УТВЕРЖДЕН

РБ.ЮСКИ.08003-06 34 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС

«ПЕРСОНАЛЬНЫЙ МЕНЕДЖЕР СЕРТИФИКАТОВ АВЕСТ»

AvPCM

Руководство оператора

РБ.ЮСКИ.08003-06 34 01

Листов 151

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

2023

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта РБ.ЮСКИ.08003-06 «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM» (далее – ПК AvPCM). В документе приведены описание действий оператора при установке и использовании ПК AvPCM.

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

Изготовителем ПК AvPCM является белорусское предприятие «Закрытое акционерное общество «АВЕСТ» (ЗАО «АВЕСТ»).

Адрес предприятия: 220116, Республика Беларусь, г. Минск, пр-т газеты «Правда», д. 5, пом. 3Н, каб. 7.

Тел.: +375 (17) 257-99-74, +375 (17) 318-92-34, факс: +375 (17) 303-91-49.

Интернет-страница: https://www.avest.by.

Электронная почта: welcome@avest.by.

При обнаружении неисправности при эксплуатации ПК AvPCM необходимо прекратить эксплуатацию ПК AvPCM и связаться с производителем по вышеуказанным телефонам или электронной почте.

Гарантийный срок, обязательства изготовителя, дата изготовления ПК AvPCM указываются в лицензионном договоре при поставке ПК AvPCM в соответствии с законодательством 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, списками отозванных сертификатов и атрибутными сертификатами.

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.

Атрибутный сертификат (далее – АС) — сертификат специального формата, который используется для связывания дополнительной информации с сертификатом открытого ключа. Атрибутные сертификаты позволяют управлять доступом на основе определенных принципов, ролей, должностей. АС представляет собой структуру данных, заверенных цифровой подписью, и содержащую ссылку на один или несколько сертификатов открытых ключей одного и того же субъекта. Как правило, атрибутный сертификат содержит информацию о пользователе, группах доступа, в которых он состоит, а также его открытом ключе. Наличие таких сертификатов не только позволяет увеличить срок службы открытых ключей, а также существенно упростить работу с ИОК. Например, держатель одного публичного ключа может иметь множественные права доступа. Кроме того, при смене прав доступа требуется перевыпустить только атрибутный сертификат, не изменяя сертификат открытого ключа.

Главным отличием инфраструктуры управления привилегиями (далее – ИУП) от инфраструктуры открытых ключей (далее – ИОК) состоит в том, что ИОК управляет сертификатами открытых ключей, а ИУП — атрибутными сертификатами. ИУП является скорее надстройкой над инфраструктурой открытых ключей, а не ее частью. Сертификат открытого ключа отвечает за аутентификацию пользователя, подтверждение личности (его можно сравнить с паспортом субъекта), а атрибутный сертификат — за его авторизацию, подтверждение прав (можно сравнить с визой). Кроме того, АС обычно имеют меньший срок действия, чем личные сертификаты.

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», а также специализированные программно-аппаратных СКЗИ

Для работы ПК AvPCM необходимо наличие на компьютере пользователя установленного одного из следующих криптопровайдеров или специализированных программно-аппаратных СКЗИ:

- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP» AvCSP (РБ.ЮСКИ.08000-03) (далее – криптопровайдер AvCSP): 32- разрядная версия

AvCSP в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSP в 64-разрядных версиях ОС;

- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BEL» AvCSPBEL (РБ.ЮСКИ.12004-02) (далее – криптопровайдер AvCSPBEL): 32-разрядная версия AvCSPBEL в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSPBEL в 64-разрядных версиях ОС;
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BIGN» AvCSPBIGN (РБ.ЮСКИ.12005-02) (далее – криптопровайдер AvCSPBIGN) (32-разрядная версия AvCSPBIGN в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSPBIGN в 64-разрядных версиях ОС), использующий криптографические сервисы изделия Устройства программно-аппаратные электронной цифровой подписи и шифрования «AvBign» (ИЯТА.467532.003);
- устройство программно-аппаратное криптографическое «AvHSM-Bign» (ИЯТА.466217.003) (далее – устройство «AvHSM-Bign»);
- устройство программно-аппаратное электронной цифровой подписи и шифрования «AvBign» (ИЯТА.467532.003) (далее – устройство «AvBign»).

ПК AvPCM предоставляет пользователю ИОК следующие сервисы:

- генерация с помощью криптопровайдеров личных и открытых ключей ЭЦП и шифрования пользователя, удовлетворяющих требованиям СТБ 34.101.31-2020, СТБ 34.101.45-2013, СТБ 34.101.78-2019;
- формирование запроса на сертификат к удостоверяющему центру в соответствии с требованиями СТБ 34.101.17-2012 (PKCS#10), СТБ 34.101.78-2019;
- формирование запроса на атрибутный сертификат к центру атрибутных сертификатов в соответствии с СТБ 34.101.67-2014;
- поддержка СОК и СОС, удовлетворяющих требованиям СТБ 34.101.19-2012 (X.509) и СТБ 34.101.78-2019;
- поддержка атрибутных сертификатов, удовлетворяющих требованиям СТБ 34.101.67-2014;
- поддержка форматов параметров криптографических алгоритмов согласно СТБ 34.101.23-2012 (PKCS#7), СТБ 34.101.78-2019;
- 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, ЦР и САС;
- 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, атрибутных сертификатов и СОС;
- ведение журнала работы ПК AvPCM с обеспечением контроля целостности файла журнала;
- использование криптографических сервисов, реализуемых устройством AvBign;
- использование криптографических сервисов, реализуемых устройством AvHSM-Bign.

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

Взаимодействие ПК AvPCM с устройством AvBign/AvHSM-Bign осуществляется в соответствии с интерфейсом, определенным в СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)» (PKCS#11).

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

1) СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»;
2) СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;
3) СТБ 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)» (PKCS#11);
4) СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;
5) СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»;
6) СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»;
7) СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности»;
8) СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых»;
9) СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;
10) СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»;
11) СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов»;
12) СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

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

- Windows 2008 R1 Server (x32, x64);
- Windows 2008 R2 Server (x64);
- Windows 2012 Server (x64);
- Windows 2012 R2 Server (x64);
- Windows 10 (x32, x64);
- Windows 2016 Server (x64);
- Windows 2019 Server (x64).

Примечание. Допускается работа AvPCM в среде следующих ОС Windows, которые сняты с поддержки компании Microsoft:

- Windows 2003 Server (x32, x64) SP2;
- Windows XP SP3 (x32) ;
- Windows 7 (x32, x64);
- Windows 8 (x32, x64);
- Windows 8.1 (x32, x64).

В случае использования вышеуказанных ОС, снятых с поддержки компании Microsoft, устойчивая работа AvPCM не гарантируется.

Для использования ПК AvPCM пользователь должен иметь права «Administrator (Администратор)» либо «Power User (Опытный пользователь)».

Необходимо установить поддержку русского языка для программ, не поддерживающих Юникод. Для этого:

В ОС Windows XP, Windows 2003 Server:

1. Перейти в меню «Start» - «Control Panel» («Пуск» - «Панель управления»), в зависимости от параметров просмотра элементов в панели управления (классический вид или по категориям) выбрать «Regional and Language Options» («Язык и региональные стандарты») или «Date, Time, Language and Regional Options» - «Regional and Language Options» («Дата, время, язык и региональные стандарты» - «Язык и региональные стандарты»).
2. На вкладке «Regional options» («Региональные параметры») в поле «Standards and formats» («Языковые стандарты и форматы») выбрать русский язык, в поле «Location» («Расположение») указать Беларусь, на вкладке «Advanced» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») выбрать русский язык.
3. Выполнить перезагрузку.
4. Проверить отображение кодировки.

В ОС Windows 7, Windows 2008 Server:

1. Перейти в меню «Start» - «Control Panel» («Пуск» - «Панель управления»), в зависимости от параметров отображения элементов в панели управления (категория или значки) выбрать «Clock, Language and Region» - «Region and Language» («Часы, язык и регион» - «Язык и региональные

стандарты») или «Region and Language» («Язык и региональные стандарты»).

2. На вкладке «Formats» («Форматы») выбрать русский язык, на вкладке «Location» («Расположение») выбрать «Беларусь», на вкладке «Administrative» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») нажать кнопку «Изменить язык системы…» («Change system locale...»), в окне «Region and Language settings» («Язык и региональные стандарты») выбрать русский язык.

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

В ОС Windows 8, Windows 8.1, Windows 2012 Server:

1. Перейти в «Control Panel» («Панель управления») одним из способов, предусмотренных для данных ОС. Например, навести курсор мыши на правый верхний или нижний угол рабочего стола. В открывшейся боковой панели выбрать пункт «Settings» («Параметры»). В списке параметров выбрать пункт «Control Panel» («Панель управления»). Другой способ – нажать правой клавишей мыши по кнопке «Start» («Пуск»), выбрать пункт «Control Panel» («Панель управления»). При этом нужно учитывать, что в ОС Windows 8 данная кнопка не отображается, для ее отображения нужно на рабочем столе переместить курсор в нижний левый угол экрана. Далее, в зависимости от параметров просмотра элементов, в панели управления (категория или значки) выбрать «Clock, Language and Region» - «Region» («Часы, язык и регион» - «Региональные стандарты») или «Region» («Региональные стандарты»).

2. На вкладке «Formats» («Форматы») выбрать русский язык, на вкладке «Location» («Местоположение») выбрать «Беларусь», на вкладке «Administrative» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») нажать кнопку «Изменить язык системы» («Change system locale...»), в окне «Region and Language settings» («Региональные стандарты») выбрать русский язык.

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

В ОС Windows 10, Windows 2016 Server, Windows 2019 Server:

1. Перейти в «Control Panel» («Панель управления») одним из способов, предусмотренных для данных ОС. Например, в строке поиска ввести «Control». Другой способ – нажать «Start» («Пуск»), в списке приложений найти «Windows System» («Служебные Windows»), выбрать «Control Panel» («Панель управления»). Далее, в зависимости от параметров просмотра элементов в панели управления (категория или значки) выбрать «Clock and Region» - «Region» («Часы и регион» - «Региональные стандарты») или «Region» («Региональные стандарты»).

2. На вкладке «Formats» («Форматы») выбрать русский язык, на вкладке «Administrative» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») нажать кнопку «Изменить язык системы» («Change system locale...»), в окне «Region settings» («Региональные стандарты») выбрать русский язык. Галочку на пункте «Beta: Use Unicode UTF-8 for worldwide language support» («Бета-версия: Использовать Юникод (UTF-8) для поддержки языка во всем мире») не устанавливать.

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

ПК AvPCM предназначен для работы на компьютере (сервере), имеющем следующие

минимальные технические характеристики:

- процессор x86 (x64) с тактовой частотой - не менее 2,5 ГГц;
- объем ОЗУ - не менее 4 Гб;
- жесткий диск, содержащий не менее 8 Гб свободного пространства для стандартной установки ОС;
- монитор с поддержкой VGA или более высокого разрешения;
- манипулятор «мышь» Microsoft или совместимое указывающее устройство,
- свободный USB-порт.

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

Для работы ПК AvPCM необходимо наличие на компьютере пользователя установленного криптопровайдера (AvCSP, AvCSPBEL, AvCSPBIGN) или специализированных программно-аппаратных СКЗИ (устройство AvBign/AvHSM-Bign), подробнее см. п. 1. Назначение программы.

Для возможности работы с хранилищем данных в БД на компьютере должно быть установлено клиентское программное обеспечение для одной из приведенных ниже СУБД:

- MySQL Community Edition версии 5.0, 5.5, 5.6, 5.7, 8.0.11 со специальным драйвером ODBC (поставляется ЗАО "АВЕСТ" по запросу);
- Sybase ASE 12.5.3 (возможно лишь восстановление уже существующей БД из резервной копии/импорт базы данных сертификатов);
- Oracle 9.0.2.1, 10.2.0.4, 11.1.0.6, 11.2.0.3, 12.1.0.1, 19.3c.

Отдельные параметры выполнения ПК AvPCM настраиваются посредством редактирования файла AvCmMsg.ini. Описание параметров приведено в Приложение 2, пример конфигурационного файла – в Приложение 3.

ВНИМАНИЕ. Если инфраструктура предполагает необходимость подключения к базе данных конечных пользователей, не рекомендуется подключение пользователей напрямую к базе данных Удостоверяющего центра. Следует создать дублирующую базу данных, в которую будет происходить репликация данных из основной базы данных УЦ в одностороннем порядке. При этом каждый пользователь должен иметь свою собственную учетную запись в БД.

2.1. Режим безопасной загрузки (Secure Boot)

Для ОС Microsoft Windows 8.1 и выше характерно наличие включенного режима безопасной загрузки (SecureBoot) в BIOS. В большинстве случаев данный режим характерен для ноутбуков с предустановленной ОС, однако современные материнские платы для стационарных ПК также могут содержать данный режим.

Если в BIOS режим безопасной загрузки Secure Boot включен, то перед аутентификацией по TLS в браузере Microsoft Internet Explorer данный режим нужно отключить. Инструкции по отключению настройки Secure Boot в BIOS следует искать в сопутствующей документации к модели компьютера, опираясь на модель материнской платы и версию BIOS.

Проверить статус данного режима можно следующим образом: запустить утилиту msinfo32, просмотреть статус строки «Состояние безопасной загрузки». Если состояние «Вкл.», то Secure Boot включен и его следует отключить (см. Рисунок 1. Состояние безопасной загрузки).

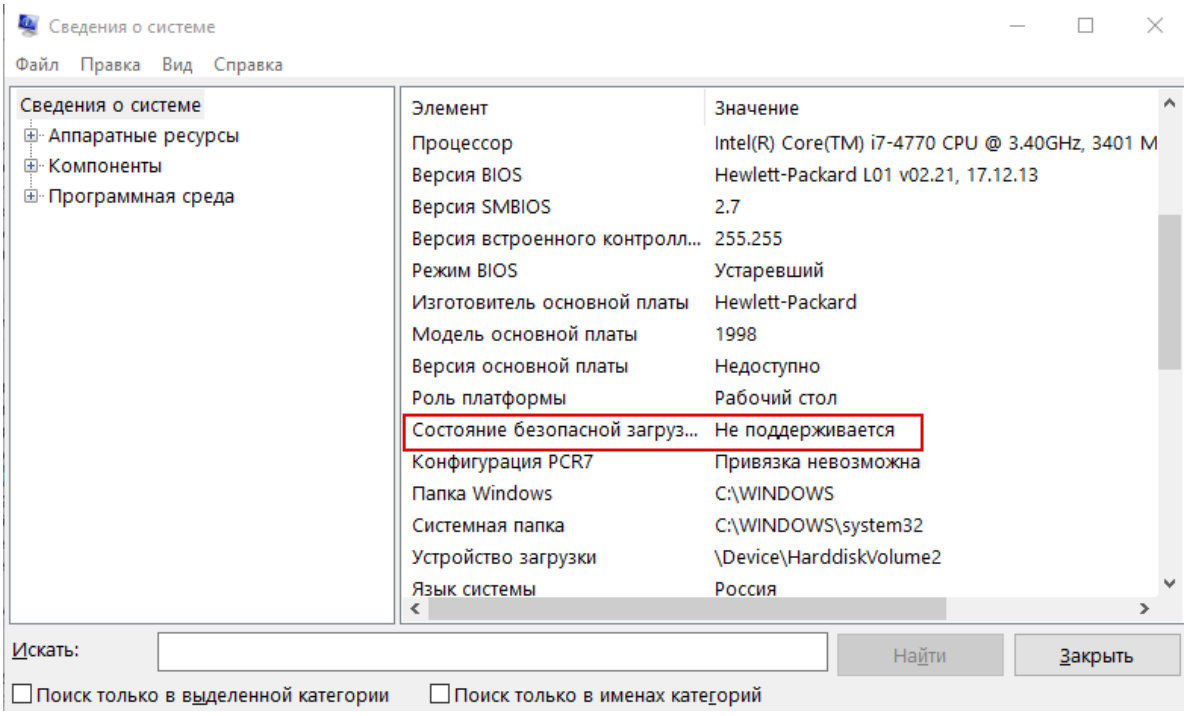


Рисунок 1. Состояние безопасной загрузки

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 нужно 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 нужно проверить, установлен ли на компьютере, на котором будет произведена установка программы, криптопровайдер Avest CSP («Пуск»⇒ «Панель управления» ⇒ «Программы и компоненты») и подключен ли свободный носитель для записи личных ключей пользователя. В случае, если криптопровайдер еще не был установлен, произвести его установку. Установка криптопровайдера не требуется в случае использования устройств AvBign/AvHSM-Bign (в соответствии с интерфейсом PKCS#11) в качестве хранилища личных ключей пользователя.

ПК AvPCM поддерживает 4 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;
- установка с хранилищем в AvHSM/AvBign.

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

Для использования ПК AvPCM с криптопровайдером Avest CSP BEL X.X.X.XXX в качестве файла настроечных данных следует использовать файлы типа AvCmED_Main_Bel.zip.

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

Примечание. В зависимости от комплекта поставки названия файлов настроечных данных могут отличаться.

Выбор варианта установки программы зависит от необходимости использования различных криптографических алгоритмов и OID (см. Приложение 1).

4.1. Установка с сетевой БД

ВНИМАНИЕ! Перед установкой 64-разрядной версии ПК AvPCM с сетевой БД MySQL нужно установить mysql-connector-odbc-8.0.X-winx64.msi.

Для работы ODBC connector обязательна установка версии Microsoft .NET версии 4.2 и выше, а также Microsoft Visual C++ 2015 Redistributable (x64). Подробная информация по установке 64-битного MySQL ODBC connector в зависимости от версии БД MySQL указана в соответствующей документации разработчика БД.

ВНИМАНИЕ! При подключении к базе данных Oracle необходимо зарегистрировать библиотеку OraOLEDB11.dll. Для этого нужно зайти в каталог с установленной базой данных, найти папку BIN, вызвать из нее командную строку от имени администратора и запустить команду:

```
regsvr32 OraOLEDB11.dll
```

После чего требуется перезагрузить компьютер.

Действия по установке ПК AvPCM:

1) запустить с дистрибутива программу AvPCM_DB_setup.exe (AvPCMEx_DB_setup.exe) - 32-разрядные версии, или AvPCM_DB_setup64.exe (AvPCMEx_DB_setup64).exe - 64-разрядные версии.

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

В начале установки выводится стандартное окно с информацией о предполагаемом к установке программном обеспечении (см. Рисунок 2. Заставка начала инсталляции ПК AvPCM).

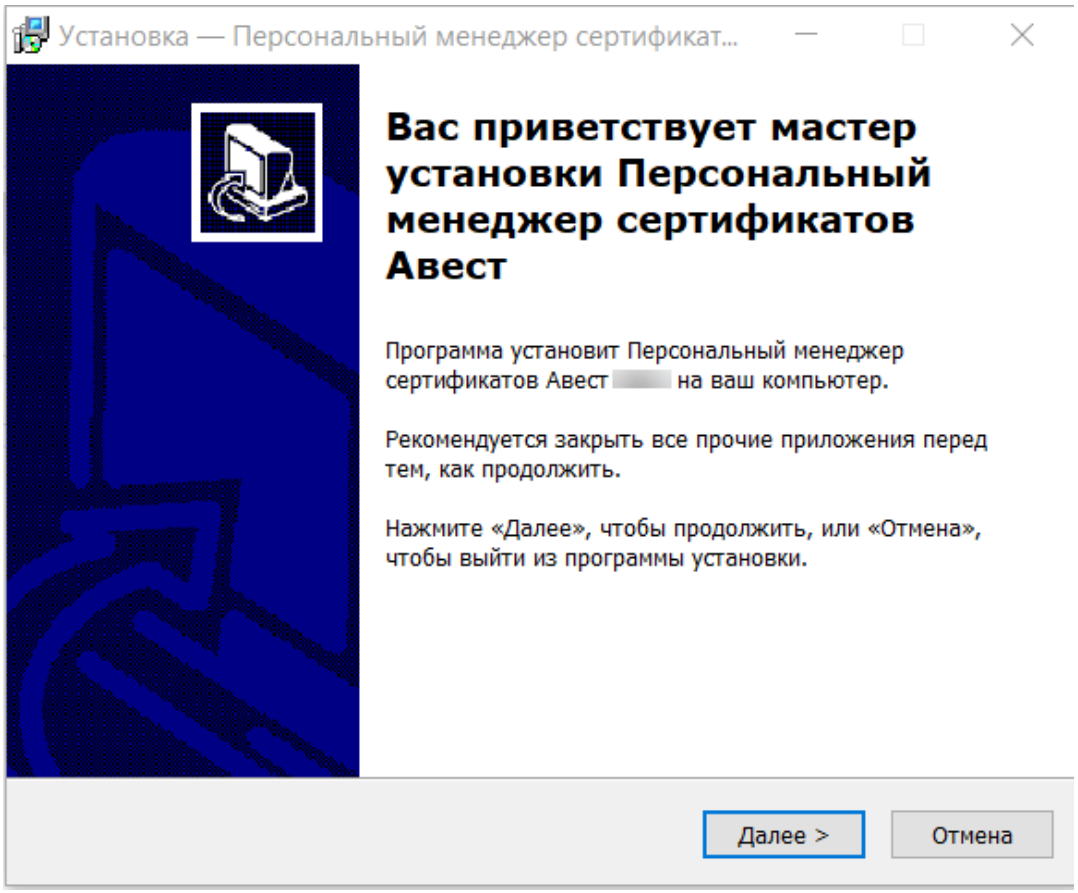


Рисунок 2. Заставка начала инсталляции ПК AvPCM

2) 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, надо нажать кнопку «Отмена» для выхода из программы.

3) Определить основную папку, в которой будут расположены устанавливаемые компоненты (см. Рисунок 3. Выбор папки установки программы).

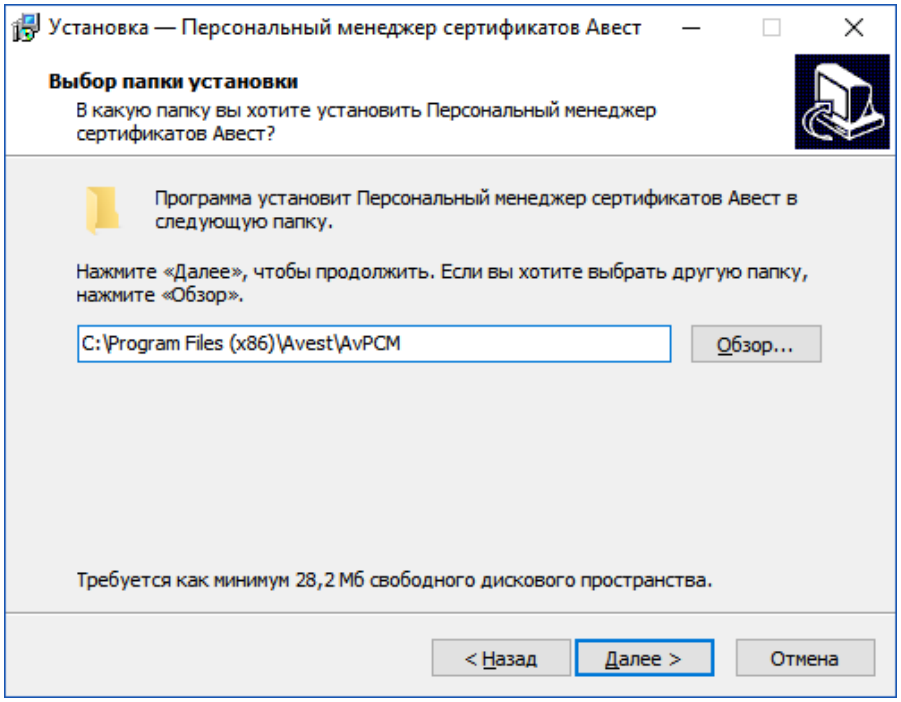


Рисунок 3. Выбор папки установки программы

4) 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 4. Выбор компонентов).

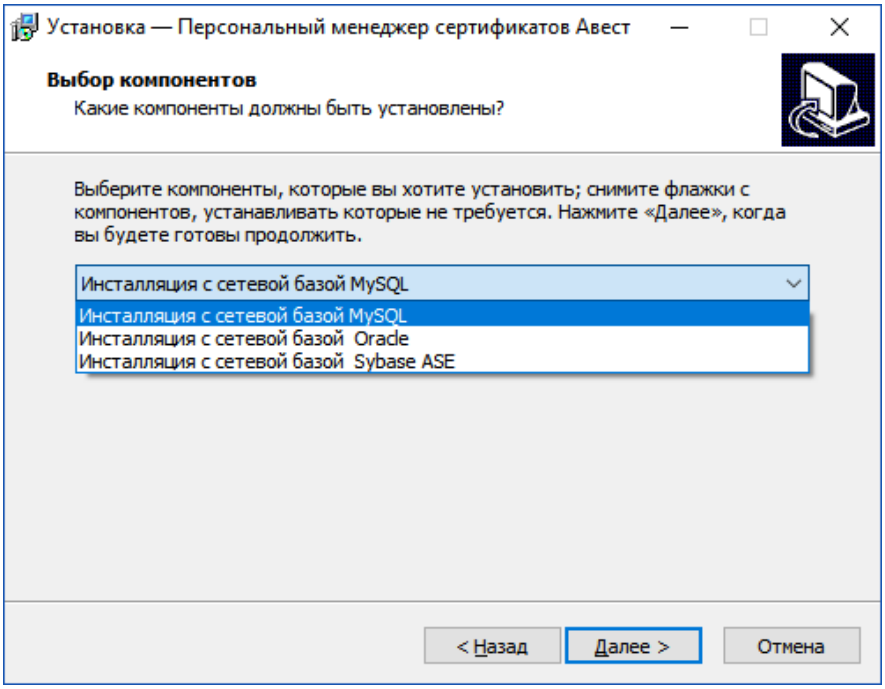


Рисунок 4. Выбор компонентов

5) 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 5. Параметры установки программы).

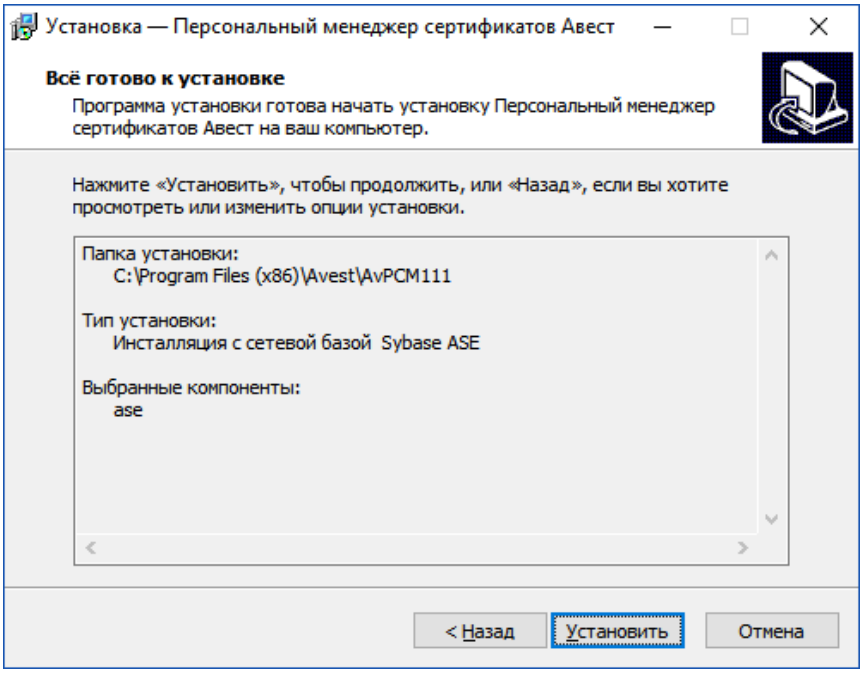


Рисунок 5. Параметры установки программы

ПК AvPCM произведет распаковку и копирование файлов программного обеспечения.

6) 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 надо снять все флажки и нажать кнопку «Завершить».

7) Затем следует произвести настройку сетевого доступа к базе данных справочников сертификатов (см. Приложение 4. Настройка сетевого подключения к базе данных).

Процесс установки ПК AvPCM завершен.

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»;
- «Персональный менеджер сертификатов (Руководство пользователя)».

На рабочем столе появится ярлык для быстрого запуска «Персональный менеджер сертификатов Авест».

Примечание. В зависимости от комплекта поставки название папки в меню «Пуск» и название ярлыка на рабочем столе могут отличаться.

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 (см. п. 4.1 Установка с сетевой БД). Основное отличие в том, что используются установочные файлы AvPCM_setup.exe (AvPCMEx_setup.exe) – 32-разрядные версии, или AvPCM_setup64.exe (AvPCMEx_setup64.exe) – 64-разрядные версии, и в окне «Выбор компонентов» требуется указать «Инсталляция с файловой базой данных сертификатов» или «Инсталляция с базой данных сертификатов в реестре» (см. Рисунок 6. Выбор компонентов).

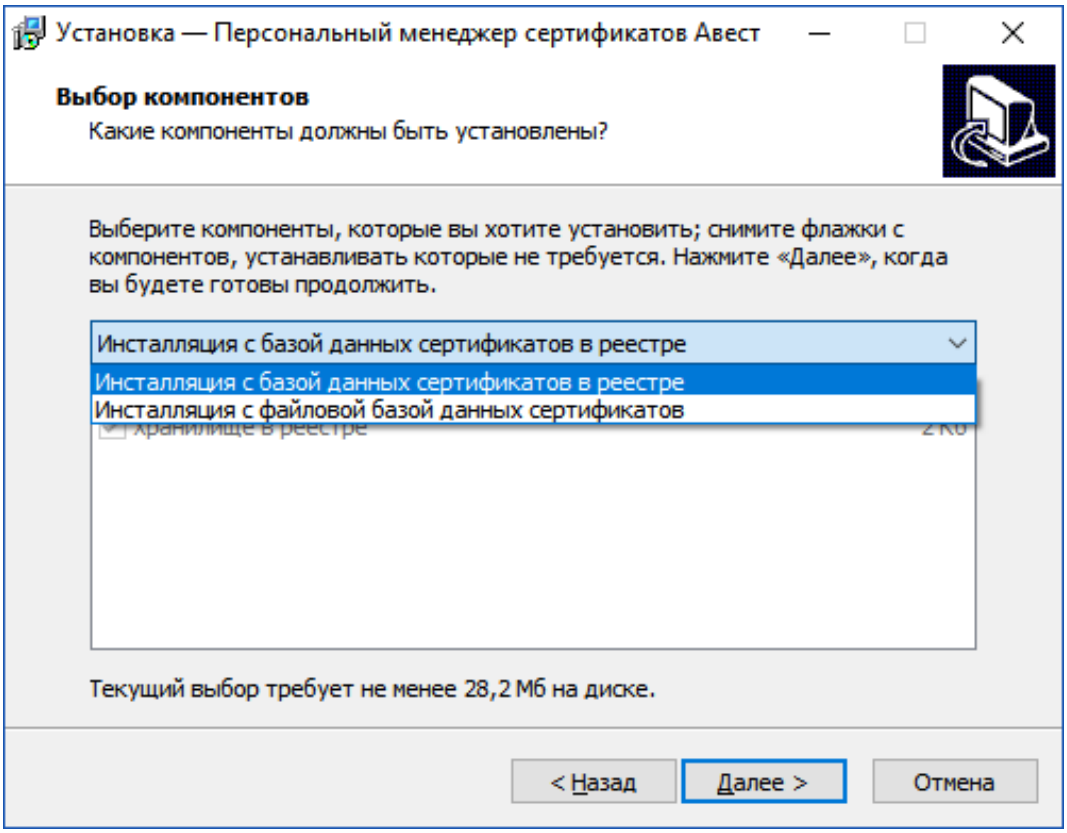


Рисунок 6. Выбор компонентов

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. Завершение работы мастера установки программы).

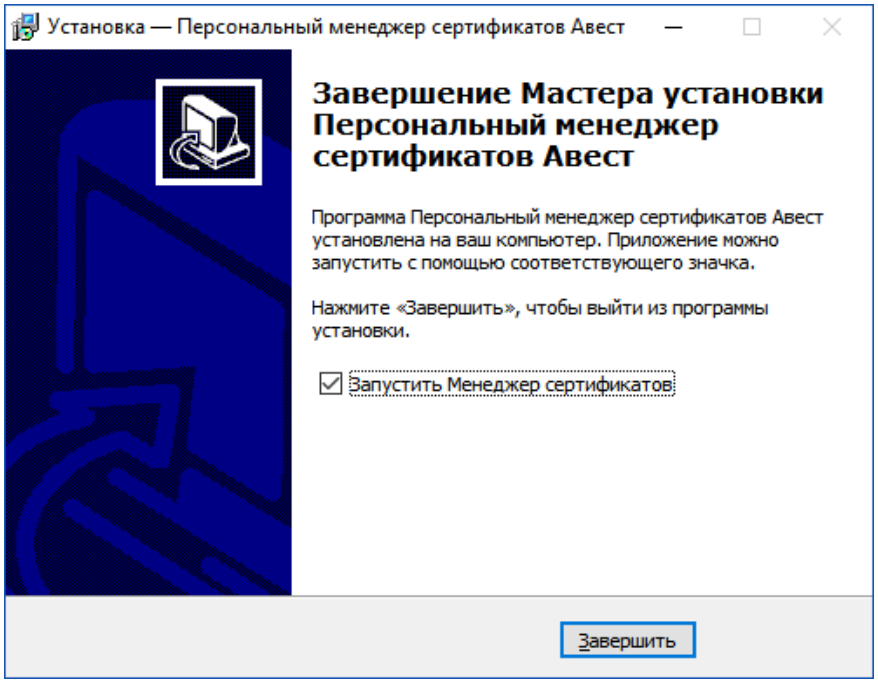


Рисунок 7. Завершение работы мастера установки программы

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»;
- «Персональный менеджер сертификатов (Руководство пользователя)».

На рабочем столе появится ярлык для быстрого запуска «Персональный менеджер сертификатов Авест».

Примечание. В зависимости от комплекта поставки название папки в меню «Пуск» и название ярлыка на рабочем столе могут отличаться.

4.3. Установка с использованием устройства AvBign и сетевой БД

ВНИМАНИЕ! Перед установкой AvPCM с использованием устройства AvBign, обеспечивающего использование аппаратной реализации криптографических алгоритмов в соответствии с интерфейсом PKCS#11, нужно убедиться, что на компьютере пользователя AvPCM установлен драйвер для устройства AvBign и устройство AvBign установлено в USB-порт.

ВНИМАНИЕ! Перед установкой 64-разрядной версии ПК AvPCM с сетевой БД MySQL нужно установить mysql-connector-odbc-8.0.X-winx64.msi.

Для работы ODBC connector обязательна установка версии Microsoft .NET версии 4.2 и выше, а также Microsoft Visual C++ 2015 Redistributable (x64). Подробная информация по установке 64-битного MySQL ODBC connector в зависимости от версии БД MySQL указана в соответствующей документации разработчика БД.

ВНИМАНИЕ! При подключении к базе данных Oracle необходимо зарегистрировать библиотеку OraOLEDB11.dll. Для этого нужно зайти в каталог с установленной базой данной, найти папку BIN, вызвать из нее командную строку от имени администратора и запустить команду:

```
regsvr32 OraOLEDB11.dll
```

После чего требуется перезагрузить компьютер.

Действия по установке ПК AvPCM:

1) запустить с дистрибутива программу AvPCMwEx_setup.exe (32-разрядная версия) или AvPCMwEx_setup64.exe (64-разрядная версия).

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 2. Заставка начала инсталляции ПК AvPCM).

2) 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.

3) Определить основную папку, в которой будут расположены устанавливаемые компоненты (см. Рисунок 8. Выбор папку установки программы AvPCMHSM).

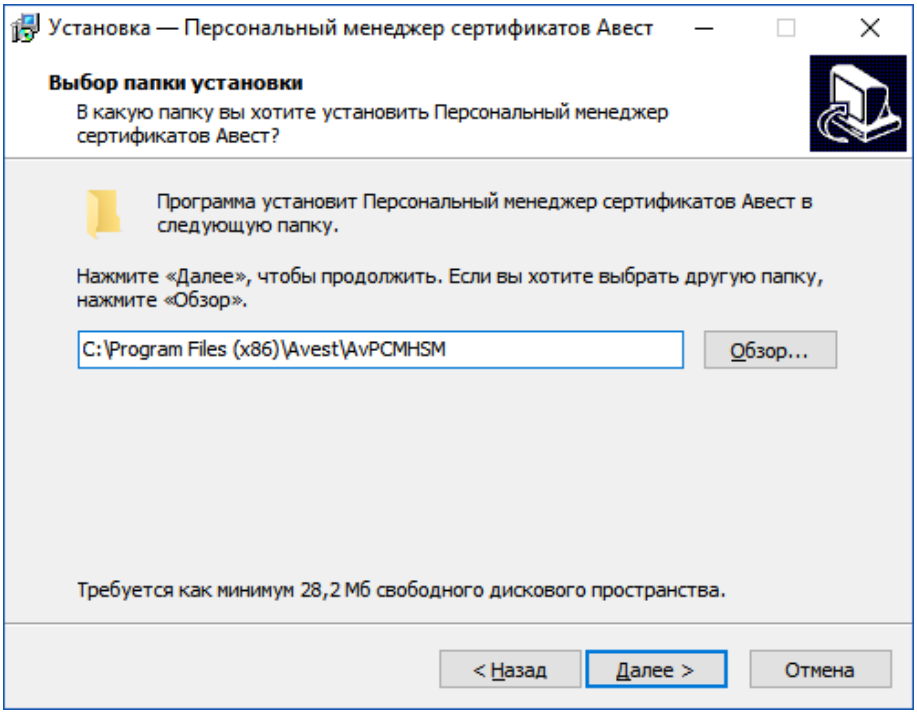


Рисунок 8. Выбор папку установки программы AvPCMHSM

4) Определить тип установки ПК AvPCM. В окне «Выбор компонентов» требуется выбрать из встроенного списка тип хранилища личных ключей **AvBign** и сертификатов (БД MySQL либо БД Oracle), и нажать кнопку «Далее» (см. Рисунок 9. Выбор компонентов).

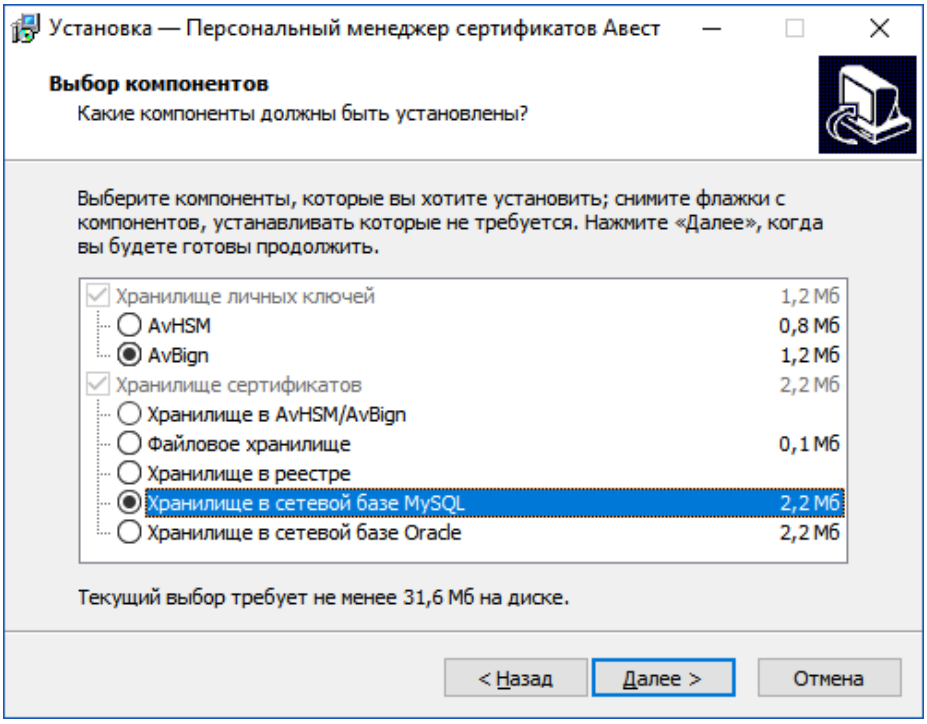


Рисунок 9. Выбор компонентов

5) 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 10. Параметры установки программы).

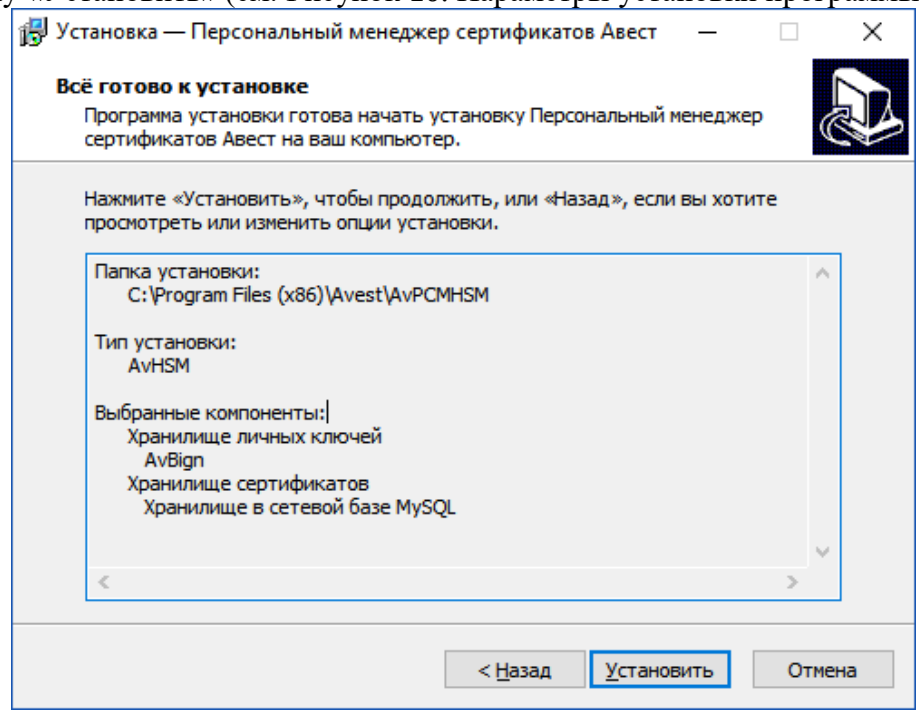


Рисунок 10. Параметры установки программы

ПК AvPCM произведет распаковку и копирование файлов программного обеспечения. В процессе установки следует произвести настройку сетевого доступа к базе данных справочников сертификатов (см. Приложение 4. Настройка сетевого подключения к базе данных).

Процесс установки ПК AvPCM завершен.

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»;
- «Персональный менеджер сертификатов (Руководство пользователя)».

На рабочем столе появится ярлык для быстрого запуска «Персональный менеджер сертификатов Авест».

Примечание. В зависимости от комплекта поставки название папки в меню «Пуск» и название ярлыка на рабочем столе могут отличаться.

4.4. Установка с устройством AvHSM-Bign и сетевой БД

ВНИМАНИЕ! Перед установкой 64-разрядной версии ПК AvPCM с сетевой БД MySQL нужно установить mysql-connector-odbc-8.0.X-winx64.msi.

Для работы ODBC connector обязательна установка версии Microsoft .NET версии 4.2 и выше, а также Microsoft Visual C++ 2015 Redistributable (x64) Подробная информация по установке 64-битного MySQL ODBC connector в зависимости от версии БД MySQL указана в соответствующей документации разработчика БД.

ВНИМАНИЕ! Перед установкой AvPCM с использованием устройства AvHSM-Bign, обеспечивающего использование аппаратной реализации криптографических алгоритмов в соответствии с интерфейсом PKCS#11, нужно убедиться, что устройство AvHSM-Bign подключено при помощи сетевого соединения Ethernet и находится с той же подсети, что и компьютер пользователя AvPCM.

ВНИМАНИЕ! При подключении к базе данных Oracle необходимо зарегистрировать библиотеку OraOLEDB11.dll. Для этого нужно зайти в папку с установленной базой данных, найти папку BIN, вызвать из нее командную строку от имени администратора и запустить команду:

```
regsvr32 OraOLEDB11.dll
```

После чего требуется перезагрузить компьютер.

Действия по установке ПК AvPCM:

процедура установки программы с использованием устройства AvHSM-Bign аналогична процедуре, описанной в п. 4.3 Установка с использованием устройства AvBign и сетевой БД. Однако для данного вида установки в окне «Выбор компонентов» требуется выбрать пункт «Хранилище личных ключей» − «**AvHSM**» (см. Рисунок 11. Выбор компонента AvHSM).

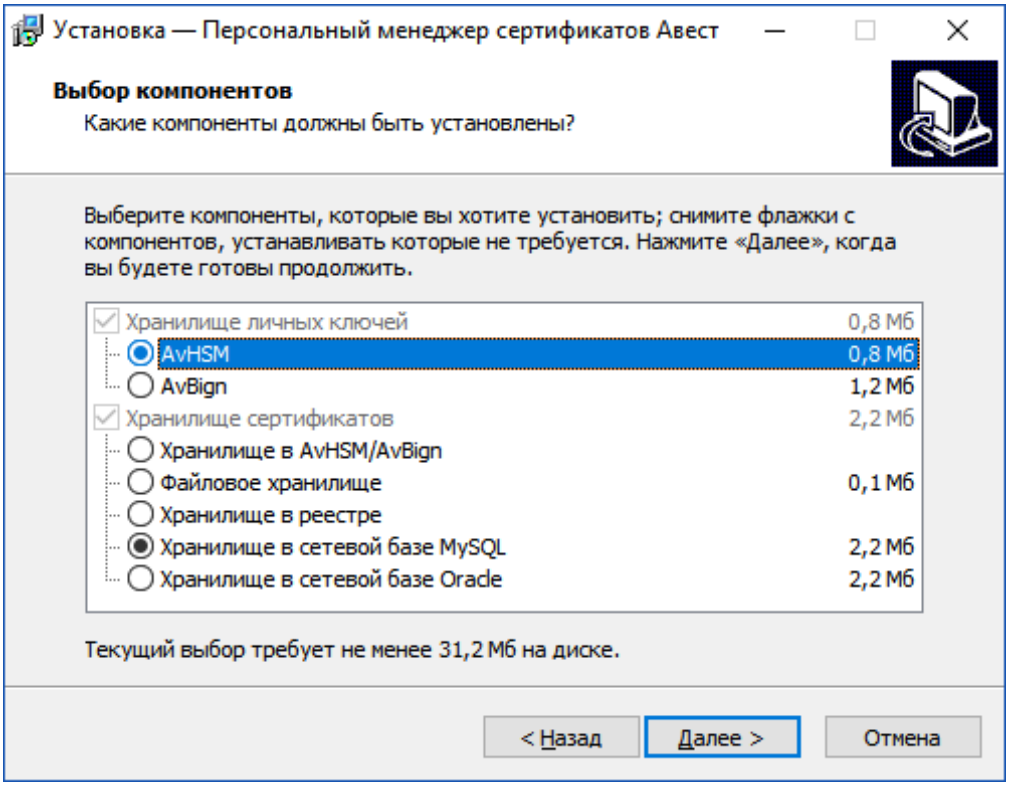


Рисунок 11. Выбор компонента AvHSM

В следующем окне нужно указать параметры подключения к устройству AvHSM-Bign. Необходимо указать IP-адрес устройства, TCP/IP порт, а также идентификатор внутреннего слота AvHSM-Bign (см. Рисунок 12. Настройка подключения к AvHSM).

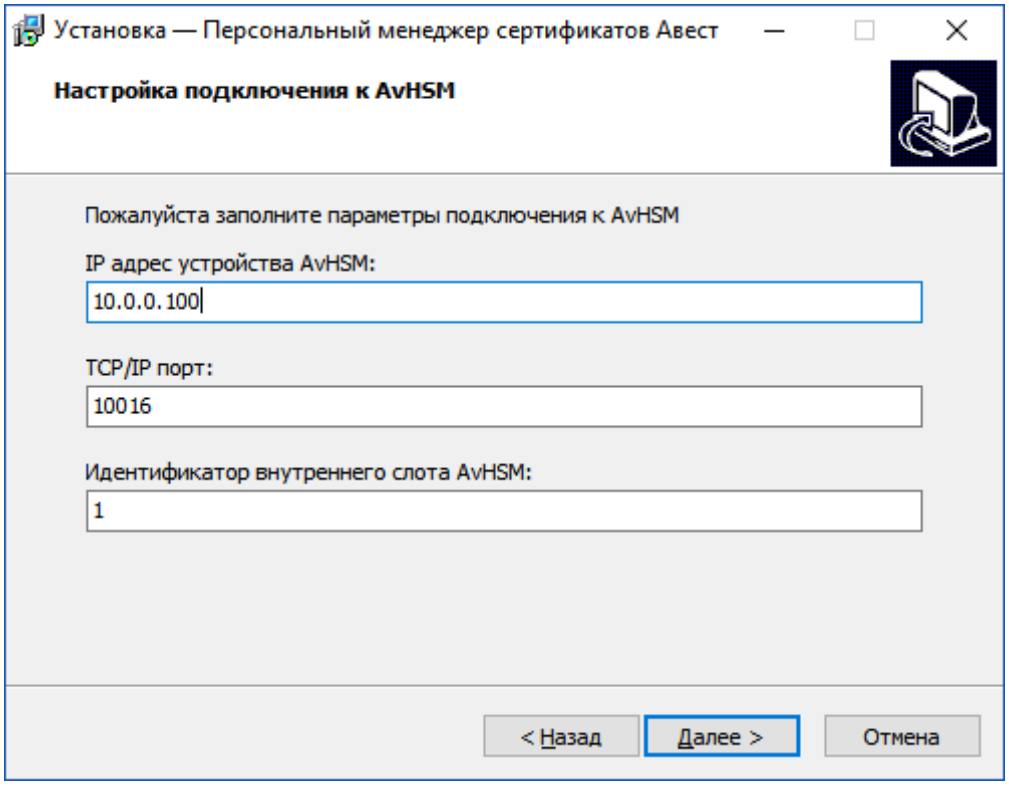


Рисунок 12. Настройка подключения к AvHSM

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 10. Параметры установки программы).

ПК AvPCM произведет распаковку и копирование файлов программного обеспечения. В процессе установки следует произвести настройку сетевого доступа к базе данных справочников сертификатов (см. Приложение 4. Настройка сетевого подключения к базе данных).

Процесс установки ПК AvPCM завершен.

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»;
- «Персональный менеджер сертификатов (Руководство пользователя)».

На рабочем столе появится ярлык для быстрого запуска «Персональный менеджер сертификатов Авест».

Примечание. В зависимости от комплекта поставки название папки в меню «Пуск» и название ярлыка на рабочем столе могут отличаться.

4.5. Установка с устройством AvBign/AvHSM-Bign и с файловой базой данных (с базой данных в реестре, с хранилищем сертификатов в AvBign/AvHSM-Bign)

Установка ПК AvPCM с файловой базой данных, базой данных сертификатов в системном реестре Windows и с хранилищем сертификатов в AvHSM/AvBign производится аналогично установке с сетевой базой данных (см. п. 4.1 Установка с сетевой БД), установке с использованием устройства программно-аппаратного хранения информации AvBign и сетевой БД (см. п. 4.3 Установка с использованием устройства AvBign и сетевой БД), установке с использованием устройства программно-аппаратного хранения информации AvHSM-Bign и сетевой БД (см. п. 4.4 Установка с устройством AvHSM-Bign и сетевой БД). Однако отличается тем, что в окне «Выбор компонентов» требуется указать не Базу данных, а «Файловое хранилище», либо «Хранилище в реестре», либо «Хранилище в AvHSM/AvBign» (см. Рисунок 9. Выбор компонентов).

ВНИМАНИЕ! Если в процессе установки было выбрано хранилище личных ключей в AvHSM (AvBign) и хранилище сертификатов в AvHSM/AvBign, и ключи, и сертификаты будут храниться во внутреннем хранилище устройства AvHSM-Bign (AvBign).

Примечание. В зависимости от комплекта поставки название папки в меню «Пуск» и название ярлыка на рабочем столе могут отличаться.

5. ЗАПУСК ПРОГРАММЫ

5.1. Запуск программы, настроенной на использование криптопровайдера

Запуск ПК AvPCM, настроенного на использование одного из криптопровайдеров (криптопровайдер AvCSP, AvCSPBEL, AvCSPBIGN), может производиться 2-мя способами:

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

Примечание. В зависимости от комплекта поставки название папки в меню «Пуск» и название ярлыка на рабочем столе могут отличаться.

Вход в систему осуществляется через авторизацию пользователя, для этого в окне авторизации надо выбрать идентификатор ключевого контейнера, соответствующий личному ключу пользователя, после чего ввести пароль доступа к нему (см. Рисунок 13. Авторизация пользователя).

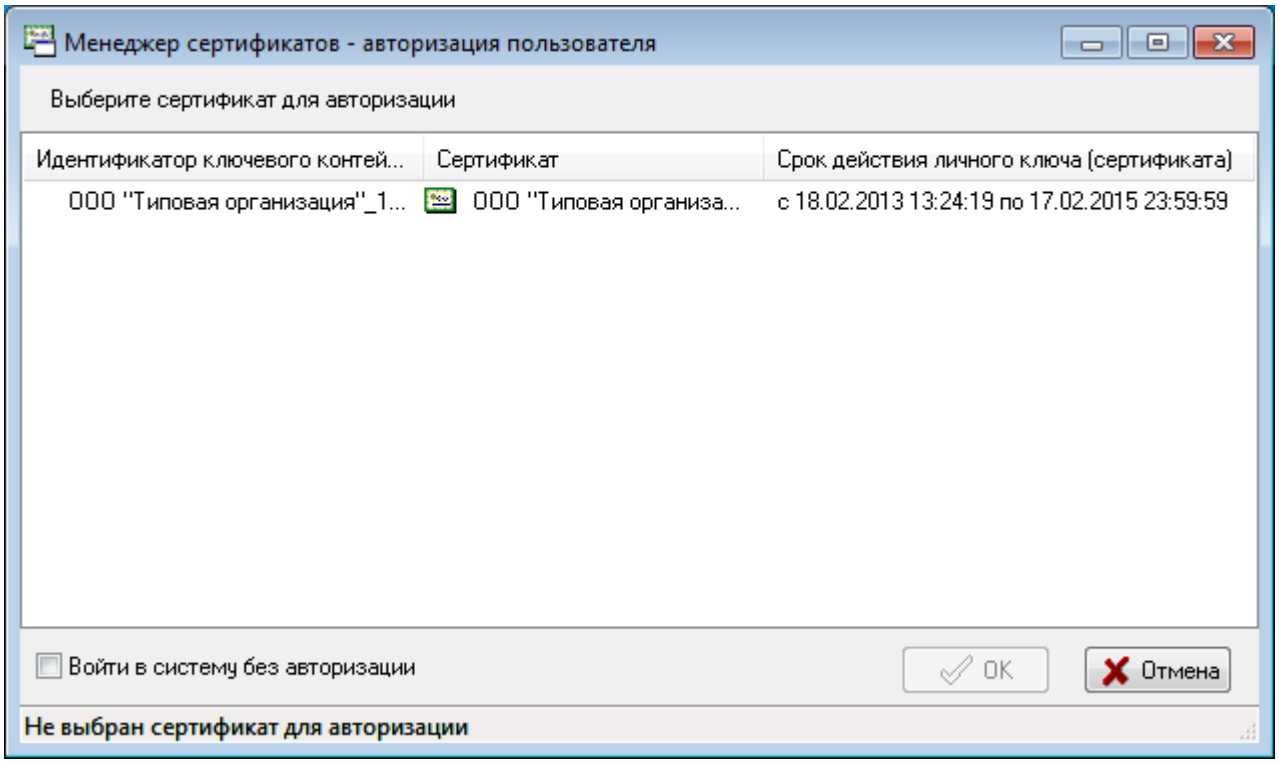


Рисунок 13. Авторизация пользователя

5.2. Запуск программы, настроенной на использование устройства AvBign

Вход в систему осуществляется через авторизацию пользователя. Для этого после запуска ПК AvPCM с ярлыка на рабочем столе, или через меню «Пуск» в появившемся окне надо ввести пароль к устройству AvBign (см. Рисунок 14. Ввод пароля к устройству AvBign).

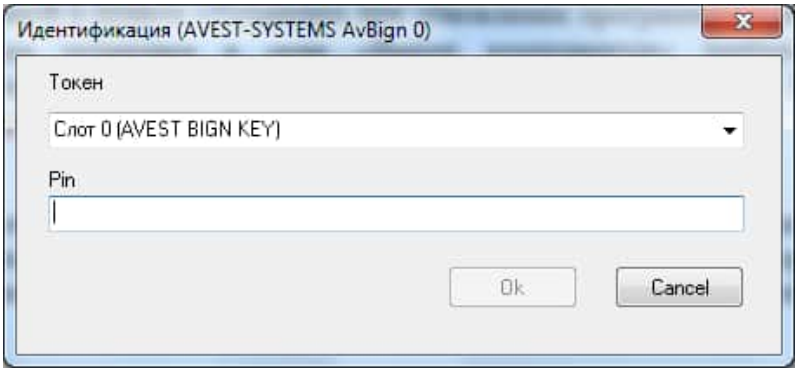


Рисунок 14. Ввод пароля к устройству AvBign

Далее надо выбрать идентификатор ключевого контейнера, нажать OK и выполнить вход в систему (см. Рисунок 15. Выбор активного сертификата).

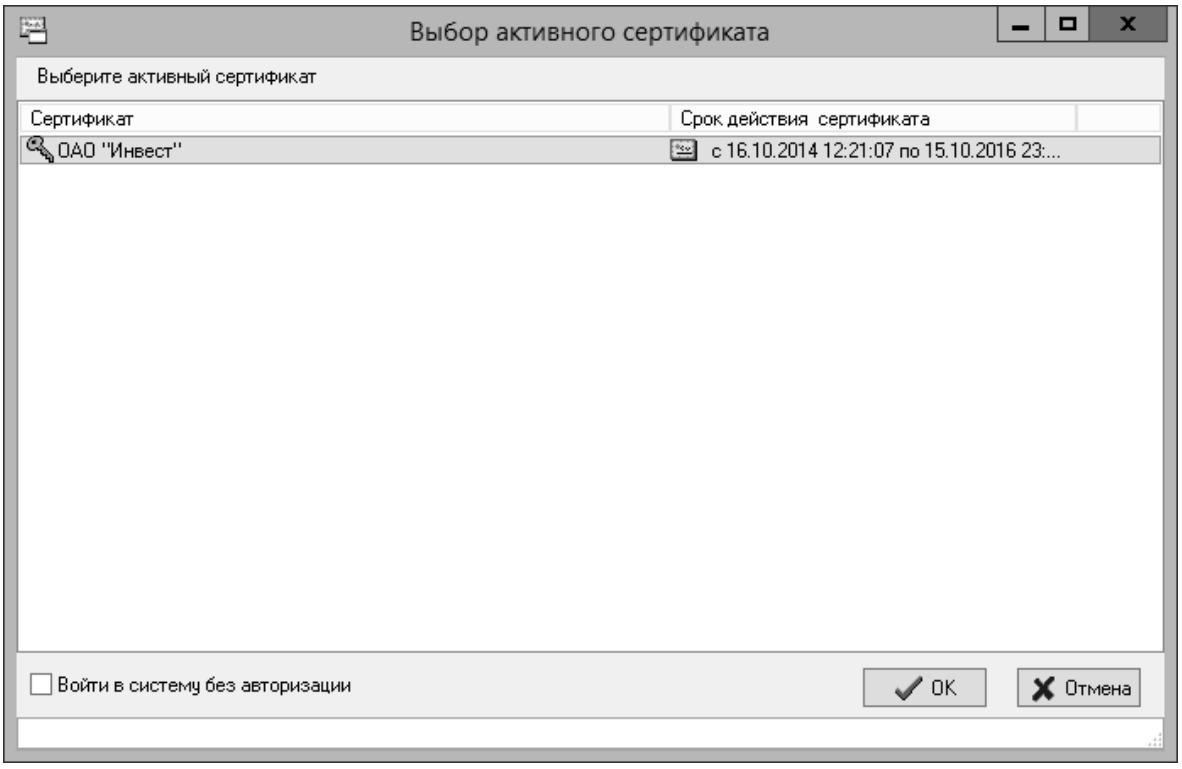


Рисунок 15. Выбор активного сертификата

5.3. Запуск программы, настроенной на использование устройства AvHSM-Bign

Вход в систему осуществляется через авторизацию пользователя. Для этого после запуска Персонального менеджера сертификатов Авест с ярлыка на рабочем столе, или через меню «Пуск» в появившемся окне надо ввести пароль к устройству AvHSM-Bign (см. Рисунок 16. Ввод пароля к внутреннему слоту устройства AvHSM-Bign).

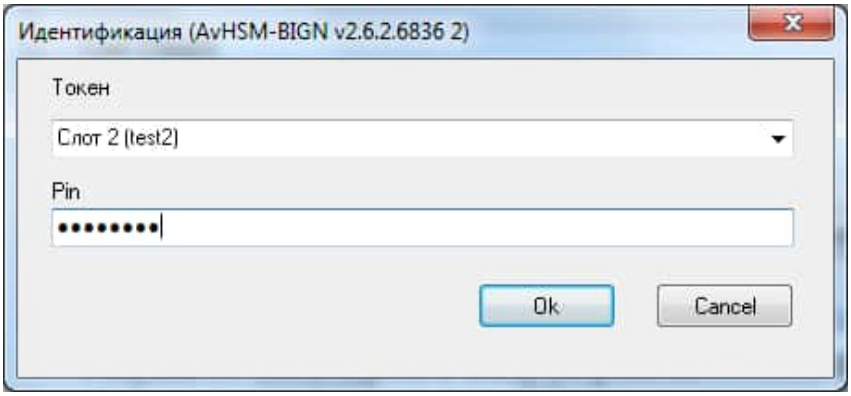


Рисунок 16. Ввод пароля к внутреннему слоту устройства AvHSM-Bign

Далее нужно выбрать идентификатор ключевого контейнера, нажать OK и выполнить вход в систему (см. Рисунок 17. Выбор активного сертификата).

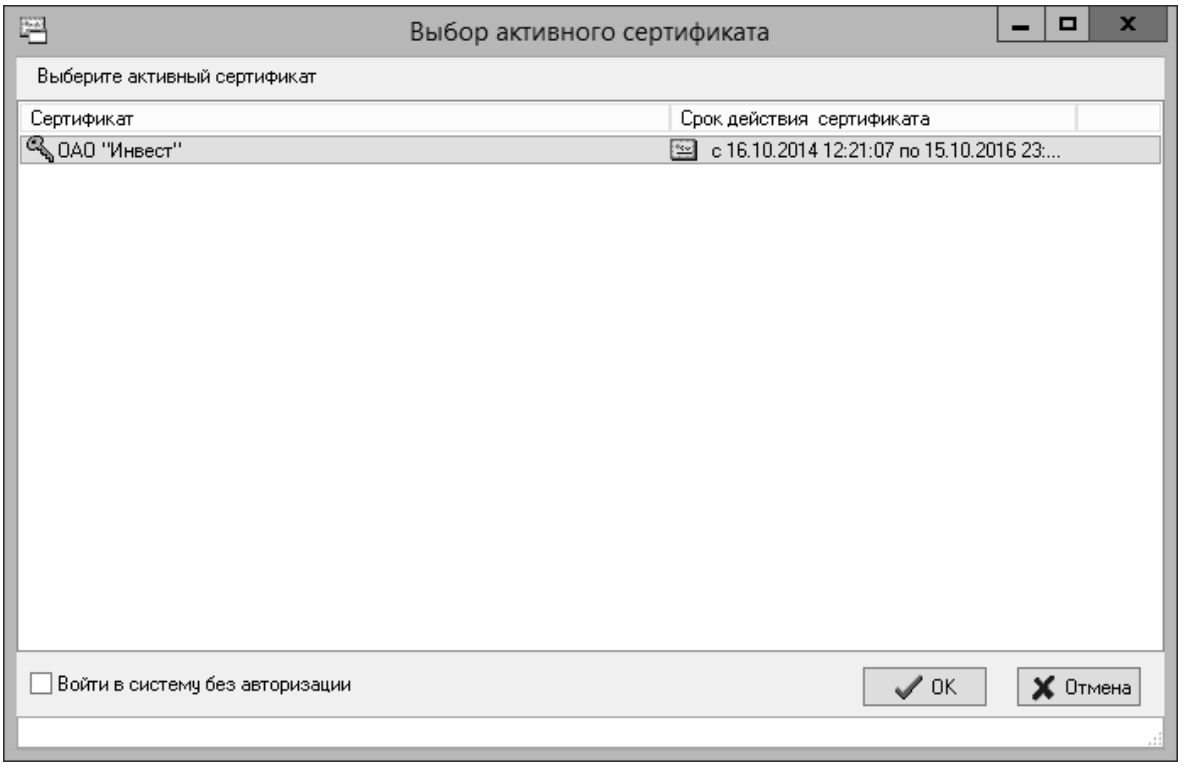


Рисунок 17. Выбор активного сертификата

6. РАБОТА С ПРОГРАММОЙ

6.1. Создание запроса на сертификат

6.1.1. Создание запроса на сертификат с использованием криптопровайдера AvCSP

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

Её выполнение нужно 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»

или

запустить ПК AvPCM, щелкнув по ярлыку «Персональный менеджер сертификатов Авест», находящемся на вашем Рабочем столе (см. п. 5.1 Запуск программы, настроенной на использование криптопровайдера). Для создания запроса на сертификат авторизацию проходить необязательно. Если появится окно авторизации, можно поставить галочку напротив пункта «Войти в систему без авторизации» и нажать «ОК». В открывшемся менеджере сертификатов нужно выбрать пункт меню «Создать запрос» → «Подготовить запрос на сертификат» (см. Рисунок 18. Запуск мастера создания запроса на сертификат).

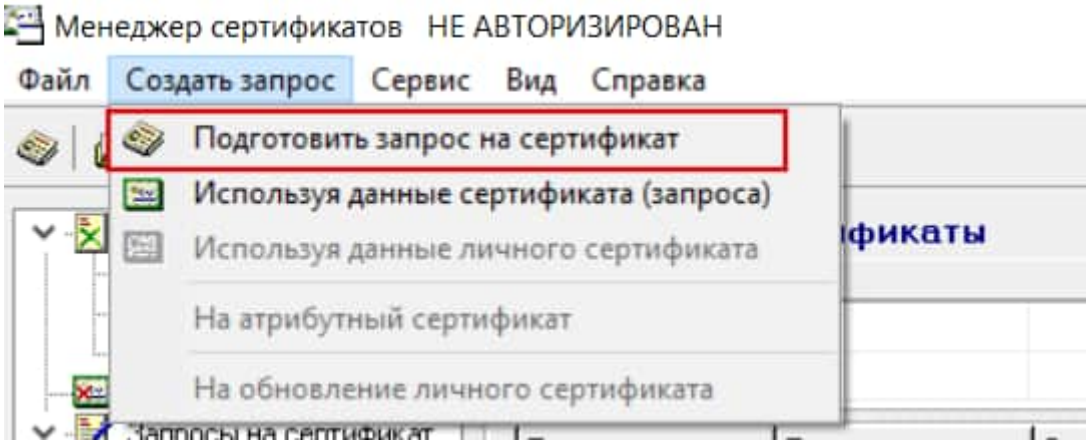


Рисунок 18. Запуск мастера создания запроса на сертификат

1) В появившемся окне мастера создания запроса на сертификат выбрать шаблон для создания сертификата (см. Рисунок 19. Выбор шаблона для создания сертификата);

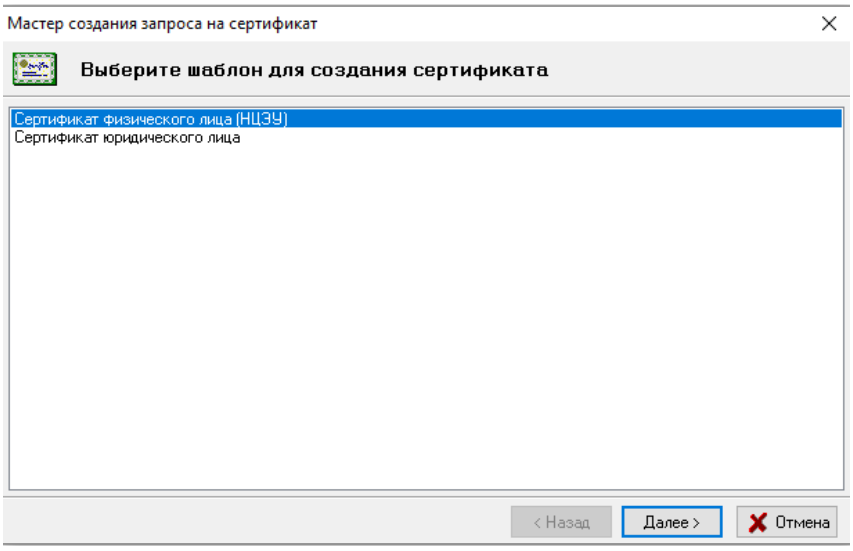


Рисунок 19. Выбор шаблона для создания сертификата

2) в следующем диалоговом окне надо задать атрибуты будущего владельца сертификата, включаемые в запрос на сертификат. Набор атрибутов, их содержание и обязательность заполнения определяется настройками конфигурации (шаблона сертификата) и зависит от политики применения сертификатов удостоверяющего центра инфраструктуры открытых ключей, а также от типа сертификата и его предназначения. Пример заполнения атрибутов для сертификата юридического лица показан на Рисунок 20. Заполнение атрибутов владельца сертификата на примере сертификата юридического лица.

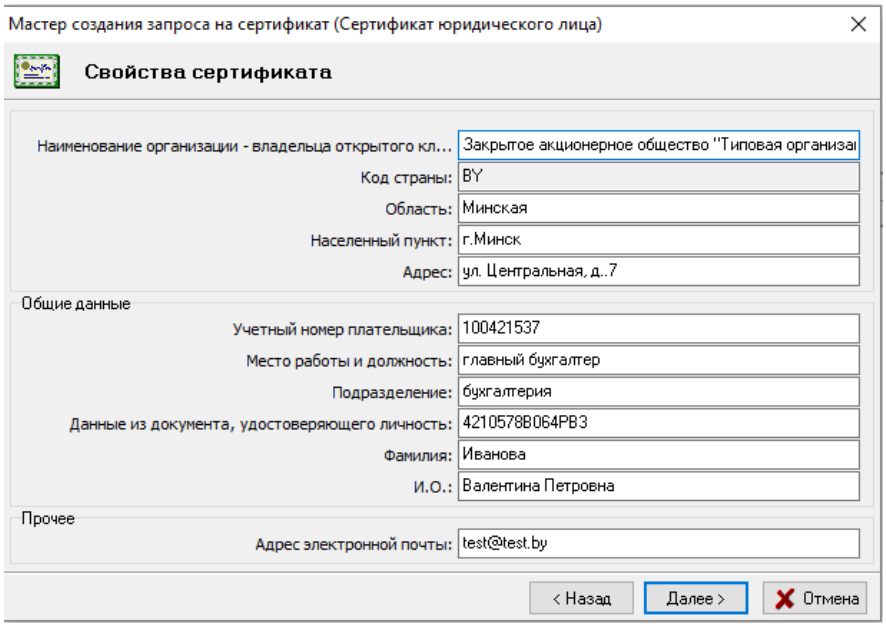


Рисунок 20. Заполнение атрибутов владельца сертификата на примере сертификата юридического лица

В данном примере нужно заполнить следующие поля:

- «Наименование организации владельца открытого ключа» – полное наименование организации, на имя которой будет выпущен сертификат;
- «Код страны» – двухбуквенный международный код страны, в которой зарегистрирована организация, в которой работает будущий владелец сертификата;

- «Область» – наименование административно-территориальной единицы деления страны, в которой зарегистрирована организация владельца 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;
- «Учетный номер плательщика» – учетный номер плательщика, присвоенный МНС РБ организации, в которой работает будущий владелец сертификата;
- «Место работы и должность» – место работы и должность лица, ответственного за работу с криптографическими ключами;
- «Подразделение» – наименование подразделения, в котором работает лицо, ответственное за работу с криптографическими ключами;
- «Данные из документа, удостоверяющего личность» – идентификационный (личный) номер (данные из документа, удостоверяющего личность: паспорта, вида на жительство и т. д.) 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.
- «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 поле из обязательных атрибутов не заполнено 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 21. Применение личного ключа).

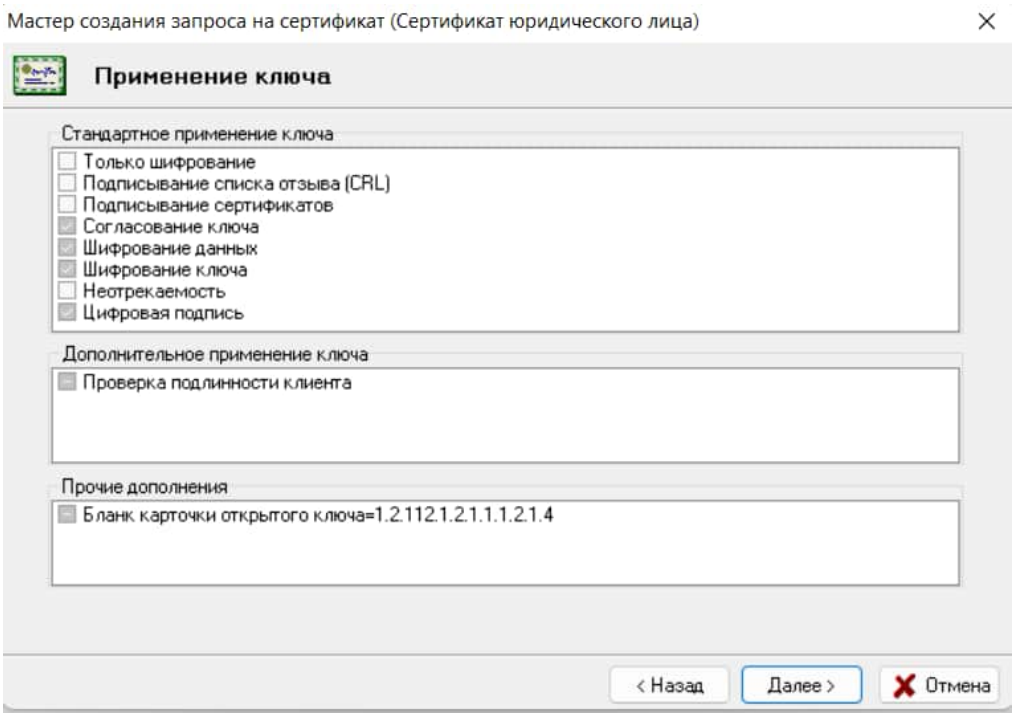


Рисунок 21. Применение личного ключа

3) В следующем диалоговом окне следует определить срок действия сертификата пользователя (см. Рисунок 22. Ввод сроков действия сертификата);

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 надо выключить флажок «Срок действия сертификата задается удостоверяющим центром» и ввести 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.

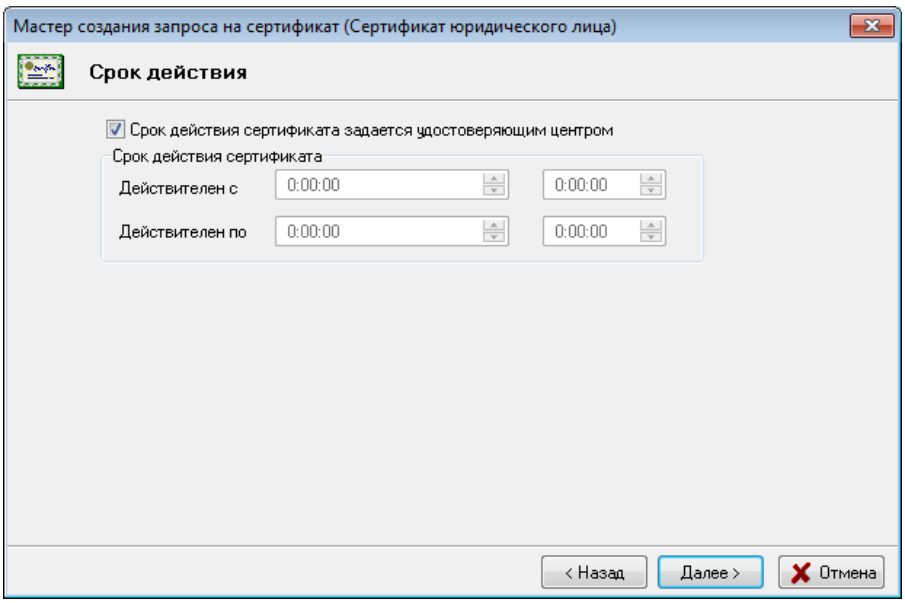


Рисунок 22. Ввод сроков действия сертификата

4) Затем, в появившемся окне, надо задать имя контейнера, в который будет помещен ваш личный ключ (см. Рисунок 23. Инициализация носителя личного ключа).

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.

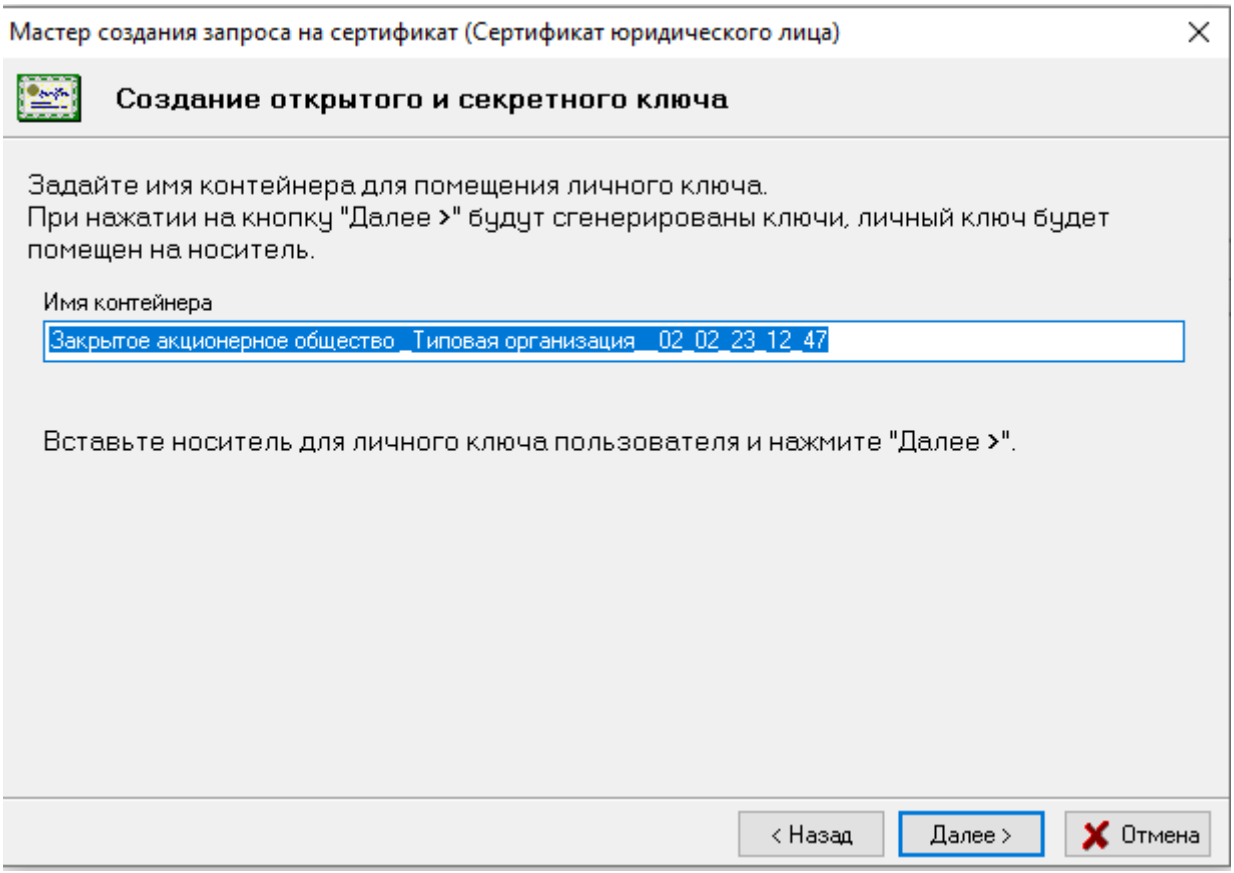


Рисунок 23. Инициализация носителя личного ключа

5) Для инициализации контейнера личных ключей в появившемся далее диалоговом окне нужно выбрать из списка физический носитель ключей, далее, в зависимости от выбранного типа носителя, ввести предварительно заданный пароль или задать в соответствующих полях пароль и его подтверждение (см. Рисунок 24. Выбор физического носителя личного ключа).

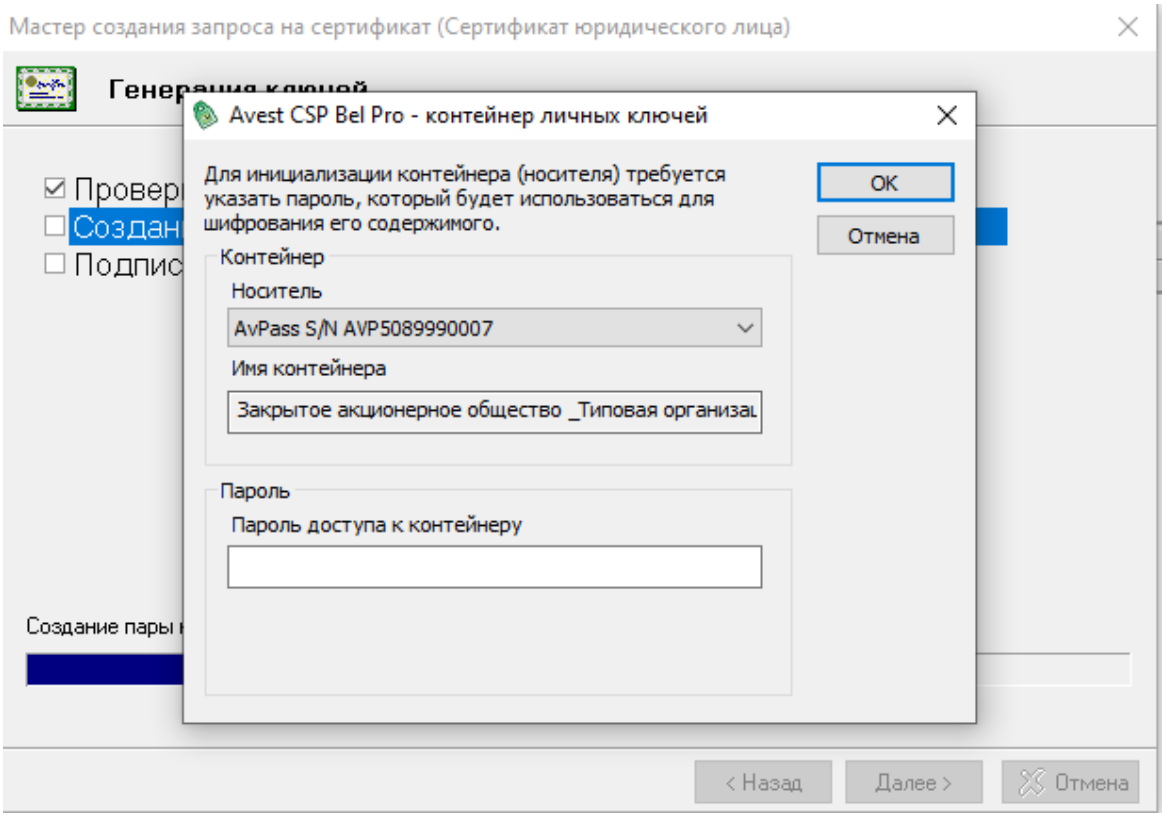


Рисунок 24. Выбор физического носителя личного ключа

6) 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 25. Окно «Сбор случайных данных»).

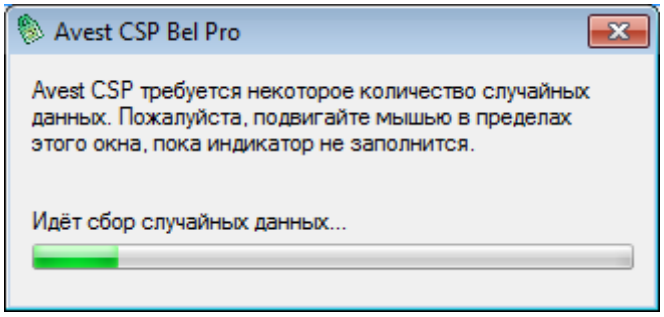


Рисунок 25. Окно «Сбор случайных данных»

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

Примечания:

1. Работоспособность носителей iButton, eToken, iKey, ruToken, Acos3, MIFARE Std Card 4K гарантируется только в режиме обратной совместимости.

2. Поскольку для функционирования носителей iButton, eToken, iKey, ruToken, Acos3, MIFARE Std Card 4K требуются драйверы сторонних производителей, полноценная работа с данными устройствами не гарантируется.

3. Работа носителей iButton, eToken, iKey, ruToken, Acos3, MIFARE Std Card 4K в режиме обратной совместимости для может осуществляться только в 32-разрядной версии криптопровайдера AvCSP. 64-разрядная версия криптопровайдера AvCSP поддерживает носители AvToken и AvPass.

4. 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.

5. 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.

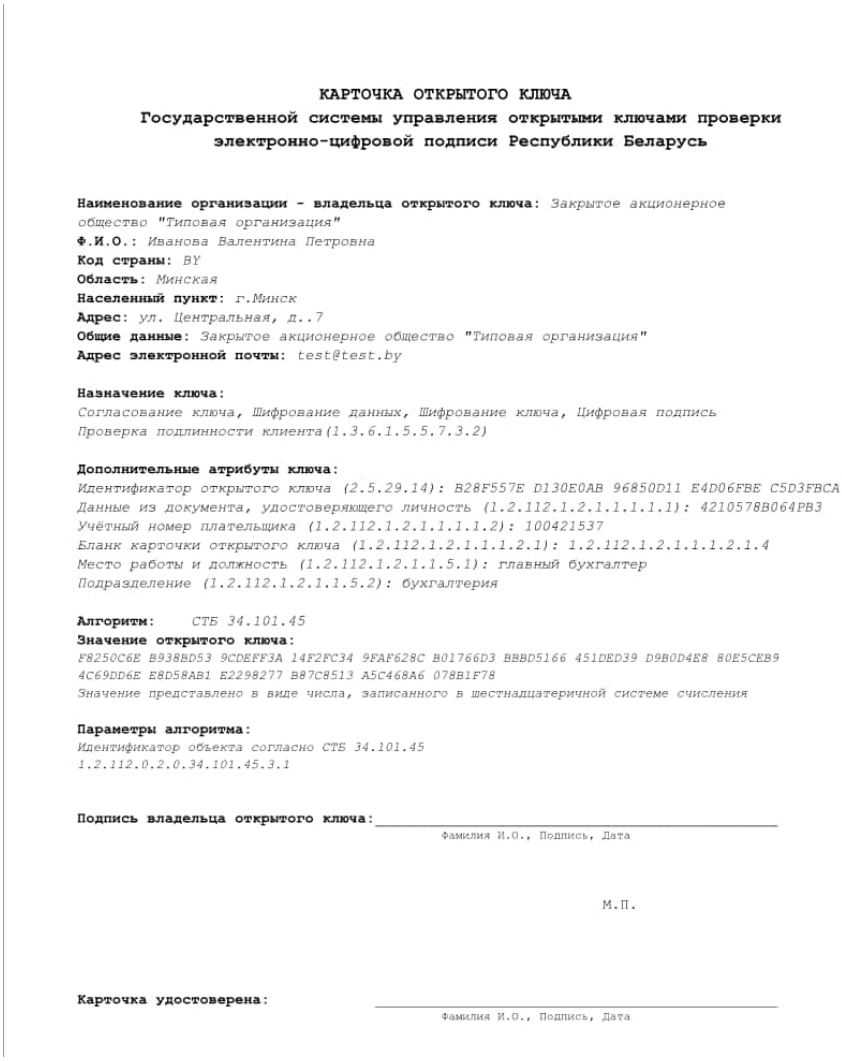
6. При использовании носителя AvToken в режиме AvToken strong после семи попыток ввода неправильного пароля на доступ к личным ключам на носителе, происходит автоматическое удаление контейнера с личными ключами на носителе.

7. ПК AvPCM обеспечивает работу со всеми типами носителей ключей, которые поддерживают криптопровайдеры AvCSP, AvCSPBEL, AvCSPBIG.

Примечание:

ЗАО «АВЕСТ» гарантирует надежное взаимодействие криптопровайдера AvCSPBEL с НКИ AvPass и AvToken. При использовании НКИ отличных от AvPass и AvToken работа криптопровайдера AvCSPBEL с данными НКИ не гарантируется.

7) После этого будет сформирована карточка открытого ключа, которую требуется распечатать (см. Рисунок 26. Карточка открытого ключа).



КАРТОЧКА ОТКРЫТОГО КЛЮЧА
Государственной системы управления открытыми ключами проверки электронно-цифровой подписи Республики Беларусь

Наименование организации - владельца открытого ключа: *Закрытое акционерное общество "Типовая организация"*
Ф.И.О.: *Иванова Валентина Петровна*
Код страны: *BY*
Область: *Минская*
Населенный пункт: *г.Минск*
Адрес: *ул. Центральная, д..7*
Общие данные: *Закрытое акционерное общество "Типовая организация"*
Адрес электронной почты: *test@test.by*

Назначение ключа:
Согласование ключа, Шифрование данных, Шифрование ключа, Цифровая подпись
Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

Дополнительные атрибуты ключа:
Идентификатор открытого ключа (2.5.29.14): B28F557E D130E0AB 96850D11 E4D06FBE C5D3FBCA
Данные из документа, удостоверяющего личность (1.2.112.1.2.1.1.1.1.1): 4210578B064PB3
Учётный номер плательщика (1.2.112.1.2.1.1.1.1.2): 100421537
Бланк карточки открытого ключа (1.2.112.1.2.1.1.1.2.1): 1.2.112.1.2.1.1.1.2.1.4
Место работы и должность (1.2.112.1.2.1.1.5.1): главный бухгалтер
Подразделение (1.2.112.1.2.1.1.5.2): бухгалтерия

Алгоритм: *СТБ 34.101.45*
Значение открытого ключа:
F8250C6E B938BD53 9CDEFF3A 14F2FC34 9FAF628C B01766D3 BBBD5166 451DED39 D9B0D4E8 80E5CEB9
4C69DD6E E8D58AB1 E2298277 B87C8513 A5C468A6 078B1F78
Значение представлено в виде числа, записанного в шестнадцатеричной системе счисления

Параметры алгоритма:
Идентификатор объекта согласно СТБ 34.101.45
1.2.112.0.2.0.34.101.45.3.1

Подпись владельца открытого ключа: _____
Фамилия И.О., Подпись, Дата

М.П.

Карточка удостоверена: _____
Фамилия И.О., Подпись, Дата

Рисунок 26. 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 попадает 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 27. Сохранение запроса).

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.

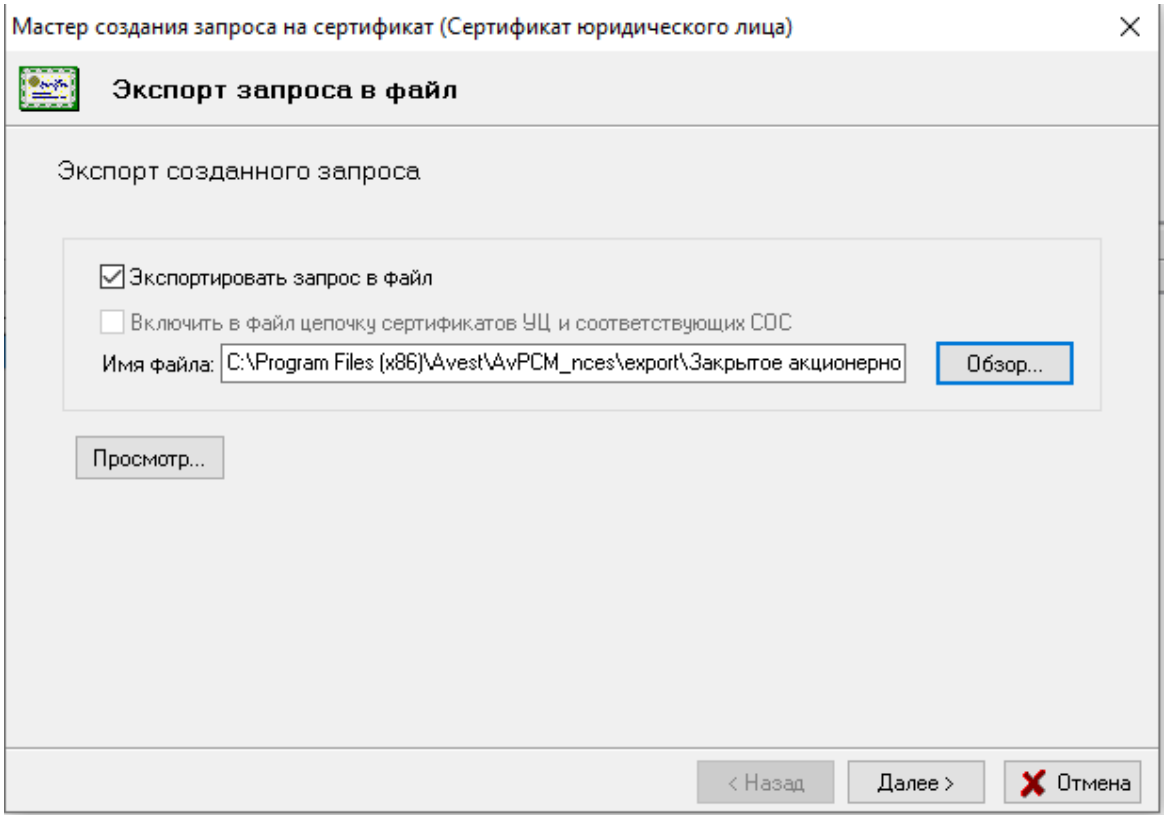


Рисунок 27. Сохранение запроса

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.

6.1.2. Создание запроса на сертификат с использованием устройства AvBign

Перед подготовкой запроса с использованием устройства AvBign, обеспечивающего использование аппаратной реализации криптографических алгоритмов в соответствии с интерфейсом PKCS#11, нужно убедиться, что на ПК пользователя установлен драйвер для устройства AvBign и устройство AvBign установлено в USB-порт.

Действия при создании запроса на сертификат:

1) выбрать из основного меню Windows: «Пуск» → «Программы» → Авест» → «Персональный менеджер сертификатов» → «Создать запрос на сертификат»

или

запустить ПК AvPCM, щелкнув по ярлыку «Персональный менеджер сертификатов Авест», находящемся на вашем Рабочем столе (см. п. 5.2 Запуск программы, настроенной на использование устройства AvBign). Для создания запроса на сертификат авторизацию проходить необязательно. Если появится окно авторизации можно поставить галочку напротив пункта «Войти в систему без авторизации» и нажать «ОК». В открывшемся менеджере сертификатов нужно выбрать пункт меню

«Создать запрос» → «Подготовить запрос на сертификат» (см. Рисунок 28. Запуск мастера создания запроса на сертификат).

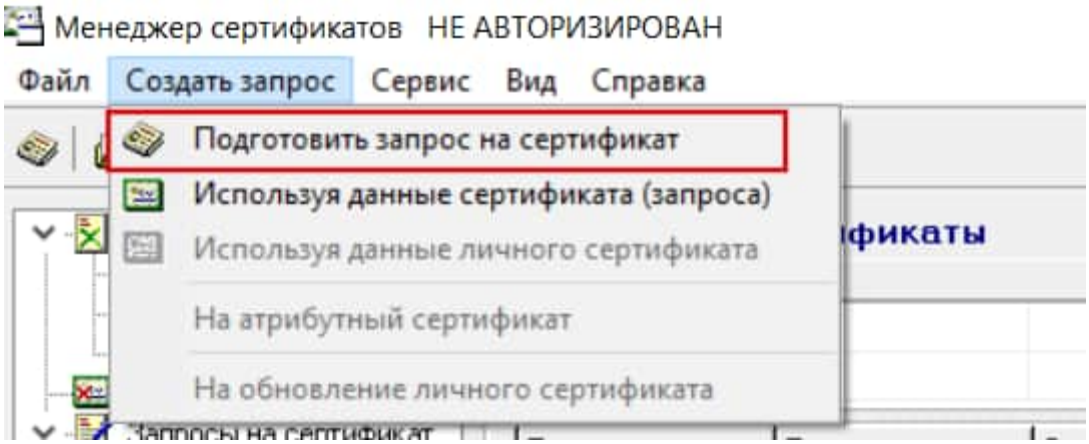


Рисунок 28. Запуск мастера создания запроса на сертификат

2) В появившемся окне мастера создания запроса на сертификат выбрать шаблон для создания сертификата (см. Рисунок 29. Выбор шаблона для создания сертификата);

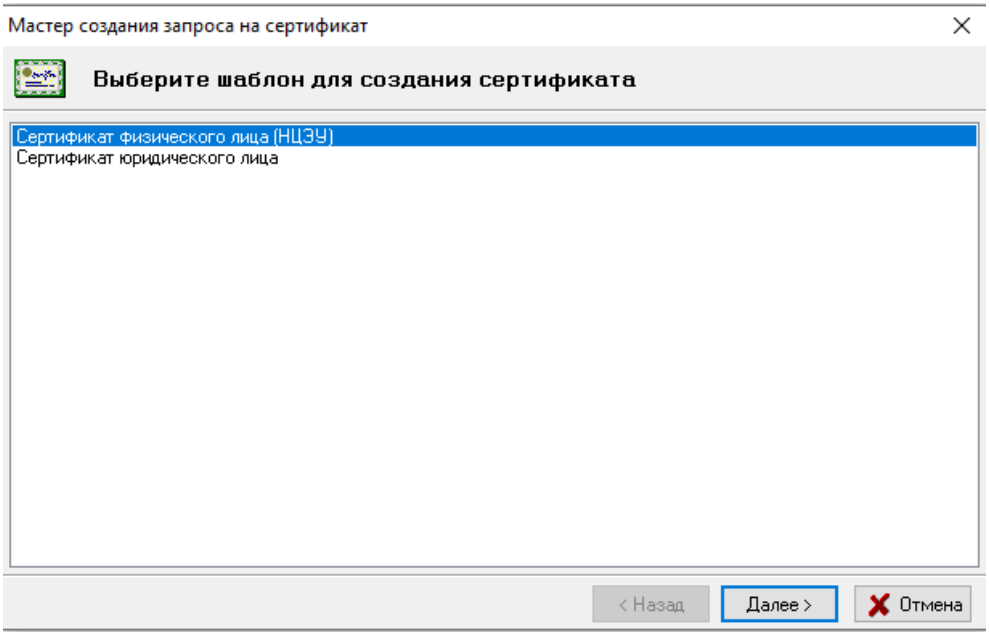


Рисунок 29. Выбор шаблона для создания сертификата

3) в следующем диалоговом окне надо задать атрибуты будущего владельца сертификата, включаемые в запрос на сертификат. Набор атрибутов, их содержание и обязательность заполнения определяется настройками конфигурации (шаблона сертификата) и зависит от политики применения сертификатов удостоверяющего центра инфраструктуры открытых ключей, а также от типа сертификата и его предназначения. Пример заполнения атрибутов для сертификата юридического лица показан на Рисунок 30. Заполнение атрибутов владельца сертификата на примере сертификата юридического лица.

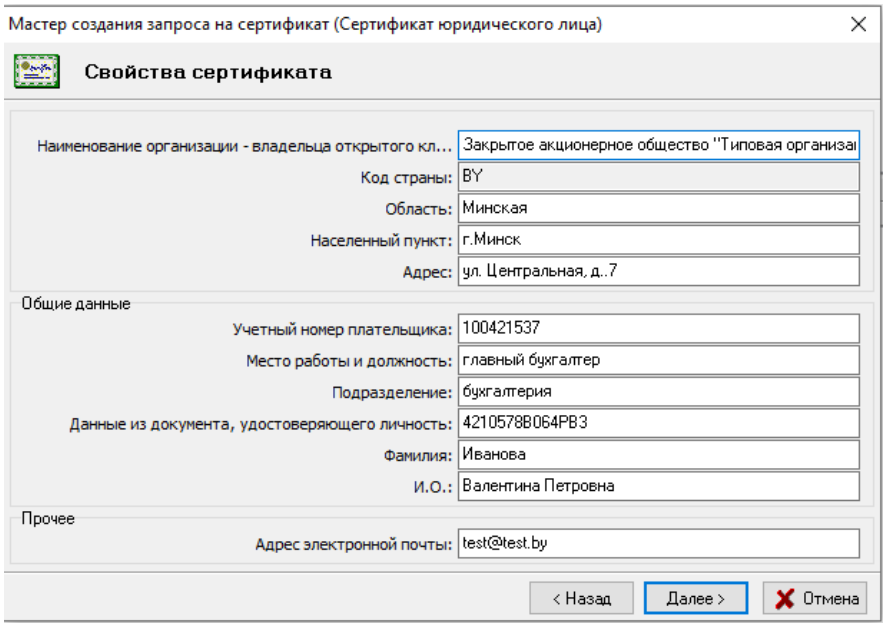


Рисунок 30. Заполнение атрибутов владельца сертификата на примере сертификата юридического лица

В данном примере нужно заполнить следующие поля:

- «Наименование организации владельца открытого ключа» – полное наименование организации, на имя которой будет выпущен сертификат;
- «Код страны» – двухбуквенный международный код страны, в которой зарегистрирована организация, в которой работает будущий владелец сертификата;
- «Область» – наименование административно-территориальной единицы деления страны, в которой зарегистрирована организация владельца 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;
- «Учетный номер плательщика» – учетный номер плательщика, присвоенный МНС РБ организации, в которой работает будущий владелец сертификата;
- «Место работы и должность» – место работы и должность лица, ответственного за работу с криптографическими ключами;
- «Подразделение» – наименование подразделения, в котором работает лицо, ответственное за работу с криптографическими ключами;
- «Данные из документа, удостоверяющего личность» – идентификационный (личный) номер (данные из документа, удостоверяющего личность: паспорта, вида на жительство и т. д.) 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.
- «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 поле из обязательных атрибутов не заполнено 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 31. Применение личного ключа).

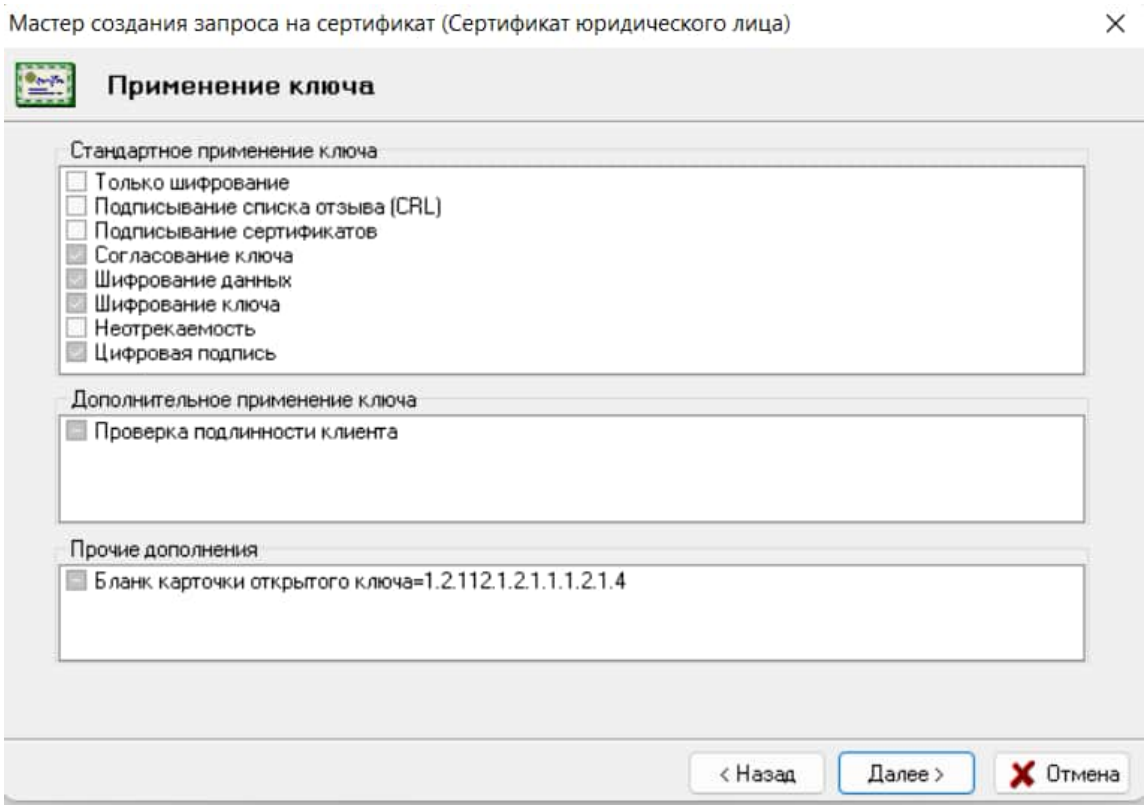


Рисунок 31. Применение личного ключа

4) В следующем диалоговом окне следует определить срок действия сертификата пользователя (см. Рисунок 32. Ввод сроков действия сертификата).

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 надо выключить флажок «Срок действия сертификата задается удостоверяющим центром» и ввести 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.

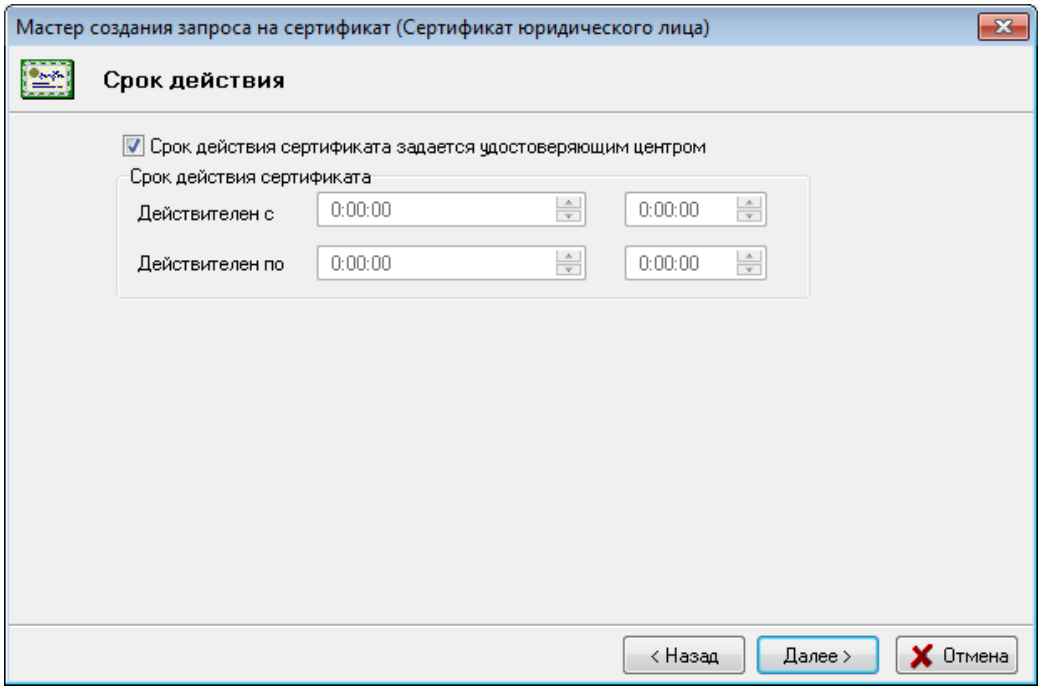


Рисунок 32. Ввод сроков действия сертификата

5) После указания сроков действия сертификата в окне «Атрибуты ключевой пары» следует задать метку ключа, алгоритм механизма генерации пар ключей и параметры выбранного алгоритма (см. Рисунок 33. Атрибуты ключевой пары).

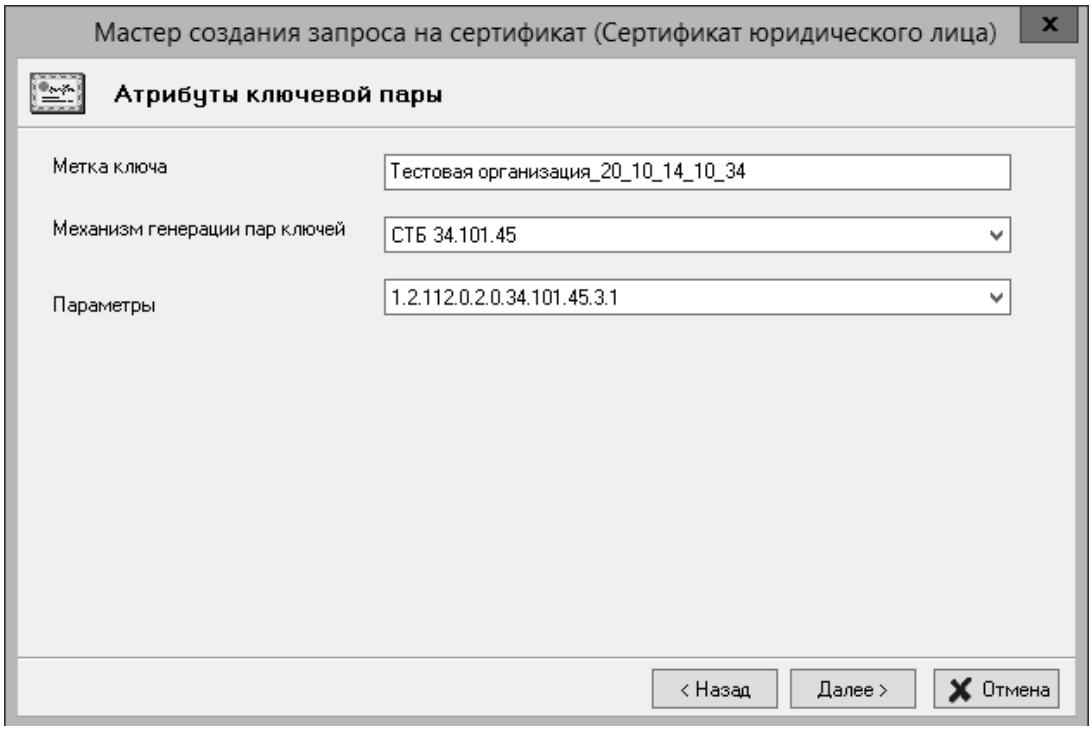


Рисунок 33. Атрибуты ключевой пары

Программа произведет запись личного ключа во внутреннюю память устройства AvBign. При этом будет сформирована карточка открытого ключа подчиненного Удостоверяющего центра, которую нужно распечатать (см. Рисунок 26. Карточка открытого ключа).

6) В следующем окне «Экспорт запроса в файл» надо указать имя файла и папку, в которую будет сохранен данный запрос (см. Рисунок 27. Сохранение запроса).

В этом окне надо включить флажок «Экспортировать запрос в файл», указать имя файла, в котором будет сохранен запрос, и путь к нему.

Нажав на кнопку «Просмотр» можно увидеть информацию, содержащуюся в самом запросе на сертификат.

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

6.1.3. Создание запроса на сертификат с использованием AvHSM-Bign

Перед созданием запроса с использованием устройства AvHSM-Bign, обеспечивающего использование аппаратной реализации криптографических алгоритмов в соответствии с интерфейсом PKCS#11, нужно убедиться, что устройство AvHSM-Bign подключено при помощи сетевого соединения Ethernet и находиться с той же подсети, что и компьютер пользователя.

Действия при создании запроса на сертификат аналогичны действиям, описанным в п. 6.1.2 Создание запроса на сертификат с использованием устройства AvBign.

6.2. Формат запроса на сертификат в соответствии с требованиями СТБ 34.101.78-2019

СТБ 34.101.78-2019 определяет новый формат сертификатов пользователей. В соответствии с данным стандартом установлен новый набор полей, заполняемых в запросе на получение сертификат. Основными сторонами ИОК, которые выполняют подготовку запроса на сертификат в менеджере сертификатов, являются юридические представители (далее – ЮП) и физические лица (далее – ФЛ).

6.2.1. Формат запроса на сертификат юридического представителя в соответствии с требованиями СТБ 34.101.78-2019

При создании запроса на сертификат юридического представителя в соответствии с требованиями СТБ 34.101.78-2019 нужно заполнить следующие поля (см. Рисунок 34. Заполнение атрибутов в запросе на сертификат юридического представителя):

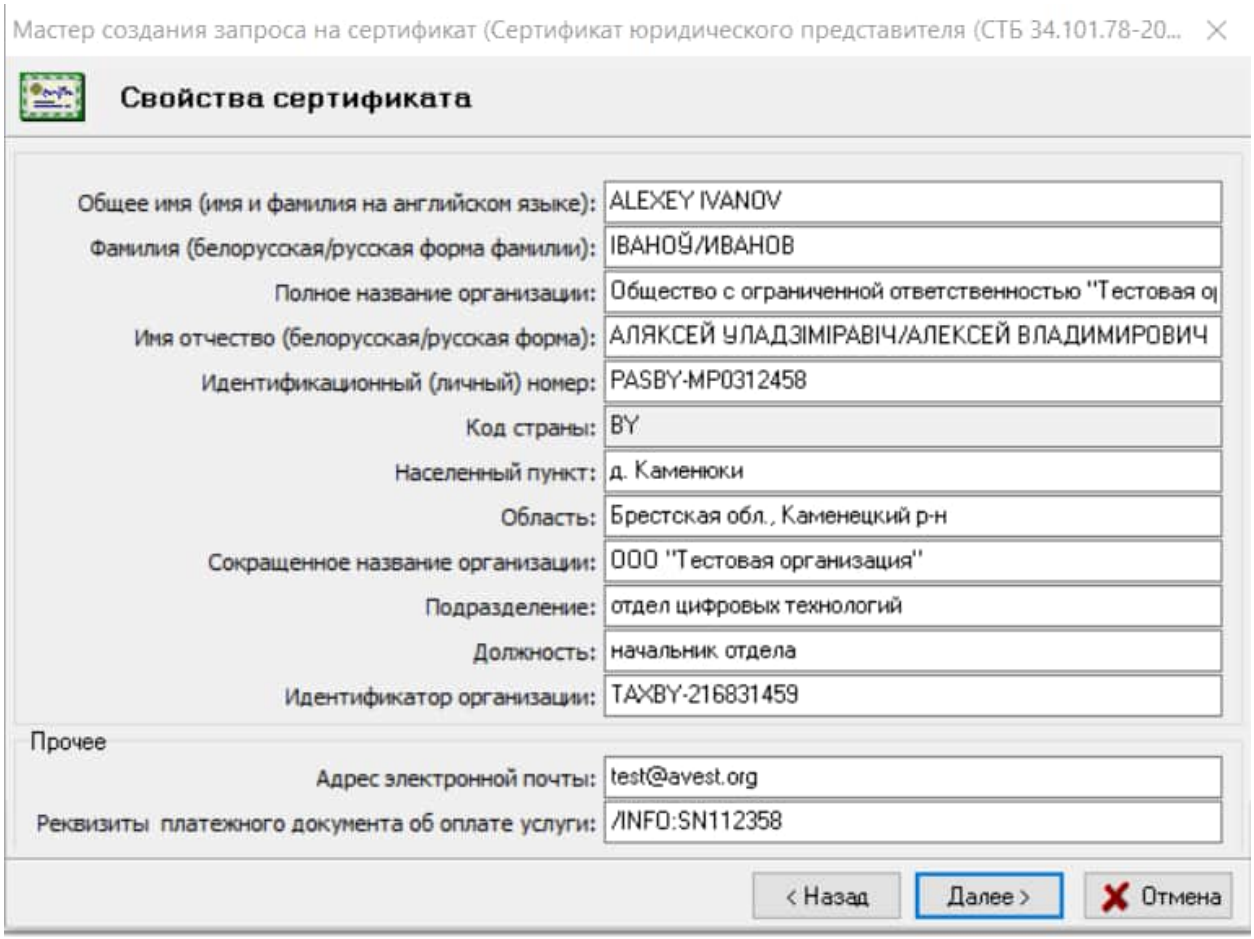


Рисунок 34. Заполнение атрибутов в запросе на сертификат юридического представителя

«Общее имя (имя и фамилия на английском языке)» – имя и фамилия ЮП на английском языке (как в паспорте). Имя и фамилия записываются в верхнем регистре, разделяются пробелом.

«Фамилия (белорусская/русская форма фамилии)» – белорусская и русская формы фамилии ЮП. Записываются прописными буквами и разделены наклонной чертой (как в паспорте).

«Полное название организации» – задается полное название организации, которую представляет ЮП, в соответствии с удостоверением организации.

«Имя отчество (белорусская/русская форма)» – содержит белорусскую и русскую формы имени и, если имеется, отчества ЮП. Имя и отчество разделяются пробелом, записываются прописными буквами, формы разделяются символом ’/’ (как в паспорте).

«Идентификационный (личный) номер» – задается идентификационный номер ЮП. Данное поле содержит (слева направо):

1. три символа типа номера: ’PAS’ — номер паспорта или ’PNO’ — личный номер,

2. два символа кода страны, в которой зарегистрирован паспорт,

3. символ ’-’,

4. символы номера.

«Код страны» – двухбуквенный международный код страны (ISO), в которой зарегистрирована организация, которую представляет ЮП. Для РБ полагается равным ’BY’.

«Населенный пункт» – указывается населенный пункт: город (’г.’), городской поселок (’г.п.’), деревня (’д.’) и др.

«Область» – указываются названия области и района. Данный атрибут не заполняется, если в поле «Населенный пункт» указан областной центр. В атрибуте опускается название района, если в поле «Населенный пункт» указан районный центр.

Поля *«Населенный пункт»* и *«Область»* задаются из юридического адреса организации, которую представляет ЮП, в соответствии с удостоверением организации.

«Сокращенное название организации» – задается сокращенное название организации, которую представляет ЮП. Сокращенное название задается в соответствии с удостоверением организации.

«Подразделение» – является необязательным параметром. Задается название подразделения, которое представляет ЮП, в соответствии с удостоверением организации.

«Должность» – задается должность ЮП в организации, которую он представляет, в соответствии с удостоверением организации.

«Идентификатор организации» – задается идентификатор организации, которую представляет ЮП. Данное поле содержит (слева направо):

1. три символа типа идентификатора. Разрешается использовать только код ’TAX’ —

учетный номер плательщика,

2. ’BY’ — код страны, в которой зарегистрирован идентификатор,

3. символ ’-’,

4. символы идентификатора.

«Адрес электронной почты» – адрес электронной почты, по которому можно будет связаться с ЮП, при возникновении проблем или для получения дополнительных разъяснений.

«Реквизиты платежного документа об оплате услуги» – информационная строка, которую требуется передать в УЦ. Например, реквизиты платежного документа об оплате услуги (процесса). Информационной строке должен предшествовать префикс ’/INFO:’.

6.2.2. Формат запроса на сертификат физического лица в соответствии с требованиями СТБ 34.101.78-2019

При создании запроса на сертификат ФЛ в соответствии с требованиями СТБ 34.101.78-2019 нужно заполнить следующие поля (см. Рисунок 35. Заполнение атрибутов в запросе на сертификат физического лица).

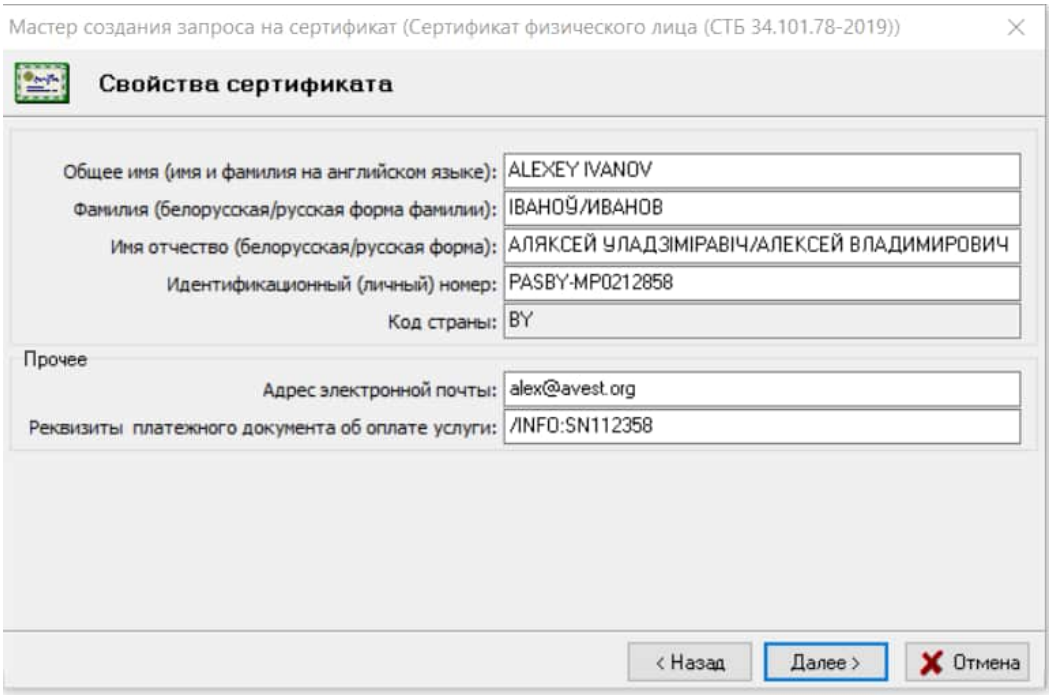


Рисунок 35. Заполнение атрибутов в запросе на сертификат физического лица

В запрос для ФЛ включаются обязательные для заполнения поля:

«Общее имя (имя и фамилия на английском языке)»,

«Фамилия (белорусская/русская форма фамилии)»,

«Имя отчество (белорусская/русская форма)»,

«Идентификационный (личный) номер» *,

«Код страны» **,

«Адрес электронной почты»,

«Реквизиты платежного документа об оплате услуги».

**«Идентификационный (личный) номер»* - в сертификатах ФЛ кроме номера паспорта и личного номера может также использоваться номер ID-карты. В этом случае тип номера обозначается кодом ’IDC’, например: ’IDCBY-590082394654’. Идентификационный номер такого типа должен использоваться только тогда, когда соответствующий личный ключ размещается на персональном криптографическом токене.

***«Код страны» – двухбуквенный международный* код страны. Для ФЛ-нерезидента – это код страны, гражданином которой он является. Во всех остальных случаях полагается равным ’BY’.

Данные по всем остальным атрибутам вносятся аналогично данным в запросе для юридического лица (см. п. 6.2.1 Формат запроса на сертификат юридического представителя в соответствии с требованиями СТБ 34.101.78-2019).

6.2.3. Другие особенности создания запроса на сертификат в соответствии с требованиями СТБ 34.101.78-2019

Другими особенностями при создании запроса на сертификат в соответствии с требованиями СТБ 34.101.78-2019 являются следующие:

1. В запрос не включается применение ключа, следовательно, соответствующее окно при создании запроса открываться не будет.
2. Дата создания запроса будет отображаться только в том случае, если был установлен предполагаемый срок действия сертификата, т.е. при создании запроса на шаге «Срок действия» была снята галочка с пункта «Срок действия сертификата задается удостоверяющим центром». Устанавливать предполагаемый срок действия сертификата можно лишь при необходимости сузить срок действия сертификата, задаваемый в УЦ по умолчанию.
3. По умолчанию программа создаст контейнер личных ключей с именем «[Общее имя (имя и фамилия на английском языке)]_дд_мм_гг_чч_мм», где «дд_мм_гг_чч_мм» – это время генерации ключей.
4. СТБ 34.101.78-2019 не предусматривает использование карточек открытого ключа, поэтому при создании запроса окно предпросмотра (печати) карточки открытого ключа открываться не будет.

6.3. Создание запроса на атрибутный сертификат

ВНИМАНИЕ! Предварительно следует авторизоваться в ПК AvPCM под тем сертификатом, на основании которого будет создаваться запрос на атрибутный сертификат (см. п. 5 Запуск программы).

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

1) В окне мастера создания запроса на сертификат указать тип шаблона (см. Рисунок 36. Выбор шаблона создания атрибутного сертификата).

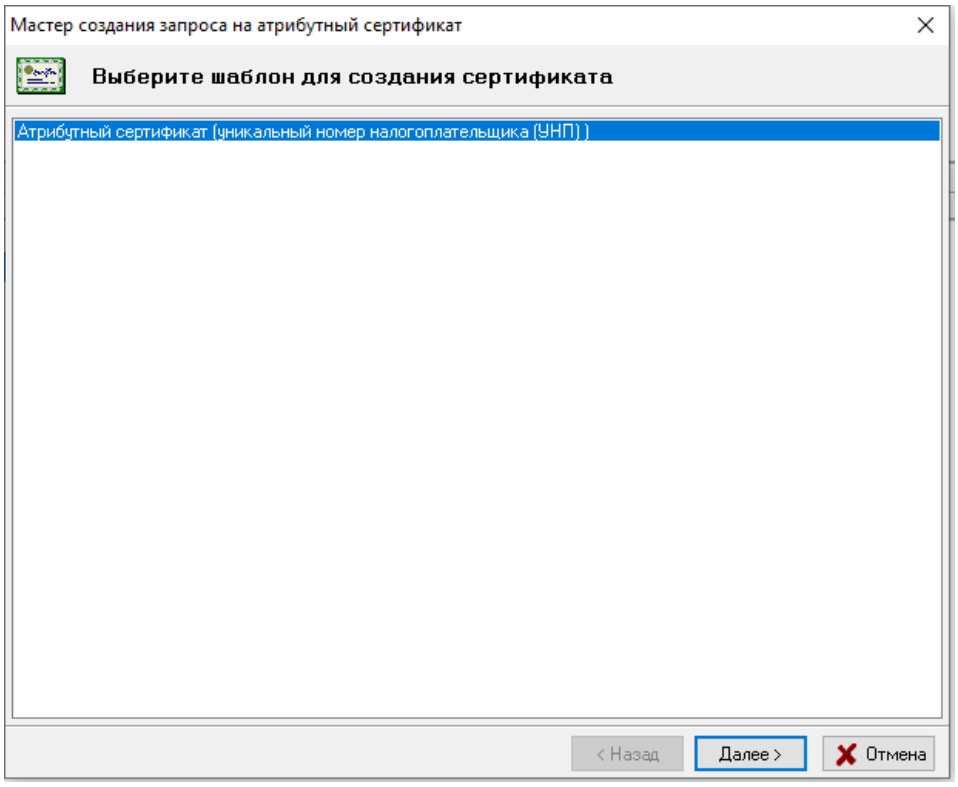


Рисунок 36. Выбор шаблона создания атрибутного сертификата

2) Далее будут выведены сведения о сертификате пользователя, на основании которого будет сформирован атрибутный сертификат (см. Рисунок 37. Сведения об исходном сертификате).

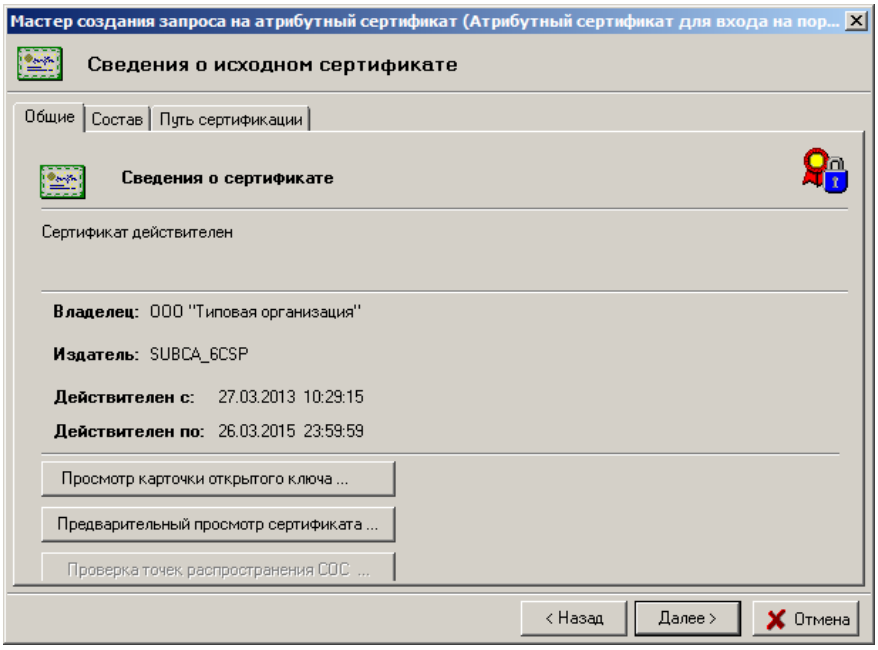


Рисунок 37. Сведения об исходном сертификате

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 38. Заполнение свойств атрибутного сертификата).

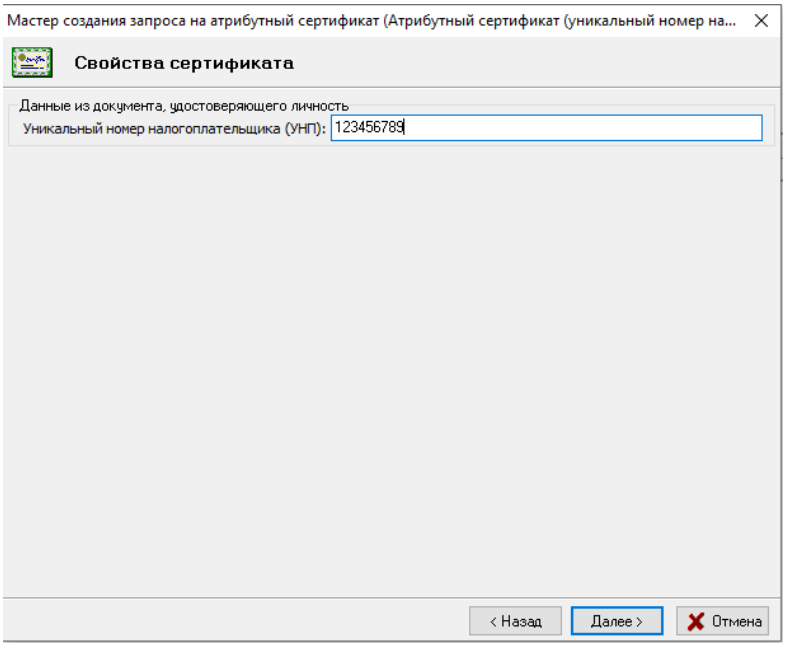


Рисунок 38. Заполнение свойств атрибутного сертификата

4) Затем нужно определить срок действия сертификата пользователя (см. Рисунок 39. Сохранение запроса на атрибутный сертификат).

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 39. Сохранение запроса на атрибутный сертификат).

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.

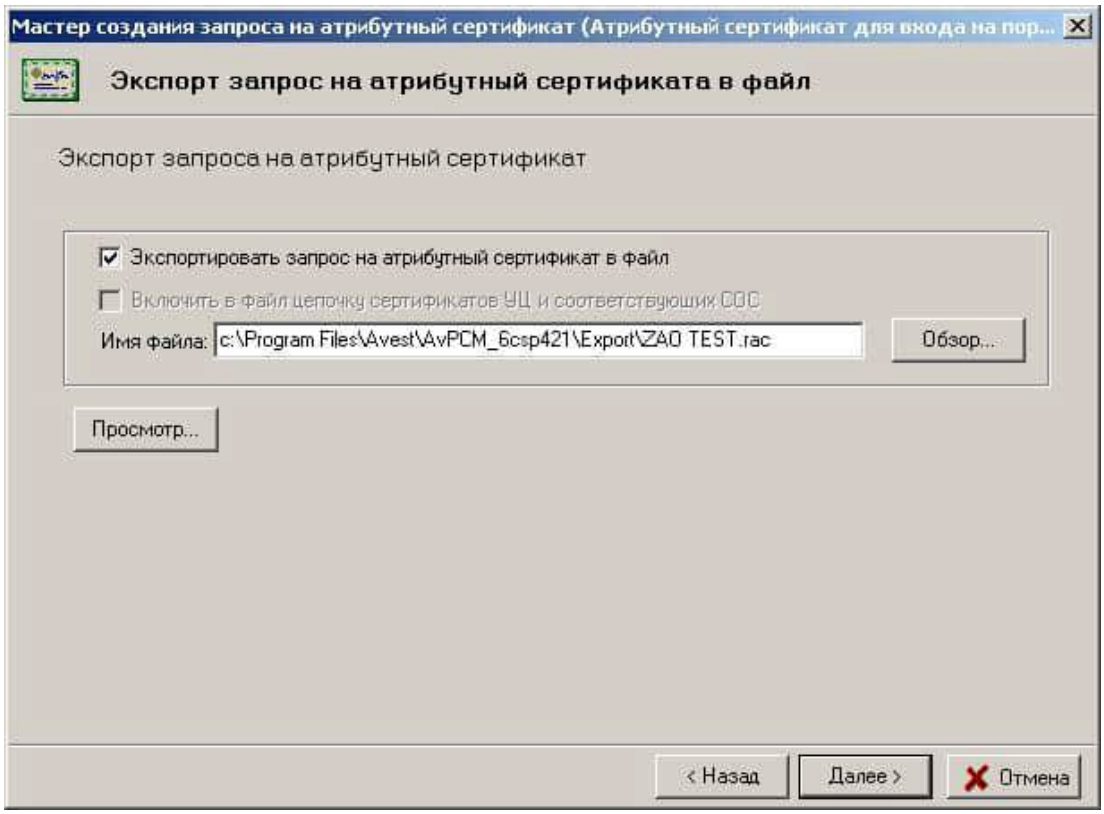


Рисунок 39. Сохранение запроса на атрибутный сертификат

6.4. Создание запроса на обновление личного сертификата

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

Предварительно следует авторизоваться в ПК AvPCM под текущим сертификатом (см. п. 5 Запуск программы).

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 (см. п. 6.1. Создание запроса на сертификат). Особенностью данного создания запроса является то, что информация о будущем владельце сертификата заполняется автоматически на основании той, которая указана 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, нужно импортировать его в программу ПК AvPCM.

Процедура импорта в программу личного/обновленного личного сертификата пользователя описана в следующих пунктах данного документа (см. 6.5. Импорт личного сертификата).

6.5. Импорт личного сертификата

6.5.1. 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»

или

запустить ПК AvPCM, щелкнув по ярлыку «Персональный менеджер сертификатов Авест», находящемся на вашем Рабочем столе. (см. п. 5. Запуск программы). Если появится окно авторизации, поставить галочку напротив пункта «Войти в систему без авторизации» и нажать «ОК». В открывшемся менеджере сертификатов нужно выбрать пункт меню «Файл»→«Импорт сертификата/СОС»;

2) в диалоговом окне мастера импорта сертификатов, нужно указать имя папки, из которой 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 40. Информация об импортируемых объектах).

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.

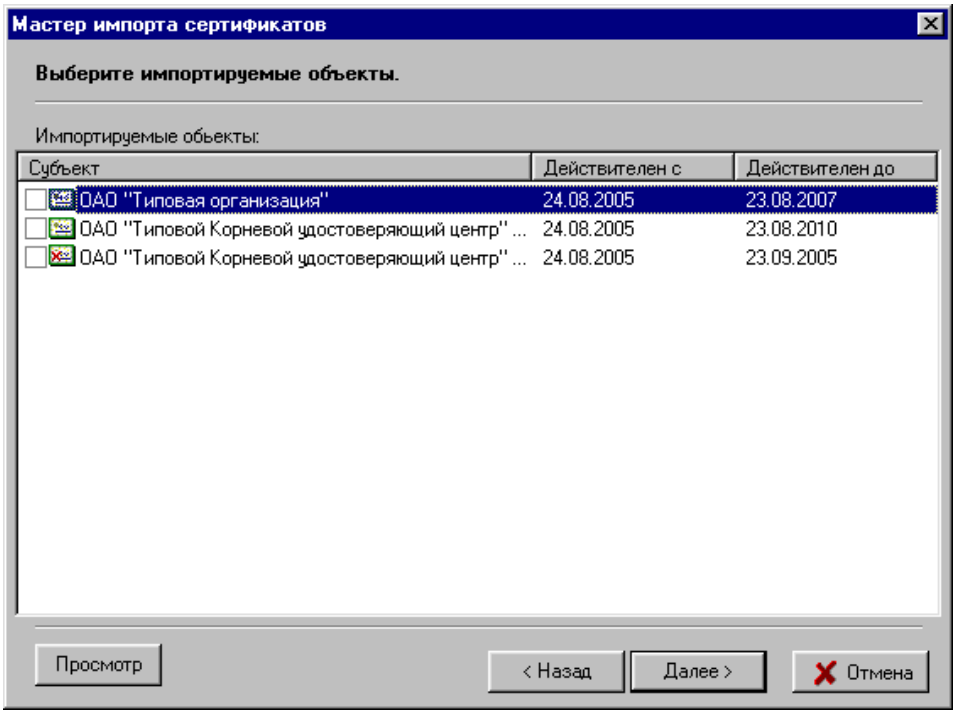


Рисунок 40. Информация об импортируемых объектах

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 указано «Сертификаты не были проимпортированы, возможно, они уже присутствуют в системе» (см. Рисунок 41. Помещение личного сертификата в персональный справочник).

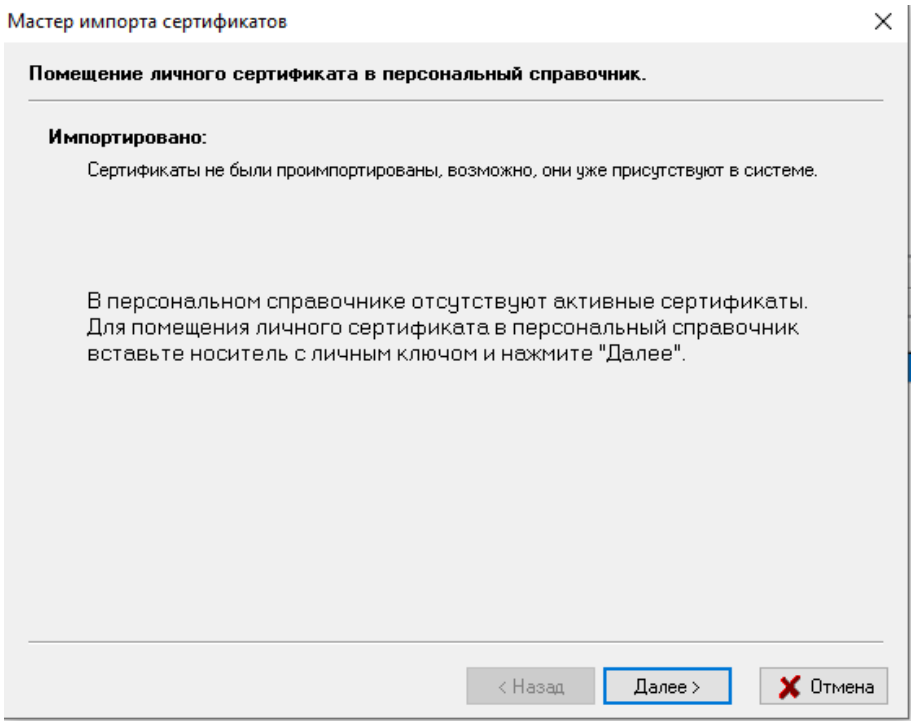


Рисунок 41. Помещение личного сертификата в персональный справочник

Для помещения личного сертификата в персональный справочник надо 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» надо 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 42. Просмотр корневого сертификата УЦ).

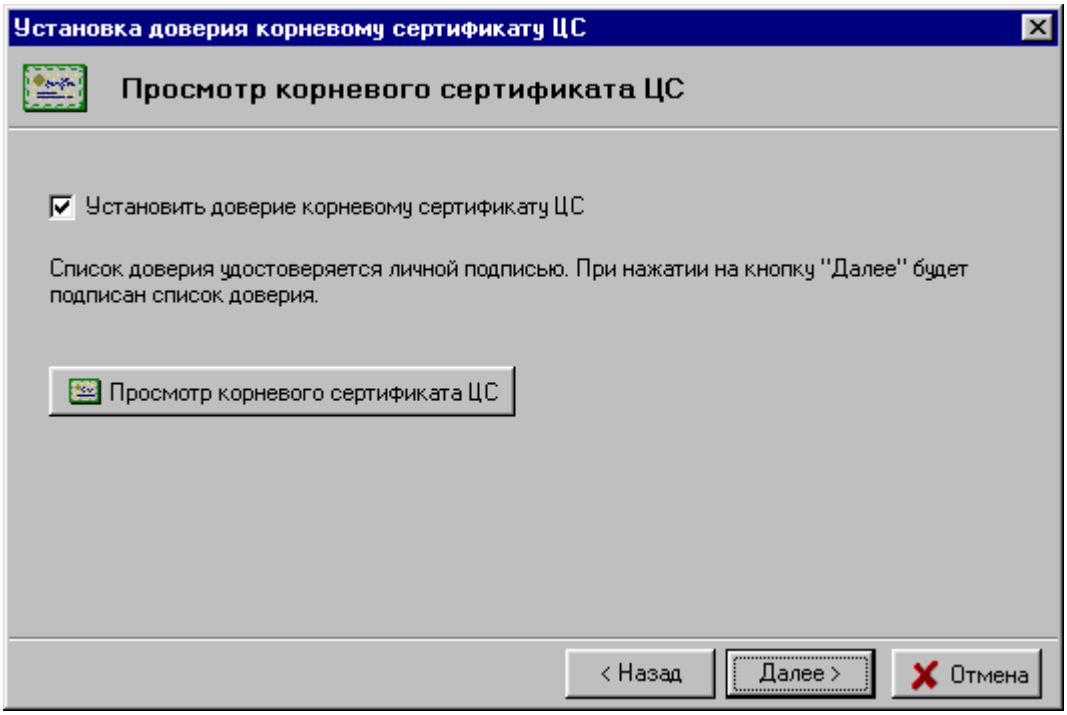


Рисунок 42. Просмотр корневого сертификата УЦ

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

После успешного импорта личный сертификат появится в личном справочнике, он будет обведен красной рамкой, в окне заголовка менеджера будет отображаться общее имя (общие данные) личного сертификата (см. Рисунок 43. Сертификат в личном справочнике).

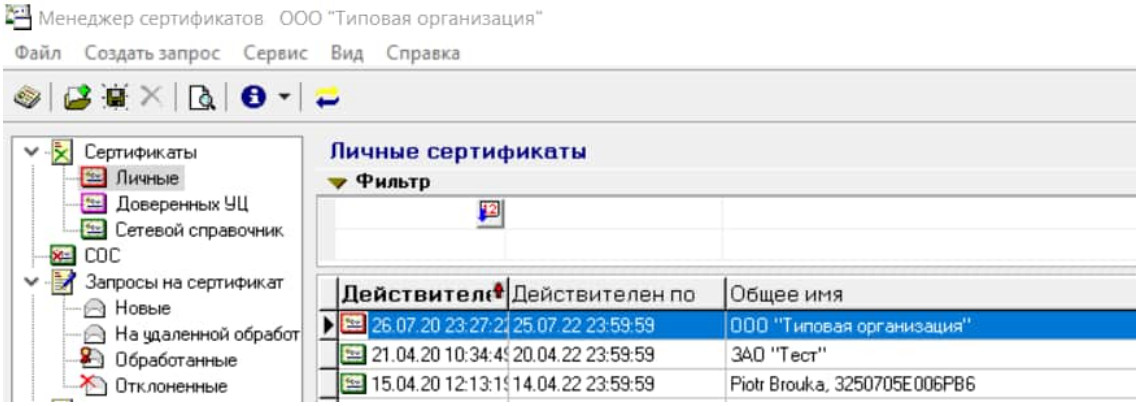


Рисунок 43. Сертификат в личном справочнике

Примечание:

Если запрос на сертификат создавался в этом же менеджере, то он будет помещен в личный справочник автоматически после выпуска сертификата в УЦ. В этом случае нужно будет лишь запустить менеджер с ярлыка на рабочем столе, в окне авторизации выбрать нужный сертификат, ввести пароль к контейнеру. После этого программа потребует установить доверие к сертификату Корневого УЦ (см. шаг 6), после успешного выполнения данной операции менеджер откроется с авторизацией под вашим личным сертификатом.

6.5.2. 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»

или

запустить ПК AvPCM, щелкнув по ярлыку «Персональный менеджер сертификатов Авест», находящемся на вашем Рабочем столе (см. п. 5. Запуск программы). Если появится окно авторизации, поставить галочку напротив пункта «Войти в систему без авторизации» и нажать «ОК». В открывшемся менеджере сертификатов нужно выбрать пункт меню «Файл»→«Импорт сертификата/СОС»;

2) в диалоговом окне мастера импорта сертификатов, нужно указать имя папки, из которой будет производиться импорт: личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и СОС, выпущенных УЦ (см. Рисунок 44. Выбор файла импортируемых данных);

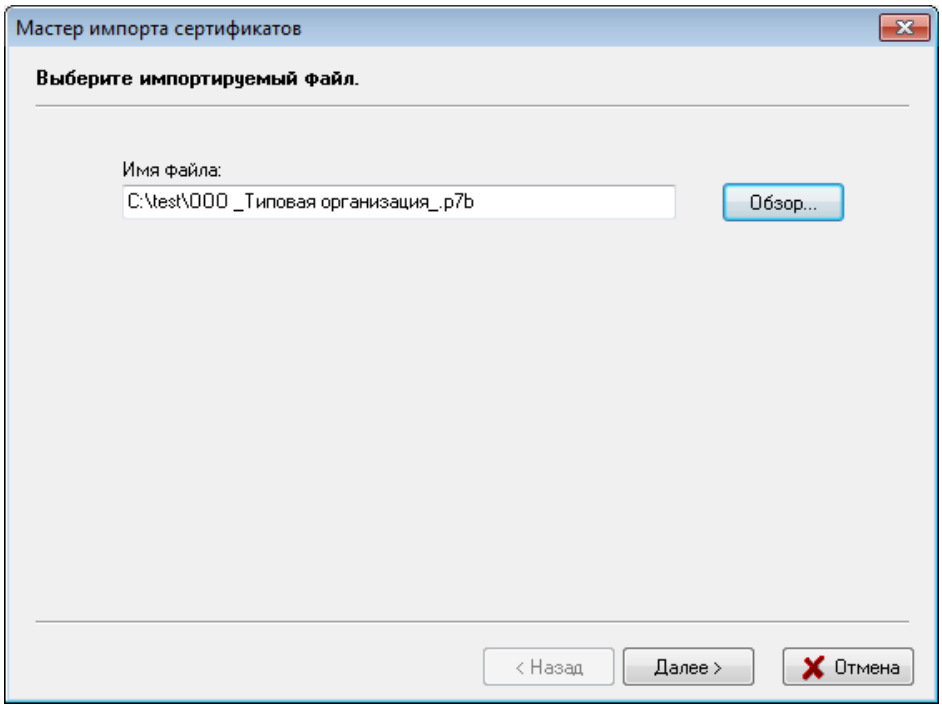


Рисунок 44. Выбор файла импортируемых данных

3) В появившемся окне в виде таблицы будут отражены все объекты, которые входят в импортируемый файл и могут быть подключены для работы (см. Рисунок 45. Информация об импортируемых объектах).

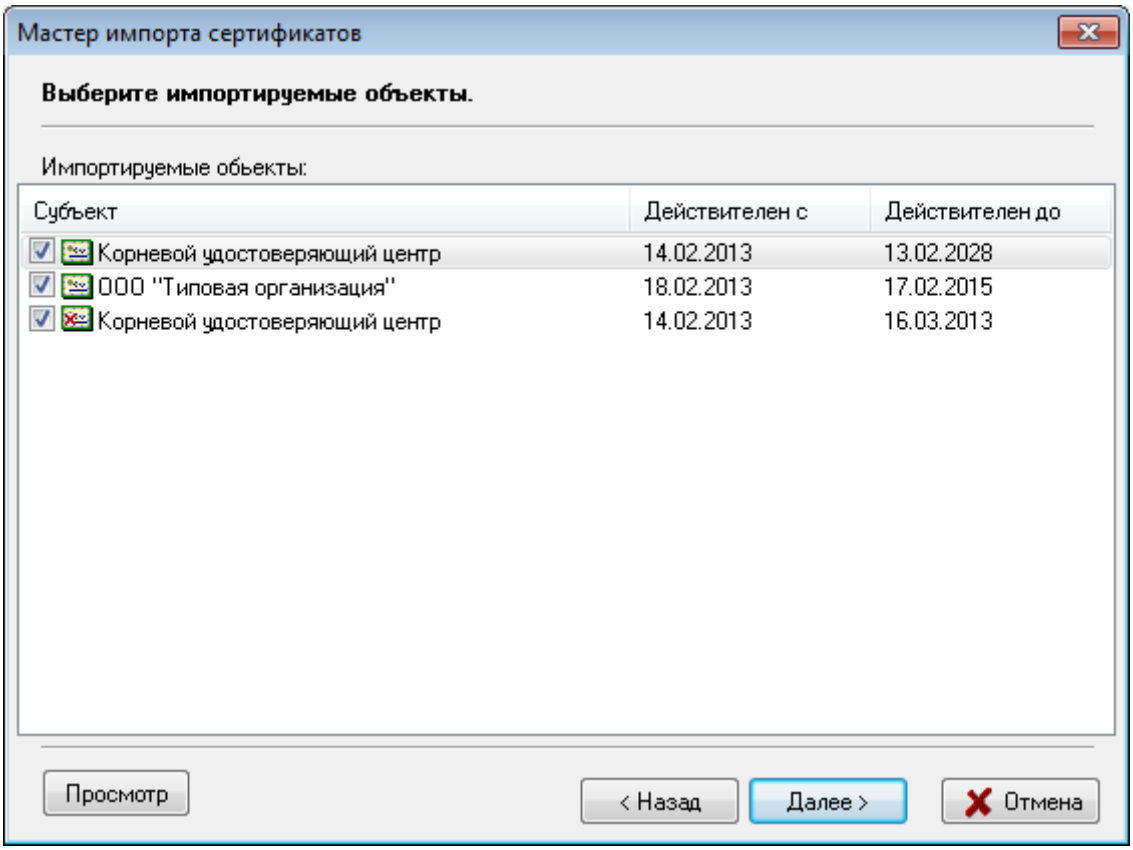


Рисунок 45. Информация об импортируемых объектах

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 46. Помещение личного сертификата в персональный справочник).

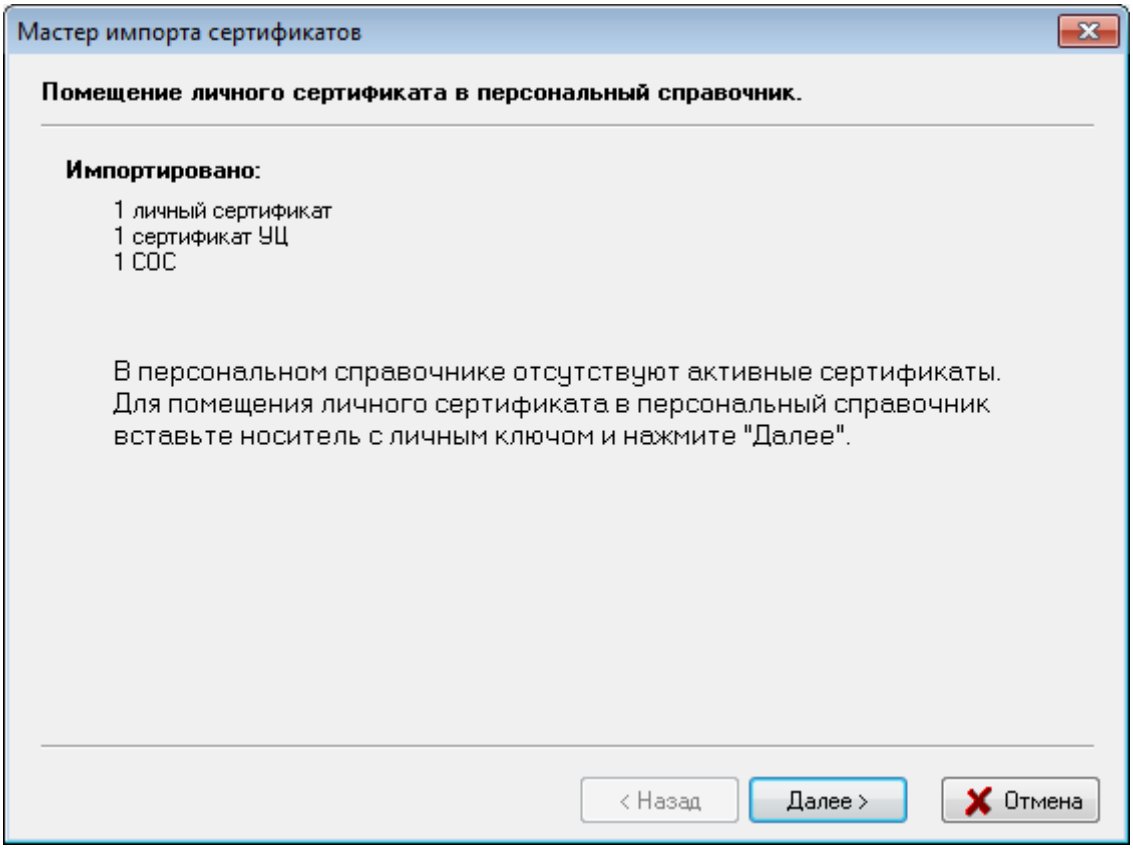


Рисунок 46. Помещение личного сертификата в персональный справочник

Т.к. это первый импорт личного сертификата в программу ПК AvPCM, то в персональном справочнике сертификатов он отсутствует. Поэтому, для помещения личного сертификата в персональный справочник нужно вставить носитель с 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 нужно из данного списка выбрать контейнер личного ключа, который соответствует личному сертификату и нажать кнопку «Далее» (см. Рисунок 47. Выбор контейнера личного ключа, соответствующего личному сертификату).

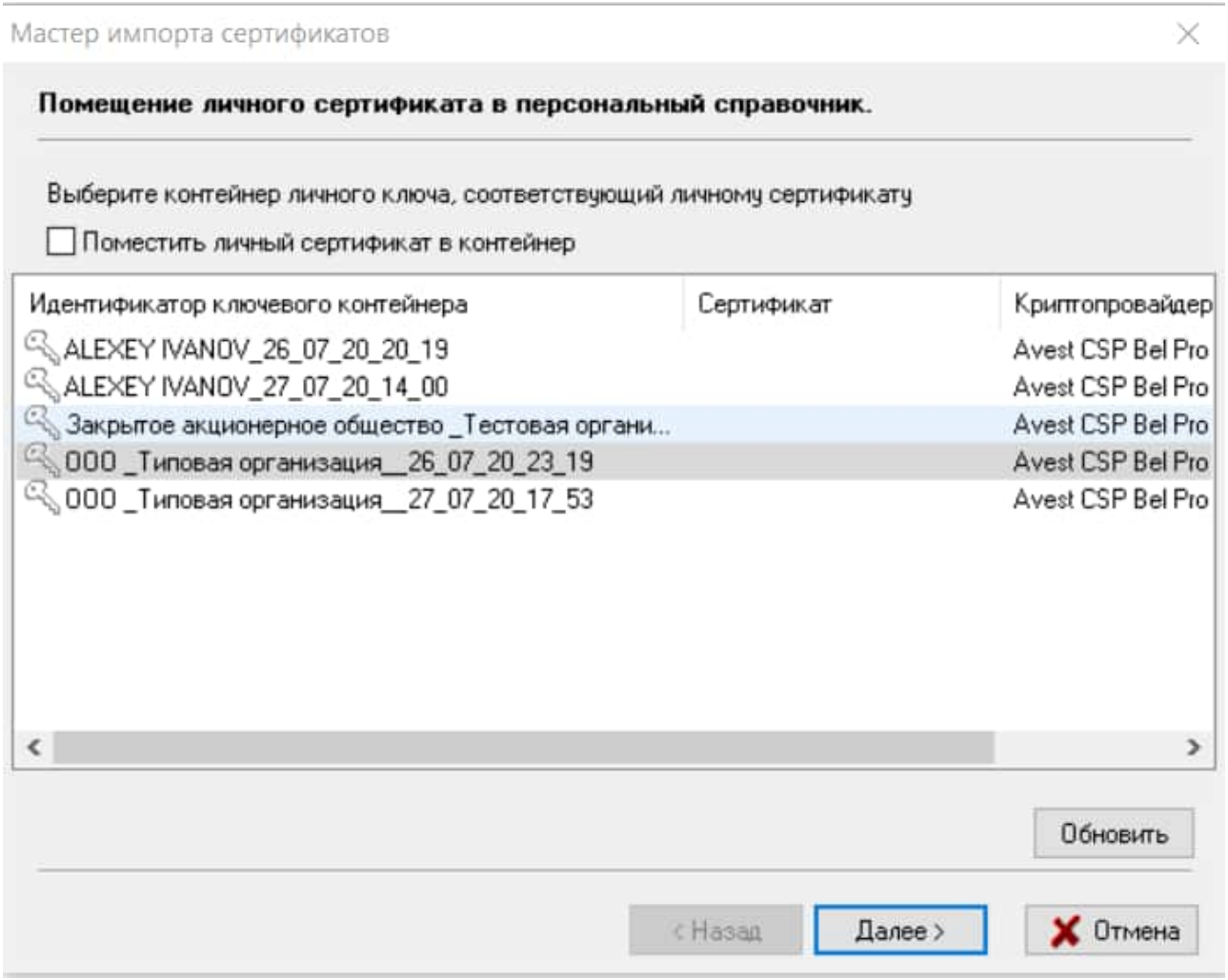


Рисунок 47. Выбор контейнера личного ключа, соответствующего личному сертификату

Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» надо ввести пароль, который вы вводили при генерации личных ключей (см. Рисунок 48. Ввод пароля доступа к контейнеру личного ключ**а**).

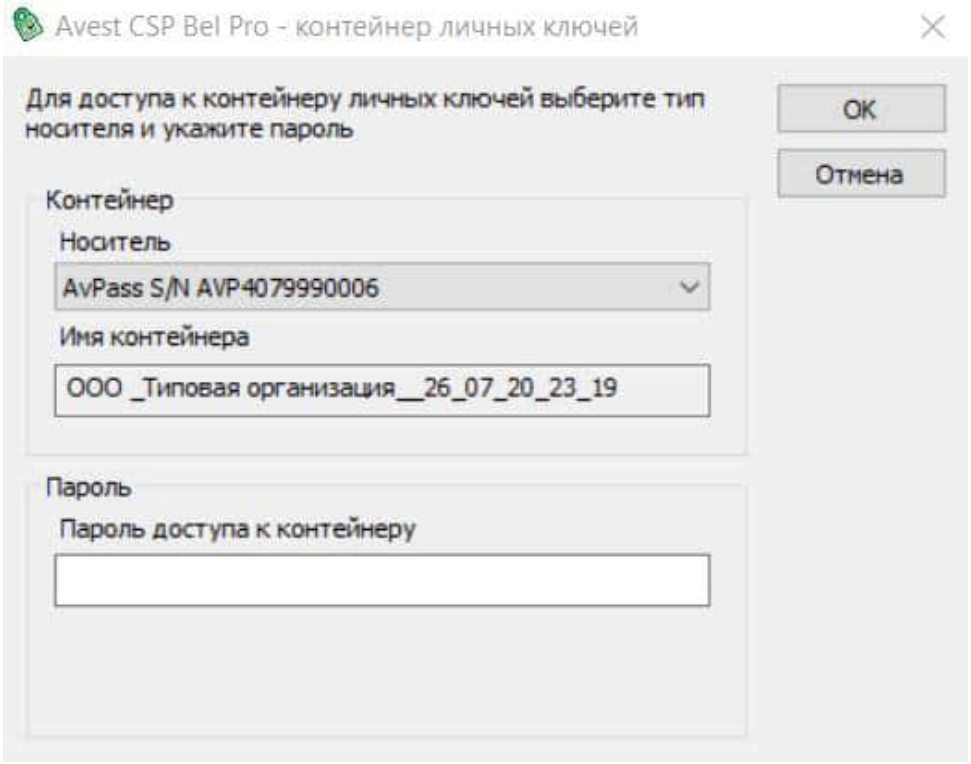


Рисунок 48. Ввод пароля доступа к контейнеру личного ключа

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

5) Для полнофункциональной работы программы нужно установить доверие к корневому сертификату УЦ. Для этого в следующем окне надо включить флажок «Установить доверие сертификату корневого УЦ» (см. Рисунок 49. Установка доверия сертификату корневого УЦ).

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».

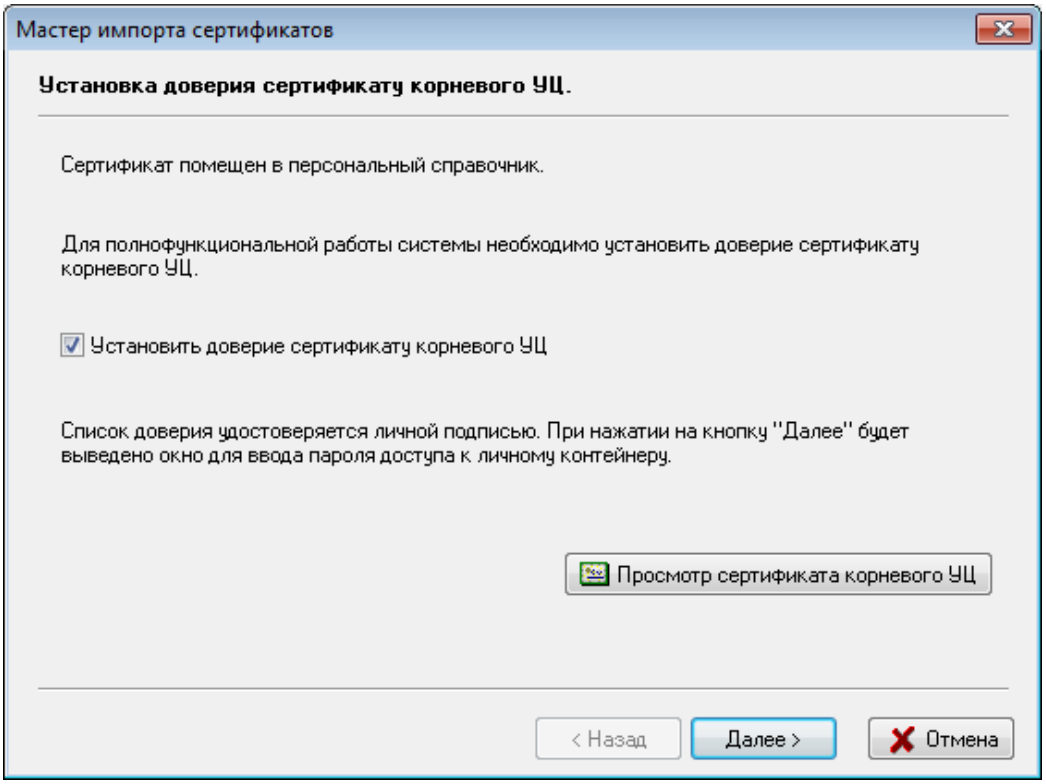


Рисунок 49. Установка доверия сертификату корневого УЦ

После этого будет выведено сообщение о том, что корневой сертификат УЦ помещен в список доверия и мастер импорта сертификатов завершил работу (см. Рисунок 50. Завершение работы мастера импорта сертификатов).

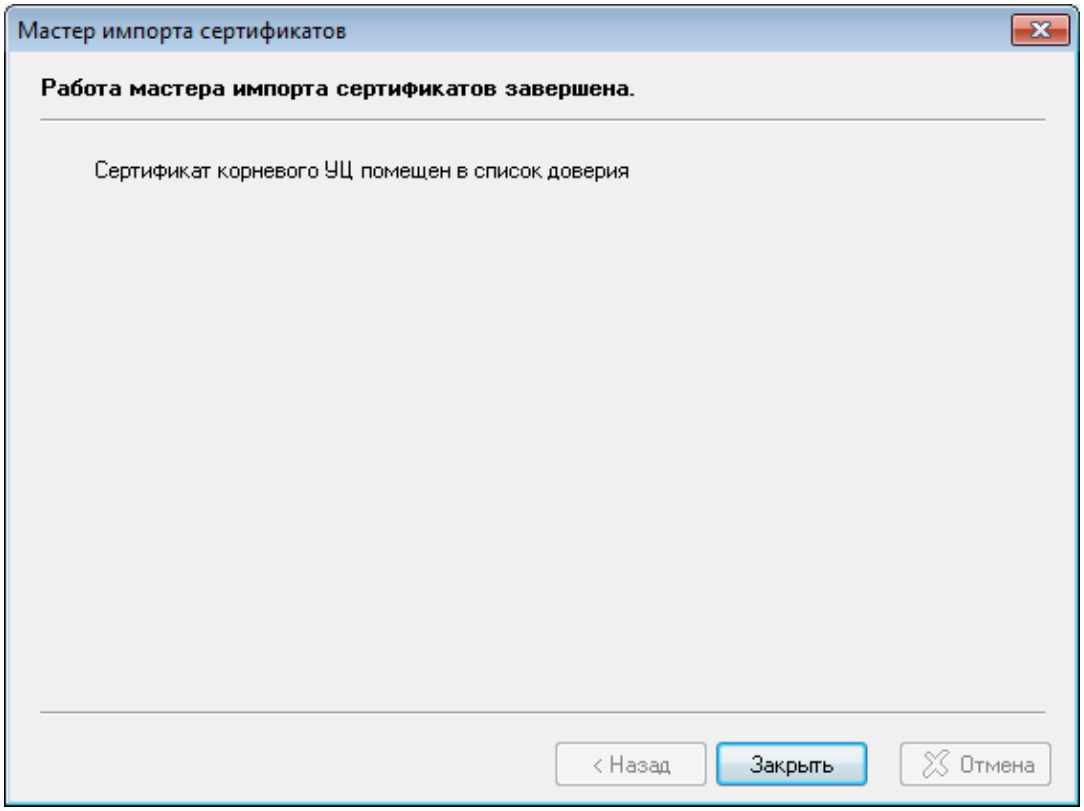


Рисунок 50. Завершение работы мастера импорта сертификатов

После успешного импорта личный сертификат появится в личном справочнике, он будет обведен красной рамкой, в окне заголовка менеджера будет отображаться общее имя (общие данные) личного сертификата (см. Рисунок 51. Сертификат в личном справочнике).

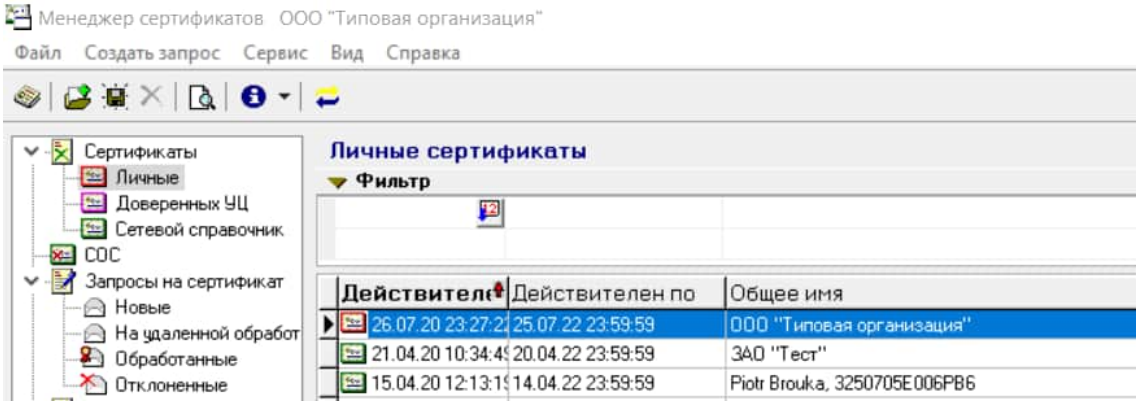


Рисунок 51. Сертификат в личном справочнике

6.5.3. Импорт личного сертификата при инсталляции с базой данных в хранилище Windows.

ВНИМАНИЕ!!! При импорте личного сертификата в хранилище Windows (реестр) нужно учитывать, что импортируемый сертификат будет привязан к учетной записи пользователя, от имени которого производится импорт, соответственно под другими учетными записями данный сертификат будет недоступен.

Действия по импорту личного сертификата при инсталляции с базой данных в хранилище Windows:

1) из основного меню Windows выбрать поочередно:
«Пуск»→»Программы»→«Авест»→«Персональный менеджер сертификатов»→»Импорт сертификатов»

или

запустить ПК AvPCM, щелкнув по ярлыку «Персональный менеджер сертификатов Авест», находящемся на вашем Рабочем столе (см. п. 5. Запуск программы). Если появится окно авторизации, поставить галочку напротив пункта «Войти в систему без авторизации» и нажать «ОК». В открывшемся менеджере сертификатов нужно выбрать пункт меню «Файл»→«Импорт сертификата/СОС»;

2) в диалоговом окне мастера импорта сертификатов, нужно указать имя каталога, из которого будет производиться импорт: личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и СОС, выпущенных УЦ (см. Рисунок 44. 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 45. 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».

4) 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 нужно из данного списка выбрать контейнер личного ключа, который соответствует личному сертификату и нажать кнопку «Далее» (см. Рисунок 47. Выбор контейнера личного ключа, соответствующего личному сертификату).

5) Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» нужно ввести пароль, который вы вводили при генерации личных ключей (см. Рисунок 48. Ввод пароля доступа к контейнеру личного ключа).

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

6) Для полнофункциональной работы программы нужно установить доверие сертификату корневого УЦ. Для этого надо в окне «Установка доверия корневому сертификату ЦС», где следует нажать «Далее» (см. Рисунок 49. Установка доверия сертификату корневого УЦ).

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» (см. Рисунок 49. Установка доверия сертификату корневого УЦ).

7) После этого будет выведено предупреждение операционной системы Windows о добавлении сертификата Корневого Удостоверяющего центра в корневое хранилище, в этом сообщении указаны атрибуты помещаемого сертификата. Если они соответствуют данным вашего Корневого УЦ, то нужно нажать «Да» (см. Рисунок 52. Проверка соответствия атрибутов корневого сертификата).

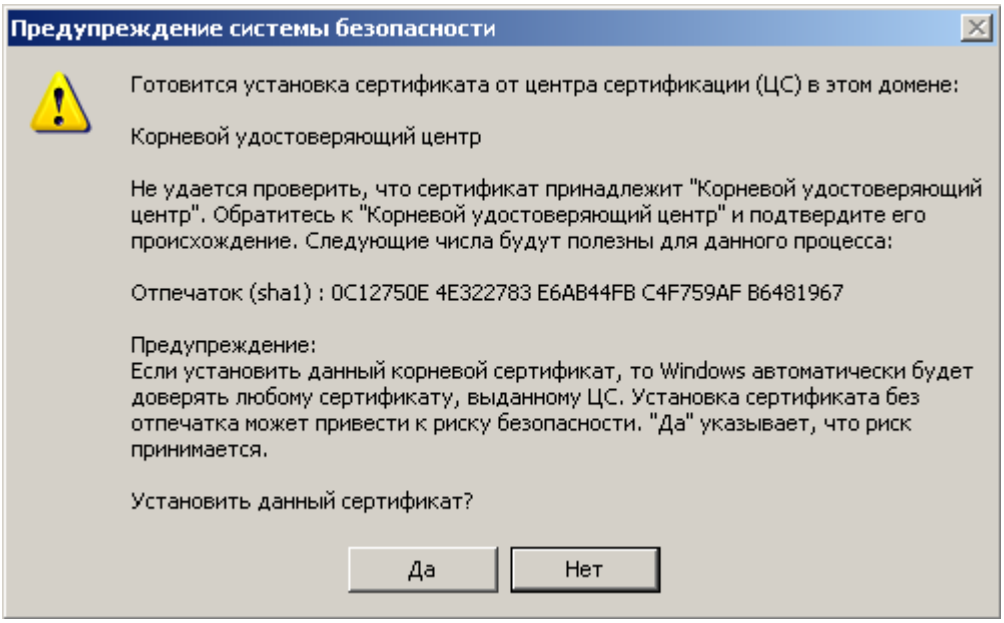


Рисунок 52. Проверка соответствия атрибутов корневого сертификата

После этого будет выведено сообщение о том, что корневой сертификат УЦ помещен в список доверия и мастер импорта сертификатов завершил работу (см. Рисунок 50. Завершение работы мастера импорта сертификатов).

После успешного импорта личный сертификат появится в личном справочнике, он будет обведен красной рамкой, в окне заголовка менеджера будет отображаться общее имя (общие данные) личного сертификата (см. Рисунок 53. Сертификат в личном справочнике).

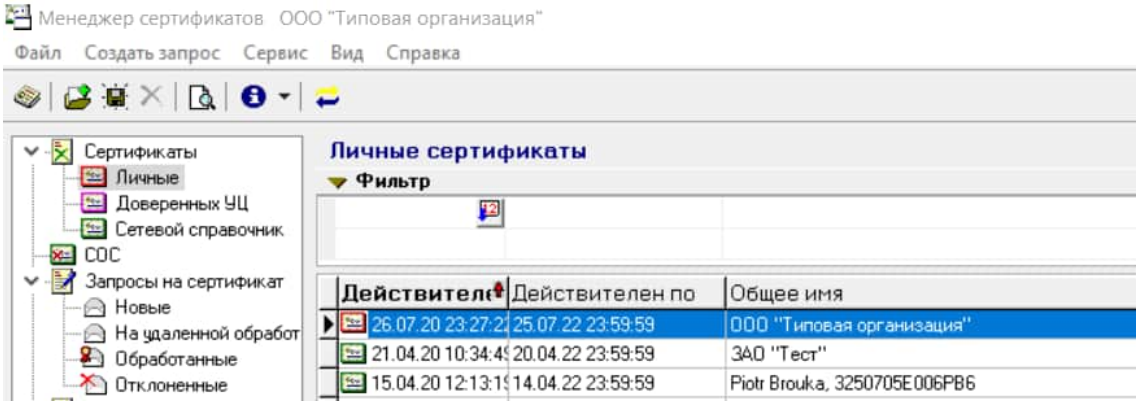


Рисунок 53. Сертификат в личном справочнике

6.5.4. Импорт личного сертификата при инсталляции с использованием устройств AvBign/AvHSM-Bign и хранилищем сертификатов в реестре Windows, с файловой базой, 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.

Действия при подключении личного сертификата:

1) из основного меню Windows выбрать поочередно: «Пуск»→«Программы»→ «Авест»→ «Персональный менеджер сертификатов»→»Импорт сертификатов»

или

запустить ПК AvPCM, щелкнув по ярлыку «Персональный менеджер сертификатов Авест», находящемся на вашем Рабочем столе (см. п. 5. Запуск программы). Если появится окно авторизации, поставить галочку напротив пункта «Войти в систему без авторизации» и нажать «ОК». В открывшемся менеджере сертификатов нужно выбрать пункт меню «Файл»→«Импорт сертификата/COC»;

2) В диалоговом окне мастера импорта сертификатов, нужно указать имя каталога, из которого будет производиться импорт: личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и COC, выпущенных УЦ (см. Рисунок 54. Выбор файла импортируемых данных);

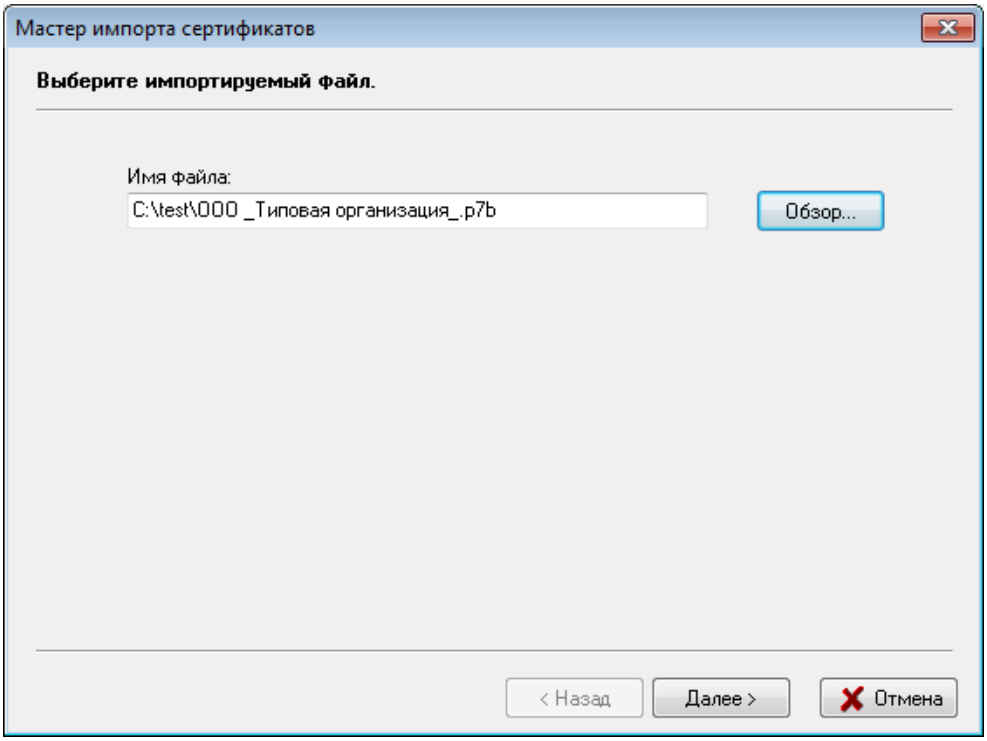


Рисунок 54. Выбор файла импортируемых данных

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 55. Информация об импортируемых объектах).

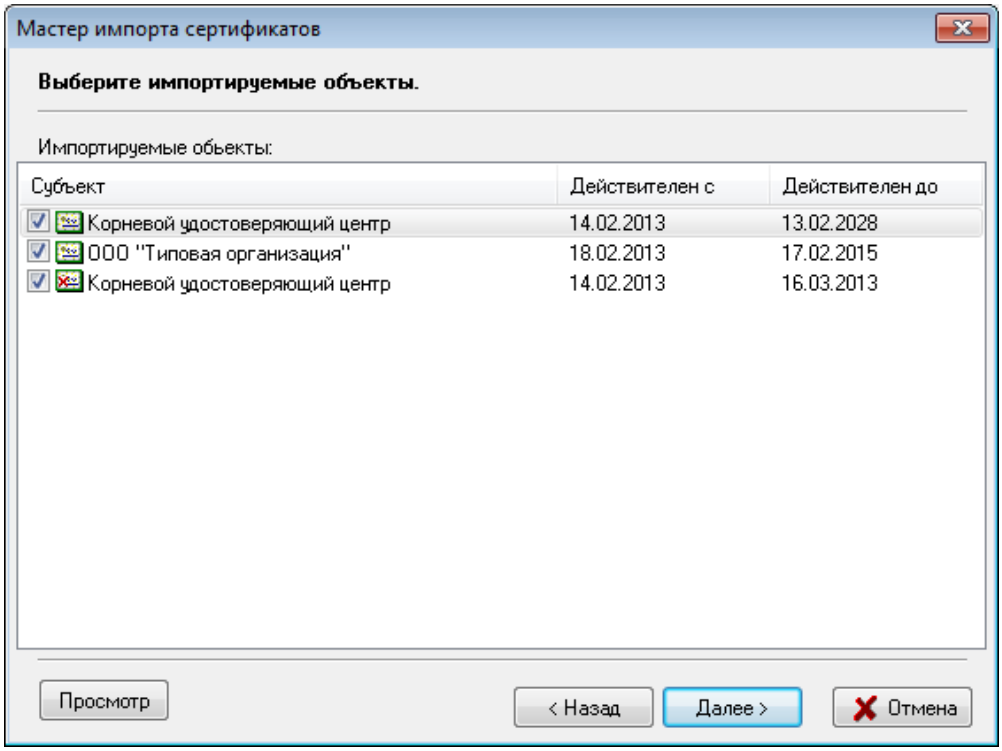


Рисунок 55. Информация об импортируемых объектах

4) В следующем окне содержится информация о необходимости перезапуска программы для выбора личного сертификата (см. Рисунок 56. Помещение личного сертификата в персональный справочник).

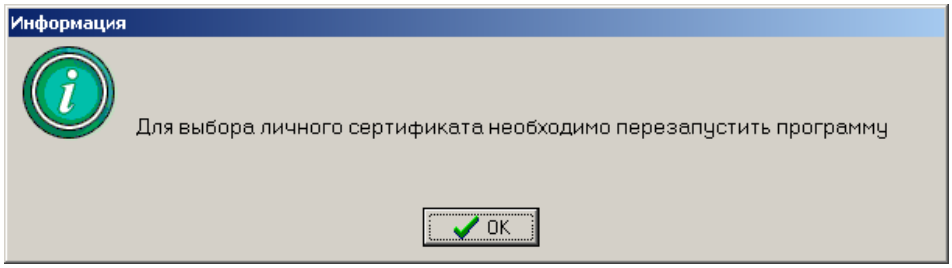


Рисунок 56. Помещение личного сертификата в персональный справочник

5) Далее программа выдаст сообщение об успешном импорте сертификатов и СОС (см. Рисунок 57. Завершение мастера импорта сертификатов).

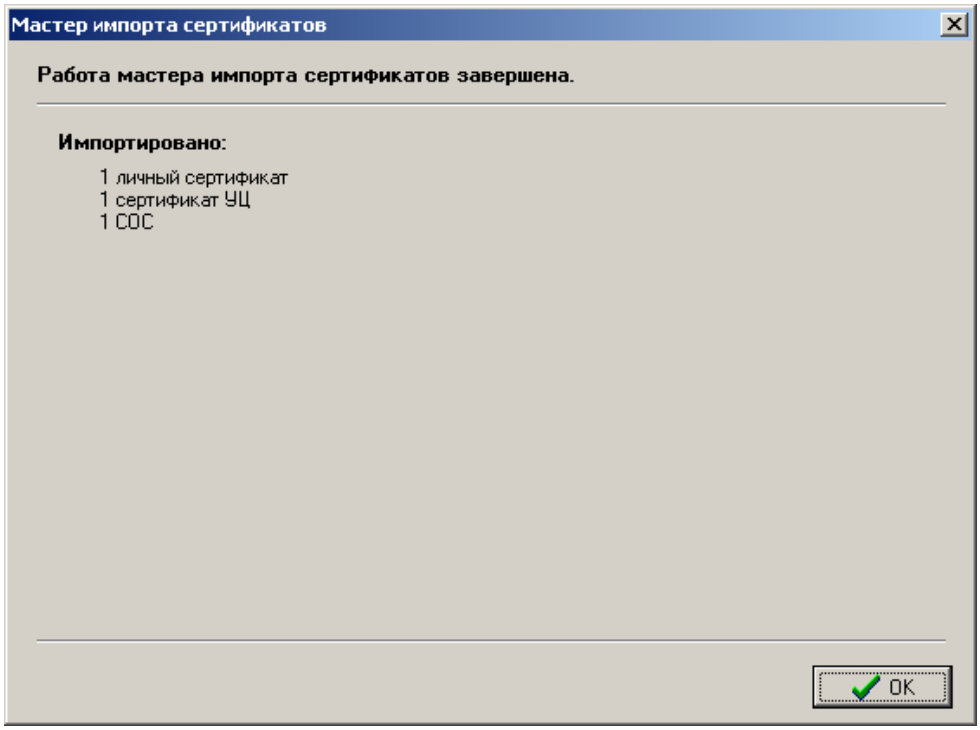


Рисунок 57. Завершение мастера импорта сертификатов

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

6) Для полнофункциональной работы программы нужно установить доверие сертификату корневого УЦ. Для этого надо перезапустить AvPCM и при авторизации выбрать личный сертификат. Далее появится окно «Установка доверия корневому сертификату ЦС», где следует нажать «Далее» (см. Рисунок 58. Установка доверия сертификату корневого УЦ).

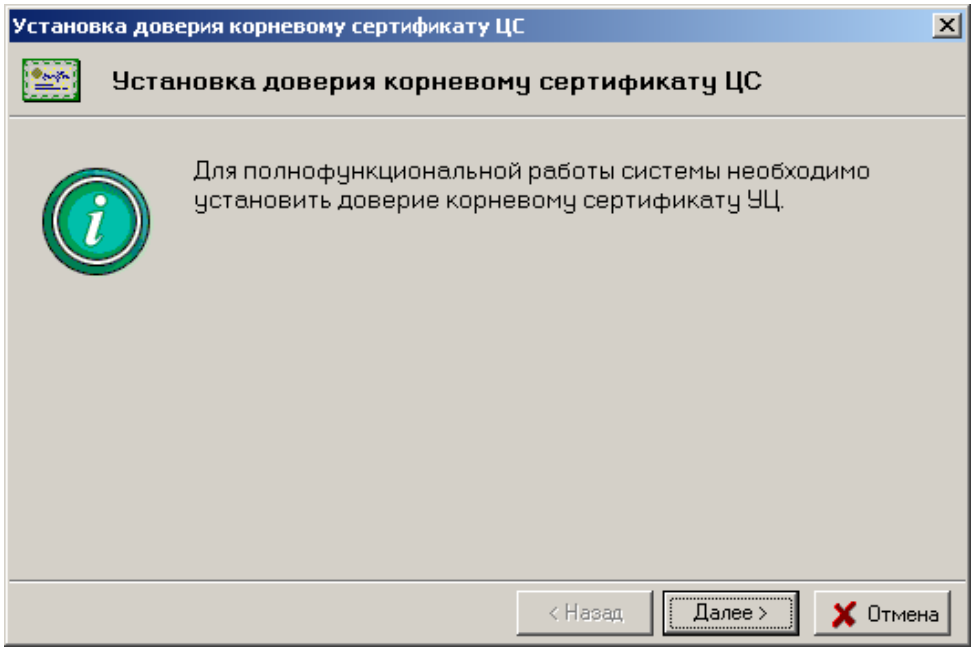


Рисунок 58. Установка доверия сертификату корневого УЦ

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» (см. Рисунок 59. Просмотр корневого сертификата ЦС).

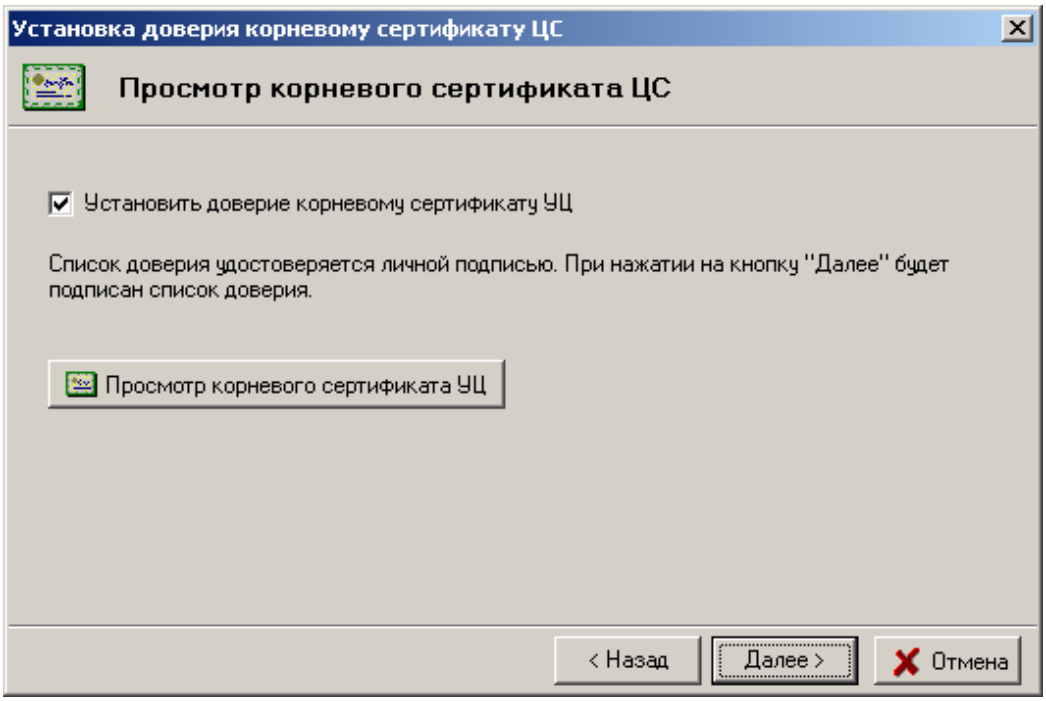


Рисунок 59. Просмотр корневого сертификата ЦС

В следующем окне программа сообщит о помещении корневого сертификата УЦ в список доверия. Здесь надо нажать на кнопку «Закрыть» (см. Рисунок 60. Завершение работы мастера импорта сертификатов).

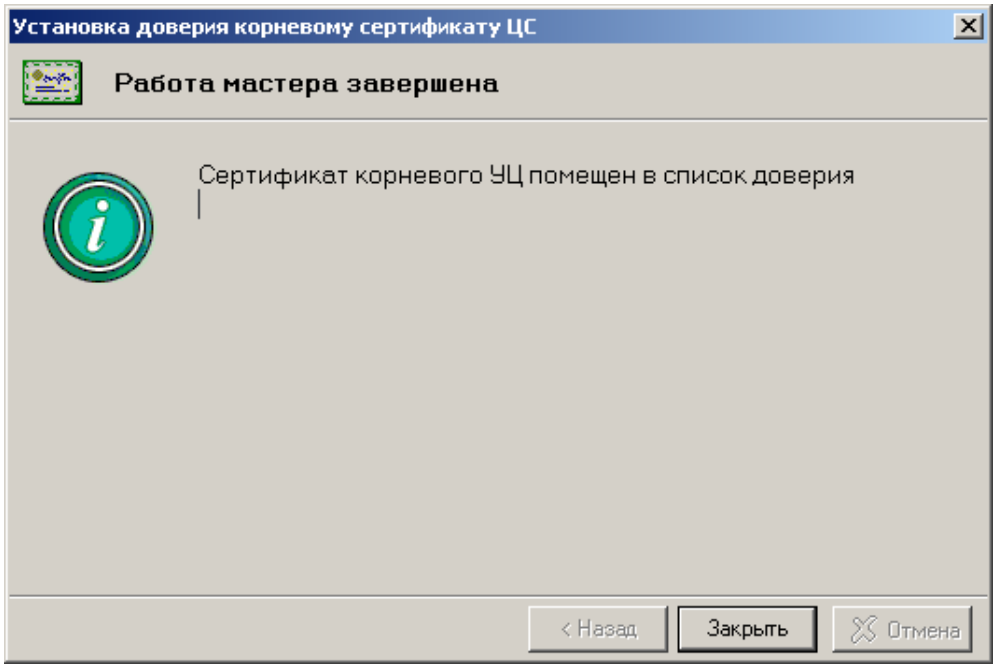


Рисунок 60. Завершение работы мастера импорта сертификатов

После успешного импорта личный сертификат появится в личном справочнике, он будет обведен красной рамкой, в окне заголовка менеджера будет отображаться общее имя (общие данные) личного сертификата (см. Рисунок 61. Сертификат в личном справочнике).

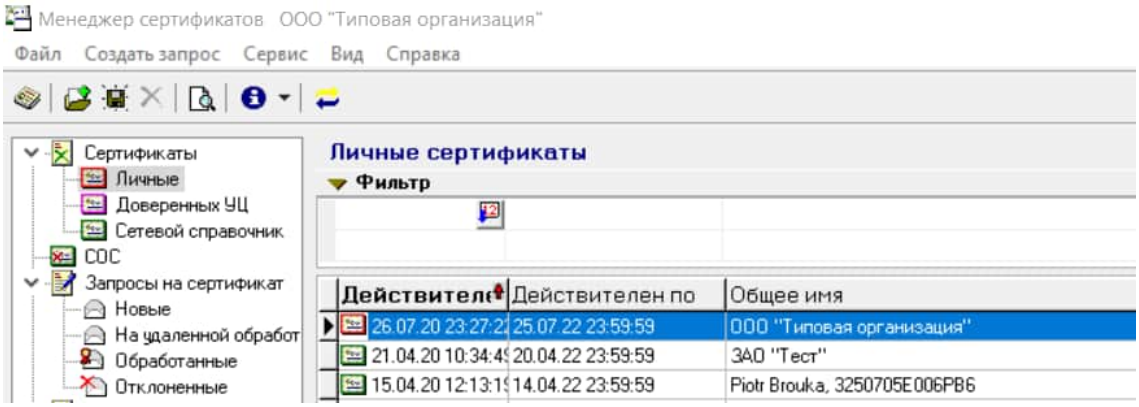


Рисунок 61. Сертификат в личном справочнике

6.5.5. Импорт сертификатов с сервера УЦ

Существует возможность импортировать с сервера УЦ личный сертификат, атрибутный сертификат (сертификаты), цепочки сопутствующих сертификатов Удостоверяющих центров, Службы атрибутных сертификатов и СОС, выпущенных УЦ.

Для того, чтобы ПК AvPCM мог взаимодействовать с сервером УЦ, в файл *AvCmMsg.ini*, который находится в папке с установленным менеджером, нужно внести секцию [certLookup], настройки из которой будут использоваться при соединении с сервером. Это будет IP-адрес или DNS-имя хоста, на котором располагается сервер.

ПРИМЕР заполнения секции [certLookup]:

```
[certLookup]
URL=https://test.nces.by/certdb/certificates/v1/
```

В случае, если на рабочем месте организован доступ к интернету через прокси-сервер, то в файл *AvCmMsg.ini*, надо дополнительно внести данные для подключения к прокси (см. п. 6.14.5 Задание настроек подключения через прокси-сервер).

При необходимости в файле *AvCmMsg.ini* можно указать протокол TLS, который будет использоваться при подключении к серверу (см. п. 6.14.6 Настройка протокола TLS).

Для подключения к серверу нужно поместить в справочник доверенных УЦ сертификат Корневого УЦ из инфраструктуры открытых ключей, выпустившей сертификат сервера УЦ (см. п. 6.7.3 Справочник «Доверенных Удостоверяющих центров»

Действия по импорту сертификатов с сервера УЦ:

1) вставить носитель с вашим личным ключом подписи/шифрования в считывающее устройство и нажать кнопку «Далее».

2) Выбрать пункт меню «Сервис» - «Импорт сертификатов с сервера УЦ» (см. Рисунок 62. Импорт сертификатов с сервера УЦ).

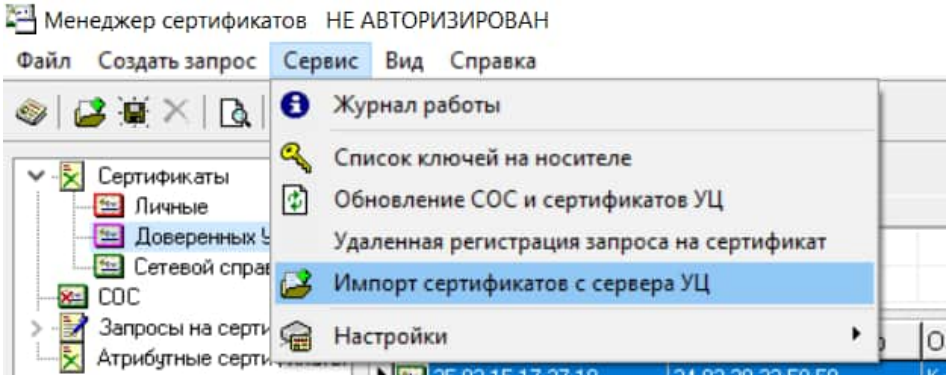


Рисунок 62. Импорт сертификатов с сервера УЦ

3) Произойдёт опрос установленных носителей и в появившемся окне будет выведена информация обо всех доступных личных ключах (см. Рисунок 63. Список ключей на носителе).

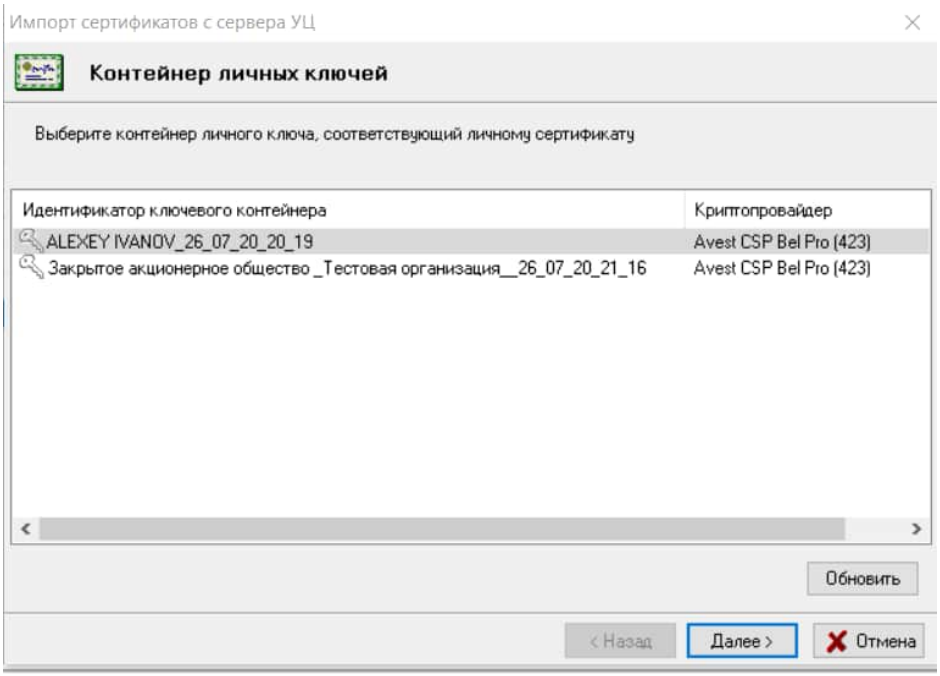


Рисунок 63. Список ключей на носителе

4) Для продолжения процедуры помещения личного сертификата в персональный справочник нужно из списка ключей на носителе выбрать контейнер с личным ключом, который соответствует личному сертификату и нажать кнопку «Далее».
5) Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» надо ввести пароль, который задавался при генерации личных ключей (см. Рисунок 64. Ввод пароля доступа к контейнеру личного ключа).

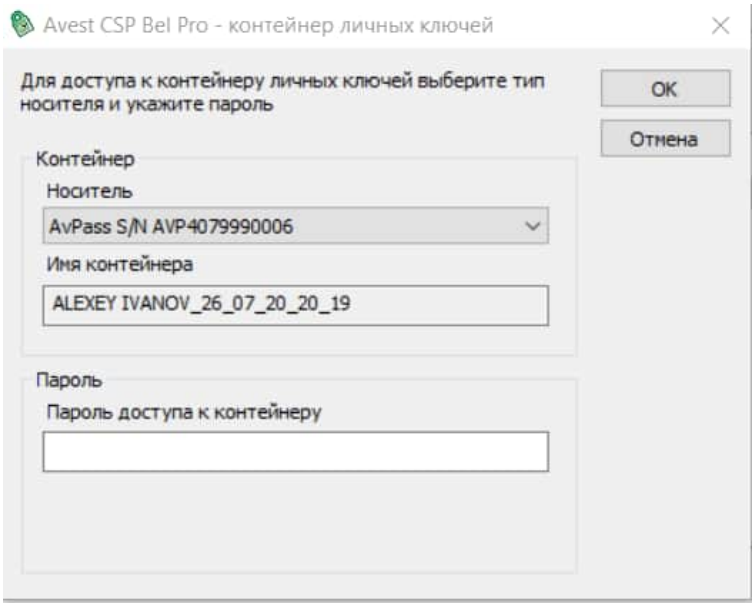


Рисунок 64. Ввод пароля доступа к контейнеру личного ключа

6) После ввода пароля отобразится окно, в котором будет указан URL-адрес сервиса УЦ (см. Рисунок 65. URL-адрес сервиса УЦ). Следует убедиться в корректности указанного адреса и изменить его, если нужно, после чего нужно нажать кнопку «Далее».

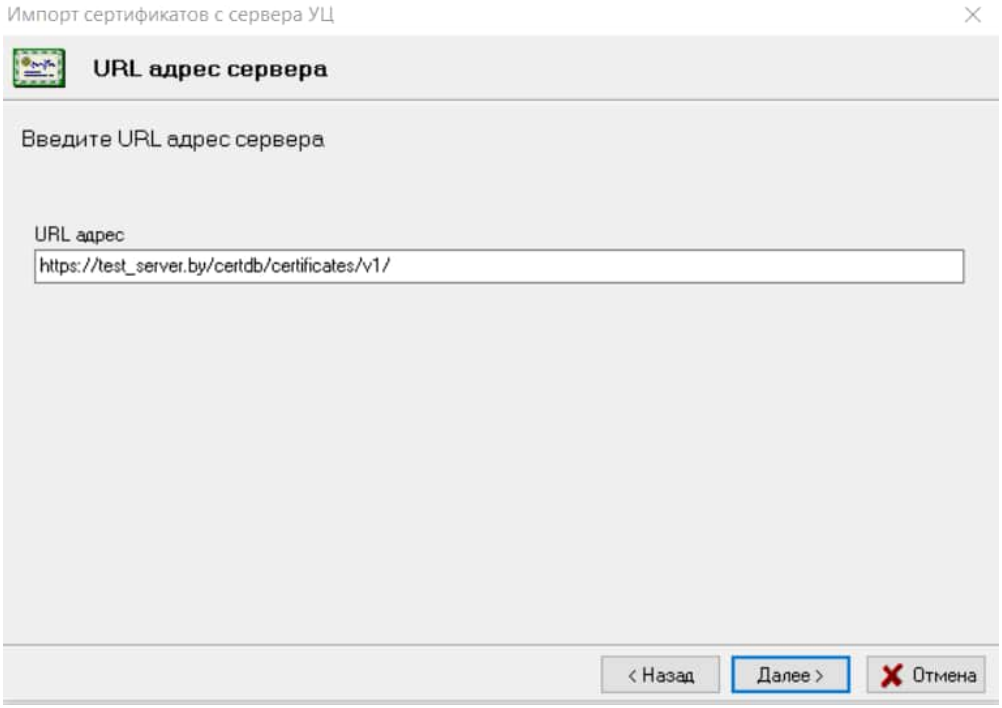


Рисунок 65. URL-адрес сервиса УЦ

7) После нажатия кнопки «Далее» будет отправлен запрос на сервер.

В случае, если в базе данных УЦ по данному URL адресу хранится сертификат, соответствующий личному ключу, выбранному на шаге 4, появится окно, в котором в виде таблицы будут отражены все объекты, которые хранятся на сервере УЦ (личный сертификат, атрибутный сертификат/сертификаты, сертификаты УЦ, Службы атрибутных сертификатов, СОС УЦ и Службы атрибутных сертификатов) и могут быть подключены для работы (см. Рисунок 66. Информация об импортируемых объектах). Выделив соответствующий объект в таблице, можно просмотреть

информацию, содержащуюся в файле, для этого надо нажать по нему правой клавишей мыши и нажать кнопку «Просмотр сертификата».

Галочками отмечены сертификаты, которые отсутствуют в системном справочнике и будут проимпортированы. 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».

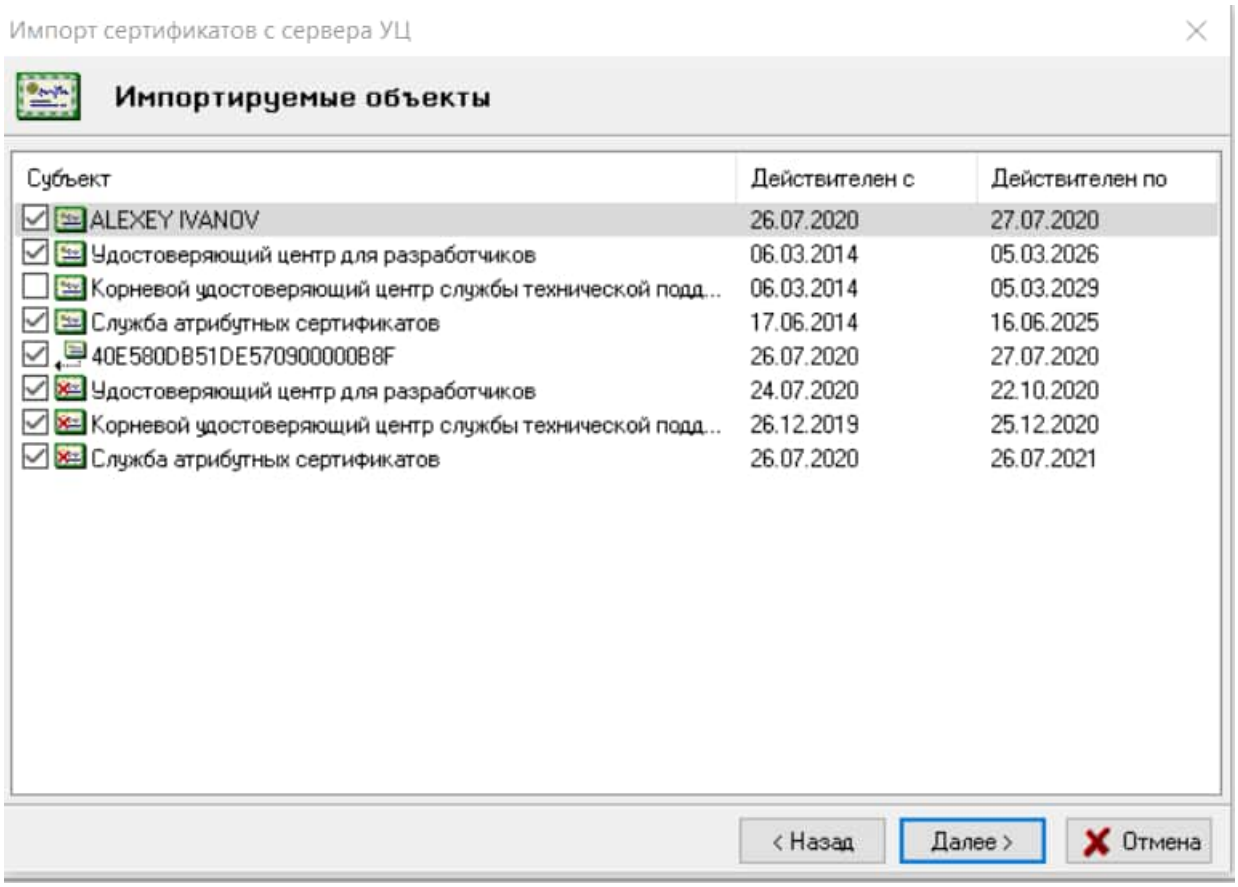


Рисунок 66. Информация об импортируемых объектах

8) После нажатия кнопки «Далее» будет произведен импорт выбранных объектов, а также помещение личного сертификата в справочник «Личные». Мастер импорта уведомит о количестве импортированных сертификатов (см. Рисунок 67. Завершение мастера работы). Работа мастера завершена, нужно нажать кнопку «Закрыть».

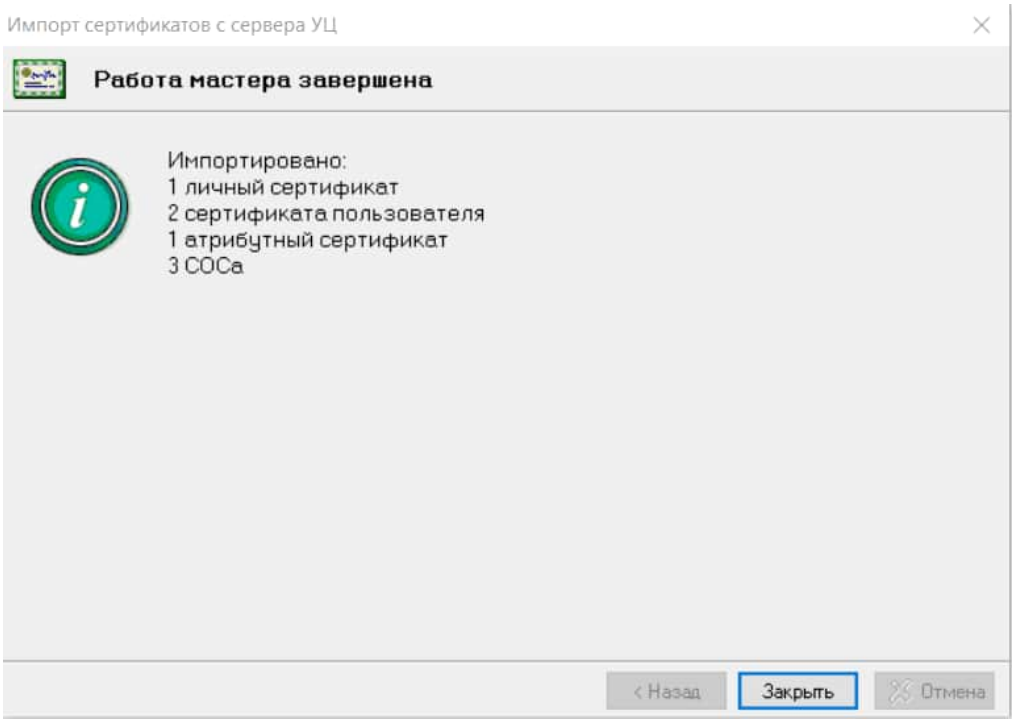


Рисунок 67. Завершение мастера работы

После успешного импорта личный сертификат появится в личном справочнике, он будет обведен красной рамкой, в окне заголовка менеджера будет отображаться общее имя (общие данные) личного сертификата, атрибутный сертификат будет отображаться в нижней части главного окна после выбора соответствующего личного сертификата в верхней части окна (см. Рисунок 68. Сертификат в личном справочнике).

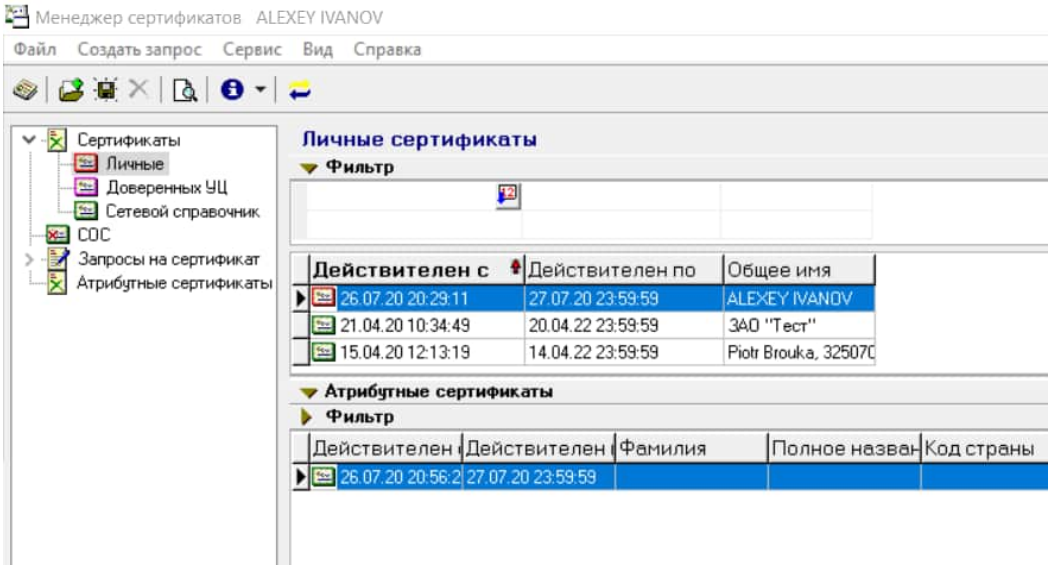


Рисунок 68. Сертификат в личном справочнике

Ошибки, которые могут возникнуть при подключении к серверу УЦ:

1. Если URL адрес сервера УЦ задан некорректно, будет ошибка «Ошибка HTTP: Неверно задан URL» (см. Рисунок 69. Ошибка HTTP: Неверно задан URL). Нужно указать верный адрес URL сервера УЦ.

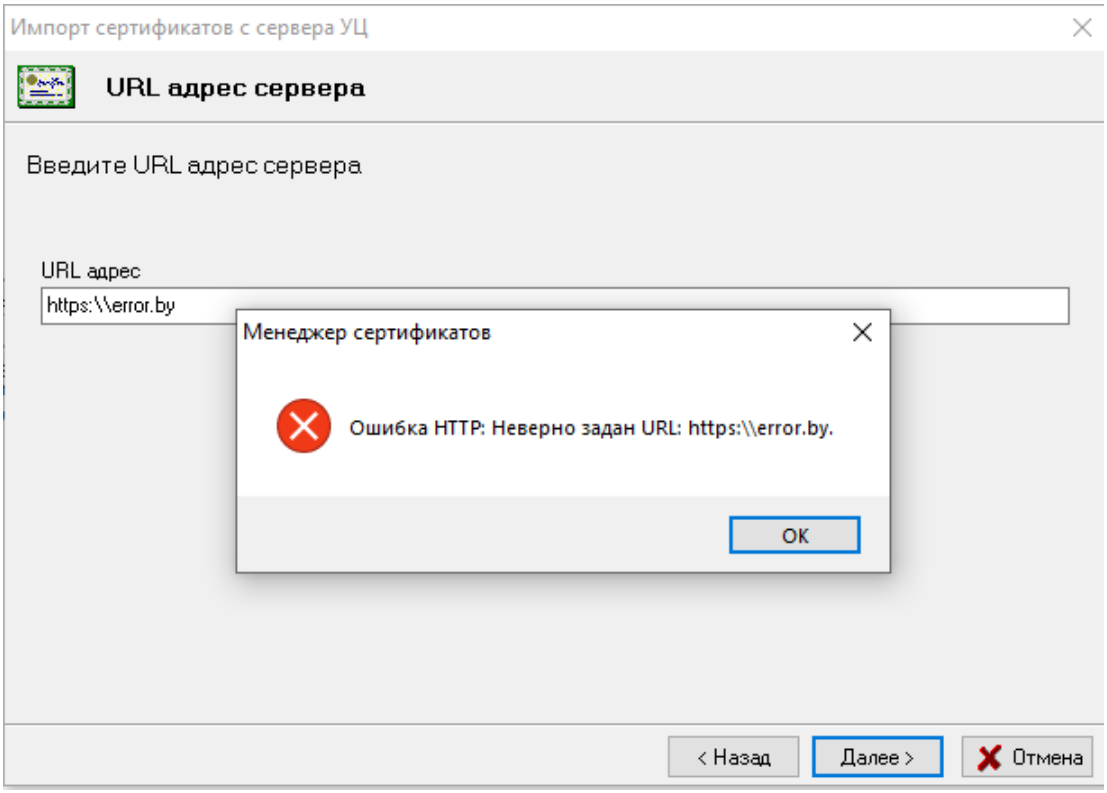


Рисунок 69. Ошибка HTTP: Неверно задан URL

2. Если URL адреса сервера УЦ не существует, то будет ошибка «Ошибка HTTP: Socket Error # 11001 Host not found» (см. Рисунок 70. Ошибка HTTP: Socket Error # 11001 Host not found). Нужно указать верный адрес URL сервера УЦ.

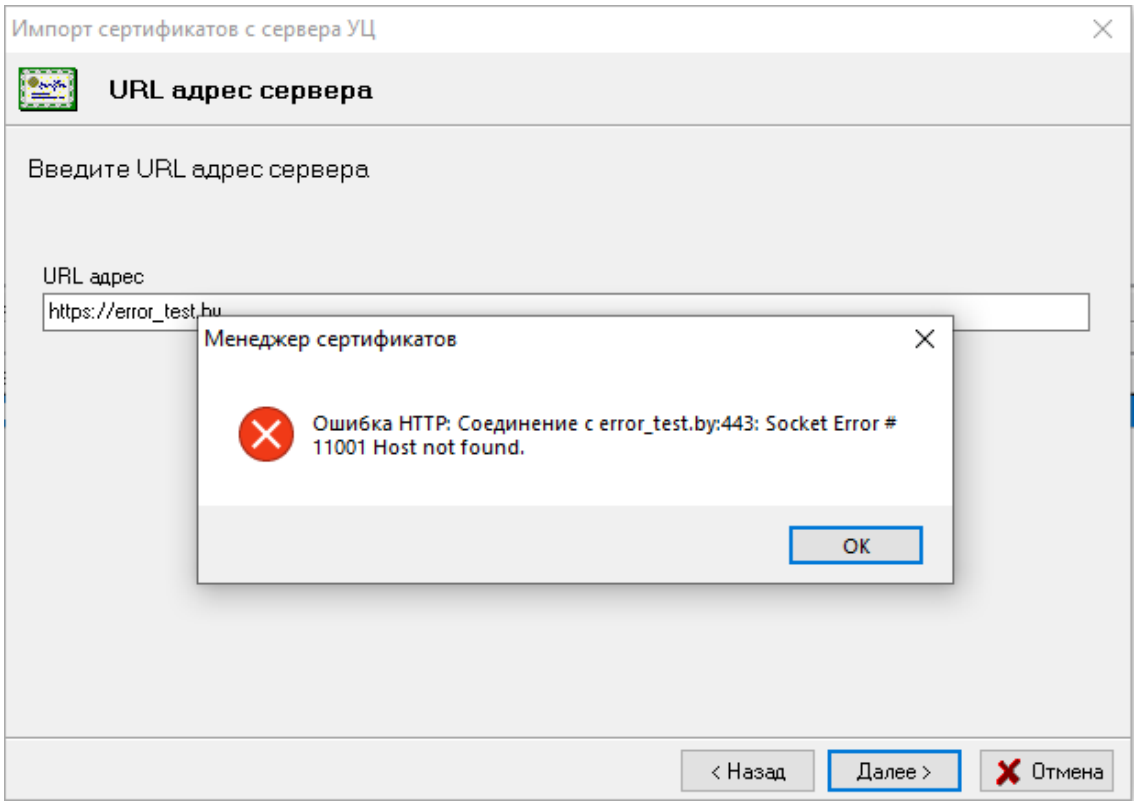


Рисунок 70. Ошибка HTTP: Socket Error # 11001 Host not found

3. Если в базе данных УЦ нет личного сертификата, соответствующего личному ключу, выбранному на шаге 4, появится ошибка: «Для данного ключа нет сертификата на сервере» (см. Рисунок 71. Ошибка подключения к серверу). Ошибка говорит о том, что на этапе 4 был выбран неподходящий контейнер с личным ключом или указан неправильный сервер, на котором не хранятся сертификаты, подходящие к данному личному ключу. В этом случае нужно или изменить адрес сервера, или выбрать другой контейнер с личным ключом на носителе или подключить другой носитель.

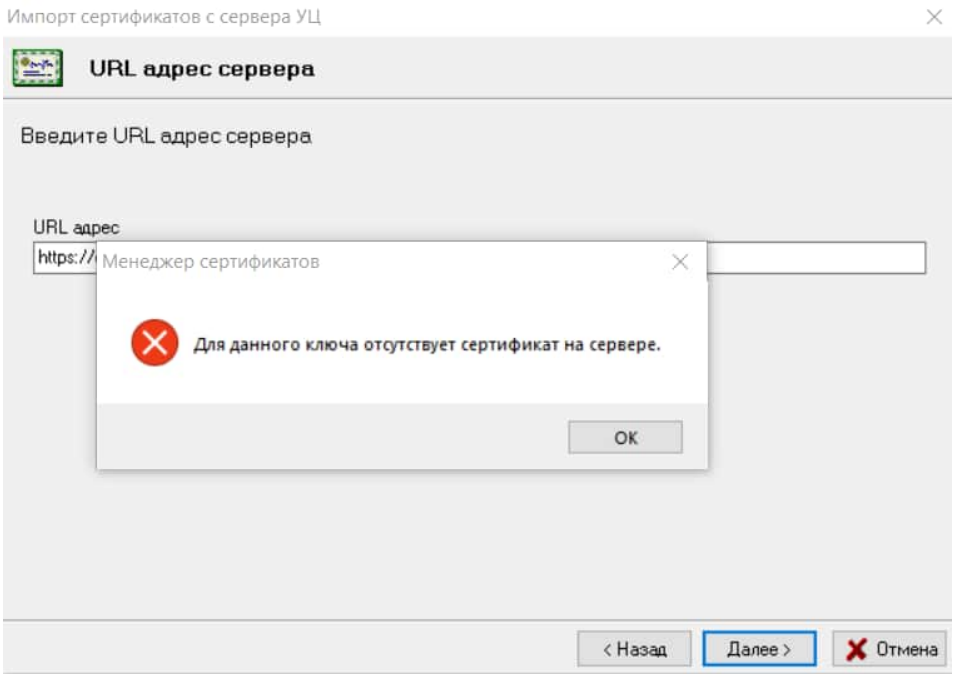


Рисунок 71. Ошибка подключения к серверу

4. Если не установлено доверие к сертификату Корневого удостоверяющего центра из инфраструктуры открытых ключей, выпустившей сертификат сервера УЦ, появится ошибка: «Нет доверия сертификату [KeyID=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX]» (см. Рисунок 72. Ошибка: «Нет доверия сертификату»). В этом случае надо проимпортировать сертификат КУЦ с данным идентификатором ключа субъекта (KeyID), если он не проимпортирован, и поместить его в справочник доверенных УЦ (см. п. 6.7.3 Справочник «Доверенных Удостоверяющих центров»).

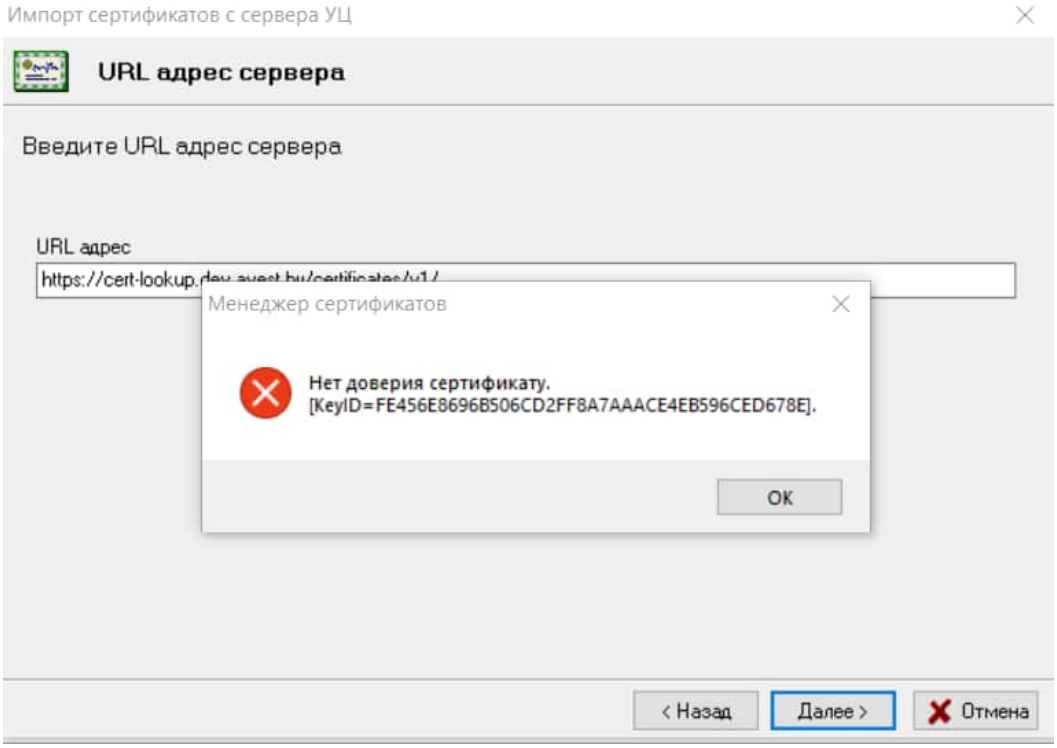


Рисунок 72. Ошибка: «Нет доверия сертификату»

5. В некоторых случаях могут возникнуть ошибки подключения к серверу, связанные с настройками протоколов TLS (см. Рисунок 73. Ошибка подключения к серверу «The signature was not verified»). В этом случае надо указать вручную протокол TLS для подключения к серверу (см. п. 6.14.6 Настройка протокола TLS).

Рисунок 73. Ошибка подключения к серверу «The signature was not verified»

6. Если истек срок действия СОС удостоверяющего центра из инфраструктуры открытых ключей, выпустившей сертификат сервера УЦ, появится ошибка: «Срок действия СОС истек» (см. Рисунок 74. Ошибка: «Срок действия СОС истек»). Необходимо проимпортировать актуальный СОС УЦ (см. пп. 6.9.5 Импорт сертификатов (СОС) и 6.14.1 Обновление СОС и сертификатов УЦ с использованием пункта меню «Сервис» - «Обновление СОС и сертификатов УЦ»).

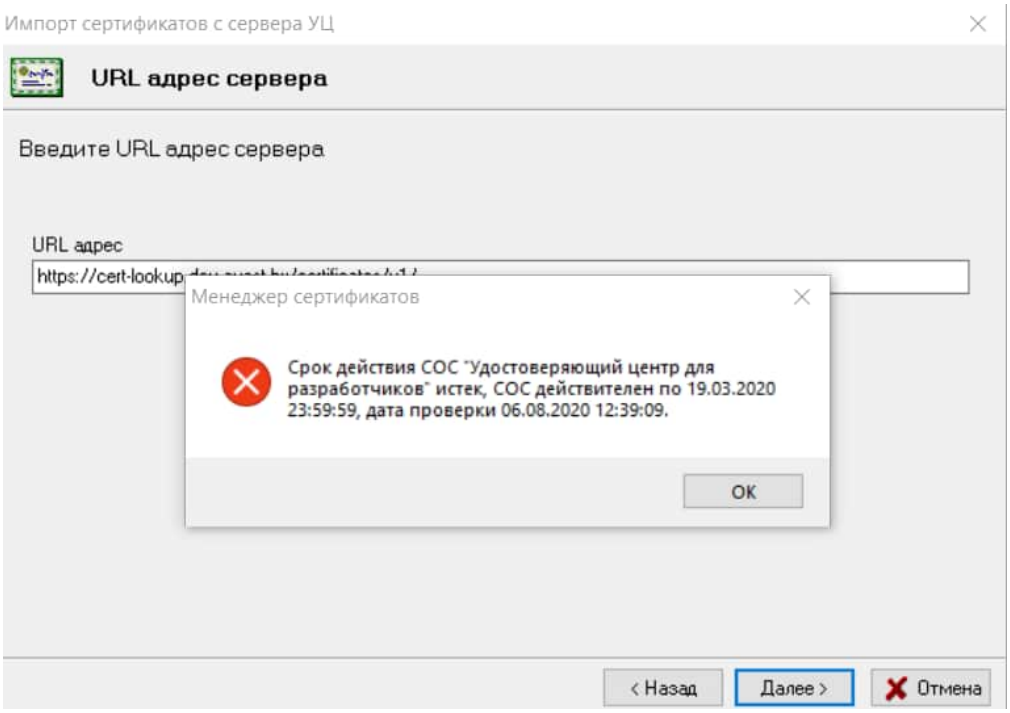


Рисунок 74. Ошибка: «Срок действия СОС истек»

6.6. Главное окно программы

После запуска программы ПК AvPCM и прохождения процедуры авторизации на экране появится главное окно программы (см. Рисунок 75. Интерфейс программы ПК AvPCM).

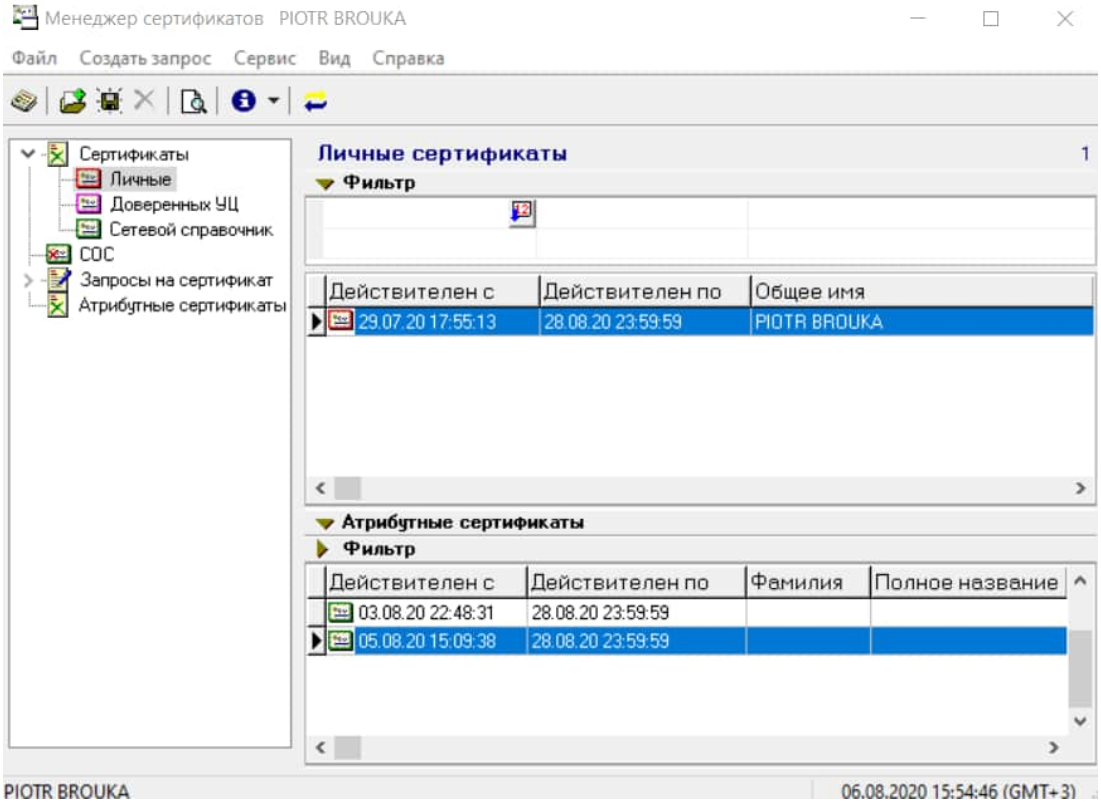


Рисунок 75. Интерфейс программы ПК AvPCM

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 три части для визуализации базы данных сертификатов пользователя.

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

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

В правой нижней части главного окна отображается детализация информации об атрибутных сертификатах. Если в правой верхней части окна выбран конкретный объект из справочника «Сертификаты», то в правой нижней части отобразится информация об атрибутных сертификатах, выпущенных для выбранного объекта.

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);
- –действие сертификата, находящегося в базе данных программы, временно приостановлено;
- – сертификат (атрибутный сертификат), находящийся в базе данных программы действителен;
- – атрибутные сертификаты;
- – 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». Появится дополнительное окно для поиска нужной информации и значок изменит свою форму на ▼ «Фильтр». В появившемся дополнительном окне надо стать курсором в графу с тем параметром, по которому будет проводиться отбор, и ввести одно из значений интересующего вас сертификата. В нижнем окне 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. (Если нужные поля не отображаются, то их можно настроить, подробнее см. п. 6.7.1 Просмотр содержимого справочников).

В 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 нужно 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 всплывающем меню выбрать пункт «Печать списка»;
3) в появившемся окне можно просмотреть список сертификатов, и нажав на соответствующую пиктограмму в меню, распечатать (см. Рисунок 76. Список сертификатов).

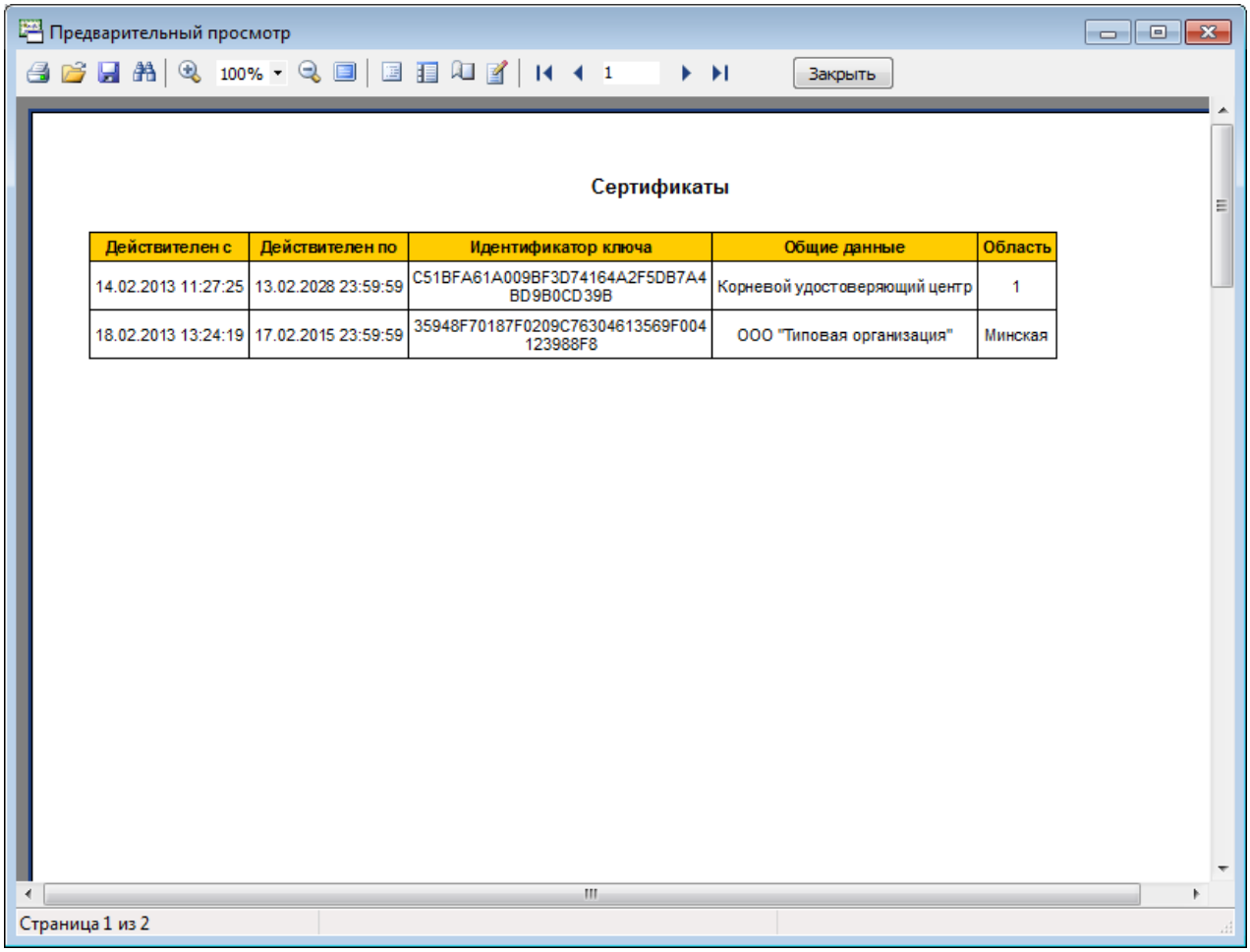


Рисунок 76. Список сертификатов

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

Таблица 1. Элементы, входящие в основное меню.

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).
	Импорт сертификата/СОС	Позволяет установить для использования сертификаты и/или СОС из определенной пользователем папки.
	Открыть запрос на сертификат	Позволяет просмотреть содержимое файла с запросом на сертификат.

Пункт основного меню	Пункт подменю	Пояснение
	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 сертификат	Сформировать и поместить в файл запрос на выпуск 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).

Пункт основного меню	Пункт подменю	Пояснение
	Список ключей на носителе	Позволяет пользователю увидеть список личных ключей на носителе, установленном в считывателе.
	Обновление СОС и сертификатов УЦ	Проверка точек распределения СОС (список СОС берется из конфигурационного файла *CrlDpExt.txt*) на наличие актуальных списков отозванных сертификатов.
	Удаленная регистрация запроса на сертификат	Позволяет произвести удалённую регистрацию запроса на сертификат с помощью сервиса AvSCEP и проимпортировать полученный личный сертификат в хранилище Личные.
	Импорт сертификатов с сервера УЦ	Позволяет проимпортировать личный сертификат, атрибутный сертификат (сертификаты), цепочки сопутствующих сертификатов Удостоверяющих центров, Службы атрибутных сертификатов и СОС, выпущенных УЦ, с сервера УЦ.
	Настройки	Определяет основные настройки работы программы (включает подпункты: Вывод информационных окон и Сроки действия).
	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 ПК AvPCM используются справочники, в которые помещена информация по сертификатам, атрибутным сертификатам, спискам отозванных сертификатов УЦ.

Полный список существующих справочников, следующий:

- Сертификаты;
  - Личные;
  - Доверенных Удостоверяющих центров;
  - Сетевой справочник;
- Списки отозванных сертификатов (СОС);
- Запросы на сертификат;
  - Новые;
  - На удаленной обработке;
  - Обработанные;
  - Отклоненные;
- Атрибутные сертификаты.

Внимание: Сертификаты, атрибутные сертификаты, запросы на сертификат и СОС можно удалить из любого справочника, если не используется хранилище сертификатов в сетевой БД.

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 надо вызвать подменю управления таблицей на этом поле и выбрать пункт «Спрятать колонку». Для вывода невидимого поля нужно 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 надо 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 (COC), выпущенный указанным выше УЦ и являющийся действительным (проверяется, что текущая дата входит в период действия COC), проверяется корректность подписи УЦ под ним;
- проверяется, не указан ли номер сертификата пользователя в списке найденного и проверенного COC.

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) авторизоваться в менеджере личным сертификатом;
2) найти в Сетевом справочнике сертификатов сертификат того УЦ, который мы хотим поместить в справочник «Доверенных Удостоверяющих центров»;
3) подвести курсор к этому сертификату, и, нажав правую клавишу мыши вызвать всплывающее меню, в котором выбираем пункт «Поместить сертификат в справочник доверенных УЦ»;
4) появится окно, в котором надо ввести серийный номер помещаемого в список доверия сертификата УЦ (см. Рисунок 77. Информация о сертификате, помещаемом в список Доверенных УЦ);

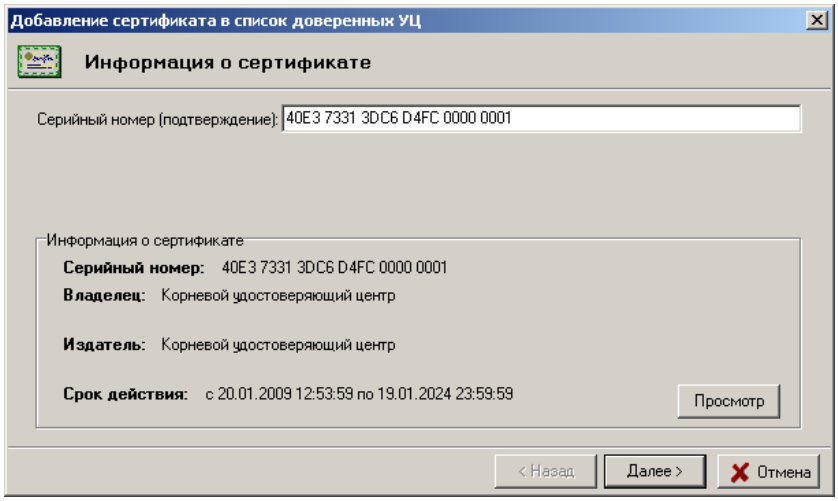


Рисунок 77. Информация о сертификате, помещаемом в список Доверенных УЦ

5) в следующем окне отражается уже существующий список доверяемых Удостоверяющих центров, в который будет помещен сертификат УЦ. Здесь надо только нажать кнопку «Далее» (см. Рисунок 78. Список доверяемых Центров сертификации);

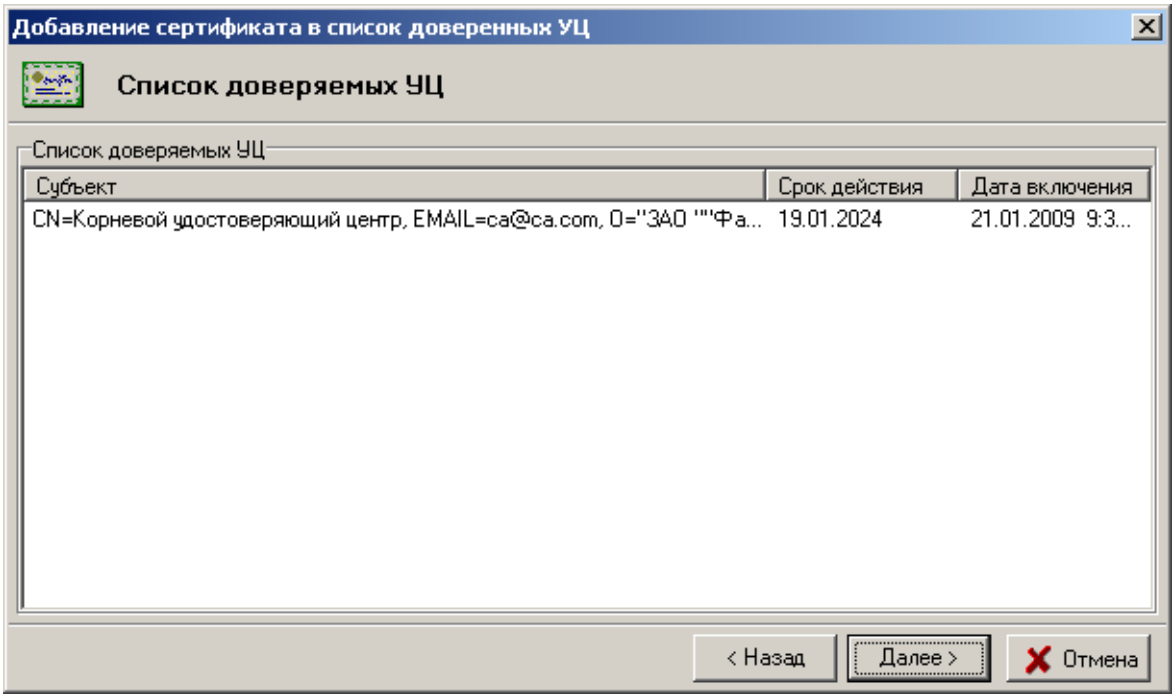


Рисунок 78. Список доверяемых Центров сертификации

6) затем надо вставить носитель личного ключа в считыватель и в появившемся окне ввести пароль доступа к контейнеру с личным ключом пользователя (см. Рисунок 79. Издание списка Доверенных Центров сертификации);

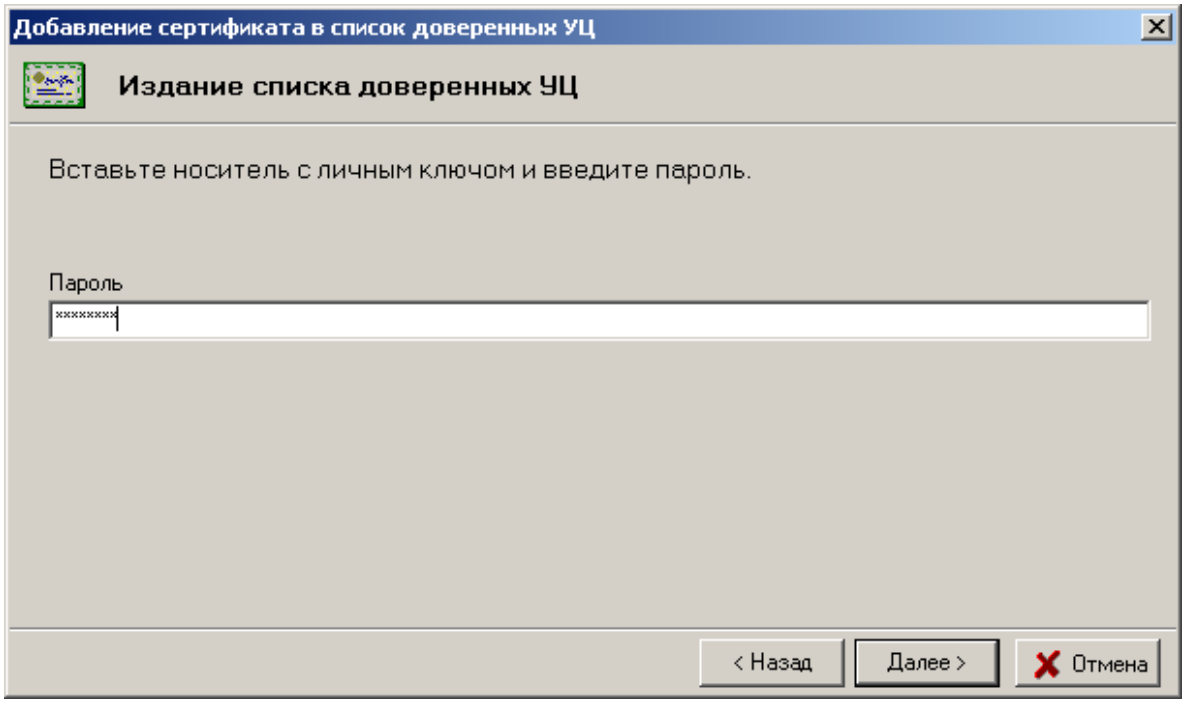


Рисунок 79. Издание списка Доверенных Центров сертификации

7) в последнем окне программа сообщит о том, что Список доверенных Удостоверяющих центров издан и помещен в сетевой справочник (см. Рисунок 80. Завершение работы мастера «Добавление сертификатов в список доверенных УЦ»), нажать кнопку «Закрыть».

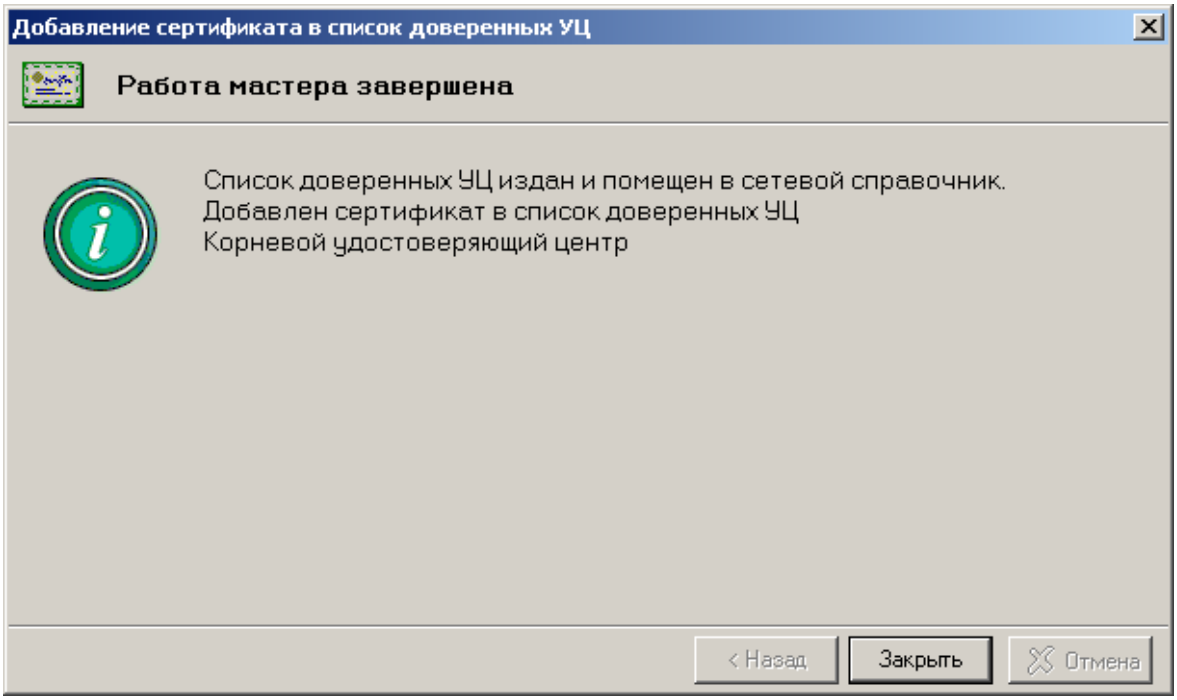


Рисунок 80. Завершение работы мастера «Добавление сертификатов в список доверенных УЦ»

Для ПК AvPCM с базой данных сертификатов в хранилище Windows для помещения сертификата в справочник «Доверенных Удостоверяющих центров» заходить в менеджер с авторизацией необязательно, процедура «Добавления сертификата в список доверенных УЦ» из Сетевого справочника выглядит 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) после этого будет выведено предупреждение операционной системы Windows о добавлении сертификата Корневого Удостоверяющего центра в корневое хранилище, в этом сообщении указаны атрибуты помещаемого сертификата. Если они соответствуют данным вашего Корневого УЦ, то нужно нажать «Да» (см. Рисунок 81. Предупреждение системы безопасности).

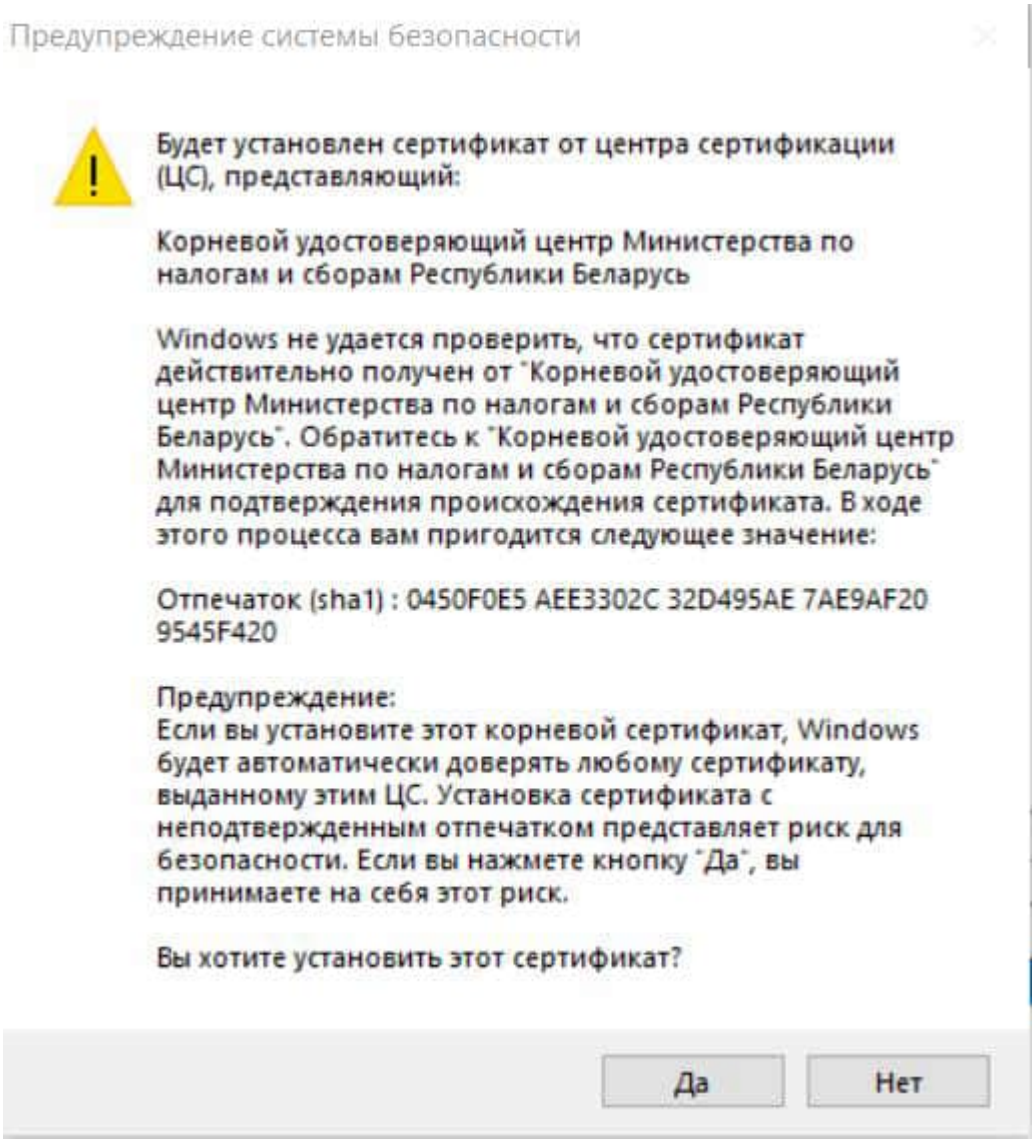


Рисунок 81. Предупреждение системы безопасности

4) после нажатия кнопки «Да» сертификат будет помещен в «Справочник Доверенных Удостоверяющих центров».

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, надо удалить данный сертификат из справочника «Доверенных Удостоверяющих центров».

Действия при исключении сертификата УЦ из списка Доверенных УЦ:

1) авторизоваться в менеджере личным сертификатом;
2) в справочнике «Доверенных УЦ» нужно стать курсором на нужный сертификат;
3) щелкнуть по нему правой клавишей мыши и во всплывающем меню выбрать пункт «Исключить сертификат из справочника доверенных УЦ»;
4) в появившемся окне надо указать серийный номер и нажать кнопку «Далее» (см. Рисунок 82. Исключение сертификата из списка Доверенных УЦ).

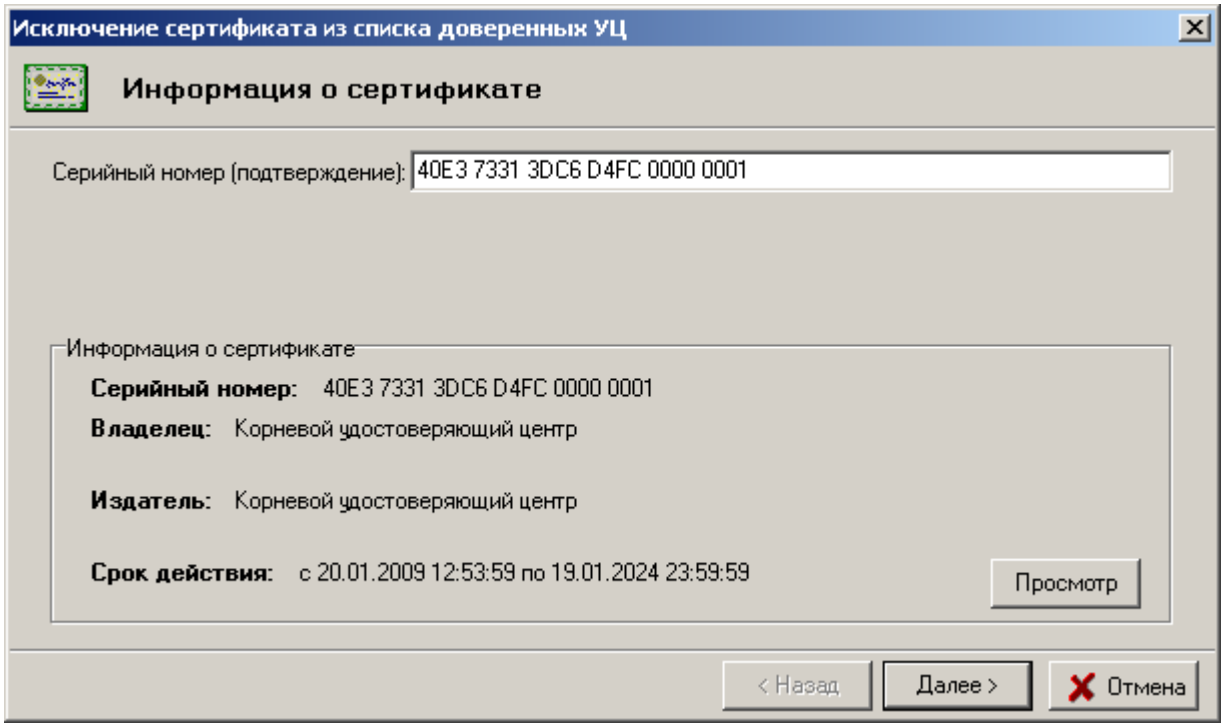


Рисунок 82. Исключение сертификата из списка Доверенных УЦ

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

Для ПК AvPCM с базой данных сертификатов в хранилище Windows для исключения сертификата из справочника «Доверенных Удостоверяющих центров» заходить в менеджер с авторизацией необязательно, процедура «Исключение сертификата из списка доверенных УЦ» выглядит следующим образом:

1) в справочнике «Доверенных УЦ» нужно 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) после этого будет выведено предупреждение операционной системы Windows об удалении сертификата Корневого Удостоверяющего центра из корневого хранилища, в этом сообщении указаны атрибуты удаляемого сертификата. Если они соответствуют данным сертификата Корневого УЦ, который нужно исключить из Корневого хранилища, то нужно нажать «Да» (см. Рисунок 83. Предупреждение системы безопасности).

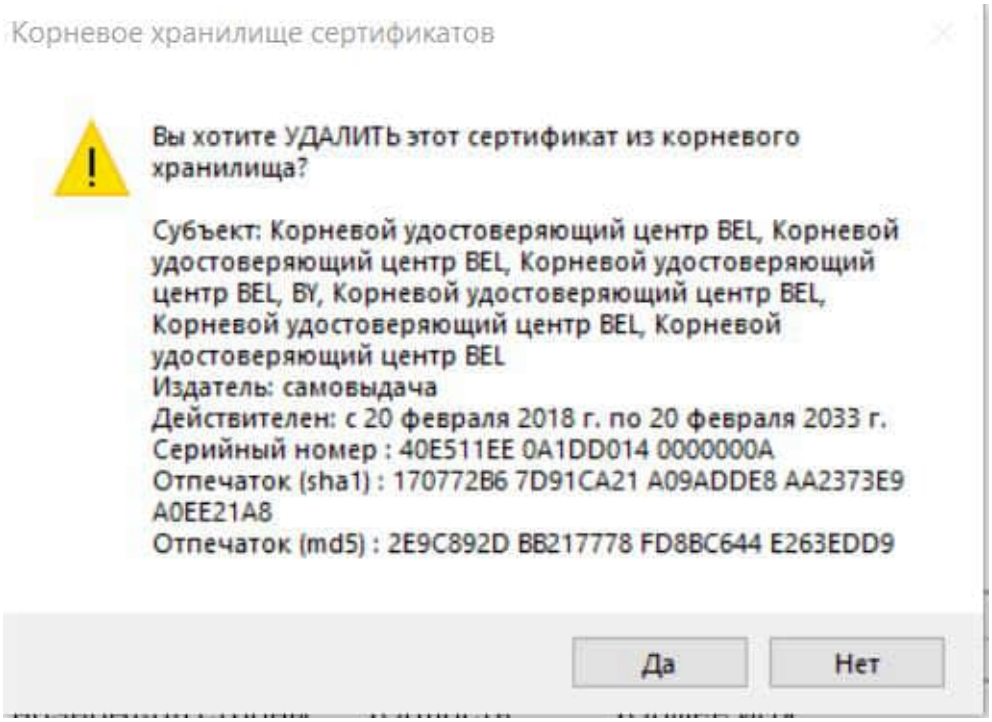


Рисунок 83. Предупреждение системы безопасности

4) после нажатия кнопки «Да» сертификат будет исключен из «Справочника Доверенных Удостоверяющих центров».

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.

6.7.6. Справочник «Запросы на сертификат»

В этом справочнике хранятся все запросы абонентов на выдачу сертификата. Справочник пополняется при создании абонентом очередного запроса на сертификат.

Справочник состоит из четырех разделов:

- *«Новые»* – содержит запросы на выдачу сертификат, на основании которых еще не были изданы сертификаты пользователей;
- *«На удаленной обработке»* – содержит запросы, которые были переданы на обработку в ЦР посредством сервиса SCEP, и на которые еще не были выпущены сертификаты;
- *«Обработанные»* – содержит запросы, на основании которых были изданы сертификаты пользователей и помещены в хранилище менеджера сертификатов;
- *«Отклоненные»* – содержит запросы на сертификат, по которым администратором УЦ было решено не выдавать сертификат.

6.7.7. Справочник «Атрибутные сертификаты»

В справочник «Атрибутные сертификаты» входят все атрибутные сертификаты абонентов, хранящиеся в хранилище данного менеджера сертификатов.

6.8. Просмотр и печать содержимого сертификата/СОС/запроса/атрибутного сертификата

6.8.1. 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, надо 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 (или нажать по сертификату правой клавишей мыши и выбрать «Просмотр»). При этом появится окно просмотра содержимого выбранного сертификата (см. Рисунок 84. Просмотр сертификата).

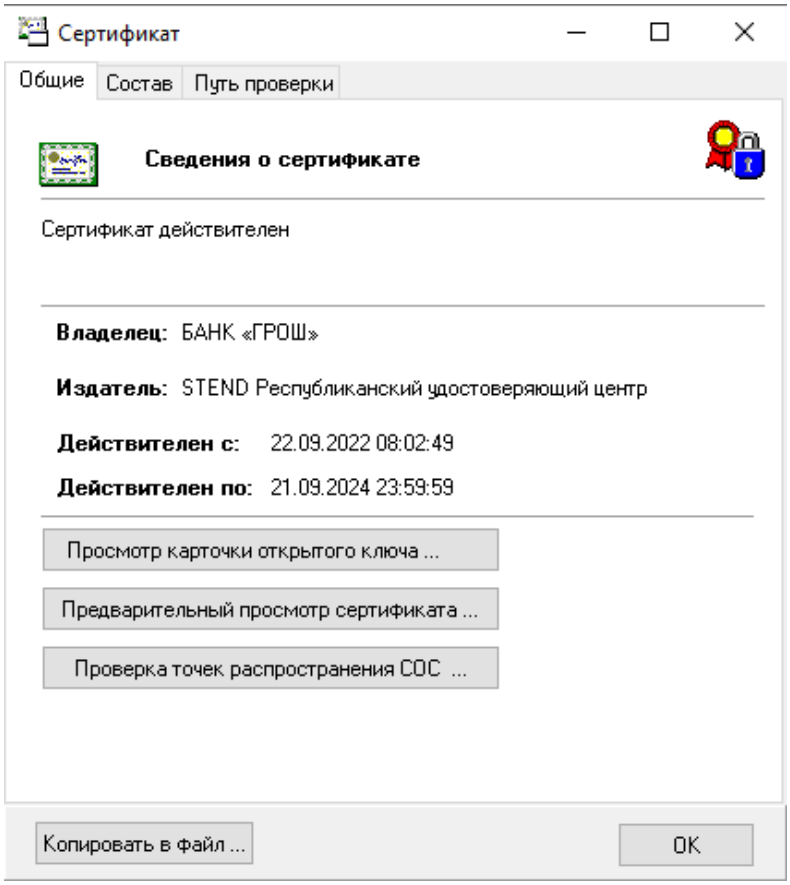


Рисунок 84. Просмотр сертификата

Данное окно состоит из трех закладок:

- «Общие» - сведения о сертификате,
- «Состав» - содержимое сертификата,
- «Путь проверки» - показана вся цепочка сертификатов, удостоверяющих данный сертификат, вплоть до сертификата корневого УЦ;

и трех дополнительных кнопок:

- «Просмотр карточки открытого ключа…»,
- «Предварительный просмотр сертификата…»,
- «Проверка точек распространения COC…».

Закладка *«Общие»*

Описание общих свойств 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.

Кнопка «Проверка точек распространения СОС…» будет активна, если точки распространения СОС (т.е. URL адрес, где хранится файл СОС УЦ) присутствуют в сертификате. Нажав на нее можно скачать и проимпортировать СОС с данного адреса (см. п. 6.14.2 Обновление СОС с использованием кнопки «Проверка точек распространения СОС» в сертификате (атрибутном сертификате)).

Закладка *«Состав»*

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 пункта «Серийный номер» внизу будет отображено значение серийного номера сертификата (см. Рисунок 85. Состав сертификата).

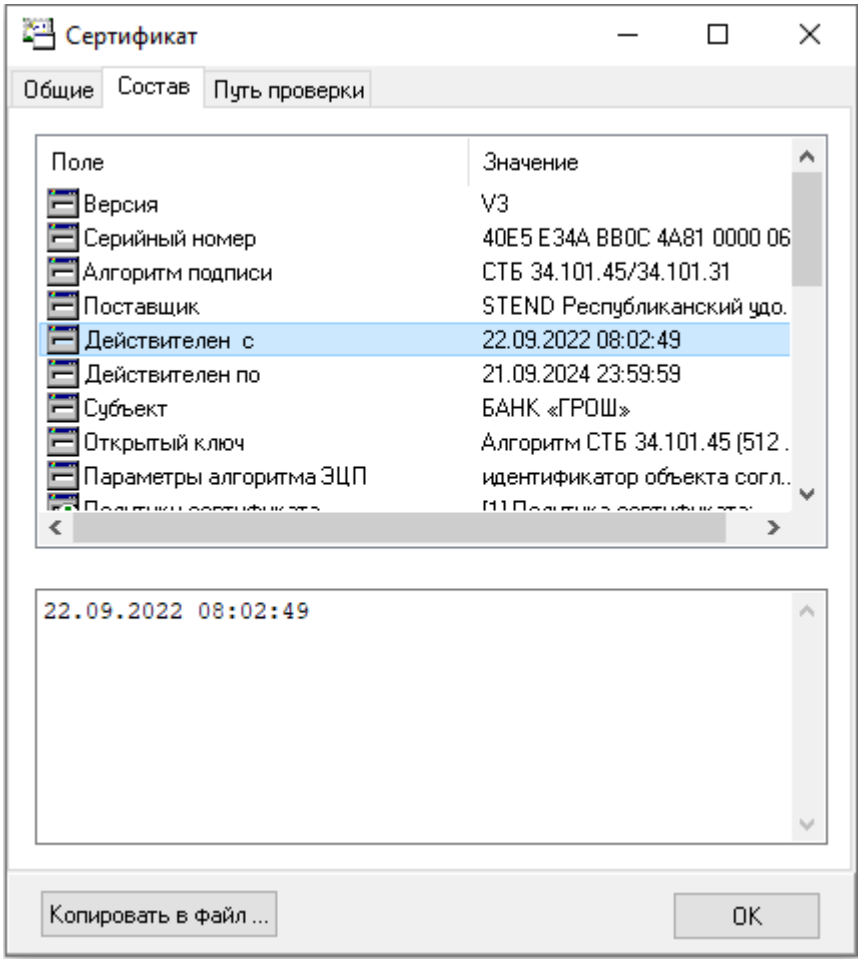


Рисунок 85. Состав сертификата

Закладка *«Путь проверки»*

В данной панели можно увидеть, каким сертификатом УЦ был выдан данный сертификат, и в каком списке отозванных сертификатов он был проверен (см. Рисунок 86. Путь проверки).

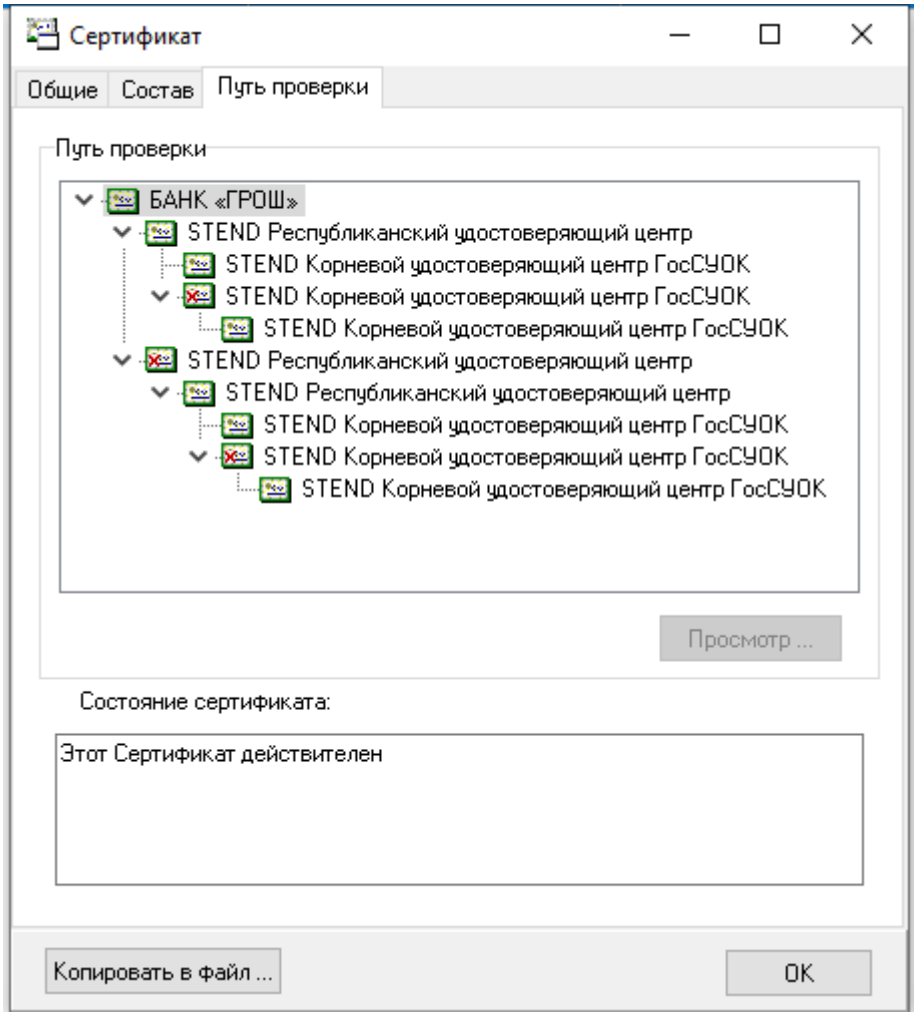


Рисунок 86. Путь проверки

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.

6.8.2. 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, нужно 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»,
- «Список отзыва»,
- «Путь проверки» (см. Рисунок 87. Окно «Список отозванных сертификатов»).

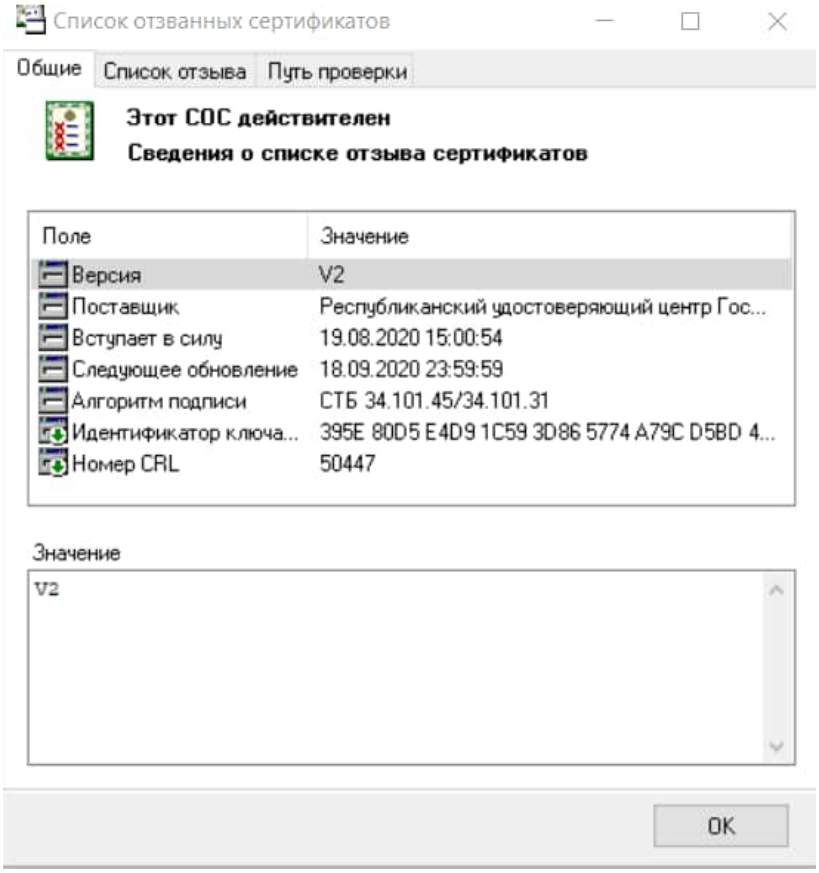


Рисунок 87. Окно «Список отозванных сертификатов»

Закладка «*Общие*»

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.

Закладка «*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.

Закладка «*Путь проверки*»

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

6.8.3. 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», нужно 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 пяти закладок:

- «Общие»,
- «Состав»,
- «Значение ключа»,
- «Удостоверяющие подписи,
- Сертификат;

и двух дополнительных кнопок:

- «Просмотр карточки открытого ключа»,
- «Предварительный просмотр» (см. Рисунок 88. Окно «Запрос на сертификат»).

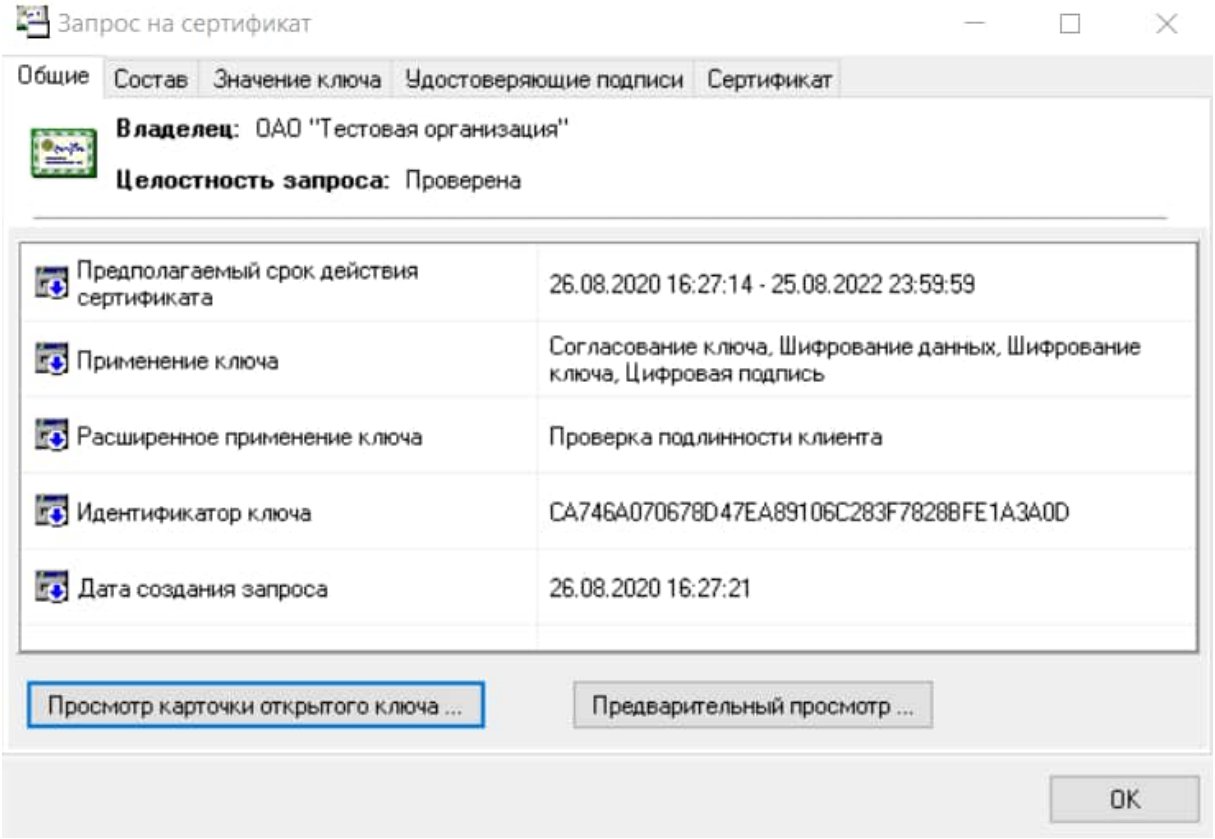


Рисунок 88. Окно «Запрос на сертификат»

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

«Владелец» –имя будущего владельца сертификата;

- «Целостность запроса» – результаты проверки ЭЦП, выработанной под запросом на сертификат;

«Предполагаемый срок действия сертификата» – необязательный параметр, включается в состав запроса, если нужно сузить срок действия сертификата, задаваемый в УЦ по умолчанию;

- «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-значение от значения открытого ключа;
- «Дата создания запроса» - дата и время создания запроса 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.

Закладка *«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.

Закладка *«Значение ключа».*

В данной панели можно увидеть значение открытого ключа проверки подписи.

Закладка *«Удостоверяющие подписи».*

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

Закладка *«Сертификат».*

Данная панель появляется, если по запросу был выпущен сертификат и проимпортирован в менеджер. Просмотреть сведения о сертификате можно, нажав кнопку «Просмотр сертификата».

6.8.4. Просмотр запроса на сертификат, созданного в соответствии с требованиями СТБ 34.101.78-2019

СТБ 34.101.78-2019 определяет новый формат и структуру запроса на получение сертификата. Пример такого запроса представлен ниже (см. Рисунок 89. Окно «Запрос на сертификат» в соответствии с СТБ 34.101.78-2019).

Данное окно состоит из пяти закладок:

- «Общие»,
- «Состав»,
- «Значение ключа»,
- «Удостоверяющие подписи,
- Сертификат;

и двух дополнительных кнопок:

- «Просмотр карточки открытого ключа»,
- «Предварительный просмотр».

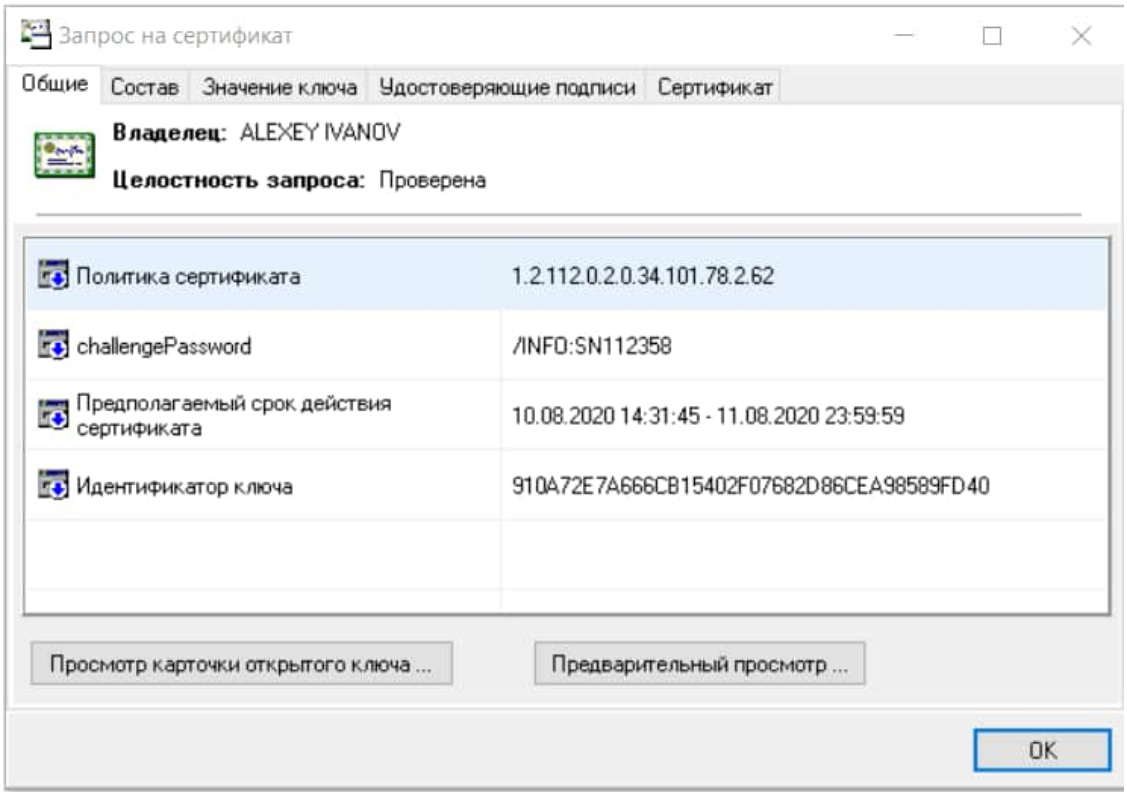


Рисунок 89. Окно «Запрос на сертификат» в соответствии с СТБ 34.101.78-2019

Закладка *«Общие»* (см. Рисунок 89. Окно «Запрос на сертификат» в соответствии с СТБ 34.101.78-2019) содержит общие параметры запроса на сертификат:

«Владелец» – показывает имя будущего владельца сертификата.

- «Целостность запроса» – результаты проверки ЭЦП, выработанной под запросом на сертификат.

«Политика сертификата» - описывает политику, в соответствии с которой был выпущен сертификат, и цели, в которых сертификат может использоваться.

«challengePassword» - информационная строка, которую требуется передать в УЦ, например, в данном случае это реквизиты платежных документов об оплате услуг.

«Предполагаемый срок действия сертификата» – необязательный параметр, включается в состав запроса, если нужно сузить срок действия сертификата, задаваемый в УЦ по умолчанию.

«Идентификатор ключа» – хэш-значение от значения открытого ключа.

С помощью кнопки «Просмотр карточки открытого ключа…» можно просмотреть и распечатать карточку открытого ключа данного запроса на сертификат из дополнительно раскрывшегося окна. При этом следует иметь в виду, что СТБ 34.101.78-2019 не предусматривает использование карточки открытого ключа.

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

Закладка *«Состав»* (см. Рисунок 90. Закладка «Состав» в запросе на сертификат в соответствии с СТБ 34.101.78-2019).

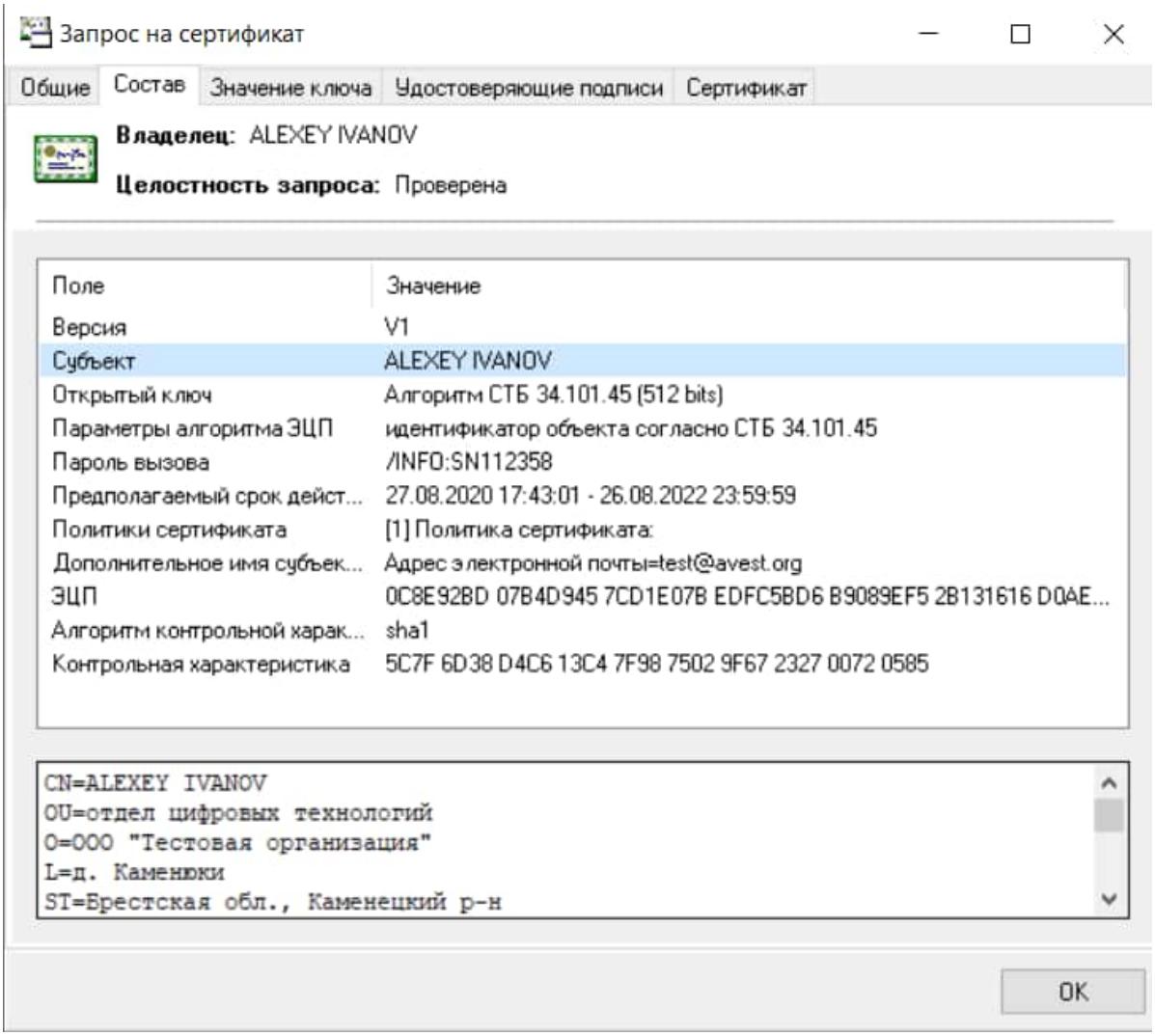


Рисунок 90. Закладка «Состав» в запросе на сертификат в соответствии с СТБ 34.101.78-2019

В данной панели можно увидеть точный состав запроса на сертификат, в том числе его открытый ключ, параметры алгоритма ЭЦП, политики сертификата, пароль вызова, дополнительное имя субъекта и т.д. При выборе одного из полей запроса внизу панели будет отображена информация о его составе.

Закладка *«Значение ключа»*.

В данной панели можно увидеть значение открытого ключа проверки подписи.

Закладка *«Удостоверяющие подписи»*.

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

Закладка *«Сертификат»* (см. Рисунок 91. Закладка «Сертификат» в запросе на сертификат в соответствии с СТБ 34.101.78-2019).

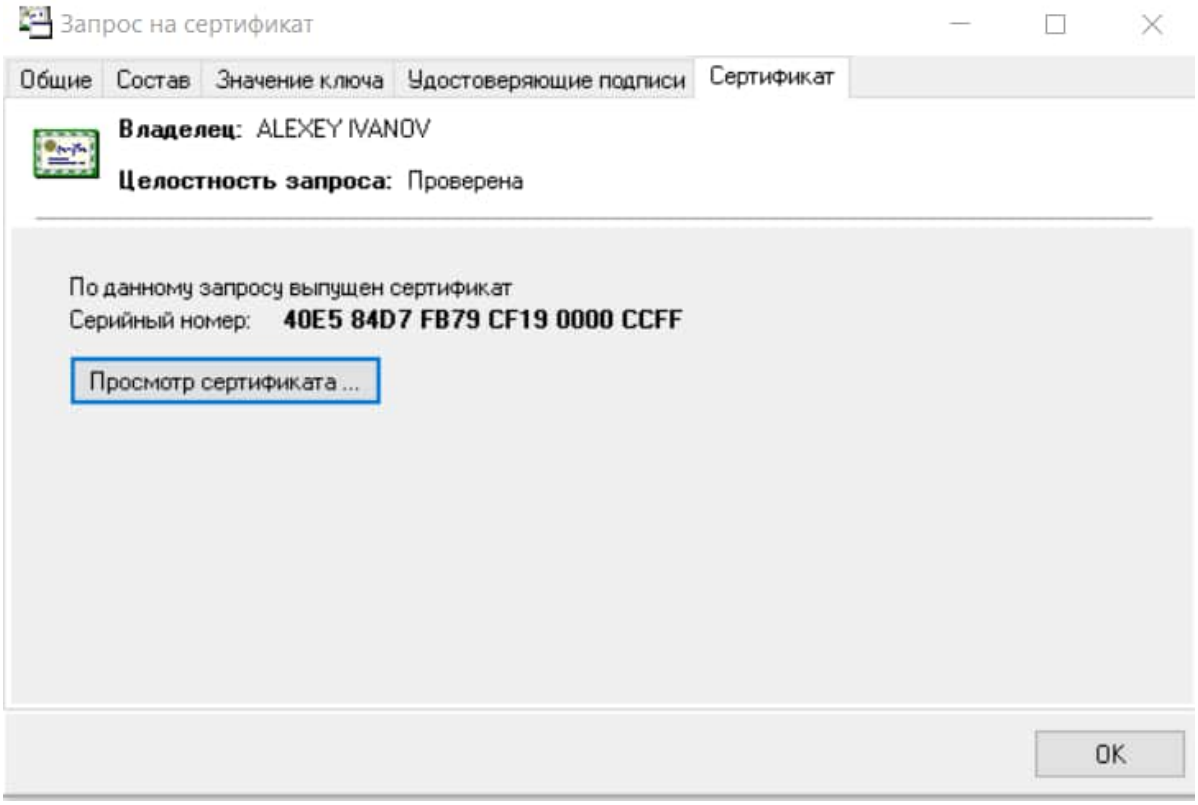


Рисунок 91. Закладка «Сертификат» в запросе на сертификат в соответствии с СТБ 34.101.78-2019

Данная панель отображается, если по запросу был выпущен сертификат и проимпортирован в менеджер. Просмотреть сведения о сертификате можно, нажав кнопку «Просмотр сертификата».

6.8.5. Просмотр и печать содержимого атрибутного сертификата

Пользователь может просматривать содержимое (атрибуты) атрибутного сертификата, как находящегося справочнике, так и при импорте атрибутных сертификатов. Для просмотра содержимого атрибутного сертификата надо выбрать нужный справочник в дереве сертификатов/СОС в левой панели программы, затем с помощью фильтра найти нужный атрибутный сертификат в правой панели окна, и открыть его свойства двойным нажатием левой клавиши мыши по атрибутному сертификату. При этом появится окно просмотра содержимого (см. Рисунок 92. Просмотр атрибутного сертификата).

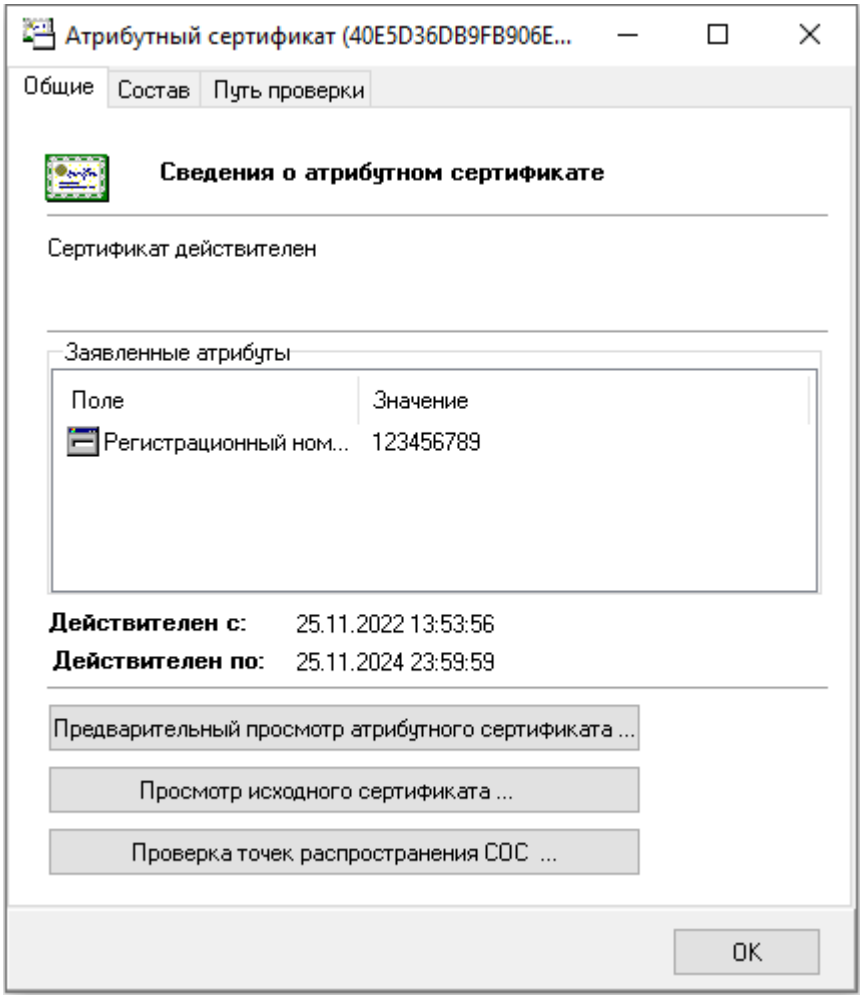


Рисунок 92. Просмотр атрибутного сертификата

Данное окно состоит из трех закладок:

- «Общие» - сведения о атрибутном сертификате,
- «Состав» - содержимое атрибутного сертификата,
- «Путь проверки» - показана вся цепочка сертификатов, удостоверяющих данный сертификат, вплоть до сертификата корневого УЦ;

и трех дополнительных кнопок:

- «Предварительный просмотр атрибутного сертификата…»,
- «Просмотр исходного сертификата…»,
- «Проверка точек распространения COC…».

Закладка *«Общие»*

Данная панель описывает общие свойства атрибутного сертификата:

- «Сертификат действителен» или «Сертификат не действителен» позволяет увидеть текущее состояние сертификата. В том случае, если сертификат не действителен, будет приведена причина его недействительности;
- «Заявленные атрибуты» – атрибуты, включенные в сертификат;
- «Действителен с:», «Действителен по:» – показывают период, в течение которого сертификат действителен.

Нажав на кнопку «Предварительный просмотр атрибутного сертификата» позволяет в дополнительном окне просмотреть и распечатать атрибутный сертификат.

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

Кнопка «Проверка точек распространения СОС…» будет активна, если точки распространения СОС (т.е. URL адрес, где хранится файл СОС УЦ) присутствуют в атрибутном сертификате. Нажав на нее можно скачать и проимпортировать СОС с данного адреса (см. п. 6.14.2 Обновление СОС с использованием кнопки «Проверка точек распространения СОС» в сертификате (атрибутном сертификате)).

Закладка *«Состав»*

В данной панели можно увидеть точный состав сертификата, в том числе его серийный номер, алгоритм подписи, серийных номер исходного сертификата и т.д. При выборе одного из полей сертификата внизу панели будет отображена информация о его составе (см. Рисунок 93. Состав атрибутного сертификата).

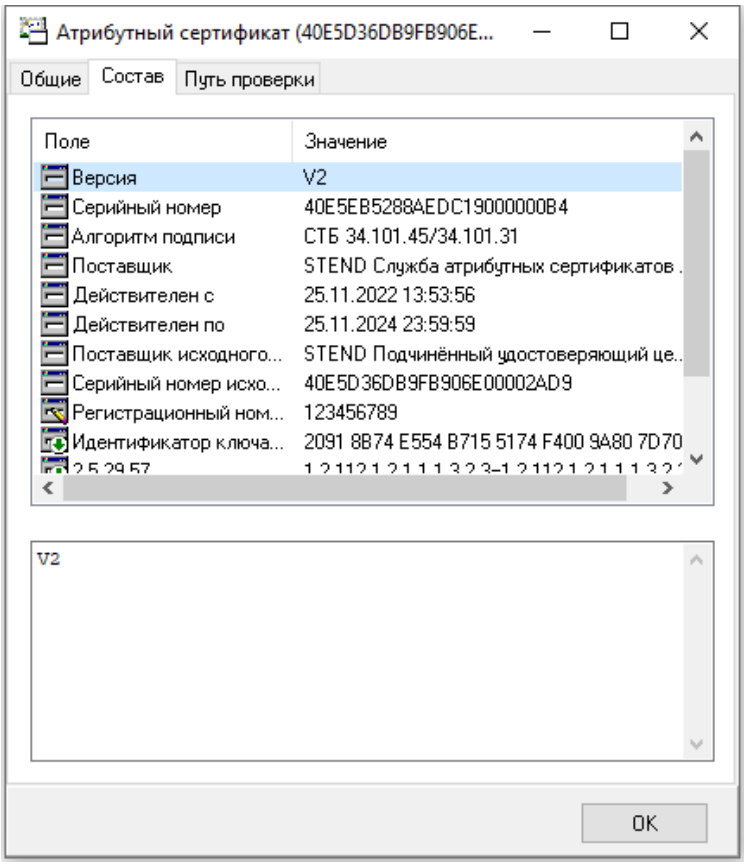


Рисунок 93. Состав атрибутного сертификата

Закладка *«Путь сертификации»*

В данной панели можно увидеть, каким Центром атрибутных сертификатов 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.

С помощью кнопки «Просмотр исходного сертификата…» на закладке «Общие» можно просмотреть сертификат пользователя, для которого был издан данный атрибутный сертификат.

Кнопка «Предварительный просмотр атрибутного сертификата…» на закладке «Общие» позволяет в дополнительном окне просмотреть и распечатать атрибутный сертификат (см. Рисунок 94. Печать атрибутного сертификата).

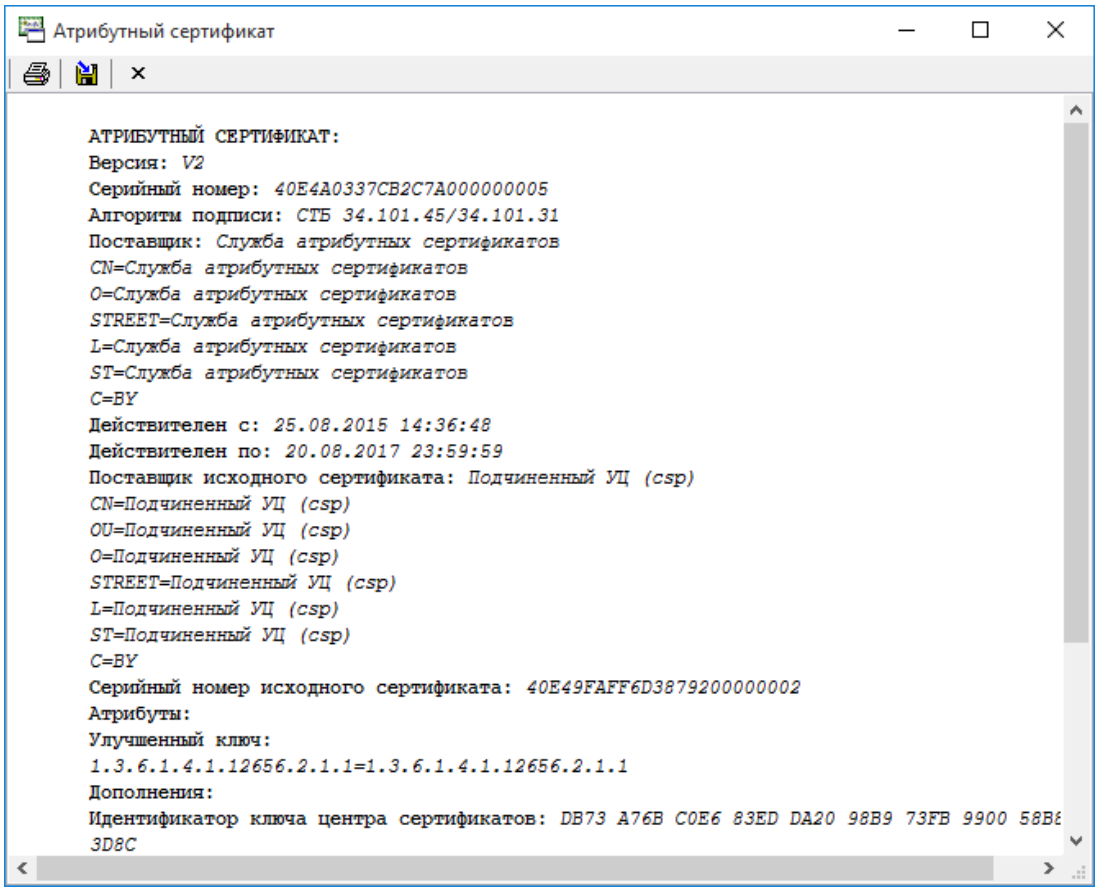


Рисунок 94. Печать атрибутного сертификата

6.9. Экспорт и импорт сертификатов/СОС

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

6.9.1. 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 всплывающем меню выбрать «Экспорт сертификата в файл»;
3) в открывшемся окне указать:
    - место, куда должен быть сохранен файл (Папка:),

- тип файла:
  - сертификат (*.cer) – будет экспортирован только пользовательский сертификат,
  - сертификаты (весь путь) PKCS#7 (*.p7b) – будет экспортирована вся цепочка сертификатов,
  - сертификат (в Base64 кодировке) (*.cer),
  - сертификат (в PEM кодировке) (*.cer),
  - цепочка сертификатов в PEM кодировке (для Open SSL) (*.crt),
  - цепочка сертификатов в PEM кодировке (*.pem),
- имя файла для экспорта сертификата;

4) нажать кнопку «Сохранить» (см. Рисунок 95. Экспорт сертификата в файл).

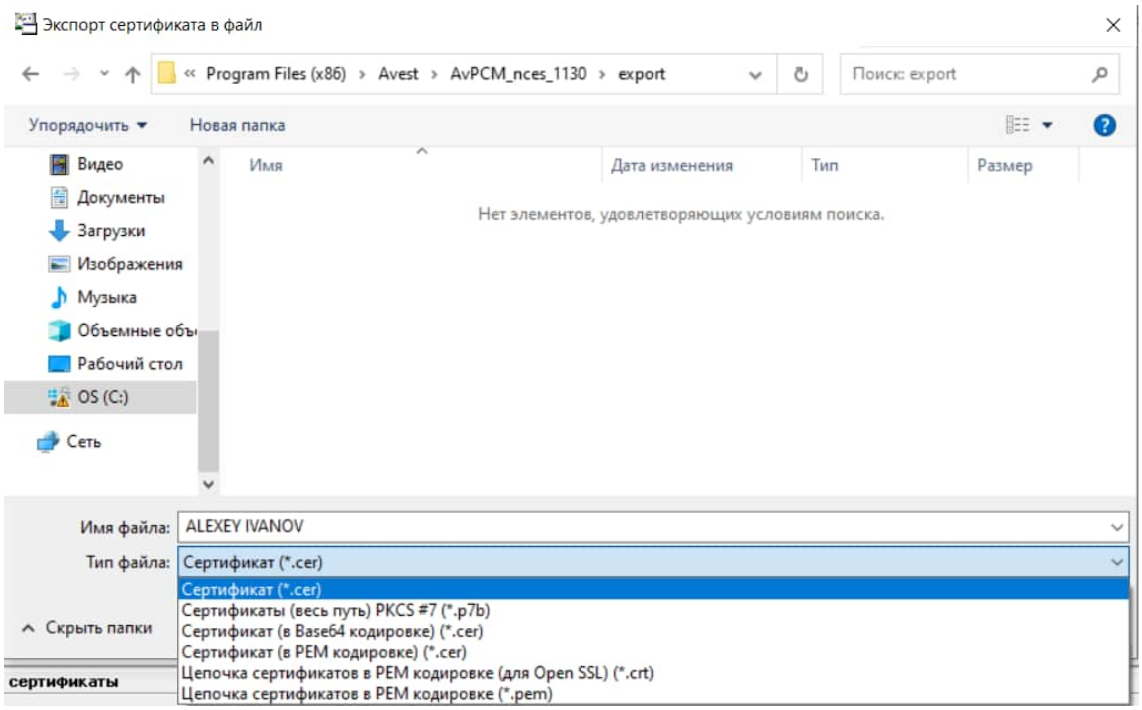


Рисунок 95. Экспорт сертификата в файл

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».

6.9.2. Экспорт СОС

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

6.9.3. 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 (*.p7b),
     - сертификаты (весь путь, включая атрибутные) PKCS#7 (*.p7b),
3) нажать кнопку «Сохранить» (см. Рисунок 96. Экспорт списка сертификатов и СОС).

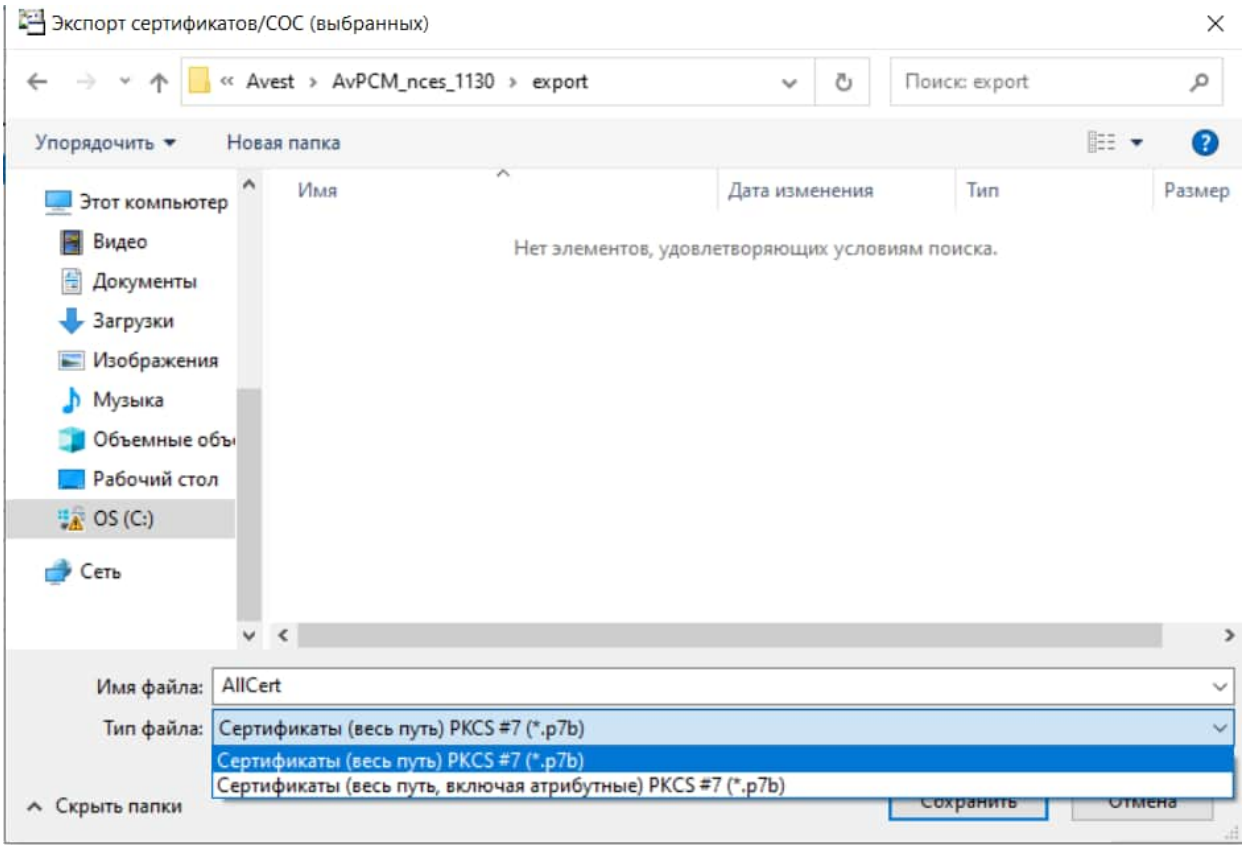


Рисунок 96. Экспорт списка сертификатов и СОС

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

После успешного экспорта списка сертификатов программа выдаст окно сообщения, в котором будет прописан путь к файлу и его содержимое (см. Рисунок 97. Информация об окончании экспорта списка сертификатов).

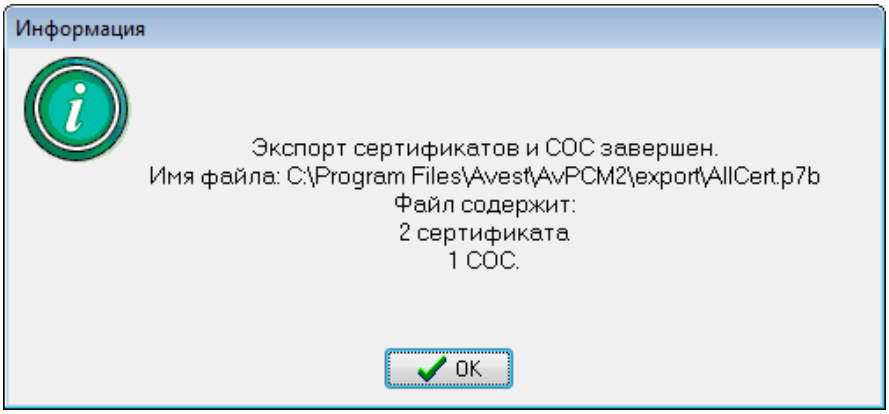


Рисунок 97. Информация об окончании экспорта списка сертификатов

6.9.4. Экспорт атрибутного сертификата

Для экспорта одного атрибутного сертификата нужно выполнить:

1) выбрать нужный атрибутный сертификат в справочнике;
2) выбрать в основном меню пункт «Файл» – «Экспорт атрибутного сертификата в файл» или щелкнуть правой клавишей мыши по сертификату и в контекстном меню выбрать «Экспорт атрибутного сертификата в файл»;
3) можно экспортировать, как только атрибутный сертификат (в формате **.acr*), так и всю цепочку сертификатов (в формате **.p7b*). Следует учесть, что при экспорте атрибутного сертификата в формате **.acr* полученный файл не открывается стандартными средствами Windows.

В открывшемся окне указать: место, куда должен быть сохранен файл (Папка:), имя файла для экспорта сертификата, – и нажать кнопку «Сохранить» (см. Рисунок 98. Экспорт атрибутного сертификата в файл).

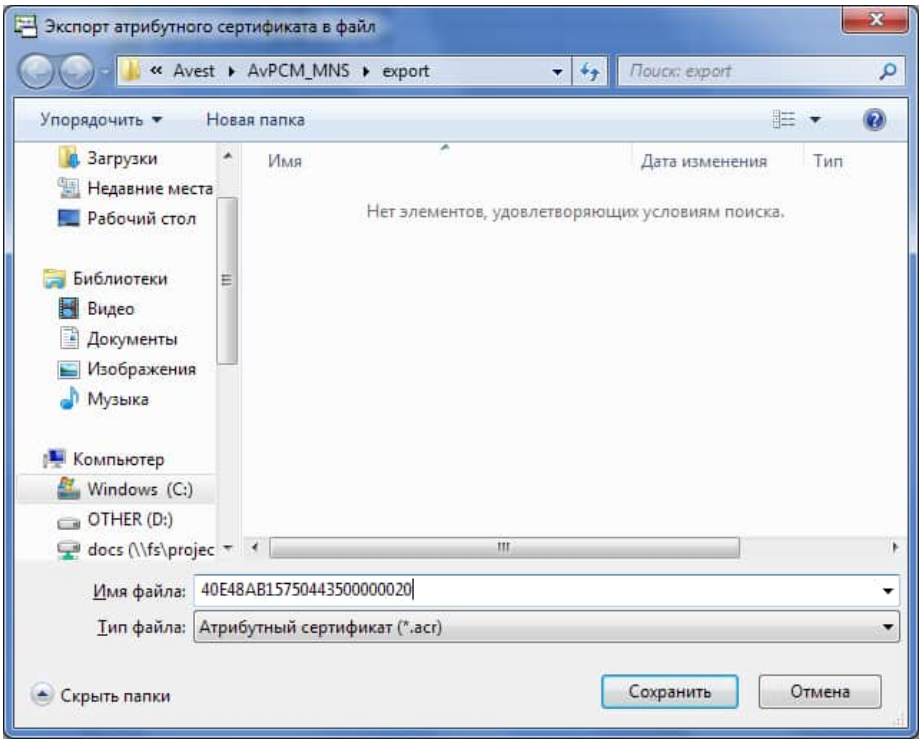


Рисунок 98. Экспорт атрибутного сертификата в файл

6.9.5. Импорт сертификатов (СОС)

Для выполнения импорта сертификатов (СОС) 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 действиям в п. 6.5.2 Импорт личного сертификата при инсталляции с файловой базой данных.

6.9.6. Импорт атрибутных сертификатов

Для выполнения импорта атрибутных 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». В окне «Выбор файла» в разделе *Тип файла:* следует выбрать пункт *Объекты сертификации (*.p7b;*.cer;*.crl;*.crt;*.acr)* либо *Атрибутный сертификат (*.acr)* и, далее, выбрать файл атрибутного сертификата, импорт которого нужно произвести.

После импорта атрибутный сертификат будет отображаться в нижней части главного окна после выбора соответствующего исходного сертификата в верхней части окна (см. Рисунок 99. Отображение атрибутного сертификата).

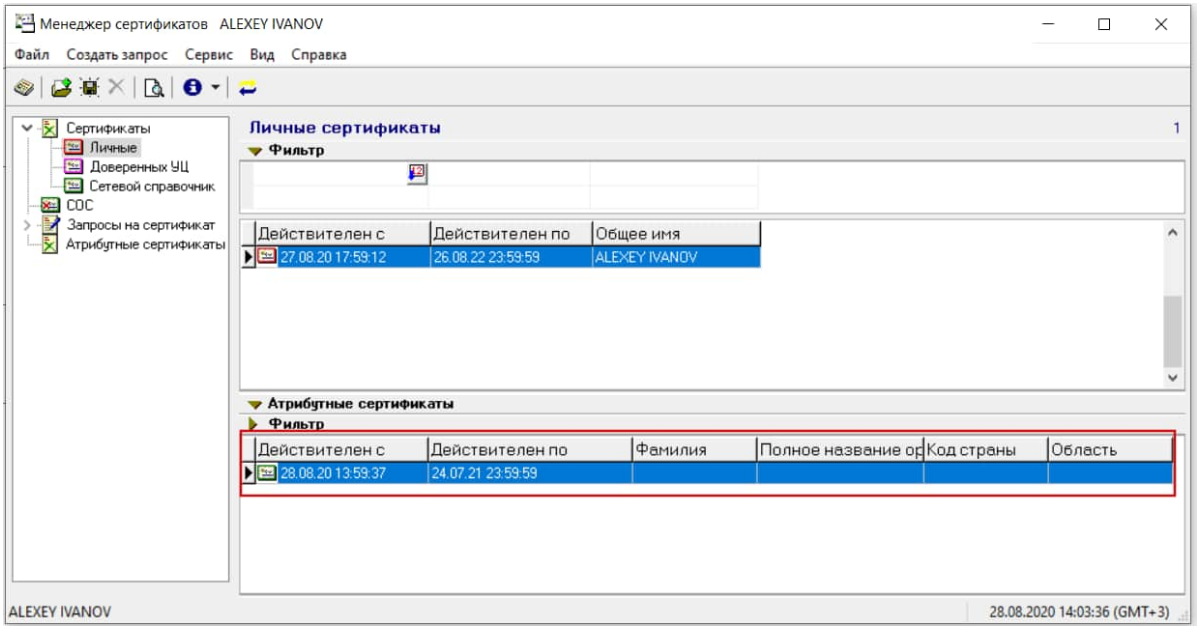


Рисунок 99. Отображение атрибутного сертификата

6.10. Управление контейнерами личных ключей на носителе

ВНИМАНИЕ. Если изменить имя контейнера средствами криптопровайдера Avest CSP, ПК AvPCM и сторонние программные комплексы, использующие менеджер для выполнения

криптографических операций, не смогут использовать данный контейнер. В данном случае нужно удалить сертификат и повторно произвести импорт личного сертификата пользователя.

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 100. Список ключей на носителе).

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 нужно выполнить по окончании срока действия личного ключа и при отзыве сертификата.

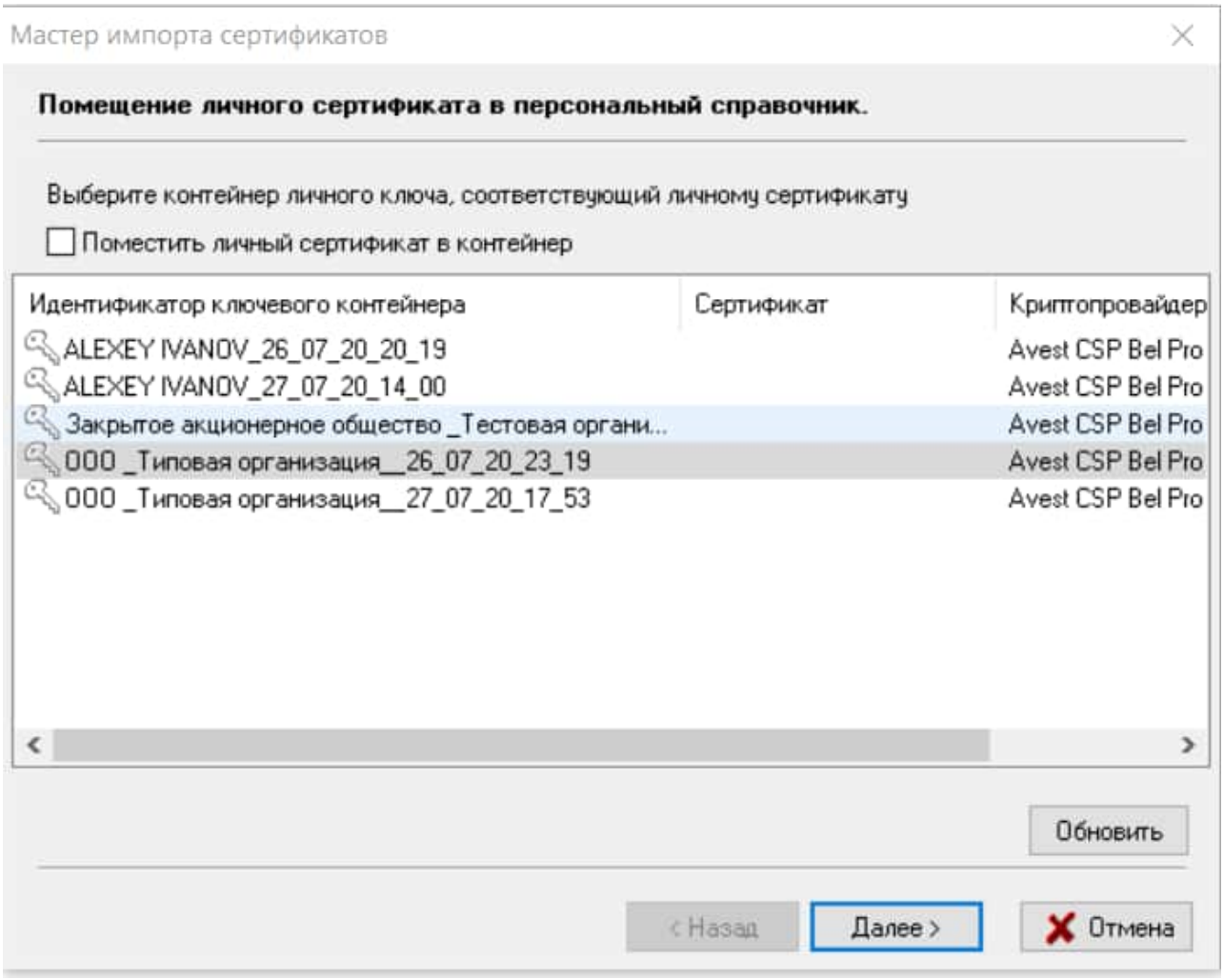


Рисунок 100. Список ключей на носителе

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.

6.11. Журнал работы

В процессе работы программы ведется журнал работы. Для просмотра журнального файла нужно 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

№	Поле	Данные	Примечание
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 нужно 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 101. Настройка журнала работы (контроль файла по размеру)):
  - *Имя файла журнала* – выбор папки 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.

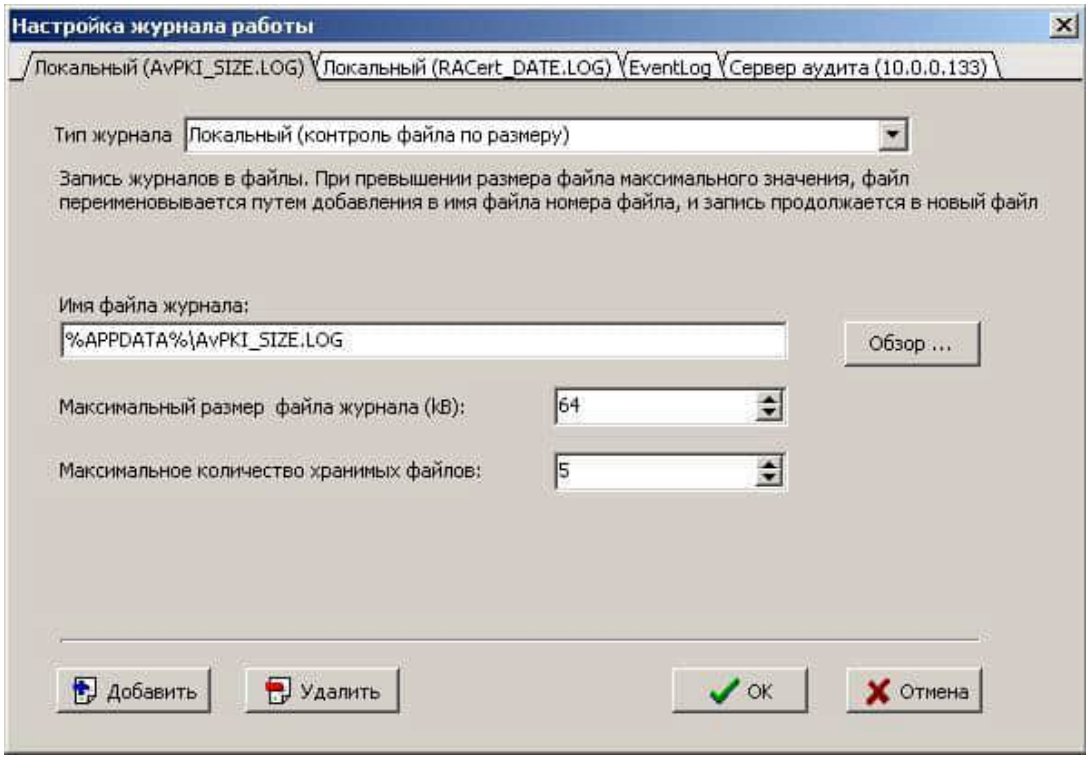


Рисунок 101. Настройка журнала работы (контроль файла по размеру)

- 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 102. Настройка журнала работы (контроль файла по дате)):

– *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.

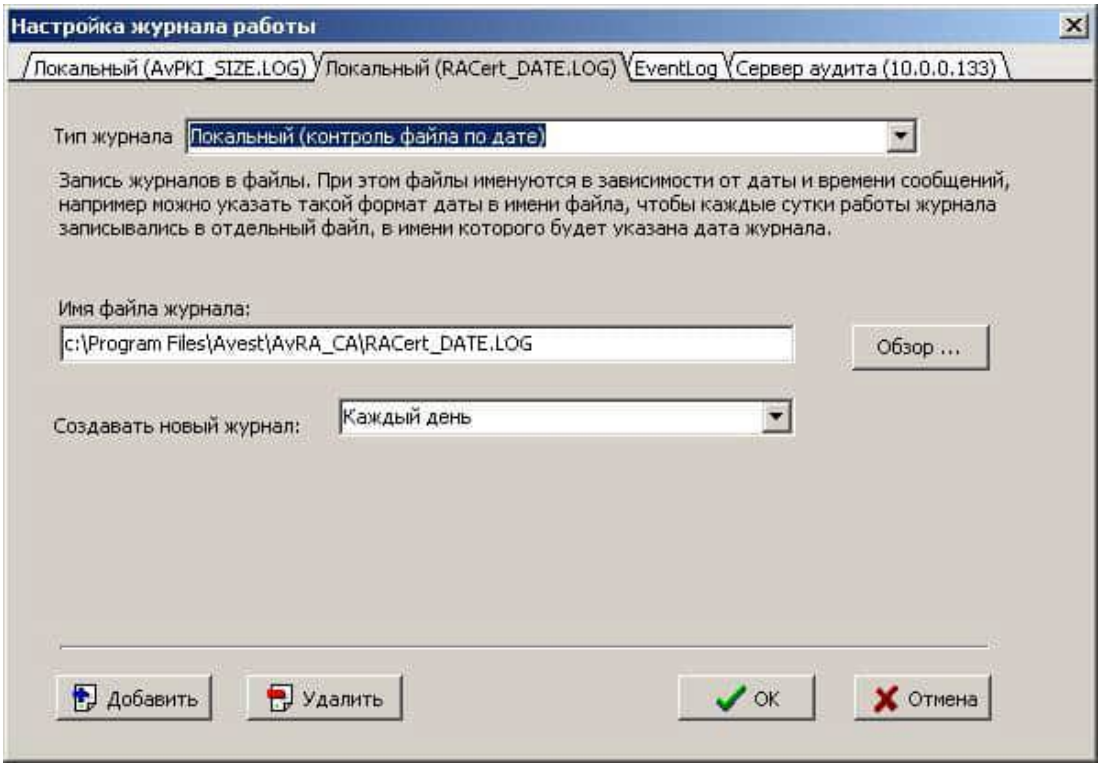


Рисунок 102. Настройка журнала работы (контроль файла по дате)

- 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 103. Настройка журнала работы (сервер журналов аудита)):

  – *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.

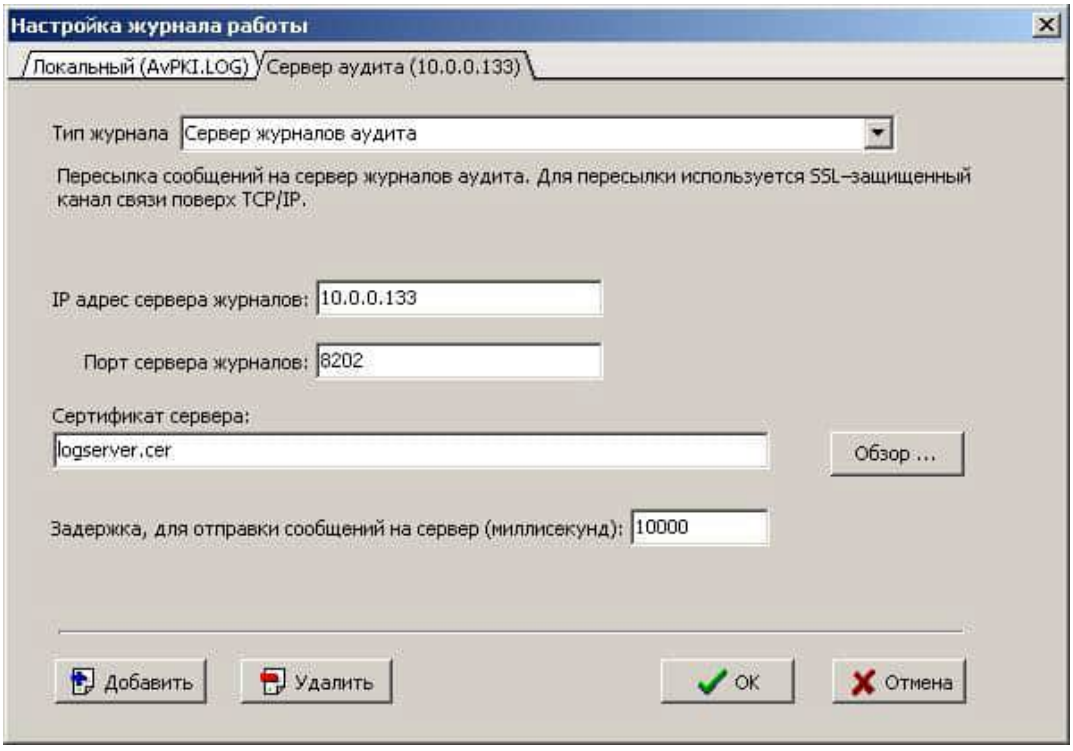


Рисунок 103. Настройка журнала работы (сервер журналов аудита)

- 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 104. Настройка журнала работы (журнал удаленного сервера)):

  – *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.

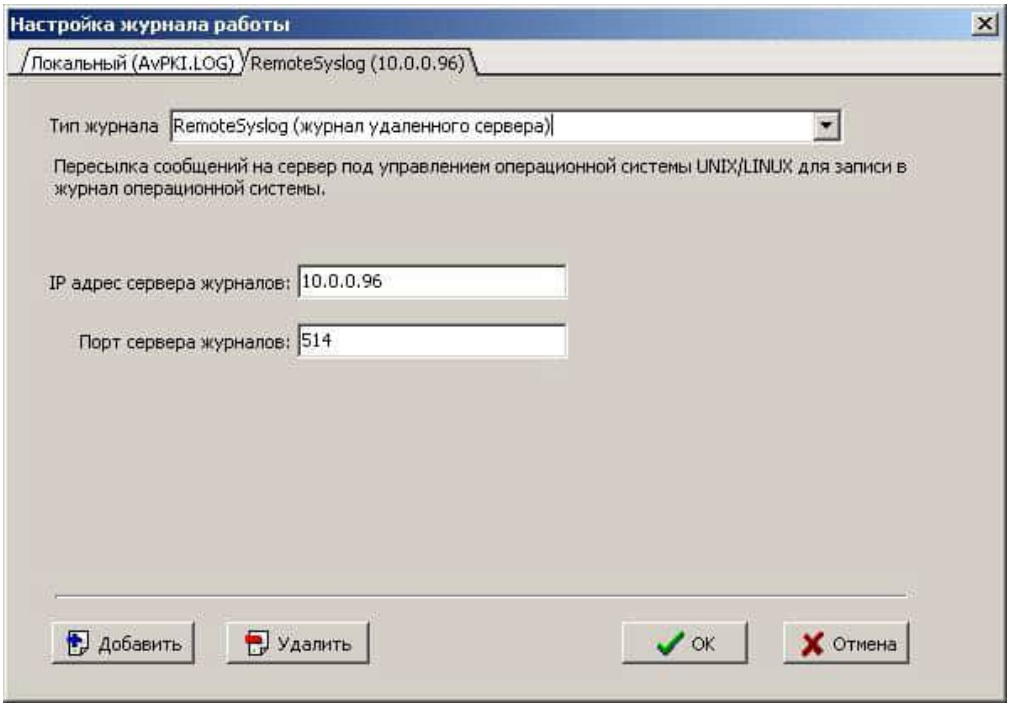


Рисунок 104. Настройка журнала работы (журнал удаленного сервера)

- Eventlog (журнал операционной системы). При данном типе журнала происходит запись в журнал операционной системы Windows (см. Рисунок 105. Запись в журнал операционной системы).

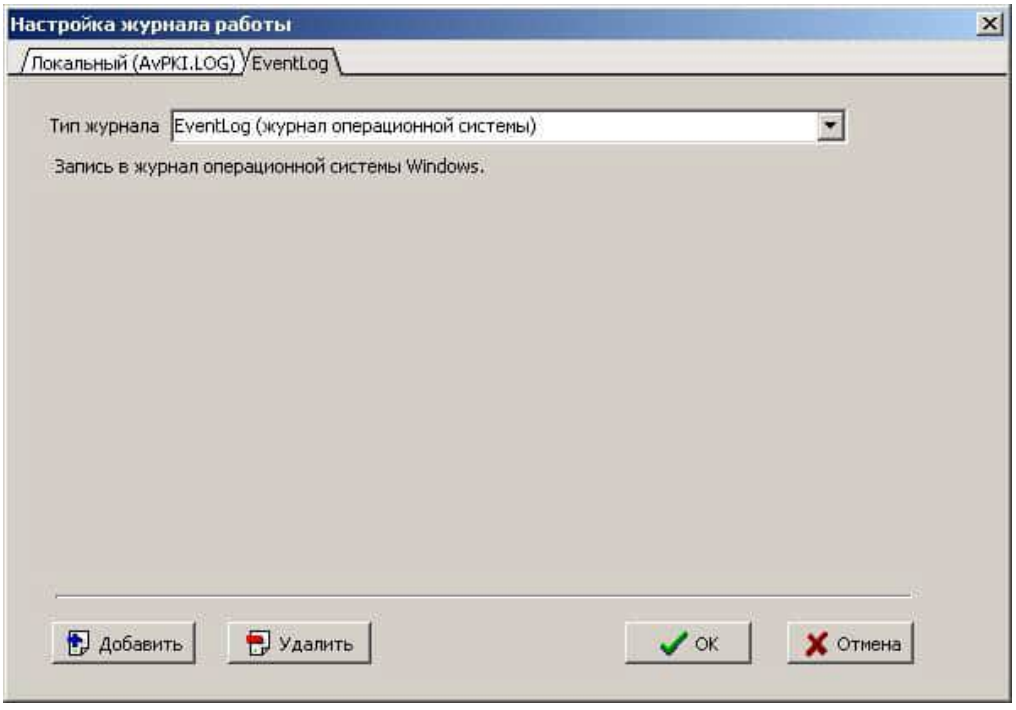


Рисунок 105. Запись в журнал операционной системы

6.12. Включение отладочного лога

Для того, чтобы включить отладочный лог **AvCmDebug.log,** нужно открыть файл **AvCmMsg.ini (**находится в папке с установленным менеджером) 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.

6.13. Отправка запроса и получение сертификата через сервис SCEP

Существует возможность отправки запроса на сертификат в ЦР (УЦ) с использованием сервиса SCEP (простой протокол регистрации сертификата). Однако следует помнить, что сервис SCEP лишь помещает запросы пользователей в базу данных УЦ или ЦР в зависимости от того, какой из компонентов системы проводит первичную идентификацию абонентов в системе.

Сервис AvSCEP не предназначен для автоматической выдачи сертификатов, он – удобное средство для оперативной доставки запросов от пользователя в органы регистрации запросов.

6.13.1. Настройка ПК AvPCM для взаимодействия с сервисом SCEP

Для того, чтобы ПК AvPCM мог взаимодействовать с сервисом SCEP, в файл *AvCmMsg.ini*, который находится в папке с установленным менеджером, нужно внести секцию, настройки из которой будут использоваться при соединении с сервисом AvSCEP. Это будет IP-адрес или DNS-имя хоста, на котором располагается сервис SCEP. В нашем случае, эта секция будет выглядеть так:

```
[SCEP]
URL=http://srv03AvRA:8080/AvScep/avpkiclient
BasicAuthentication=False
ProxyPassword=
ProxyPort=
ProxyServer=
ProxyUsername=
```

В случае, если на рабочем месте организован доступ к интернету через прокси-сервер, то значение *Basic Authentication* нужно изменить на **true** и остальные параметры заполнить актуальными значениями (адрес прокси сервера, порт, имя пользователя и пароль).

После внесения изменений в настроечный файл *AvCmMsg.ini* его нужно сохранить.

Также можно настроить менеджер сертификатов на отправку запроса в ЦР (УЦ) сразу после генерации запроса. Для этого нужно в желаемый шаблон (**.tpl*), который находится также в каталоге с установленным менеджером, добавить приводившуюся выше секцию, открыв шаблон с помощью текстового редактора, например, Блокнота (Notepad.exe).

6.13.2. Регистрация запроса при автоматической отправке на сервис SCEP

Первоначальное создание запроса с автоматической отправкой запроса на сертификат на сервис SCEP аналогично пунктам 1 – 8 п. 6.1 Создание запроса на сертификат.

После закрытия карточки открытого ключа отобразиться окно, в котором будет указан URL-адрес сервера SCEP (см. Рисунок 106. URL-адрес сервера SCEP). Следует убедиться в корректности указанного адреса и изменить его, если нужно.

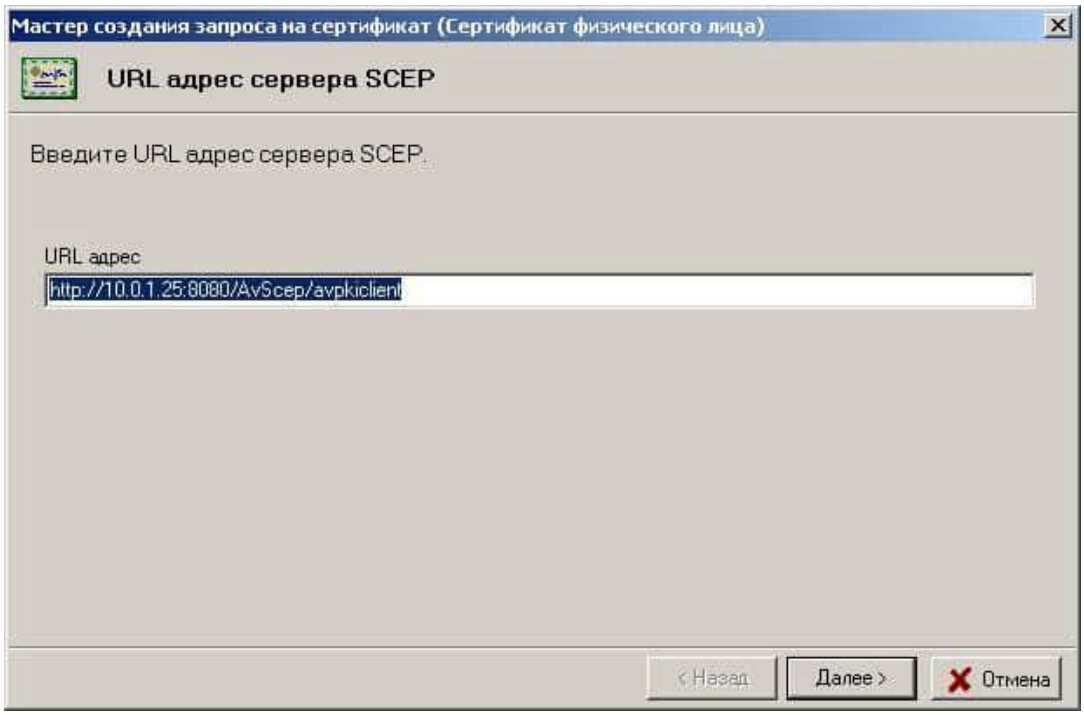


Рисунок 106. URL-адрес сервера SCEP

После нажатия кнопки «Далее» в открывшемся окне надо ввести пароль к контейнеру личного ключа (см. Рисунок 107. Ввод пароля в окне мастера удаленной регистрации).

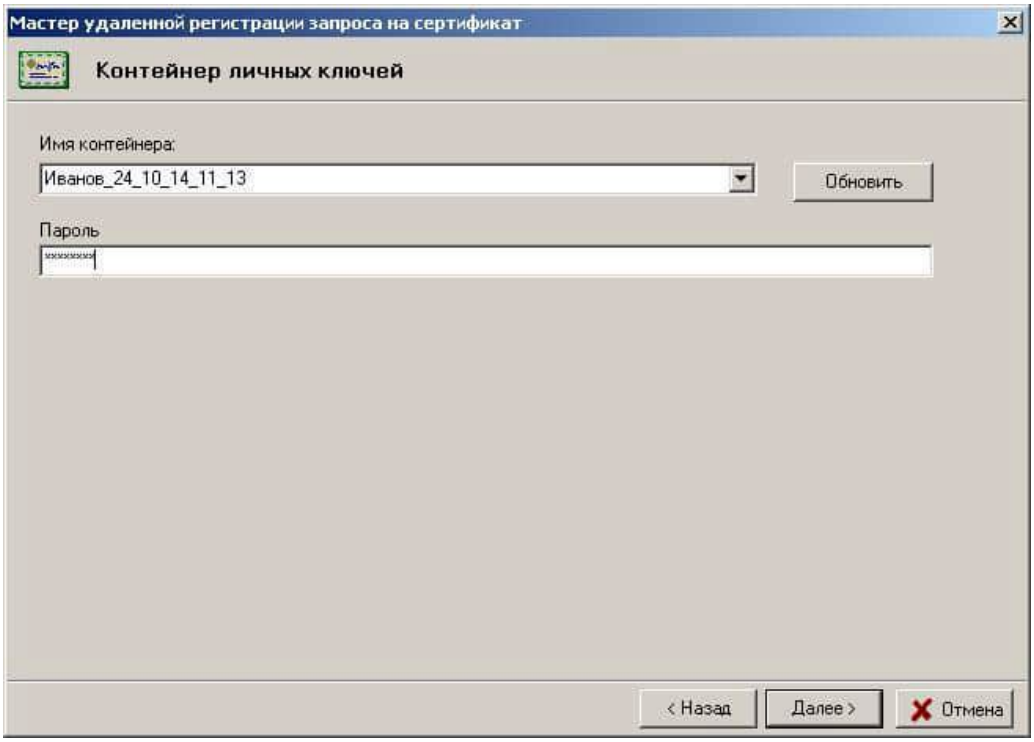


Рисунок 107. Ввод пароля в окне мастера удаленной регистрации

Если после ввода пароля запрос отправлен успешно, отобразится окно с уведомлением об ожидании ручной обработки запроса на сертификат (см. Рисунок 108. Ответ сервера SCEP). Следует нажать кнопку «Далее» и закрыть мастер создания запроса на сертификат.

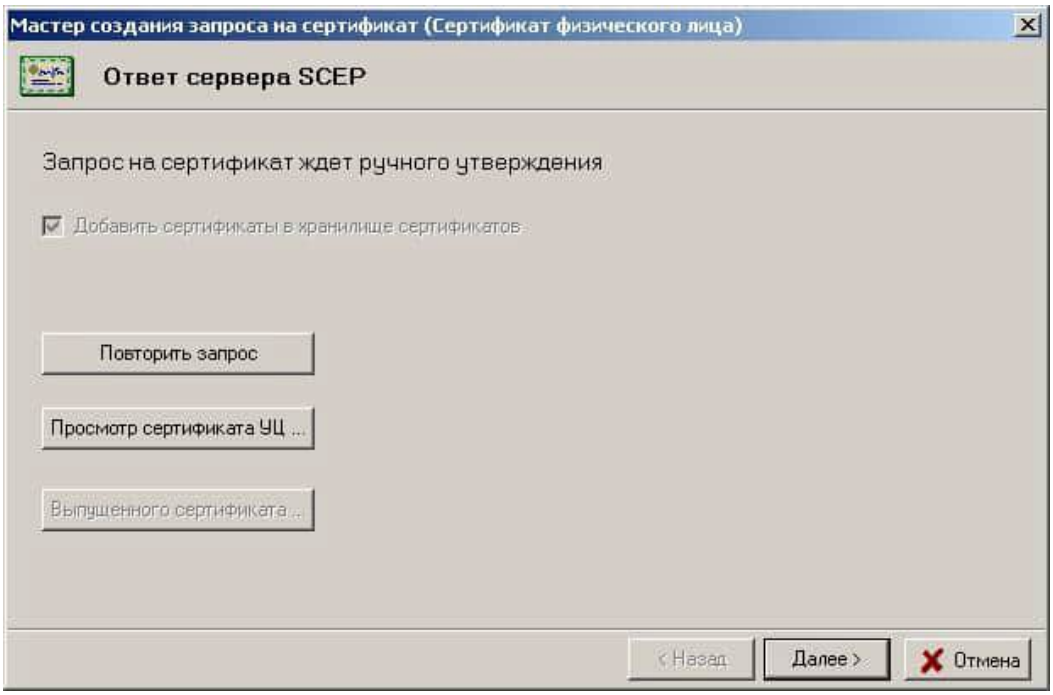


Рисунок 108. Ответ сервера SCEP

6.13.3. Регистрация запроса при ручной отправке на сервис SCEP

Первоначальное создание запроса с автоматической отправкой запроса на сертификат на сервис SCEP аналогично пунктам 1 – 8 п. 6.1 Создание запроса на сертификат.

После печати карточки открытого ключа надо перейти в раздел «Запросы на сертификат», найти созданный запрос, открыть контекстное меню, нажав правой кнопкой мыши по запросу, и выбрать пункт «Удаленная регистрация запроса на сертификат» (см. Рисунок 109. Удаленная регистрация запроса).

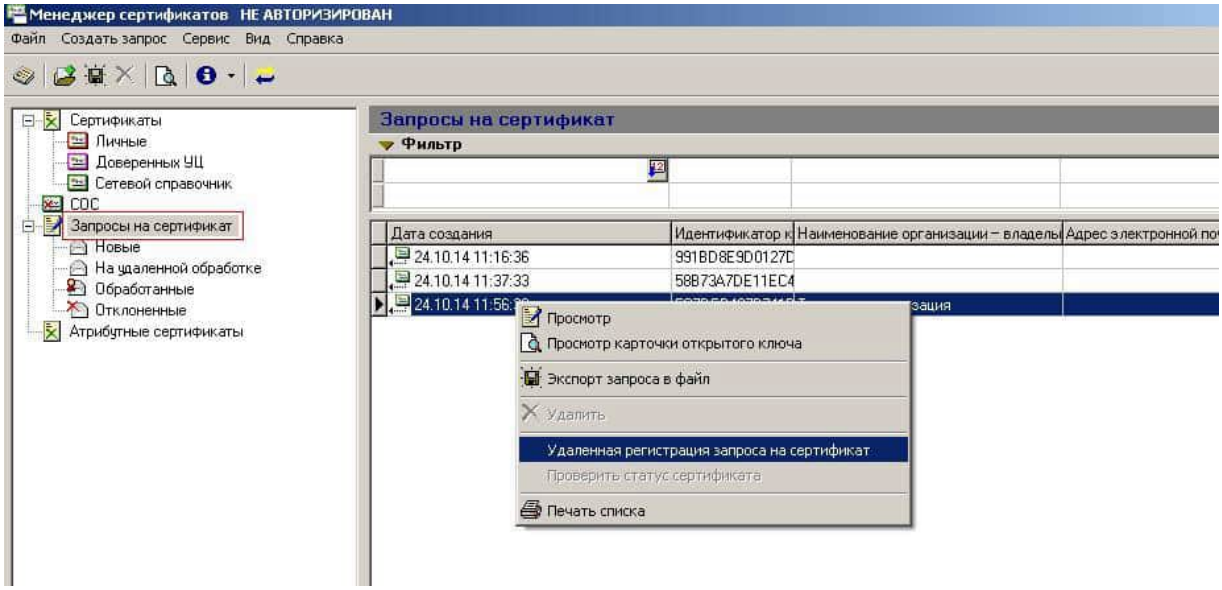


Рисунок 109. Удаленная регистрация запроса

В следующем окне отобразится информация о запросе на сертификат (см. Рисунок 110. Сведения о запросе на сертификат).

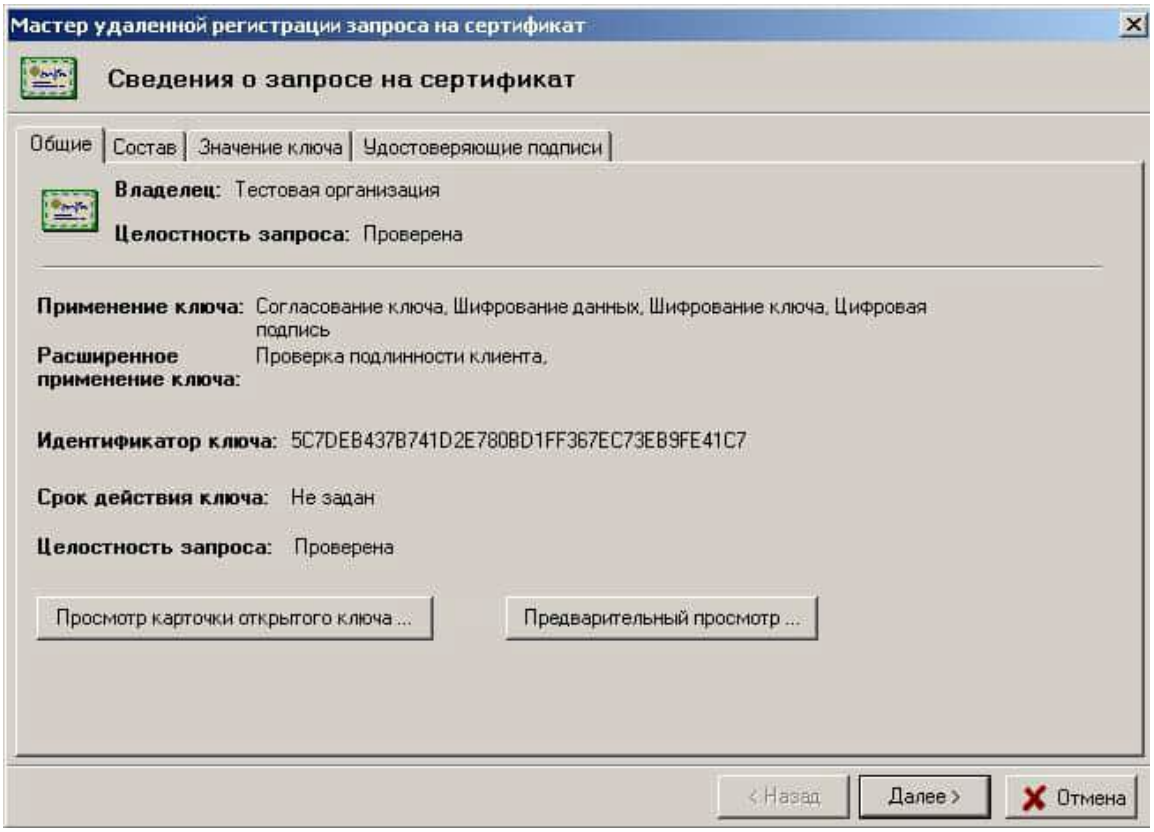


Рисунок 110. Сведения о запросе на сертификат

Далее будет указан URL-адрес сервера SCEP (см. Рисунок 106. URL-адрес сервера SCEP). Следует убедиться в корректности указанного адреса и изменить его, если нужно.

После нажатия кнопки «Далее» в открывшемся окне надо ввести пароль к контейнеру личного ключа (см. Рисунок 107. Ввод пароля в окне мастера удаленной регистрации).

Если после ввода пароля запрос отправлен успешно, отобразится окно с уведомлением об ожидании ручной обработки запроса на сертификат (см. Рисунок 108. Ответ сервера SCEP). Следует нажать кнопку «Далее» и закрыть мастер создания запроса на сертификат.

6.13.4. Проверка статуса сертификата через сервис SCEP

После того, как запрос на сертификат будет обработан в Регистрационном центре, можно с проверить «Статус сертификата» и проимпортировать полученный сертификат хранилище Личных сертификатов.

Для этого надо перейти в раздел «Запросы на сертификат», найти запрос, открыть контекстное меню, нажав правой кнопкой мыши по запросу, и выбрать пункт «Проверить статус сертификата» (см. Рисунок 111. Проверка статуса сертификата).

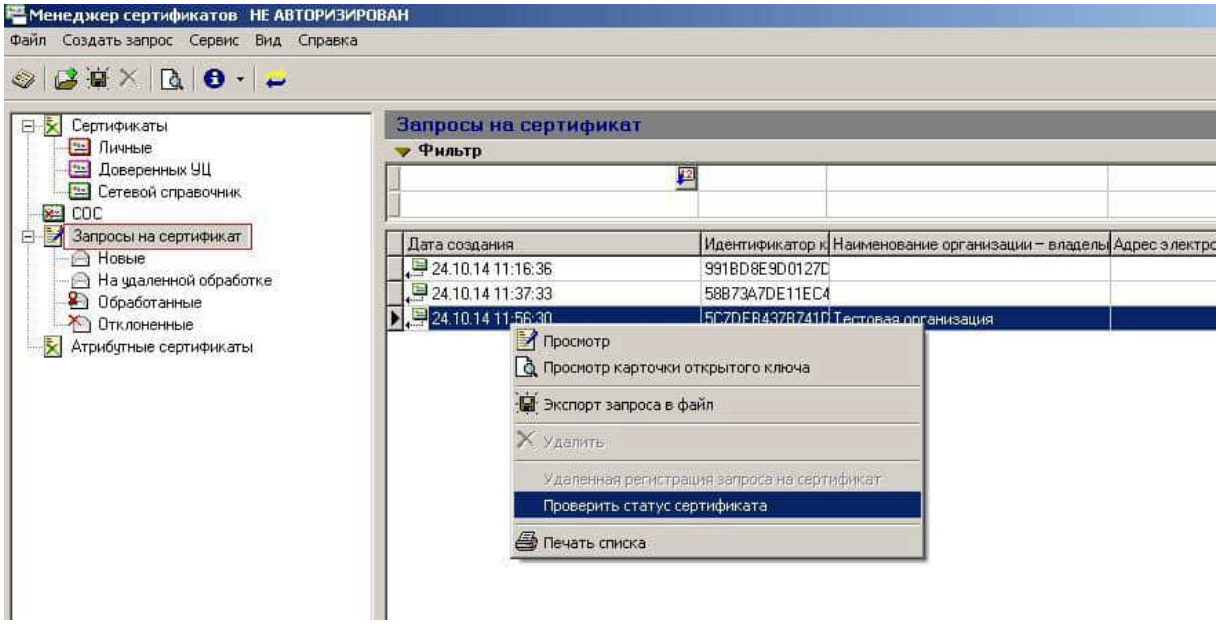


Рисунок 111. Проверка статуса сертификата

После нажатия кнопки «Далее» в открывшемся окне надо ввести пароль к контейнеру личного ключа (см. Рисунок 112. Ввод пароля в окне мастера удаленной регистрации).

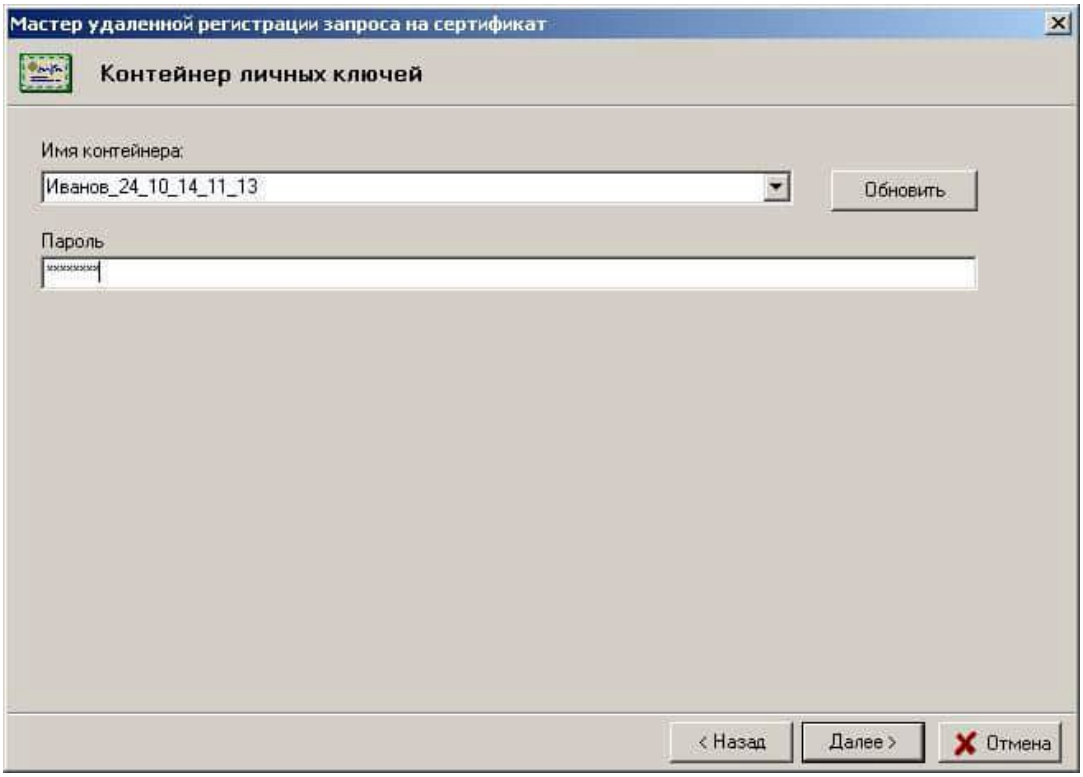


Рисунок 112. Ввод пароля в окне мастера удаленной регистрации

После ввода пароля отобразится окно с информацией о выпуске сертификата Удостоверяющим центром (см. Рисунок 113. Ответ сервера SCEP). Если в данном окне отметить пункт «Добавить сертификаты в хранилище сертификатов», то сертификат будет помещен в справочник «Личные».

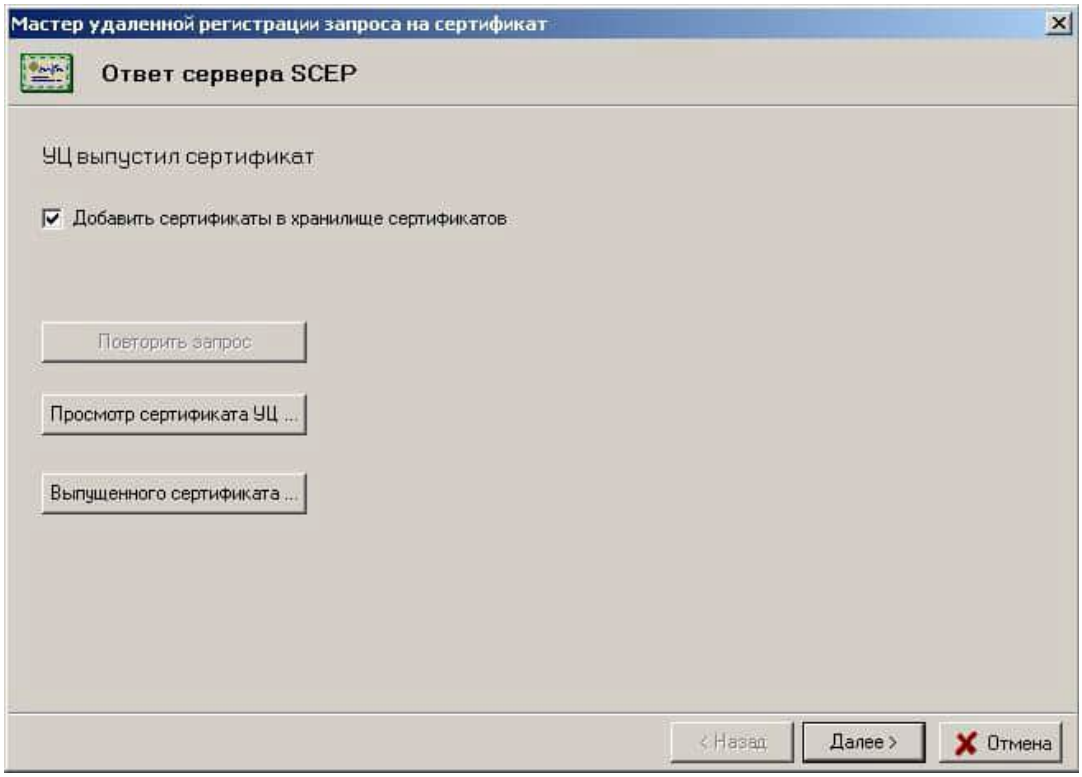


Рисунок 113. Ответ сервера SCEP

На последнем этапе мастера будет отображена информацию о полученном сертификате и сертификатах, помещенных в хранилище Менеджера сертификатов (см. Рисунок 114. Окончание работы мастера удаленной регистрации).

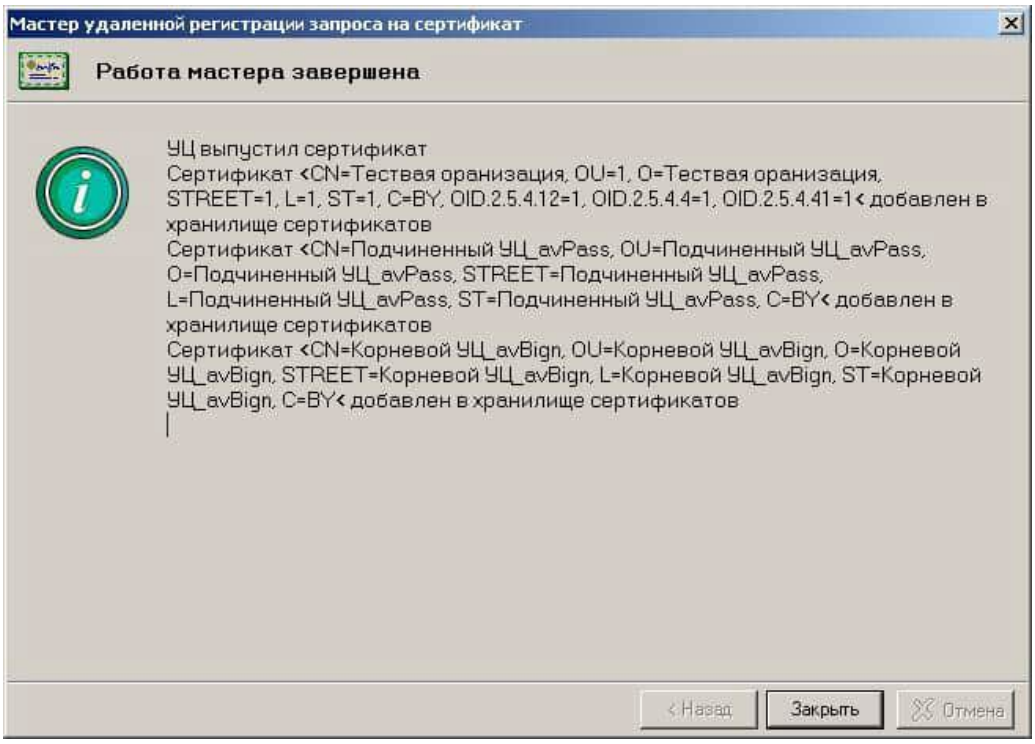


Рисунок 114. Окончание работы мастера удаленной регистрации

6.14. Обновление СОС и сертификатов УЦ, проверка статуса сертификата

6.14.1. Обновление СОС и сертификатов УЦ с использованием пункта меню «Сервис» - «Обновление СОС и сертификатов УЦ»

Точки распространения – расширения сертификата открытого ключа, содержащие URL доступа к ресурсу. Соответственно, когда говорится о точках распространения списка отозванных сертификатов, то имеются в виду URL, по которому размещены файлы с СОС.

Также ПК AvPCM может загружать и производить импорт сертификатов Удостоверяющих центров, если имеется URL, по которому размещены файлы сертификатов УЦ.

Для того, чтобы ПК «Персональный менеджер сертификатов Авест» мог произвести обновление сертификатов и СОС, нужно:

1) в папке с установленным ПК «Персональный менеджер сертификатов Авест» с помощью текстового редактора (например, Блокнот (Notepad)) создать файл *CrlDPExt.txt*;

2) в данный файл поместить URL, по которому доступны точки распространения СОС. Точек распространения в файле C*rlDPExt.txt* может быть указано несколько. Дублирование точек распространения делают для повышения надежности по доступности ресурсов. Например,
```
http://dev.avest.by/ca/cert/stend-gossuok-root-2019.cer
http://dev.avest.by/ca/crl/stend-gossuok-root-2019.crl
http://dev.avest.by/ca/cert/stend-gossuok-sub-2019.cer
http://dev.avest.by/ca/crl/stend-gossuok-sub-2019.crl
http://dev.avest.by/ca/cert/stend-gossuok-ruc-attr-2021.cer
http://dev.avest.by/ca/crl/stend-gossuok-ruc-attr-2021.crl
```

3) В случае, если на рабочем месте организован доступ к интернету через прокси-сервер, надо задать настройки подключения через прокси-сервер (см. п. 6.14.5 Задание настроек подключения через прокси-сервер).

4) В случае необходимости также можно напрямую задать настройки протокола TLS, по которому будет проходить подключение по защищенному соединению (см. п. 6.14.6 Настройка протокола TLS).

5) Выбрать пункт меню «Сервис» - «Обновление СОС и сертификатов УЦ» (см. Рисунок 115. Обновление СОС).

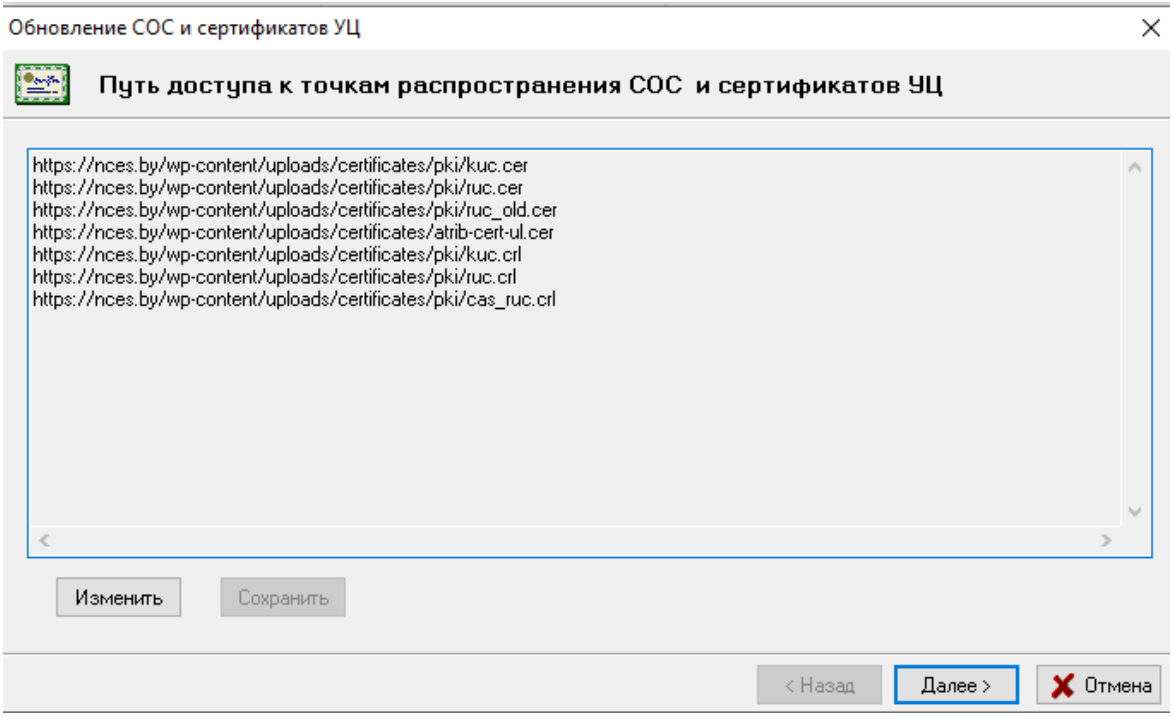


Рисунок 115. Обновление СОС

6) В открывшемся окне можно изменить содержимое файла *CrlDPExt.txt*, добавив или удалив URL, по которому размещены файлы сертификатов УЦ и СОС.

7) После нажатия кнопки «Далее» произойдет загрузка файлов из указанных адресов с выводом информации в окне (см. Рисунок 116. Процесс выполнения обновления сертификатов и СОС).

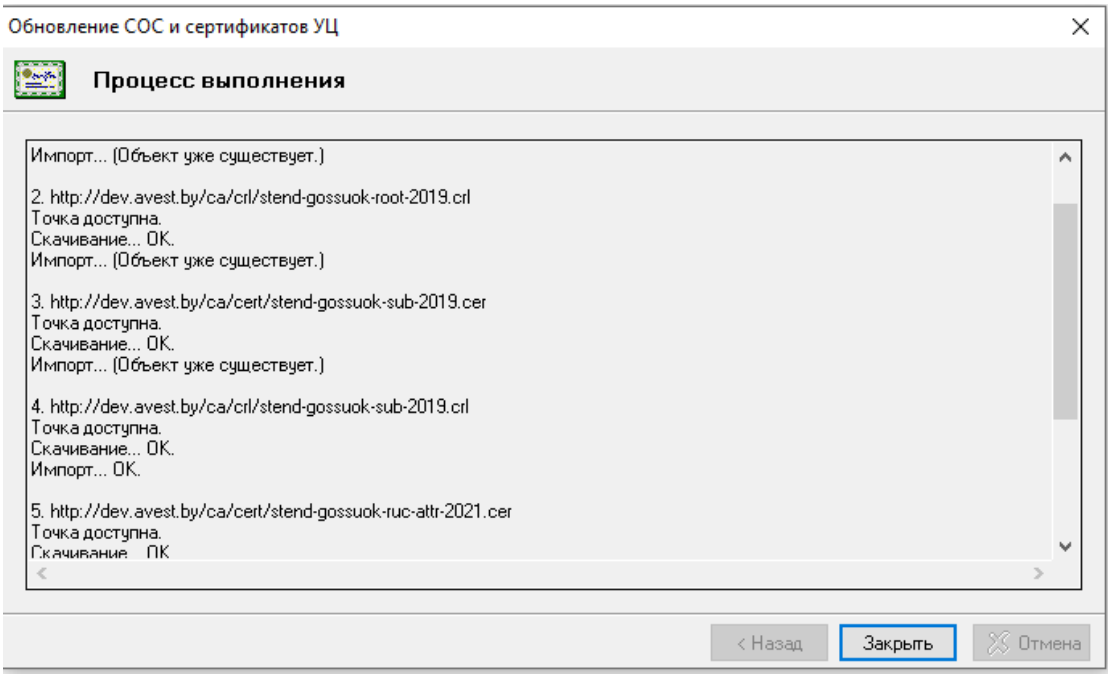


Рисунок 116. Процесс выполнения обновления сертификатов и СОС

8) Если точка распространения СОС недоступна, а также, если СОС по указанным адресам аналогичны уже загруженным в базу данных, будет выведена соответствующая информация (см. Рисунок 117. Информация об обновлении СОС). После завершения процесса Обновления СОС и сертификатов УЦ и вывода соответствующей информации нужно нажать кнопку «Закрыть».

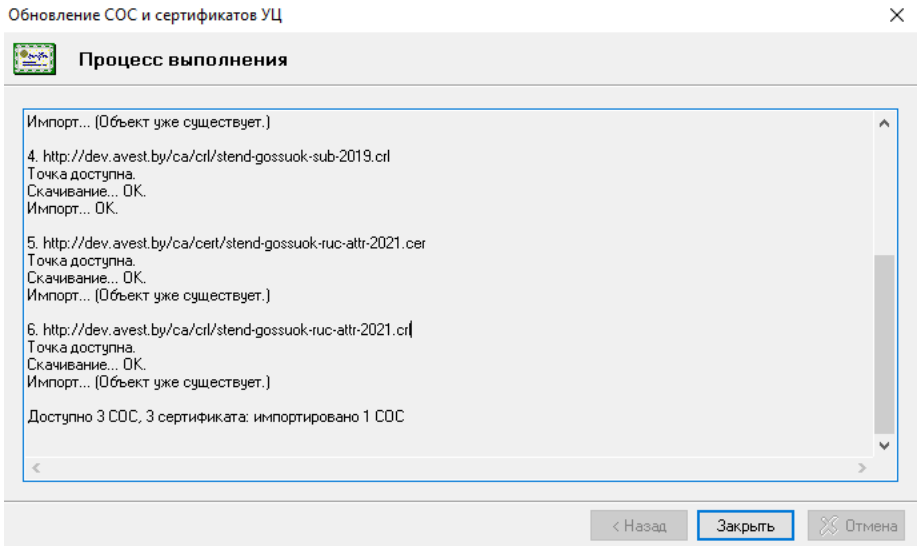


Рисунок 117. Информация об обновлении СОС

6.14.2. Обновление СОС с использованием кнопки «Проверка точек распространения СОС» в сертификате (атрибутном сертификате)

Точки распространения – расширения сертификата открытого ключа, содержащие URL доступа к ресурсу. Соответственно, когда говорится о точках распространения списка отозванных сертификатов, то имеются в виду URL, по которому размещены файлы с СОС.

Если такой URL добавлен в сертификат, то чтобы обновить СОС, нужно:

1) открыть просмотр сертификата в окне авторизации или в менеджере (нажать по сертификату правой клавишей мыши и выбрать «Просмотр)» и нажав кнопку «Проверка точек распространения СОС…» (см. Рисунок 118. Проверка точек распространения СОС).

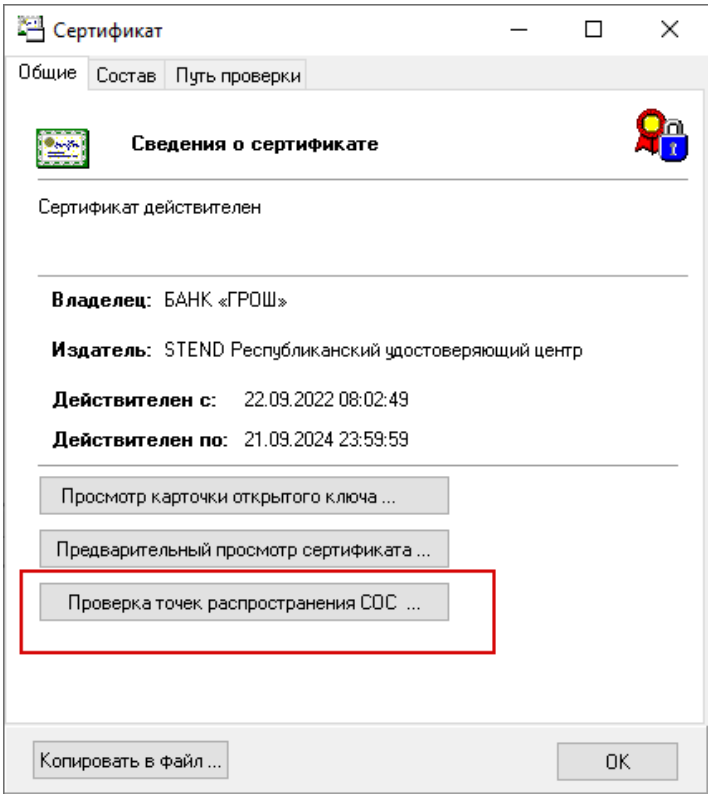


Рисунок 118. Проверка точек распространения СОС

2) Откроется окно «Обновление СОС», нажать «Далее» (см. Рисунок 119. Обновление СОС):

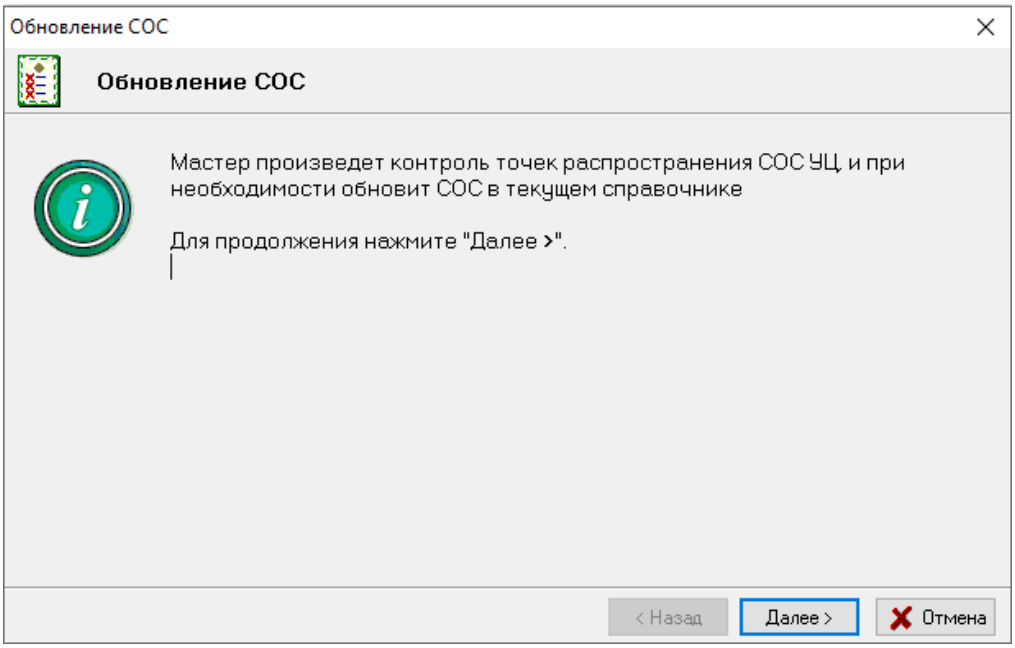


Рисунок 119. Обновление СОС

3) В следующем окне отобразится URL, с которого будет скачан СОС, нажать «Далее» (см. Рисунок 120. URL, на котором размещен актуальный СОС УЦ).

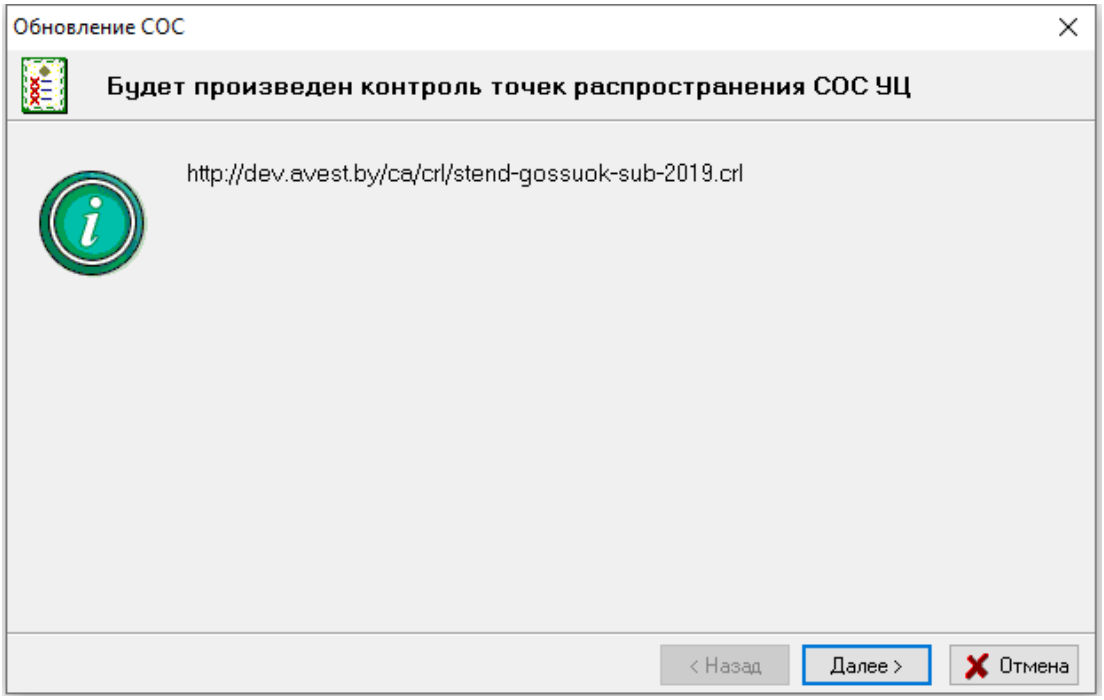


Рисунок 120. URL, на котором размещен актуальный СОС УЦ

4) Будет выведена информация о начале действия СОС, полученного с удаленного ресурса, и начале действия текущего СОС, хранящегося в базе данных. При нажатии кнопки «Просмотр» можно просмотреть полную информацию о полученном СОС. По умолчанию будет установлена галочке на пункте «Импортировать полученный СОС», если вы согласны проимпортировать данный СОС, нужно галочку не убирать и нажать «Далее» (см. Рисунок 121. Информация о полученном СОС).

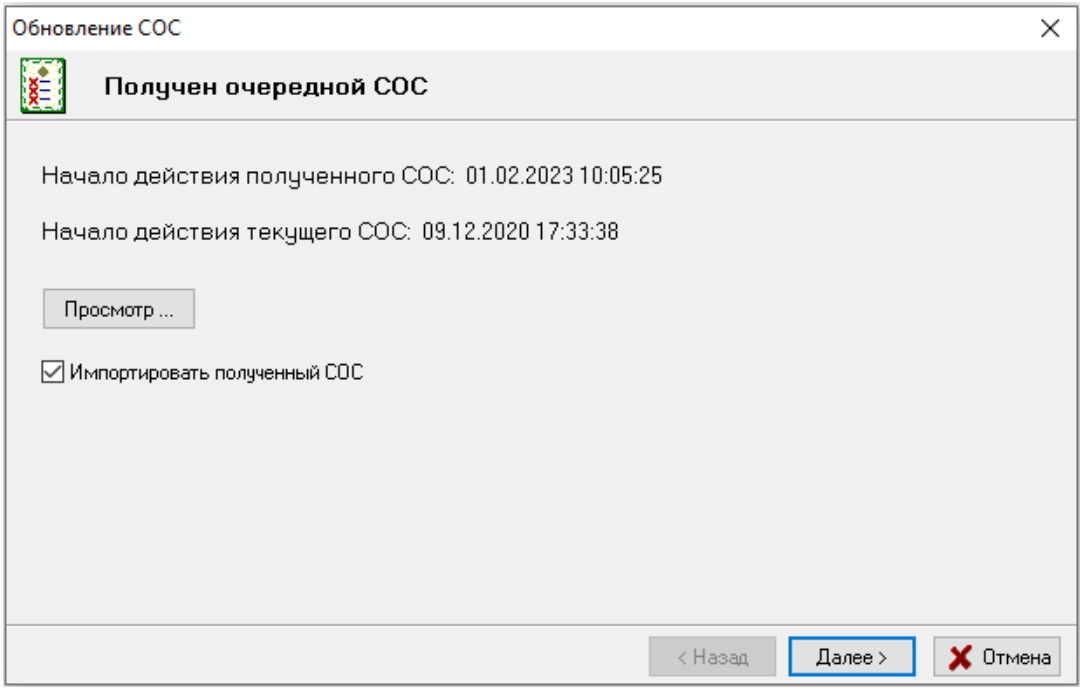


Рисунок 121. Информация о полученном СОС

5) В последнем окне буден выведен результат работы мастера по обновлению СОС, например, что СОС был проимпортирован, нужно нажать «ОК» (см. Рисунок 122. Работа мастера завершена).

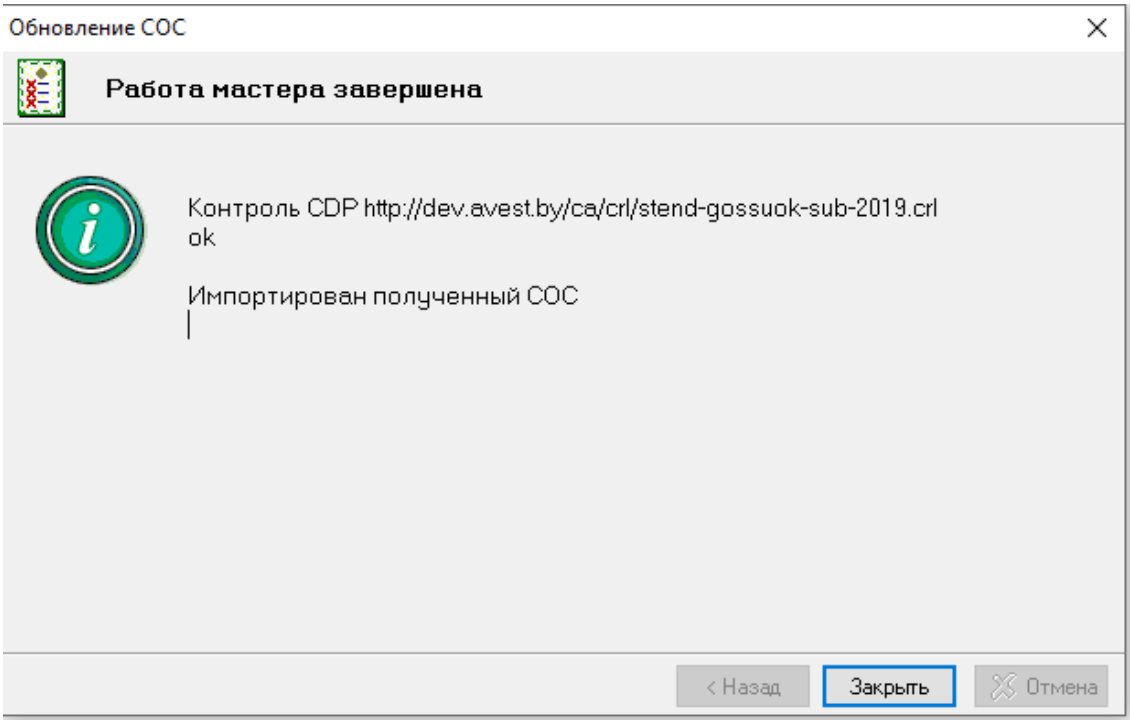


Рисунок 122. Работа мастера завершена

Если URL доступа к ресурсу добавлен в атрибутный сертификат, то, чтобы обновить СОС, нужно открыть просмотр атрибутного сертификата в менеджере (нажать по сертификату правой клавишей мыши и выбрать «Просмотр)» и нажав кнопку «Проверка точек распространения СОС…» (см. Рисунок 123. Проверка точек распространения СОС в атрибутном сертификате).

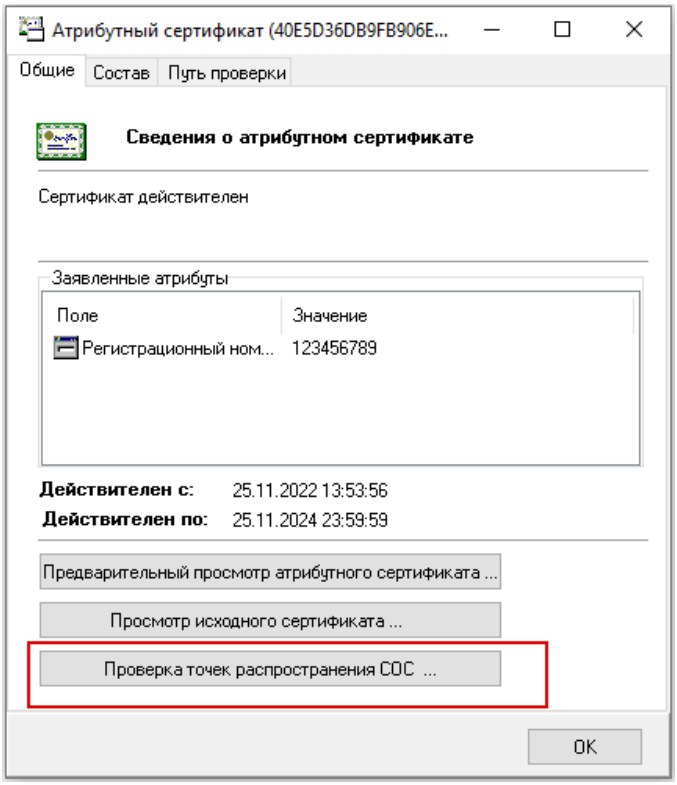


Рисунок 123. Проверка точек распространения СОС в атрибутном сертификате

Все дальнейшие действия по обновлению СОС для атрибутного сертификата будут аналогичны действиям, описанным выше для исходного сертификата.

6.14.3. Настройка автоматической проверки статуса сертификата (атрибутного сертификата) при помощи сервиса онлайн-проверки сертификата (OCSP-сервера)

ПК AvPCM имеет возможность автоматической проверки статуса сертификатов открытого ключа и атрибутных сертификатов при помощи сервиса онлайн-проверки сертификатов (OCSP-сервера). Существует два варианта использования данной функции:

1. Адрес, по которому доступен OCSP-сервер (authorityInfoAccess OCSP), **присутствует** в сертификате. В данном случае следует добавить в конфигурационный файл **AvCmMsg.ini**, который находится в папке с установленным менеджером, раздел `[OCSP]`, внести следующую строки и сохранить изменения:

```
[OCSP]
UseOCSPforCheckCert=True
UseOCSPforCheckAttributeCert=True
```

2. Адрес, по которому доступен OCSP-сервер (authorityInfoAccess OCSP) **отсутствует** в сертификате. В данном случае следует добавить в конфигурационный файл **AvCmMsg.ini**, который находится в папке с установленным менеджером, раздел `[OCSP]`, внести туда строчку `UseOCSPforCheckCert=True`. Далее добавить раздел `[OCSPServers]`, в котором указать адрес OCSP-сервера и сохранить изменения:

```
[OCSP]
UseOCSPforCheckCert=True
UseOCSPforCheckAttributeCert=True
[OCSPServers]
Подчиненный УЦ=http://10.0.0.10:8080/responder/
Служба атрибутных сертификатов=http://10.0.0.10:8080/responder/
```

При необходимости можно отключить проверку статуса сертификата для определенного УЦ. Для этого нужно добавить в секцию `[OCSPServers]` строку с общим именем УЦ и параметром `NOTUSED`, например:

```
[OCSP]
UseOCSPforCheckCert=True
UseOCSPforCheckAttributeCert=True
[OCSPServers]
Корневой удостоверяющий центр=NOTUSED
Подчиненный УЦ=http://10.0.0.10:8080/responder/
Служба атрибутных сертификатов=http://10.0.0.10:8080/responder/
```

В случае, если время на компьютере с ПК AvPCM отличается от времени на OCSP-сервере, полученный от сервера OCSP-ответ может содержать недействительное время. Для того, чтобы разница во времени была устранена, нужно внести соответствующие изменения в конфигурационный файл *AvOCSPClient.ini* (файл находится в папке с установленным менеджером): в секции `[Rules]` указать допустимое отклонение по времени (не больше 3600 сек.).

Например:

```
[Rules]
NextUpdateTolerance=500
ThisUpdateTolerance=500
```

Также в файле *AvOCSPClient.ini* можно указать алгоритм хэширования, который будет использован при взаимодействии с OCSP-сервером. В секции `[Crypto]` по умолчанию указан алгоритм хэширования sha1:

```
[Crypto]
HashAlgOid=1.3.14.3.2.26
```

Допускается использование также алгоритмов Belt, sha512 и sha256, для этого нужно внести соответствующие изменения в данной секции.

Для Belt:

```
[Crypto]
HashAlgOid=1.2.112.0.2.0.34.101.31.81
```

Для sha512:

```
[Crypto]
HashAlgOid=2.16.840.1.101.3.4.2.3
```

Для sha256:

```
[Crypto]
HashAlgOid=2.16.840.1.101.3.4.2.1
```

6.14.4. Настройка автоматической проверки точек распространения COC

Если сертификат пользователя содержит точку распространения COC, ПК AvPCM может проверить в автоматическом режиме фукционирование данной точки распространения COC. Для этого нужно в файле **AvCmMsg.ini** (файл находится в папке с установленным менеджером) добавить раздел `[OCSP]`, внести в него следующую строчку и сохранить изменения:

```
[OCSP]
CDPCheckPeriod=10
```

Период измеряется в минутах. Минимальное значение = 0 (в этом случае автоматическая проверка не производится). Максимальное значение ограничено числом 2^{32} и выбирается, исходя из особенностей функционирования пользовательского программного обеспечения, требующего

обращения к точкам распространения СОС. В приведенном выше примере число 10 означает, что через 10 минут после проверки статуса сертификата пользователя ПК AvPCM инициирует новую проверку с использованием точек распространения из данного сертификата.

6.14.5. Задание настроек подключения через прокси-сервер

В случае, если на рабочем месте организован доступ к интернету через прокси-сервер, то для импорта сертификатов с сервера УЦ (см. п. 6.5.5 Импорт сертификатов с сервера УЦ), а также для обновления СОС и сертификатов УЦ (см. п. 6.14.1 Обновление СОС и сертификатов УЦ с использованием пункта меню «Сервис» - «Обновление СОС и сертификатов УЦ») нужно задать настройки подключения через прокси-сервер. Для этого в файл *AvCmMsg.ini*, который находится в папке с установленным менеджером, нужно внести секцию HttpProxy с актуальными значениями для подключения, например:

```
[HttpProxy]
ProxyServer=10.0.0.0
ProxyPort=8855
ProxyUsername=user
ProxyPassword=Password
BasicAuthentication=TRUE
ReadTimeOut=180
```

В строке `ProxyServer=` указывается адрес прокси-сервера.

В строке `ProxyPort=` указывается порт для подключения прокси.

В строке `BasicAuthentication=` указывается параметр подключения к прокси-серверу (`TRUE` - с авторизацией, `FALSE` - без авторизации).

В строке `ProxyUsername=` указывается имя пользователя для подключения прокси с авторизацией.

В строке `ProxyPassword =` указывается пароль для подключения пользователя прокси с авторизацией.

Если авторизация не требуется (`BasicAuthentication=FALSE`), то строки `ProxyUsername=` и `ProxyPassword=` можно или не вносить, или закомментировать (внести перед параметром знак препинания «;»):

```
;ProxyUsername=
;ProxyPassword=
BasicAuthentication=FALSE
```

Существует промежуток времени, в который программа ожидает ответ от сервера. По умолчанию этот период равен 180 секундам. Но этот параметр можно увеличить или уменьшить путем редактирования соответствующей строки:

```
ReadTimeOut=180
```

После внесения изменений в настроечный файл *AvCmMsg.ini* его нужно сохранить.

6.14.6. Настройка протокола TLS

В файле *AvCmMsg.ini* (находится в папке с установленным менеджером) можно задать вручную протокол TLS, по которому будет происходить защищенное соединение с сервером для импорта сертификатов с сервера УЦ (см. п. 6.5.5 Импорт сертификатов с сервера УЦ), а также для обновления СОС и сертификатов УЦ (см. п. 6.14.1 Обновление СОС и сертификатов УЦ с использованием пункта меню «Сервис» - «Обновление СОС и сертификатов УЦ»). Для этого в файл *AvCmMsg.ini* нужно внести секцию TLS, в которой будет задан протокол TLS для подключения к серверу:

```
[TLS]
;Protocol=TLS 1.0
;Protocol=128

;Protocol=TLS 1.1
;Protocol=512

;Protocol=TLS 1.2
;Protocol=2048
```

В данной секции нужно снять комментарий (удалить знак препинания «;») с тех строчек, которые отвечают за подключение к нужному протоколу. Например, для установки защищенного соединения с сервером по протоколу TLS 1.0 нужно снять комментарий со строки `Protocol=TLS 1.0` или `Protocol=128`:

```
[TLS]
Protocol=TLS 1.0
;Protocol=128

;Protocol=TLS 1.1
;Protocol=512

;Protocol=TLS 1.2
;Protocol=2048
```

А для подключения по протоколу TLS 1.2 нужно снять комментарий со строки `Protocol=TLS 1.2` или `Protocol=2048`:

```
[TLS]
;Protocol=TLS 1.0
;Protocol=128

;Protocol=TLS 1.1
;Protocol=512

;Protocol=TLS 1.2
Protocol=2048
```

Допускается одновременное подключение нескольких протоколов. После внесения изменений в настроечный файл *AvCmMsg.ini* его нужно сохранить.

6.14.7. Импорт СОС в тихом режиме

Чтобы импорт СОС проходил в "тихом" режиме, без запроса действий оператора, в командной строке Windows нужно запустить команду:

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

где *name.crl* – импортируемый СОС.

6.14.8. Настройка времени кэширования СОС

Время кэширования СОС можно настроить в **AvCmMsg.ini (**конфигурационный файл, который находится в папке с установленным менеджером), открыв его (например, с помощью Блокнота) и вставив секцию [CRLCache], с возможными ключами (если секция отсутствует устанавливается Default=300):

Default=время кэширования всех СОС в секундах;

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

Пример:

[CRLCache]

Default=120

Корневой удостоверяющий центр=600

6.15. Настройка хранилища сертификатов на учетную запись компьютера

По умолчанию менеджер сертификатов, использующий базу данных в реестре Windows, настроен на хранилище сертификатов для учетной записи пользователя. Если для учетной записи пользователя права ограничены (например, такое часто встречается при использовании доменных учетных записей), то могут возникнуть трудности при работе с сертификатами. Наиболее часто встречающаяся проблема - сертификат Корневого УЦ не помещается в справочник Доверенных УЦ. Решить эту проблему можно, перенастроив хранилище сертификатов на учетную запись компьютера. Для этого в конфигурационном файле AvCmMsg.ini (находится в папке с установленным менеджером сертификатов) в секции [LOGIN] после CONNECTSTR=SYSTEMSTORE нужно поставить «;» и дописать StoreLocations=LOCAL_MACHINE:

```
[LOGIN]
CONNECTSTR=SYSTEMSTORE; StoreLocations=LOCAL_MACHINE
```

После внесения изменений в настроечный файл *AvCmMsg.ini* его нужно сохранить. Далее проимпортировать сертификаты, установить доверие к сертификату Корневого УЦ (см. п. 6.7.3. Справочник «Доверенных Удостоверяющих центров»).

Если права учетной записи пользователя сильно ограничены, то при запуске менеджера сертификатов, настроенного на хранилище сертификатов учетной записи компьютера может возникнуть ошибка: «Не найдено (испорчено) хранилище сертификатов» (см. Рисунок 124. Не найдено (испорчено) хранилище сертификатов).

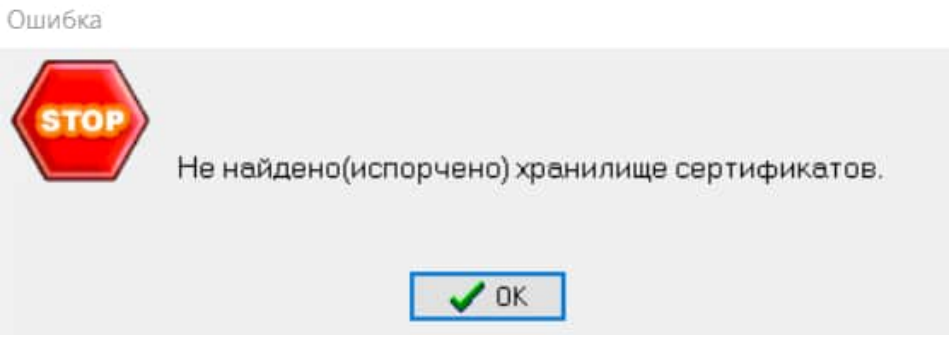


Рисунок 124. Не найдено (испорчено) хранилище сертификатов

Данная ошибка означает, что у учетной записи пользователя нет прав доступа на хранилища сертификатов учетной записи компьютера. Решение: добавить дополнительные права пользователю на хранилища сертификатов или запустить менеджер с правами администратора.

Следует учитывать, что для авторизации по защищенному соединению в сети Интернет используется сертификат, хранящийся в учетной записи пользователя. Поэтому менеджер сертификатов с хранилищем СОК в учетной записи компьютера зачастую целесообразно использовать только для помещения сертификатов Корневых УЦ в Справочник Доверенных УЦ, а личные сертификаты нужно импортировать в менеджер с хранилищем СОК в учетной записи пользователя.

6.16. Включение отображения информационных окон

Для появления возможности отображения окна «Вывод информационных окон» нужно 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
```

6.17. Настройка шифрования для обеспечения обратной связи

В случае если происходит обмен зашифрованными сообщениями, но отправитель и получатель имеют разные алгоритмы шифрования, отправителю нужно в файле *AvCmMsg.ini*

(находится в папке с установленным менеджером сертификатов) сделать настройки, чтобы получатель мог расшифровать сообщение.

Для этого нужно добавить секцию [ENCRYPTALGORITHMS], где указать идентификатор алгоритма открытого ключа сертификата получателя и алгоритм шифрования.

Пример:

```
[ENCRYPTALGORITHMS]
1.2.112.0.2.0.34.101.45.2.1=1.2.112.0.2.0.34.101.31.43
```

Если сообщение будет зашифровано на несколько получателей, то алгоритм шифрования будет использоваться первый. Если в ENCRYPTALGORITHMS не будет найден алгоритм открытого ключа, то будет взят алгоритм из секции [CSP].

Пример:

```
[ENCRYPTALGORITHMS]
1.3.6.1.4.1.12656.1.37=1.3.6.1.4.1.12656.1.34.1.2
1.2.112.0.2.0.34.101.45.2.1=1.2.112.0.2.0.34.101.31.43
```

7. ПЕРЕХОД ИЗ ДРУГОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Для перехода из одного Удостоверяющего центра в другой нужно сделать следующее: отозвать свой сертификат в старом Удостоверяющем центре.

Для того, чтобы отозвать свой сертификат, нужно:

1. обратиться в старый Удостоверяющий центр с заявлением об отзыве своего сертификата;
2. после отзыва сертификата, получить в Удостоверяющем центре обновленный список отозванных сертификатов (СОС);
3. импортировать полученный список отозванных сертификатов (СОС) средствами ПК AvPCM на свой компьютер;
4. сгенерировать новый ключ и получить сертификат в новом Удостоверяющем центре;
5. получить новые сертификаты и СОС и импортировать их средствами ПК AvPCM на свой компьютер;
6. в ПК AvPCM удалить из справочника «Личные» старый (отозванный) сертификат.

8. УТИЛИТА КОМАНДНОЙ СТРОКИ AVCMUT

ПК AvPCM позволяет производить контрольные криптографическиее процедуры, включающие в себя выработку/проверку электронно-цифровой подписи, предварительное зашифрование, контроль целостности путём вычисления хэш-значения от файла при помощи утилиты AvCmUt.exe (находится в папке с установленным менеджером сертификатов).

Порядок использования утилиты командной строки описан в руководстве оператора программного продукта РБ.ЮСКИ.13008-02 «Утилита командной строки AvCmUt».

9. УДАЛЕНИЕ ПРОГРАММЫ

Действия по удалению ПК AvPCM с компьютера зависят от операционной системы.

В ОС Windows XP (Windows 2003 Server):

1) выбрать из основного меню Windows: «Пуск» – «Настройка» – «Панель управления» – «Установка и удаление программ»;
2) в окне «Установка и удаление программ» на закладке «Изменение или удаление программ» в окне перечисления программ выбрать «Персональный менеджер сертификатов Авест» и нажать кнопку «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.

В ОС Windows 7 (Windows 2008 Server):

1) выбрать из основного меню Windows: «Пуск» – «Панель управления» – «Программы и компоненты» (или «Программы» / «Удаление программы»);
2) в окне «Удаление или изменение программы» в списке программ выбрать «Персональный менеджер сертификатов Авест», нажать по нему правой клавишей мыши, нажать кнопку «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.

В ОС Windows 8 (Windows 2012 Server):

1) навести курсор мыши на левый нижний угол рабочего стола до появления кнопки «Пуск», нажать по ней правой клавишей мыши, выбрать «Программы и компоненты»;
2) в окне «Удаление или изменение программы» в списке программ выбрать «Персональный менеджер сертификатов Авест», нажать по нему правой клавишей мыши, нажать кнопку «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.

В ОС Windows 8.1:

1) переместите курсор в нижний левый угол экрана, нажать по отобразившейся кнопке «Пуск» правой клавишей мыши, выбрать «Программы и компоненты»;
2) в окне «Удаление или изменение программы» в списке программ выбрать «Персональный менеджер сертификатов Авест», нажать по нему правой клавишей мыши, нажать кнопку «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.

В ОС Windows 10 (Windows 2016 Server, Windows 2019 Server):

1) нажать по кнопке «Пуск» правой клавишей мыши, выбрать «Приложения и возможности»;
2) в окне «Приложения и возможности» в списке программ выбрать «Персональный менеджер сертификатов Авест», нажать кнопку «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.

10. 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.

10.1 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 (ЗАО «АВЕСТ»);
- 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 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности»;
- в состав AvPCM входит тестовая утилита AvCmUt, позволяющая потребителю самостоятельно вычислить хэш-значения полученных программных компонентов ПО;
- ПО обеспечивает в своем GUI-интерфейсе отображение используемой версии программного продукта.

При получении потребителем ПО, в случае, когда он не запрашивал его у ЗАО «АВЕСТ», нужно связаться с сотрудниками ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия https://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.

10.2 Меры безопасности при установке и эксплуатации

Установка ПО на компьютер 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 с хэш-значениями, указанными в сертификате соответствия на ПО, с помощью программного обеспечения по расчету хэш-значений, полученных потребителями из доверенного источника;
- установка ПО должна производиться уполномоченным сотрудником потребителя, ознакомленным с данным документом и выполняющим обязанности администратора;
- на компьютере, предназначенном для установки ПО, должны отсутствовать вредоносные программы («компьютерные вирусы», «резиденты», «отладчики», «клавиатурные шпионы» и т.д.);
- после установки ПО отчуждаемый носитель (компакт-диск) с эталонным установочным файлом ПО и список эталонных хэш-значений программных компонентов должны быть помещены в безопасное хранилище, доступ к которому должен иметь только уполномоченный персонал потребителя.

Эксплуатация ПО на компьютере 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 и электронной цифровой подписи» или в иных случаях;
- для эксплуатации ПО должен использоваться, по возможности, выделенный компьютер с установленным на нем лицензионным системным и прикладным программным обеспечением и только необходимым по технологии использования ПО в информационной системе потребителя;
- компьютер, предназначенный для эксплуатации ПО должен быть защищен от «закладок», «компьютерных вирусов», несанкционированного изменения системного и прикладного программного обеспечения;
- любое изменение (реконфигурирование, дополнение и т.д.) системного и прикладного программного обеспечения компьютера 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;
- в процессе эксплуатации запрещается передавать НКИ, содержащие личные ключи ЭЦП и шифрования, посторонним лицам, оставлять НКИ без присмотра;

- ответственность за сохранность НКИ и содержащихся на нем данных несет сотрудник потребителя, работающий с НКИ;
- доступ к компьютеру с установленным ПО должен быть ограничен и разрешен только уполномоченным на работу с ПО сотрудникам потребителя;
- средствами ОС 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 компьютера);
- при проведении ремонтных и профилактических работ в отношении компьютер, на котором 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 компьютера для ремонта в сторонние организации производится только после демонтажа накопителя информации (накопителя на жестком магнитном диске и/или SSD-диска);
- ремонт накопителя информации, на котором инсталлированы программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования накопителя информации.

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 технической поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия https://www.avest.by**)** и действовать в соответствии с рекомендациями сотрудника отдела технической поддержки.
2. Убедиться в работоспособности компьютера, его 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 технической поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия https://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела технической поддержки.

Процедура «безопасного восстановления» ПО заключается в переинсталляции ПО на ПЭВМ с носителя (компакт-диска) с эталонным установочным файлом ПО. При этом рекомендуется предварительно проверить работоспособность компьютера без установленного на нем 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», если иное не определено в договоре между организацией-поставщиком и ЗАО «АВЕСТ».

10.3 Меры контроля

ПК AvPCM контролирует целостность своих программных модулей путем вычисления хэш-значений согласно СТБ 1176.1-99 от файлов MngCert.exe, AvCmUt4.exe, 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 ПК AvPCM выдаст соответствующее предупреждение (см. Рисунок 125. Нарушение целостности файла). При нарушении целостности данных файлов работа невозможна.

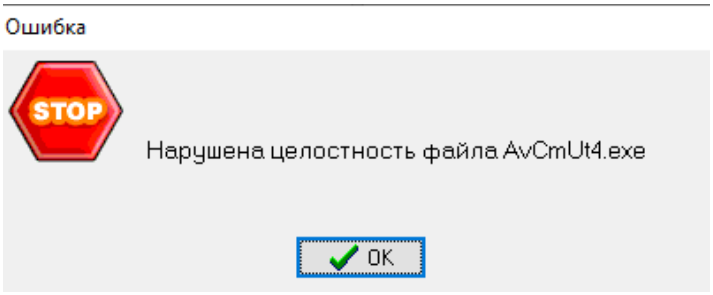


Рисунок 125. Нарушение целостности файла

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 1

Настоящее приложение к документу РБ.ЮСКИ.08003-06 34 01 «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» содержит описание и информацию о возможности настроек программного комплекса на соответствие требованиям:

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

– разделов 6, 7, 8 документа СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

– разделов 8, 9 документа СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

– СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»;

– СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» (класс 2);

– подразделы 7.3, 7.4, 7.5, 7.8 документа СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности»;

– подразделы 6.2, 6.3, 7.1, 7.2, приложение Е документа СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;

– подраздел 6.2 документа СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

– СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»;

– СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов»;

– подразделы 8.2, 8.3, 8.5, 8.8, раздел 11 документа СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».

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 (В СООТВЕТСТВИИ С СТБ 34.101.78)

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

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

Допустимые ключи:

Name = ‘наименование’ – наименование шаблона;

addSigningTime=False - добавить в запрос время создания запроса (по умолчанию True);

addSubjectKeyIdentifier=False - добавить в запрос SubjectKeyIdentifier (по умолчанию True);

useCertificateValidity=True - использовать bpki-at-certificateValidity для задания предполагаемого срока действия сертификата (по умолчанию False).

Секция **[HiddenPages] –** отключение отображения информационных окон.

Допустимые ключи:

FrmKey_USAGE=True – скрывать окно «Применение ключа»;

FrmPrintReq=True – скрывать окно «Печать карточки открытого ключа»;

PrintRequest=True – скрывать окно «Предварительный просмотр карточки открытого ключа».

Секция **[certificatePolicies] –** задание политики применения сертификата.

Допустимые ключи:
OID политики применения сертификата.

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 значения атрибута. Значение ключа может быть DIGITS - ['0'..'9'], IA5STRING - ['!'..'~'];

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

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

AltNameChoice= ‘значение’ – задается тип атрибута альтернативного имени, описывающий цифровые ресурсы стороны, значения могут быть следующие:

rfc822Name - адрес электронной почты,

dNSName - DNS-имя,

URI - URL;

IP - IP-адрес;

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 **[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 ЭЦП 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 используется ***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 1176.1-99 со следующими значениями параметров:

H=4E4E9C9C9C9C4E4E9C9C4E4E4E4E9C9C9C9C4E4E4E4E9C9C4E4E9C9C9C9C4E4E

(в шестнадцатеричной системе счисления), L=160;

3 – результат хэширования функцией в соответствии с алгоритмом, установленным в СТБ 1176.1-99 со следующими значениями параметров:
H=4E4E9C9C9C9C4E4E9C9C4E4E4E4E9C9C9C9C4E4E4E4E9C9C4E4E9C9C9C9C4E4E

(в шестнадцатеричной системе счисления), L=256.

4 - результат хэширования функцией в соответствии с алгоритмом belt-hash, установленным в СТБ 34.101.31-2020.

ПРИЛОЖЕНИЕ 2

Основные параметры, задаваемые в файле инициализации AvCmMsg.ini

Секция	Используемый ключ	Допустимые параметры
[Login] Параметры подключения к хранилищу сертификатов.	**CONNECTSTR=**'хранилище сертификатов и параметры подключения'	Указывается несколько параметров, отделяемых символом «**;**»: **SYSTEMSTORE** - используется хранилище сертификатов MS Windows (реестр CURRENT_USER); **StoreLocations=LOCAL_MACHINE** - для SYSTEMSTORE - используется хранилище сертификатов MS Windows (реестр LOCAL_MACHINE); **FileName='имя файла'** – используется файловое хранилище сертификатов Авест; **HSM -** используется устройство программно-аппаратного хранения информации AvHSM-Bign; **Provider=MSDASQL.1 -** используется сетевой справочник Авест, с хранением сертификатов в базе данных MySQL (определяется параметром **DRIVER**); **Provider=OraOLEDB.Oracle.1 –** используется сетевой справочник Авест, с хранением сертификатов в базе данных Oracle; **DRIVER='имя' -** имя драйвера для доступа к базе данных MySQL; **SERVER='имя'** – имя (IP адрес) сервера базы данных MySQL; **PORT='номер' –** номер порта сервера базы данных MySQL; **DATABASE='имя'** – имя базы данных MySQL; **Data Source='имя'** – имя базы данных Oracle; **User ID='имя'** – имя пользователя базы данных; **EncryptPassword='пароль'** – зашифрованный пароль для доступа к базе данных; **UsesContainer='True/False'–** для авторизации сертификаты выбираются/не выбирается из контейнеров личных ключей; **PUB_KEY_ID='идентификатором ключа'** – для авторизации использовать сертификат с заданным идентификатором ключа; **COMMON_NAME='имя'** – для авторизации использовать

		сертификаты с заданным атрибутом имени субъекта (общие данные); **PASSWORD_KEY='пароль'** – пароль для доступа к контейнеру личных ключей.
	DbType='тип базы данных'	Указывается тип базы данных.
	CryptoKI='True/False'	Указывает на использование интерфейса PKCS#11 для взаимодействия с программно-аппаратными средствами ЭЦП
[CSP] Параметры криптопровайдера.	**PROVNAME**='имя'	Указывается имя криптопровайдера.
	PROVTYPE='тип'	Указывается тип криптопровайдера.
	KEYSPEC='тип'	Указывается тип ключа: **1** - AT_KEYEXCHANGE, **2** - AT_SIGNATURE.
	HASHALGORITHM='OID'	Указывается OID алгоритма хеширования, если требуется отличный от значения криптопровайдера по умолчанию.
	PublicKeyObjId='OID'	Указывается OID открытого ключа.
	ENCRYPTALGORITHM='OID'	Указывается OID алгоритма шифрования.
	NeedPassword='True/False'	Для открытия контейнера требуется/не требуется пароль.
	NeedEnumContainer='True/False'	При авторизации производится/не производится предварительный поиск личного контейнера.
	FullFindCertForPublicKey='True/False'	Поиск сертификата, соответствующего личному ключу, производится по открытому ключу/по идентификатору открытого ключа.
	KeyIdentifierType='алгоритм'	Указывается алгоритм расчета идентификатора ключа: **0** - SHA1 от открытого ключа, **1** - как у Майкрософта (вызов функции CryptHashPublicKeyInfo), **2** – 20 байт хэш-значений согласно СТБ 1176.1-99 от открытого ключа.
	HASH_ALGID='алгоритм'	Указывается алгоритм хеширования, если требуется отличный от значения криптопровайдера по умолчанию.
	CSPFlags='значение'	Указывается дополнительное значение флага, передаваемое в функцию CryptAcquireContext.
	DblCERT='True/False'	Добавление возможности использования раздельных сертификатов для подписи и шифрования
	FullParameters='True/False'	Кодирование параметров открытого ключа по значению/по ссылке.
	FullAuthorityKeyId='True/False'	Дополнительно включить/не включать в дополнение сертификата AUTHORITY_KEY_IDENTIFIER

		издателя и серийный номера сертификата.
	UseMSCryptoApi2ToSignCertificate='True/False'	Использовать функцию CryptSignAndEncodeCertificate MS Crypto Api 2 для создания сертификата (по умолчанию используется MS Crypto Api 1 и функции AvBelCert.dll).
	CRYPT_FORCE_KEY_PROTECTION_HIGH='True/False'	Настройка для AvBign. Включает режим "высокой настороженности": запрос на ввод пароля появляется при каждом обращении к контейнеру.
[RDRB] Специальные настройки кодирования сертификатов/СОС согласно РД РБ 07040.1206-2004, противоречащие X 509	**OID_CRLNumber=**'OID'	Указывается OID дополнения с номером СОС.
[DEBUG] Отладочный лог. По умолчанию закомментирован. Для использования нужно удалить символ **;**	**LogFileName=**'имя файла'	Указывается имя файла отладочного лога.
[CommonName] Алгоритм получения краткого имени субъекта	**OID=**'значение атрибута'	Указывается значение атрибута с указанным OID, включается в краткое имя.
	Text='текст'	Текст, включаемый в краткое имя.
[LocalizeReasonName] Локализованное наименование причин отзыва сертификатов. Диапазон кодов причин отзыва от 1 до 18.	Код причины='наименование'	Указывается локализованное наименование причины отзыва сертификата.
	Код причины =NotUsed	Указывается, если код причины не используется.
[RDN] Локализованное наименование атрибутов имени субъекта.	**OID=**'наименование'	Указывается локализованное наименование атрибута имени субъекта с указанным OID.
[PERIOD] Сроки действия сертификатов/СОС по умолчанию**.** Значения определяется политикой удостоверяющего центра.	**MAX_CERTCA_MONTH_AFTER=**'месяцев'	Указывается срок действия сертификата удостоверяющего центра в месяцах.
	MAX_CERT_MONTH_AFTER='месяцев'	Указывается срок действия сертификата в месяцах.
	DayNextCRL='дней'	Указывается срок действия СОС в днях.
[PublicKeyOID_'тип криптопровайдера'] OID открытого ключа для установления связи между контейнером личных ключей и	**OID=**'OID открытого ключа'	Указывается OID открытого ключа для установления связи между контейнером личных ключей и сертификатом.

сертификатом для указанного типа криптопровайдера.		
[ENCRYPTALGORITHMS]	'**идентификатор открытого ключа сертификата, на который мы шифруем**'='алгоритм шифрования'	Указывается идентификатор открытого ключа сертификата, на который мы шифруем и алгоритм шифрования. Если шифруем на несколько получателей - алгоритм шифрования берется для первого. Если в ENCRYPTALGORITHMS не найден алгоритм открытого ключа - берется алгоритм из секции CSP.
[OCSP] Автоматическое использование сервисов OCSP и CDP (точек распространения COC), вызывается при любой проверке валидности сертификата.	**CDPCheckPeriod**='минут'	Указывается период проверки CDP, если CDP задано в сертификате. Если CDPCheckPeriod не задан или =0, CDP не проверяется.
	UseOCSPforCheckCert='True/False'	Использовать сервис OCSP для проверки сертификатов открытых ключей, если authorityInfoAccess OCSP задан в сертификате или CN издателя задано в секции [OCSPServers].
	UseOCSPforCheckAttributeCert='True/False	Использовать сервис OCSP для проверки атрибутных сертификатов, если authorityInfoAccess OCSP задан в сертификате или CN издателя задано в секции [OCSPServers].
[OCSPServers]	**'CN издателя сертификата'**='адрес OCSP сервера'	Указываются адреса серверов OCSP.
[AttributeCert]	**UseAttributeCertForSubject**='True/False'	Атрибутный сертификат привязывается к Subject сертификата, а не к конкретному сертификату (если TRUE).
	ReMakeAttributeCert='True/False'	Можно выпустить атрибутный сертификат с такими же атрибутами, если атрибутный сертификат отозван, или истек его срок действия (если TRUE).
	CheckPeriodAttributeCert='True/False'	Не давать выпустить атрибутный сертификат со сроком больше, чем исходный СОК (если TRUE).
[certLookup] Указание адреса сервера УЦ для импорта сертификатов с сервера УЦ	**URL**='адрес сервера УЦ'	Указывается адрес сервера УЦ.
[HttpProxy] Задание настроек для подключения к прокси серверу	**ProxyServer**='адрес прокси сервера'	Указывается адрес прокси сервера.
	ProxyPort='порт для подключения прокси'	Указывается порт для подключения прокси.
	ProxyUsername=имя пльзователя для подключения прокси'	Указывается имя пользователя для подключения прокси с авторизацией.
	ProxyPassword='пароль для подключения прокси'	Указывается пароль для подключения пользователя прокси с авторизацией.

	BasicAuthentication=TRUE	Указывается параметр подключения к прокси серверу (`TRUE` - с авторизацией, `FALSE` - без авторизации).
	ReadTimeOut=180	Указывается промежуток времени (в секундах), в который программа ожидает ответ от сервера (180 секунд по умолчанию).
[TLS] Задание протокола TLS для установки защищенного соединения	Protocol=TLS 1.0	Устанавливается протокол TLS 1.0
	Protocol=128	Устанавливается протокол TLS 1.0
	Protocol=TLS 1.1	Устанавливается протокол TLS 1.1
	Protocol=512	Устанавливается протокол TLS 1.1
	Protocol=TLS 1.2	Устанавливается протокол TLS 1.2
	Protocol=2048	Устанавливается протокол TLS 1.2

ПРИЛОЖЕНИЕ 3

Пример конфигурационного файла AvCmMsg.ini

```
[LOGIN]
CONNECTSTR=SYSTEMSTORE

[CSP]
NeedEnumContainer=False
ProvType=423
PublicKeyObjId=1.2.112.0.2.0.34.101.45.2.1
ENCRYPTALGORITHM=1.2.112.0.2.0.34.101.31.33

[DEBUG]
;LogFileName=AvCmDebug.log

[DefFileName]
2.5.4.3=

[CommonName]
2.5.4.3=

[RDN]
2.5.4.10=Сокращенное название организации
1.2.112.1.2.1.1.1.2=УНП организации
2.5.4.4=Фамилия
2.5.4.41=Полное название организации
1.3.6.1.5.5.7.9.1=Дата рождения
2.5.4.6=Код страны
2.5.4.8=Область
2.5.4.7=Населенный пункт
2.5.4.11=Подразделение
2.5.4.12=Должность
1.3.6.1.4.1.12656.5.1=Место работы и должность
1.3.6.1.4.1.12656.5.3=Данные из документа, удостоверяющего личность
2.5.4.9=Адрес
2.5.4.3=Общее имя
1.2.840.113549.1.9.1=Адрес электронной почты
1.2.112.1.2.1.1.2.1=Бланк карточки открытого ключа
```

```
2.5.4.42=Имя отчество
2.5.4.5=Идентификационный (личный) номер
2.5.4.97=Идентификатор организации

[AliasOID]
CN=2.5.4.3
O=2.5.4.10
SN=2.5.4.4
IO=2.5.4.41
C=2.5.4.6
L=2.5.4.7
S=2.5.4.8
STREET=2.5.4.9
OU=2.5.4.11
T=2.5.4.12
E=1.2.840.113549.1.9.1

[PERIOD]
MAX_KEYCA_MONTH_AFTER=180
MAX_CERTCA_MONTH_AFTER=180
MAX_KEY_MONTH_AFTER=24
MAX_CERT_MONTH_AFTER=24
DayNextCRL=30
NoticeDayCert=3
NoticeDayCRL=1

[PublicKeyOID_423]
1.3.6.1.4.1.12656.1.37=1.3.6.1.4.1.12656.1.37

[AttributeCert]
UseAttributeCertForSubject=True
CheckPeriodAttributeCert=False
ReMakeAttributeCert=True

[OCSP]
UseOCSPforCheckCert=True
UseOCSPforCheckAttributeCert=True
```

```
[OCSPServers]
Подчиненный удостоверяющий центр=http://10.0.1.20:8081/responder/
Служба атрибутных сертификатов=http://10.0.1.20:8081/responder/

[certLookup]
URL=https://test.nces.by/certdb/certificates/v1/

[TLS]
Protocol=TLS 1.0
;Protocol=128

;Protocol=TLS 1.1
Protocol=512

Protocol=TLS 1.2
;Protocol=2048

;[HttpProxy]
;ProxyServer=10.1.0.50
;ProxyPort=3128
;ProxyUsername=user
;ProxyPassword=password
;BasicAuthentication=TRUE
;ReadTimeOut=180
```

ПРИЛОЖЕНИЕ 4

Настройка сетевого подключения к базе данных

1. Настройка сетевого доступа к базе данных на Oracle

Если установка производится с использованием сетевой базы Oracle, то (см. Рисунок 126 Настройка сетевого подключения к БД на Oracle) надо:

- в группе «База данных сертификатов» указать наименование источника данных, настроенного на локальном компьютере для доступа к базе данных сервера Oracle, имя и пароль доступа администратора базы данных Oracle и нажать кнопку «Проверить подключение». При этом будет проверено, существуют ли в указанной базе данных таблицы, необходимые для работы программы, и при необходимости таблицы и другие объекты базы данных будут созданы;
- в группе «Пользователь БД» ввести, или выбрать из существующих имя пользователя, используемое при подключении к базе данных и ввести его пароль. Список уже зарегистрированных пользователей становится доступным только после нажатия на кнопку «Проверить подключение», выполняемое на предыдущем шаге. При этом в список пользователей помещаются только те пользователи, которые обладают достаточными правами для работы с таблицами базы данных удостоверяющего центра;
- если было введено новое имя пользователя, то требуется нажать кнопку «Создать пользователя БД» при этом в базе данных будет создана учетная запись, с правами доступа к таблицам базы данных удостоверяющего центра.

Внимание: Не рекомендуется вводить новое имя пользователя при установке с обновлением программного обеспечения, следует согласиться с указанным в данном поле именем пользователя.

- далее следует нажать кнопку «Проверить подключение», чтобы убедится в том, что параметры подключения к базе данных введены корректно;
- нажать кнопку «Сохранить конфигурацию» для сохранения настроек сетевого подключения.

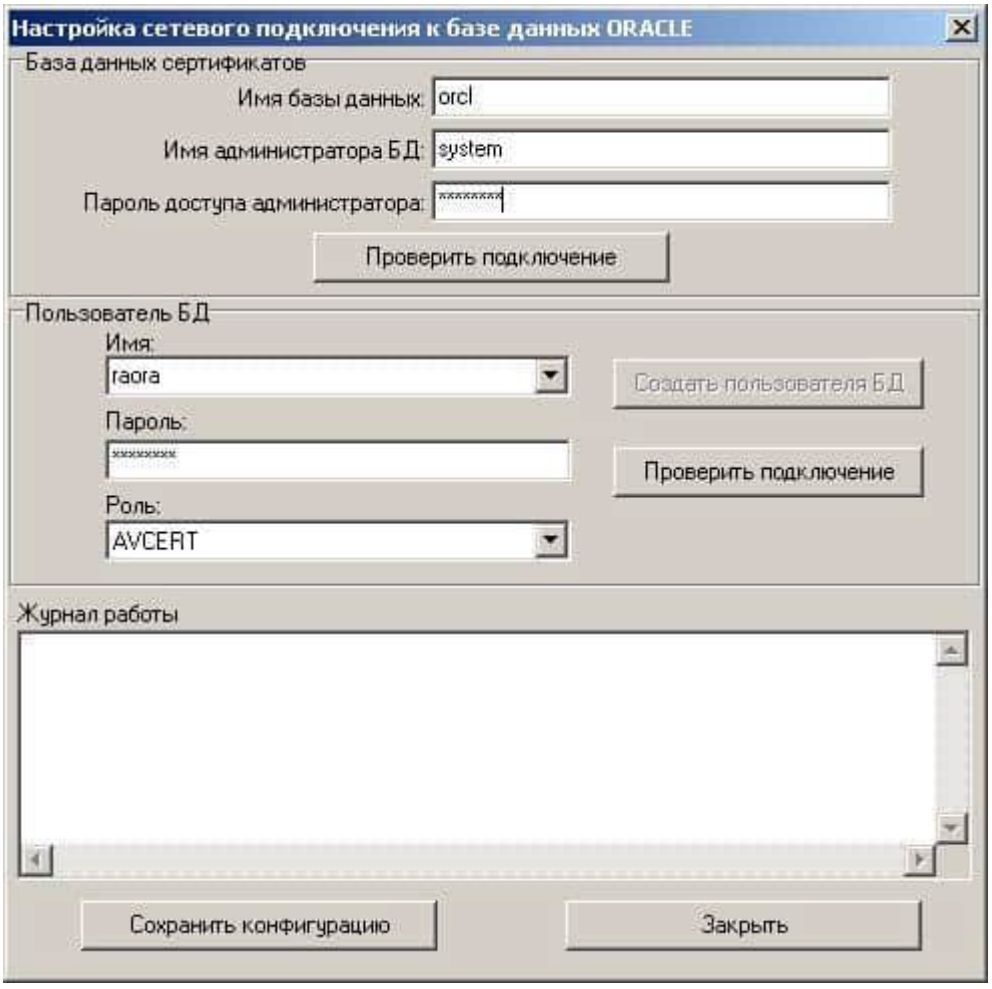


Рисунок 126 Настройка сетевого подключения к БД на Oracle

2. Настройка сетевого доступа к базе данных на MySQL

Если установка производится с использованием сетевой базы MySQL, то (см. Рисунок 127. Настройка сетевого подключения к БД MySQL) надо:

- в группе «Сервер MySQL» указать имя сервера БД MySQL или его IP-адрес и номер порта сервера MySQL;
- в группе «База данных сертификатов» указать имя существующей или создаваемой базы данных и имя, и пароль администратора сервера MySQL и нажать кнопку «Проверить подключение». При этом будет произведена попытка подключения администратора к серверу MySQL, поиск и при необходимости создание базы данных, создание схемы базы данных (таблиц и других объектов);
- в группе «Пользователь БД» ввести новое, или выбрать из существующих имя пользователя, которое будет в последствии использоваться при доступе к базе данных, и ввести его пароль;
- если было введено новое имя пользователя, то необходимо нажать кнопку «Создать пользователя БД». При этом будет создан новый пользователь базы данных, и ему будут предоставлены права для использования требуемых таблиц;

Внимание: Не рекомендуется вводить новое имя пользователя при установке с обновлением программного обеспечения, следует согласиться с указанным в данном поле именем пользователя.

- затем необходимо нажать кнопку «Проверить подключение», для того чтобы убедится, что заданный пользователь существует, задан правильный пароль пользователя, и требуемые права указанному пользователю предоставлены;
- Нажать кнопку «Сохранить конфигурацию» для сохранения настроек подключения к базе данных в конфигурационных файлах программы «Центр цифровых сертификатов Авест».

На этом процедура установки с обновлением программного обеспечения ПО «Центр цифровых сертификатов Авест» завершена.

В последнем окне мастер установки программы надо нажать кнопку «Завершить».

Внимание: Рекомендуется после проведения установки с обновлением базы данных сертификации, проверить целостность базы данных сертификации на наличие ошибок и, в случае их обнаружения, устранить их.

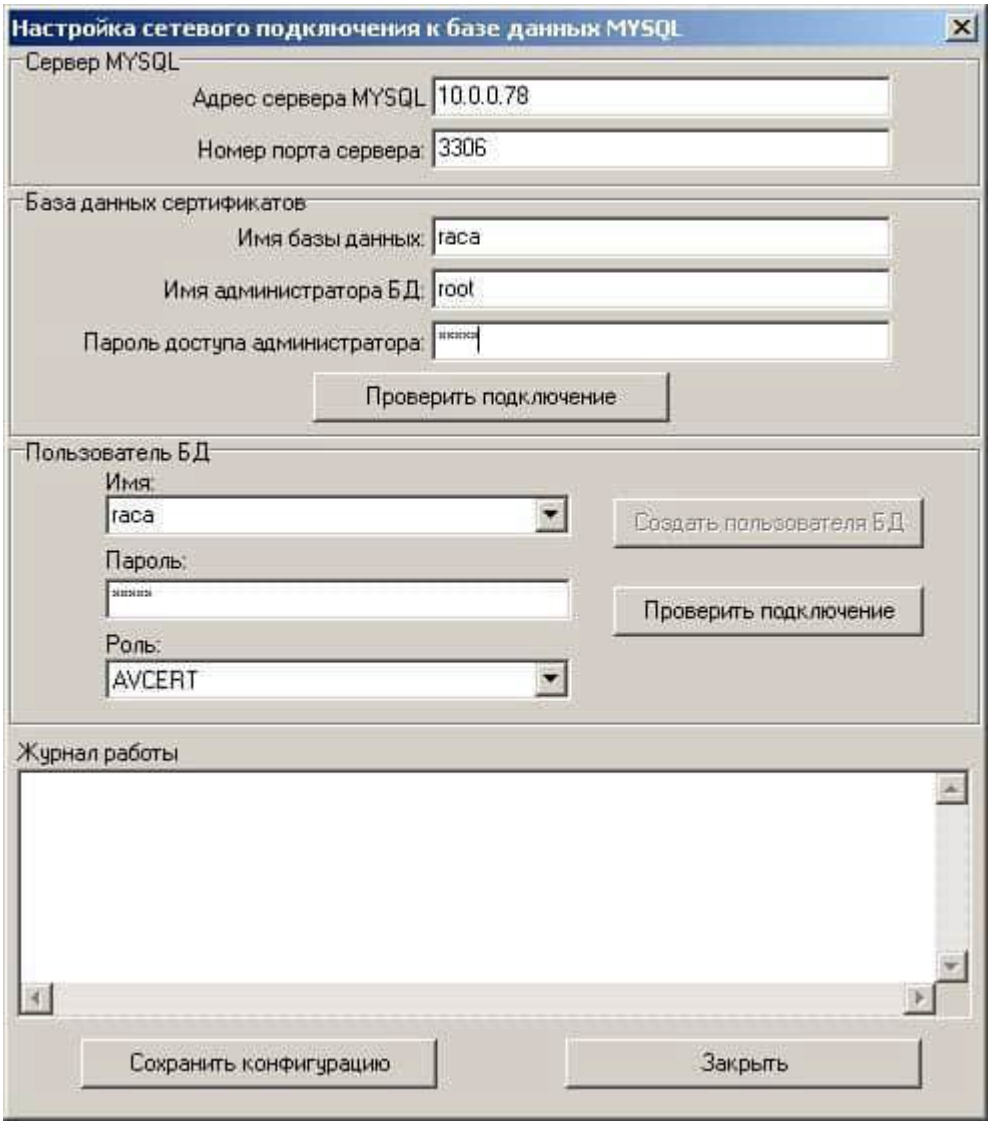


Рисунок 127. Настройка сетевого подключения к БД MySQL

11. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС – атрибутный сертификат;

БД – база данных;

ИОК – инфраструктура открытых ключей;

ИУП – инфраструктура управления привилегиями;

КУЦ – корневой удостоверяющий центр;

НЖМД - накопитель на жёстких магнитных дисках;

НКИ – носитель ключевой информации;

ОО – объект описания;

ПК – программный комплекс;

ПО – программное обеспечение;

ПСКЗИ – программное средство криптографической защиты информации;

ПУЦ – подчиненный удостоверяющий центр;

ПЭВМ – персональная электронно-вычислительная машина;

САС – служба атрибутных сертификатов;

СОК – сертификат открытого ключа;

СОС – список отозванных сертификатов;

ТНПА – технические нормативные правовые акты;

УЦ – удостоверяющий центр;

ФЛ – физическое лицо;

ЦР – центр регистрации;

ЦС – центр сертификации;

ЭЦП – электронная цифровая подпись;

ЮЛ – юридическое лицо;

ЮП – юридический представитель;

OCSP (Online Certificate Status Protocol) – онлайновый протокол проверки статуса сертификата, определенный в СТБ 34.101.26;

TLS (Transport Layer Security) – протокол защиты транспортного уровня, определенный в СТБ 34.101.65.

Лист регистрации изменений

Номер листов (страниц)					Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	Измененных	Замененных	Новых	Аннулированных					