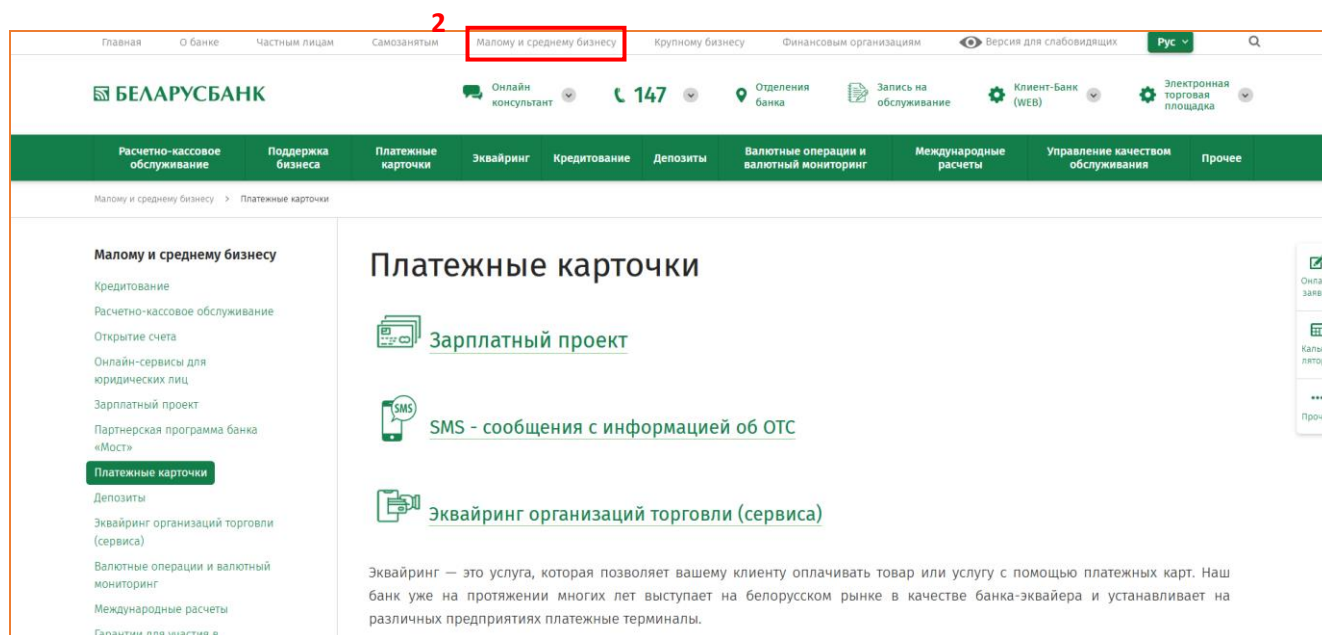


# Инструкция по установке и настройке программного обеспечения КП СОБ (Cryptoservice) и «Комплект Абонента АВЕСТ» (AvUSK) для работы в ПК «Студенческая карта»

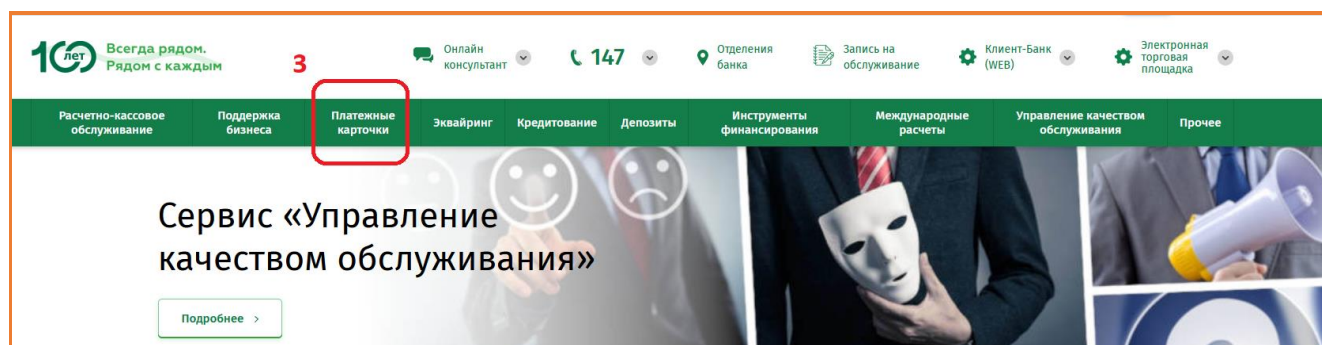
Настоящая инструкция предназначена только для учреждений образования, которые получили от Банка технологический ключ ГосСУОК.

## 1. Установка КП СОБ (Cryptoservice)

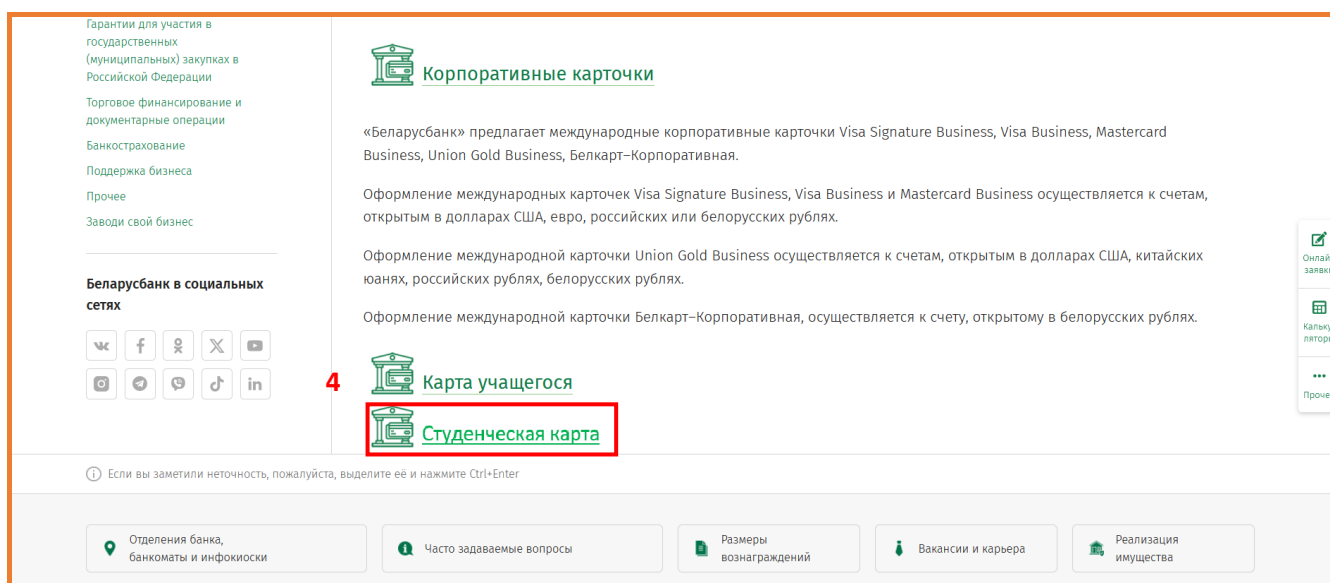
Необходимо зайти на сайт ОАО «АСБ Беларусбанк» (<https://belarusbank.by/>) (1) и перейти в меню «Малому и среднему бизнесу»:



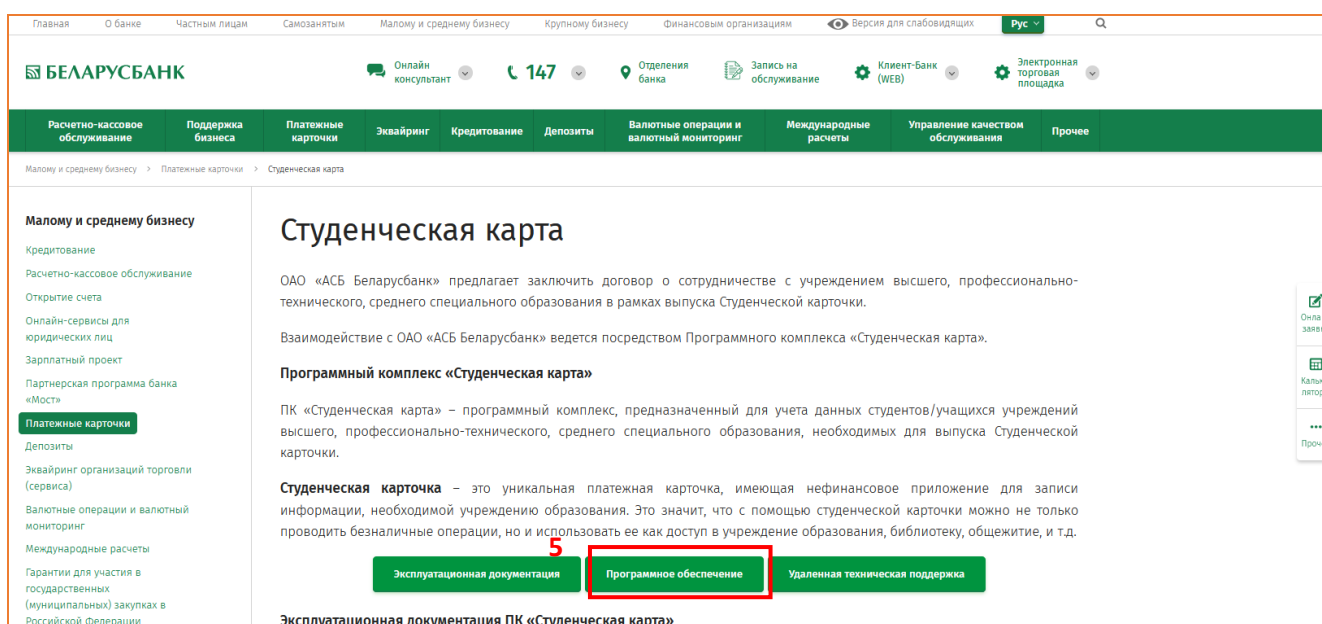
- нажать вкладку «Платежные карточки»:



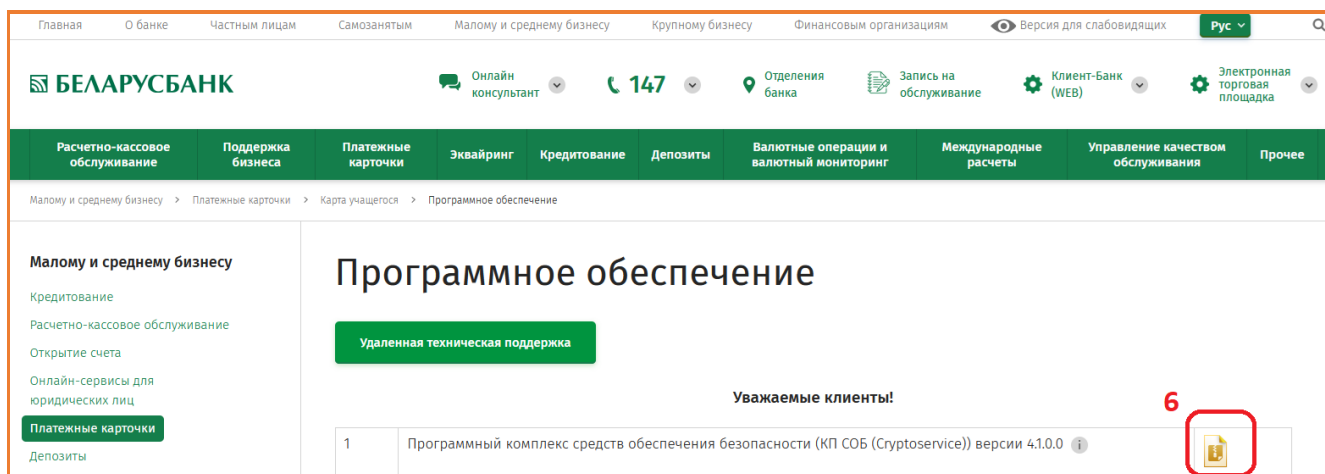
- зайти в раздел «Студенческая карта»:



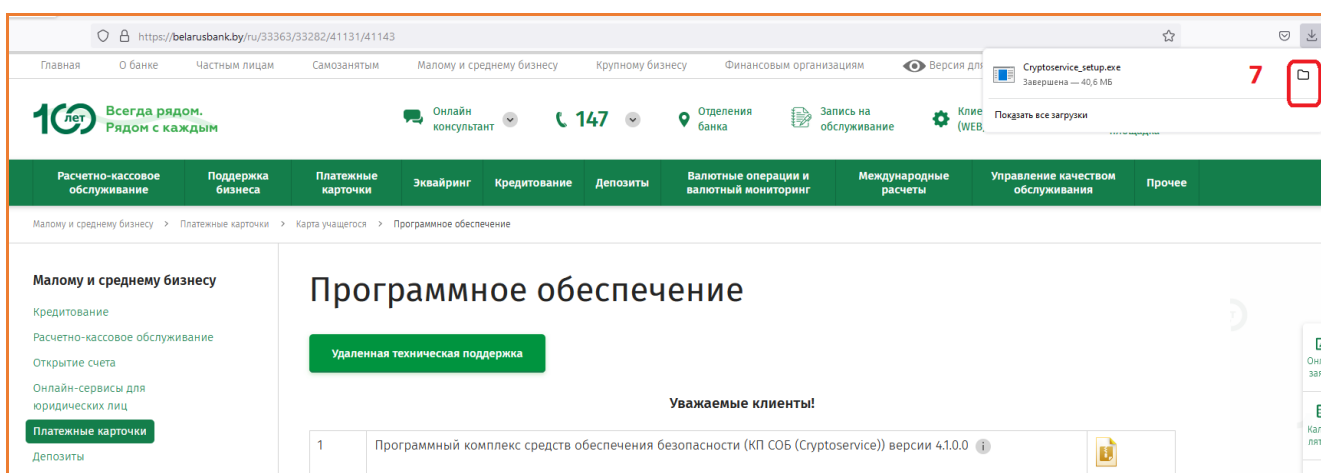
- нажать навигационную кнопку «Программное обеспечение»:



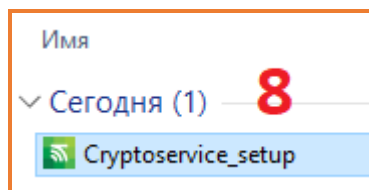
- сохранить дистрибутив КП СОБ (Cryptoservice), кликнув 1 раз левой клавишей мыши по ссылке:



- после завершения скачивания открыть папку с файлом:



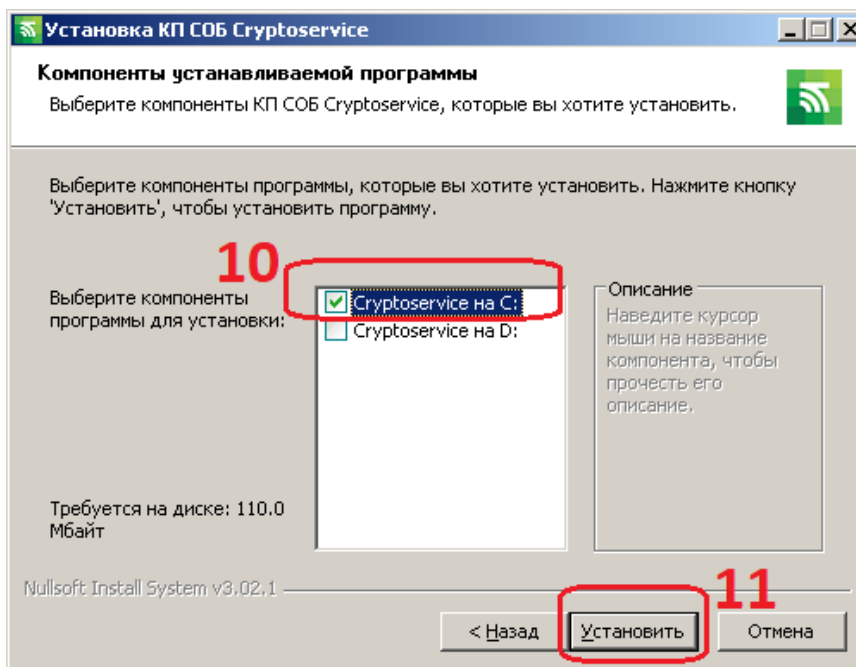
- запустить установку КП СОБ (Cryptoservice), дважды кликнув левой клавишей мыши по файлу:



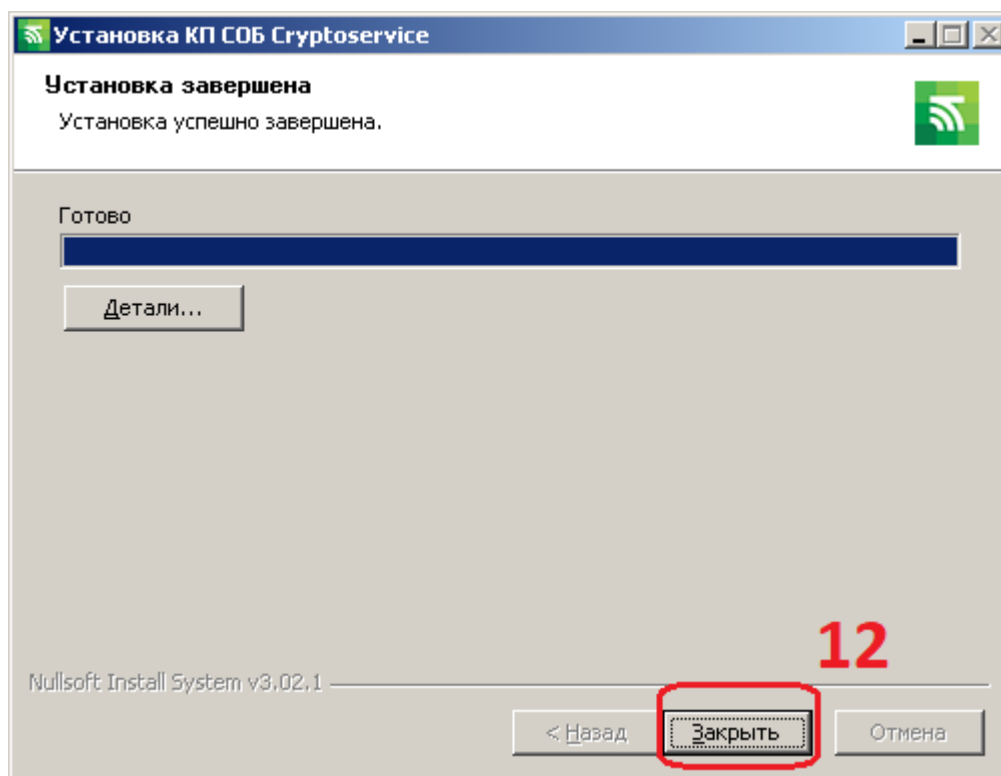
Открывается окно установки, в котором необходимо нажать кнопку «Далее»:





Затем выбрать системный диск (C или D), на который произойдет установка КП СОБ (Cryptoservice), и нажать кнопку «Установить»:





После окончания процесса установки нажать кнопку «Заккрыть»:



При успешной установке КП СОБ (Cryptoservice) в панели задач (правом нижнем углу экрана) появятся иконка КП СОБ (Cryptoservice) «» и приложения ssf-server «»:



### **Важно!**

Для работы в ПК «Студенческая карта» должны быть запущены одновременно оба указанных приложения: КП СОБ (Cryptoservice) «» и ssf-server «». Они автоматически запускаются при первичной установке КП СОБ (Cryptoservice) и далее каждый раз при загрузке компьютера.

Если автоматического запуска приложений не произошло, их можно запустить в ручном режиме с локального диска компьютера:

КП СОБ (Cryptoservice) запускается файлом по адресу C:\CryptoServiceASB\CryptoService\_41.exe (или D:\CryptoServiceASB\CryptoService\_41.exe - в зависимости от того, какой выбор был сделан на шаге № 10 процесса установки);

ssf-server запускается файлом по адресу  
C:\CryptoServiceASB\CbWEBCrypt\ssf\_server.exe  
(или D:\CryptoServiceASB\CbWEBCrypt\ssf\_server.exe).

## 2. Настройка КП СОБ (Cryptoservice) в зависимости от типа используемого соединения

При использовании учреждением образования (далее – УО) канала связи с банком «Интернет» без прокси-сервера дополнительные настройки в КП СОБ (Cryptoservice) производить не требуется.

При использовании УО канала связи с банком «Интернет» с прокси-сервером необходимо уточнить у системного администратора УО возможность открытия доступа к ip-адресам внешнего реестра сертификатов по портам, указанным в секции транспортных настроек в параметре:

```
<CA Description="Транспортные атрибуты УЦ">  
<HTTP URL="http://86.57.255.37:4080;http://194.158.196.37:4080" Sending-  
Timeout="60 sec" ReceivingTimeout="90 sec">
```

В случае получения от системного администратора положительного ответа необходимо:

1. узнать у системного администратора УО параметры для работы через прокси-сервер (адрес прокси – сервера, порт на котром работает прокси – сервер (при необходимости), логин и пароль клиента);

2. открыть для редактирования файл [drive]:\CryptoServiceASB\CryptoServiceSettings.xml на компьютере УО с ранее установленным КП СОБ (Cryptoservice);

найти в данном файле в секции транспортных настроек и заполнить их согласно данным полученным от системного администратора (выделено красным):

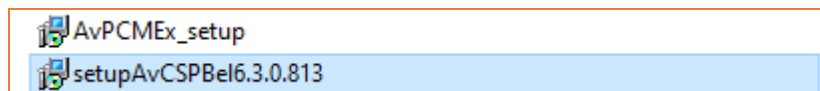
```
<Transport Description="Траспортные настройку">  
<HTTP-Request Repeat="4" Delay="5 msec"/>  
<CA Description="Транспортные атрибуты УЦ">  
<HTTP URL="http://86.57.255.37:4080;http://194.158.196.37:4080" SendingTimeout="60 sec" Receiving-  
Timeout="90 sec">  
<Proxy Type="1" Address="10.200.1.1" Port="8080" Login="login" Password="password"/>  
</HTTP>
```

### 3. Работа с ключами ГосСУОК в КП СОБ (Cryptoservice)

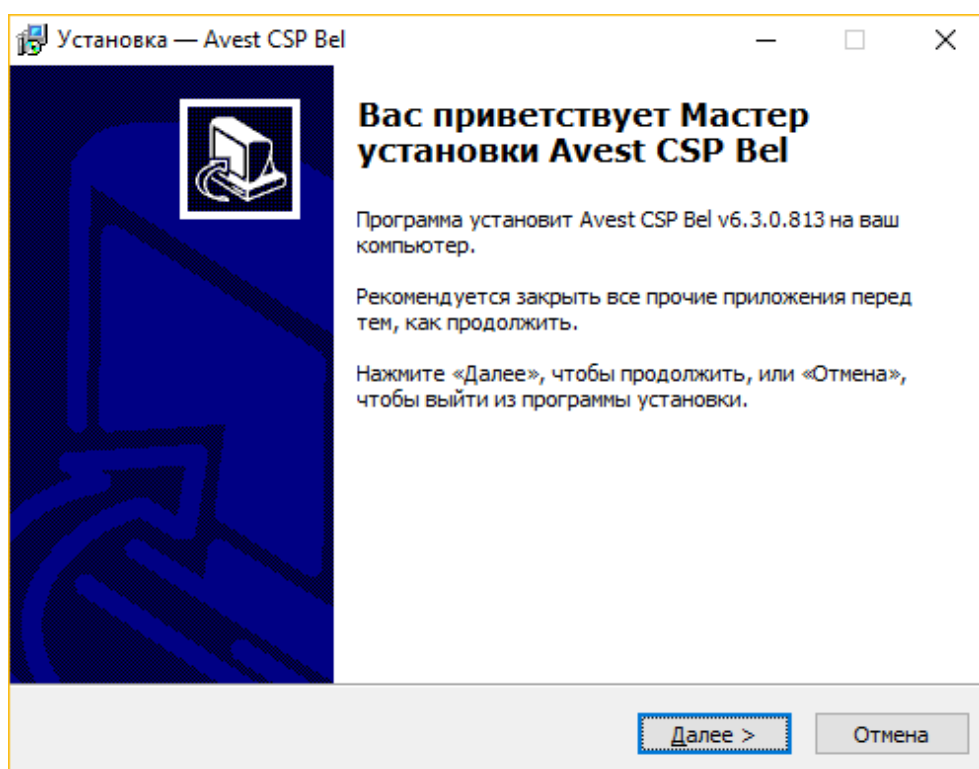
#### 3.1. Установка Криптопровайдера Avest CSP Bel.

Архив с программным обеспечением **AvUCK\_TSOK.zip**, полученный от Банка по электронной почте, необходимо сохранить на локальный диск компьютера, например в каталог d:\Install\.

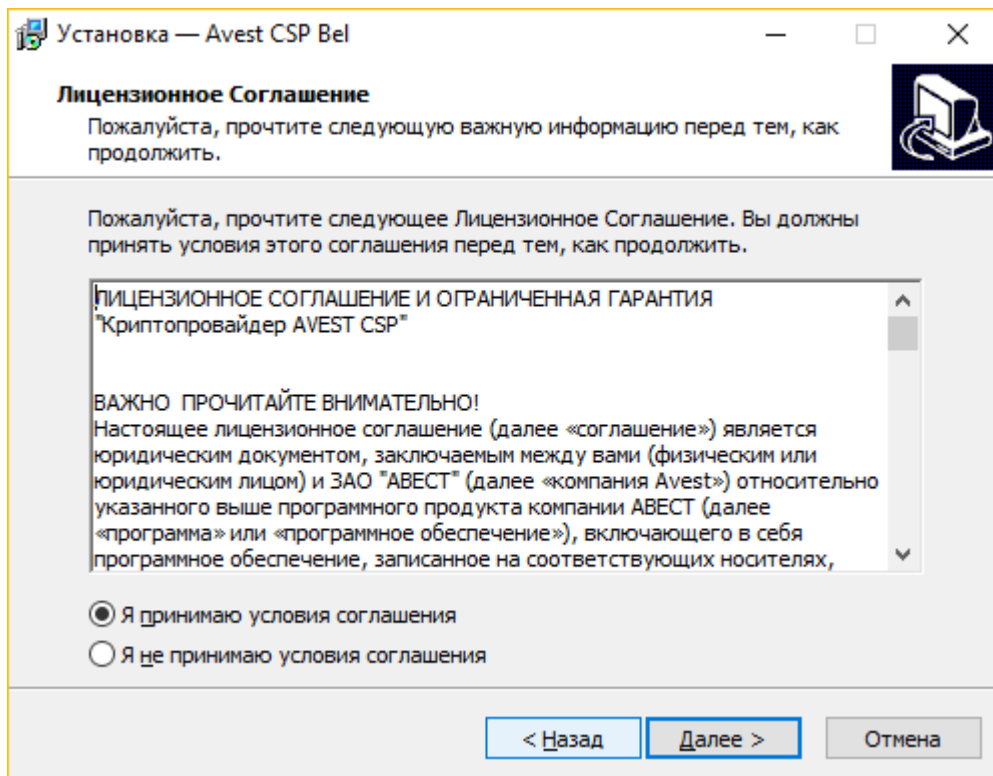
Распаковать архив, после чего запустить установку из файла **setupAvCSPBel6.3.0.813.exe**



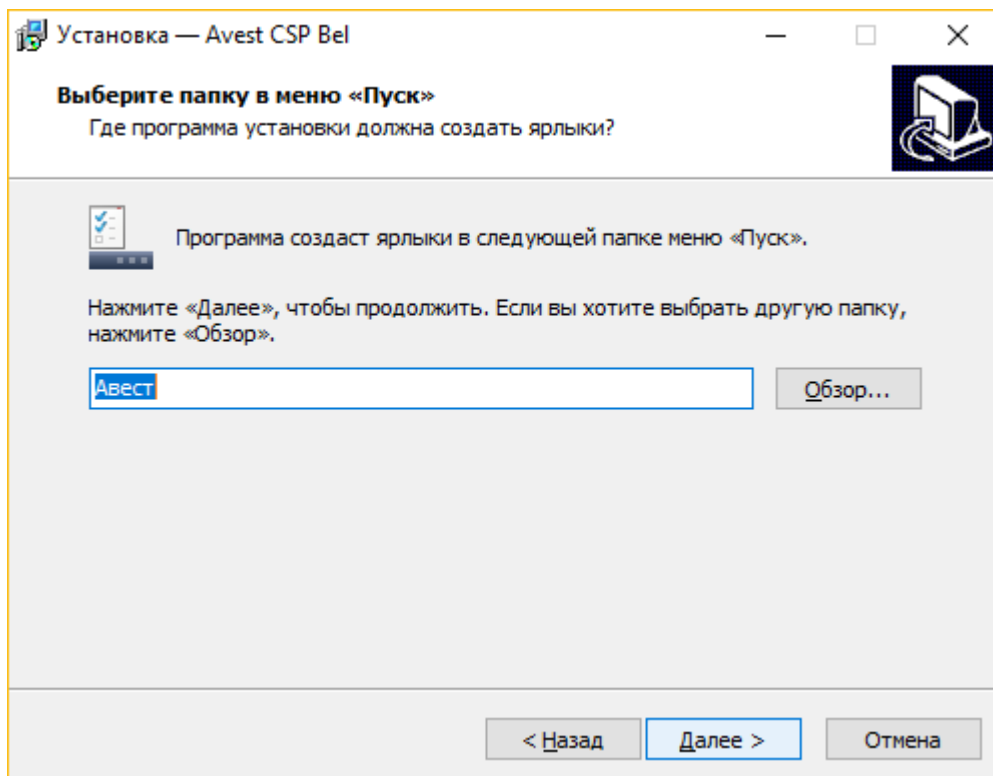
Нажать «Далее»:



Выбрать пункт «Я принимаю условия соглашения» и нажать «Далее»:

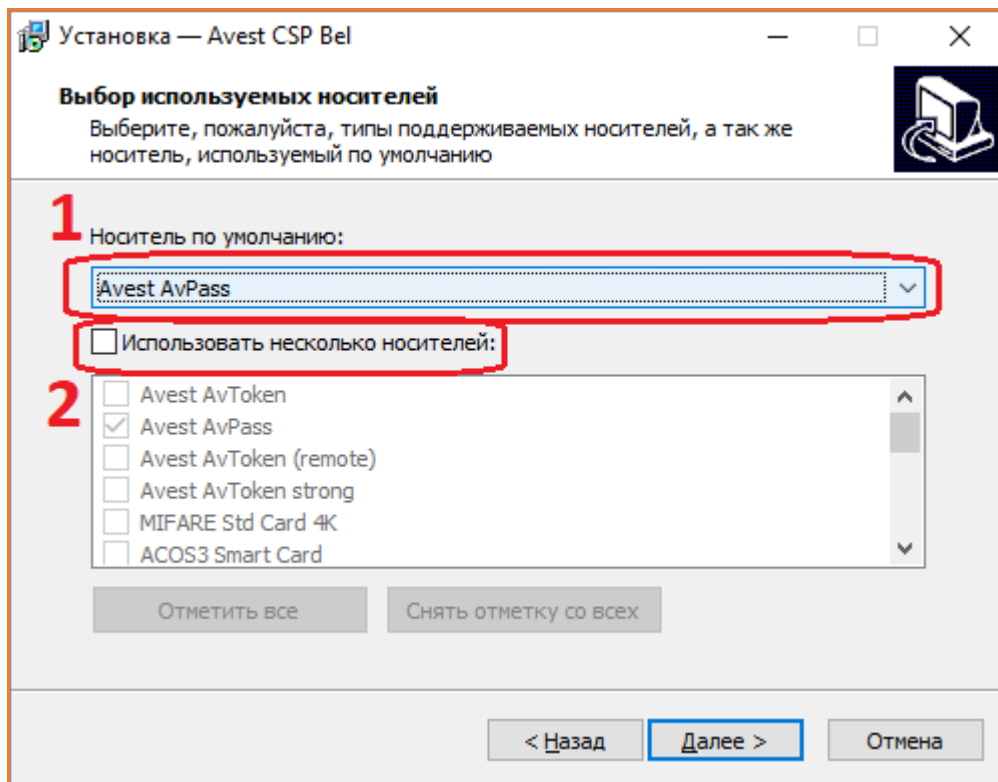


Повторно нажать «Далее»:

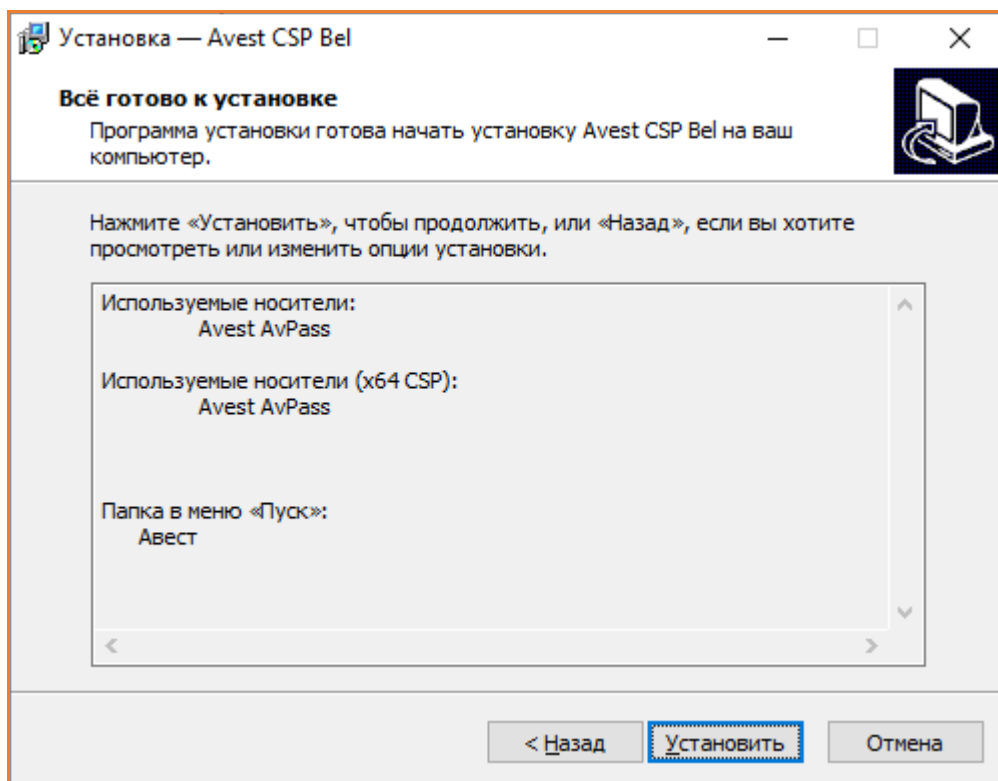




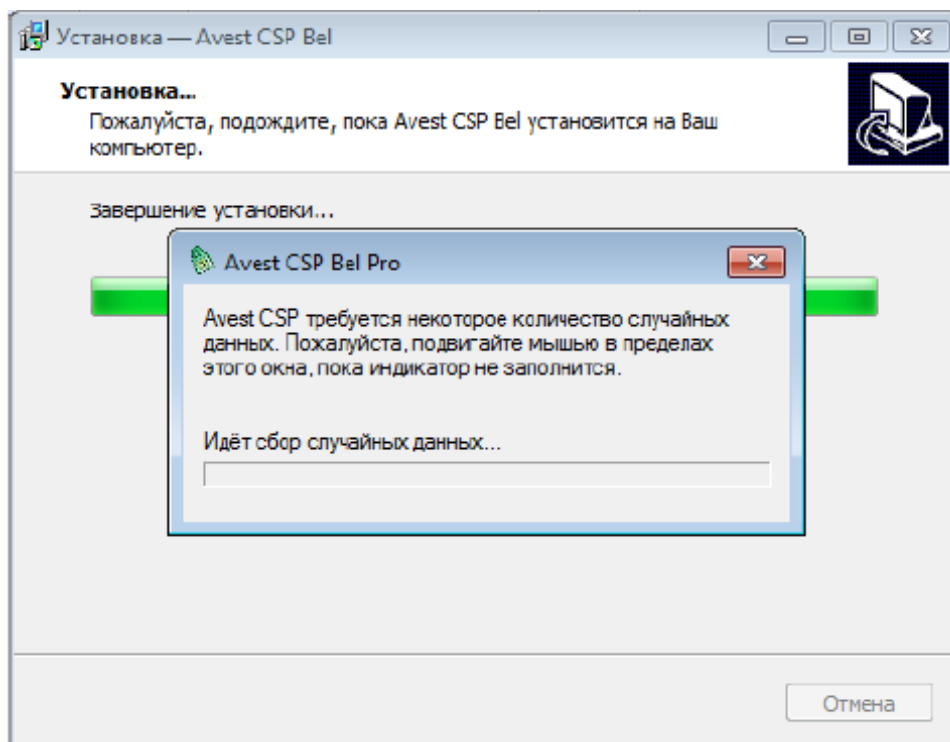
Выбрать носитель «Avest AvPass», убрать «галочку» «Использовать несколько носителей» и нажать «Далее»:



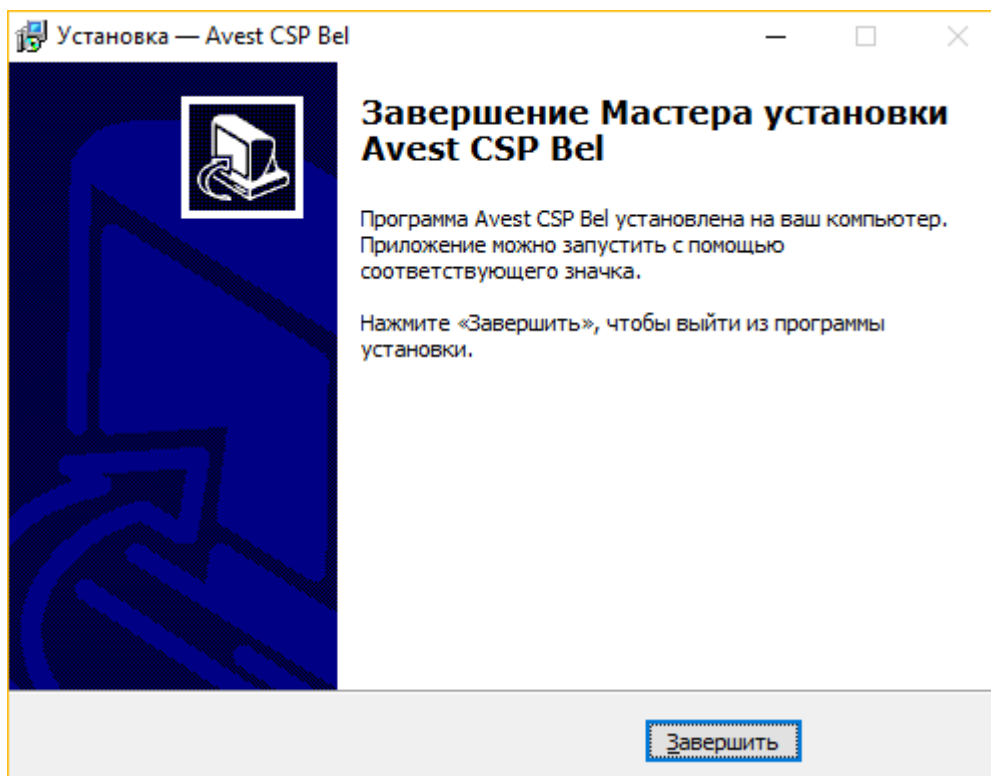
Нажать «Установить»:



В следующем окне необходимо подвигать мышью для сбора случайных данных:



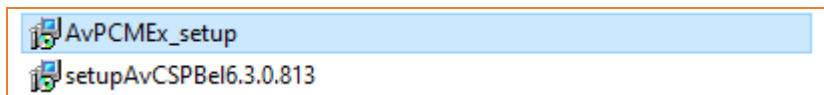
На этом мастер установки криптопровайдера закончит свою работу:



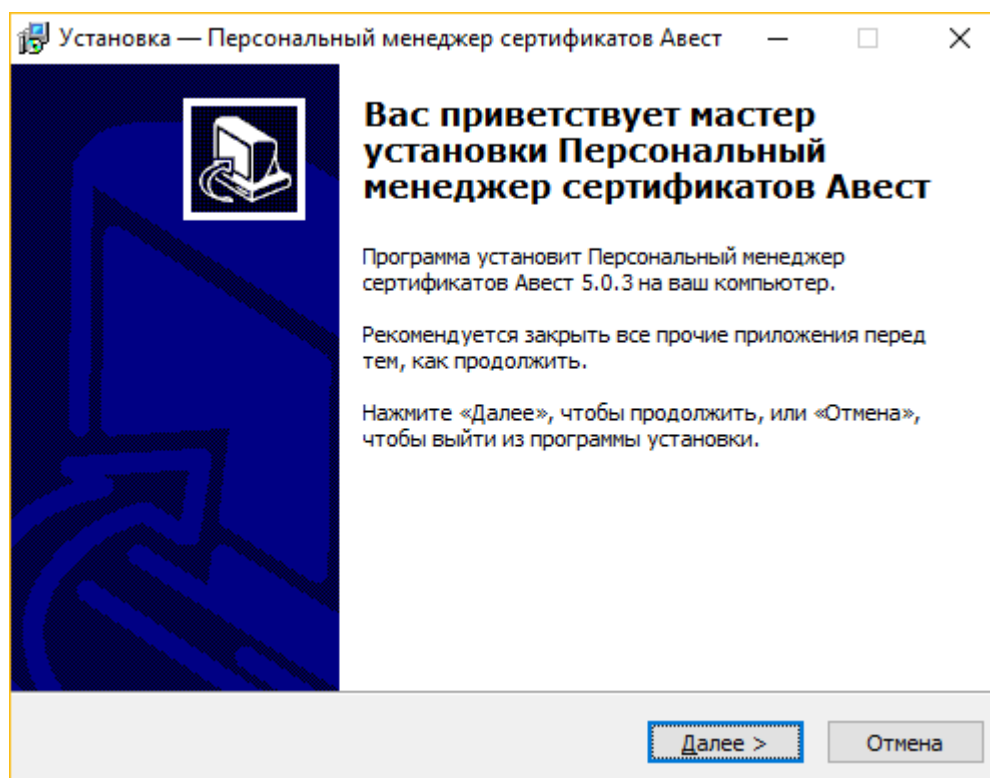
Также необходимо выполнить перезагрузку, если мастер установки предлагает ее сделать.

### 3.2. Установка Персонального менеджера сертификатов Авест

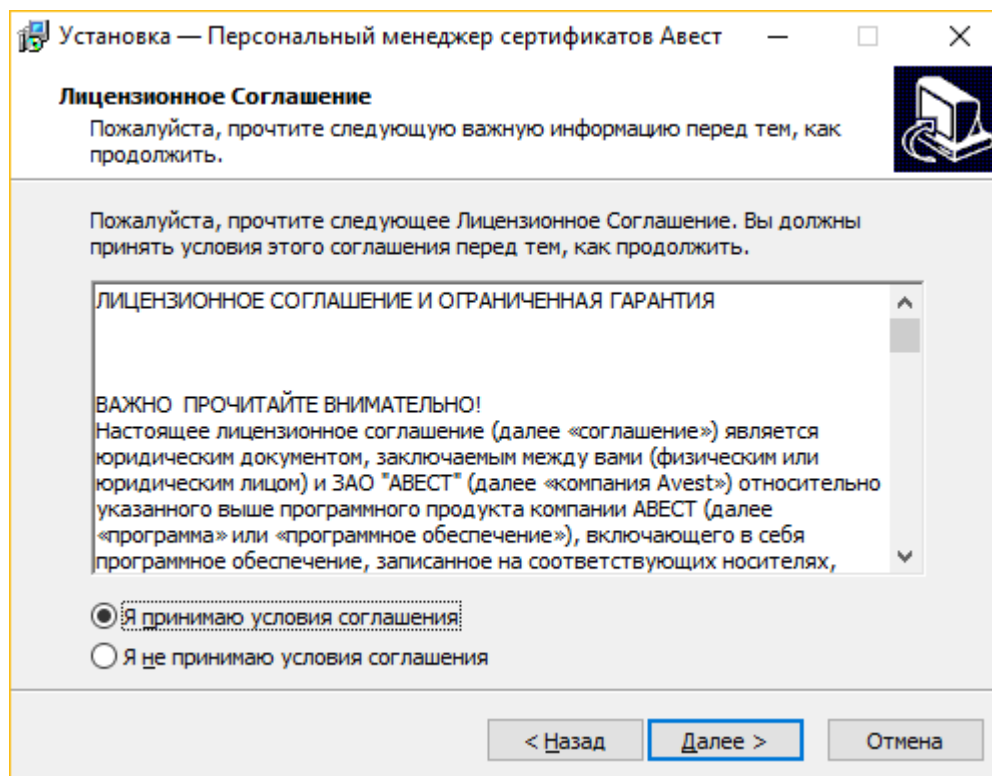
Открыть каталог, где был распакован архив **AvUCK\_TSOK.zip**, полученный от Банка по электронной почте, и запустить файл «AvPCME<sub>x</sub>\_setup.exe»



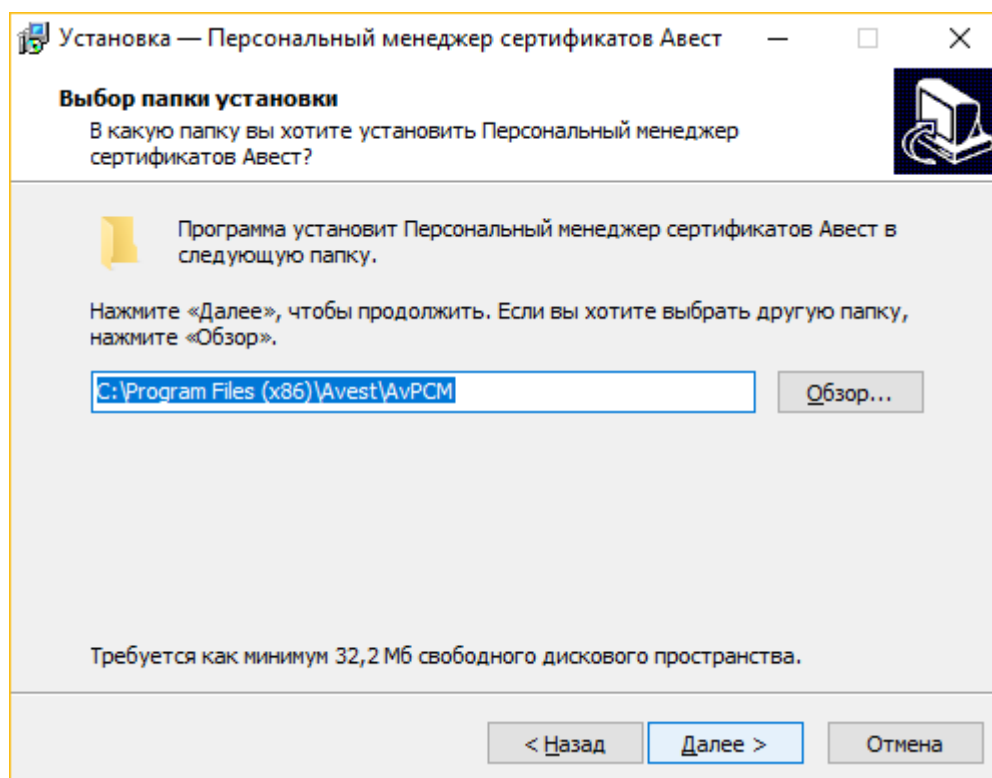
Нажать «Далее»:



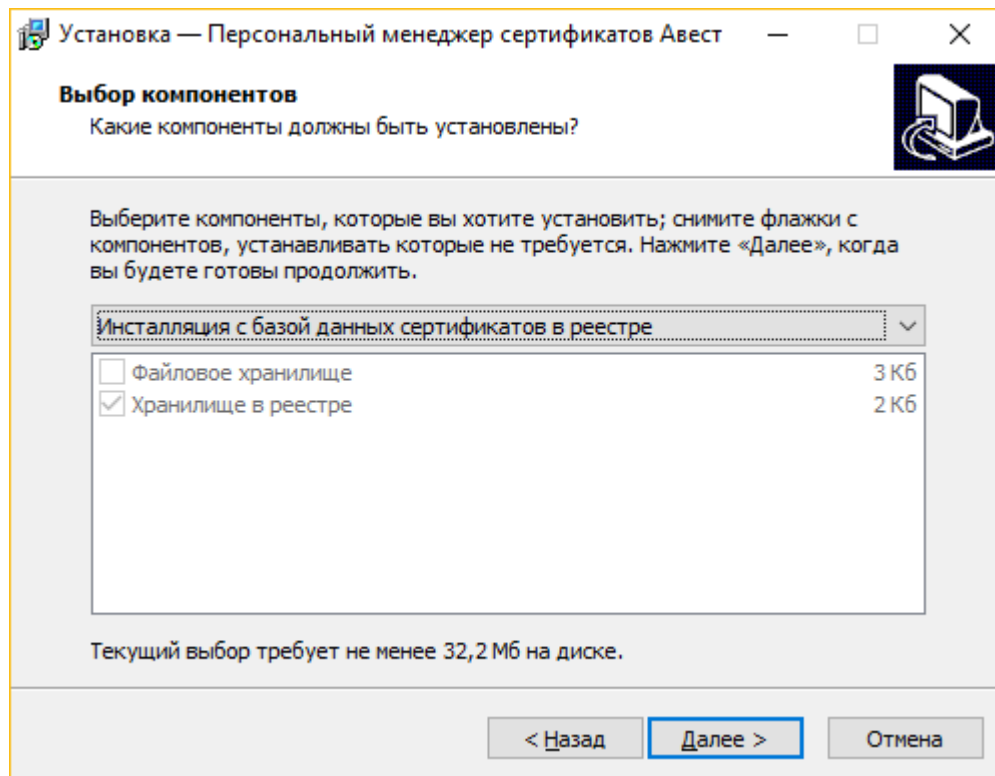
Выбрать пункт «Я принимаю условия соглашения» и нажать «Далее»:



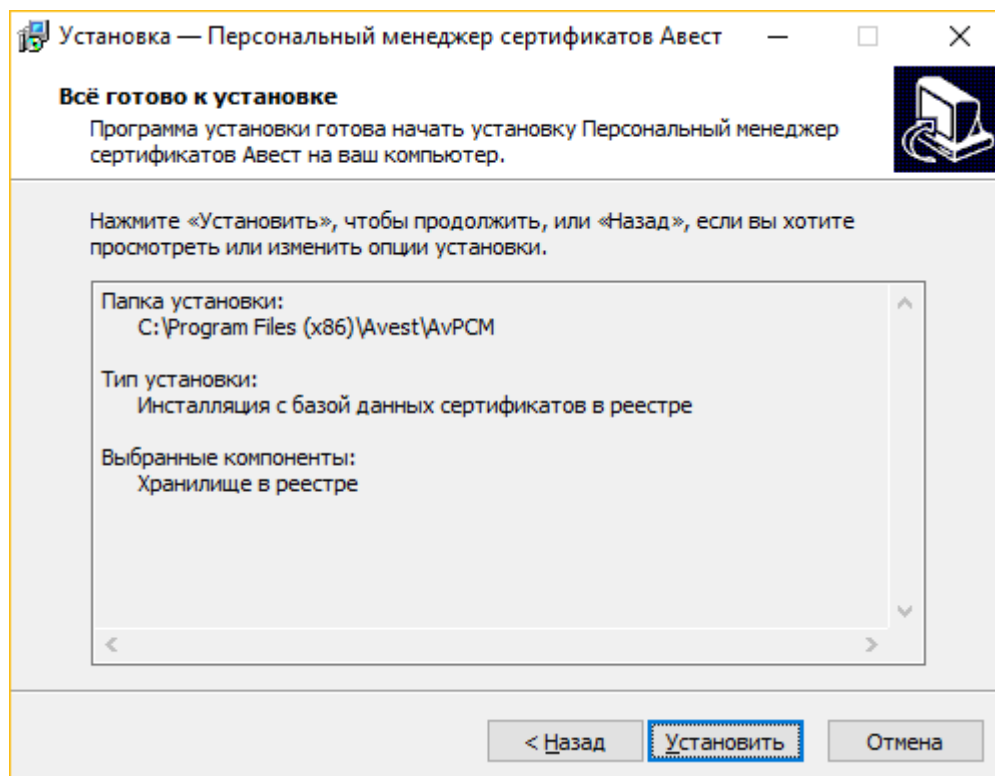
Повторно нажать «Далее»:



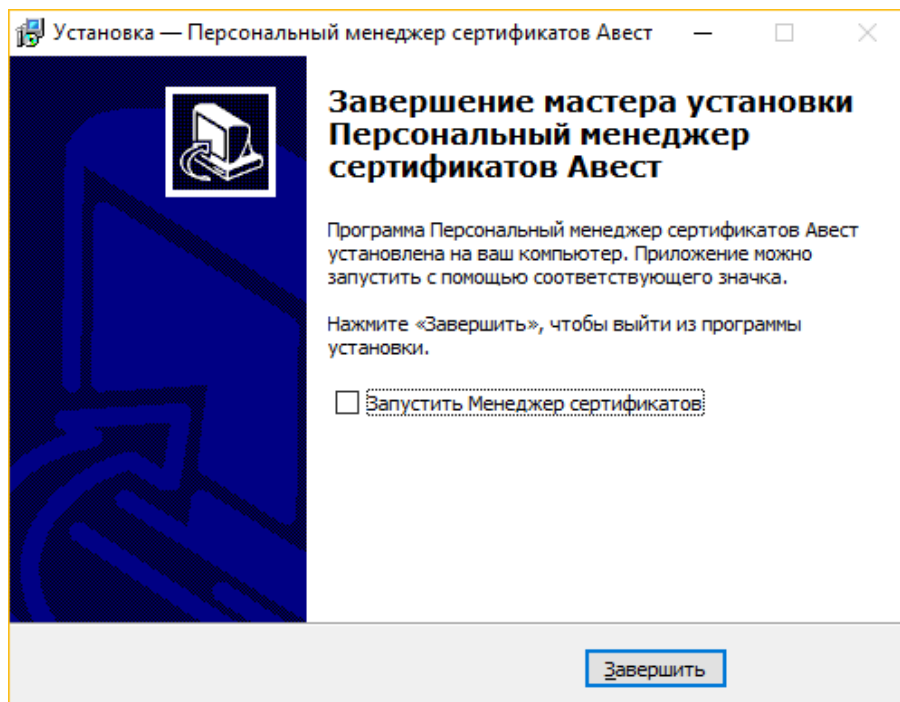
В следующем окне выбрать Инсталляция с базой данных сертификатов в реестре:



и нажать «Установить»:

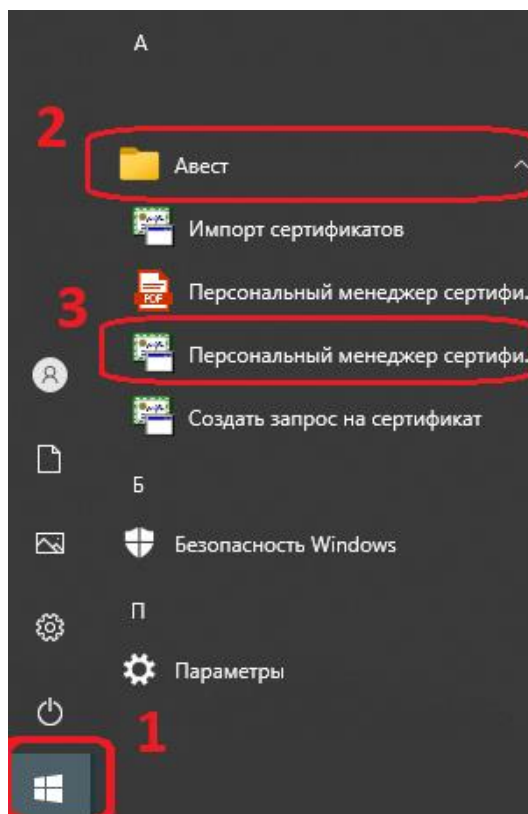


В случае успешного завершения установки ПК AvPCM на экране появится окно с сообщением о выполненной инсталляции. После чего необходимо нажать кнопку «Завершить».



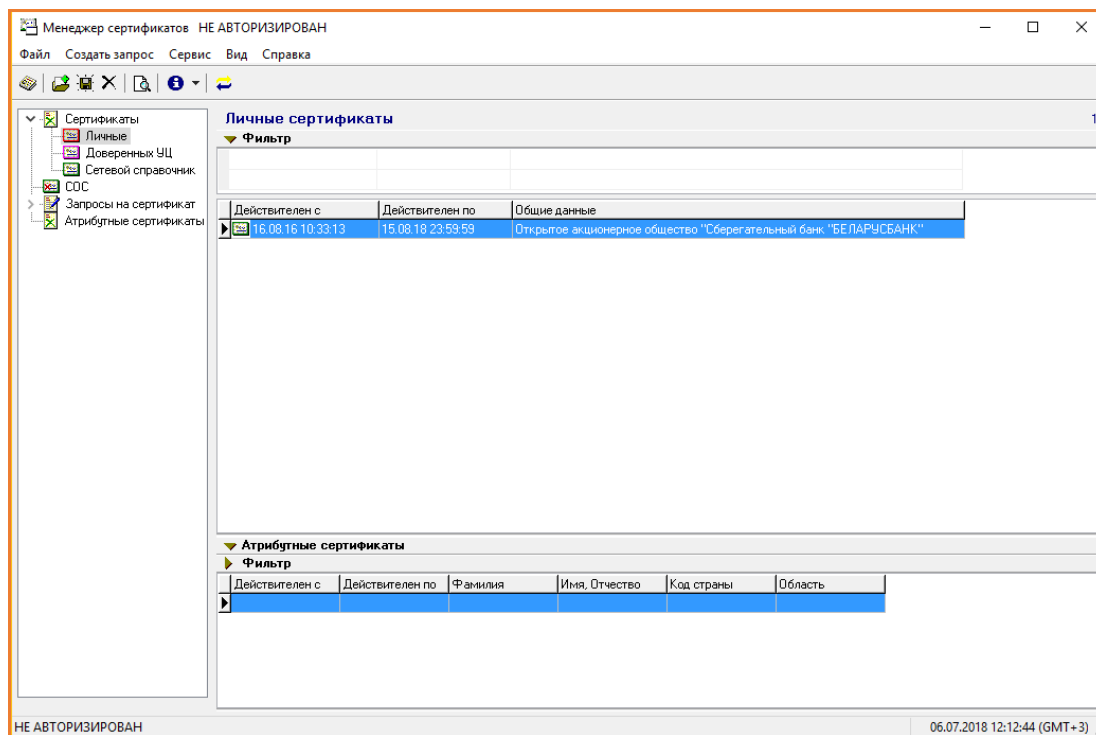
Далее необходимо открыть Персональный менеджер сертификатов через меню «Пуск» Windows:

**Пуск – Авест – Персональный менеджер сертификатов:**



В Персональном менеджере сертификатов через меню **Файл - Импорт сертификата/СОС** необходимо импортировать все сертификаты ГосСУОК, полученные от Банка по электронной почте (\*.p7b).

После их импорта должен появиться сертификат в разделе **Сертификаты – Личные** (см. рис):

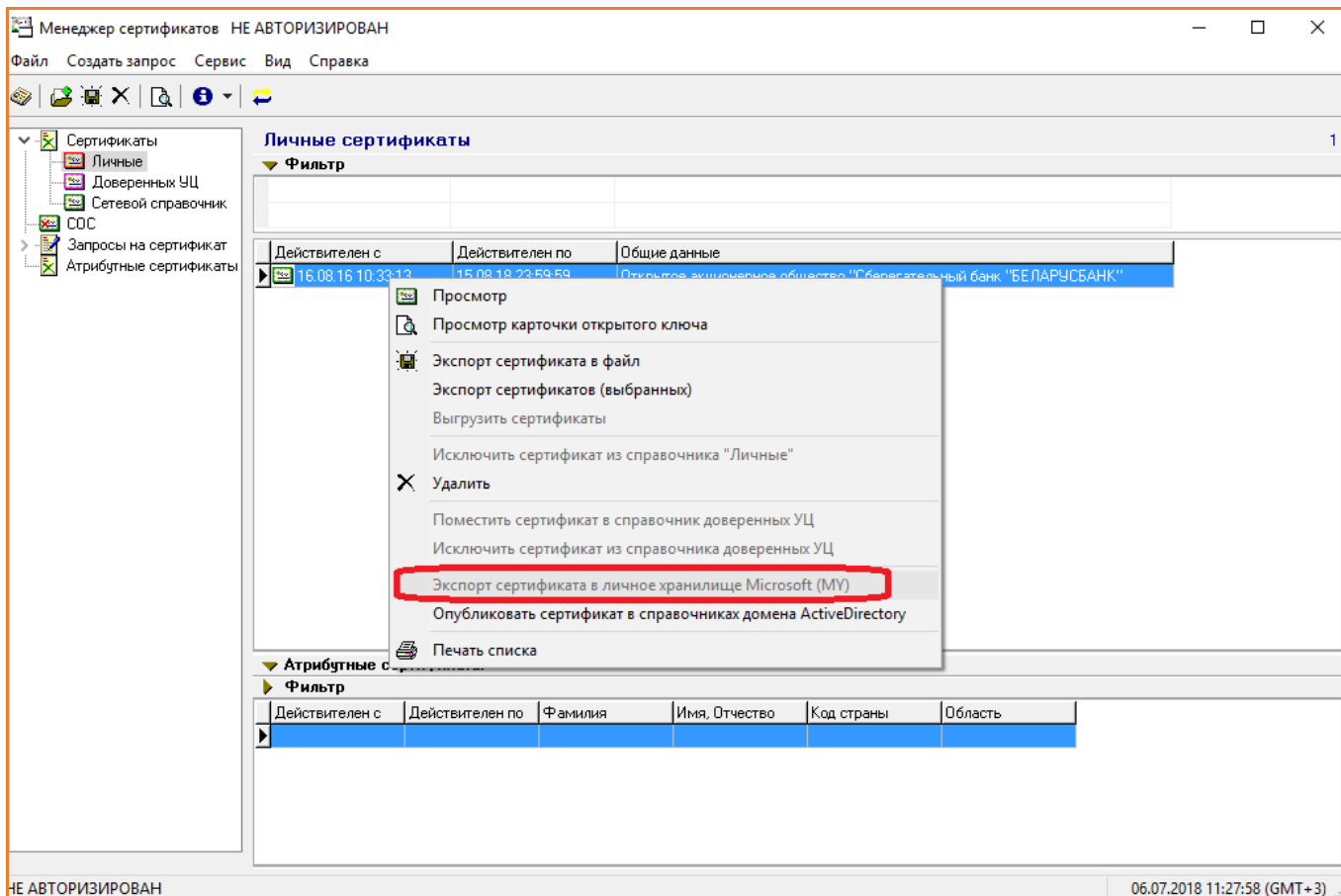


Затем следует загрузить актуальные СОС (списки отозванных сертификатов) через меню Персонального менеджера сертификатов (необходимо подключение к Интернету):

### **Сервис – Обновление СОС и сертификатов УЦ**

В появившемся окне нажать «Далее» и подождать, пока завершится загрузка СОС.

Затем в Персональном менеджере сертификатов выбрать **Сертификаты – Личные**. Нажать правой кнопкой мыши на сертификате и выберите пункт **Экспорт сертификата в личное хранилище Microsoft (MY)** – см. рисунок ниже.

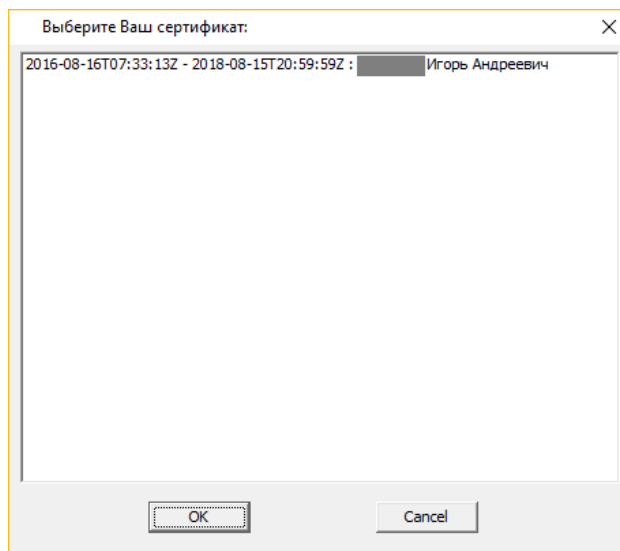


Настройка Персонального менеджера сертификатов Авест завершена.



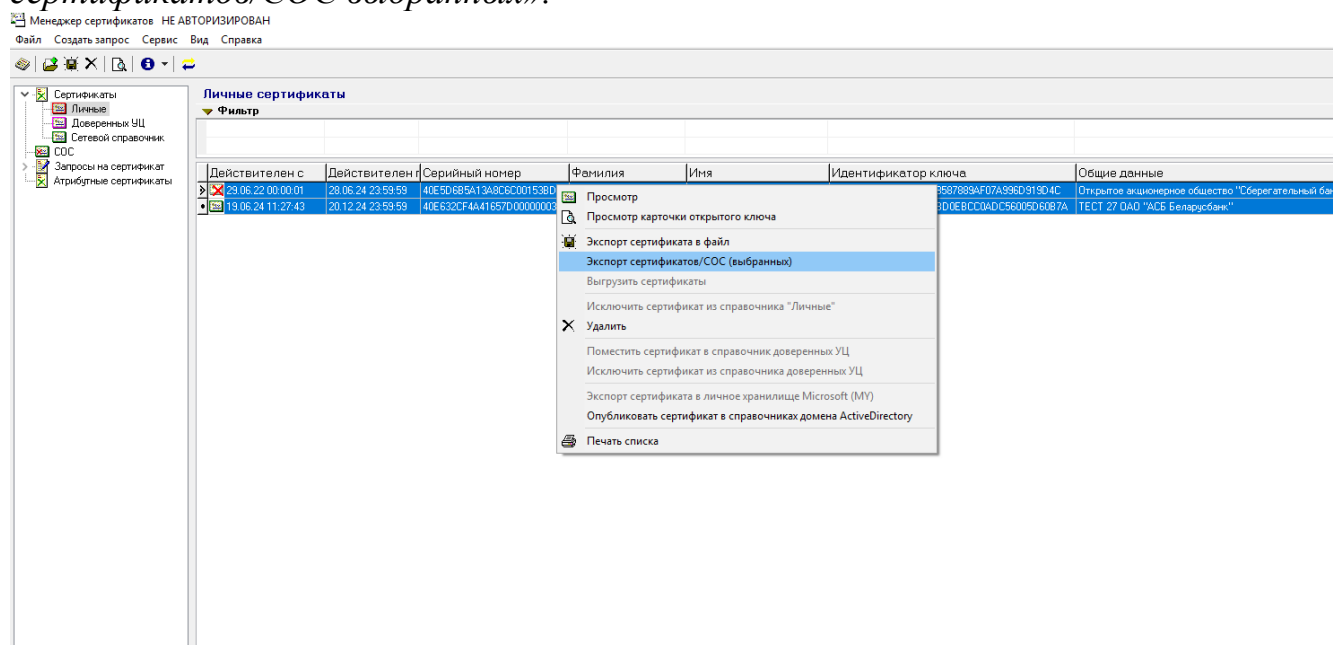
### 3.3. Настройка КП СОБ (Cryptoservice) для работы с ключом ГосСУОК.

Поместить носитель с ключом ГосСУОК (AvPass) в USB-порт, запустить утилиту **USBKeyPairs** из папки **C:\CryptoServiceASB\CryptoServiceASB\USBKeyPairs** (или **D:\CryptoServiceASB\CryptoServiceASB\USBKeyPairs**) – появится окно с сертификатом (сертификатами) пользователя. Выбрать в списке сертификат, парный Технологическому ключу, находящемуся на носителе AvPass, и нажать клавишу ОК.



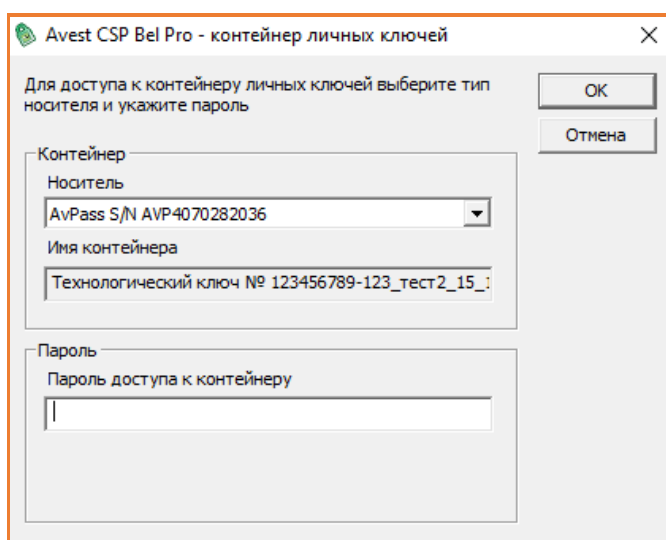
*Примечание:* Если в Usbkeypairs присутствует более 1 сертификата в списке – может возникнуть Ошибка при нажатии кнопки «ОК».

*Решение:* Запустите Персональный менеджер сертификатов Авест без авторизации (Пуск – Авест – Персональный менеджер сертификатов) и откройте раздел Личные. Выделите все сертификаты и нажмите «Экспорт сертификатов/СОС выбранных».

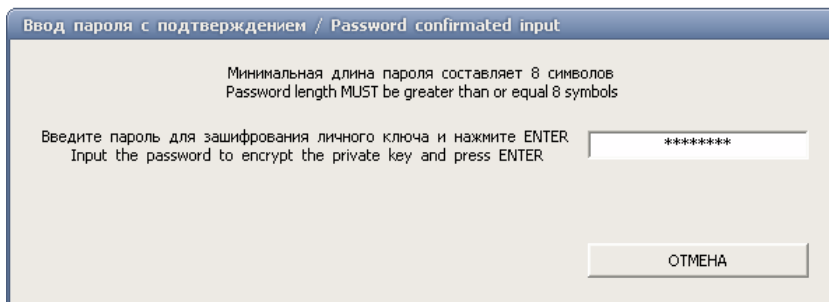


Сохраните сертификаты в любую папку. После экспорта необходимо из раздела Личные удалить (временно) ВСЕ сертификаты за исключением сертификата, который используется для входа в ПК «Студенческая карта». Далее снова запустить Usbkeypairs, выбрать единственный сертификат и нажать «ОК». При необходимости после работы с Usbkeypairs снова импортируйте другие Ваши сертификаты в Персональный менеджер сертификатов.

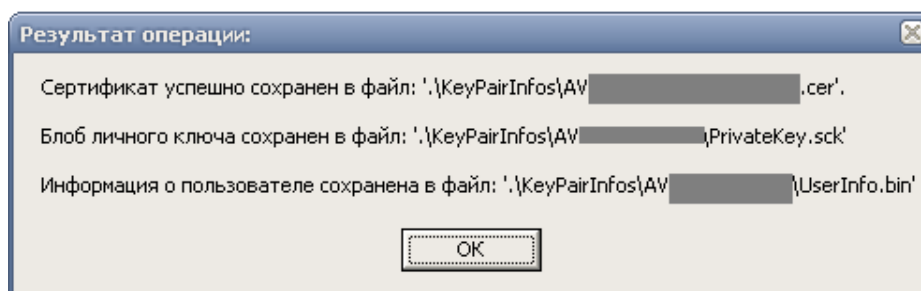
По выбранному сертификату производится поиск ключевого контейнера на устройстве. При успешном поиске откроется окно от криптопровайдера Avest CSP Bel, где нужно выбрать используемый носитель и ввести пароль доступа к ключевому контейнеру носителя, после чего нажать «ОК»:




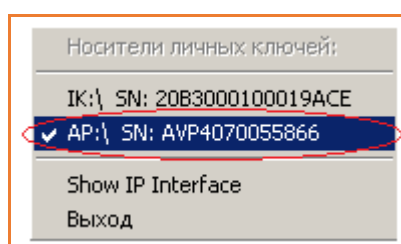
Для дальнейшей работы КП СОБ (Cryptoservice) с ключом ГосСУОК необходимо в следующем открывшемся окне ввести **тот же пароль**, что и пароль доступа к ключевому контейнеру носителя:



После подтверждения ввода пароля в следующем открывшемся окне нажать кнопку «ОК»:



Нажать правой кнопкой мыши по иконке приложения ssf-server «» и выбрать носитель AvPass (AP:\):




Теперь все готово для работы в ПК «Студенческая карта» с ключом ГосСУОК.

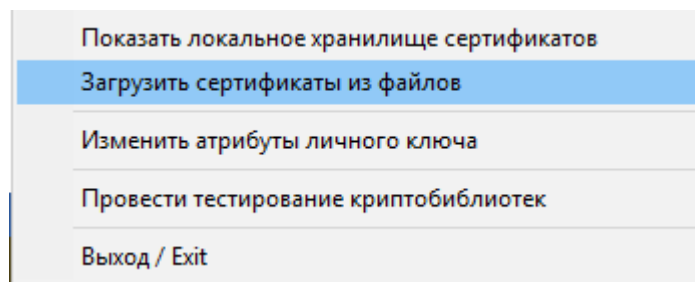
**При возникновении вопросов по установке или эксплуатации КП СОБ (Cryptoservice) необходимо обращаться в Службу поддержки пользователей ОАО «АСБ Беларусбанк» по телефону (017) 309-04-04.**

### 3.4 Загрузка сертификатов в КП СОБ (Cryptoservice) (необязательный пункт)

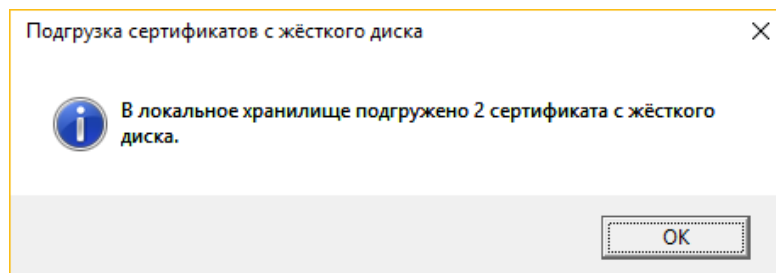
Все сертификаты ГосСУОК, полученные от Банка по электронной почте в формате \*.p7b либо \*.cer, необходимо сохранить в каталог:

**C:\CryptoServiceASB\CertificateStorage\ForCertificatesLoading\  
(или D:\CryptoServiceASB\CertificateStorage\ForCertificatesLoading\)**

Затем нажать правой клавишей мыши на иконке КП СОБ (Cryptoservice) «» и выбрать меню «Загрузить сертификаты из файлов»:



После этого должно появиться сообщение:



Сертификаты успешно загружены.