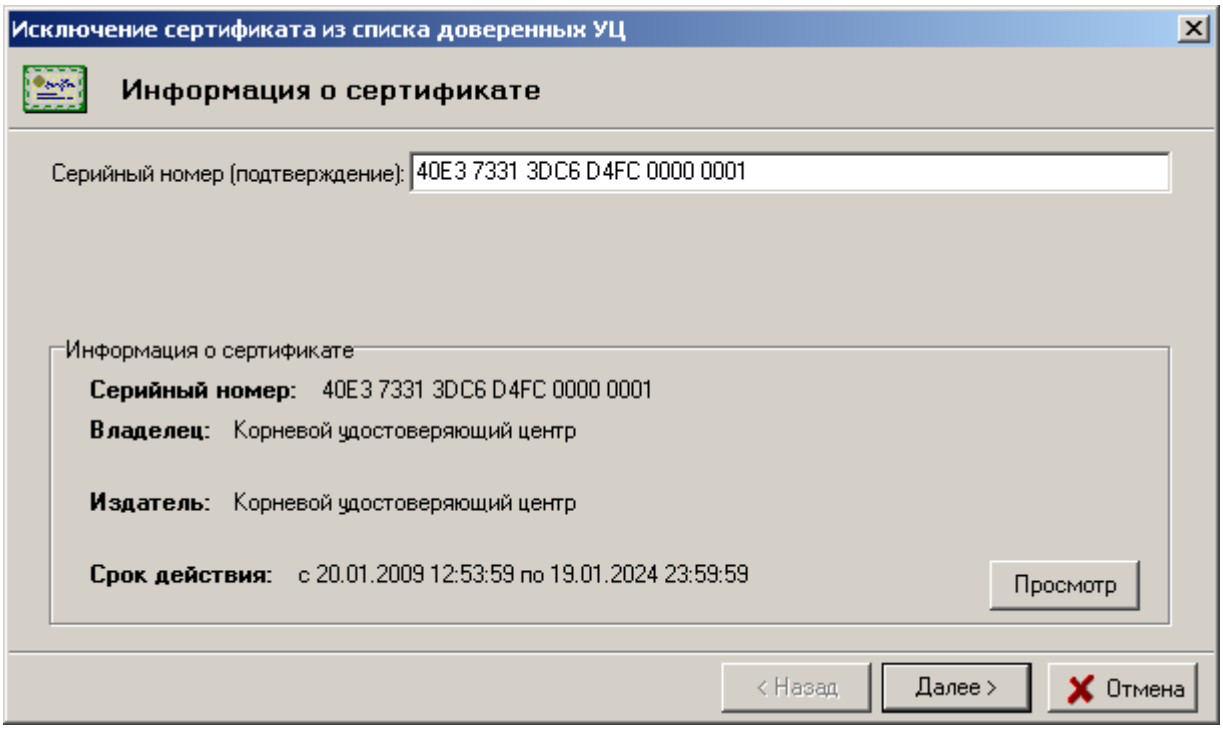

Рисунок 38. Исключение сертификата из списка Доверенных УЦ

Дальнейшие действия при исключении сертификата из списка доверенных УЦ аналогичны описанным выше при добавлении сертификата в список доверенных УЦ.

Внимание: При наличии сертификата УЦ в разделе доверенных, любая информация, корректно подписанная соответствующим личным ключом УЦ, будет автоматически считаться корректной.

6.7.4. Сетевой справочник сертификатов

В этом справочнике хранятся сертификаты всех УЦ и их пользователей, которые были импортированы из других баз данных.

Информация может быть добавлена только при выполнении процедуры импорта сертификатов. Для этого надо в основном меню программы выбрать пункт «Файл»→ «Импорт сертификата/СОС», после чего будет запущен мастер импорта сертификатов.

Действия при импорте сертификатов других пользователей аналогичны описанным выше действиям при импорте личного сертификата.

Предлагаемая к загрузке информация всегда может быть просмотрена оператором, после чего он может принять окончательное решение об установке сертификата для использования.

6.7.5. Справочник Списков отозванных сертификатов (СОС)

В этом справочнике хранятся списки отозванных сертификатов УЦ, импортированные из других баз данных.

Для случая сетевого варианта, внесение изменений в этот справочник, предполагается администратором УЦ. В связи с этим далее рассматривается изменение информации для случая локального варианта.

Пополнение справочника происходит при подключении (импорте) очередного СОС УЦ. Следует учесть тот факт, что если в справочнике будет обнаружен список отозванных сертификатов, подписанный тем же издателем и имеющий дату выпуска более старую, чем добавляемый, то старый СОС будет удален при добавлении нового.

6.8. Просмотр и печать содержимого сертификата

Пользователь может просматривать содержимое (параметры) сертификата, как находящегося в одном из справочников, так и при импорте сертификатов. Для просмотра содержимого сертификата, находящегося в одном из справочников, необходимо выбрать нужный справочник в дереве сертификатов/СОС в левой панели программы, затем с помощью фильтра найти нужный сертификат в правой панели окна, и открыть свойства сертификата двойным нажатием левой клавиши мыши. При этом появится окно просмотра содержимого выбранного сертификата (см. **Рисунок 39**) .

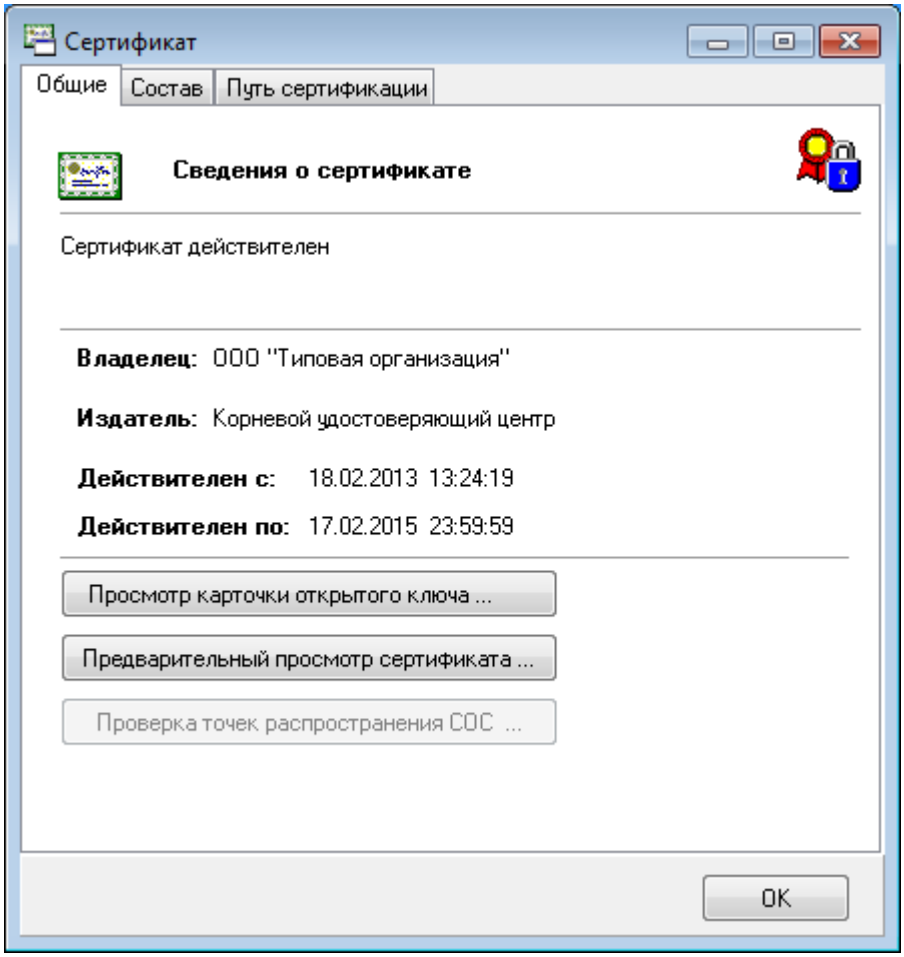

Рисунок 39. Просмотр сертификата

Данное окно состоит из трех закладок: Общие (сведения о сертификате), Состав (содержимое сертификата) и Путь сертификации (показана вся цепочка сертификатов, удостоверяющих данный сертификат, до корневого) – и двух дополнительных кнопок: «Просмотр карточки открытого ключа» и «Предварительный просмотр сертификата».

Описание общих свойств сертификата

Общие свойства сертификата, находящегося в базе данных программы:

– «Сертификат действителен» или «Сертификат не действителен» позволяет увидеть текущее состояние сертификата. В том случае, если сертификат не действителен, будет приведена причина его недействительности.
– «Владелец», «Издатель» – показывают владельца сертификата и его издателя.
– «Действителен с», «Действителен по» – показывают период, в течение которого сертификат действителен.

Нажав на кнопку «Просмотр карточки открытого ключа…» можно увидеть карточку открытого ключа, соответствующего данному сертификату.

Кнопка «Предварительный просмотр сертификата…» позволяет в дополнительном окне просмотреть и распечатать сертификат.

Описание состава сертификата

В данной панели можно увидеть точный состав сертификата, в том числе его серийный номер, алгоритм подписи, открытый ключ сертификата. При выборе одного из полей сертификата внизу панели будет отображена информация о его составе, например при выборе серийный номер, внизу будет отображено значение серийного номера сертификата (см. **Рисунок 40**).

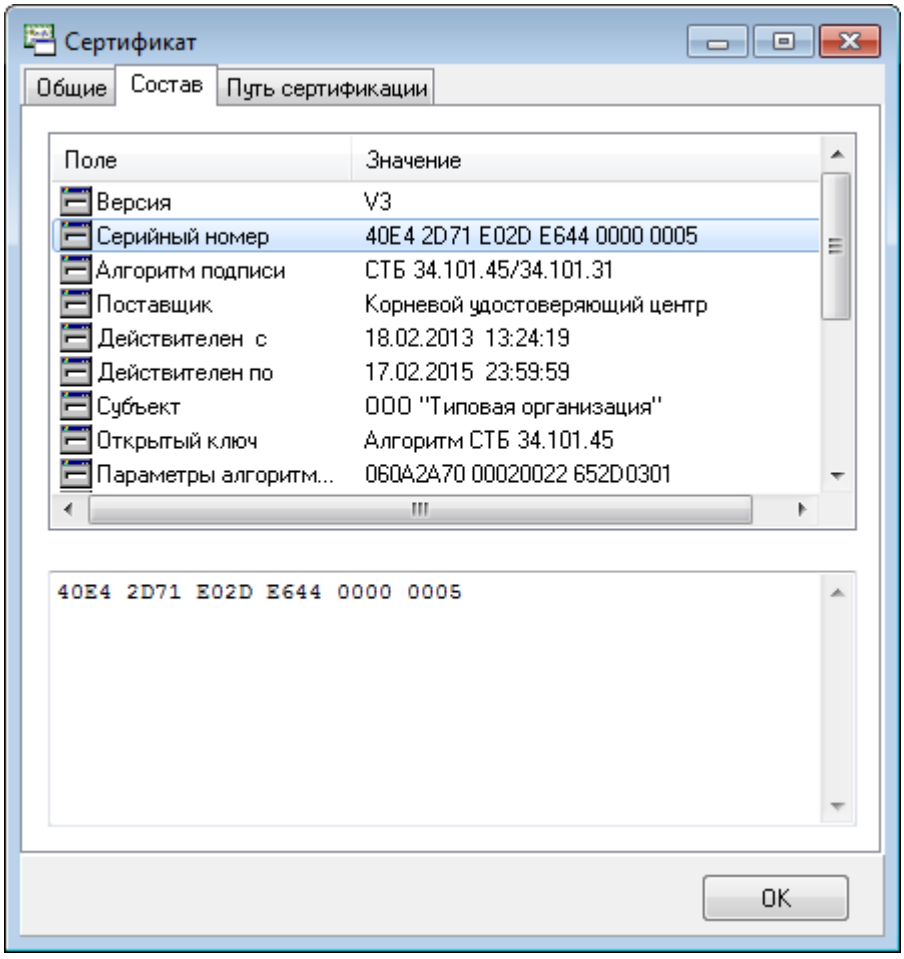

Рисунок 40. Состав сертификата

Путь сертификации

В данной панели можно увидеть, каким сертификатом был выдан данный сертификат, и в каком списке отозванных сертификатов он был проверен. Если при проверке какого-либо из

показанных сертификатов или при проверке СОС возникла какая-либо ошибка, например неверная подпись, сертификат будет отображен с крестиком в красном круге. Внизу панели будет отображена информация о результате проверки цепочки сертификатов и СОС.

6.9. Просмотр свойств Списка отозванных сертификатов (СОС)

Оператор может просматривать содержимое СОС как находящегося в справочнике, так и при импорте СОС. Для просмотра содержимого СОС, находящегося в справочнике, необходимо выбрать его группу в дереве сертификатов/СОС в левой панели программы. При этом в правой панели появится возможность с помощью фильтра отобрать нужный СОС.

При двойном нажатии мыши на выбранном СОС откроется окно свойств СОС.

Данное окно состоит из трех закладок: Общие сведения, Список отзыва и путь сертификации (см. **Рисунок 41**).

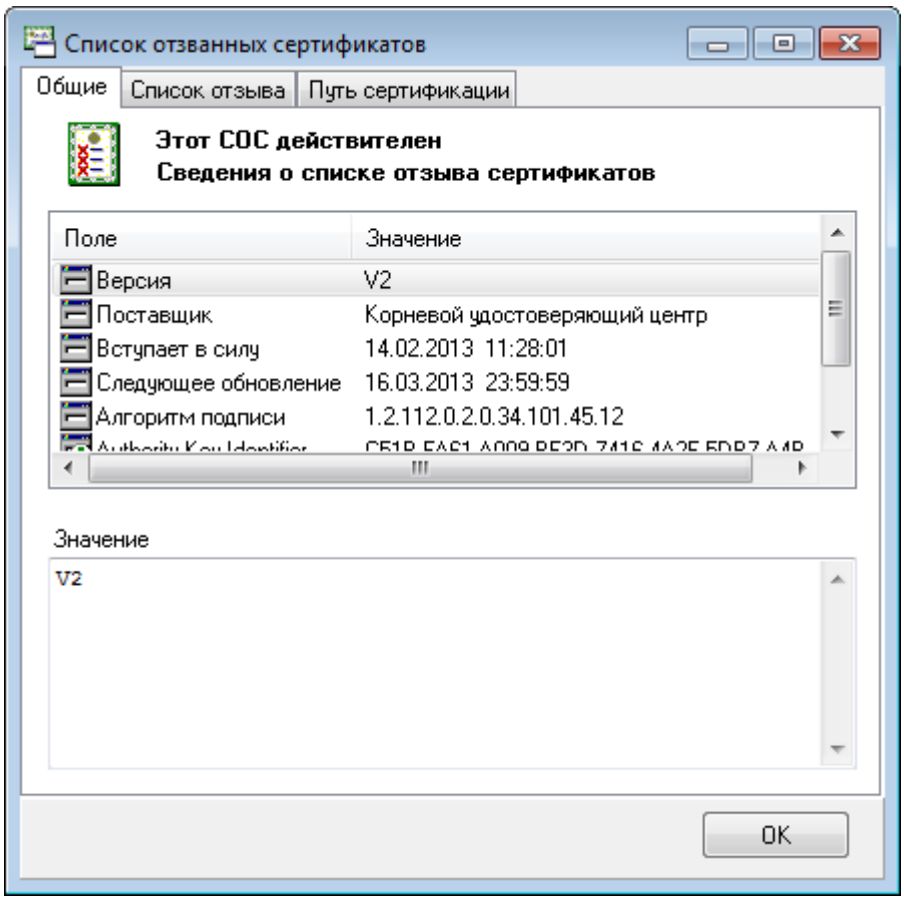

Рисунок 41. Окно «Список отозванных сертификатов»

Общие сведения

Данная закладка содержит общие параметры СОС:

- «Поставщик» – имя издателя;
- «Вступает в силу» – дата и время выпуска СОС;
- «Следующее обновление» – дата и время истечения срока использования данного СОС;
- «Алгоритм подписи» – алгоритм, использованный при подписывании СОС;
- «Идентификатор ключа центра сертификатов» – идентификатор открытого ключа сертификата, которым была выполнена подпись СОС.

Список отзыва

Данная закладка содержит список всех сертификатов, которые были отозваны издателем данного СОС. Можно посмотреть как свойства любого из отозванных сертификатов (нажав кнопку «Просмотр»), так и дату отзыва каждого из сертификатов, и причину отзыва.

Путь сертификации СОС

На данной закладке, можно увидеть каким сертификатом был выпущен данный СОС.

6.10. Просмотр и печать запроса на сертификат

Пользователь может просматривать содержимое запросов как находящихся в справочнике «Запросы на сертификат», так и при обработке запроса. Для просмотра содержимого запроса, находящегося в справочнике «Запросы на сертификат», необходимо выбрать его группу в дереве сертификатов/СОС в левой панели программы. При этом в правой панели появится возможность с помощью фильтра отобрать нужный запрос.

Окно свойств запроса на сертификат открывается двойным щелчком мыши по запросу.

Данное окно состоит из четырех закладок: Общие, Состав, Значение ключа и Удостоверяющие подписи – и двух дополнительных кнопок: «Просмотр карточки открытого ключа» и «Предварительный просмотр» (см. **Рисунок 42**).

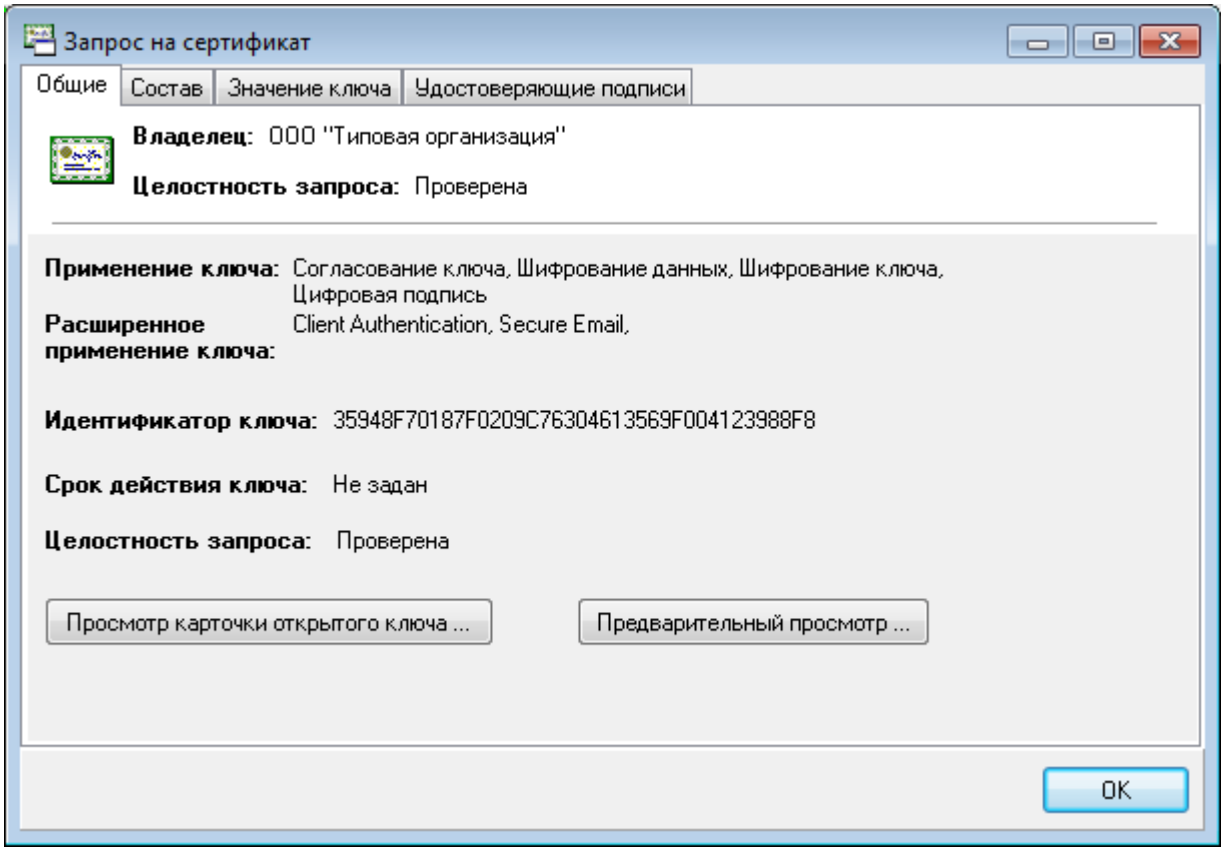

Рисунок 42. Окно «Запрос на сертификат»

Закладка *«Общие»* содержит общие параметры запроса на сертификат:

- «Применение ключа» – цели, для которых может быть использован личный ключ парный которому находится в карточке открытого ключа;
- «Расширенное применение ключа» – позволяет идентифицировать сертификат в системе;
- «Идентификатор ключа» – хэш-функция от значения открытого ключа;
- «Срок действия ключа» – дата начала и окончания периода действия личного ключа;
- «Целостность запроса» – результаты проверки ЭЦП выработанной под запросом на сертификат.

С помощью кнопки «Просмотр карточки открытого ключа…» можно просмотреть и распечатать карточку открытого ключа данного запроса на сертификат из дополнительно раскрывшегося окна.

Кнопка «Предварительный просмотр…» позволяет в дополнительном окне просмотреть и распечатать запрос на сертификат.

Состав:

В данной панели можно увидеть точный состав запроса на сертификат, в том числе его открытый ключ, параметры алгоритма ЭЦП, использование личного ключа, идентификатор ключа субъекта, срок действия открытого ключа. При выборе одного из полей запроса внизу панели будет отображена информация о его составе.

Значение ключа:

В данной панели можно увидеть значение открытого ключа проверки подписи.

Удостоверяющие подписи:

В данной панели можно увидеть дополнительные ЭЦП, которыми заверен данный запрос на сертификат.

6.11. Экспорт и импорт сертификатов/СОС

ПК AvPCM позволяет, как импортировать сертификаты из других баз, так и экспортировать их.

6.11.1. Экспорт сертификата

Для экспорта сертификата надо проделать следующие действия:

1) Найти нужный сертификат в одном из справочников;
2) Выбрать в основном меню пункт «Файл» / «Экспорт сертификата в файл» или щелкнуть правой клавишей мыши по сертификату и во всплывающее меню выбрать «Экспорт сертификата в файл»;
3) В открывшемся окне указать: место, куда должен быть сохранен файл (Папка:), имя файла для экспорта сертификата и нажать кнопку «Сохранить» (см. **Рисунок 43**).

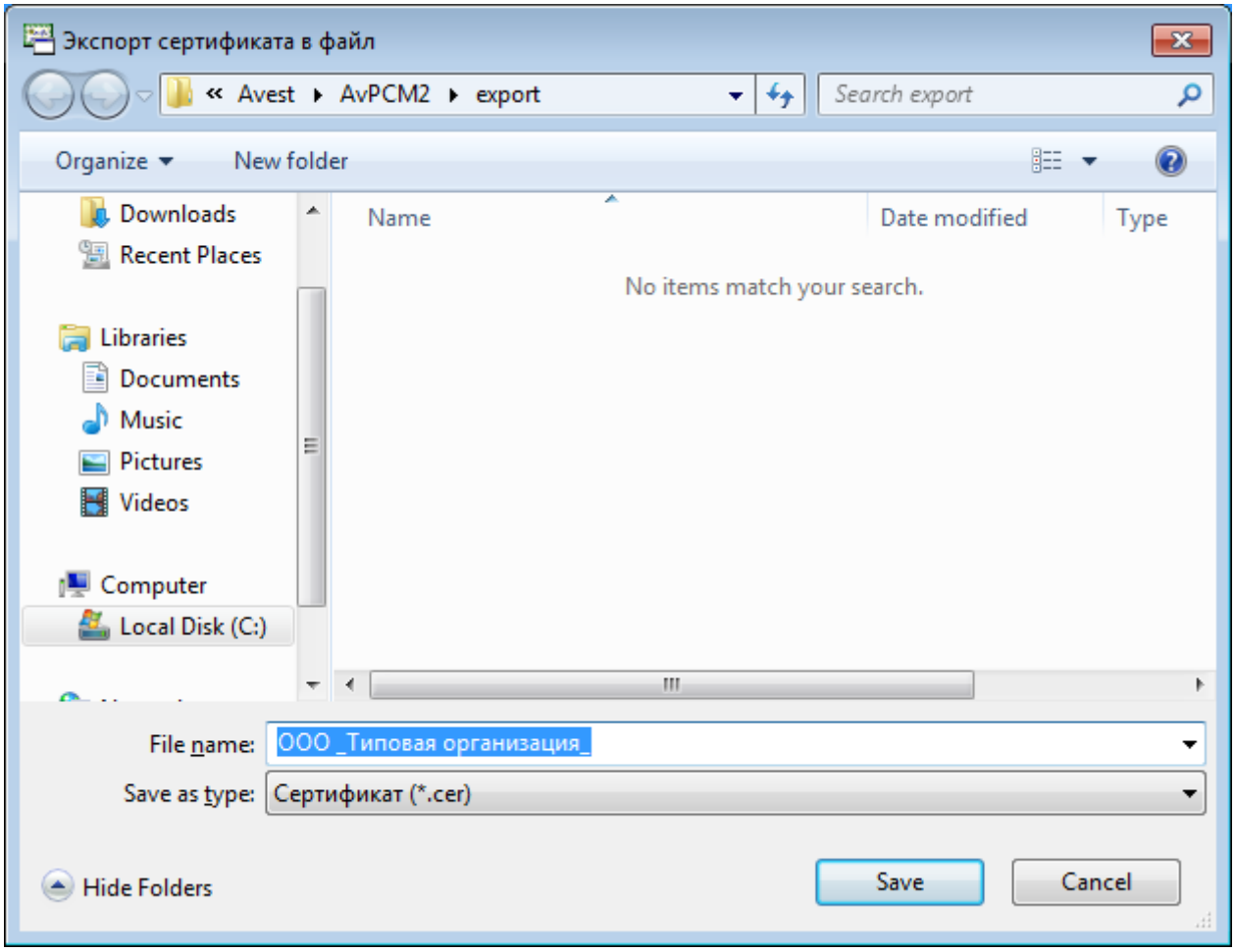

Рисунок 43. Экспорт сертификата в файл

В случае успешного завершения процедуры экспорта, на экран будет выдано окно подтверждения, содержащее полный путь к файлу экспорта. Для закрытия этого окна требуется нажать кнопку «ОК».

6.11.2. Экспорт СОС

Экспорт СОС производится из справочника «СОС». Процедура экспорта СОС аналогична описанной выше процедуре для экспорта сертификата.

6.11.3. Экспорт списка сертификатов и СОС

Если требуется экспортировать список сертификатов и СОС, то тогда действия пользователя будут следующими:

1) Выбрать нужные сертификаты, в одном из справочников, и щелкнув правой клавишей мыши вызвать всплывающее меню, в котором выбрать «Экспорт сертификатов (выбранных)»;

2) В открывшемся окне указать:

– место, куда должны быть сохранены сертификаты (Папка:);
– в строке (Имя файла:) по умолчанию задается имя «AllCert»;
– в строке (Тип файла): Сертификаты (весь путь): PKCS#7,
– нажать кнопку «Сохранить».

При соблюдении всех этих условий сертификаты будут помещены в один файл формата PKCS#7.

После успешного экспорта списка сертификатов программа выдаст окно сообщение, в котором будет прописан путь к файлу и его содержимое (см. **Рисунок 44**).

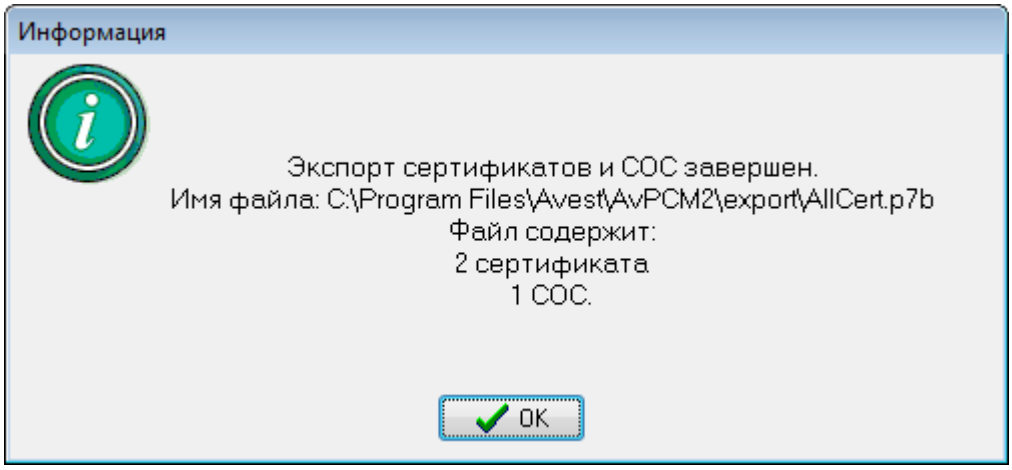

Рисунок 44. Информация об окончании экспорта списка сертификатов

6.11.4. Импорт сертификатов

Для выполнения импорта сертификатов можно воспользоваться пунктом основного меню «Файл»/»Импорт сертификата/СОС» или из основного меню Windows: «Пуск»→«Программы»–→ «Авест»→«Персональный менеджер сертификатов»→«Импорт сертификатов». После чего на экране появится окно «Мастер импорта сертификатов».

Дальнейшие действия при импорте сертификатов других пользователей аналогичны рассмотренным выше действиям в разделе «Импорт личного сертификата при инсталляции с файловой базой данных».

6.12. Управление контейнерами личных ключей на носителе

Для контроля того, какие контейнеры с личными ключами имеются на носителе ключевой информации, в программе предусмотрена специальная возможность – окно списка контейнеров

личных ключей на носителе. Данное окно можно просмотреть, выбрав в основном меню пункт «Сервис», подпункт «Список ключей на носителе».

В этом окне будут отражены все личные ключи, находящиеся на вставленном носителе (см. **Рисунок 45**).

При щелчке правой кнопкой «мыши» на выделенном контейнере пользователю ПК AvPCM доступны следующие операции:

- просмотр сертификата;

- поместить сертификат в личный справочник;

- поместить сертификат в контейнер;

- удалить личный ключ;

- сменить пароль контейнера.

В случае если срок действия личного ключа закончился, или если сертификат отозван, то можно удалить контейнер с личным ключом с носителя. Данную процедуру обязательно необходимо выполнить по окончании срока действия личного ключа и при отзыве сертификата.

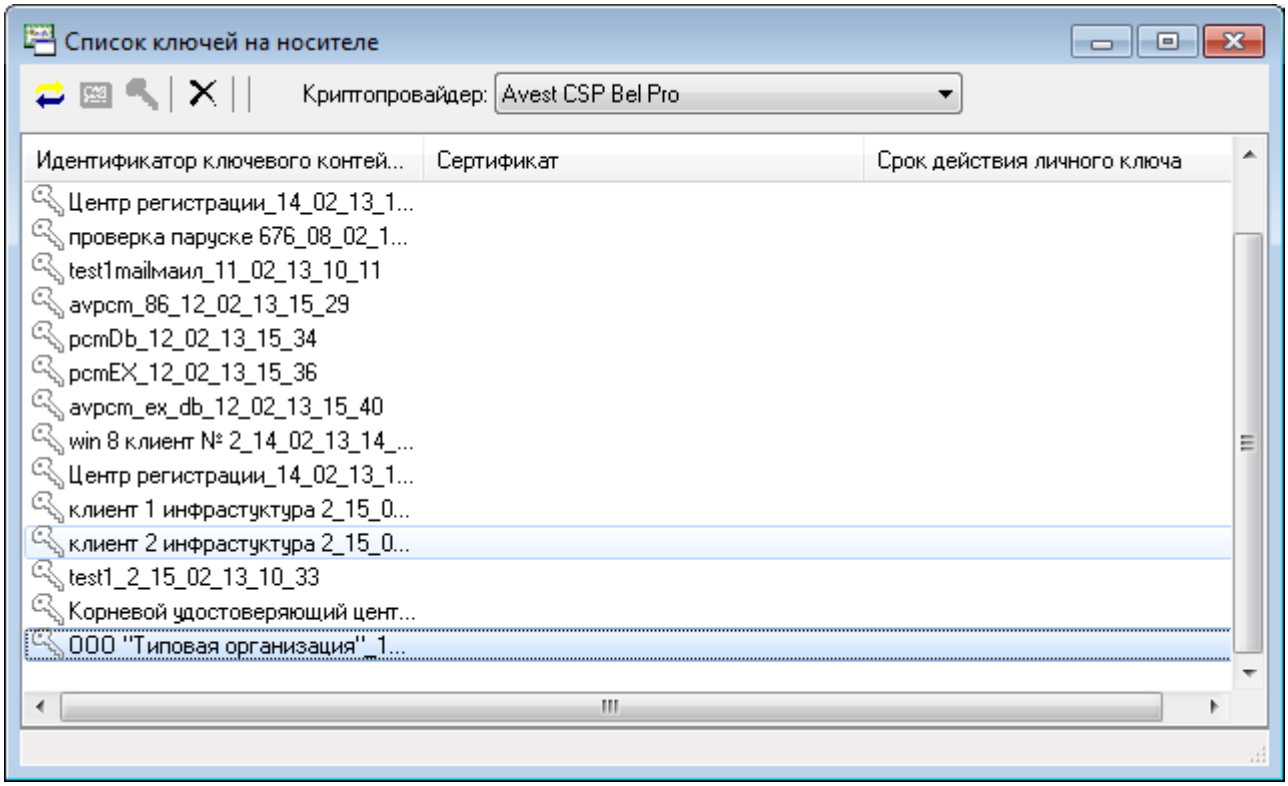

Рисунок 45. Список ключей на носителе

Внимание: Владелец или уполномоченное лицо несет полную ответственность за сохранность носителей с личными ключами и конфиденциальность личных ключей. Рекомендуется не загружать ПК AvPCM без необходимости, а при загруженном программном обеспечении не оставлять компьютер без контроля.

6.13. Журнал работы

В процессе работы программы ведется журнал работы. Для просмотра журнального файла необходимо выбрать в основном меню «Сервис», пункт «Журнал работы».

Схематично представить журнал работы можно в виде таблицы (см. Таблица 2 – Журнал работы).

Таблица 2. Журнал работы

№	Поле	Данные	Примечание
1	Дата и время события	Дд.мм.гггг Чч:мм:сс	
2	Субъект	Текст	Имя абонента, зарегистрировавшегося в системе и выполнившего операцию
3	Объект	Текст	Название выполняемой процедуры или идентификатор обрабатываемого объекта
4	Операция	Текст	Краткое название выполняемой операции
5	Дополнительная информация	Текст	Описывает действия, производимые функцией. Может содержать значения возможных критичных параметров
6	Результат	Текст	Результат выполнения операции

Можно настроить несколько типов ведения журнала работы. Для этого необходимо открыть журнал работы, выбрать пункт меню «Журнал работы» – «Настройка журнала работы». В открывшемся окне выбрать тип журнала:

- Локальный (контроль файла по размеру) – запись журнала происходит в файл. При превышении файлом максимального значения, выставленного в настройках, файл журнала переименовывается путем добавления в имя файла номера, и запись продолжается в новый файл. При данном типе ведения журнала возможны следующие настройки (см. **Рисунок 46**):
  - *Имя файла журнала* – выбор каталога хранения и имени файла журнала;
  - *Максимальный размер файла журнала (kB)* – настройка размера, при котором файл журнала будет переименовываться, и создаваться новый файл;

– *Максимально количество хранимых файлов* – максимальное количество файлов, которые будут созданы при достижении файлом журнала максимального значения. Более старые файлы будут удалены.

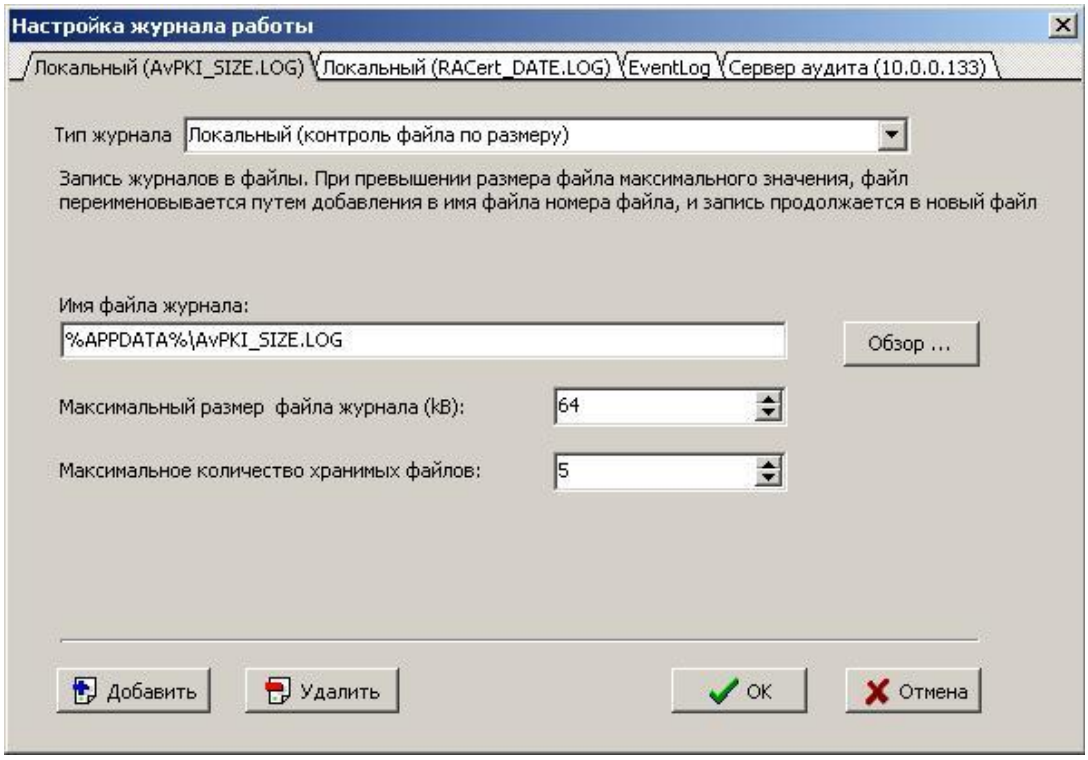

Рисунок 46. Настройка журнала работы (контроль файла по размеру)

- Локальный (контроль файла по дате) – запись журнала происходит в файл. При этом файлы именуются в зависимости от даты и времени сообщений. Например, можно указать такой формат даты в имени файла, чтобы каждые сутки (месяц, год) работы журнала записывались в отдельный файл, в имени которого будет указана дата создания журнала.

  При данном типе ведения журнала возможны следующие настройки (см. **Рисунок 47**):

  – *Имя файла журнала* – выбор каталога хранения и имени файла журнала;

  – *Создавать новый журнал* – временной интервал, по достижению которого файл журнала будет переименовываться, и создаваться новый файл.

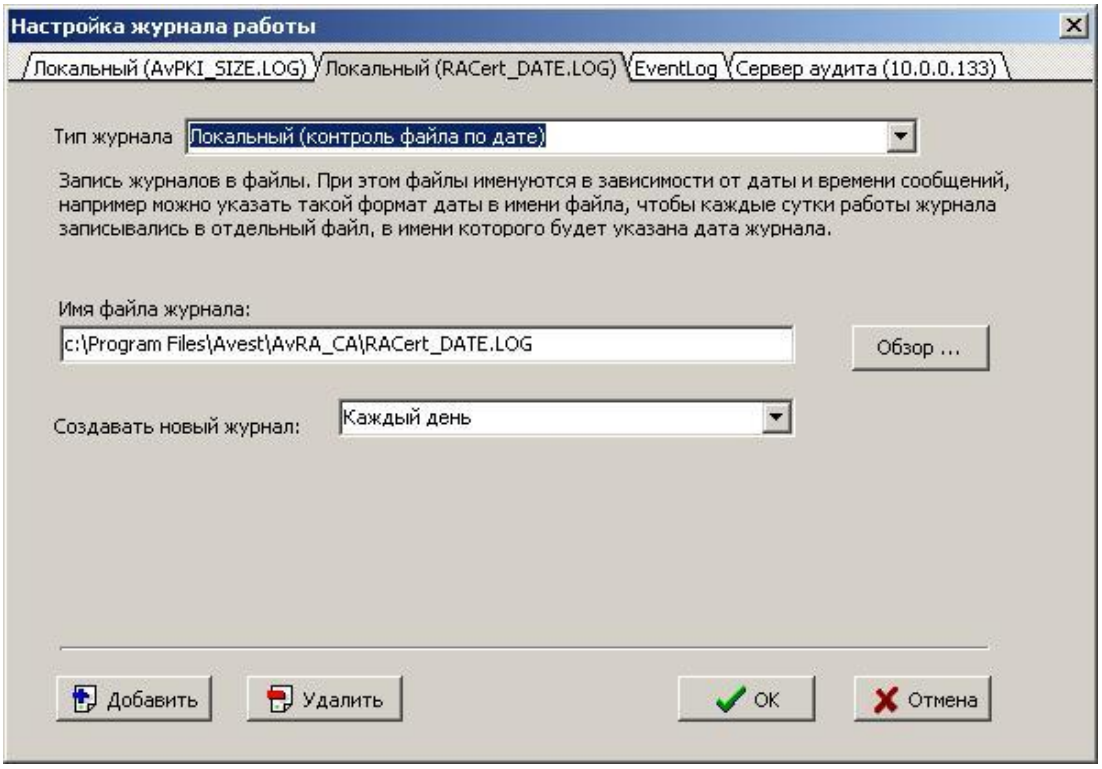

Рисунок 47. Настройка журнала работы (контроль файла по дате)

- Сервер журналов аудита. При данном типе журнала происходит пересылка сообщений на сервер журналов аудита. Для пересылки используется SSL-защищенный канал связи поверх TCP/IP.

  При данном типе ведения журнала возможны следующие настройки (см. **Рисунок 48**):

  – *IP адрес сервера журналов* – IP адрес компьютера, на котором запущен сервер журналов аудита;

  – *Порт сервера журналов* – порт, по которому происходит обращение к серверу журналов аудита;

  – *Сертификат сервера* – выбор сертификата сервера журналов аудита;

  – *Задержка, для отправки сообщений на сервер (миллисекунд)* – временной интервал, через который информация будет отослана на сервер журналов аудита.

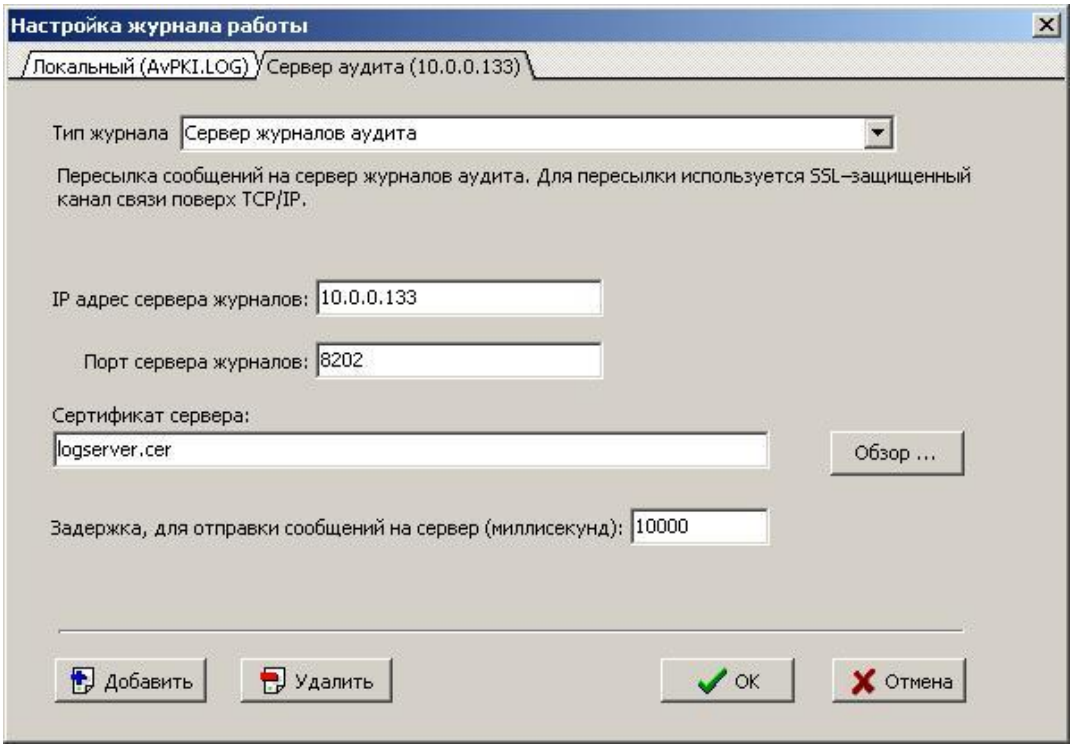

Рисунок 48. Настройка журнала работы (сервер журналов аудита)

- RemoteSyslog (журнал удаленного сервера). При данном типе журнала происходит пересылка сообщений на сервер под управлением операционной системы UNIX/LINUX для записи в журнал операционной системы.

  При данном типе ведения журнала возможны следующие настройки (см. **Рисунок 49**):

  – *IP адрес сервера журналов* – IP адрес компьютера, на котором запущен сервис ведения журнала удаленного доступа;

  – *Порт сервера журналов* – порт, по которому происходит обращение к сервису ведения журнала удаленного доступа.

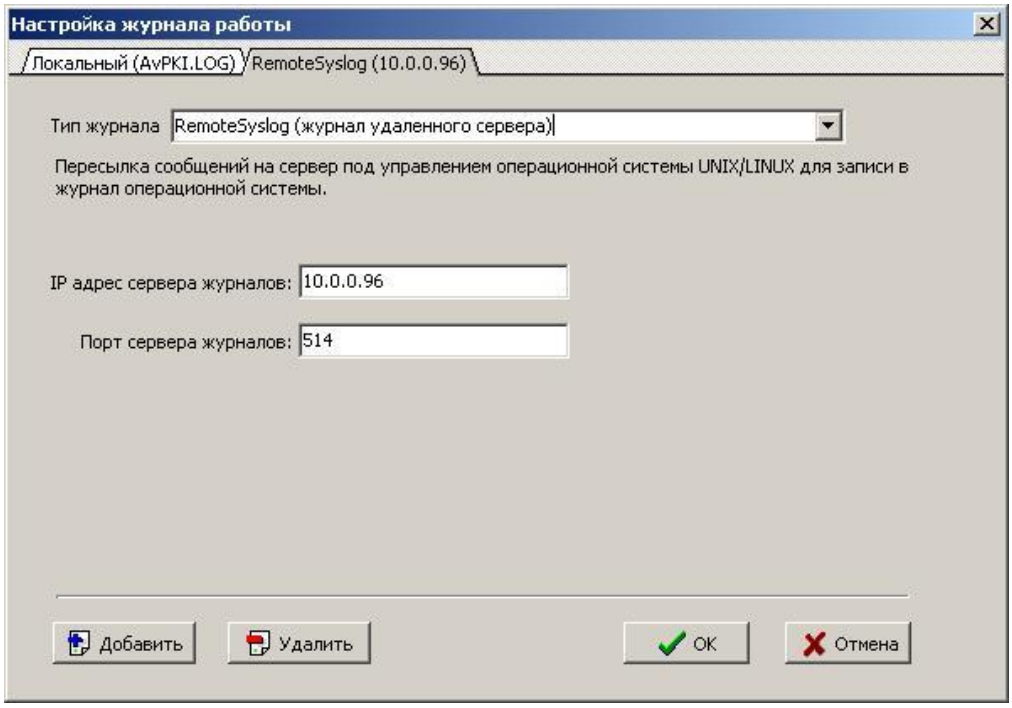

Рисунок 49. Настройка журнала работы (журнал удаленного сервера)

- Eventlog (журнал операционной системы). При данном типе журнала происходит запись в журнал операционной системы Windows (см. **Рисунок 50**).

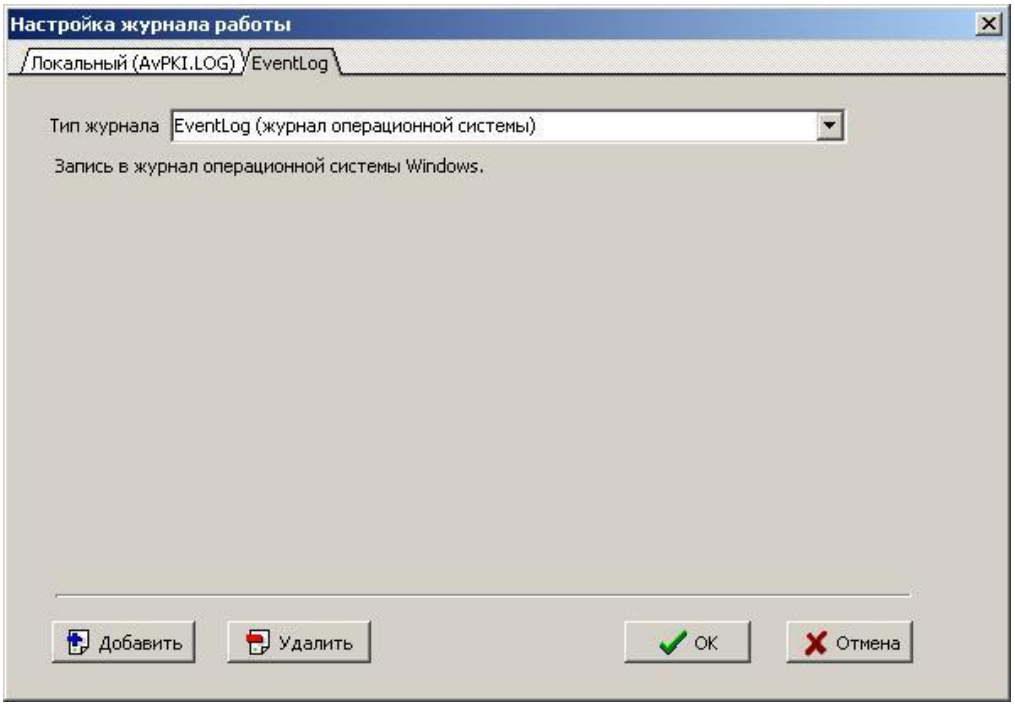

Рисунок 50. Запись в журнал операционной системы

6.14. Дополнительные возможности программы

6.14.1. Включение отладочного лога

Для того, чтобы включить отладочный лог **AvCmDebug.log,** нужно открыть файл **AvCmMsg.ini** для редактирования (например, с помощью Блокнота), найти раздел [DEBUG] и удалить знак препинания «;», который стоит перед параметром

```
LogFileName=AvCmDebug.log
```

После этого сохранить изменения и закрыть файл **AvCmMsg.ini.**

После снятия отладочного лога рекомендуется вернуть точку с запятой, чтобы файл **AvCmDebug.log** не разрастался и не занимал свободное дисковое пространство.

6.14.2. Импорт СОС в тихом режиме

Чтобы импорт СОС проходил в "тихом" режиме, без запроса действий оператора, необходимо запустить команду:

```
MngCert.exe name.crl /IMPORTCRL /SilentRun
```

где *name.crl* – импортируемый СОС.

6.14.3. Контроль точек распределения СОС

Для корректной работы проверки точек распространения СОС, необходимо в папке с установленным менеджером сертификатов создать файл CrlDPExt.txt, в котором указать адреса, где опубликованы актуальные СОС-ы, например:

```
http://localhost:8080/avcrlserver/curentcrl.crl
http://localhost/avcrlserver/curentcrl.crl
```

6.14.4. Включение отображения информационных окон.

Для появления возможности отображения окна «Вывод информационных окон» необходимо в папке с установленным менеджером сертификатов создать файл под названием

ViewWindows.ini со следующим содержимым (содержание этого файла может изменяться, в зависимости от требуемых условий):

```
[master]
FrmReq=Мастер создания запроса на сертификат

[FrmReq]
FrmKey_USAGE=Применение ключа
FrmContainerName=Задание имени контейнера

[FrmKey_USAGE]
Visible=True

[FrmContainerName]
Visible=False
```

6.14.5. Настройка времени кэширования СОС

Время кэширования СОС можно настроить в **AvCmMsg.ini**, открыв его (например, с помощью Блокнота) и вставив секцию [CRLCache], с возможными ключами (если секция отсутствует устанавливается Default=60):

Default=время кэширования всех СОС в секундах;

[Common name]=время кэширования СОС указанного издателя в секундах;

Пример:

[CRLCache]
Default=120
Корневой удостоверяющий центр=600

7. ПЕРЕХОД ИЗ ДРУГОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для перехода из одного Удостоверяющего центра в другой необходимо сделать следующее. Отозвать свой сертификат в старом Удостоверяющем центре.

Для этого:

- Обратиться в старый Удостоверяющий центр с заявлением об отзыве своего сертификата.
- После отзыва сертификата, получить в Удостоверяющем центре обновленный список отозванных сертификатов (СОС).
- Импортировать полученный список отозванных сертификатов (СОС) средствами ПК AvPCM на свой компьютер.
- Сгенерировать новый ключ и получить сертификат в новом Удостоверяющем центре
- Получить новые сертификаты и СОС и импортировать их средствами ПК AvPCM на свой компьютер.

В ПК AvPCM удалить из справочника «Личные» старый (отозванный) сертификат.

8. УДАЛЕНИЕ ПРОГРАММЫ

Действия по удалению ПК AvPCM с компьютера:

1) Выбрать из основного меню Windows: «Пуск» – «Настройка» – «Панель управления» – «Установка и удаление программ»;
2) В окне «Свойства: Установка и удаление программ» на закладке «Установка/удаление» в окне перечисления программ выбрать «Персональный менеджер сертификатов Авест» и нажать кнопку «Добавить/удалить»;
3) В окне запроса о подтверждении решения об удалении нажать кнопку «Да»

После процедуры удаления появится окно с сообщением об удалении ПК AvPCM с компьютера.

9. МЕРЫ БЕЗОПАСНОСТИ

Данный раздел содержит рекомендуемые требования обеспечения безопасности поставки, установки и эксплуатации ПК AvPCM, которым должны следовать потребители в процессе приобретения и использования ПК AvPCM.

Данные требования направлены на достижение следующих целей:

– предупреждение нарушений целостности и подлинности программных компонентов ПК AvPCM;

– обеспечение защиты криптографических ключей и данных потребителя от компрометации;

– обеспечение надежного функционирования ПК AvPCM.

9.1. Меры безопасности при поставке

Передача программного обеспечения ПК AvPCM (далее - ПО) потребителю может осуществляться следующими способами:

– передача потребителю компакт-диска с записанным ПО;

– запись ПО на носитель потребителя при очной явке уполномоченного лица на предприятие;

– пересылка по электронной почте (допускается в отдельных случаях, при тестовой эксплуатации ПО, либо при необходимости обновления ПО).

Во всех данных случаях для защиты от несанкционированной модификации ПО в процессе доставки ПО до потребителя применяются следующие меры безопасности:

– представитель потребителя в процессе получения ПО взаимодействует с конкретным сотрудником ЗАО «АВЕСТ», уполномоченным на передачу ПО, при этом представитель потребителя документально подтверждает свои полномочия;

– по согласованию с потребителем ЗАО «АВЕСТ» предоставляет перечень программных компонентов ПО с указанием эталонных значений версий и контрольных характеристик в виде хэш-значений, выработанных от файлов программных компонентов в соответствии со стандартом Республики Беларусь СТБ РБ 1176.1-99 «Информационная технология. Защита информации. Процедура хэширования»;

– по согласованию с потребителем ЗАО «АВЕСТ» предоставляет, при необходимости, потребителю тестовую утилиту, позволяющую тому самостоятельно вычислить хэш-значения полученных программных компонентов ПО;

– ПО содержит механизмы, указанные в данном документе позволяющие потребителю контролировать версии и текущие хэш-значения программных компонент ПО.

При получении потребителем ПО, в случае, когда он не запрашивал его у ЗАО «АВЕСТ», необходимо связаться с сотрудниками ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия http://www.avest.by) и уточнить факт отправки ПО в свой адрес. При подтверждении отправки ПО, потребитель должен вышеуказанным способом проконтролировать соответствие версий и целостность полученного ПО. При отсутствии подтверждения от ЗАО «АВЕСТ» факта отправки ПО, потребитель должен воздержаться от использования полученного ПО.

9.2. Меры безопасности при установке и эксплуатации

Установка ПО на ПЭВМ потребителя должна производиться в соответствии с данным руководством. При этом должны быть обеспечены следующие условия:

– перед установкой должна быть произведена проверка хэш-значения установочного файла ПО согласно процедуре указанной в предыдущем разделе данного документа;

– установка ПО должна производиться уполномоченным сотрудником потребителя, ознакомленным с данным документом и выполняющим обязанности администратора;

– на ПЭВМ предназначенной для установки ПО должны отсутствовать вредоносные программы («компьютерные вирусы», «резиденты», «отладчики», «клавиатурные шпионы» и т.д.);

– после установки ПО, отчуждаемый носитель (компакт-диск CD-R) с эталонным установочным файлом ПО и эталонные хэш-значения программных компонентов должны быть помещены в безопасное хранилище, доступ к которому должен иметь только уполномоченный персонал потребителя.

Эксплуатация ПО на ПЭВМ потребителя должна производиться в соответствии с данным руководством. При этом должны быть обеспечены следующие условия:

– сотрудник, эксплуатирующий ПО должен быть предупрежден о гражданской, правовой и финансовой ответственности, возлагаемой на него при использовании ПО в информационных системах электронного документооборота, обеспечивающих средствами ПО электронную

цифровую подпись в соответствии с Законом Республики Беларусь «Об электронном документе» или в иных случаях;

– для эксплуатации ПО должна использоваться, по возможности, выделенная ПЭВМ с установленным на ней лицензионным системным и прикладным программным обеспечением и только необходимым по технологии использования ПО в информационной системе потребителя;

– ПЭВМ предназначенная для эксплуатации ПО должна быть защищена от «закладок», «компьютерных вирусов», несанкционированного изменения системного и прикладного программного обеспечения;

– любое изменение (реконфигурирование, дополнение и т.д.) системного и прикладного программного обеспечения ПЭВМ должно быть согласовано с уполномоченным сотрудником потребителя, выполняющим обязанности администратора;

– сотрудник потребителя, эксплуатирующий ПО должен изучить данный документ;

– НКИ, содержащие личные ключи ЭЦП и шифрования в отсутствие работы с ними должны храниться в надежном хранилище, доступ к которому имеют только уполномоченные сотрудники потребителя. Пароль на доступ к данным на НКИ должен храниться в тайне. Запрещается сообщать кому-либо значение пароля. При смене сотрудника, работающего с НКИ, новый сотрудник в первую очередь должен сменить пароль на доступ к НКИ и хранить его в дальнейшем в тайне;

– ответственность за сохранность НКИ и содержащихся на нем данных несет сотрудник потребителя, работающий с НКИ;

– доступ к ПЭВМ с установленным ПО должен быть ограничен и разрешен только уполномоченным на работу с ПО сотрудникам потребителя;

– средствами ОС MS Windows должна быть обеспечена аутентификация пользователя при запуске ОС, а также аудит событий связанных с ПО (запуск ПО, чтение-запись файлов и данных ПО, хранящихся на жестком диске ПЭВМ);

– при проведении ремонтных и профилактических работ ПЭВМ, на которой установлено ПО должны приниматься организационные меры и использоваться технические средства для исключения несанкционированного доступа к ПО;

– осмотр и ремонт ПЭВМ представителями сторонних организаций проводятся только под наблюдением уполномоченного сотрудника потребителя;

– передача ПЭВМ для ремонта в сторонние организации производится только после демонтажа накопителя на жестком магнитном диске (НЖМД);

– ремонт НЖМД, на котором инсталлированы программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования НЖМД.

В случае возникновения ошибок или сбоев в работе ПО уполномоченный сотрудник потребителя, выполняющий роль администратора должен:

1. Сравнить версии и хэш-значения программных компонентов используемого ПО с эталонными. В случае несовпадения сообщить своему руководству, связаться с отделом поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия http://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела поддержки;
2. Убедиться в работоспособности ПЭВМ, ее аппаратных и программных систем;
3. Проанализировать журналы аудита ОС;
4. При необходимости провести процедуру «безопасного восстановления» ПО (см. ниже);
5. В случае невозможности выполнения процедуры безопасного восстановления, прекратить эксплуатацию ПО, связаться с отделом поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия http://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела поддержки.

Процедура «безопасного восстановления» ПО заключается в переинсталляции ПО на ПЭВМ с носителя (компакт-диск CD-R) с эталонным установочным файлом ПО. При этом рекомендуется предварительно проверить работоспособность ПЭВМ без установленного на ней ПО.

Примечания:

1. Взаимодействие с отделом поддержки ЗАО «АВЕСТ» по вопросам эксплуатации программного обеспечения ЗАО «АВЕСТ» возможно при условии заключения потребителем договора с ЗАО «АВЕСТ» на сопровождение программных продуктов ЗАО «АВЕСТ».
2. Потребитель, получившей программное обеспечение ЗАО «АВЕСТ» на законных основаниях от третьей стороны, по вопросам эксплуатации программного обеспечения ЗАО «АВЕСТ» должен обращаться в организацию-поставщика программного обеспечения ЗАО «АВЕСТ».

9.3. Меры контроля

ПК AvPCM контролирует целостность своих программных модулей путем вычисления хэш-значений согласно СТБ 1176.1-99 от файлов MngCert.exe, AvCmUt.exe, avcryptokimt.dll, avcryptokibignmt.dll, AvCryptMail.dll, AvBelCert2.dll, AvLog4c.dll, avc.dll, CertStore.xml (при использовании файлового хранилища СОК и СОС), mac.ini. Перечень файлов и контрольных хэш-значений находится в файле mac.ini. При нарушении целостности данных файлов работа ПК AvPCM невозможна.

Пользователь может дополнительно контролировать целостность данных программных модулей ПК AvPCM путем вычисления хэш-значений согласно СТБ 1176.1-99 от данных файлов и сравнением их с эталонными, которые указаны в файле mac.ini.

ПРИЛОЖЕНИЕ

Настоящее приложение к документу РБ.ЮСКИ.08003-02 34 01 «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» содержит описание и информацию о возможности настроек программного комплекса на соответствие требованиям:

– разделов 6, 7 документа СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

– разделов 6, 7 документа РД РБ 07040.1206-2004 «Банковские технологии. Формат сертификатов открытых ключей и списков отозванных сертификатов»;

– раздела 5 документа СТБ 34.101.17-2012 Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».

Данное приложение содержит описание перечня полей, идентифицирующих пользователей и удостоверяющие центры, способе вычисления ЭЦП (определение входных данных алгоритмов ЭЦП), способе вычисления идентификаторов открытых ключей.

1. ПЕРЕЧЕНЬ ПОЛЕЙ, ИДЕНТИФИЦИРУЮЩИХ ПОЛЬЗОВАТЕЛЕЙ И УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

Определение полей идентифицирующих пользователей и удостоверяющие центры задается в файле шаблона на сертификат (файлы с расширением .tpl). Формат файла:

Секция **[TemplateName]** – наименование шаблона.

Допустимые ключи:

Name = 'наименование' – наименование шаблона;

Секция **[CommonName]** – алгоритм формирования атрибута «Общие данные» (CN) имени субъекта.

Допустимые ключи:

OID = – значение атрибута с указанным OID, включается в атрибут «Общие данные»;

Text = 'текст' – текст включается в атрибут «Общие данные»;

HASH=SHA1 – в итоге значение атрибута «Общие данные» будет содержать SHA1 от сформированного ранее значения атрибута;

Секция **[DATA]** – алгоритм формирования имени субъекта.

Допустимые ключи:

GroupName = 'наименование' – наименование группы данных;

OID = 'наименование атрибута' – атрибут с указанным OID, включается в имя субъекта;

Секция **[OID]** – алгоритм формирования атрибута имени субъекта.

Допустимые ключи:

Mandatory=Yes – данный атрибут должен иметь не пустое значение;

Default = 'значение' – значение атрибута по умолчанию;

ReadOnly=Yes – значение атрибута нельзя изменить оператором;

MaxLength = 'байт' – максимальная длина значение атрибута;

MinLength = 'байт' – минимальная длина значение атрибута;

CharSet = 'значение' – допустимый набор символов при заполнении значение атрибута. Значение ключа может быть DIGITS - ['0'..'9'], IA5STRING - ['!'..'~'];

CharCase = 'значение' – регистр при заполнении значение атрибута. Значение ключа может быть UPPERCASE - верхний, LOWERCASE - нижний;

ALT_NAME = True – данный атрибут будет помещен в дополнение альтернативное имя субъекта;

Control_Ext_Key_Usage = 'OID' – если данный атрибут имеет не пустое значение – в расширенное дополнение ключа будет добавлен указанный OID;

ExtDLL = 'секция' – для заполнения значения имени субъекта будет использована внешняя dll, описанная указанной секции;

SelectFrom = 'имя файла' – для заполнения имени субъекта будут использованы данные из файла, структура которого описана ниже. Если в качестве имени файла указано LDAP – данные будут получены из Active Directory по протоколу ldap.

Секция **[KEY_USAGE]** – применение ключа.

Допустимые ключи:

CERT_ENCIPHER_ONLY_KEY_USAGE = True - только шифрование;

CERT_CRL_SIGN_KEY_USAGE = True - автономное подписание CRL, Подписание CRL(C6);

CERT_KEY_CERT_SIGN_KEY_USAGE = True - подписание сертификата;

CERT_KEY_AGREEMENT_KEY_USAGE = True - согласование ключа;

CERT_DATA_ENCIPHERMENT_KEY_USAGE = True - шифрование данных;

CERT_KEY_ENCIPHERMENT_KEY_USAGE = True - шифрование ключа;

CERT_NON_REPUDIATION_KEY_USAGE = True - неотрекаемый;

CERT_DIGITAL_SIGNATURE_KEY_USAGE = True - цифровая подпись.

Секция **[EXT_KEY_USAGE]** – дополнительное применение ключа.

Допустимые ключи:

OID дополнительного применения ключа.

Секция **[CONTAINER_NAME]** – имя контейнера по умолчанию.

Допустимые ключи:

OID = значение атрибута с указанным OID, включается в имя контейнера;

Text = 'текст' – текст включается в имя контейнера;

Date = текущее дата и время включается в имя контейнера.

2. СПОСОБ ВЫЧИСЛЕНИЯ ЭЦП (ОПРЕДЕЛЕНИЕ ВХОДНЫХ ДАННЫХ АЛГОРИТМОВ ЭЦП)

Определение алгоритмов ЗЦП задается в настроечном файле программного комплекса AvCmMsg.ini, либо в файле шаблона на сертификат, в секции [CSP]. Допустимые ключи:

PROVNAME = 'имя' – имя криптопровайдера;

PROVTYPE = 'тип' – тип криптопровайдера;

KEYSPEC = 'тип' – тип ключа (1 - AT_KEYEXCHANGE, 2 - AT_SIGNATURE);

HASHALGORITHM = 'OID' - OID алгоритма хэширования;

PublicKeyObjId = 'OID' – OID открытого ключа;

ENCRYPTALGORITHM = 'OID' – OID алгоритма шифрования;

HASH_ALGID = 'алгоритм' - алгоритм хеширования (если требуется отличный от значения криптопровайдера по умолчанию);

CSPFlags = 'значение' – дополнительное значение флага передаваемое в функцию CryptAcquireContext;

DblCERT = True - использование раздельных сертификатов для подписи и шифрования;

FullParameters = True - кодирование параметров открытого ключа по значению, иначе по ссылке;

UseMSCryptoApi2ToSignCertificate = True - использовать функцию CryptSignAndEncodeCertificate MS Crypto Api 2 для создания сертификата (по умолчанию искользуется MS Crypto Api 1 и функции AvBelCert.dll).

3. СПОСОБ ВЫЧИСЛЕНИЯ ИДЕНТИФИКАТОРОВ ОТКРЫТЫХ КЛЮЧЕЙ

Идентификатор открытых ключей содержит результат хэширования функцией закодированного значения открытого ключа. Для совместимости с различными системами криптографической обработки информации существует несколько способов вычисления идентификатора открытого ключа, порядок которого задается в настроечном файле программного комплекса AvCmMsg.ini, либо в файле шаблона на сертификат, в секции [CSP] ключом KeyIdentifierType.

KeyIdentifierType может принимать нижеследующие значения:

0 – результат хэширования функцией в соответствии с алгоритмом SHA1;

1 – вычисление с использованием вызова функции MS Crypto API CryptHashPublicKeyInfo;

2 – результат хэширования функцией в соответствии с алгоритмом, установленным в СТБ 1176.1 со следующими значениями параметров:

H=4E4E9C9C9C9C4E4E9C9C4E4E4E4E9C9C9C9C4E4E4E4E9C9C4E4E9C9C9C9C4E4E

(в шестнадцатеричной системе счисления), L=160;

3 – результат хэширования функцией в соответствии с алгоритмом, установленным в СТБ 1176.1 со следующими значениями параметров: H=4E4E9C9C9C9C4E4E9C9C4E4E4E4E9C9C9C9C4E4E4E4E9C9C4E4E9C9C9C9C4E4E

(в шестнадцатеричной системе счисления), L=256.

10.ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД – база данных;

НКИ – носитель ключевой информации;

ПО – программное обеспечение;

ПСКЗИ – программное средство криптографической защиты информации;

СОК – сертификат открытого ключа;

СОС – список отозванных сертификатов;

УЦ – удостоверяющий центр;

ЦР – центр регистрации;

ЦС – центр сертификации.

Лист регистрации изменений

Номер листов (страниц)					Всего листов (страниц) в документе	№ документа	Входящий № сопроводи-тельного документа и дата	Подп.	Дата
Изм	Изме-нен-ных	Замененных	Новых	Аннули-рованных					