Краткие инструкции по установке:

Криптопровайдера «Avest»;
Персонального менеджера сертификатов «Avest»;
Системы «Интернет-Клиент».

2016 г.

Содержание

!!! Зайдите на сайт rbank.by, раздел Юридические лица ->Интернет Банк -> Скачайте «Комплект Абонента»

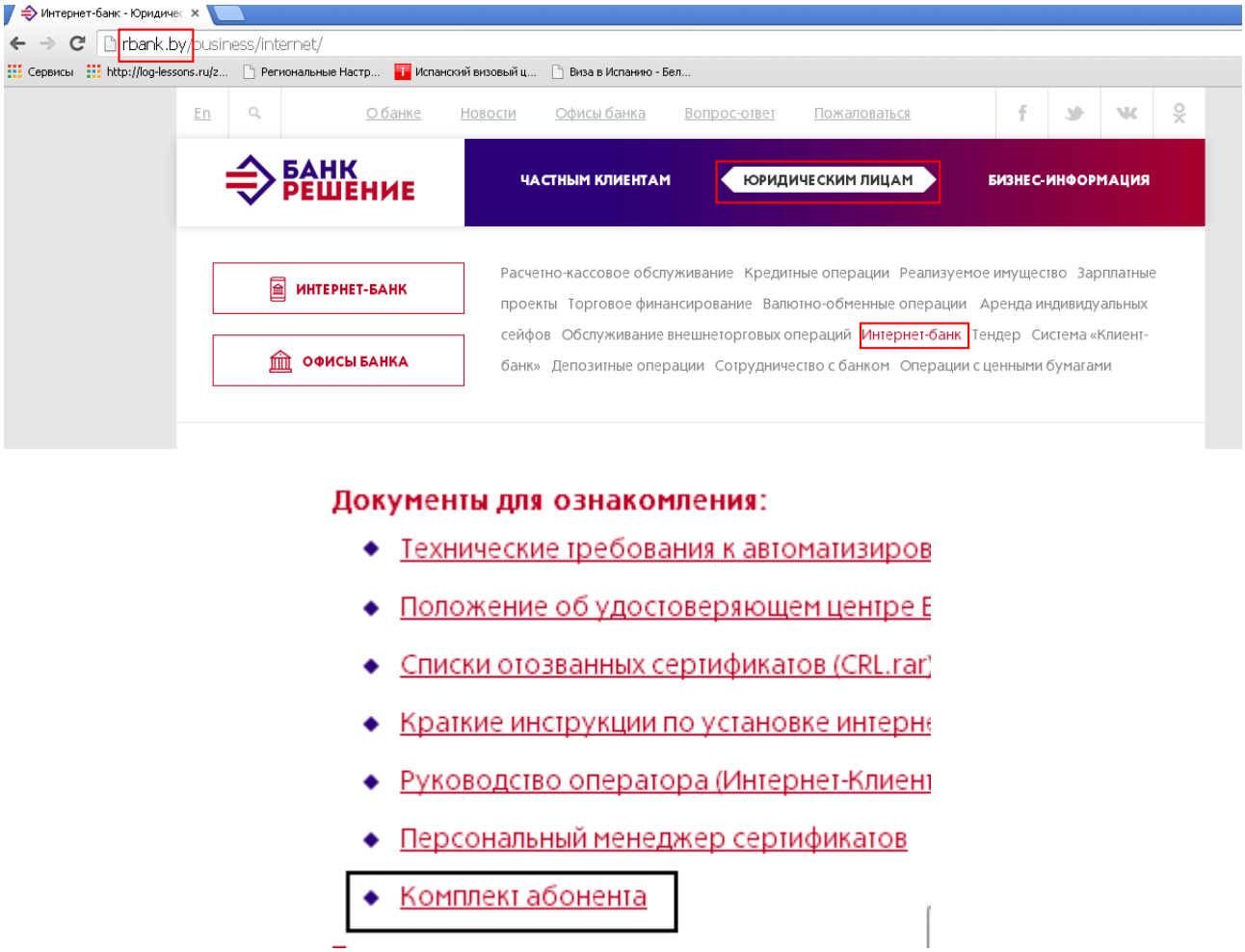

Рисунок 1 – Скачивание «Комплекта абонета»

1. Установка криптопровайдера «AVEST».

Все установки необходимо производить только с правами **!!!** **локального администратора.**

Действия по установке криптопровайдера:

1) Запустить с CD диска программу ***setupAvCSP6.1.0.741.exe*** (*КОМПЛЕКТ АБОНЕНТА\Avest\AvCSP*);

2) В первом окне мастера установки содержится описание устанавливаемого продукта, для начала установки программы на компьютер нажмите кнопку «*Далее*» (см. Рис. 2).

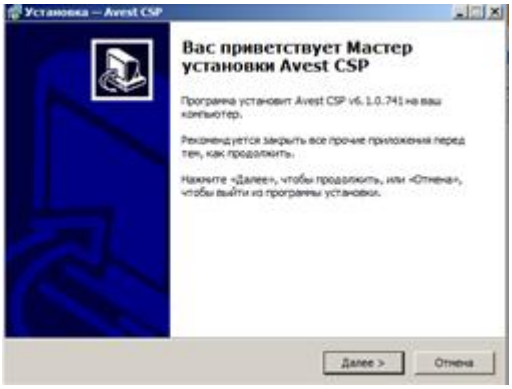

Рисунок 2 – Заставка мастера установки криптопровайдера

Почти все окна программы установки имеют 3 кнопки: «*<Назад*», «*Далее>*», «*Отмена*». Нажатие на кнопку «*<Назад*» приводит к возврату к предыдущему окну программы установки. Нажатие на кнопку «*Далее>*» позволяет перейти к следующему окну программы установки. Нажатие на кнопку «*Отмена*» приведет к выходу из программы установки.

3) После нажатия на кнопку «*Далее*» будет приведена страница с лицензионным соглашением, условия которого надо изучить и, в случае согласия с лицензионным соглашением, нажать на кнопку «*Далее*» для продолжения установки (см. Рис. 2.1).

Если Вы не согласны с условиями указанными в лицензионном соглашении, то нажмите на кнопку «*Отмена*» для выхода из программы установки.

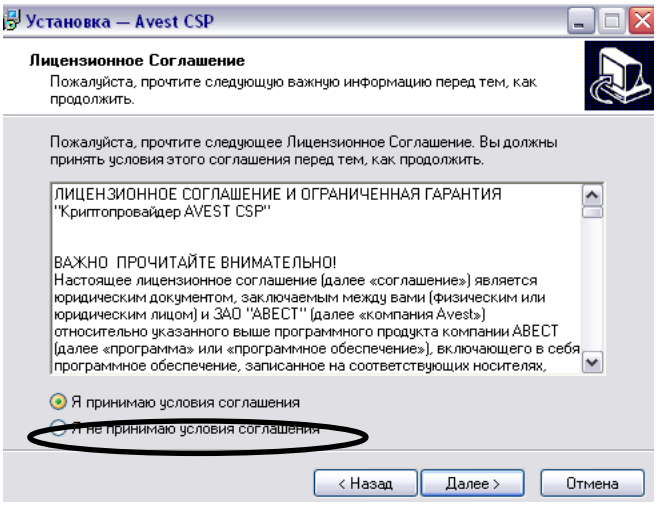

Рисунок 2.1 – Лицензионное соглашение

4) После этого надо определить основной каталог, в котором будут расположены устанавливаемые компоненты, и нажать кнопку «*Далее*». По умолчанию установка программы производится в каталог «*\Program Files\Avest\ Avest CSP*» на системном диске (см. Рис. 3).

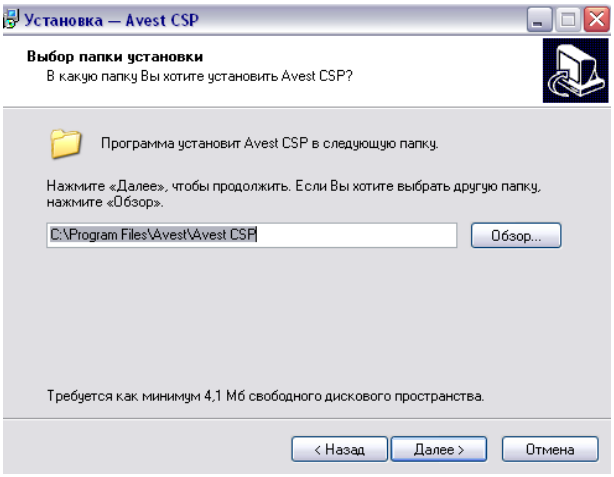

Рисунок 3 – Выбор каталога установки

5) Следующим шагом является выбор папки в меню «*Пуск*», в которой будут созданы ярлыки программы для быстрого её запуска.

Название папки Вы можете указать как вручную, так и при помощи кнопки «*Обзор*». По умолчанию будет создана папка «*Авест*» (См. Рис.4).

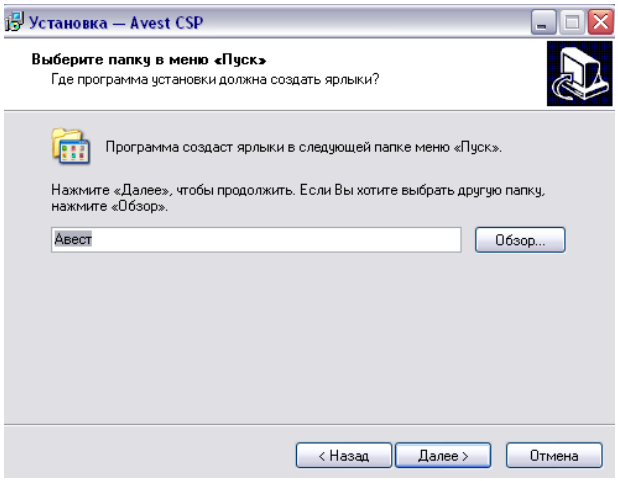

Рисунок 4 – Выбор папки для создания ярлыков в меню «Пуск»

6) На следующей странице мастера установки предлагается выбрать тип носителя, который будет использоваться для хранения личных ключей по умолчанию (Это значит, что при создании личного ключа первым будет предложен этот носитель) (См. Рис. 5).

Чтобы использовать несколько носителей, нужно включить соответствующую опцию. Включенный флажок на любом из носителей в списке означает, что указанный носитель или несколько носителей будут использоваться для хранения личных ключей пользователя, с которым пользователь сможет работать в программном обеспечении.

Так же можно нажать на кнопку «*Отметить все*», и при работе с ПО, пользователь сможет использовать любой тип носителя, поддерживаемый данным криптопровайдером.

Или нажать кнопку «*Снять отметку со всех*», тогда будет использоваться один носитель, который выставлен по умолчанию.

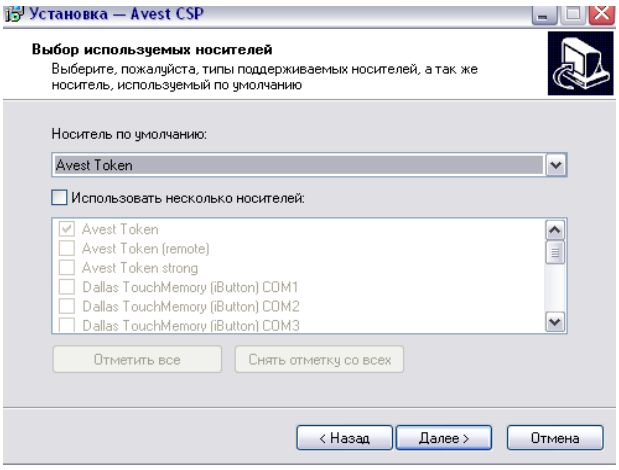

Рисунок 5 – Выбор носителя личных ключей по умолчанию.

7) Теперь всё готово для установки программы на компьютер, о чем сообщает следующее окно мастера установки. В нём отражена информация о последовательности действий пользователя при установке криптопровайдера (описанных выше), (См. Рис. 6). Если пользователь согласен с указанными в данном окне параметрами, то надо нажать кнопку «*Установить*».

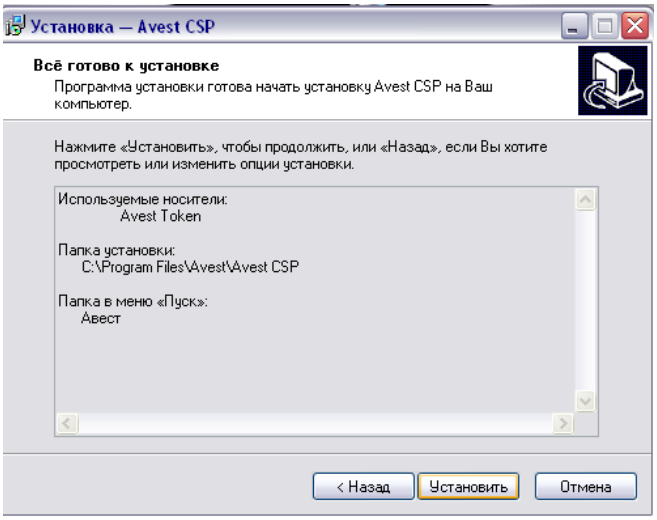

Рисунок 6 – Установка криптопровайдера на компьютер

После этого будет произведена распаковка, копирование файлов и регистрация библиотек на компьютере.

8) Далее необходима регистрация криптопровайдера, для этого нужно некоторое количество случайных данных, необходимо «*подвигать мышью*» в пределах следующего появившегося окна. (См. Рис. 7) .

Примечание. При повторной инсталляции данное окно появляться не будет.

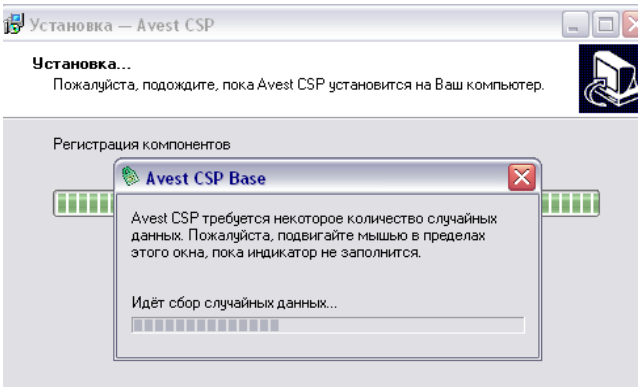

Рисунок 7 – Сбор случайных данных для регистрация криптопровайдера

На этом мастер установки криптопровайдера закончит свою работу, о чем сообщается в последнем окне (См. Рис. 8). Нажмите кнопку «*Завершить*».

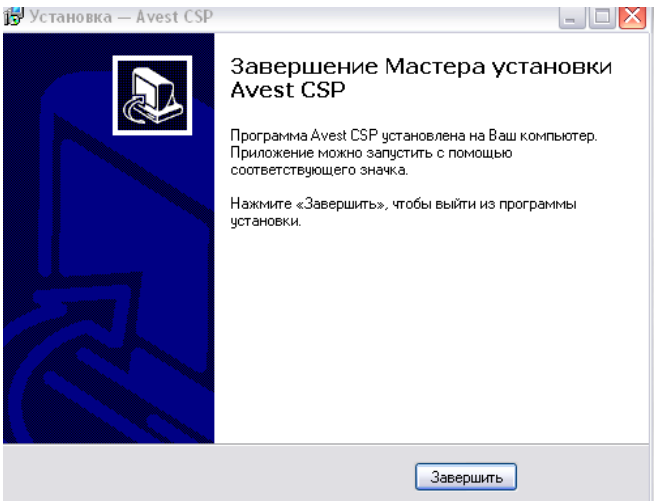

Рисунок 8 – Завершение установки криптопровайдера

После установки криптопровайдера на компьютер в меню «*Пуск*» → «*Программы*» → «*Авест*» появляется ярлык программы «*Avest CSP*».

Более подробное описание криптопровайдера «*Avest CSP*» смотрите *\КОМПЛЕКТ АБОНЕНТА\Avest\Docs**AvCSP_POn.pdf***

2. Установка персонального менеджера сертификатов «AVEST».

Действия по установке ПК *AvPCM*:

1) Запустить с дистрибутива программу ***AvPCMEx_setup.exe*** (*КОМПЛЕКТ АБОНЕНТА\Avest\AvPCMTrust*).

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. Рис.9).

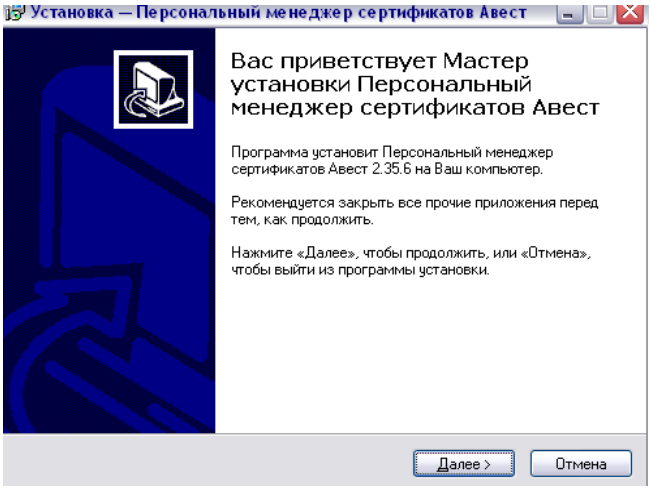

Рисунок 9 – Заставка начала инсталляции ПК *AvPCM*

В следующем окне установки ПК *AvPCM* оговариваются условия лицензионного соглашения. Для продолжения процедуры инсталляции надо принять условия лицензионного соглашения и нажать кнопку «*Далее*» (см. Рис.10).

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

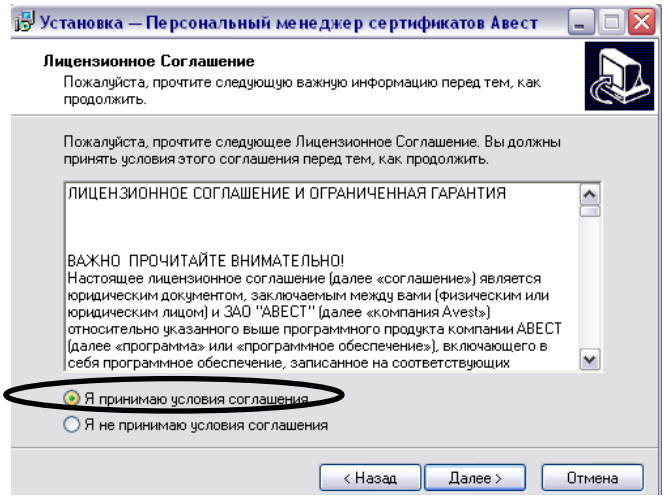

Рисунок 10 – Условия лицензионного соглашения

2) Определить основной каталог, в котором будут расположены устанавливаемые компоненты, по умолчанию это будет *C:\Program Files\Avest\AvPCM* и допишите **Trust** (без пробела) как показано на рисунке 11.

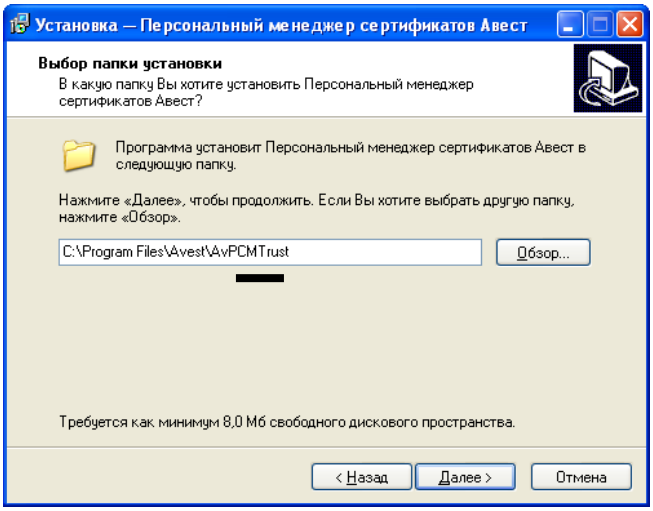

Рисунок 11 – Выбор каталога установки программы

3) Определить тип установки ПК *AvPCM*. В окне «*Выбор компонентов*» (см. Рис.12), требуется выбрать из встроенного списка тип установки программы – **!!! «*Инсталляция с базой данных сертификатов в реестре*»**, выбрать используемую базу данных и нажать кнопку «*Далее*» (см. Рис.13).

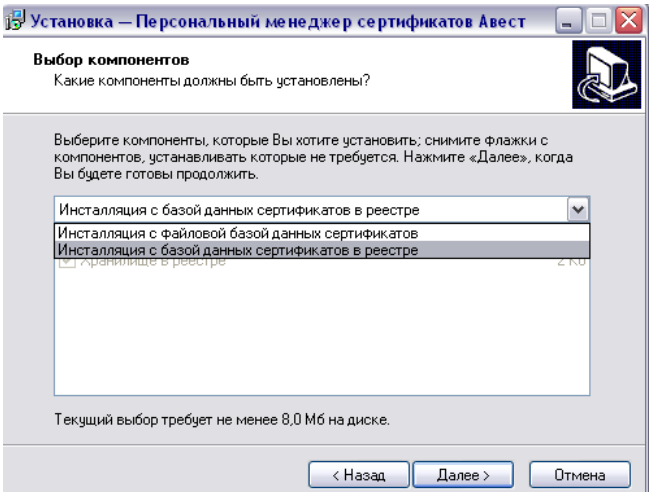

Рисунок 12 – Выбор компонентов

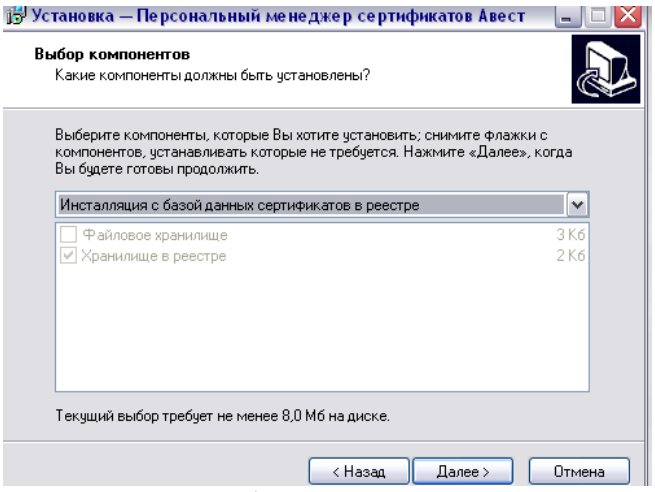

Рисунок 13 – Выбор компонентов

Следующая страница мастера установки проинформирует о том, что всё 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. Рис. 14).

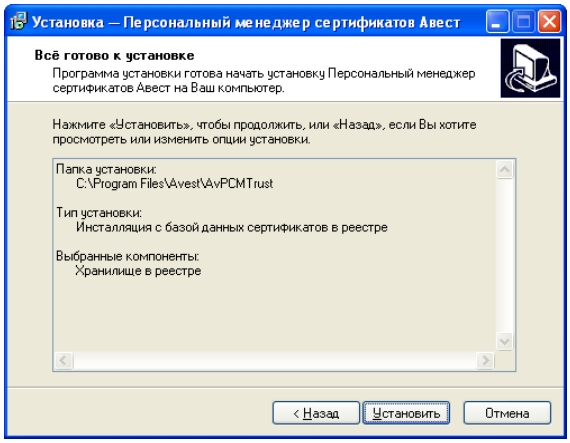

Рисунок 14 – Параметры установки программы

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. Рис. 15).

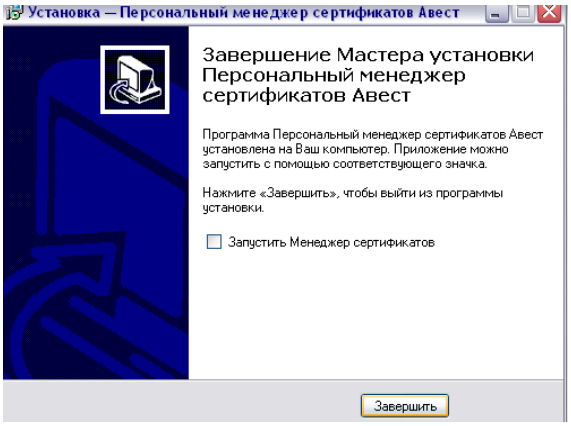

Рисунок 15 – Завершение работы мастера установки программы

После завершения программы установки раздел «*Программы*» в основном меню *Windows* → «*Пуск*» будет дополнен подразделом «*Авест*», который включает в себя следующие пункты:
– «*Персональный менеджер сертификатов Авест*»;
– «*Создать запрос на сертификат*»;
– «*Импорт сертификатов*».

На рабочем столе появится ярлык для быстрого запуска ПК *AvPCM*. (Персональный менеджер сертификатов Авест).

Более подробное описание менеджера сертификатов «*AvPCM.* » смотрите *\КОМПЛЕКТ АБОНЕНТА\Avest\Docs**AvPCM_POn.pdf***

3. Создание файловой структуры криптозащиты.

Запустите с CD диска файл ***create_str.bat*** *(\КОМПЛЕКТ АБОНЕНТА\BSS_Client\Command\)*
Который создаст каталоги:
*"C:\Program Files\Avest\AvPCMTrust**CERT****CA**"*
*"C:\Program Files\Avest\AvPCMTrust**CERT****CRL**"*
*"C:\Program Files\Avest\AvPCMTrust**CERT****PER**"*
*"C:\Program Files\Avest\AvPCMTrust**CERT****BANK**"*
В случае если после запуска ***create_str.bat*** каталоги, по каким либо причинам не создались, создайте папку ***CERT*** *(C:\Program Files\Avest\AvPCMTrust\)* и в неё скопируйте соответственно папки ***CA***, ***CRL***, ***PER***, ***BANK*** расположенные – *\КОМПЛЕКТ АБОНЕНТА\BSS_Client\Command*.

4. Настройка параметров Internet Explorer.

Перед началом установки ознакомьтесь с разделом 1 «Требование к аппаратно-программному обеспечению компьютера и настройкам Microsoft Internet Explorer» (стр. 6) (*\КОМПЛЕКТ АБОНЕНТА\BSS_Client\Docs**Руководство оператора (Интернет-Клиент).pdf***)
настройте параметры *Internet Explorer* описанные в разделе
1.4 «Настройка параметров Internet Explorer»

5. Генерация личного ключа и создание запроса на выпуск сертификата.

Запуск ПК *AvPCM* может производиться 2 способами:

1. Из основного меню *Windows*: «*Пуск*»→«*Программы*» →«*Авест*» →«*Персональный менеджер сертификатов Авест*»; 2. Щелкнув по ярлыку ПК *AvPCM (Персональный менеджер сертификатов Авест)*, находящемся на вашем Рабочем столе после инсталляции.

Если на компьютере уже используется АВЕСТ, выберите идентификатор ключевого контейнера соответствующий личному ключу пользователя, после чего поставьте «галочку» в поле «*Войти в систему без авторизации*» (см. Рис. 16) и нажмите «*ОК*», если же АВЕСТ ранее не использовался на Вашем компьютере, то появится окно: «**Менеджер сертификатов НЕ АВТАРИЗОВАН**» (см. Рис. 17).

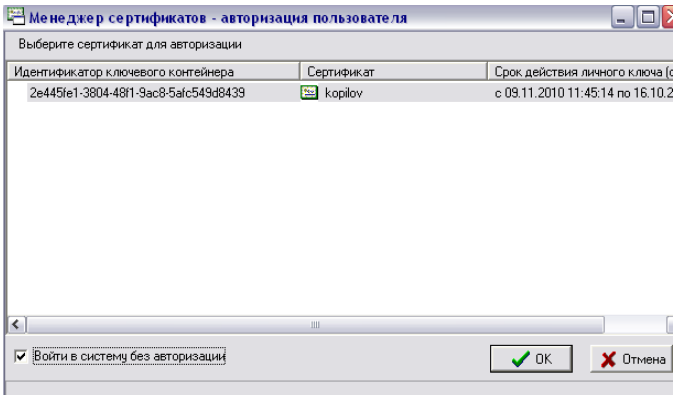

Рисунок 16 – Авторизация пользователя

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

Действия при создании запроса на сертификат:

1) Выбрать из основного меню *Windows*: «*Пуск*» →«*Программы*» → «*Авест*» → «*Персональный менеджер сертификатов*» → «*Создать запрос на сертификат*» (см. Рис. 17);

2) В появившемся окне мастера создания запроса на сертификат выбрать шаблон для создания сертификата – «*Сертификат юридического лица*» (см. Рис. 18);

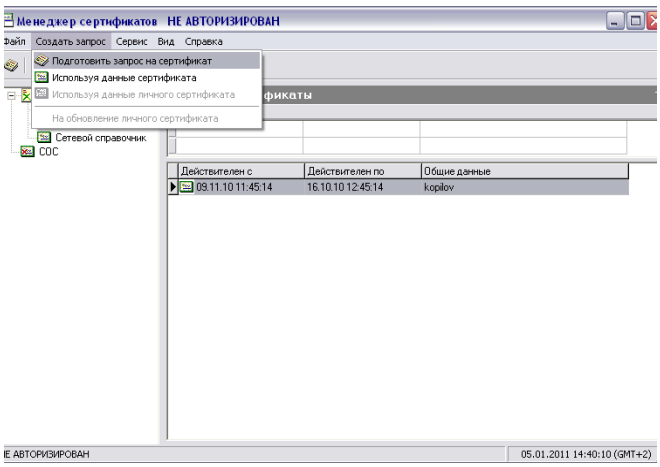

Рис. 17 – Создание запроса на сертификат

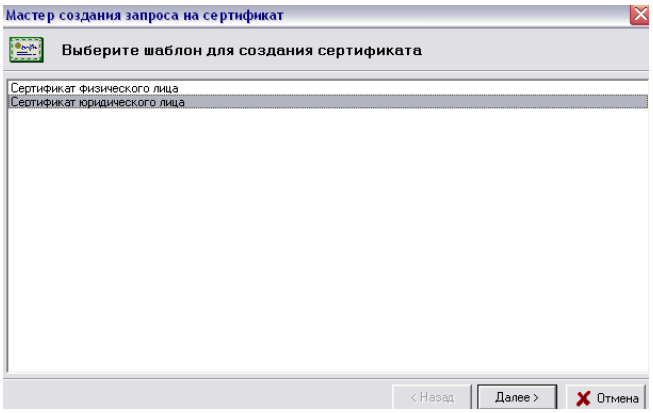

Рисунок 18 – Выбор шаблона для создания сертификата

3) В следующем диалоговом окне надо задать атрибуты будущего владельца сертификата для карточки открытого ключа, включаемые в запрос на сертификат (см. Рис. 19);

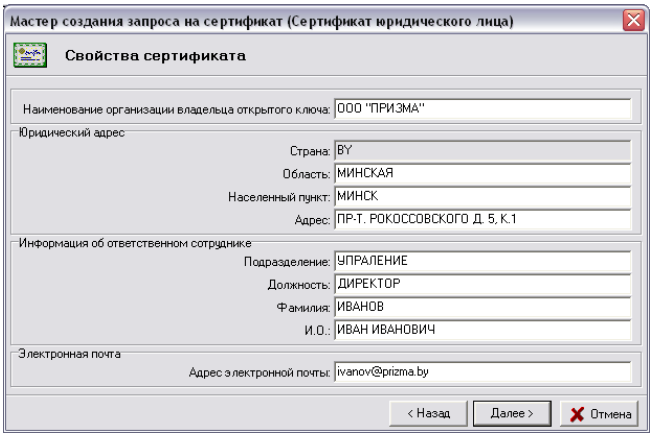

Рисунок 19 – Заполнение атрибутов владельца сертификата

Внимание: Эти атрибуты в дальнейшем изменять не рекомендуется. В связи с этим обращаем особое внимание на тщательность выполнения первой генерации личного ключа и заполнения атрибутов пользователя. В случае если, какое-либо из обязательных атрибутов не заполнен и была нажата кнопка «*Далее*», то программа сообщит об ошибке и предложит заполнить его значение. Затем появится окно, в котором будет указано применение личного ключа пользователя (см.Рис.20).

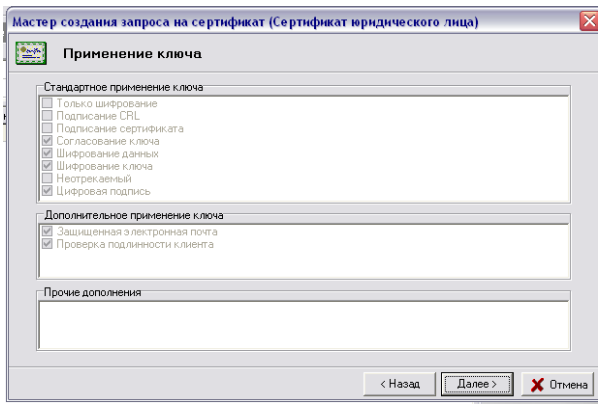

Рисунок 20 – Применение личного ключа

4) В следующем диалоговом окне надо определить срок действия сертификата пользователя (см. Рис. 21);

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

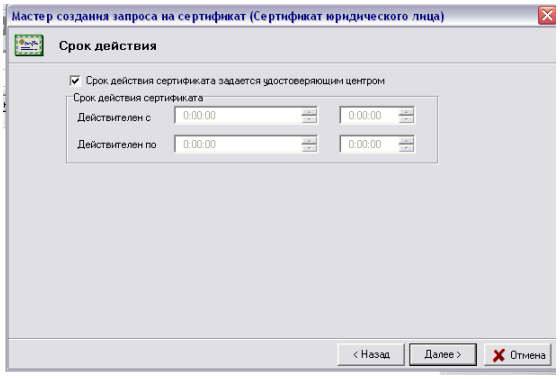

Рисунок 21 – Ввод сроков действия сертификата

5) Затем, в появившемся окне, надо задать имя контейнера, в который будет помещен Ваш личный ключ (см. Рис. 22).

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:*** измените поле «*время генерации*» на *УНП* Вашей организации_*Фамилия* владельца ключа, как показано на рисунке 22.1. (В случае перевыпуска сертификата поле должно быть следующего формата *УНП* Вашей организации_*Фамилия* владельца ключа**_2** и т.д.)

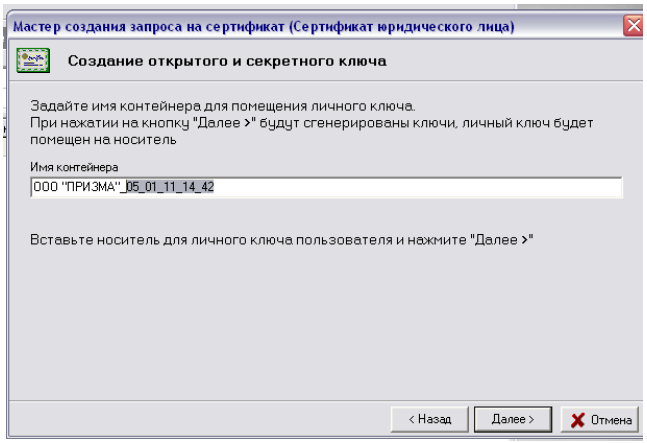

Рисунок 22 – Инициализация носителя личного ключа

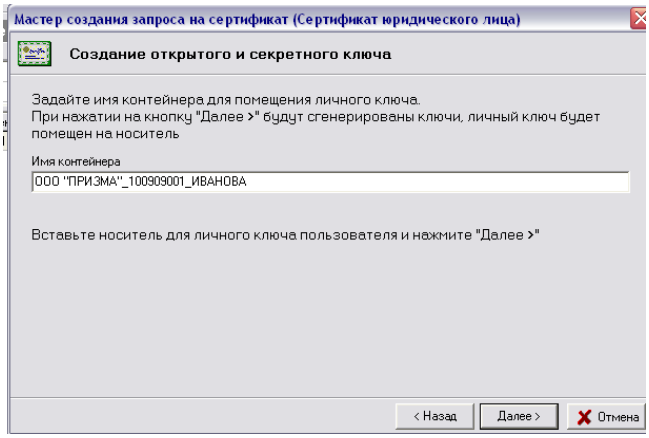

Рис 22.1 – Инициализация носителя личного ключа ЗАО «Банк «Решение»

6) Для инициализации контейнера личных ключей в появившемся далее диалоговом окне необходимо выбрать из списка физический носитель ключей, ввести в соответствующих полях пароль и его подтверждение и нажать «*ОК*»(см. Рис.23);

Важно: При вводе пароля обратите внимание на раскладку клавиатуры (RU/EN) и регистр символов.

(!!! Все иные USB устройства кроме носителя AvToken должны быть извлечены из USB портов).

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

восстановлению не подлежит.

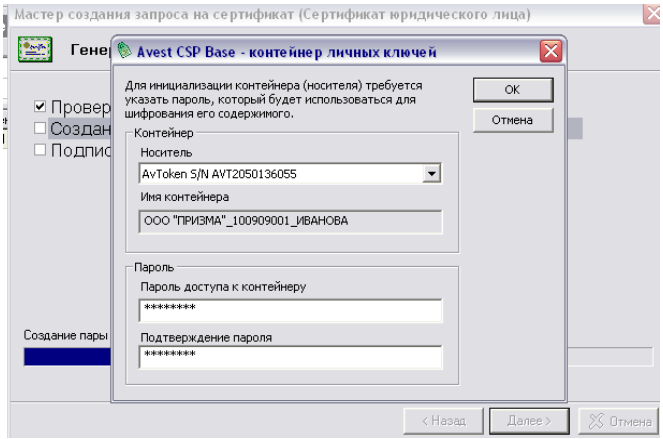

Рисунок 23 – Выбор физического носителя личного ключа

7) Для создания личных ключей программе требуется некоторое количество случайных данных, поэтому «*подвигайте» курсором мыши* в пределах появившегося окна до полного заполнения полосы индикации (см. Рис. 24);

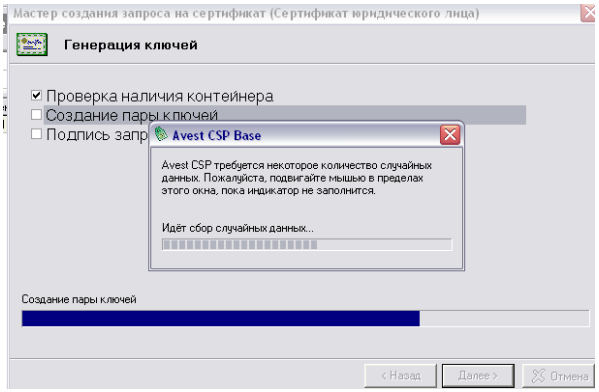

Рисунок 24 – Окно «сбор случайных данных»

8) После этого будет сформирована *карточка открытого ключа* (см. Рис.25), которую требуется распечатать в 2 экземплярах, подписать и поставить штамп организации (пример рис. 25.1), и передать в Банк 1 экземпляр карточки открытого ключа (**без карточки открытого ключа сертификат не может быть обработан**).

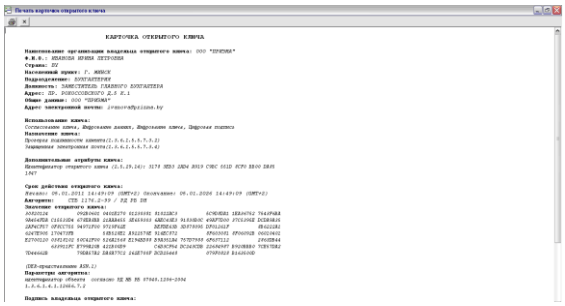

Рисунок 25 – Карточка открытого ключа

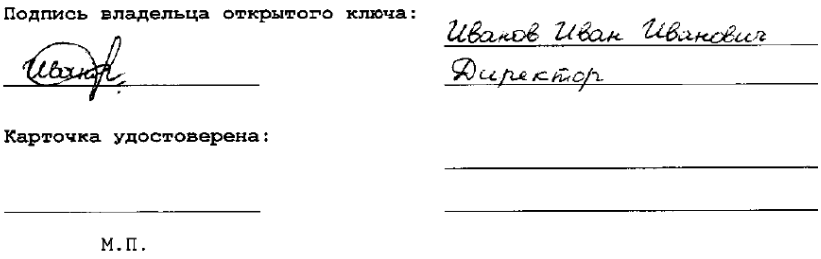

Рисунок 25.1 – Пример подписи карточки открытого ключа

Закройте карточку открытого ключа и включите флажок «*Экспортировать запрос в файл*» и указать имя файла. (см. Рис. 26). 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.

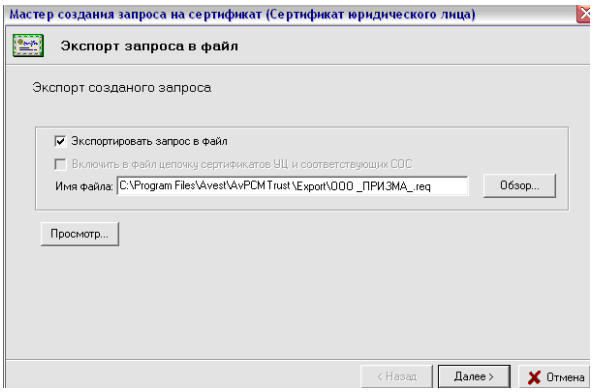

Рисунок 26 – Сохранение запроса

В случае успешного создания запроса на экране появится окно (см. Рис. 27). Для выхода из мастера создания запроса на сертификат нажмите кнопку «*Закрыть*».

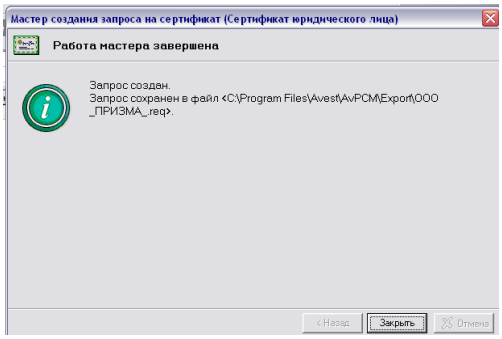

Рисунок 27 – Завершение работы мастера установки программы

6. Передача в Банк запроса на сертификат

Зайдите *C:\Program Files\Avest\AvPCMTrust\Export* и отправьте по электронной почте файл с расширением ***.req*** (например *ООО_ПРИЗМА_.req*) на адрес ibank@rbank.by с заголовком письма «**Запрос на сертификат_Название организации**», (для перевыпуска сертификата заголовок письма должен быть «**Запрос на перевыпуск сертификата_Название организации**»). Далее **!!! передайте в Банк карточку открытого ключа** с подписью и печатью организации (без карточки открытого ключа сертификат не может быть обработан).

7. Получение из Банка файлов сертификатов.

После отправки запроса, ожидайте «*ответное*» письмо на Ваш электронный ящик, в котором будут содержаться заархивированные сертификаты с расширениями ***.cer*** (например *cl_1708.cer*) и ***.p7b*** (например *cl_1708.p7b*). Полученные файлы необходимо разархивировать архиватором ***WinRAR*** (***пароль архива будет выдан в Банке после получения Вами данных сертификатов*** (см. 9 раздел данной инструкции), в случае перевыпуска сертификата используйте пароль для *WinRaR* выданный Вам ранее) и переложить сертификаты в папку *PER*. ***(C:\Program Files\Avest\AvPCMTrust\CERT\PER\).***

8. Импорт сертификата.

Зайдите в «*Персональный менеджер сертификатов Авест*», щелкнув по ярлыку ПК *AvPCM* (*Персональный менеджер сертификатов Авест*), находящемся на Рабочем столе. Если на компьютере уже используется АВЕСТ поставьте «галочку» в поле «*Войти в систему без авторизации*» (см. Рис. 28) и нажмите «*ОК*», если же не использовался (см. Рис.29).

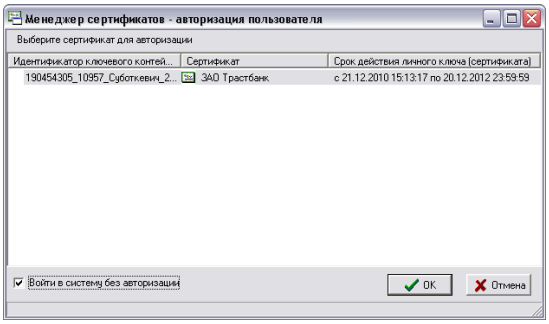

Рисунок 28 – Авторизация пользователя

Затем нажмите «*Файл*»→ «*Импорт сертификата/СОС*» (см. Рис. 29)

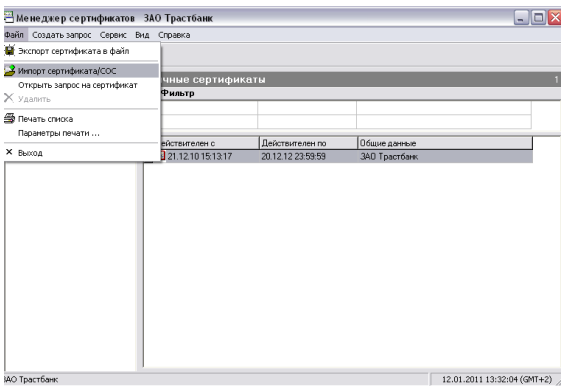

Рисунок 29 – Выбор импорта сертификата

В появившемся окне (см. Рис. 30) нажмите «*Обзор*». В диалоговом окне мастера импорта сертификатов, надо указать имя каталога, из которого будет производиться импорт личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и СОС. (*C:\Program Files\Avest\AvPCMTrust\CERT\PER*), (см. Рис. 30.1).

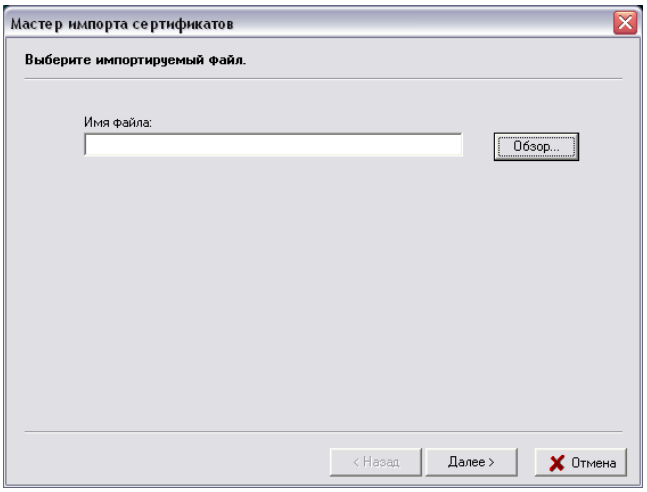

Рисунок 30 – Выбор файла импортируемых данных

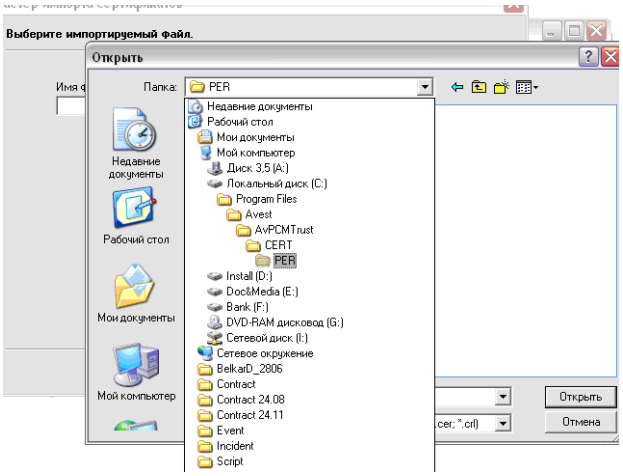

Рисунок 30.1 – Выбор файла импортируемых данных

Установите «***Тип Файлов*»→«*Сертификаты PKCS #7 (*.p7b)*»,** и выделив файл с расширением ***.p7b*** (например *cl_1708.p7b*) как показано на рисунке 30.2 нажмите «*Открыть*».

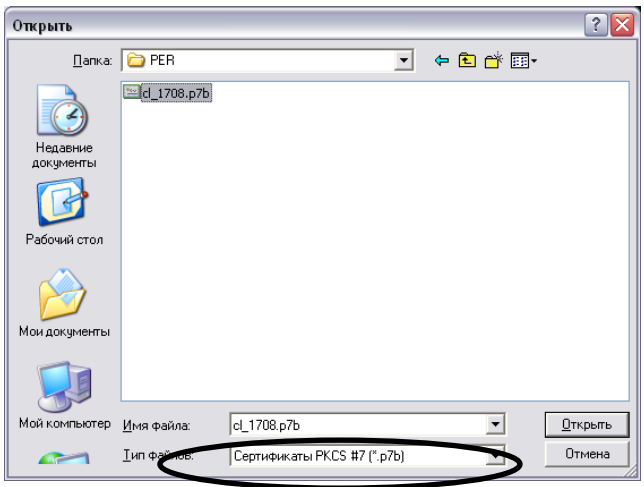

Рисунок 30.2 – Выбор файла импортируемых данных

В появившемся окне(см. Рис. 30.3) нажмите кнопку «*Далее*».

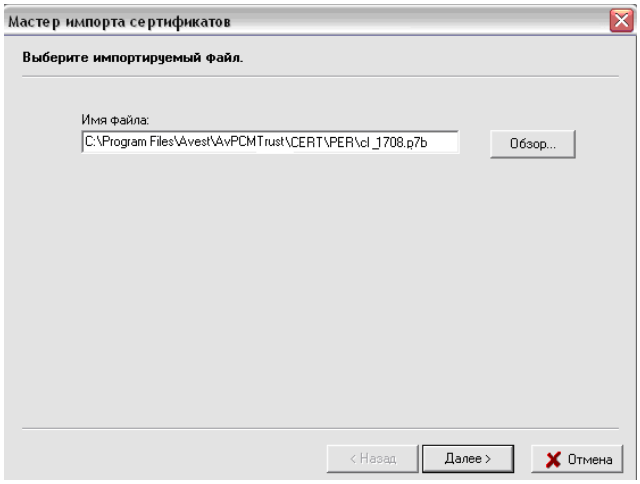

Рисунок 30.3 – Выбор файла импортируемых данных

В появившемся окне в виде таблицы будут отражены все объекты, которые входят в импортируемый файл и могут быть подключены для работы (см. Рис. 31).

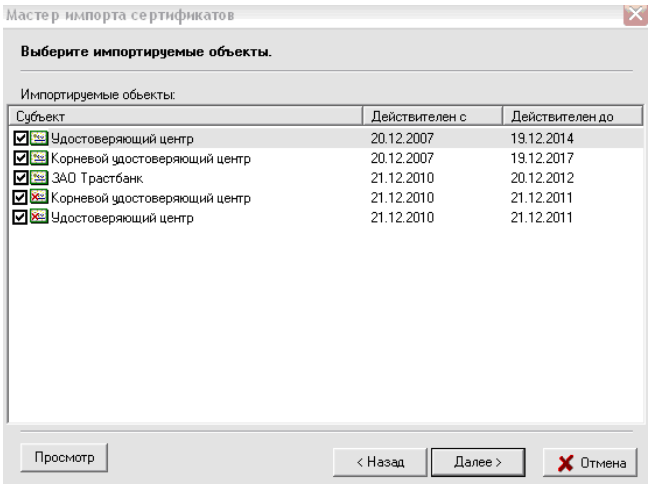

Рисунок 31 – Информация об импортируемых объектах

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

Внимание: При импорте своего личного сертификата в первый раз рекомендуем выделить и импортировать все отображаемые в данном окне файлы. И нажмите «*Далее*». В следующем окне содержится информация о количестве импортированных объектов и предложено поместить личный сертификат в персональный справочник (см. Рис.32).

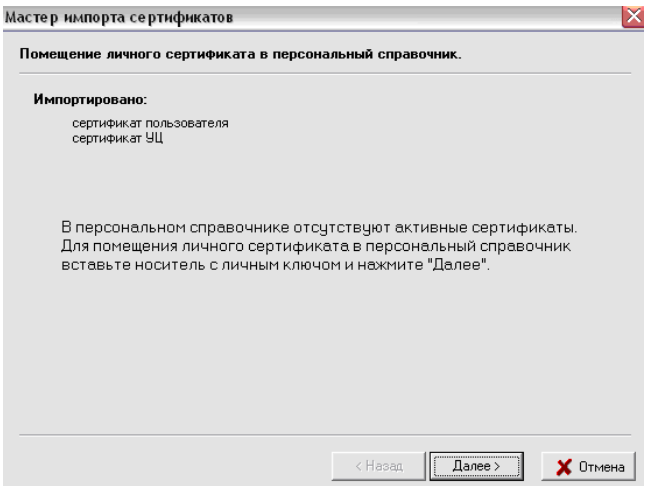

Рисунок 32 – Помещения личного сертификата в персональный справочник

Так как это Ваш первый импорт личного сертификата в программу ПК AvPCM, то в персональном справочнике сертификатов он отсутствует. Поэтому, для помещения личного сертификата в персональный справочник необходимо вставить носитель с Вашим личным ключом подписи/шифрования в считывающее устройство и нажать кнопку «*Далее*». Будет проведена проверка носителя ключей и в появившемся окне будет выведена информация обо всех находящихся

на данном носителе личных ключах. Для продолжения процедуры помещения личного сертификата в персональный справочник надо из данного списка выбрать контейнер личного ключа, который соответствует личному сертификату и нажать кнопку «*Далее*» (см. Рис. 33).

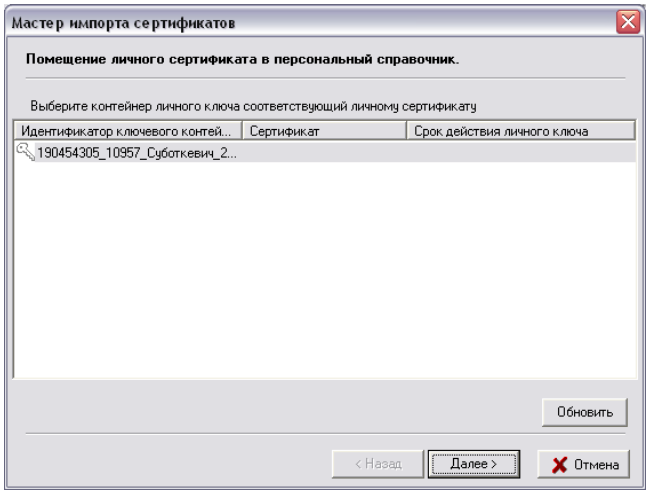

Рисунок 33 – Выбор контейнера личного ключа соответствующего личному сертификату

Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» необходимо ввести пароль, который Вы вводили при генерации личных ключей.(см. Рис. 33.1). После успешного ввода пароля будет предложено установить сертификат центра сертификации необходимо нажать «***Да***». (см. Рис. 33.2).

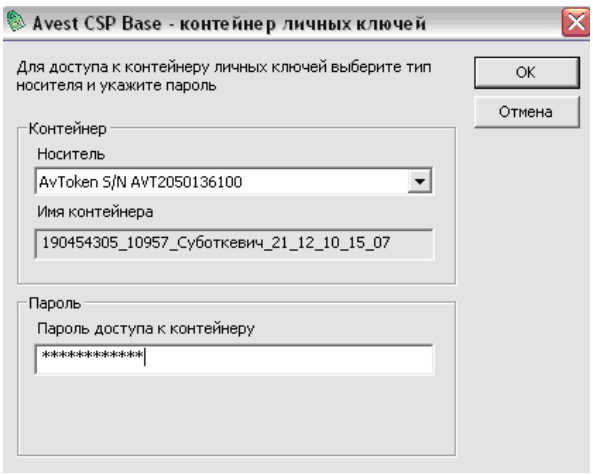

Рисунок 33.1 – Ввод пароля доступа к контейнеру личного ключа

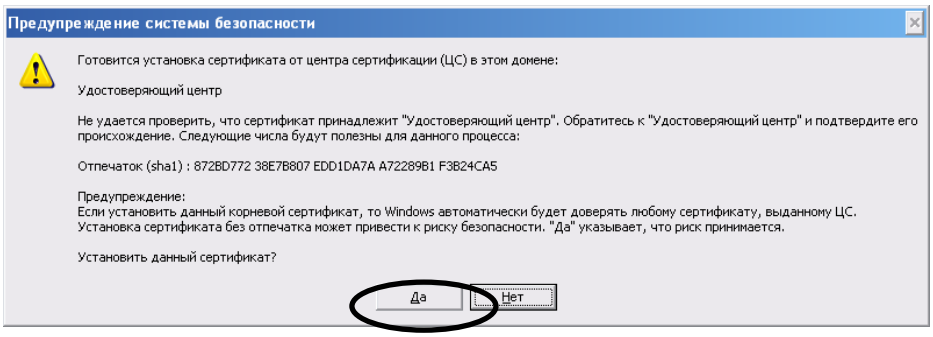

Рисунок 33.2 – Установка сертификата ЦС

Для полнофункциональной работы программы необходимо установить доверие к корневому сертификату УЦ. Для этого в следующем окне надо включить флажок «*Установить доверие сертификату корневого УЦ*» (см. Рис. 34).

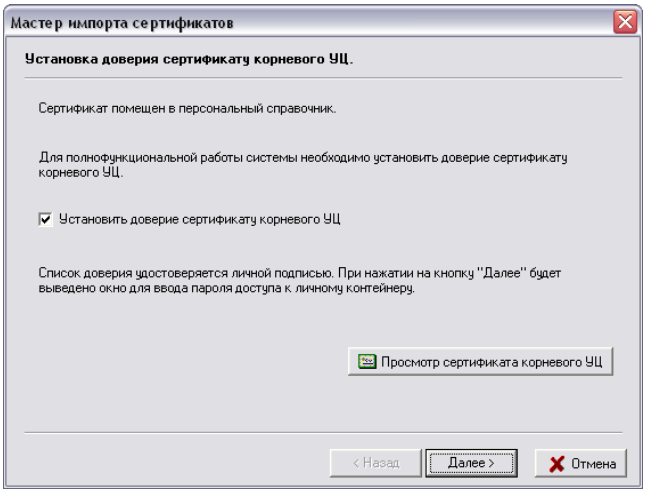

Рисунок 34 – Установка доверия сертификату корневого УЦ

После этого будет выведено сообщение о том, что корневой сертификат УЦ помещен в список доверия и мастер импорта сертификатов завершил работу. (см. Рис. 35).

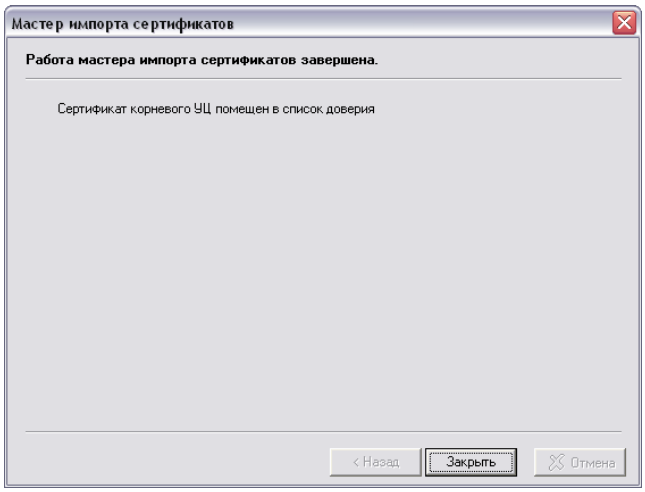

Рисунок 35 – Завершение работы мастера импорта сертификатов

9. Получение из Банка «логина» и «пароля».

Получите в Банке в запечатанном конверте «*логин*» и «*пароль*» который необходим для авторизации пользователя по учётной записи в системе «Интернет-Клиент», а так же пароль для архива WinRAR. Персональный пароль клиента является конфиденциальной информацией и в случае утери восстановлению не подлежит, просим Вас обеспечить надлежащее хранение данных.

10. Первый вход в подсистему «Интернет-Клиент».

Для запуска подсистемы «*Интернет-Клиент*» откройте браузер *Microsoft Internet Explorer 6.0* и выше, и в адресной строке браузера наберите адрес сайта сервиса «*Интернет-Клиента*» – ***https://ibank.rbank.by*** (см. Рис. 36). Добавьте адрес сайта в надёжные узлы (*Microsoft Internet Explorer* → «*Сервис*» → «*Свойство обозревателя*» → вкладка «*Безопасность*» → «*Надёжные узлы*» → «*Узлы*» → «*Добавить*» см. рисунок 36.1).

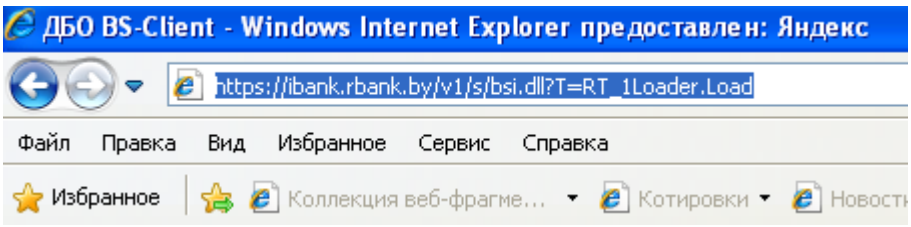

Рисунок 36 – Ввод адреса в браузере Internet Explorer

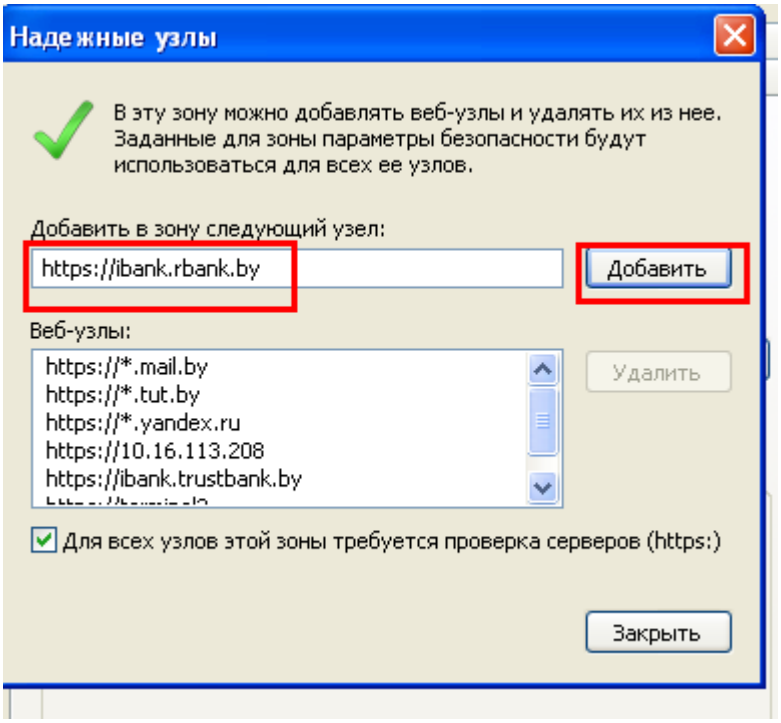

Рисунок 36.1 – Окно «Надёжные узлы»

При первом входе в систему, веб-узел будет пытаться установить надстройку «*BSS ActiveX library*». Для установки надстройки Вам необходимо мышью кликнуть по данной надстройке и выбрать – «*Установить эту надстройку*». см. Рис. 37. Расположение всплывающего окна надстройки может быть отличное от приведенного на рисунке в зависимости от версии *Internet Explorer*.

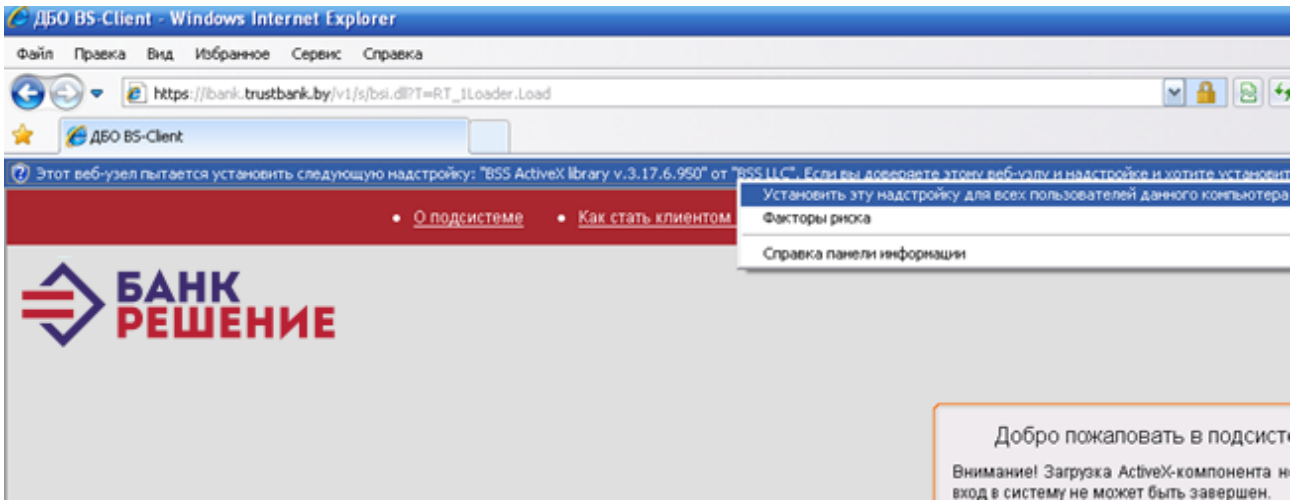

Рисунок 37 – Всплывающие окно надстройки «BSS ActiveX library»

Затем будет предложено установить ПО «*BSS ActiveX library*» нажимаем «*Установить*». (см. Рис. 38).

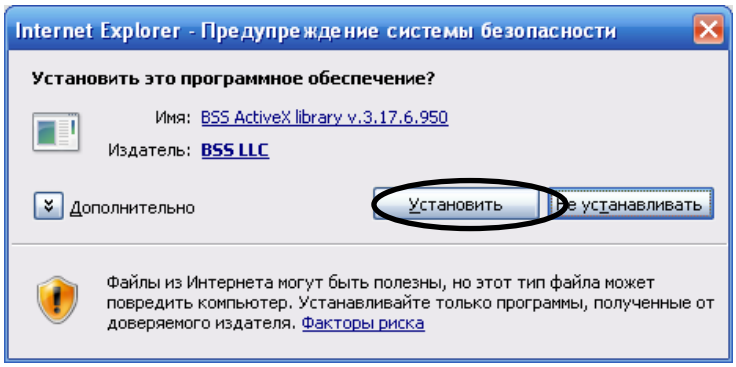

Рисунок 38 – Установка «BSS ActiveX library»

Выбираем язык «*Русский*» нажимаем *OK*. (см. Рис. 39).

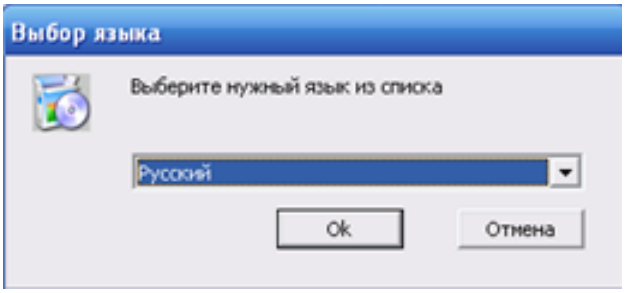

Рисунок 39 – Окно выбора языка

Далее на экран будет выведено окно следующего вида (см. Рис. 40):

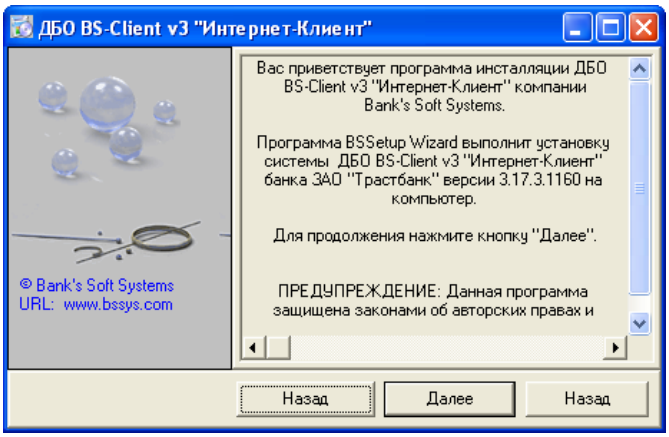

Рисунок 40 – Установка подсистемы «Интернет-Клиент»

Нажмите «*Далее*», появится путь установки (см. Рис. 41).

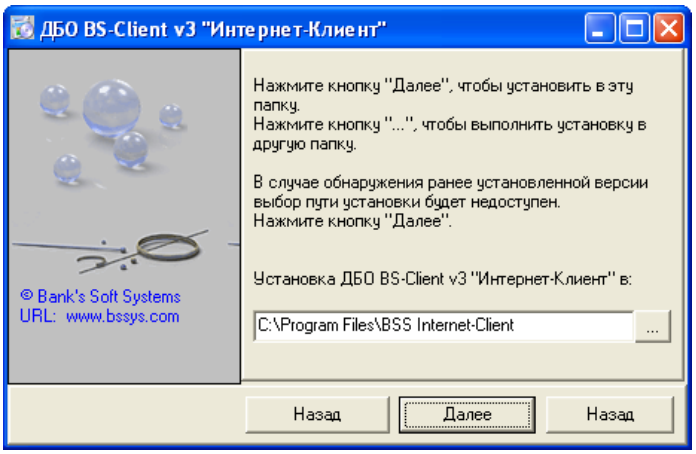

Рисунок 41 – Путь установки

Нажмите «*Далее*» для запуска установки. В процессе установки происходит копирование файлов на Ваш компьютер, которое отображается в окне распаковки файлов (см. Рис. 42).

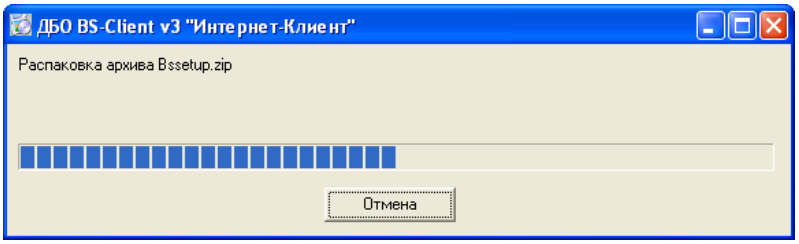

Рисунок 42 – Распаковка файлов

По окончанию процесса установки появится окно (см. Рис. 43). Нажмите «*ОК*».

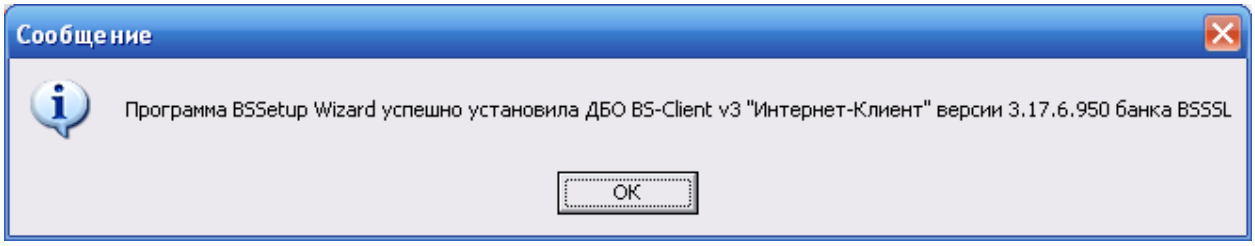

Рисунок 43 – Установка выполнена

В полях «*Логин*» и «*Пароль*» введите полученные из Банка системное имя (*Логин*) и *пароль* пользователя для входа в систему и нажмите кнопку «*Далее*» 1 раз (см. Рис. 44).

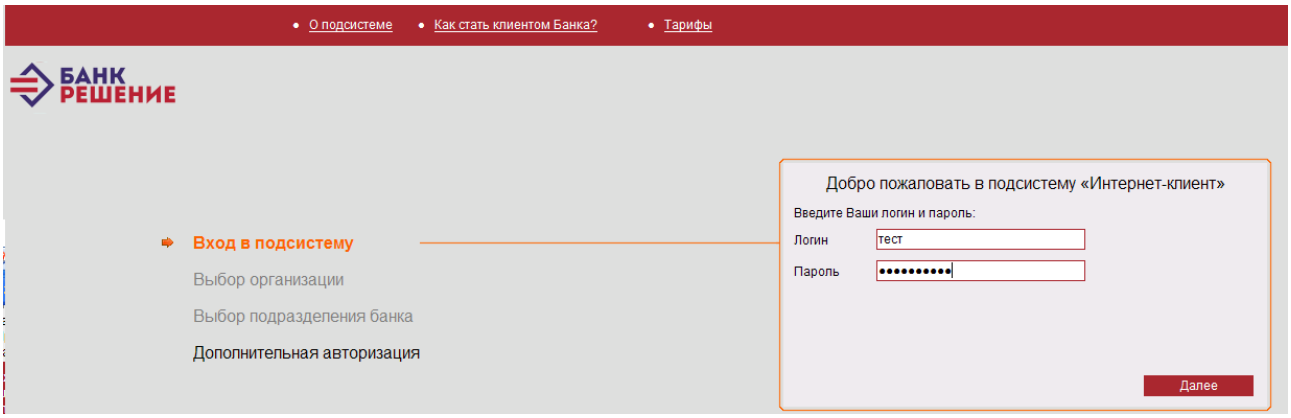

Рисунок 44 – Страница входа в подсистему «Интернет-клиент»

Вам будет предложено установить надстройку «*BSS ActiveX library*», для её установки необходимо мышью кликнуть по надстройке и выбрать – «*Запустить надстройку*» (см. Рис. 45).

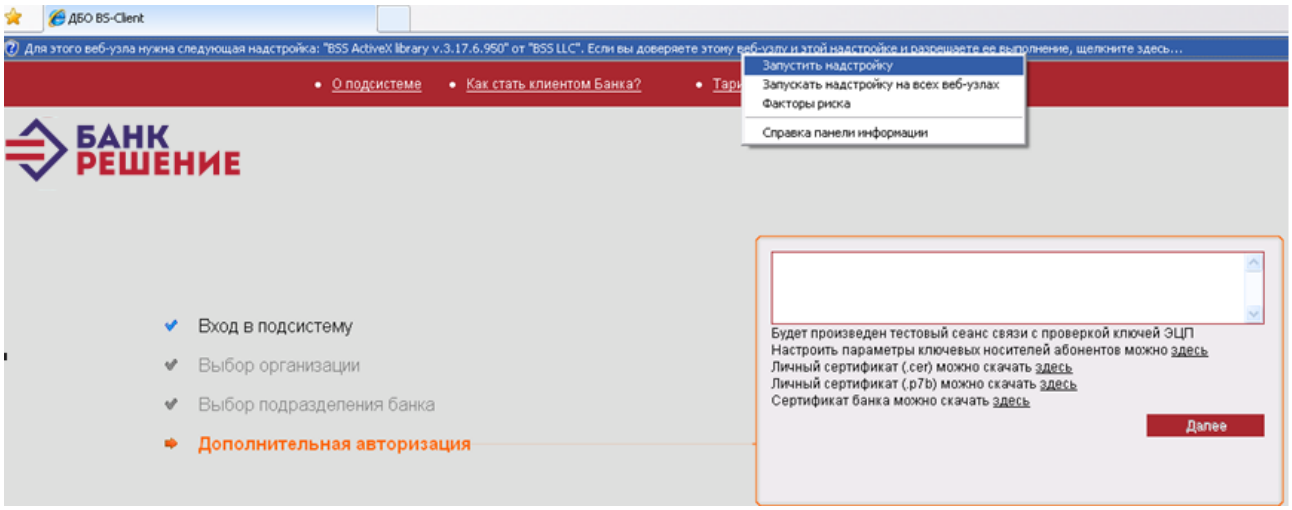

Рисунок 45 – Всплывающие окно надстройки «BSS ActiveX library»

Затем кликнете мышью «Настроить *параметры ключевых носителей абонентов можно* ***здесь***» (см. Рис. 46).

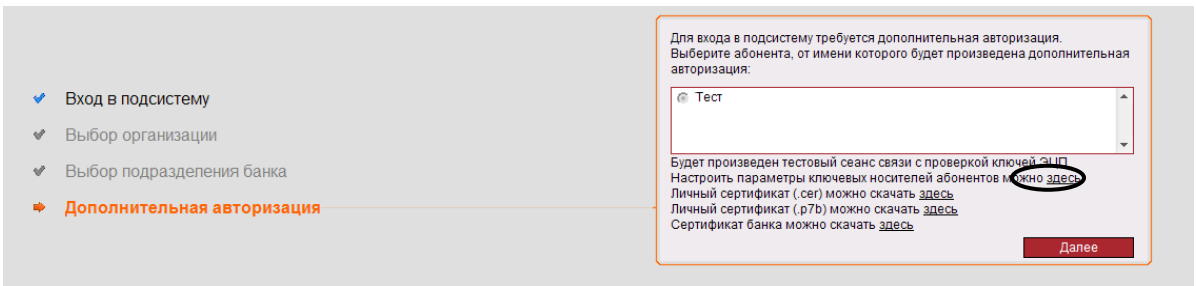

Рисунок 46 – Страница Дополнительная авторизация

Заполните поля «*Файл личного сертификата*» (где *cl_тест* будет соответствовать имени Вашего сертификата), «*Директория сертификата центра сертификации*», «*Директория справочника сертификатов*», «*Директория списков отозванных сертификатов*» аналогично рисунку (см. Рис. 47). После заполнения нажмите «*ОК*», Вам выдаст сообщение (см. Рис. 47.1).

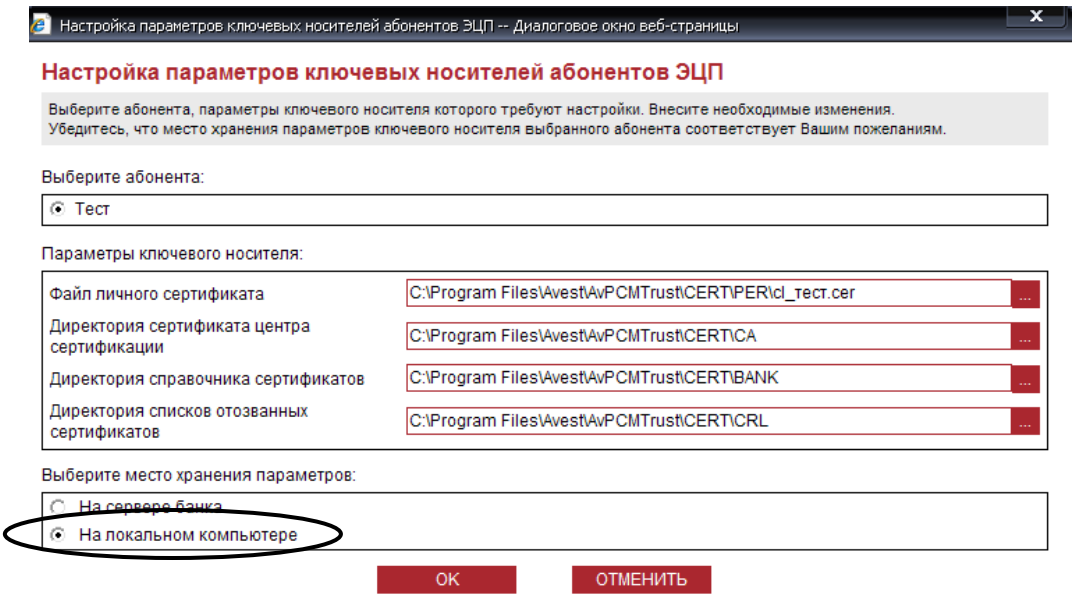

Рисунок 47 – Окно настройки параметров ключевых носителей абонентов ЭЦП

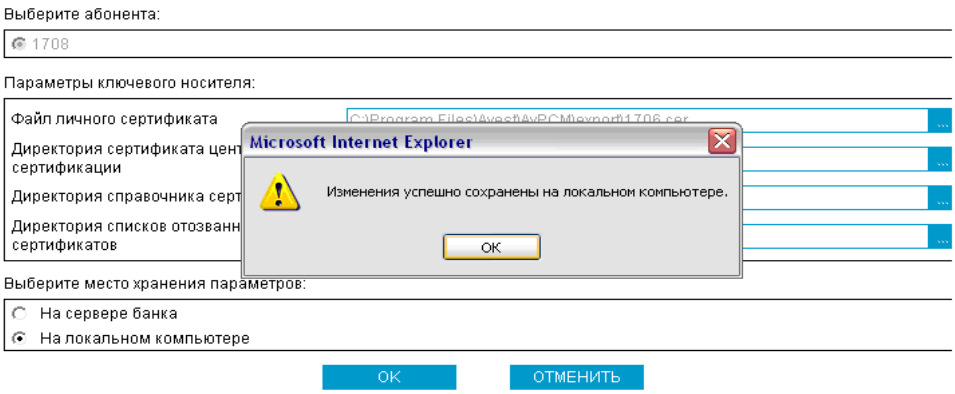

Рисунок 47.1 – Информационное окно

Нажмите кнопку «*Далее*», система выдаст следующее сообщение (см. Рис. 48). Вставьте ключ абонента в USB-порт и нажмите кнопку «*Далее*».

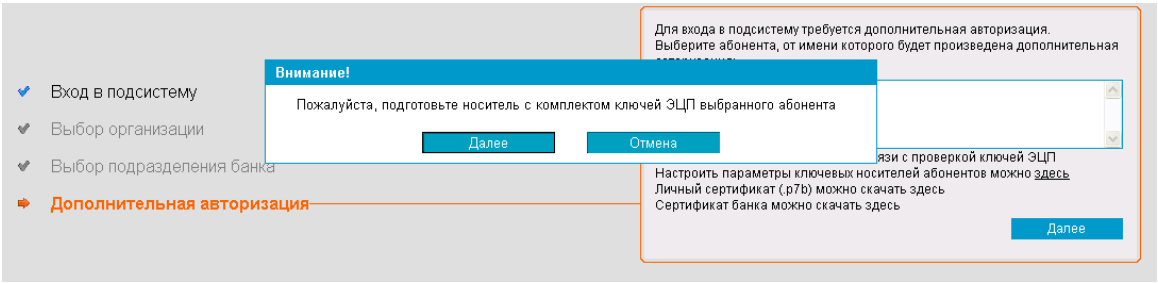

Рисунок 48 – Сообщение системы

Для установки сертификата центра сертификации необходимо нажать «***Да***» (см. Рис. 49)

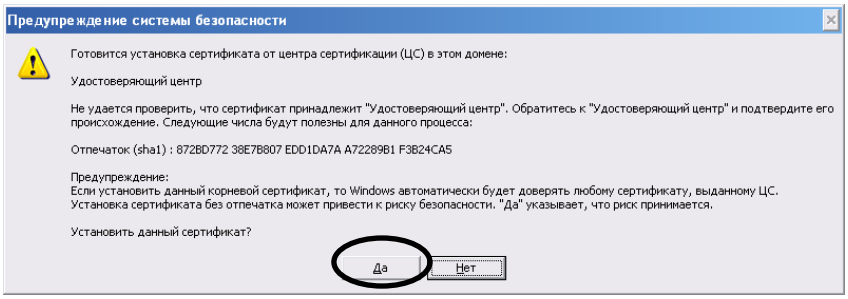

Рисунок 49 – Установка сертификата ЦС

Введите Ваш *пароль* доступа к контейнеру и нажмите «*ОК*» (см. Рис. 50).

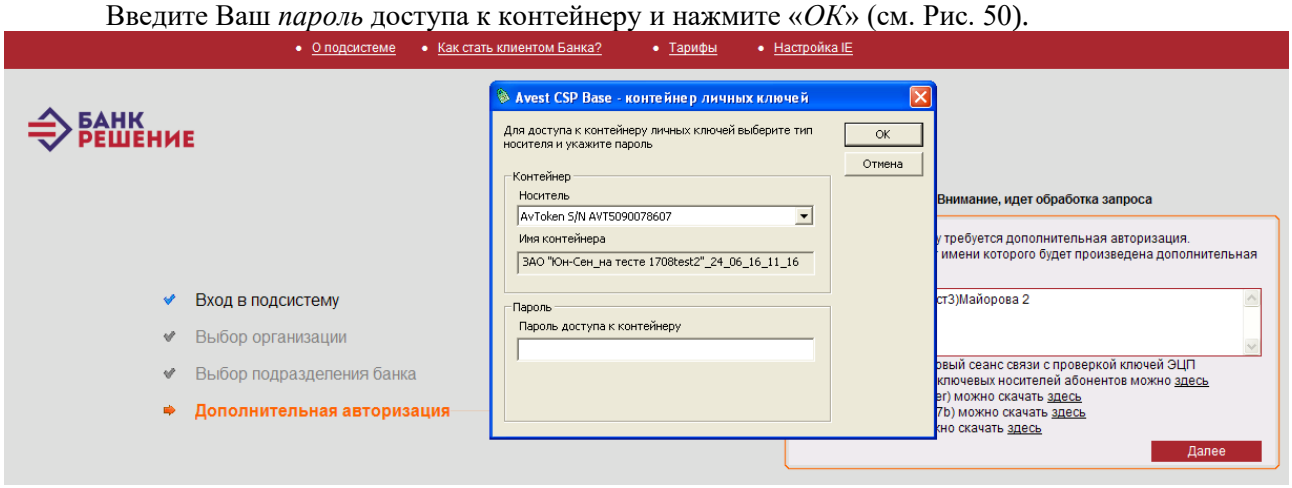

Рисунок 50 – Окно запроса пароля доступа к контейнеру

После прохождения авторизации пользователю необходимо вновь установить надстройку «*BSS ActiveX library*» для её установки необходимо мышью кликнуть по надстройке и выбрать – «*Запустить надстройку*» затем нажать «*Выполнить*» (см. Рис. 51).

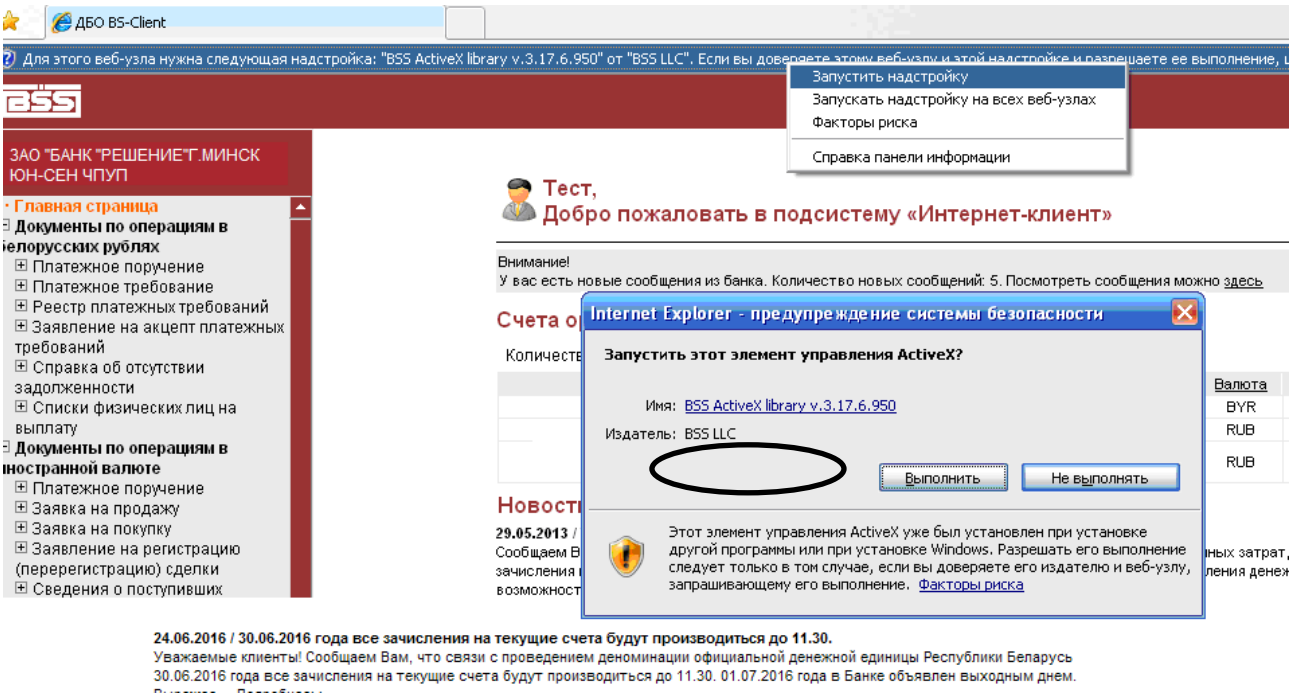

Рисунок 51 – Всплывающие окно надстройки «BSS ActiveX library»

Введите «*Логин*» и «*Пароль*» нажмите *далее* введите *пароль* доступа к контейнеру и повторите процедуру установки «*BSS ActiveX library*» описанную выше. После успешных установок надстроек, пользователь получает доступ к основному разделу сайта сервиса Интернет-Клиента (см. Рис. 52).

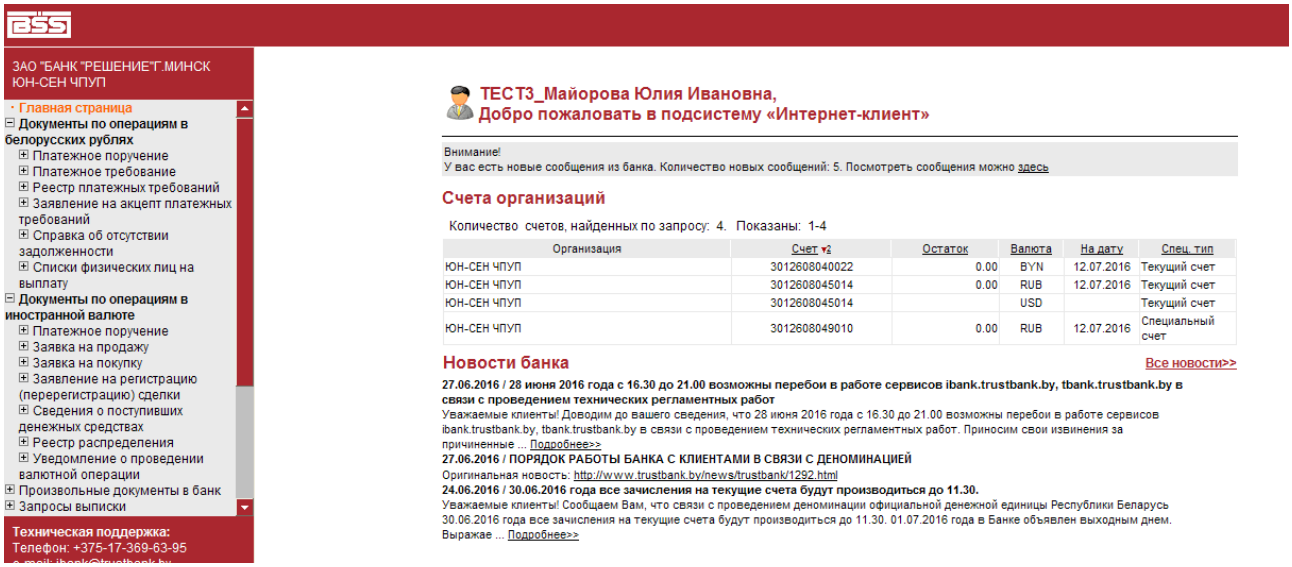

Рисунок 52 – Страница основного раздела «Интернет-Клиента»

Для корректного отображения документов при выводе на печать, сделайте следующую настройку: откройте браузер *Microsoft Internet Explorer* → «*Файл*» → «*Параметры страницы*» и заполните поля (*слева, справа, сверху, снизу*) как показано на рисунка 53.

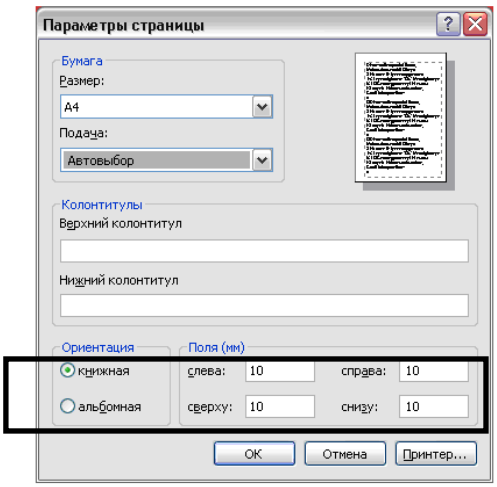

Рисунок 53 – Параметры страницы

Более подробное описание работы с подсистемой «*Интернет Клиент*» смотрите *\КОМПЛЕКТ АБОНЕНТА\BSS_Client\Docs**Руководство оператора (Интернет-Клиент).pdf***

11. Переустановка системы «Интернет-Клиент».

Для переустановки системы «Интеренет-Клиент» Вам необходимо выполнить следующие пункты данной инструкции:

1 пункт. – Установка криптопровайдера «AVEST;
2 пункт. – Установка персонального менеджера сертификатов «AVEST»;

– Скопируйте каталог /**CERT**/ (расположенный по пути – *C:\Program Files\Avest\AvPCMTrust\)* и разместите его пути *C:\Program Files\Avest\AvPCMTrust* на переустанавливаемый компьютер. В случае невозможности скопировать папку **CERT**, проделайте 3 пункт данной инструкции, а так же скопируйте полученные ***ранее*** сертификаты согласно пункту 7.

4 пункт. – Настройка параметров Internet Explorer;
8 пункт. – Импорт сертификата;
10 пункт. – Первый вход в подсистему «Интернет-Клиент».

12. Перегенерация личного ключа и сертификата.

В случае если Ваш сертификат истекает, либо истёк (срок действия сертификата можно посмотреть если открыть сертификат с расширением ***.cer*** (см.Рис. 54) распложенный по пути *C:\Program Files\Avest\AvPCMTrust\CERT\PER\)*, необходимо выполнить следующие пункты данной инструкции:

5 пункт. – Генерация личного ключа и создание запроса на выпуск сертификата;
6 пункт. – Передача в Банк запроса на сертификат;
7 пункт. – Получение из Банка файлов сертификатов;
8 пункт. – Импорт сертификата.

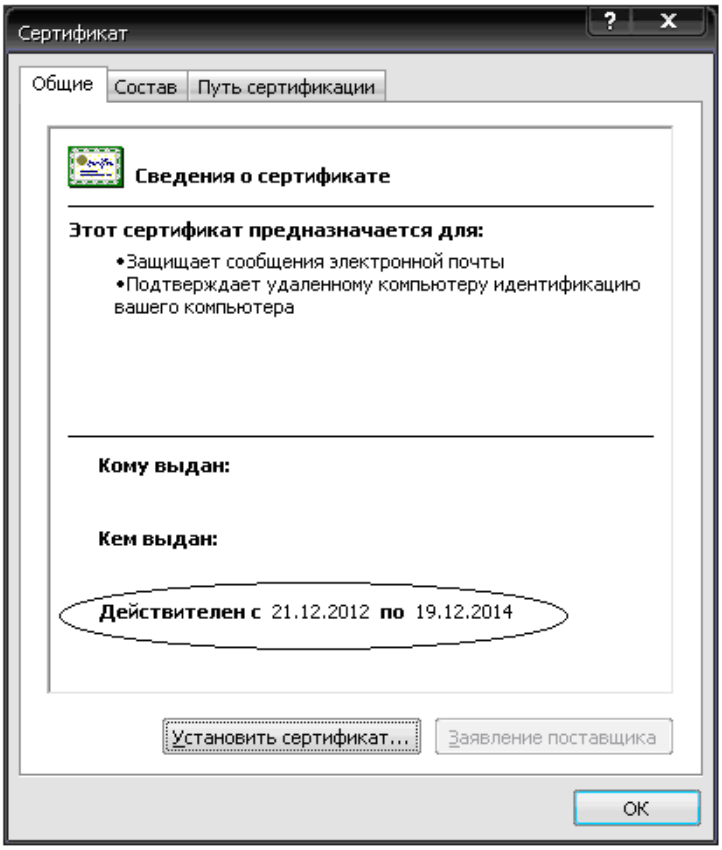

Рисунок 54 – Сведения о сертификате

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Программное средство криптографической защиты информации «Криптопровайдер Avest CSP»: Руководство оператора / – Утверждён РБ.ЮСКИ.08000-01 34 01-ЛУ, 2010г. С.31

2. Программный комплекс «персональный менеджер сертификатов Авест» AvPCM»: Руководство оператора / – Утверждён РБ.ЮСКИ.08003-01 34 01-ЛУ, 2008г. С. 69

3. Система дистанционного банковского обслуживания «BS-CLIENT» подсистема «ИНТЕРНЕТ КЛИЕНТ» »: Руководство оператора / – BY/112.ПВКУ.00601-02 34 01.: ОДО «БИ-ЛОДЖИК» 2012г. С.63

СПИСОК СОКРАЩЕНИЙ

БД – база данных;
БИК – банковский идентификационный код;
НКИ – носитель ключевой информации;
ОС – операционная система;
ПО – программное обеспечение;
ПСКЗИ – программное средство криптографической защиты информации;
Система «ДБО BS-Client» – система дистанционного банковского обслуживания «BS-Cient»;
СКЗИ – система криптографической защиты информации;
СОК – сертификат открытого ключа;
СОС – список отозванных сертификатов;
УЦ – удостоверяющий центр;
ЦР – центр регистрации;
ЦС – центр сертификации;
НКИ – носитель ключевой информации;
ЭЦП – электронная цифровая подпись.